RQF LEVEL 5

NITCS501

NETWORKING AND INTERNET TECHNOLOGIES

Cyber Security

TRAINER'S MANUAL

October, 2024

CYBER SECURITY

KOICA
Korea International Cooperation Agency

TQUM
TVET Quality Management Project

2024

AUTHOR'S NOTE PAGE (COPYRIGHT)

Copies available from:

- *HQs: Rwanda TVET Board-RTB*
- *Web: www.rtb.gov.rw*
- **KIGALI-RWANDA**

Original published version: October 2024

ACKNOWLEDGEMENTS

The publisher would like to thank the following for their assistance in the elaboration of this training manual:

Rwanda TVET Board (RTB) extends its appreciation to all parties who contributed to the development of the trainer's and trainee's manuals for the TVET Certificate V in Networking and Internet Technologies, specifically for the module "NICS501: CYBER SECURITY".

We extend our gratitude to KOICA Rwanda for its contribution to the development of these training manuals and for its ongoing support of the TVET system in Rwanda.

We extend our gratitude to the TQUM Project for its financial and technical support in the development of these training manuals.

We would also like to acknowledge the valuable contributions of all TVET trainers and industry practitioners in the development of this training manual.

The management of Rwanda TVET Board extends its appreciation to both its staff and the staff of the TQUM Project for their efforts in coordinating these activities.

This training manual was developed:

Under Rwanda TVET Board (RTB) guiding policies and directives

Under Financial and Technical support of

COORDINATION TEAM

RWAMASIRABO Aimable
MARIA Bernadette M. Ramos
MUTIJIMA Asher Emmanuel

PRODUCTION TEAM

Authoring and Review

HANYURWIMFURA Dieudonne

NEMEYIMANA Jean Baptiste

Validation

TUYIZERE Vital

MANISHIMWE Yves

HABIYAMBERE Daniel

Conception, Adaptation and Editorial works

HATEGEKIMANA Olivier

GANZA Jean Francois Regis

HARELIMANA Wilson

NZABIRINDA Aimable

DUKUZIMANA Therese

NIYONKURU Sylvestre

BYUKUSENGE Protais

Formatting, Graphics, Illustrations, and infographics

YEONWOO Choe
SUA Lim
SAEM Lee
SOYEON Kim
WONYEONG Jeong
MANISHIMWE Marc

Financial and Technical support

KOICA through TQUM Project

TABLE OF CONTENT

AUTHOR'S NOTE PAGE (COPYRIGHT)---iii
ACKNOWLEDGEMENTS---iv
TABLE OF CONTENT ---vii
ACRONYMS---ix
INTRODUCTION ---1
MODULE CODE AND TITLE: NITCS501_CYBER SECURITY ---2
Learning Outcome 1: Assess Security Risks and Vulnerabilities---3
Key Competencies For Learning Outcome 1: Assess Security Risks And Vulnerabilities---4
Indicative content 1.1: Introduction to Cyber Security---6
Indicative content 1.2: Describe Cyber Threats---9
Indicative content 1.3 Describe Cyber Vulnerabilities---11
Indicative content 1.4: Cyber Attacks and Techniques ---13
Indicative content 1.5: Identification of Asset in Cyber security ---15
Indicative content 1.6: Definition of Security Policies and Frameworks ---18
Indicative content 1.7: Cyber security Frameworks and Standards ---20
Indicative content 1.8: Identification of security risks and Vulnerability---23
Learning outcome 1: End assessment---28
Further information to the trainer---34
Learning Outcome 2: Implement Security Measures---35
Learning Outcome 2: Implement Security Measures---35
Key Competencies For Learning Outcome 2: Implement Security Measures ---36
Indicative content 2.1: Implementation of Access Control Mechanisms ---40
Indicative content 2.2: Implementation of User Authentication Mechanisms ---43
Indicative content 2.3: Implementation of Authorization Mechanisms---48
Indicative content 2.4: Description of implementation of Access Request and Approval Workflow. ---52
Indicative content 2.5: Deployment of Firewalls and IDS/IPS ---55
Indicative content 2.6: Isolate Critical Systems ---59
Indicative content 2.7: Encrypt Sensitive Data for Protection---64
Indicative content 2.8: Management of encryption keys---71
Indicative content 2.9: Update Endpoint Security for maintenance ---73

Indicative content 2.10: Implement Device Management Policies ---- 76
Indicative content 2.11: Apply Security Patches for Security Management ---- 79
Learning outcome 2 end assessment ---- 83
Further information to the trainer ---- 91
Learning Outcome 3: Perform Monitoring and Detection ---- 92
Key Competencies for Learning Outcome 3: Perform monitoring and detection ---- 93
Indicative content 3.1: Security Threats Monitoring ---- 95
Indicative content 3.2: Applying Monitoring Techniques and Threat Intelligence ---- 99
Indicative content 3.3: Conducting Methodical Threat Hunting with Intelligence Feeds 102
Indicative content 3.4: Monitoring Network and System Logs ---- 105
Indicative content 3.5: Systems Scanning and Penetration Testing ---- 110
Learning outcome 3 end assessment ---- 114
Further information to the trainer ---- 121
Learning Outcome 4: Perform Incident Response and Recovery ---- 122
Key Competencies For Learning Outcome 4: Perform Incident Response And Recovery 123
Indicative content 4.1: Developing Incident Response Plan ---- 127
Indicative content 4.2: Developing Incident Recovery Plan ---- 132
Indicative content 4.3: Identification of Security Incident ---- 136
Indicative content 4.4: Isolation of Affected System ---- 142
Indicative content 4.5: Conducting Methodical Forensic Analysis ---- 146
Indicative content 4.6: Restoring System and Data ---- 152
Learning outcome 4 end assessment ---- 157
Further information to the trainer ---- 165

ACRONYMS

ACL: Access Control List

BIA: Business Impact Analysis

CIA: Confidentiality, Integrity, and Availability

DAC: Discretionary Access Control

DDoS: Distributed Denial of Service

DR/BCP: Disaster Recovery/Business Continuity Planning

GDPR: General Data Protection Regulation

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection System

IoC: Indicator of Compromise

IPS: Intrusion Prevention System

ISAKMP: Internet Security Association and Key Management Protocol

ISO: International Organization for Standardization.

MAC: Mandatory Access Control

MFA: Multi-Factor Authentication

NIST: National Institute of Standards and Technology

NMAP: Network Mapper

RBAC: Role-based Access Control

RPO: Recovery Point Objective

RTB: Rwanda TVET Board

RTO: Recovery Time Objective

SFA: Single Factor Authentication

SIEM: Security Information and Event Management

SSL: Secure Sockets Layer

SSO: Single Sign-On

TLS: Transport Layer Security

TQUM Project: TVET Quality Management Project

INTRODUCTION

This trainer's manual encompasses all methodologies necessary to guide you to properly deliver the module titled: **Cyber security**. Students undertaking this module shall be exposed to practical activities that will develop and nurture their competences. The writing process of this training manual embraced Competency-Based Training (CBT) philosophy by providing enough practical opportunities reflecting real life situations.

The trainer's manual is subdivided into Learning Outcomes, each learning outcome has got various topics, you will start guiding a self-assessment exercise to help students rate themselves on their level of skills, knowledge and attitudes about the unit. The trainer's manual will give you the information about the objectives, learning hours, didactic materials, proposed methodologies and crosscutting issues.

A discovery activity is followed to help students discover what they already know about the unit.

This manual will give you tips, methodologies and techniques about how to facilitate students to undertake different activities as proposed in their trainee's manuals. The activities in this training manual are prepared such that they give opportunities to students to work individually and in groups. After going through all activities, you shall help students to undertake progressive assessments known as formative and finally facilitate them to do their self-reflection to identify your strengths, weaknesses and areas for improvements. Remind them to read the point to remember section which provides the overall key points and takeaways of the unit.

MODULE CODE AND TITLE: NITCS501_CYBER SECURITY

Learning Outcome 1: Assess Security Risks and Vulnerabilities
Learning Outcome 2: Implement Security Measures
Learning Outcome 3: Perform Monitoring and Detection
Learning Outcome 4: Perform Incident Response and Recovery


******
OK

Indicative contents

1.1 Introduction to Cyber Security
1.2 Describe Cyber Threats
1.3 Describe Cyber Vulnerabilities
1.4 Cyber Attacks and Techniques
1.5 Identification of Asset in Cyber security
1.6 Definition of Security Policies and Frameworks
1.7 Cyber security Frameworks and Standards
1.8 Identification of security risks and Vulnerability

Key Competencies For Learning Outcome 1: Assess Security Risks And Vulnerabilities

Knowledge	Skills	Attitudes
• Description of Cyber Security. • Description of cyber threats. • Description of Cyber Vulnerabilities and risks. • Identification of Cyber Attack and Techniques. • Classification of assets used in cyber security. • Identification of Security Policies, Frameworks and Standards.	• Analyzing Common Cyber Attack and Techniques. • Assessing security risks • Reporting security issues based to Security Assessment	• Having team spirit while working with others. • Being responsible. • Being organized to achieve the required result. • Having Curiosity. • Being Accountable • Being resilience. • Attention to details

Duration: 20hrs

Learning outcome 1 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe clearly cyber security based on security policies.
2. Describe correctly Cyber threats in cyber security.
3. Describe correctly the cyber vulnerabilities and risks in cyber security.
4. Identify properly Cyber-attacks and techniques in cyber security.
5. Identify correctly cyber security assets based on types and valuation.
6. Describe properly Security Policies, Frameworks and Standards in Cyber security.
7. Identify correctly Vulnerability and security risks according to the security
8. Assess correctly vulnerability in Cyber security.
9. Report correctly security issues based to Security Assessment

Resources

Equipment	Tools	Materials
• Computers	• Wireshark • Nessus • NMAP • OpenVAS • Air crack	• Internet

Advance Preparation:

Before delivering this learning outcome, you are recommended to:

- Avail tools, materials and equipment of cyber security.
- To have a computer with Wireshark installed
- Avail internet connection.

Indicative content 1.1: Introduction to Cyber Security

Duration: 2 hrs

Theoretical Activity 1.1.1: Description of Cyber Security.

Notes to the trainer:

- Trainer may use small group to describe cyber security

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and request trainees to answer the following questions:

i. Describe cyber security.
ii. What are the difference between cyber threats and attacks?
iii. Give importance of cyber security in the digital age
iv. Discuss The evolving landscape of cyber threats
v. Discuss on key terminology and concepts of cyber security such as Threat, Vulnerability, Attack, Malware, Phishing, Ransomware, Firewall, Encryption, Authentication, Intrusion Detection System (IDS), Security Incident, Cybersecurity Policy.
vi. What is confidentiality, integrity, and availability (CIA triad)
vii. What are Cyber security roles and responsibilities

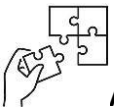
Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns

Step 5: Ask trainee to read the Key readings 1.1.1 in trainee's manuals

Points to Remember

- **Cybersecurity** refers to the practice of protecting systems, networks, and programs from digital attacks, theft, and damage
- **Cyber threats** are potential dangers arising from vulnerabilities in computer systems, networks, or digital infrastructures, often involving hacking, malware, and data breaches. While **Cyber-attacks** are deliberate, malicious actions that exploit these vulnerabilities to steal data, disrupt operations, or gain unauthorized access.

- Importance of cyber security in the digital age are Protection of Sensitive Information, Prevention of Financial Loss, Preservation of Privacy, Maintenance of Trust and Reputation, Business Continuity and Operational Resilience, Compliance with Regulations and Legal Requirements, Protection Against Emerging Threats.
- The cyber threat landscape is constantly evolving due to technological advancements, shifting cybercrime tactics, and geopolitical factors, with threats like APTs, ransomware, and supply chain attacks becoming more sophisticated. The rise of IoT and operational technology systems has expanded the attack surface, while social engineering tactics continue to exploit human vulnerabilities
- Cyber security key terminology and concepts are Threat, Vulnerability, Attack, Malware, Phishing, Ransomware, Firewall, Encryption, Authentication, Intrusion Detection System (IDS), Security Incident, Cybersecurity Policy
- The CIA triad provides a framework for addressing key objectives in cyber security: maintaining confidentiality to protect sensitive information, preserving integrity to ensure data accuracy and trustworthiness, and maximizing availability to ensure timely access to resources and services.
- Cyber security roles and responsibilities are diverse and multifaceted, encompassing various functions such as strategy development, risk management, incident response, security operations, architecture design, compliance, and awareness training



Application of learning 1.1.

GOLI School is an educational institution. As part of the IT security team at GOLI School, which uses an IoT-based facial recognition system to manage child pickups, you have recently received reports of suspicious activity. The school administration has asked you to provide basic information on cyber threats and attacks, the importance of cybersecurity in the digital age, the evolution of the cyber threat landscape, key cybersecurity terminology and concepts, the CIA triad, and cybersecurity roles and responsibilities for each user.

Checklist:

Main point to check	Observation	
	Yes	No
Basic cyber threats and attacks are well mentioned		
The importance of cybersecurity in the digital age is clearly explained		
The evolution of the cyber threat landscape is well discussed		
The cyber threat landscape is well explained		
Key cybersecurity concepts (CIA triad: Confidentiality, Integrity, Availability) are well applied		
Roles and Responsibilities for each user are well indicated		

Indicative content 1.2: Describe Cyber Threats

Duration: 2 hrs

Theoretical Activity 1.2.1: Description of cyber threats

Notes to the trainer:

- Trainer may use small group to discuss on Description to cyber threats.
- Prepare practical examples of common cyber threats in cyber security

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions:

i. Define Cyber Threats
ii. Give importance of Cyber Threat Awareness
iii. What is Evolving Landscape of Cyber Threats?
iv. Identify Types of Cyber Threats

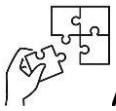
Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns

Step 5: Ask trainees to read the Key readings 1.2.1 in their manuals

Points to Remember

- Cyber threats refer to malicious activities or risks aimed at exploiting vulnerabilities in computer systems, networks, and data
- Importance of cyber threat awareness are Risk Mitigation, Vulnerability Awareness, Prevention of Attacks, Data Protection, Business Continuity, Financial Loss Prevention and Protecting Personal Privacy.
- The landscape of cyber threats is continuously evolving due to advancements in technology, changes in attacker tactics, and the expanding attack surface

- Types of Cyber Threats are Malware Threats Viruses, Worms and Trojans, Phishing Attacks, Ransomware Threats, DDoS (Distributed Denial of Service) Attacks, Insider Threats, Social Engineering Attacks and Zero-Day Exploits.



Application of learning 1.2.

H.D Company Ltd has experienced unusual network activity and Unusual Traffic. As you are a cybersecurity analyst, you are tasked to Describe of Cyber Threats, explain Importance of Cyber Threat Awareness, describe evolving Landscape of Cyber Threats and explain all cyber threats and damage they can course to computer systems.

Checklist:

Main points to check	Observation	
	Yes	No
Description of cyber threats is well explained		
Importance of cyber threat awareness is clearly highlighted		
The evolving landscape of cyber threats is discussed (new threats, increased sophistication, etc.)		
Types of cyber threats encountered are well described		
The potential damage cyber threats can cause to computer systems is explained		

Indicative content 1.3 Describe Cyber Vulnerabilities

Duration: 2 hrs

Theoretical Activity 1.3.1: Description of Cyber Vulnerabilities.

Notes to the trainer:

- Trainer may use a small group to discuss of Cyber Vulnerabilities in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to discuss on the following question:

i. Describe vulnerability system in cyber security
ii. Describe significance for identifying vulnerabilities in Cyber security
iii. Differentiate Software from Hardware vulnerabilities.
iv. Discuss on Common Vulnerabilities (Misconfigured Security Settings, Unpatched Software, Weak Passwords and Authentication, Lack of Encryption, Inadequate Access Controls, Software and Hardware Flaws)

Step 2: Ask trainees to present their findings on front of class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 1.3.1 in their manuals

Points to Remember

- Vulnerabilities in cybersecurity refer to weaknesses or flaws in computer systems, networks, software, or hardware that can be exploited by attackers to compromise security
- Identifying vulnerabilities in cybersecurity is crucial as it allows organizations to proactively address potential weaknesses in their systems, networks, and software before they can be exploited by attackers
- Software vulnerabilities often result from coding errors, design flaws, or insecure configurations, while hardware vulnerabilities may arise from design defects, backdoors, or firmware weaknesses.

- Common Vulnerabilities are Misconfigured Security Settings, Unpatched Software, Weak Passwords and Authentication, Lack of Encryption, Inadequate Access Controls Software and Hardware Flaws

Application of learning 1.3.

A GT healthcare organization has experienced a significant data breach, exposing sensitive patient information to unauthorized individuals. Upon investigation, it becomes apparent that a combination of security vulnerabilities and misconfigurations allow the attackers to gain access to the network and exfiltrate data. You are requested by CEO to Describe Vulnerabilities, Provide Significance of Identifying Vulnerabilities, Explain Common Vulnerabilities Software and Hardware Vulnerabilities and highlight impact of vulnerabilities on patient data and healthcare operations.

Checklist:

Main points to check	Observation	
	Yes	**No**
Vulnerabilities are clearly described		
Significance of identifying vulnerabilities is well explained (importance of proactive measures)		
Software vulnerabilities are explained (e.g. outdated systems, unpatched software)		
Hardware vulnerabilities are described (e.g.insecure physical devices, lack of encryption)		
Common software vulnerabilities are identified (e.g., buffer overflows, SQL injection, cross-site scripting)		
Common hardware vulnerabilities are identified (e.g., unprotected devices, weak access control)		
Impact of vulnerabilities on patient data and healthcare operations is highlighted		

Indicative content 1.4: Cyber Attacks and Techniques

Duration: 2 hrs

Theoretical Activity 1.4.1: Identification of Cyber Attack and its Techniques

Notes to the trainer:

- Trainer may use a small group to discuss on Identification of Cyber Attack and Techniques in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to discuss on:

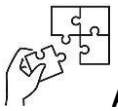
i. Definition of Cyber Attacks
ii. What are Goals, Objectives and motivation Behind Cyber Attacks
iii. Explain Common Cyber Attack Techniques (Malware Attacks, Social Engineering Attacks, Web Application Attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, Insider Attacks, SQL Injection Attack)

Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 1.4.1 in their manuals

Points to Remember

- Cyber-attacks refer to malicious activities or actions carried out by individuals or groups with the intent to compromise the security, integrity, or availability of computer systems, networks, or data
- Cyber Attacks Goals, Objectives and Motivations Behind Cyber Attacks are Financial Gain, Espionage and Intelligence Gathering, Political or Ideological Motives, Disruption and Sabotage, Personal Vendettas or Revenge and Curiosity or Challenge

- Common Cyber Attack Techniques are Malware Attacks, Social Engineering Attacks, Web Application Attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, Insider Attacks, SQL Injection Attacks and Zero-Day Exploits



Application of learning 1.4.

An international financial services firm, XYZ Financial, has recently been hit by a series of cyber-attacks targeting its internal systems and customer data. Upon further investigation, it was discovered that the attackers employed a range of sophisticated techniques, leading to significant disruption in services and potential data compromise. The company's leadership has asked you to provide a comprehensive overview of the nature of cyber-attacks, their goals, motivations, and common techniques used by attackers.

Checklist:

Main Points to Check	Observation	
	YES	NO
Cyber-attacks are clearly described		
Goals, objectives, and motivations behind cyber-attacks are well identified		
Impact of cyber-attacks on the organization's operations and customer data is clearly identified		
Common cyber-attack techniques are covered		
SQL injection attack is well identified		
Insider threat is well identified		
Zero-day exploit is well identified		
Web application vulnerabilities are well understood		

Indicative content 1.5: Identification of Asset in Cyber security

Duration: 4 hrs

Theoretical Activity 1.5.1: Classification of assets used in cyber security.

Notes to the trainer:

- Trainer may use a small group to Classify assets used in cyber security.
- Trainer may use video to show assets in cyber security

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer on:

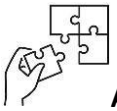
i. Define Assets in the context of cyber security
ii. What are Importance of identifying and protecting assets
iii. What is The role of assets in risk assessment and risk management?
iv. Differentiate Types of Cyber Security Assets
v. Describe Cyber Security Asset Valuation
vi. Identify Data Security as the most sensitive asset

Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 1.5.1 in trainee's manuals

Points to Remember

- Definition Assets in the context of Cyber security: Refer to any resources or entities that have value and are critical to the operations and security of an organization.
- Importance of identifying and protecting assets: Identifying and protecting assets is fundamental to help organizations safeguard their information, maintain operational efficiency, and manage risks effectively like Mitigates Risks, Ensures Compliance, Optimizes Resource Management and Protects Sensitive Information etc..

- The role of assets in risk assessment and risk management: Identifying Risks, Evaluating Impact, Assessing Threats and Vulnerabilities, Implementing Controls, Monitoring and Maintenance, Risk Mitigation Strategies and Documentation and Reporting.
- Types of Cyber Security Assets Are Digital assets, Physical assets, Human assets, Intellectual property assets and Reputation assets
- Methods for assigning value to cyber security assets: Is a critical step in effective risk management and resource allocation using Quantitative Methods, Qualitative Methods and Hybrid Methods.
- Considerations for determining the value of assets in different contexts : Determining the value of cybersecurity assets involves multiple considerations based on the business, regulatory, security, operational, intellectual property, human resource, and reputation contexts.
- The impact of asset valuation on risk assessment and resource allocation: It helps prioritize risks, allocate budgets and resources appropriately, and make informed decisions about security measures and incident response. By understanding the value of assets, organizations can ensure that their cybersecurity efforts are aligned with their strategic objectives and that critical assets receive the protection and resources they need to mitigate risks effectively.
- Definition of data Security Refers to the practices, technologies, and policies designed to protect data from unauthorized access, corruption, or theft throughout its lifecycle. Data that is stored on physical media or in databases and is not actively being accessed or transmitted.



Application of learning 1.5.

As part of your cybersecurity training, you are required to identify and evaluate the various types of assets within an organization. Your job is to analyze the assets in the context of cybersecurity, determine their importance, and suggest ways to protect them. You will also be expected to assess the value of these assets and how they impact the overall risk management strategy of the organization. Pay special attention to data security, as it is considered the most sensitive asset, and consider any special challenges related to big data.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	1. Asset in Cyber security are well identified	**A. Cyber security Assets is well introduced**		
		1. Cybersecurity assets are defined		
		2. Importance of asset identification are indicated		
		3. Assets' role in risk assessment and management is understood		
		B. Types of Cyber security Assets		
		1. Digital assets are identified and protected		
		2. Physical assets are identified and protected		
		3. Human assets are identified and protected		
		4. Intellectual property assets are identified and protected		
		5. Reputation assets are identified and protected		
		C. Cyber security Asset is well valued		
		1. Asset valuation methods are understood and applied		
		2. Asset valuation impacts risk assessment and resource allocation		
		D. The most sensitive asset is well identified		
		1. Data security as the most sensitive asset is well understood		
		2. Data states (rest, transit, in use) are clearly identified		
		3. Data security controls are implemented		
		4. Special security considerations for big data are applied		

Indicative content 1.6: Definition of Security Policies and Frameworks

Duration: 2 hrs

Theoretical Activity 1.6.1: Identification of Security Policies and Frameworks

Notes to the trainer:

- Trainer may use a small group to identify Security Policies and Frameworks.
- Trainer may use Security policies and frameworks documentation

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to discuss on:

i. Describe Data Security Policies
ii. What are Data Security Roles for Data Governance and Data Privacy Principles

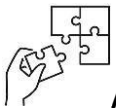
Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 1.6.1 in their manuals

Points to Remember

- Data Security Policies: These are guidelines that help protect sensitive information from unauthorized access, changes, or theft. They cover different aspects of how data should be handled, including how it is classified, stored, and transmitted. The goal of these policies is to make sure that data is secure at all times and that only authorized people can access or modify it.
- Data Classification Policies focus on sorting data into categories like public, private, or confidential, to determine how sensitive it is and how it should be protected, Data Storage Policies ensure data is safely stored, whether on physical devices or in the cloud, using methods like encryption and regular backup, Data Transmission Policies make sure data is protected when being sent over the internet or other networks, usually by using encryption or secure connections.
- Data governance in Cyber security: Refers to the management of data availability, usability, integrity, and security within an organization, data governance involves

the implementation of policies, procedures, and controls to ensure that data is protected from unauthorized access, misuse, or loss while maintaining compliance with relevant laws and regulations.

- Data privacy principles: Refers to the protection of personal information and ensuring that individuals' data is collected, processed, and stored in a manner that respects their privacy rights. Data privacy principles guide organizations in handling personal data responsibly and in compliance with privacy laws and regulations.



Application of learning 1.6.

DTech Corporation has experienced a significant data breach, exposing sensitive customer information to unauthorized individuals. Upon investigation, it becomes apparent that a combination of weak data management policies and practices allow the attackers to gain access to the data. So, as a Cyber security admin identify root because risks related to data management.

Checklist:

Main point to check	**Observation**	
	Yes	**No**
Lack of Clear Data Classification Policies is well identified		
Inadequate Data Storage Policies is well identified		
Weak Data Transmission Policies is well identified		
Insufficient Data Lifecycle Policies is well understood		

Indicative content 1.7: Cyber security Frameworks and Standards

Duration: 2hrs

Theoretical Activity 1.7.1: Identification of Security Frameworks and Standards

Notes to the trainer:

- Trainer may use a small group to Identify Security Frameworks and Standards

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer on:

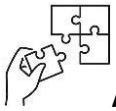
i. What are Importance of Frameworks and Standards
ii. Describe Key Cyber Security Frameworks and their implementation (NIST Cyber security Framework, ISO/IEC 27001 and 27002, Centre for Internet Security CIS Controls)
iii. Describe the following Compliance Standards: GDPR, HIPAA and Industry-specific compliance requirements

Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 1.7.1 in their manuals

Points to Remember

- Importance of Frameworks and standards: Are essential for managing cybersecurity and data protection effectively. They provide structured approaches, best practices, and specific criteria that help organizations implement consistent, effective security measures and organizations can enhance their security posture, ensure compliance, and protect their information assets more effectively.

- NIST Cyber security Framework: Is a set of guidelines developed by the National Institute of Standards and Technology (NIST) to help organizations manage and reduce cybersecurity risk.
- ISO/IEC 27001 and 27002: Are international standards developed by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) that provide a framework for establishing, implementing, maintaining, and improving information security management systems (ISMS).
- Internet Security CIS Controls: Are a set of best practices developed by the Center for Internet Security (CIS) to help organizations improve their cybersecurity posture. The controls are designed to be actionable and provide a prioritized approach to cybersecurity.
- GDPR (General Data Protection Regulation): Provides comprehensive data protection rules for organizations handling personal data of EU citizens, focusing on data subject rights and compliance requirements.
- HIPAA (Health Insurance Portability and Accountability Act): Establishes privacy and security standards for handling health information in the U.S., focusing on protected health information and safeguard requirements.
- Industry-specific compliance requirements: Vary by sector and address unique regulatory and security needs, ensuring organizations meet specific industry standards and regulations.



Application of learning 1.7.

Your task is to evaluate the importance and implementation of cybersecurity frameworks and standards for a given organization. Start by explaining why cybersecurity frameworks and standards are essential for managing risks and ensuring robust security practices. Focus on key frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001 and 27002, and the Centre for Internet Security (CIS) Controls. Assess how each framework can be implemented effectively within the organization. Additionally, review compliance standards such as GDPR, HIPAA, and other industry-specific requirements, noting how they affect the organization's security policies and practices. Prepare a report detailing your findings and recommendations on implementing these frameworks and standards to enhance the organization's cybersecurity posture.

Checklist:

Main Points to Check	Observation	
	YES	NO
Importance of cybersecurity frameworks and standards is explained		
NIST Cybersecurity Framework is accurately described and implementation methods are proposed		
ISO/IEC 27001 and 27002 are accurately described and implementation methods are proposed		
Centre for Internet Security (CIS) Controls are accurately described and implementation methods are proposed		
Compliance standards (GDPR, HIPAA) are clearly reviewed		
Industry-specific compliance requirements are addressed		
Recommendations for implementing frameworks and standards are practical and actionable		

Indicative content 1.8: Identification of security risks and Vulnerability

Duration: 4 hrs

Theoretical Activity 1.8.1: Description of Cyber Vulnerabilities and risks

Notes to the trainer:

- Trainer may use a small group to identify Security Risks and Vulnerabilities Assessment.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answers the following:

i. Describe Security risks and Vulnerabilities assessment
ii. What are Goals and Objective of Assessment
iii. Explain Asset Identification & Classification
iv. What are categories of data
v. Describe Threat Identification
vi. Describe Security risks and Vulnerabilities assessment
vii. What are Goals and Objective of Assessment
viii. Explain Asset Identification & Classification
ix. What are categories of data
x. Describe Threat Identification
xi. What are types of Assessment tools
xii. Explain Vulnerabilities Assessment techniques
xiii. Describe Security assessment techniques
xiv. Explain Risk Assessment Methodologies
xv. Describe Risk Prioritization

Step 2: Ask trainees to present their findings.

Step 3: Provide expert view

Step 4: Address any questions or concerns

Step 5: Ask trainees to read the Key readings 1.8.1 in trainee manuals

Points to Remember

- Security risks and vulnerabilities assessment involves finding and analyzing weaknesses in an organization's systems and data. The goal is to spot these vulnerabilities before attackers can exploit them.
- The main objectives are to identify security gaps, assess potential threats, comply with regulations, and prioritize risks for fixing. This helps protect the organization from potential attacks.
- Asset identification is about recognizing all the valuable resources an organization has, like hardware, software, and data. By classifying and listing these assets, organizations can ensure they are properly protected. Asset management involves keeping track of assets and maintaining their security. Standards like ISO 27001 and NIST help guide this process.
- Data classification involves organizing data based on how sensitive it is and the level of protection it needs. Data can be classified as confidential, sensitive, or public to ensure it is handled securely. Labeling and classification standards help guide how data is stored, accessed, and disposed of. Policies also outline how long data is kept and when it should be securely deleted.
- Threat identification gathers information about potential cyber threats and helps security teams understand who might attack and how. Threat modeling is a way to predict attacks and find ways to protect against them. It involves identifying critical assets, assessing how they might be attacked, and evaluating the risk. Mitigation strategies are then applied to reduce the risks.

Theoretical Activity 1.8.2: Documentation vulnerability assessment report

Notes to the trainer:

- Trainer may use a small group to document vulnerability assessment report

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answers the following:

i. What is assessment report?
ii. What is Risk Register?

iii. Describe Documentation of Assessment reports?
iv. Describe Remediation and Mitigation Strategies?

Step 2: Ask trainees to present their findings.

Step 3: Provide expert view

Step 4: Address any questions or concerns

Step 5: Ask trainees to read the Key readings 1.8.2 in trainee manuals

Points to Remember

- Assessment Reports**:** Detailed documents that summarize the findings of the security assessment, including vulnerabilities, risk levels, and recommended actions.
- Risk Register: A comprehensive log that tracks identified risks, their assessments, and treatment plans. Templates can be used to standardize entries for consistency and clarity.
- Documentation of Assessment Reports**:** Maintaining organized records of all assessments conducted, findings, and remediation efforts helps ensure accountability and provides a reference for future assessments.
- Putting in place necessary security controls, such as firewalls, intrusion detection systems, and access controls, to protect against identified threats.

Practical Activity 1.8.3: Identifying security risks and Vulnerability

Notes to the trainer

- This activity should take place in a computer lab where trainees Identify of security risks and Vulnerability
- Avail computers
- Avail internet
- Avail Protocol analyzers software

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the task and ask trainees to do the task described below:

Schools need to identify the vulnerabilities present in their computer networks and understand the associated risks. Your task is to assess and identify these vulnerabilities along with the potential risks they pose to the network and its data and provide Documentation of Assessment reports.

Step 2: Explain the task and provide clear work instruction (Task, PPE, Time allocated)

Step 3: Demonstrate how to Identify of security risks and Vulnerability. While demonstrating, explain the Identify of security risks and Vulnerability procedures.

Step 4: Asks trainee to Identify of security risks and Vulnerability and monitor the procedures.

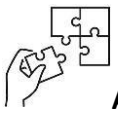
Step 5: Ask trainees to present their findings

Step 6: Address any questions or concerns
Step 7: Ask trainees to read the Key readings 1.8.3 in trainee manuals

Points to Remember

Steps to identify vulnerabilities and risks and document assessment report in the school's computer network.

1. Install and Set Up the Protocol Analyzers
2. Capture Network Traffic
3. Analyze the Captured Traffic
4. Identify Vulnerabilities
5. Assess Corresponding Risks
6. Implement Monitoring
7. Document Vulnerabilities and Risks
8. Provide Remediation Recommendations



Application of learning 1.8.

ZAYO Company has recently faced growing concerns about potential cyber threats, and you have been tasked with conducting a full security assessment, identifying risks, and implementing strategies for remediation and continuous improvement

Checklist:

Main Points to Check	Observation	
	YES	NO
Security Risks and Vulnerabilities Assessment are explained		
Asset Identification and Classification are identified		
Data Classification and Threat are identified Risk Assessment Methodologies are identified		
Risk Prioritization are described		
Security Assessment Reporting and Documentation are reported		
Remediation and Mitigation Strategies are exposed		

Learning outcome 1: End assessment

Theoretical assessment

SECTION I. Choose the letter corresponding to the correct answers

1. The primary purpose of cybersecurity is:

a) To ensure data confidentiality, integrity, and availability
b) To monitor user behaviour online
c) To limit access to the internet
d) To eliminate all threats from the internet

Answer:

A. To ensure data confidentiality, integrity, and availability

2. What is a cyber threat?

a) Any action intended to harm a system
b) A harmless computer bug
c) A computer that is slow to respond
d) A legitimate activity that poses no risk to systems

Answer:

A. Any action intended to harm a system

3. Which of the following is an example of malware?

a) Phishing
b) Trojan
c) Brute force attack
d) Social engineering

Answer:

B. Trojan

4. What type of attack floods a network or server with massive amounts of traffic to disrupt services?

a) SQL Injection
b) Ransomware
c) DDoS (Distributed Denial of Service)
d) Insider Threat

Answer:

C. DDoS (Distributed Denial of Service)

5. Phishing attacks typically aim to do which of the following?

a) Destroy hardware
b) Trick users into revealing personal or sensitive information
c) Encrypt data for ransom
d) Disable system firewalls

Answer:

B. Trick users into revealing personal or sensitive information

6. What is a zero-day exploit?

a) A vulnerability that has been known for years
b) A software flaw that is publicly known and patched
c) A vulnerability that is exploited before the developer is aware of it
d) A virus that attacks zero computers

Answer:

C. A vulnerability that is exploited before the developer is aware of it

7. Which of the following is NOT considered a common cyber vulnerability?

a) Misconfigured security settings
b) High-speed internet connection
c) Weak passwords
d) Unpatched software

Answer:

b. High-speed internet connection

8. Which term refers to an attack where an unauthorized user gains access to sensitive systems?

a) Denial of Service
b) Phishing
c) SQL Injection
d) Social Engineering

Answer:

C. SQL Injection

9. Which of the following assets are considered intellectual property assets?

a) Financial records
b) Patents and trademarks
c) Network infrastructure
d) Physical buildings

Answer:

B. Patents and trademarks

10. Why is it important to identify cyber vulnerabilities?

a) To ensure faster internet speeds
b) To detect and fix weaknesses before they are exploited by attackers
c) To improve user interface design
d) To increase the cost of software development

Answer:

B. To detect and fix weaknesses before they are exploited by attackers

11. What is the primary goal of data security policies?

a) To allow unrestricted access to data
b) To establish guidelines for protecting sensitive data
c) To eliminate the need for data encryption
d) To monitor physical assets only

Answer:

B. To establish guidelines for protecting sensitive data

12. Which of the following describes a ransomware attack?

a) Attackers demand a ransom to unlock encrypted data
b) Attackers overload a system with traffic
c) Attackers inject malicious code into a website
d) Attackers steal hardware

Answer:

A. Attackers demand a ransom to unlock encrypted data

13. Which principle in the CIA triad ensures that data can only be accessed by authorized users?

a) Confidentiality
b) Integrity
c) Availability
d) Accessibility

Answer:

A. Confidentiality

14. What type of cyber attack involves tricking individuals into revealing confidential information through manipulation?

a) Denial of Service (DoS)
b) Ransomware
c) Social Engineering
d) SQL Injection

Answer:

c. Social Engineering

SECTION II. Match the cybersecurity frameworks and standards in column A with their correct description in column B

Answers	COLUMN A	COLUMN B
. …C…	1. **NIST Cybersecurity Framework (CSF)**	A. A European regulation designed to protect personal data and ensure privacy, with a focus on data protection by design and individual rights like access and deletion.
. …D…	2. I**SO/IEC 27001 and 27002**	B. A U.S. regulation that sets standards for protecting patient health information, requiring encryption and physical safeguards for data storage.
…F…	3. **Center for Internet Security (CIS) Controls**	C. Provides a common language for understanding and managing cybersecurity risks with five core functions: Identify, Protect, Detect, Respond, and Recover.
…A…	4. **GDPR (General Data Protection Regulation)**	D. A global benchmark for information security, focusing on implementing and maintaining an information security management system (ISMS) with risk management processes and continual improvement mechanisms.
. …B….	5. **HIPAA (Health Insurance Portability and Accountability Act)**	E. Enforces rigorous security measures specific to certain industries, like PCI DSS for payment card transactions and FISMA for federal information systems.
. …E…	6. **Industry-Specific Compliance Requirements**	F. A set of prioritized, actionable security controls organized into three categories: Basic, Foundational, and Organizational, to help defend against known attacks.

SECTION III. Read the statement below and answer by TRUE if it is correct or FALSE if it is incorrect

1. Asset management refers to the process of identifying, classifying, and managing all assets within an organization**.**

Answer: True

2. A vulnerability assessment aims to exploit security weaknesses in a system rather than identify them.

Answer: False

3. ISO 27001 provides a standard for asset identification and management.

Answer: True

4. Threat modeling involves categorizing data assets based on their value to the organization.
Answer: False
5. Penetration testing is a type of security assessment technique used to identify and exploit vulnerabilities in a system.
Answer: True
6. Risk assessment methodologies can include quantitative, qualitative, or semi-quantitative approaches to evaluate risks.
Answer: True
7. The goal of a risk assessment is solely to calculate risk scores without determining risk tolerance levels.
Answer: False
8. Data retention and disposal policies are part of a data classification process that ensures sensitive data is stored and disposed of correctly.
Answer: True
9. A risk register is a document that records identified security risks, along with their assessment and treatment plans.
Answer: True
10. Continuous assessment and improvement are not necessary once security controls have been implemented.
Answer: False

Practical assessment

C&A Technologies is a rapidly growing technology firm based in Kigali, Rwanda. Over the last five years, the company has expanded its operations, establishing three branches in different districts: the first branch in Huye District, the second in Gicumbi District, and the third in Rubavu District. C&A Technologies specializes in software development and offers various online services to its clients. Due to the company's expansion, sensitive data such as customer information, payment details, and intellectual property is accessed from multiple locations. Recently, the organization has experienced several security incidents, including unauthorized access to customer data, credit card information breaches, and potential exposure of proprietary software code. These vulnerabilities have led to significant financial losses and a decrease in customer trust. As a cyber-security engineer, you are tasked to Analysing vulnerability available in their network and corresponding security risks and Reporting security issues based to Security Assessment.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	1.Cyber vulnerabilities are well identified	1.1 Common vulnerabilities are identified		
		1.2 Vulnerabilities in software and hardware are assessed		
		1.3 Common attack techniques are identified		
2	2.Security Assessment Reporting and Documentation	2.1 Assessment reports are documented		
		2.2 Risk register is maintained		
		2.3 Remediation and mitigation strategies are documented		
		2.4 Continuous assessment and improvement practices are established		

Further information to the trainer

Andress, J. (2014). The Basics of Cybersecurity: A Practical Guide for Security Professionals. Syngress.

Graham, R. (2020). Cyber Security for Executives: A Practical Guide. Springer.

ISO/IEC 27001:2013. (2013). Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization (ISO).

Miller, M. (2021). Cybersecurity for Dummies. Wiley.

NIST Special Publication 800-53 Rev. 5. (2020). Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology (NIST).

CrowdStrike. (n.d.). *Cybersecurity 101: Fundamentals of Cybersecurity Topics*. Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/

Virginia Cyber Range. (n.d.). *Understanding Cyber Threats and Vulnerabilities*. Retrieved from https://www.virginiacyberrange.org/courseware/k-12-uncurated-content/understanding-cyber-threats-and-vulnerabilities-59-65-

IT Governance USA. (n.d.). *Cybersecurity Risk Assessment*. Retrieved from https://www.itgovernanceusa.com/cyber-security-risk-assessments

National Cyber Security Centre. (n.d.). *The Fundamentals and Basics of Cyber Risk*. Retrieved from https://www.ncsc.gov.uk/collection/risk-management/the-fundamentals-and-basics-of-cyber-risk


ACCESS
AUONTROLL
FIREWALK
ACCESS
MECHNIIUMS
USER
AUTHENTICATION
METHOMS
INTUSION
DETECTION
PREVENTION
DEVICE
MANAGEMENT
INTRUSION
DETECTION/
/PREVENTION
DEVICE
MANAGEMENT

Indicative contents

2.1 Implementation of Access Control Mechanisms
2.2 Implementation of User Authentication Mechanisms
2.3 Implementation of Authorization Mechanisms
2.4 Implementation of Access Request and Approval Workflow
2.5 Deployment of Firewalls and IDS/IPS
2.6 Isolate Critical Systems
2.7 Encrypt Sensitive Data for Protection
2.8 Manage Encryption Keys
2.9 Update Endpoint Security for Maintenance
2.10 Implement Device Management Policies
2.11 Apply Security Patches for Security Management

Key Competencies For Learning Outcome 2: Implement Security Measures

Knowledge	Skills	Attitudes
• Description of Role-Based access control(RBAC) • Description of Access Request and Approval Workflow • Description Single Factor Authentication (SFA) • Description Multi-Factor Authentication (MFA) • Description Single Sign-On (SSO) • Description of network segmentation • Identification of Critical Systems • Description of Firewalls • Description of IDS • Description of IPS	• Configuring Role-Based access control(RBAC) in a system • Implementing User Authentication mechanisms • Implementing Authorization Mechanisms • Implementing Access Request and Approval Workflow • Deploying Firewall and IDS/IPS • Developing a Network Segmentation Plan • Implementing network segmentation measures • Isolating Critical Systems • Implementing data encryption • Updating Endpoint Security for Maintenance	• Attention to Detail • Responsibility • Accountability • Team Spirit • Curiosity • Resilience • Adaptability

• Description of Encryption in cyber security • Description of management of encryption keys • Description Endpoint Security update • Describe device management policies	• Implementing device management policies • Testing and deployment security management	

Duration: 70 hrs

Learning outcome 2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Implement properly access control mechanisms to manage user privileges and protect resources.
2. Implement properly user authentication methods to ensure secure login and system access.
3. Implement corectly authorization mechanisms to control access to resources based on user roles and permissions.
4. Apply access request and approval workflows for better security governance.
5. Describe the process of isolating critical systems to prevent unauthorized access or cyber threats.
6. Deploy corectly firewall and IDS/IPS solutions to detect and prevent unauthorized access and potential threats.
7. Isolate properly critical system from affected system.
8. Encrypt properly sensitive data for protection, ensuring data integrity and confidentiality in transit and at rest.
9. Identify the principles of encryption key management and its importance in securing sensitive data.
10. Update properly endpoint security for future maintenance
11. Implement correctly device management policies used in cybersecurity.
12. Apply correctly security patches for security management

Resources

Equipment	Tools	Materials
• Computers • Computer server • Routers • Switches • Firewalls • IPS/IDS	• Snort • FreeIPA • Cisco packet tracer • Virtualization software	• Internet Access

Advance Preparation:

Before delivering this learning outcome, you are recommended to:

- Avail equipment, tools, material and software used in cyber security for implementing security measures
- Avail working environment

Indicative content 2.1: Implementation of Access Control Mechanisms

Duration: 6 hrs

Theoretical Activity 2.1.1: Description of Access Control Mechanisms

Notes to the trainer:

- Trainer may use small group to describe access control mechanisms
- Avail images, videos to be used as didactic materials

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. What is Role-Based Access control(RBAC)?

ii. Describe Key RBAC Principles and Key Concepts in RBAC

iii. What are Benefits and Advantages of RBAC?

iv. Describe Role Definition and Description

v. Describe Role Assignment

vi. Describe Criteria Role Hierarchy and Inheritance

vii. Describe RBAC Implementation in IT Systems

viii. VIII. Explain RBAC Policy Design

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.1.1

Points to Remember

- Access control mechanisms manage how users access systems and data within an organization. Role-Based Access Control (RBAC) is a common method that grants access based on users' roles instead of individual identity.
- Key principles of RBAC include separating duties, granting only necessary access (least privilege), assigning access based on roles, and ensuring roles align with organizational policies.
- Advantages of RBAC are Enhanced Security, Simplified Access Management, Scalability, Compliance with Regulations, Increased Productivity, Separation of Duties, Centralized Control.
- User roles and permissions is central to RBAC. Roles are created based on specific tasks or responsibilities, and users are assigned roles according to their job needs.

Practical Activity 2.1.2: Implement RBAC in a System

Notes to the trainer

This activity should take place in a computer lab where trainees should Configure RBAC

Avail computers

Avail FreeIPA software installed in all computers to be used.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

Your school currently facing challenges in managing access permissions manually, leading to excessive permissions, unnecessary access to sensitive data, and difficulty in audit. To solve this issue, they decide to implement RBAC using their existing IT infrastructure with the open-source tool **FreeIPA**

Step 2: Explain the task and provide clear work instruction

Step 3: Demonstrate how to configure RBAC. While demonstrating, explain the RBAC configuration procedures.

Step 4: Ask trainees to configure RBAC and monitor the procedures.

Step 6: Verify whether RBAC is configured

Step 7: Address any questions or concerns

Step 8: Ask trainee to read key reading 2.1.2

Points to Remember

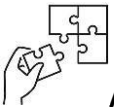
While configuring RBAC using FreeIPA tools you follow the following steps:

Step 1: Defining roles and permissions based on system requirements.

Step 2: Create Commands

Step 3: Assigning users to appropriate roles.

Step 4: Establishing policies for granting and revoking roles



Application of learning 2.1.

ISH Inc. is a medium-sized software company with multiple departments such as Engineering, Sales, HR, and IT Support. The organization is currently facing challenges in managing access permissions manually, leading to excessive permissions, unnecessary access to sensitive data, and difficulty in audit. To solve this issue, they decide to implement RBAC using their existing IT infrastructure with the open-source tool **FreeIPA**.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	Defining User Roles and Permissions are well defined	1.1 Role definition is cleared		
		1.2 Permissions are assigned based on job function		
		1.3 Roles are Alignment with job functions		
2	RBAC is clearly configured	2.1 Role creation is configured		
		2.2 Users are assigned to roles		
		2.3 Permissions are configured correctly		
		2.4 RBAC Policy Designed		

Indicative content 2.2: Implementation of User Authentication Mechanisms

Duration: 6 hrs

Theoretical Activity 2.2.1: Description of Single Factor Authentication (SFA)

Notes to the trainer:

- Trainer may use small group to describe Single Factor Authentication (SFA)
- Avail images, videos to be used as didactic materials

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Password-Based Authentication
ii. Describe Biometric Authentication
iii. Describe Token-Based Authentication

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.2.1

Points to Remember

- Single-Factor Authentication (SFA) Implementation involves using just one method of authentication to verify a user's identity.
- Password-Based Authentication: This is the most common form of SFA, where users log in using a username and password.
- Biometric Authentication: Uses unique biological characteristics, such as fingerprints or facial recognition, for authentication.
- Token-Based Authentication: Users are authenticated via physical or digital tokens, such as hardware tokens or app-generated OTPs.

Theoretical Activity 2.2.2: Description of Multi Factor Authentication (MFA)

Notes to the trainer:

- Trainer may use small group to describe multi Factor Authentication (MFA)
- Avail images, videos to be used as didactic materials

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. What is Introduction to MFA
ii. What are Components of MFA

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.2.2

Points to Remember

- Multi-Factor Authentication (MFA) is a security process that enhances protection by requiring users to provide multiple forms of identification to access systems or accounts
- MFA's key components are divided into three categories: "Something You Know," such as a password or PIN; "Something You Have," like hardware tokens or mobile apps generating one-time passcodes; and "Something You Are," involving biometric data such as fingerprints or facial recognition.

Theoretical Activity 2.2.3: Description of Single Sign-On (SSO) Solutions

Notes to the trainer:

- Trainer may use small group to describe Single Sign-On (SSO) Solutions

- Avail images, videos to be used as didactic materials

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe SSO Overview
ii. What are Advantages and Challenges of SSO
iii. Describe SSO Implementation Considerations

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.2.3

Points to Remember

- Single Sign-On (SSO) is an authentication solution that enables users to access multiple applications and websites using a single set of credentials.
- SSO offers several advantages, such as improving user experience by reducing the number of credentials to remember, centralizing authentication to make security enforcement easier, and lowering helpdesk costs by reducing password reset requests.
- Challenges, including creating a single point of failure, requiring complex configuration across different systems, and increasing security risks if SSO credentials are compromised, potentially giving attackers access to multiple systems.

Practical Activity 2.2.4: Implementing of User Authentication mechanisms

Notes to the trainer

- This activity should take place in a computer lab where trainees should implement authentication mechanisms
- Avail computers

- Avail FreeIPA software

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

> The school need to enhance its security due to increasing cyber threats. Initially relying on Single Factor Authentication (SFA) through passwords. To strengthen security, they need to implement Multi-Factor Authentication (MFA), requiring users to verify their identity using multiple methods, like passwords and biometrics. Use FreeIPA to enable Multi-Factor Authentication (MFA) for school users.

Step 2: Explain the task and provide clear work instruction (Task, PPE, Time allocated)

Step 3: Demonstrate how to configure Multi-Factor Authentication**.** While demonstrating, explain the Multi-Factor Authentication configuration procedures.

Step 4: Asks trainees to configure Multi-Factor Authentication and monitor the procedures.

Step 6: Ask trainees to present their findings

Step 7: Address any questions or concerns

Step6: Ask trainee to read the key readings on activity 2.1.4

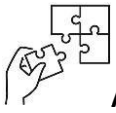
Points to Remember

Steps to Implement Multi-Factor Authentication (MFA) with FreeIPA to enable MFA

Step 1: Enable OTP Authentication for FreeIPA

Step 2: Configure OTP Tokens for Users

Step 3: Test MFA Configuration



Application of learning 2.2.

ABC Corporation need to enhance its security due to increasing cyber threats. Initially relying on Single Factor Authentication (SFA) through passwords. To strengthen security, they need to implement Multi-Factor Authentication (MFA), requiring users to verify their identity using multiple methods, like passwords and biometrics. Use FreeIPA to enable Multi-Factor Authentication (MFA) for school users.

Checklist:

Criteria	Indicators	Observation	
		YES	NO
Multi-Factor Authentication (MFA) is well configured	MFA methods is identified		
	devices and solutions for MFA are chosen		
	password-based authentication for users are enabled		
	biometrics or token-based authentication methods are integrated		
	MFA setup are tested		

Indicative content 2.3: Implementation of Authorization Mechanisms

Duration: 6 hrs

Theoretical Activity 2.3.1: Description of Authorization Mechanisms

Notes to the trainer:

- Trainer may use small group to describe authorization mechanisms
- Avail images, videos to be used as didactic materials

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Permission Models?
ii. Describe Access Control Lists (ACLs)

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.3.1

Points to Remember

- The implementation of authorization mechanisms involves setting up permission models to control user access to resources. Common models include: Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based Access Control (RBAC)
- Access Control Lists (ACLs) define specific permissions for users or groups, specifying which resources they can access and what actions they can perform.

Practical Activity 2.3.2: Implementing of Authorization Mechanisms

Notes to the trainer

- This activity should take place in a computer lab where trainees should implement authentication mechanisms
- Avail computers
- Avail virtualization software(Oracle Virtual Box)
- Avail cisco packet tracer software
- Avail IDS, IPS and **pfsence** devices

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

> A school needs to restrict access to its webpage, allowing only staff users while denying access to student users. The Access Control List (ACL) should be configured correctly to permit staff members to access the website while ensuring that students are denied access.

Step 2: Explain the task and provide clear work instruction (Task, PPE, Time allocated)
Step 3: Demonstrate how to configure Access control list. While demonstrating, explain access control list procedures.
Step 4: Asks trainees to configure ACL and monitor the procedures.
Step 6: Ask trainees to present their findings
Step 7: Address any questions or concerns
Step6: Ask trainee to read the key readings on activity 2.3.2

Points to Remember

Steps to Configure ACL in pfSense using virtualization tools
Step 1: Launch VirtualBox and click on "**New**" to create a new virtual machine.
Step 2: Allocate Memory: A minimum of 1GB of RAM is recommended for pfSense,
Step 3: Configuring pfSense Network Settings

Step 4: Installing pfSense

Configuring pfSense network interfaces using the shell

Step 1: Boot up your pfSense virtual machine.

Step 2: Modifying the LAN interface configuration with the actual gateway address provided through the shell with the new address in network address range of (192.168.20.0/24)

Step 3: Enabling the DHCP server on LAN by providing the start address and end address based on your network range address (192.168.20.0/24)

Accessing the pfsense using the web interface and making further configuration.

Step 1: create another client machine in your virtual box with any operating system. On our side we are having a virtual machine with UBUNTU linux operating system.

Step 2: Open your terminal and check if your client machine is getting the ip address from the DHCP server of the pfsense firewall. By using (**ip a**) command

Step 3: Check if your client machine is getting the default route ip of the LAN interface of pfsense firewall

Step 4: open any browser and access the pfsense by using the default route ip(**192.168.20.5**) in the URL.

Step 5: click next, and set the hostname of your firewall by "**BTECHFIREWALL"** and set the domain name as **"btechfirewall.home"** as follow and click next.

Step 6: set the timezone of your firewall as **Africa/cairo,** and click next

Step 7: set LAN interface IP and the subnet mask or leave it's as the default form the pfsense**,** and click next

Step 8: set the Admin password to confirm the pfsense configuration**,** and click next

Step 9: by clicking on change the password, set the Admin new password and click next

Applying different rules in pfsense on LAN interfaces.

(rejecting the client for using the HTTP and HTTPS protocol while the client is browsing anything in the browsers on a network.)

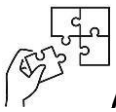
Step1: Before setting this rules lets check if the HTTP and HTTPS services are working properly

Step 2: Go to the **Firewall** tab click on **Rules** sub-tab

Step 3: Choose the **LAN** interface and **add** the new rules

Step 4: Change the **pass** action to **reject,** and also select the **TCP/UDP** protocol as the protocol that provide the HTTP and HTTPS services. **Blocking HTTP(80) and Blocking HTTPS(443)**

Step 5: Apply changes to the firewall rule configuration, to allow its to take effect on the system



Application of learning 2.3.

BPR (Bank Populaire du Rwanda) Headquarter located in Kigali city; it has two branches, one in Nyanza district and another on in Nyagatare district. The employees from Nyanza branch no longer provide efficient services to the customers, but instead they are often busy doing unnecessary activities on the internet. As Network technician; you are requested to make necessary configurations on appropriate router so that the users in Nyanza branch cannot communicate with the web server which is located at headquarter network.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	**NO**
1	security configuration is well planned	1.1 Devices are selected		
		1.2 Headquarter Network (Kigali) are identified		
		1.3 Nyagatare Branch Network are identied		
		1.4 Nyanza Branch Network are identified		
		1.5 ACL Type are chosen		
		1.6 Placement of ACL are decided		
2	Security is well configured	2.1 Login Credentials are configured		
		2.2 Access List Deny Rule are created		
		2.3 Other Traffic are allowed		
		2.4 ACL to Interface are applied		
3	Network security monitoring is well implemented	3.1 Log Traffic are genereted		
		3.2 Review ACL are schedured		
		3.3 Documentation are genereted		

Indicative content 2.4: Description of implementation of Access Request and Approval Workflow.

Duration: 6 hrs

Theoretical Activity 2.4.1: Description of implementation of Access Request and Approval Workflow.

Notes to the trainer:

- Trainer may use small group to describe implementation of Access Request and Approval Workflow

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Access Request Workflow (Initiating Access Requests, Request Routing and Handling, Requester Responsibilities)?

ii. Describe Access Approval Mechanisms (Approval Authorities and Workflows, Approval Decision Criteria, Escalation and Exception Handling)?

iii. Describe Access Review and Recertification (Access Review Process, Purpose of Access Review, Periodicity of Access Reviews, Reviewer Roles and Responsibilities)?

iv. Describe Recertification Procedure (Identifying and Validating User Permissions, Recertification Reporting and Remediation Actions)?

Step2: Ask trainees to present their findings to the whole class.

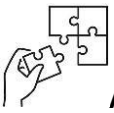
Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.4.1

Points to Remember

- The Access Request and Approval Workflow ensures that only authorized users can access specific resources. It starts with users submitting access requests, which are routed to the appropriate authorities for approval. Requesters are responsible for providing accurate information and justifying their need for access
- Access Approval Mechanisms involve designated approvers who review and decide on requests based on set criteria. If needed, requests can be escalated for further review or handled through exception processes.
- Access Review and Recertification involves regularly checking user access to ensure it is still appropriate. Reviewers ensure users only have the permissions needed for their roles, maintaining security and compliance.
- Recertification Procedures validate user permissions, generate reports, and address any issues found, keeping the system secure and updated.



Application of learning 2.4.

ABC is a company with employees from different department, the company need to manage Access Request and Approval Workflow ensures that only authorized users can access specific resources. Describe Access Request Workflow, Access Approval Mechanisms, Access Review and Recertification and Recertification Procedures in order to help company to manage use access

Checklist:

Main point to check	Observation	
	Yes	No
Initiating access requests clearly defined		
Access requests properly routed		
Responsibilities of the requester clearly described		
Approval authorities and workflows clearly identified		
The criteria for making approval decisions clearly described		

	Process for escalating requests and handling exceptions clearly described		
	intervals for conducting access reviews clearly defined		
	Roles and responsibilities of reviewers clearly identified		
	Reports generated to document the recertification process and results clearly defined		
	Clear remediation actions defined		

Indicative content 2.5: Deployment of Firewalls and IDS/IPS

Duration: 6 hrs

Theoretical Activity 2.5.1: Description of Firewalls and IDS/IPS

Notes to the trainer:

- Trainer may use small group to describe firewalls and IDS/IPS
- Avail images, videos to be used as didactic materials

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Firewalls fundamentals
ii. Describe IDS
iii. Describe IPS
iv. What is Proactive Threat Mitigation
v. Describe Rule Management Firewall

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.5.1

Points to Remember

- A firewall is a network security tool that controls the flow of traffic between a trusted internal network and untrusted external sources like the internet. It can be hardware or software and helps protect against unauthorized access.
- Intrusion Detection Systems (IDS) An Intrusion Detection System (IDS) monitors network or system activities for signs of malicious behavior. There are two main types: Network-based IDS (NIDS), which monitors network traffic, and Host-based IDS (HIDS), which monitors individual devices

- Intrusion Prevention Systems (IPS) An Intrusion Prevention System (IPS) goes a step further than IDS by automatically blocking or stopping detected threats.
- Firewall Configuration and Rule Management Firewalls must be configured with security policies and rules to control what traffic is allowed or blocked. Regularly reviewing and updating these rules, using Role-Based Access Control (RBAC) to limit access based on roles, and enabling logging to track rule effectiveness are key practices.

Practical Activity 2.5.2: Deploying Firewall and IDS/IPS

Notes to the trainer

- This activity should take place in a computer lab where trainees should implement authentication mechanisms
- Avail computers
- Avail cisco packet tracer software
- Avail IDS,IPS and Firewall devices

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

You school decided to implement a firewall, an Intrusion Detection System (IDS), and an Intrusion Prevention System (IPS) to ensure a robust security posture. You need to configure a firewall school, ensuring that security policies are well-defined, deploy an IDS to monitor network traffic and detect potential threats. And Set up an IPS to prevent any malicious traffic from entering the network**.**

Step 2: Explain the task and provide clear work instruction (Task, PPE, Time allocated)

Step 3: Demonstrate how to configure firewall and IDS/IPS.While demonstrating, explain configuration procedures.

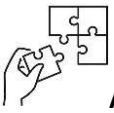
Step 4: Asks trainees to configure firewall and IDS/IPS and monitor the procedures.

Step 6: Ask trainees to present their findings

Step 7: Address any questions or concerns
Step6: Ask trainee to read the key readings on activity 2.5.1

Points to Remember

- To create a standard access list, you use the command syntax on the router, specifying whether to "permit" or "deny" traffic from a source IP address using a source wildcard. The standard ACL range is between 1-99 or 1300-1999, and it is typically placed close to the destination device. For instance, to block Admin LAN users from accessing the Operations server in a given network, you calculate the appropriate wildcard and apply the ACL to the E0 interface of the remote router. Key commands include entering global configuration mode, defining the access list, and applying it to the correct interface.
- For an extended access list, which provides more flexibility, you specify not just the source but also the protocol, destination, and associated port numbers. In this example, to block FTP and Telnet access to the Operations server, the ACL must include the relevant port numbers (21 for FTP, 23 for Telnet) and be applied on the E0 outbound interface of the remote router. Like standard ACLs, you use commands to deny or permit traffic, but with more detailed criteria.
- Once the access list is configured, it can be applied to interfaces, and you can use show commands to review the ACLs in place. If needed, the entire access list can be removed using the "no access-list" command. For both standard and extended access lists, it's important to test and verify their effectiveness after implementation.
- Extended access lists are particularly useful when needing to block specific protocols like FTP or Telnet while allowing other types of traffic, offering greater control over network traffic management.



Application of learning 2.5.

You are part of an IT security team tasked with securing a small business's network infrastructure. The business has a mix of internal and external traffic, and it is critical to protect sensitive customer data and prevent unauthorized access. Your team has decided to implement a firewall, an Intrusion Detection System (IDS), and an Intrusion Prevention System (IPS) to ensure a robust security posture. You need to configure a firewall for the small business, ensuring that security policies are well-defined, deploy an IDS to monitor network traffic and detect potential threats. And Set up an IPS to prevent any malicious traffic from entering the network.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	Firewall are properly configured	1.1 Security policies defined clearly		
		1.2 Firewall rules implemented correctly		
		Documentation of settings provided		
2	IDS is well Deployed	2.1. IDS installed and operational		
		2.2.Detection rules configured effectively		
		2.3.Alerts generated for test attacks		
3	IPS is well configured	3.1 IPS installed		
		3.2 Custom rules to block threats set		
		3.3 Effective blocking of simulated attacks		

Indicative content 2.6: Isolate Critical Systems

Duration: 6 hrs

Theoretical Activity 2.6.1: Description of network segmentation.

Notes to the trainer:

- Trainer may use small group to describe network segmentation.
- The use of physical objects, images, videos, and illustrations as didactic materials is required.

Key steps:

While delivering this activity, pass through the following steps:

Step1: Involve trainees in group formulation

Step2: Introduce the activity and ask trainees to answer to following questions:

i. What is of Network Segmentation
ii. Describe Types of Network Segmentation
iii. What are Benefits of Network Segmentation
iv. What are ways for identifying Critical Systems

Step3: Ask trainees to present their findings to the whole class.

Step4: Provides expert view on presented contents.

Step5: Address any questions or concerns.

Step6: Ask trainee to read the key readings on activity 2.6.1

Points to Remember

- Network segmentation is the practice of dividing a computer network into smaller, manageable segments or sub-networks. This approach enhances security by limiting exposure to potential threats, improves performance by controlling traffic flow, and simplifies network management.
- There are different types of network segmentation. Physical segmentation, Logical segmentation, Virtual segmentation and application segmentation
- The benefits of network segmentation are significant. It enhances security by reducing the attack surface and containing potential breaches. It also improves network performance by minimizing congestion and optimizing bandwidth usage.
- Identifying critical systems is essential for effective network segmentation. Critical systems are those vital for business operations and often handle sensitive data. To identify these systems, organizations should create an inventory of all systems and applications, assess the impact of each on business operations, and prioritize them based on their importance and data sensitivity.

Practical Activity 2.6.2: Implementing network segmentation measures

Notes to the trainer

- This activity should take place in a computer lab where trainees should implement network segmentation
- Avail computers
- Avail computer network (wireless or Wired)

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

Your school has been tasked with developing and implementing a network segmentation plan for school network to enhance security and compliance. The management is concerned about potential data breaches between staff, trainers and

trainee and wants to ensure that critical systems are adequately protected while maintaining efficient network performance.

Step 2: Explain the task and provide clear work instruction (Task, PPE, Time allocated)

Step 3: Demonstrate how to implement network segmentation. While demonstrating, explain the network segmentation implementation procedures.

Step 4: Asks trainees to implement network segmentation and monitor the procedures.

Step 6: Ask trainees to present their findings

Step 7: Address any questions or concerns

Points to Remember

Steps to Perform network segmentation:

1. Create a Segmentation Strategy
2. Identify Objectives
3. Select Technologies
4. Implement the Plan
5. Configure and Set Up
6. Monitor Continuously

Practical Activity 2.6.3: Isolating Critical Systems

Notes to the trainer

- This activity should take place in a computer lab where trainees should isolate critical systems
- Avail computers
- Avail computer network (wireless or wired)

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

You are part of an IT team in an organization that handles sensitive customer data. Your task is to implement network segmentation measures to enhance security and ensure that critical systems are isolated from potential threats.

Step 2: Explain the task and provide clear work instruction (Task, PPE, Time allocated)

Step 3: Demonstrate how to isolate critical systems. While demonstrating, explain isolate critical systems procedures.

Step 4: Asks trainees to isolate critical systems and monitor the procedures.

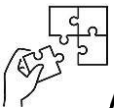
Step 6: Ask trainees to present their findings

Step 7: Address any questions or concerns

Points to Remember

Steps to Perform isolation of critical system:

1. Implementation Phases
2. Configuration and Setup
3. Continuous Monitoring
4. Isolating Critical Systems



Application of learning 2.6.

H.D is an organization that processes sensitive customer data collected from various departments, including Marketing, Sales, and Administration. Your task is to implement a network segmentation plan that includes isolating critical systems to enhance security and improve overall network performance. This involves identifying critical systems, creating a segmentation strategy, and ensuring continuous monitoring of the network.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	Segmentation Strategy are Developed	1.1 Scope of segmentation is well defined		
		1.2 critical systems are identified		
		1.3 objectives and timelines are established		
2	Network segmentation is well configured	2.1 network design is well described		
		2.3 Devices are correctly Configured		

SN	Criteria	Indicators	Observation	
			YES	NO
		2.4 segmentation plan is well executed		
		2.5 Critical Systems is well isolated		

Indicative content 2.7: Encrypt Sensitive Data for Protection

Duration: 6 hrs

Theoretical Activity 2.7.1: Description of Encryption in cyber security

Notes to the trainer:

- Trainer may use small group to explain encryption in cyber security

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Encryption
ii. Explain Encryption Terminology (Plaintext, Ciphertext, Encryption Key,
iii. Encryption Algorithm, Decryption)
iv. Principles of Confidentiality, Integrity, and Availability (CIA) in data Encryption
v. Differentiate Types of Encryption Algorithms

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.7.1

Points to Remember

- Encryption is a critical cybersecurity measure used to protect sensitive data by converting readable information (plaintext) into an unreadable format (cipher-text).
- This process ensures confidentiality, integrity, and availability (CIA), making sure that only authorized individuals with the correct decryption key can access or manipulate the data. Encryption is essential for safeguarding personal, financial, and confidential business information from unauthorized access.

- There are different types of encryption algorithms used depending on the specific needs of an organization. Symmetric encryption, Asymmetric encryption and Hashing algorithms.
- For effective implementation, organizations must establish encryption policies, identify sensitive data, and classify it appropriately. Data at rest (e.g., in databases) and data in transit (e.g., during network transmission) must be encrypted using industry-standard algorithms.

Theoretical Activity 2.7.2: Identification of Sensitive Data

Notes to the trainer:

i. Trainer may use small group to identify sensitive data

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. How to recognize sensitive data?
ii. Describe Data Classification and Labelling

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.7.2

Points to Remember

- Sensitive data may include personal identifiable information (PII), financial records, health records, and intellectual property. Recognizing data sensitivity helps organizations prioritize encryption efforts to protect high-value information from potential harm, ensuring that sensitive details are secured appropriately.

- Data classification and labelling play a key role in managing sensitive information. Organizations classify data based on its sensitivity and associated risk levels, which can range from public (low sensitivity) to confidential (moderate sensitivity) and restricted (high sensitivity). Labelling ensures that employees handle data correctly and apply the right level of encryption, thereby safeguarding critical information according to its importance.

Theoretical Activity 2.7.3: Description Data Encryption Policies

Notes to the trainer:

- Trainer may use small group to describe Data Encryption Policies

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. What are process for Developing Data Encryption Policies?
ii. Define Encryption Scope

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.7.3

Points to Remember

- Developing data encryption policies is essential for safeguarding sensitive information within an organization. These policies should clearly define which types of data require encryption and assign responsibilities for implementing encryption practices. Key management procedures, including secure storage of encryption keys, must be established to prevent unauthorized access. Additionally, regular auditing and monitoring are necessary to ensure ongoing compliance with encryption protocols, helping to maintain data security over time.

- The encryption policy should also define the scope of encryption, ensuring protection across critical stages of the data lifecycle. This includes encrypting **data at rest** (such as databases and backups), **data in transit** (such as email and web traffic), and securing endpoints like laptops and mobile devices. By setting clear guidelines, organizations can consistently apply encryption to sensitive areas, reducing the risk of data breaches.

Theoretical Activity 2.7.4: Description Encryption Implementation

Notes to the trainer:

- Trainer may use small group to describe Encryption Implementation

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. What are Implementing Data Encryption
ii. Describe Securing Data at Rest and in Transit

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.7.4

Points to Remember

- Developing data encryption policies is essential for safeguarding sensitive information within an organization. These policies should clearly define which types of data require encryption and assign responsibilities for implementing encryption practices. Key management procedures, including secure storage of encryption keys, must be established to prevent unauthorized access. Additionally, regular auditing and monitoring are necessary to ensure ongoing compliance with encryption protocols, helping to maintain data security over time.

- The encryption policy should also define the scope of encryption, ensuring protection across critical stages of the data lifecycle. This includes encrypting **data at rest** (such as databases and backups), **data in transit** (such as email and web traffic), and securing endpoints like laptops and mobile devices. By setting clear guidelines, organizations can consistently apply encryption to sensitive areas, reducing the risk of data breaches.

Practical Activity 2.7.5: Implementing data encryption

Notes to the trainer

This activity should take place in a computer lab where trainees should Select different software and hardware monitoring tools implement data encryption
Avail computers with windows 10 installed

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity, ask trainees to refer to the theoretical activity (2.7.4) and do the task described below:

You are tasked to go in computer lab and encrypt data stored to their storage devices in computers using BitLocker

Step 2: Explain the task and provide clear work instruction

Step 3: Demonstrate how to select Cyber Security Monitoring to encrypt data ols. While demonstrating, explain the data encryption procedures.

Step 4: Ask trainees to select Cyber Security Monitoring to encrypt data and monitor the procedures.

Step 6: Verify whether encryption is conducted

Step 7: Address any questions or concerns

Step 8: Ask trainee to read key reading 2.7.5

Points to Remember

Steps to perform data encryption in windows 10

Step 1: Press Win + R then on run dialog type "**Control Panel"** hit Enter button
Step 2: Go to "**System and Security**" > "**BitLocker Drive Encryption** ".
Step 3: Under the "**Operating system drive**" section, click the on "**Turn on BitLocker**" option.
Step 2: Go to "**System and Security**" > "**BitLocker Drive Encryption** ".
Step 3: Under the "**Operating system drive**" section, click the on "**Turn on BitLocker**" option.
S**tep 7**: Click the **Next** button.
Step 8: Choose the "**New encryption mode**" option.
Step 9: Click the **Next** button.
(Optional) Select the "**Run BitLocker system check**" option.
Step 10: Click the **Restart now** button.
That's it! Your system drive is now protected by BitLocker encryption, helping to keep your data safe from unauthorized access.

Application of learning 2.7.

ISHEMO is a company with many computers that have Windows 10 installed. The company needs to encrypt data to ensure data confidentiality, integrity, and availability. You are tasked with encrypting the data stored on their secondary storage.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	1.Encryption are prepared	1.1 All secondary storage devices to be encrypted are identified		
		1.2 Administrative access to devices are confirmed		
2	2.Data encryption is well implemented	2.1 Appropriate encryption software are chosen		
		2.2 software is compatible with Windows 10 is verified		

SN	Criteria	Indicators	Observation	
			YES	NO
		2.3 Ensure encryption software is licensed		
		2.4 Encryption software on each computer is installed		
		2.5 Encryption on secondary storage devices is enabled		

Indicative content 2.8: Management of encryption keys

Duration: 6 hrs

Theoretical Activity 2.8.1: Description of management of encryption keys

Notes to the trainer:

- Trainer may use small group to Describe of management of encryption keys

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Endpoint Security
ii. Describe Endpoint Security solution
iii. Describe Endpoint Security Configuration

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

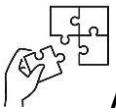
Step5: Ask trainee to read the key readings on activity 2.8.1

Points to Remember

- Maintaining endpoint security is crucial to protect an organization's devices from threats like malware and unauthorized access.
- Key solutions for endpoint security include deploying antivirus and anti-malware software, Endpoint Detection and Response (EDR) systems for advanced threat detection, firewalls to filter network traffic, and Data Loss Prevention (DLP) tools to monitor sensitive data

- Proper configuration is essential to maximize endpoint security. This includes applying patches and software updates to fix vulnerabilities, implementing access control measures like multi-factor authentication (MFA) and role-based access control (RBAC), and using network segmentation to isolate devices and minimize risks. Con-

tinuous endpoint monitoring and logging provide real-time threat detection, allowing organizations to identify and address potential security issues early on.



Application of learning 2.8.

ISH Corp is a financial services company that handles sensitive customer data, including payment details and personal identification information. To protect this data, ISH Crop uses encryption across its systems. Recently, a security audit highlighted the need for stronger encryption key management practices to prevent unauthorized access and ensure compliance with data protection regulations like GDPR. The company has tasked you to develop a comprehensive encryption key management strategy.

Checklist

Main point to check	**Observation**	
	YES	**NO**
Key Generation and Initialization are identified		
Key Usage are described		
Secure Storage Solutions are identified		
Rotation Strategies are implemented		
Key Retirement and Disposal are identified		

Indicative content 2.9: Update Endpoint Security for maintenance

Duration: 6 hrs

Theoretical Activity 2.9.1: Description of Endpoint security update

Notes to the trainer:

- Trainer may use small group to Describe of endpoint security update

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Endpoint Security.
ii. Describe Endpoint Security solution
iii. Describe Endpoint Security Configuration

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.9.1

Points to Remember

- Encryption Key Lifecycle include Key Generation and Initialization, Key Usage and Maintenance
- Key Management Policies deal with Establishing Key Management Policies, Policy Enforcement and Auditing
- Secure Key Storage and Distribution include Secure Storage Solutions and Key Distribution Methods
- Key Rotation and Retirement include Key Rotation Strategies, Key Retirement and Disposal Procedures

Practical Activity 2.9.2: Updating Endpoint Security for Maintenance

Notes to the trainer

- This activity should take place in a computer lab where trainees should update compute available in computer Lab
- Avail computers with windows 11 installed
- Avail internet connection

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

You are tasked to go in computer lab and update computer that is available computer lab

Step 2: Explain the task and provide clear work instruction

Step 3: Demonstrate how to update computer. While demonstrating, explain computer updating procedures.

Step 4: Ask trainees to update computer and monitor the procedures.

Step 6: Verify whether computer are updated

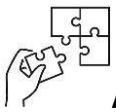
Step 7: Address any questions or concerns

Step 8: Ask trainee to read key reading 2.8.2

Points to Remember

Steps to update windows 11 computers

1. Check your current version
2. Backup your data
3. Install the updates
4. Review the changes



Application of learning 2.9.

HAN is a mid-sized company with various computers running Windows 11. The company needs to enhance its security measures to protect its systems and data. You are assigned the task of updating their computers to improve overall security. This includes implementing necessary updates, security patches, and configurations to safeguard their infrastructure.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	1. Update are well prepared	1.1 All computers running Windows 11 are identified		
		1.2 Security updates and patches are available for all systems		
		1.3 Current security software and configurations documented		
2	2. Computers are well Updated	2.1 System setting is accessed		
		2.2 Critical security patches are identified		
		2.3 System is up to date		

Indicative content 2.10: Implement Device Management Policies

Duration: 6 hrs

Theoretical Activity 2.10.1: Description of Device Management Policies

Notes to the trainer:

- Trainer may use small group to Describe of Device Management Policies

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Define Scope of Device Management?
ii. Describe Device Classification and Inventory
iii. Describe Configuring Device Settings and Access
iv. Describe Policy Enforcement and Compliance
v. Describe User Education on Device Management
vi. Describe Raising Awareness of Device Security
vii. Describe Continuous Policy Monitoring
viii. Describe Adapting Policies to Changing Needs

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.9.1

Points to Remember

- Maintaining endpoint security is crucial to protect an organization's devices from threats like malware and unauthorized access.
- Key solutions for endpoint security include deploying antivirus and anti-malware software, Endpoint Detection and Response (EDR) systems for advanced threat detection, firewalls to filter network traffic, and Data Loss Prevention (DLP) tools to monitor sensitive data

- Proper configuration is essential to maximize endpoint security. This includes applying patches and software updates to fix vulnerabilities, implementing access control measures like multi-factor authentication (MFA) and role-based access control (RBAC), and using network segmentation to isolate devices and minimize risks. Continuous endpoint monitoring and logging provide real-time threat detection, allowing organizations to identify and address potential security issues early on.

Practical Activity 2.10.2: Implementing Device Management Policies

Notes to the trainer

- This activity should take place in a computer lab where trainees should implement device management policies
  Avail internet connection

Key steps:

While delivering this activity, pass through the following steps:

- **Step 1:** Introduce the activity and ask trainees do the task described below:

Your school need to implement device management policies, advice the schools steps to implement device security policies.
Step 2: Explain the task and provide clear work instruction

Step 3: Demonstrate steps to implement device security policies. While demonstrating, explain each procedure.

Step 4: Ask trainees to explain steps and monitor the procedures.

Step 6: Verify whether each step is clear

Step 7: Address any questions or concerns

Step 8: Ask trainee to read key reading 2.10.2

Points to Remember

Steps for Implementing Device Management Policies

1. Device Management Scope
2. Device Configuration Policies
3. User Training and Awareness
4. Policy Monitoring and Adaptation

Application of learning 2.10.

You are the IT administrator at a mid-sized company, tasked with implementing comprehensive device management policies. The company utilizes various devices, including laptops, smartphones, tablets, and desktops, all of which require consistent management to ensure security, compliance, and efficiency. Your goal is to implement and manage device policies that address device classification, configuration, user training, and continuous monitoring.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	Device Management Scope are well identified	1.1 Devices are identified		
		1.2 Devices are classified		
		1.3Scope of device management is defined		
2	Device Management Policies are clearly implemented	2.1 Evidence of policy implementation is provided		
		2.2 Compliance audit report is submitted		
		2.3 Compliance checks are set up with device management software		

Indicative content 2.11: Apply Security Patches for Security Management

Duration: 10 hrs

Theoretical Activity 2.11.1: Description of Security Patches for Security Management

Notes to the trainer:

- Trainer may use small group to Describe of Security Patches for Security Management

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Patch Management Procedures?
ii. Describe Developing Patch Management Procedures
iii. Patch Assessment and Classification
iv. Describe Controlled Testing Environments
v. What are Deployment Strategies and Phases
vi. **Step2**: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 2.9.1

Points to Remember

- Apply Security Patches for Security Management focuses on keeping systems secure by ensuring that they are up to date with the latest security patches. Patches are essential to fix vulnerabilities that could be exploited by attackers. Implementing a structured approach to patching ensures that systems remain secure and stable.
- Patch Management Procedures outlines the importance of having a clear process for managing patches. This includes developing a schedule, assigning roles, and determining how patches are tracked and applied. Patches must be assessed based on

their severity—critical patches that address significant security vulnerabilities are prioritized, while less critical updates may be scheduled for later.

- Testing and Deployment ensures that patches are applied smoothly without causing system disruptions. Patches should be tested in a controlled environment before system-wide deployment to avoid compatibility issues. Once tested, a phased deployment strategy is used to gradually apply patches across systems, starting with critical infrastructure, to minimize risks. Continuous monitoring ensures successful implementation.

Practical Activity 2.11.2: Configuring automatic updates and update service location

Notes to the trainer

- This activity should take place in a computer lab where trainees should configure automatic update
- Avail server computer with windows server 2016 installed
- Avail server computer with Microsoft WSUS (Windows Server Update Services) installed
- Avail internet connection

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

Your school needs to enable automatic updates for computers connected to its domain by using Windows Server Update Services (WSUS). This will ensure that all systems receive timely updates while allowing centralized control over the update process.

Step 2: Explain the task and provide clear work instruction

Step 3: Demonstrate steps configure Microsoft WSUS (Windows Server Update Services). While demonstrating, explain each procedure.

Step 4: Ask trainees to configure Microsoft WSUS (Windows Server Update Services) and monitor the procedures.

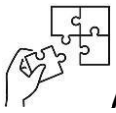
Step 6: Verify whether configure Microsoft WSUS are configured

Step 7: Address any questions or concerns

Step 8: Ask trainee to read key reading 2.11.2

Points to Remember

To configure the Configure Automatic Updates and Intranet Microsoft Update Service Location Group Policy settings for your environment
Open Group Policy Management Console (gpmc.msc).
Expand *Forest**Domains**Your_Domain*.
Right-click **Your_Domain**, and then select **Create a GPO in this domain, and Link it here**.
In the **New GPO** dialog box, name the new GPO **WSUS - Auto Updates and Intranet Update Service Location**.
Right-click the **WSUS - Auto Updates and Intranet Update Service Location** GPO, and then select **Edit**.
In the Group Policy Management Editor, go to Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update.
Right-click the **Configure Automatic Updates** setting, and then select **Edit**.
In the **Configure Automatic Updates** dialog box, select **Enable**.
Under **Options**, from the **Configure automatic updating** list, select **3 - Auto download and notify for install**, and then select **OK**.
Right-click the **Specify intranet Microsoft update service location** setting, and then select **Edit**.
In the **Specify intranet Microsoft update service location** dialog box, select **Enable**.
Under **Options**, in the **Set the intranet update service for detecting updates** and **Set the intranet statistics server** options, type http://Your_WSUS_Server_FQDN:PortNumber, and then select **OK**.



Application of learning 2.11.

At **H_D Company**, the IT department is responsible for ensuring that all computers connected to the company's domain are regularly updated with the latest security patches, features, and system improvements. To accomplish this, the company has decided to implement **Windows Server Update Services (WSUS)**, a solution that will provide centralized control over the update process, ensuring that all devices are updated automatically while allowing IT to manage update approval and distribution as system administrator you are requested to enable automatic update for their computers.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	**1.WSUS is well configured**	1.1 WSUS system requirements are verified		
		1.2 Sufficient storage space on the WSUS server are available		
		1.3 Group Policy Object (GPO) are created		
		1.4 GPO are linked to the relevant Organizational Units (OUs)		
		1.5 WSUS to sync with Microsoft Update are configured		

Learning outcome 2 end assessment

Written assessment

SECTION I: fill the following paragraph with appropriate word from provided word below

Access control mechanisms play a crucial role in ensuring the security of systems and sen-

- Restrict	- single-factor authentication (SFA)
- Role based	- unauthorized
- multi-factor authentication (MFA)	

sitive information. These mechanisms help to **……** access to data and resources only to authorized users, thereby reducing the risk of breaches and attacks. One common approach is **……** access control, which assigns permissions based on user roles within an organization. Additionally, **……** enhances security by requiring users to verify their identity using two or more verification factors. Properly implemented access control not only prevents **……** access but also helps to maintain integrity and confidentiality across the network.

Answer:

Access control mechanisms play a crucial role in ensuring the security of systems and sensitive information. These mechanisms help to **restrict** access to data and resources only to authorized users, thereby reducing the risk of breaches and attacks. One common approach is **role-based** access control, which assigns permissions based on user roles within an organization. Additionally, **multi-factor authentication (MFA)** enhances security by requiring users to verify their identity using two or more verification factors. Properly implemented access control not only prevents **unauthorized** access but also helps to maintain integrity and confidentiality across the network.

SECTION II. Read the statement below and answer by TRUE if it is correct or FALSE if it is incorrect

1. Discretionary Access Control (DAC) allows resource owners to control who has access to their resources.

Answer: True

2. In Mandatory Access Control (MAC), users have the flexibility to modify access permissions on their own files.

Answer: False

3. Role-Based Access Control (RBAC) assigns permissions based on the user's role within an organization.

Answer: True

4. Access Control Lists (ACLs) are used to manage both permissions for users and access control for network traffic.

5. ACLs are primarily used for restricting physical access to hardware systems.

Answer: False

6. In RBAC, users can only access the resources that are permitted to the roles they are assigned.

Answer: True

7. Access Control Lists (ACLs) can only be applied to user accounts, not network devices or traffic.

Answer: False

8. RBAC simplifies permission management in large organizations by grouping users into roles with common access needs.

Answer: True

9. In DAC, the permissions associated with a file can be modified by any user, not just the owner of the file.

Answer: False

10. Access Control Lists (ACLs) can be used in firewalls and routers to filter network traffic.

Answer: True

SECTION III. Choose the letter corresponding to the correct answers

1. **What is the first step in the access request workflow?**
   a) Approval decision
   b) Initiating access requests
   c) Escalation handling
   d) Recertification review
   Answer: b) Initiating access requests
2. **Who is responsible for initiating access requests?**
   a) IT Administrator
   b) Requester

c) Supervisor
d) Security Officer
Answer: b) Requester

3. **Which of the following is a key responsibility of an access request approver?**
   a) Request routing
   b) Approving or denying requests
   c) Logging user activities
   d) Performing access reviews
   Answer: b) Approving or denying requests
4. **What is the purpose of an access review?**
   a) To define escalation rules
   b) To verify if users have appropriate access
   c) To initiate access requests
   d) To route access requests
   Answer: b) To verify if users have appropriate access
5. **What happens if an access request is not approved in the workflow?**
   a) It is routed to the next level
   b) The request is automatically approved
   c) It is denied
   d) It is escalated or returned to the requester
   Answer: d) It is escalated or returned to the requester
6. **Which of the following is part of recertification procedures?**
   a) Identifying user permissions
   b) Routing access requests
   c) Approving access requests
   d) Requesting additional privileges
   Answer: a) Identifying user permissions

7. **What is the primary function of a firewall?**
   a) To allow all traffic
   b) To monitor and block unauthorized traffic
   c) To grant administrative privileges
   d) To install security patches
   Answer: b) To monitor and block unauthorized traffic
8. **Which type of firewall inspects traffic based on pre-configured rules?**
   a) Packet-filtering firewall
   b) Application firewall
   c) Host-based firewall

d) Intrusion prevention system

Answer: a) Packet-filtering firewall

9. **An IDS primarily:** a) Blocks traffic in real-time
   b) Detects and alerts on potential intrusions
   c) Prevents access to malicious websites
   d) Configures network policies
   Answer: b) Detects and alerts on potential intrusions
10. **Which of the following techniques is used by IPS to stop threats in real-time?**
    a) Signature-based detection
    b) Packet filtering
    c) Role-based access control
    d) Application whitelisting
    Answer: a) Signature-based detection
11. **What should be done after deploying a firewall to ensure its effectiveness?**
    a) Enable default rules
    b) Test and review firewall rules
    c) Disable logging
    d) Implement recertification procedures
    Answer: b) Test and review firewall rules
12. **Which of the following is a proactive threat mitigation technique used by an IPS?**
    a) Packet filtering
    b) Anomaly-based detection
    c) Enabling default configurations
    d) Approving access requests
    Answer: b) Anomaly-based detection

13. **What is the primary goal of network segmentation?**
    a) To allow all traffic to pass
    b) To isolate critical systems and improve security
    c) To consolidate user permissions
    d) To allow full network access to administrators
    Answer: b) To isolate critical systems and improve security
14. **Which type of network segmentation separates users based on department or function?**
    a) Physical segmentation
    b) Logical segmentation
    c) Access segmentation
    d) Role-based segmentation
    Answer: b) Logical segmentation
15. **What is the benefit of isolating critical systems?**
    a) Easier network access for all users

b) Increased protection against unauthorized access
c) Decreased network traffic
d) Reduced need for security reviews
Answer: b) Increased protection against unauthorized access

16. **What is an essential step in developing a network segmentation plan?**
a) Identifying segmentation objectives
b) Reducing firewall complexity
c) Recertifying user access
d) Deploying IDS solutions
Answer: a) Identifying segmentation objectives

17. **What is the primary purpose of encryption?**
a) To store data in plain text
b) To protect sensitive data from unauthorized access
c) To increase file size
d) To reduce processing power
Answer: b) To protect sensitive data from unauthorized access

18. **Which encryption method uses the same key for encryption and decryption?**
a) Symmetric encryption
b) Asymmetric encryption
c) Hashing
d) Biometric encryption
Answer: a) Symmetric encryption

19. **In which scenario is encryption at rest used?**
a) Data being transmitted over the network
b) Data stored on a hard drive
c) Data being printed
d) Data used in volatile memory
Answer: b) Data stored on a hard drive

20. **Which encryption principle ensures data has not been altered?**
a) Confidentiality
b) Integrity
c) Availability
d) Authentication
Answer: b) Integrity

21. **What is a critical component of managing encryption keys?**
a) Key rotation
b) Access review
c) Password complexity
d) Recertification of permissions
Answer: a) Key rotation

22. **What is the role of endpoint security solutions?**
    a) To patch network firewalls
    b) To protect individual devices from threats
    c) To configure access control lists
    d) To manage encryption policies
    Answer: b) To protect individual devices from threats
23. **Which of the following is essential for securing endpoint devices?**
    a) Enabling automatic software updates
    b) Disabling antivirus programs
    c) Storing encryption keys on the device
    d) Allowing all software installations
    Answer: a) Enabling automatic software updates

24. **What is the first step in the patch management process?**
    a) Patch deployment
    b) Patch testing
    c) Patch assessment
    d) Patch removal
    Answer: c) Patch assessment

25. **Why is patch testing necessary?**
    a) To remove outdated patches
    b) To ensure patches do not cause system issues
    c) To delete unused software
    d) To configure firewalls
    Answer: b) To ensure patches do not cause system issues
26. **Which environment should patches be tested in before deployment?**
    a) Production environment
    b) Controlled testing environment
    c) External network
    d) Internal firewall
    Answer: b) Controlled testing environment
27. **Which of the following is a key benefit of patch management?**
    a) Increased system downtime
    b) Protection against known vulnerabilities
    c) Simplified access request workflows
    d) Reduced need for network segmentation
    Answer: b) Protection against known vulnerabilities

28. **Which phase of the encryption key lifecycle involves securely generating keys?**
    a) Key rotation
    b) Key initialization
    c) Key retirement
    d) Key encryption
    Answer: b) Key initialization
29. **How are keys stored securely?**
    a) In plaintext
    b) Using secure storage solutions like HSM (Hardware Security Module)
    c) On user devices
    d) In email attachments
    Answer: b) Using secure storage solutions like HSM
30. **What is the purpose of key retirement?**
    a) To generate new keys
    b) To store keys in a secure database
    c) To securely decommission outdated or compromised keys
    d) To update encryption algorithms
    Answer: c) To securely decommission outdated or compromised keys

Practical assessment

MP Company Headquarter located in Kigali city; it has three branches, one in Nyanza district, Musanze District and another on in Nyagatare district. The employees from Musanze branch no longer provide efficient services to the customers, but instead they are often busy doing unnecessary activities on the internet. As Network technician; you are requested to make necessary configurations on appropriate router so that the users in Musanze branch cannot communicate with the web server which is located at headquarter network and make necessary IDS configuration to monitor network traffic.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	**NO**
	security configuration is well planned	1.1 Devices are selected		
		1.2 Headquarter Network (Kigali) are identified		
		1.3 Nyagatare Branch Network are identied		

SN	Criteria	Indicators	Observa-tion	
			YES	**NO**
1		1.4 Musanze branch network is identified		
		1.5 Nyanza Branch Network are identified		
		1.6 ACL Type are chosen		
		1.7 Placement of ACL are decided		
2	Security is well configured	2.1 Login Credentials are config-ured		
		2.2 Access List Deny Rule are cre-ated		
		2.3 Other Traffic are allowed		
		2.4 ACL to Interface are applied		
3	Network security monitoring is well implemented	3.1 Log Traffic are genereted		
		3.2 Review ACL are schedured		
		3.3 Documentation are genereted		

Further information to the trainer

Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2003). *Role-Based Access Control*. Artech House.

FIPS PUB 197. (2001). *Advanced Encryption Standard (AES)*. National Institute of Standards and Technology (NIST).

Harris, S. (2016). *CISSP All-in-One Exam Guide*. McGraw-Hill Education.

ISO/IEC 27001:2013. (2013). *Information technology – Security techniques – Information security management systems – Requirements*. International Organization for Standardization (ISO).

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94.

SolarWinds. (n.d.). What Is Role-Based Access Control (RBAC)? Definition and Benefits . https://www.solarwinds.com/resources/it-glossary/role-based-access-control

Rippling. (2024, August). Role-based access control (RBAC): What it is, benefits, and examples. https://www.rippling.com/blog/role-based-access-control

Fortinet. (n.d.). Configuring Intrusion Detection. *FortiRecorder 7.2.2 Administration Guide*. https://docs.fortinet.com/document/fortirecorder/7.2.2/administration-guide/206849/configuring-intrusion-detection


SECURITY BREACH!

Indicative contents

3.1 Security Threats Monitoring
3.2 Applying Monitoring Techniques and Threat Intelligence
3.3 Conducting Methodical Threat Hunting with Intelligence Feeds
3.4 Monitoring Network and System Logs
3.5 Systems Scanning and Penetration Testing

Key Competencies for Learning Outcome 3: Perform monitoring and detection

Knowledge	Skills	Attitudes
• Description of Security Threats Monitoring and Detection • Description of Monitoring Tools • Description of Monitoring Techniques • Description of Advanced Monitoring Techniques • Description of Security Threat Hunting • Description of Network and System Logs • Identification of Logging Tools and Real-time Monitoring • Description of Efficient Systems Scanning • Description of Penetration Testing	• Selecting Cyber Security Monitoring Tools • Conducting Methodical Threat Hunting with Intelligence Feeds • Using Logging Tools for Real-time Monitoring • Conducting Efficient Systems Scanning • Conducting penetration testing	• Having team spirit while working with others. • Being responsible. • Being organized to achieve the required result. • Having Curiosity. • Being Accountable • Being resilience. • Attention to details

Duration: 15 hrs

Learning outcome 3 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe clearly Security Threats Monitoring within an organization.
2. Describe clearly Security Threats Detection within an organization
3. Describe Accurately the different types of monitoring tools used in cybersecurity
4. Differentiate Clearly between standard and advanced monitoring techniques
5. Describe properly the process of security threat hunting, using intelligence feeds to actively search for potential threats.
6. Analyze correctly Network and System Logs for detecting suspicious activity
7. Select properly Logging and Monitoring Tools
8. Describe correctly Efficient System Scanning Methods
9. Conduct properly Cybersecurity Penetration Testing
10. Conduct properly System Scanning and Logging for Real-time Threat Monitoring
11. Apply clearly methodical approaches to threat hunting by utilizing intelligence feeds and advanced monitoring techniques.
12. Report correctly Findings from Penetration Testing and Monitoring

Resources

Equipment	Tools	Materials
• Computer	• SIEM • Solar Wind Snort • Wireshark • Nessus • Graylog • Anti-virus	• Internet

Advance Preparation:

Before delivering this learning outcome, you are recommended to:

- Avail equipment, tools, material and software used in cyber security for implementing security measures
- Avail working environment

Indicative content 3.1: Security Threats Monitoring

Duration: 3 hrs

Theoretical Activity 3.1.1: Description of Security Threats Monitoring and Detection

Notes to the trainer:

- Trainer may use small group to describe Security Threats Monitoring and Detection

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Overview of Security Threats and Attacks

ii. What is Threat Monitoring

iii. What are Importance of Threat Monitoring

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 3.1.1

Points to Remember

- There are many types of threats such us Malware, Phishing Attacks, Distributed Denial-of-Service (DDoS), Insider Threats, SQL Injection, Man-in-the-Middle (MitM) Attacks, Advanced Persistent Threats (APTs), Zero-Day Exploits, Brute Force Attacks
- Security threats monitoring involves keeping a close watch on network activities, system logs, and user behaviour to detect any suspicious or harmful actions.
- The goal is to identify potential threats early so that organizations can respond quickly, prevent data breaches, and protect their systems from attacks

Theoretical Activity 3.1.2: Description of Monitoring Tools

Notes to the trainer:

- Trainer may use small group to describe monitoring tools

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Intrusion Detection Systems (IDS) tools
ii. What are Security Information and Event Management (SIEM) Tools
iii. How can you Identify the Right IDS Tools and Right SIEM Tools?

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 3.1.2

Points to Remember

- Intrusion Detection Systems (IDS) monitor network traffic and system activity for signs of attacks or suspicious behaviour. They alert security teams when something unusual is detected. There are two types: Network-based IDS (NIDS) and Host-based IDS (HIDS).
- Security Information and Event Management (SIEM) Tools gather and analyze security data from various sources like network devices and servers. SIEM tools provide a complete view of security events in real time, help identify complex threats, and generate reports for compliance with regulations.
- When selecting IDS tools, it's important to ensure the tool covers all necessary areas, such as network or device monitoring. It should be able to detect both known threats (using signature-based methods) and new, unknown threats (through anomaly detection.

- SIEM tools, organizations need to choose one that can easily collect and analyze data from multiple sources, detect patterns of complex attacks, and grow with the network. The SIEM tool should be user-friendly and help meet compliance requirements by generating reports needed for audits.

Practical Activity 3.1.3: Selecting Cyber Security Monitoring Tools

Notes to the trainer

- This activity should take place in a computer lab where trainees should Select different software and hardware monitoring tools
- Avail computers
- Avail IDS Tools and SIEM Tools

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

You are tasked to go in computer and select different tools to be used in network monitoring

Step 2: Explain the task and provide clear work instruction

Step 3: Demonstrate how to select Cyber Security Monitoring Tools. While demonstrating, explain the selecting procedures.

Step 4: Ask trainees to select Cyber Security Monitoring Tools and monitor the procedures.

Step 6: Verify whether Cyber Security Monitoring Tools are selected

Step 7: Address any questions or concerns

Step 8: Ask trainee to read key reading 3.1.3

Points to Remember

Steps to selecting the right cybersecurity monitoring tools

1. Assess Organizational Needs
2. Define Functional Requirements
3. Evaluate Tool Types
4. Consider Ease of Use and Management.
5. Test & Compare Tool Options
6. Budget and Total Cost of Ownership

Application of learning 3.1.

H.D is a company with many employees across different departments. The company needs to monitor its network traffic, and you are tasked with selecting tools that can help achieve this goal.

Checklist:

Main Points to Check	Observation	
	YES	NO
IDE is well selected		
SIEM is well selected		

Indicative content 3.2: Applying Monitoring Techniques and Threat Intelligence

Duration: 3 hrs

Theoretical Activity 3.2.1: Description of Monitoring Techniques

Notes to the trainer:

- Trainer may use small group to describe monitoring techniques

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe to Monitoring Techniques
ii. What is Indicator of Compromise (IoC) Monitoring
iii. What is Behavior-Based and Signature-Based Monitoring

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 3.1.2

Points to Remember

Monitoring techniques are vital for the real-time identification and response to security threats within an organization's network. These techniques include various strategies and tools designed to detect, analyze, and address potential threats, thereby improving security and ensuring compliance with regulatory standards.

Indicators of Compromise (IoCs), which are forensic data points that signal potentially malicious activities, such as unusual file changes or abnormal traffic. Continuous monitoring for IoCs allows organizations to detect intrusions early and take action to reduce potential harm, often utilizing tools that integrate threat intelligence feeds for current threat information.

Signature-based monitoring detects known threats using predefined patterns

Behavior-based monitoring focuses on analyzing deviations from normal user and entity behavior to identify anomalies that may indicate security breaches.

Theoretical Activity 3.2.2: Description Advanced Monitoring Techniques

Notes to the trainer:

- Trainer may use small group to describe Advanced Monitoring Techniques

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Zero-Day, Phishing, and Malware Attacks Monitoring
ii. What is Vulnerability Monitoring
iii. Explain Threat Hunting and Incident Response

Step2: Ask trainees to present their findings to the whole class.

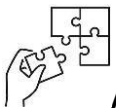
Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 3.2.2

Points to Remember

- Advanced monitoring techniques are crucial for detecting sophisticated threats, including zero-day exploits, phishing attacks, and malware.
- Zero-day exploits take advantage of vulnerabilities unknown to vendors, while phishing tricks users into revealing sensitive information, and malware can compromise systems and exfiltrate data
- vulnerability monitoring plays a key role by continuously scanning systems for known vulnerabilities, allowing organizations to prioritize remediation efforts based on severity. Regular vulnerability assessments and effective patch management are essential to maintaining robust security.
- Tthreat hunting proactively identifies potential threats, while incident response focuses on managing security incidents when they occur, minimizing damage and facilitating rapid recovery. Integrating both practices enhances an organization's adaptability to evolving threats and strengthens its overall security posture.



Application of learning 3.2.

XYZ Corporation is enterprise, Recently, the company has faced increased threats, including phishing attacks and potential vulnerabilities in its systems. To enhance its security posture, XYZ Corporation aims to implement advanced monitoring techniques. As a cybersecurity analyst at XYZ Corporation, you are tasked to explain both basic and advanced monitoring techniques.

Checklist:

Main Points to Check	Observation	
	YES	NO
Indicator of Compromise (IoC) Monitoring is well explained		
Behavior-Based and Signature-Based Monitoring are well explained		
Zero-Day, Phishing, and Malware Attacks Monitoring are well explained		
Vulnerability Monitoring is well explained		
Threat Hunting and Incident Response is well explained		

Indicative content 3.3: Conducting Methodical Threat Hunting with Intelligence Feeds

Duration: 3 hrs

Theoretical Activity 3.3.1: Description Threat Hunting

Notes to the trainer:

- Trainer may use small groups to describe threat hunting

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Security Threat Hunting Methods
ii. What are threat hunting process (Collecting and Analyzing Threat Intelligence, Identifying and Validating Threats, Incident Response Procedures, Documentation and Reportings)

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 3.3.1

Points to Remember

- The primary methods of threat hunting include: Hypothesis-Driven Hunting**,** Indicator-Based Hunting**,** Behavioral Analysis**,** Machine Learning and Automation
- Threat hunting process include Collecting and Analyzing Threat Intelligence, Identifying and Validating Threats, Incident Response Procedures, Documentation and Reporting.

Practical Activity 3.3.2: Conducting Methodical Threat Hunting with Intelligence feeds

Notes to the trainer

- This activity should take place in a computer lab where trainees should Select different software and hardware monitoring tools
- Avail computers with Malware Information Sharing Platform

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

You are tasked to go in computer and use Malware Information Sharing Platform for threat hunting

Step 2: Explain the task and provide clear work instruction

Step 3: Demonstrate how to conduct threat hunting. While demonstrating, explain the conducting procedures.

Step 4: Ask trainees to select to conduct threat hunting and monitor the procedures.

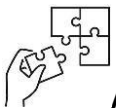
Step 5: Address any questions or concerns

Step 6: Ask trainee to read key reading 3.3.2

Points to Remember

Steps for using MISP (Malware Information Sharing Platform) for threat hunting:

1. Setup and Configuration
2. Data Collection
3. Creating Attributes and Events
4. Data Analysis and Correlation
5. Threat Hunting
6. Collaboration and Information Sharing
7. Documentation and Reporting
8. Continuous Improvement
9. Automation (Optional)



Application of learning 3.3.

In VITAL financial institution, the security team has identified an uptick in phishing attempts targeting their employees. To enhance their threat-hunting efforts, they decide to utilize MISP to share, analyze, and respond to relevant threat intelligence.

Checklist:

Main point to check	**observation**	
	YES	**NO**
Relevant IoCs collected		
IoCs documented accurately in the event		
Successful phishing attempts or suspicious activities identified		
Response activities are documented		

Indicative content 3.4: Monitoring Network and System Logs

Duration: 3 hrs

Theoretical Activity 3.4.1: Description of Network and System Logs

Notes to the trainer:

- Trainer may use small groups to describe network and system logs

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Network and System Logs Monitoring
ii. What are Role of Logs in Security?
iii. Describe of Logging Policies and Standards?

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 3.3.1

Points to Remember

- Monitoring Network and System Logs involves collecting, analyzing, and reviewing log data from network devices, servers, applications, and systems to detect security threats, performance issues, and operational irregularities. Logs capture critical events like user access, configuration changes, and network errors, helping organizations identify potential risks in real time.
- Role of Logs in Security is essential for detecting anomalies, supporting incident response, and ensuring compliance. Logs provide a detailed history of system activities, assisting in identifying suspicious behavior and breaches, aiding forensic investigations, and helping organizations meet regulatory requirements.

- Logging Policies and Standards define how logs should be generated, stored, and managed. These policies cover data retention, log integrity, log generation, and audit reviews. Protecting logs from tampering and ensuring they are reviewed regularly is critical for maintaining security.
- Common standards, like NIST Special Publication 800-92 and ISO/IEC 27001, provide guidelines for effective log management and monitoring, helping organizations follow best practices for security and compliance.

Theoretical Activity 3.4.2: Identification of Logging Tools and Real-time Monitoring

Notes to the trainer:

- Trainer may use small groups to describe Identify Logging Tools and Real-time Monitoring

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. What are criteria for Selecting of Logging Tools
ii. How can you Implementing Log Management for Real-time Monitoring?
iii. How can you Implementing Automated Alerts and Thresholds?

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 3.3.1

Points to Remember

- Selection of Logging Tools is crucial for effective log management. When choosing a logging tool, consider factors like scalability, ensuring it can handle your organization's log volume, and centralized log management, which consolidates logs from different sources into one place. It should support search and analysis to help quickly detect anomalies and integrate with other security tools like SIEM or IDS.

Common tools include Syslog (for Unix systems), Windows Event Viewer, Splunk, and Graylog for log collection and analysis.

- Implementing Log Management for Real-time Monitoring involves continuously analyzing logs to detect issues as they occur. This process requires centralizing logs, ensuring log normalization for easy analysis, setting log retention policies, and using SIEM systems to provide a comprehensive view of network security. These steps ensure logs are efficiently managed and monitored.
- Automated Alerts and Thresholds are vital for real-time log monitoring. They notify security teams when suspicious activities arise by defining thresholds (e.g., for failed logins), configuring alerts to trigger notifications via email or SMS, and tuning alerts to balance between sensitivity and false positives. Response mechanisms should be in place, outlining actions when alerts are triggered, like investigation or incident escalation.

Practical Activity 3.4.3: Using Logging Tools for Real-time Monitoring

Notes to the trainer

- This activity should take place in a computer lab where trainees should monitor Logs
- Avail computers with greylog installed

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

You are tasked help school to monitor network and system logs by using Graylog tools
Step 2: Explain the task and provide clear work instruction

Step 3: Demonstrate how to monitor network and system logs. While demonstrating, explain the monitoring procedures.

Step 4: Ask trainees to select to monitor network and system logs and monitor the procedures.

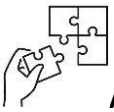
Step 5: Address any questions or concerns

Step 6: Ask trainee to read key reading 3.4.3

Points to Remember

Steps for using Greylog for network and system logs monitoring:

Step 1: On the sign-in screen, enter the default admin username and password to navigate to the dashboard.
Step 2: click on System/Inputs to configure a Global input to listen to incoming messages.
Step 3: Select Raw/Plaintext TCP from the drop-down selection and click on Launch new input to open the configuration page for the Global input
Step 4: Leave all TLS settings as their defaults
Step 5: Send a message via the command line
Step 6: Data collection and organization
Step 7: Configure Rsyslog messages



Application of learning 3.4.

You have been tasked by INET's IT department to help monitor their network and system logs to improve cybersecurity. The company wants to ensure timely identification and response to any security incidents. Your role is to implement Graylog for centralized log management, collect logs from key network devices and systems, and configure Graylog to generate alerts for suspicious activities or anomalies.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	1 Graylog is well used	1.1 Graylog on the server is configured		
		1.2 Logs from network device are collected		
		1.3 Logs from key systems are collected		
		1.4 Real-time alerts for suspicious activities are configured		

SN	Criteria	Indicators	Observation	
			YES	NO
		1.5 Log monitoring dashboard for analysis are used		

Indicative content 3.5: Systems Scanning and Penetration Testing

Duration: 3 hrs

Theoretical Activity 3.5.1: Description of Efficient Systems Scanning

Notes to the trainer:

- Trainer may use small groups to describe efficient system scanning

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. What is Efficient Systems Scanning
ii. Importance of Efficient Systems Scanning
iii. Describe Explaining the Significance of Efficient Scanning
iv. Describe Well-Established Cybersecurity Principles
v. Explain Methods for Efficient Systems Scanning
vi. Describe of Vulnerability Scanning Tools and Management
vii. Explain Regular Compliance Scanning and Patch Management

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 3.5.1

Points to Remember

- Efficient systems scanning is essential for identifying vulnerabilities, weaknesses, and misconfigurations in an organization's infrastructure, enabling faster responses to security threats. It improves overall security by detecting risks in real-time and ensuring compliance with standards.
- Effective scanning is based on cybersecurity principles such as confidentiality, integrity, and risk management.
- Methods for efficient scanning include maintaining an asset inventory, using vulnerability scanning tools like Nessus and OpenVAS, and implementing strong vulnerability management practices.

- Regular compliance scanning helps organizations meet regulatory requirements, while patch management ensures timely remediation of vulnerabilities. Together, these practices strengthen an organization's security posture and protect it from emerging threats.
-

Theoretical Activity 3.5.2: Description of penetration testing

Notes to the trainer:

- Trainer may use small groups to describe penetration testing

Key steps:

While delivering this activity, pass through the following steps:

Step1: Introduce the activity and ask trainees to answer to following questions:

i. Describe Penetration Testing
ii. What are Importance of Penetration Tests
iii. Identify Tools for Penetration Tests
iv. Implementing Effective Penetration Tests

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 3.5.2

Points to Remember

- Penetration testing, or ethical hacking, simulates cyber attacks on an organization's systems, networks, or web applications to identify and exploit vulnerabilities, thereby assessing the security posture of the organization. This process mimics the tactics of real attackers, helping organizations discover weaknesses before they can be maliciously exploited.
- The importance of penetration testing includes identifying security flaws not detected in regular assessments, evaluating the risk of vulnerabilities, ensuring compliance with regulations like PCI DSS and HIPAA, improving overall security, and testing the effectiveness of existing security measures.

- Various tools assist in penetration testing, such as Metasploit, Nessus, Burp Suite, OWASP ZAP, and Kali Linux, which automate processes and provide analysis capabilities.
- Effective penetration tests follow a structured approach, including planning, reconnaissance, scanning, exploitation, post-exploitation, reporting, remediation, and retesting. By adhering to this approach, organizations can enhance their security posture and address vulnerabilities effectively.

Practical Activity 3.5.3: Conducting system scanning penetration testing

Notes to the trainer

- This activity should take place in a computer lab where trainees conduct system scanning and penetration testing
- Avail computers with Kali linux installed

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

You are tasked to help school for system and network scanning and conduction penetration testing by using Kali Linux

Step 2: Explain the task and provide clear work instruction

Step 3: Demonstrate how to conduct system and network scanning and penetration testing. While demonstrating, explain procedures.

Step 4: Ask trainees to select to conduct system and network scanning and penetration testing and monitor the procedures.

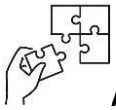
Step 5: Address any questions or concerns

Step 6: Ask trainee to read key reading 3.5.3

Points to Remember

Steps for using kali linux for scanning and penetration testing:

Step 1: Planning and Preparation
Step 2: Reconnaissance
Step 3: Network Scanning
Step 4: Vulnerability Scanning
Step 5: Exploitation
Step 6: Post-Exploitation
Step 7: Reporting
Step 8: Remediation and Retesting



Application of learning 3.5.

ICP Company has identified the need to enhance its cybersecurity posture due to recent security incidents. As part of this initiative, they have decided to conduct a thorough penetration test using Kali Linux to identify vulnerabilities in their network infrastructure. The penetration testing team will follow a structured approach to ensure all aspects of the test are covered, from planning to remediation.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	**1.Penetration Testing is well conducted**	1.1 systems, networks, or applications are identified		
		1.2 Open ports on the target systems are identified		
		1.3 Vulnerability Scanners are used		
		1.4 vulnerability reports are generated		

Learning outcome 3 end assessment

Theoretical assessment

SECTION I. Choose the letter corresponding to the correct answers

1. **What is the primary purpose of security threat monitoring?**

   a) To prevent data loss
   b) To detect and respond to security threats
   c) To create security policies
   d) To perform regular backups
   Answer: B) To detect and respond to security threats

2. **Which of the following is a key component of an Intrusion Detection System (IDS)?**

   a) Network segmentation
   b) User authentication
   c) Traffic analysis
   d) Firewall rules
   Answer: C) Traffic analysis

3. **What does SIEM stand for in the context of cybersecurity?**

   a) Security Information and Event Management
   b) Security Incident and Emergency Management
   c) Security Infrastructure and Event Monitoring
   d) Security Integration and Event Management
   Answer: A) Security Information and Event Management

4. **Which type of monitoring focuses on known malicious behaviors?**

   a) Behavior-Based Monitoring
   b) Signature-Based Monitoring
   c) IoC Monitoring
   d) Vulnerability Monitoring
   Answer: B) Signature-Based Monitoring

5. **What is an Indicator of Compromise (IoC)?**

    a) A threat detection system
    b) A piece of forensic evidence
    c) A malicious actor's IP address
    d) A signature of a known threat
    Answer: D) A signature of a known threat

6. **Which of the following techniques helps in identifying potential security threats before they materialize?**

    a) Signature-Based Monitoring
    b) Behavior-Based Monitoring
    c) Threat Hunting
    d) Log Analysis
    Answer: C) Threat Hunting

7. **What is a zero-day attack?**

    a) An attack that occurs after a vulnerability is patched
    b) An attack that exploits a previously unknown vulnerability
    c) An attack that occurs on the first day of a new system
    d) An attack that uses outdated software
    Answer: B) An attack that exploits a previously unknown vulnerability

8. **Which of the following is NOT a common tool used for security monitoring?**

    a) IDS
    b) SIEM
    c) Antivirus Software
    d) Firewall
    Answer: C) Antivirus Software

9. **What does threat intelligence refer to?**

    a) Information about current and potential security threats
    b) User access levels and permissions
    c) Data encryption methods
    d) System backup strategies
    Answer: A) Information about current and potential security threats

10. **Which of the following is an example of a phishing attack?**

    a) Sending an email that looks legitimate but leads to a malicious site
    b) Exploiting a software vulnerability to gain unauthorized access
    c) Using social engineering to manipulate an insider
    d) Distributing malware via a USB device
    Answer: A) Sending an email that looks legitimate but leads to a malicious site

11. **What is the main objective of conducting vulnerability monitoring?**

    a) To identify and fix software bugs
    b) To ensure compliance with security policies
    c) To discover weaknesses in systems that could be exploited
    d) To enhance system performance
    Answer: C) To discover weaknesses in systems that could be exploited

12. **Which method is used to validate the effectiveness of security controls?**

    a) Incident Response
    b) Penetration Testing
    c) Threat Hunting
    d) Vulnerability Scanning
    Answer: B) Penetration Testing

13. **What is the role of automated alerts in security monitoring?**

    a) To create user accounts
    b) To provide notifications of potential security incidents
    c) To manage user access permissions
    d) To perform data backups
    Answer: B) To provide notifications of potential security incidents

14. **What type of monitoring technique involves analyzing system and network logs?**

    a) Behavioral Monitoring
    b) Signature-Based Monitoring
    c) IoC Monitoring
    d) Log Analysis
    Answer: D) Log Analysis

15. **Which of the following best describes incident response procedures?**

    a) Steps taken to monitor system activity
    b) Actions taken to address and manage the aftermath of a security incident
    c) Guidelines for user behavior
    d) Techniques for vulnerability scanning
    Answer: B) Actions taken to address and manage the aftermath of a security incident

16. **Which tool is primarily used to aggregate and analyze security data from multiple sources?**

    a) IDS
    b) SIEM
    c) Antivirus
    d) Firewall
    Answer: B) SIEM

17. **What does behavior-based monitoring rely on?**

    a) Known attack signatures
    b) User and entity behavior analytics
    c) Real-time system updates
    d) Historical performance data
    Answer: B) User and entity behavior analytics

18. **In the context of threat hunting, what is the purpose of collecting threat intelligence?**

    a) To prepare budget estimates for security tools
    b) To understand the tactics, techniques, and procedures of threat actors
    c) To classify user roles
    d) To perform compliance audits
    Answer: B) To understand the tactics, techniques, and procedures of threat actors

19. **Which term describes malicious software designed to disrupt or damage a computer system?**

    e) Phishing
    a) Malware
    b) Ransomware

c) Spyware
Answer: B) Malware

20. **What is a primary benefit of using SIEM tools in security monitoring?**

a) Simplified software installation
b) Comprehensive threat detection and analysis
c) Reduced need for user training
d) Faster system performance
Answer: B) Comprehensive threat detection and analysis

SECTION II. Read the statement below and answer by TRUE if it is correct or FALSE if it is incorrect

1. Network and system logs play a critical role in identifying and responding to security incidents.
Answer: True

2. Logging policies and standards are irrelevant to the effectiveness of log monitoring.
Answer: False

3. Real-time monitoring of logs allows organizations to detect security threats as they occur.
Answer: True

4.Implementing automated alerts and thresholds is an optional step in log management that does not significantly enhance security monitoring.
Answer: False

5. The selection of logging tools is crucial for ensuring that log data is captured and analyzed effectively.
Answer: True

6. Network and system logs can only provide historical data and do not assist in real-time threat detection.
Answer: False

7. Comprehensive logging practices contribute to regulatory compliance and help in audits.
Answer: True

SECTION II. Match Systems Scanning and Penetration Testing topics in column A with their correct description in column B

Answers	COLUMN A	COLUMN B
…C…	1. Asset Inventory Methods	A. Regular evaluations of systems to ensure compliance with security policies
…B…	2. Penetration Tests	B. Techniques used to simulate attacks on a system to identify security vulnerabilities.
…D…	3. Vulnerability Scanning Tools	C. The process of identifying and managing hardware and software assets.
…A…	4. Compliance Scanning and Patch Management	D. Tools used to assess vulnerabilities in applications and systems

Practical assessment

AGZA is organization. Recently, the organization has experienced an increase in security incidents, including phishing attempts and potential malware infections. An organization has decided to enhance its security posture by implementing security threat monitoring strategies. You are tasked To set up an effective monitoring system using Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) tools, apply monitoring techniques, conduct threat hunting, monitor logs, and perform penetration testing.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	**1.Monitoring Tools are well Setup**	1.1 IDS tools are selected		
		1.2.SIEM tools are selected		
		1.3.IDS and SIEM tools are installed		
		1.4.Tools are configured		
2	**2.Monitoring Techniques well Applied**	2.1 IoC monitoring are implemented		
		2.2 behavior-based monitoring are established		
		2.3 signature-based monitoring are established		

SN	Criteria	Indicators	Observation	
			YES	NO
3	**3. Threat Hunting are well Conducted**	3.1 Relevant threat intelligence are gathered		
		3.2 Threat hunting session are conducted		
		3.3 Findings and incidents are documented		
4	**4. Network and System Logs are well Monitored**	4.1 Policies and standards are established		
		4.2 Log management tools are implemented		
		4.3 Automated alerts and thresholds are configured		
		4.4 Penetration testing are conducted		
		4.5 Results are documented		

Further information to the trainer

Manning, K., & Williams, D. (2017). *Security Operations Center: Building, Operating, and Maintaining Your SOC*. Syngress.

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. National Institute of Standards and Technology (NIST) Special Publication 800-94.

Wang, C. (2020). *Cybersecurity Monitoring and Threat Intelligence: A Practical Guide*. CRC Press.

Zhao, W. (2019). *Penetration Testing: A Hands-On Introduction to Hacking*.

Montclair State University. (2024, July 5). *Cybersecurity Awareness Training*. Retrieved from https://www.montclair.edu/information-technology/security/cybersecurity-awareness-training/

SentinelOne. (n.d.). *Cyber Security Monitoring: Definition and Best Practices*. Retrieved from https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-monitoring/

Exabeam. (2024, January 5). *Threat Detection and Response: Technologies and Best Practices*. Retrieved from https://www.exabeam.com/explainers/new-scale-siem/threat-detection-and-response-technologies-and-best-practices/

Cyvent. (2024, January 5). *Choosing the Right Cybersecurity Monitoring System: Tips and Tools*. Retrieved from https://www.cyvent.com/blog/choosing-the-right-cybersecurity-monitoring-system

ECCU. (2024, January 5). *Methods and Technologies to Detect Cyber Attacks*. Retrieved from https://www.eccu.edu/blog/methods-technologies-detect-cyber-attacks/

SISA Infosec. (2024, January 5). *4 Types Of Cyber Threat Hunting Tools In 2024*. Retrieved from https://www.sisainfosec.com/blogs/4-types-of-cyber-threat-hunting-tools/

Exabeam. (2024, January 5). *SOC and SIEM: The Role of SIEM Solutions in the SOC*. Retrieved from https://www.exabeam.com/explainers/siem-security/the-soc-secops-and-siem/


Recovery
65%
Cancel

Indicative contents
4.1 Developing Incident Response Plan **4.2 Developing Incident Recovery Plan** **4.3 Identification of Security Incident** **4.4 Isolation of Affected System** **4.5 Conducting Methodical Forensic Analysis** **4.6 Restoring System and Data**

Key Competencies For Learning Outcome 4: Perform Incident Response And Recovery

Knowledge	Skills	Attitudes
• Description Incident Response Planning. • Description of Develop in Incident Response Plans. • Description of Plan Incident Recovery. • Description of Developing Incident Recovery Plans • Description of Security Incident. • Identification of Incident Detection Techniques. • Description of response and reporting in security incident. • Description of threat intelligence integration for incident classification and prioritization. • Description of Immediate Action and Communication in isolation of affected system. • Description system isolation techniques and analysis of affected systems. • Description of recovery planning and communication.	• Creating Incident Response Policy. • Assessing risk and Business Impact Analysis (BIA). • Developing Incident Recovery Plans. • Testing of Incident Recovery. • Applying response in security incident. • Developing System Isolation Techniques • Analysing affected systems. • Conducting Forensic Analysis. • Restoring and validating of system and data. • Auditing and Compliance	• Being mind set focused. • Being Commitment. • Being Collaboration. • Being resilience. • Attention to details

• Description of fundamentals forensic Analysis. • Description of evidence documentation and analysis. • Description of quality assurance and legal aspects. • Description of System and Data Restoration. • Description of post-restoration actions and documentation.	Checks of system and data restoration	

Duration: 15hrs

Learning outcome 4 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe clearly Security Threats Monitoring within an organization.
2. Describe clearly Security Threats Detection within an organization
3. Describe Accurately the different types of monitoring tools used in cybersecurity
4. Differentiate Clearly between standard and advanced monitoring techniques
5. Describe properly the process of security threat hunting, using intelligence feeds to actively search for potential threats.
6. Analyze correctly Network and System Logs for detecting suspicious activity
7. Select properly Logging and Monitoring Tools
8. Describe correctly Efficient System Scanning Methods
9. Conduct properly Cybersecurity Penetration Testing
10. Conduct properly System Scanning and Logging for Real-time Threat Monitoring
11. Apply clearly methodical approaches to threat hunting by utilizing intelligence feeds and advanced monitoring techniques.
12. Report correctly Findings from Penetration Testing and Monitoring

Resources

Equipment	Tools	Materials
• Computers • External HDD	• Cuckoo Sandbox • Virus Total • Wireshark • SolarWinds • QRadar • CrowdStrike • Carbon Black • Autopsy • Proofpoint • Veeam • Acronis • Firewalls	• Internet Access

Advance Preparation:

Before delivering this learning outcome, you are recommended to:

- Avail tools, materials and equipment used for Incident Response Plan in cyber security.
- To have a Computer, which installed Cuckoo, Sandbox and Acronis with accept internet connection.

Indicative content 4.1: Developing Incident Response Plan

Duration:3hrs

Theoretical Activity 4.1.1: Description of Incident Response Planning.

Notes to the trainer:

- Trainer may use small group to describe Incident Response Plan

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and request trainees to answer the following questions:

i. What is importance of incident response?
ii. Identify Key Stakeholders in Incident Response.
iii. Define Scope and Objectives.

Step2: Ask trainees to present their findings to the whole class.

Step3: Provides expert view on presented contents.

Step4: Address any questions or concerns.

Step5: Ask trainee to read the key readings on activity 4.1.1

Points to Remember

- An incident response plan (IRP) is a structured approach to handling and mitigating security breaches and other cyber incidents
- Key stakeholders in incident response are IT Security Team, Legal/Compliance Team, Public Relations (PR) Team, Human Resources (HR) Team, Executive Management, Third-Party Vendors
- The IRP should define the types of incidents it covers, such as data breaches, malware attacks, and denial-of-service (DoS) attacks.
- The plan should outline the goals of incident response, such as minimizing damage, restoring operations quickly, and complying with legal requirements.

Theoretical Activity 4.1.2: Description of Incident Response Plans development

Notes to the trainer:

- Trainer may use small group to describe incident response plans development.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions:

i. Describe incident response policy
ii. Identify incident detection and reporting
iii. What is response procedures
iv. What is incident containment
v. What is eradication and recovery
vi. Give Legal and Regulatory Compliance
vii. Explain Documentation and Record Keeping
viii. Describe Training and Awareness
ix. What is Post-Incident Analysis
x. Describe Board and Executive Reporting
xi. Describe Public Relations and Reputation Management
xii. Describe DR/BCP Integration

Step 2: Ask trainees to present their findings to the whole class.

Step 3: Provide expert view on presented content

Step 4: Address any questions or concerns

Step 5: Ask trainees to read the Key readings 4.1.2 in the trainee manuals

Points to Remember

- An Incident Response Plan (IRP) helps an organization respond to security incidents quickly and efficiently. It outlines steps to detect, manage, and recover from incidents to reduce damage and downtime.
- The Incident Response Policy explains how incidents will be handled. It lists the steps for reporting, responding to, and resolving security incidents, ensuring everyone understands their role.
- Incident detection involves identifying threats using tools like Intrusion Detection Systems (IDS). Once detected, incidents should be reported immediately, so the response team can act quickly.

- Response procedures are step-by-step actions the team takes to manage an incident. The goal is to limit the damage and ensure critical systems continue to function.
- Incident containment focuses on stopping the spread of the incident. For example, compromised systems may be disconnected from the network to prevent further harm.
- Once contained, the focus shifts to eradication, which involves removing the cause of the incident, such as malware. Then, the team works on recovery, restoring systems to normal operation.
- A communication plan ensures that everyone, including staff and external stakeholders, is informed during the incident. Clear communication builds trust and helps manage the situation.
- It's important to follow legal and regulatory guidelines during an incident. Organizations must ensure they comply with laws like GDPR or HIPAA, reporting incidents when required.
- Keeping detailed records during an incident helps with future analysis and legal reporting. Proper documentation ensures that every action taken is tracked.
- Training and awareness programs help employees recognize and report incidents. Regular training ensures everyone is prepared to respond when necessary.
- After an incident, a post-incident analysis reviews what happened and identifies ways to improve the response for the future.
- The incident response team must provide reports to leadership, explaining the incident's impact and actions taken to resolve it.
- Managing public communication during an incident is crucial. A clear public relations strategy ensures the organization's reputation is protected.
- The incident response plan should be integrated with the organization's Disaster Recovery (DR) and Business Continuity Plans (BCP) to ensure the company continues operating during an incident.

Practical Activity 4.1.3: Creating Incident Response Policy

Notes to the trainer

- This activity should take place in a computer lab where trainees should create incident response policy
- Avail computers with Document editor installed
- Avail Incident recovery plan template

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

> By ensuring that all trainer and trainee are aware of their roles and responsibilities, creating incident response policy that formalize set of guidelines and procedures to govern the school's response to security incidents.

Step 2: Explain the task and provide clear work instruction
Step 3: Identify how to Create Incident Response Policy. While identifying, explain the creation of incident response policy procedures.
Step 4: Ask trainees to create response incident policy and monitor the procedures.
Step 6: Verify whether response incident policy is created
Step 7: Address any questions or concerns
Step 8: Ask trainee to read key reading 4.1.3

Points to Remember

While creating incident response policy you must consider key point:
1. Authority and Review
2. Purpose and Objectives
3. Standards and Frameworks
4. Common Security (Common Threat Vectors and Common Cyber Incidents)
5. Roles and Responsibilities
6. Communications
7. Incident Notification and Reporting
8. Containment
9. Documentation

Application of learning 4.1.

IGN, a growing sales company, relies heavily on its digital infrastructure to manage customer data, sales transactions, and vendor communications. Recently, there has been a noticeable rise in phishing emails targeting staff, resulting in a few incidents where unauthorized access to company emails was granted. You are tasked to develop a formal incident response policy to manage these security threats efficient.

Checklist:

SN	Criteria	Indicators	Observation	
			Yes	No
1	Incident response policy is well created	1.1 Authority and Review are included		
		1.2 Purpose and Objectives are identified		
		1.3 Standards and Frameworks are provided		
		1.4 Common Security are identified		
		1.5 Roles and Responsibilities are identified		
		1.6 Communications are provided		
		1.7 Incident Notification and Reporting are prepared		
		1.8 Containment are identified		
		1.9 Documentation in provided		

Indicative content 4.2: Developing Incident Recovery Plan

Duration: 3hrs

Theoretical Activity 4.2.1: Description of Plan Incident Recovery

Notes to the trainer:

- Trainer may use small group to describe on plan incident recovery.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions:

i. Identify key Stakeholders
ii. Describe Objectives and Scope
iii. Describe Risk Assessment and Business Impact Analysis (BIA)
iv. Explain Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)

Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 4.2.1 in the trainee manuals

Points to Remember

- The Incident Recovery Plan is an essential part of cybersecurity that outlines how an organization can recover from security incidents like cyberattacks or system failures. This plan focuses on restoring normal operations while minimizing the impact on business functions.
- Identify the key stakeholders involved in the recovery process. This includes IT teams, cybersecurity experts, management, legal departments, and external service provider.
- Clearly define the objectives of the recovery plan, such as restoring services, protecting sensitive data, and minimizing financial losses.
- Conduct a risk assessment to identify potential threats and vulnerabilities. Perform a Business Impact Analysis (BIA) to evaluate how these threats could affect business operations.
- RTO specify the maximum time allowed for a system or process to be down before it disrupts business operations.

- RPO specify he maximum acceptable amount of data loss, indicating how far back in time data should be restored after an incident.

 **Theoretical Activity 4.2.2: Description of Incident Recovery Plans development**

 **Notes to the trainer:**

- Trainer may use small group to describe Incident Recovery Plans development

 **Key steps:**

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions:

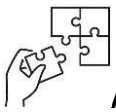
i. What is incident response integration?
ii. Describe communication and notification in incident recovery plans?
iii. What are recovery procedures?
iv. What is the purpose of testing and validation?
v. Define Resource allocation.
vi. Explain documentation and reporting in incident recovery plans?
vii. What is Regulatory and legal compliance
viii. Why we need employee training and awareness in incident recovery Plans
ix. What is continuous improvement?
x. What is review and approval?
xi. What is business continuity integration
xii. Difference between public relations and reputation management?
xiii. Define post-incident analysis and improvement

Step 2: Ask trainees to present their findings.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 4.2.2

Points to Remember

- An Incident Recovery Plan outlines how an organization can recover from security incidents, such as cyberattacks or system failures.
- Incident Response Integration ensures that the incident response efforts align with the recovery plan.
- Communication and Notification is critical during a security incident. The recovery plan should specify who needs to be notified, both internally and externally, and outline the tools and methods for communication.
- Recovery Procedures should detail the steps to recover affected systems and data. This includes restoring systems from backups, recovering lost data, and prioritizing the resumption of critical services.
- Regular testing of the recovery plan is essential to ensure it works as intended. This can involve conducting drills and simulations to practice recovery procedures and confirm that all necessary tools and technologies function correctly.
- Identifying the necessary resources for recovery is important. This includes personnel, technology, and financial resources needed to execute the recovery plan successfully.
- Documentation and Reporting includes maintaining logs of the incident and recovery actions, as well as post-incident reports summarizing what occurred and how it was handled.
- The recovery plan must adhere to relevant laws and regulations. This includes data protection laws and industry-specific requirements that may affect recovery processes.
- Regular training helps employees understand their roles in the recovery plan. This can include workshops and awareness campaigns to educate staff about cybersecurity threats and recovery procedures.
- Organizations should strive for continuous improvement by gathering feedback after incidents and updating the recovery plan based on new threats and best practices.
- The recovery plan should be regularly reviewed and approved by key stakeholders to ensure it remains relevant and effective. This includes updating the plan based on changes in the organization or emerging risks.
- The recovery plan should align with the organization's overall business continuity plan (BCP). This ensures that recovery efforts support broader business objectives and do not interfere with ongoing operations.

- Managing public perception is essential during an incident. The recovery plan should include strategies for communicating with the public and stakeholders and rebuilding trust afterward.
- After recovering from an incident, a thorough analysis should be conducted to identify lessons learned. This involves reviewing the recovery process to assess effectiveness and making necessary adjustments to improve future responses.
- Regularly testing and updating the recovery plan documentation helps maintain readiness and ensures that procedures reflect current organizational needs.



Application of learning 4.2.

The sales company HD has recently experienced a data breach that compromised sensitive customer information and disrupted normal operations. In light of this incident, you are requested to develop a comprehensive Incident Recovery Plan (IRP) to address potential future incidents, ensure rapid recovery, and safeguard against similar threats

Checklist:

Main points to check	Observation	
	Yes	No
Roles and responsibilities clearly defined		
Objectives with the organization's overall mission are aligned		
Potential threats and vulnerabilities identified		
RTOs and RPOs are explained		
Links between response and recovery clearly defined		
Methods for internal and external communication specified		
Testing schedules included		
Budget outline for recovery efforts are identified		
Responsible for approval are identified		
Documentation are produced		

Indicative content 4.3: Identification of Security Incident

Duration: 3hrs

Theoretical Activity 4.3.1: Description of Security Incident

Notes to the trainer:

- Trainer may use a small group to discuss on Security Incident in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions:

i. List Common incident categories?
ii. What are detection tools and systems used to monitor security incident?
iii. Describe baseline normal behaviour.

Step 2: Ask trainees to present their findings.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 4.3.1 in their manuals

Points to Remember

- Identifying a security incident involves recognizing and classifying events that may threaten the integrity, confidentiality, or availability of information.
- Incidents can be categorized based on their nature and impact. Common categories include: Malware Attacks, Phishing Attacks, Unauthorized Access, Denial of Service and Insider Threats
- To effectively identify security incidents, organizations rely on various detection tools and systems, including Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) Tools, Endpoint Detection and Response (EDR), Firewalls and Network Traffic Analysis Tools
- Baseline Normal Behavior refers to the standard patterns of activity within an organization's systems, networks, and applications under normal operating conditions

Theoretical Activity 4.3.2: Identification of Incident Detection Techniques

Notes to the trainer:

- Trainer may use a small group to discuss on Incident Detection Techniques in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions:

i. What is Anomaly Detection
ii. What is Signature-Based Detection
iii. What is User and Entity Behavior Analytics (UEBA)
iv. Describe Incident Reporting

Step 2: Ask trainees to present their findings.

Step 3: Provide expert view on presented content.

Step 4: Address any questions or concerns.

Step 5: Ask trainees to read the Key readings 4.3.2 in their manuals.

Points to Remember

- Anomaly detection monitors network and user activities to find unusual behavior compared to what is considered normal.
- Signature-based detection works by comparing data against a database of known threat signatures or patterns.
- UEBA analyzes the behavior of users and devices within a network. It establishes a baseline of normal behavior and looks for deviations that might signal a security issue, such as unusual login times or access to sensitive information.
- Incident reporting involves documenting and sharing details about detected security incidents with relevant teams

Theoretical Activity 4.3.3: Description of accident response and reporting

Notes to the trainer:

- Trainer may use a small group to describe accident response and reporting in security security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions:

i. What is Security information sharing?
ii. Describe Logging and Monitoring.
iii. What is Security awareness training?
iv. Describe Incident Response Playbooks.
v. Give types of Third-Party Services
vi. Describe Compliance with Regulations

Step 2: Ask trainees to present their findings.

Step 3: Provide expert view on presented content

Step 4: Address any questions or concerns

Step 5: Ask trainees to read the Key readings 4.3.3 in their manuals

Points to Remember

- Sharing information about security threats and incidents with other organizations and government bodies helps improve overall security. By collaborating, organizations can stay updated on emerging threats and enhance their responses.
- Logging involves recording events and actions in an IT environment. Monitoring is the real-time analysis of these logs to spot suspicious activities.
- Training employees on cybersecurity risks and best practices increases awareness. Educated employees can recognize potential incidents and respond correctly, reducing the likelihood of human errors that could lead to breaches.
- These are documented procedures that guide teams on how to handle specific security incidents. Playbooks provide clear steps for response, ensuring a consistent and efficient approach, which minimizes confusion during incidents.

- Organizations can engage third-party services for additional expertise in incident response and threat detection. These providers can offer managed security services and support, enhancing the organization's overall capabilities.
- Adhering to industry regulations is crucial for incident management. Organizations must understand and follow legal requirements regarding incident reporting and data protection, which builds trust with customers and stakeholders.

Theoretical Activity 4.3.4: Description of threat intelligence integration for incident classification and prioritization.

Notes to the trainer:

- Trainer may use a small group to discuss on threat intelligence integration for incident classification and prioritization in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions:

i. Define threat intelligence.
ii. Describe steps for integration of threat intelligence into incident classification and Prioritization.

Step 2: Ask trainees to present their findings.

Step 3: Provide expert view on presented content.

Step 4: Address any questions or concerns.

Step 5: Ask trainees to read the Key readings 4.3.4 in their manuals.

Points to Remember

• Threat intelligence is the process of gathering, analyzing, and using information about potential or actual cyber threats. It helps organizations understand who is attacking them, how they are being attacked, and what the attackers are trying to achieve.

• Steps for Integration of Threat Intelligence into Incident Classification and Prioritization: Collecting Threat Data, Analyzing Threats, Integrating into Detection Systems, Classifying Incidents, Prioritizing Incidents, continuous Updates.

Practical Activity 4.3.5 Applying Incident Response and Reporting

Notes to the trainer

- This activity should take place in a computer lab where trainees should apply incident response and reporting
- Avail computers installed:

✓ SIEM Tools (eg:Splunk, IBM QRadar),
✓ Endpoint Detection and Response (EDR) (e.g: CrowdStrike,
✓ Carbon Black),Email Security Gateway(eg:Proofpoint, Mimecast).

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

The school has experienced a ransomware attack, how school must respond swiftly to minimize the damage, restore operations, and ensure customer data remains protected.

Step 2: Explain the task and provide clear work instruction

Step 3: Identify how to apply response in security incident. While identifying, explain the how to apply response in security incident.

Step 4: Ask trainees to apply response in security incident and monitor the procedures.

Step 6: Verify whether the apply response in security incident are applied.

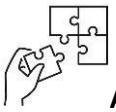
Step 7: Address any questions or concerns

Step 8: Ask trainee to read key reading 4.3.5.

Points to Remember

While apply response in security incident you follow the following steps:

1. Identify how to recognize the ransomware attack
2. Containment immediate actions to limit the spread
3. Eradication: Removing the ransomware and eliminating its root cause
4. Recovery for restoring operations and ensuring system integrity
5.post-incident analysis and prevention



Application of learning 1.2.

Our school experiences a phishing attack where an employee unknowingly clicks on a malicious email link. This leads to the compromise of their account, and the attacker gains access to sensitive customer information stored in cloud services. The attacker begins exfiltrating customer data. How our school must respond swiftly to contain the breach, minimize damage, and ensure compliance with regulatory requirements.

Checklist:

Main points to check	Observation	
	Yes	No
Recognizing the Incident are well Identified		
Containment of Limiting the Damage are well identified		
Eradication of Removing the Threat are well removed		
Recovery for Restoring Normal Operations are well recovered		
Post-Incident Analysis event are well learned		
Employee Security Awareness (Security Awareness Training , Incident Reporting) are well enhanced		
Logging and Monitoring are well Improved		

Indicative content 4.4: Isolation of Affected System

Duration: 2 hrs

Theoretical Activity 4.4.1: Description of Immediate Action and Communication in isolation of affected system

Notes to the trainer:

- Trainer may use a small group to describe Immediate Action and Communication in isolation of affected system in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions

i. What are immediate action upon incident detection?

ii. Describe how to establish communication procedures.

Step 2: Ask trainees to present their findings to the whole class.

Step 3: Provide expert view on presented content

Step 4: Address any questions or concerns

Step 5: Ask trainees to read the Key readings 4.4.1 in their manuals

Points to Remember

- The isolation of affected systems is a crucial part of incident response to prevent the spread of cyber threats. When a security breach or attack occurs, it is essential to quickly isolate the compromised system from the rest of the network
- The first step in incident response is to take immediate action to contain the threat. This could involve shutting down the affected system, disconnecting it from the network, or disabling its internet access. The goal is to quickly stop any ongoing malicious activity, minimizing damage and preventing the threat from worsening.

- Effective communication is critical during an incident. As soon as the issue is detected, it is important to inform all relevant stakeholders, such as the incident response team, IT staff, and company management. A clear communication procedure ensures everyone knows their roles and responsibilities in responding to the incident. Identifying a security incident involves recognizing and classifying events that may threaten the integrity, confidentiality, or availability of information.

Theoretical Activity 4.4.2: Description system isolation techniques and analysis of affected systems.

Notes to the trainer:

Trainer may use a small group Immediate Action and Communication in isolation of affected system in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions

i. Describe the system isolation techniques
ii. Identify analysis of affected systems

Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 4.4.2 in their manuals.

Points to Remember

- Four techniques used to isolate affected systems are Network segmentation divides a network into smaller, isolated sections, disabling network ports on compromised systems cuts off the attacker's ability to use those ports for malicious activity, adjust firewall rules, administrators can block all traffic to and from a compromised device or segment of the network and Isolation switches can quickly disconnect affected systems or network segments from the larger network.
- After a security incident, analyzing the affected systems is essential for understanding the extent of the damage and planning the recovery process. This analysis involves several key steps: Incident Analysis**,** Impact Assessment**,** Validation of Isolation**,** Logging and Documentation

Theoretical Activity 4.4.3: Description of recovery planning and communication

Notes to the trainer:

- Trainer may use a small group to describe on recovery planning and communication in Cyber security.

Key steps:

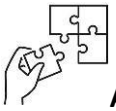
While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions

i. Describe recovery planning
ii. Describe Communication and Reporting
iii. Describe Remediation and System Restoration
iv. Describe Policy and Procedural Updates

Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 4.4.3 in their manuals.

- Recovery planning is the first step in responding to cybersecurity incidents. It starts with assessing the impact to identify affected systems and data. This understanding helps prioritize recovery actions.
- Effective communication keeps everyone informed during recovery. Clear internal channels among the incident response team and management ensure efficient coordination. Regular updates on recovery progress maintain alignment.
- Once immediate recovery efforts are done, organizations should focus on fixing vulnerabilities.
- After an incident, organizations need to review and update their policies and procedures. This review helps identify weaknesses that contributed to the incident.



Application of learning 1.1.

You've just been alerted to a potential data breach in your organization. What are the immediate actions you will take to respond to the incident, and how will you establish effective communication procedures across your team, identify system isolation techniques will you employ to contain the threat and prevent it from spreading?

Checklist:

Main point to check	**Observation**	
	Yes	**No**
Immediate Action and Communication are quickly assessed and established		
System Isolation Techniques are correctly implemented		
Analysis of Affected Systems based on logs and alerts are well analyzed to identify all affected systems.		
Communication are done		
Recovery Planning are developed based on the current state of the systems.		

Indicative content 4.5: Conducting Methodical Forensic Analysis

Duration: 2 hrs.

Theoretical Activity 4.5.1: Description of fundamentals forensic Analysis

Notes to the trainer:

Trainer may use a small group to describe fundamentals forensic Analysis in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions

i. What is Planning and Preparation?
ii. Define Legal Considerations?
iii. Discuss on evidence preservation?
iv. Differentiate Isolation and Segmentation?
v. What is Data Collection
vi. Explain Forensic Imaging

Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 4.5.1 in their manuals

Points to Remember

- Planning and Preparation: refers to the proactive steps an organization takes to be ready for potential incidents before they occur.
- Legal Considerations: refer to the laws, regulations, and compliance requirements that organizations must adhere to during and after an incident.
- Evidence preservation: refers to the process of securing and maintaining the integrity of digital and physical evidence collected during an incident investigation.

It ensures that the evidence remains unaltered, making it admissible in legal proceedings.

- Isolation and Segmentation: Isolation is an emergency response action taken during or after an incident to immediately disconnect or cut off compromised systems from the rest of the network to prevent the spread of threats.Where as Segmentation is strategy that divides a network into smaller, more secure zones or segments to limit lateral movement of threats within a network. Each segment can have its own security controls.
- Data Collection: is the process of gathering relevant information during an incident response or investigation to understand the nature, scope, and impact of the incident.
- Forensic Imaging: is the process of creating an exact bit-by-bit copy of a digital storage device, such as a hard drive, SSD, or USB drive, for forensic analysis.

Theoretical Activity 4.5.2: Description of evidence documentation and analysis

Notes to the trainer:

- Trainer may use a small group to describe the evidence documentation and analysis in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions

i. What is Evidence Documentation?
ii. Discuss the Analysis and Examination?
iii. What is the difference between Artifact and Event Reconstruction?

Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 4.5.2 in their manuals.

Points to Remember

- **Evidence Documentation:** is the process of meticulously recording all steps, activities, and details related to the collection, handling, and analysis of evidence during an incident investigation.
- **Analysis and Examination:** are critical stages in the forensic investigation of an incident, where collected evidence is scrutinized to uncover relevant information.
- **Artifact**: refers to a piece of digital data or a trace left behind by a system or user action. This could be files, logs, registry keys, memory contents, or network traffic captures.
- **Event Reconstruction:** is the process of piecing together the sequence of events that occurred during an incident by analyzing various artifacts and other evidence sources.

Theoretical Activity 4.5.3: Description of quality assurance and legal aspects

Notes to the trainer:

Trainer may use a small group to discuss on quality assurance and legal aspects in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions

i. Define Documentation and Reporting
ii. What is Quality Assurance
iii. Discuss on Legal Support

Step 2: Ask trainees to present their findings to the whole class.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 4.5.3 in their manuals.

Points to Remember

- **Documentation** involves maintaining accurate and detailed records of all actions taken during an incident or investigation.
- **Reporting** is the process of summarizing the investigation's results or incident response actions in a clear, structured format to inform various stakeholders, such as management, legal teams, regulatory authorities, or external partners. Reports can be technical (e.g., for IT teams) or high-level (e.g., for executives).
- **Quality Assurance (QA)** is a systematic process designed to ensure that products, services, or procedures meet defined standards of quality.
- **Legal Support** in incident response refers to the involvement of legal professionals to guide the organization through the legal aspects of managing a cybersecurity incident.

Practical Activity 4.5.4: Conducting Forensic Analysis in Cyber security.

Notes to the trainer

- This activity should take place in a computer lab where trainees should conduct Forensic analysis in Cyber security.
- Avail computers installed a kali linux.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

You are requested to conduct forensic analysis to determine how the breach occurred, recover deleted data, and analyze the compromised systems.

Step 2: Explain the task and provide clear work instruction

Step 3: Identify how to conduct forensic analysis. While conducting, explain conduct forensic analysis procedures

Step 4: Ask trainees to conduct forensic analysis and monitor the procedures.

Step 6: Verify forensic analysis is conducted

Step 7: Address any questions or concerns

Step 8: Ask trainee to read key reading 4.5.4.

Points to Remember

While conduct forensic analysis using Autopsy in kali Linux you follow the following steps:

Step 1 : Installation of Autopsy

Step 2: Opening Autopsy by typing the command in the terminal.

Step 3: Launching Autopsy through the browser.

Step 4: Adding Host.

Step 5: Adding Image.

Step 6: Analyzing Files.

Application of learning 4.5.

IRWANDA is a large technology services company that recently experienced a suspected data breach. Sensitive customer data may have been exfiltrated, and there are signs that the breach may have involved deleted files. You are requested a thorough forensic investigation to determine how the breach occurred, recover deleted data, and analyze the compromised systems.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	**1. Conducting Methodical Forensic Analysis are well applied**	**A. Fundamentals of Forensic Analysis are well identified**		
		1. Planning and Preparation are described		
		2. Legal Considerations are considered		
		B. Conducting Forensic Analysis are well conducted		
		1. Evidence Preservation are identified		
		2. Isolation and Segmentation are applied		
		3. Data Collection are collected		
		4. Forensic Imaging are applied		
		C. Evidence Documentation and Analysis are well identified		
		1. Evidence Documentation are documented		

		2. Analysis and Examination are described		
		3. Artifact and Event Reconstruction are applied		
		D. Quality Assurance and Legal Aspects are well described		
		1. Documentation and Reporting are created		
		2. Quality Assurance are identified		
		3. Legal Support are identified		

Indicative content 4.6: Restoring System and Data

Duration: 2 hrs.

Theoretical Activity 4.6.1: Description of System and Data Restoration.

Notes to the trainer:

- Trainer may use a small group to describe System and Data Restoration in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions:

i. What is recovery plan?
ii. Why we prioritize system and data for restoration?
iii. Identify hardware and infrastructure needed in restoration preparation.
iv. Discuss on RPOs and RTOs
v. What is Data Restoration
vi. Discuss on System Restoration
vii. Identify Testing and Validation
viii. What is User and Stakeholder Communication

Step 2: Ask trainees to present their findings.
Step 3: Provide expert view on presented content
Step 4: Address any questions or concerns
Step 5: Ask trainees to read the Key readings 4.6.1 in their manuals

Points to Remember

- Recovery plan: is a comprehensive document that outlines the steps to be taken to restore systems and data after a disaster or security incident.

- Prioritize system and data for restoration: Prioritizing systems and data for restoration is crucial for several reasons: Business Continuity,Data Loss Prevention,Regulatory Compliance.
- The hardware and infrastructure needed for restoration preparation, include: Backup servers, Storage devices,Network equipment,Servers
- Recovery Point Objective (RPO): This is the maximum amount of data loss that an organization can tolerate. It defines the point in time to which data should be restored. Recovery Time Objective (RTO): This is the maximum amount of time that an organization can be without a particular system or data before it impacts business operations.
- Data restoration : is the process of recovering lost or corrupted data from backups or other sources.
- System restoration: involves bringing a system back to a functional state after a failure or disruption.
- Testing and validation:are essential steps in system and data restoration. Testing ensures that restored systems and data are functioning correctly and that all necessary components are in place. Validation verifies that the restored systems and data meet the organization's requirements and expectations.
- User and stakeholder communication: is critical during and after system and data restoration. It involves informing users about the restoration process, providing updates on progress, and addressing any concerns.

Theoretical Activity 4.6.2: Description of post restoration actions and documentation

Notes to the trainer:

- Trainer may use a small group to describe post restoration actions and documentation in Cyber security.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees to answer the following questions:

i. Define Documentation in Cybersecurity.
ii. What are Parallel Operations in Cybersecurity Incident Response?
iii. What is Post-Restoration Monitoring?

iv. Describe the purpose and importance of User Training and Support in Cybersecurity.
v. How do you conduct a Review and identify Lessons Learned after a Cybersecurity Incident?
vi. Describe the process of Documentation Updates in a Cybersecurity Program.
vii. What are Audit and Compliance Checks, and how are they implemented in Cybersecurity?

Step 2: Ask trainees to present their findings.

Step 3: Provide expert view on presented content

Step 4: Address any questions or concerns

Step 5: Ask trainees to read the Key readings 4.6.2 in their manuals.

Points to Remember

- Documentation in cybersecurity refers to the creation and maintenance of records related to all aspects of cybersecurity, including incident response, risk management, and compliance.
- Parallel operations in cybersecurity incident response refer to the ability to continue critical business functions on alternate systems or data centers while the primary systems are being restored or repaired.
- Post-restoration monitoring involves closely observing restored systems and data for signs of issues or problems.
- User Training and Support User training and support are essential for ensuring that employees are aware of cybersecurity best practices and can effectively use security tools. Training can help prevent incidents by educating employees about phishing scams, social engineering attacks, and other threats.
- A review and lessons learned process involves analyzing the incident to understand what happened, identify root causes, and determine how to prevent similar incidents in the future. This may involve conducting interviews, reviewing logs, and analyzing data.
- Documentation updates are necessary to ensure that cybersecurity policies, procedures, and records are accurate and up-to-date. This may involve updating incident response plans, reviewing risk assessments, and documenting changes to security controls.
- Audit and compliance checks are used to verify that an organization is meeting its cybersecurity obligations and complying with relevant regulations. This may involve internal audits, external assessments, or compliance reviews.

Practical Activity 4.6.3: Restoring and validating of system and data.

Notes to the trainer

- This activity should take place in a computer lab where trainees should restore and validate system and data in Cyber security.
- Avail server computer installed a Veeam.

Key steps:

While delivering this activity, pass through the following steps:

Step 1: Introduce the activity and ask trainees do the task described below:

School web server has been compromised due to a ransomware attack, resulting in data encryption and service disruption. The school IT needs to restore the server and validate its functionality.

Step 2: Explain the task and provide clear work instruction

Step 3: Identify how to restore and validate system and data in cyber security.

Step 4: Ask trainees to restore and validate web server and monitor the procedures.

Step 6: Verify whether the web server is restored and validated.

Step 7: Address any questions or concerns

Step 8: Ask trainee to read key reading 4.6.3.

Points to Remember

While Restoring and validating of system and data you follow the following steps:

Step 1. Launch File Level Restore Wizard

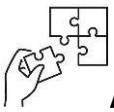
Step 2. Select Machine

Step 3. Select Restore Point

Step 4. Specify Restore Reason

Step 5. Verify Restore Settings

Step 6. Finalize Restore



Application of learning 1.1.

You are the incident response manager for a BWIZA Company that has recently experienced a ransomware attack. The attackers have encrypted critical systems and data, disrupting business operations. Based on the provided guidelines, using Veeam software for restoring systems and data, ensuring minimal downtime and maintaining compliance with relevant regulations.

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	**1. Restoring System and Data with Veeam is well conducted**	1.1 System is identified		
		1.2 Data Restoration is identified		
		1.3 Data are restored		
		1.4 System is restored		
		1.5 Documentation is provided		

Learning outcome 4 end assessment

Written assessment

SECTION I. Read the statement below and answer by TRUE or FALSE if it is correct or incorrect.

1. Is it important to include key stakeholders when developing an Incident Response Plan?

Answer: True

2. An Incident Response Policy is not necessary as long as you have response procedures in place.

Answer: False

3. Incident containment should occur before eradication and recovery in the Incident Response Plan.

Answer: True

4. Training and awareness are not part of an effective Incident Response Plan.

Answer: False

5. Post-incident analysis is crucial to improving future incident response efforts.

Answer: True

6. A Communication Plan is unnecessary in the context of an Incident Response Plan.

Answer: False

7. A Business Impact Analysis (BIA) helps in defining Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

Answer: True

8. The recovery plan should be tested and validated regularly to ensure effectiveness.

Answer: True

9. Documentation and reporting are not required when developing an Incident Recovery Plan.

Answer: False

10. Anomaly detection is a technique used for identifying incidents.

Answer: True

11. System isolation techniques, such as disabling network ports and using firewalls, are key to controlling the spread of an incident.

Answer: True

12. The validation of isolation is not required once a system is affected.

Answer: False

13. Incident analysis and impact assessment are critical after isolating the affected system.

Answer: True

14. Forensic analysis involves evidence preservation and data collection following an incident.

Answer: True

15. Legal considerations should be ignored when conducting forensic analysis.

Answer: False

16. Restoring systems and data after an incident should follow the recovery plan and prioritize critical systems first.

Answer: True

17. Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are not relevant in system restoration efforts.

Answer: False

18. Parallel operations should be monitored post-restoration to ensure system integrity.

Answer: True

19. Reviewing and updating documentation is an unnecessary step after system and data restoration.

Answer: False

SECTION II: fill the following paragraph with appropriate word from provided word

1. The process of creating a framework to handle and mitigate security incidents is known as developing an _____.
   - **A.** Incident Response Plan
   - **B.** External Plan
   - **C.** Stakeholders
   - **D.** Recovery

   Answer: A: Incident Response Plan
2. A key element in incident response is the involvement of _____ to ensure smooth coordination and decision-making.
   - A. Incident Response
   - **B.** Backup Plan
   - **C.** Key Stakeholders
   - **D.** Recovery process

   Answer: C: Key Stakeholders

3. _____ and Reporting are critical for quickly identifying and managing a cybersecurity breach.

- A. Restoration
- B. Documentation
- C. Incident Detection
- D. Network Segmentation

Answer: C: Incident Detection

4. The step taken after identifying a cybersecurity breach to prevent it from spreading is called _____.

- A. Communication
- B. Incident Containment
- C. Incident Response
- D. Firewall

Answer: B: Incident Containment

5. To ensure proper communication during a cybersecurity incident, an organization must establish a _____ Plan.

A. Documentation
B. Monitoring
C. Communication
D. Testing and Validation
E. System Restoration

Answer: C: Communication

6. After a cybersecurity incident, organizations must perform a _____ to understand what went wrong and how to improve future responses**.**

A. Security Incident
B. Public Relations
C. Incident Detection
D. Post-Incident Analysis

Answer: D: Post-Incident Analysis

7. Combining incident response and disaster recovery ensures better handling of both scenarios, which is referred to as _____ Integration.

A. Reputation Management
B. DR/BCP
C. Regulatory Compliance
D. Executive Reporting

Answer: B:DR/BCP

8. Recovery Time Objectives (RTOs) and _____ are key measures used to define recovery goals in incident recovery plans.

A. Recovery Point Objectives (RPOs)
B. Objectives and Scope
C. Recovery Joint Objectives
D. Incident Recovery Plans

Answer: A: Recovery Point Objectives (RPOs)

9. The use of _____ techniques, such as anomaly detection or signature-based detection, helps in identifying cybersecurity incidents.

1. Incident Detection
2. Risk Assessment
3. Value Detection
4. Normal Behavior

Answer: A: Incident Detection

10. The process of ensuring an organization meets legal and industry standards after a breach is called _____.

A. Employee Training
B. Resource Allocation
C. Regulatory and Legal Compliance
D. Continuous Improvement

Answer: C. Regulatory and Legal Compliance

11. To avoid further damage during an incident, affected systems must undergo _____ techniques like network segmentation or disabling network ports**.**

A. Impact Assessment
B. Recovery Planning
C. System Isolation
A. Logging and Documentation

Answer: C: System Isolation

12. Ensuring that the isolation of systems is successful requires _____ and documentation.

1. Logging
2. Restoration
3. Collection
4. Validation

Answer: D: Validation

13. A thorough investigation into a cybersecurity incident involves _____ and Data Collection to preserve evidence.

1. Evidence Documentation
2. Legal Considerations
3. Forensic Imaging
4. Forensic Analysis

Answer: C: Forensic Imaging

14. After gathering data, the process of reconstructing artifacts and events for deeper analysis is known as _____.

1. Evidence Documentation

B. Examination
C. Event Reconstruction
D. Quality Assurance

Answer: C: Event Reconstruction

15. Once systems are restored, organizations must engage in _____ to monitor the effectiveness of recovery.

A. Documentation
B. Parallel Operations
C. Post-Restoration Monitoring
D. Incident Analysis

Answer: C: Post-Restoration Monitoring

16. Conducting _____ of incidents is crucial for understanding the severity and impact of the attack.

A. Parallel Operations
B. Data Restoration
C. Documentation Updates
D. Incident Analysis

Answer: D: Incident Analysis

17. After restoring systems, an organization must review and update their _____ to reflect lessons learned.

A. Review and Lessons Learned
B. Documentation
C. Stakeholder Communication
D. System Restoration

Answer: B: Documentation

18. The process of performing checks to ensure an organization remains compliant with cybersecurity standards is called _____.

A. Audit and Compliance Checks
B. Documentation Updates
C. User Training and Support

Answer: A: Audit and Compliance Checks

SECTION III. Choose the letter corresponding to the correct answers from Colum A and Column B.

ANSWER	COLUMN A	COLUMN B
…B…	A. Incident Response Plan	1.The process of identifying and reporting potential security incidents
…A…	B. Incident Detection and Reporting	2.A documented, organized approach to handling and managing cybersecurity incidents.
…D…	C. Incident Containment	3.A review process to evaluate how an incident was handled and lessons learned

…C…	D. Post-Incident Analysis	4.Limiting the damage of a security breach to prevent further harm.
…F…	E. Legal and Regulatory Compliance	5. Guidelines for how and when to communicate with stakeholders during an incident.
…E…	F. Communication Plan	6.Ensuring incident response and recovery procedures meet legal and regulatory standards
…N…	G. Recovery Time Objectives (RTOs)	7.Verifying that incident response and recovery processes align with internal policies and external regulations.
…J…	H. Baseline Normal Behavior	8.The maximum acceptable amount of data loss in a recovery scenario
…K…	I. Firewall Rules	9. Technology used to detect security incidents, such as intrusion detection systems (IDS).
…G…	J. Recovery Point Objectives (RPOs)	10.The target time to recover systems after an incident
…H…	K. Incident Detection Tools and Systems	11.A standard of expected system behavior used to detect anomalies.
…I…	L. Network Segmentation	12. A set of policies defining what traffic is allowed or blocked in a network.
…M…	M. Disaster Recovery (DR) and Business Continuity Planning (BCP) Integration	13. Incorporating response and recovery plans into broader business continuity strategies
…L…	N. Audit and Compliance Checks	14. Dividing a network into smaller segments to limit the spread of incidents.

Practical assessment

BELL Company Ltd has experienced a major security incident involving a ransomware attack. You are a member of the incident response team responsible for managing the incident and restoring business operations. Your task is to implement a complete incident response and recovery plan, ensuring that all necessary steps are taken to contain, recover, analyze the incident and provide documentation report

Checklist:

SN	Criteria	Indicators	Observation	
			YES	NO
1	**1: Incident Response Plan**	1.1 Identify the importance of an incident response plan.		
		List key stakeholders.		
		1.2 Define scope and objectives.		
		1.3 Develop detection and reporting procedures.		
		1.4 Outline response procedures (containment, eradication, recovery).		
		1.5 Create a communication plan.		
		1.6 Ensure compliance and record-keeping.		
		1.7 Include post-incident analysis and reporting		
2.	**2: Incident Recovery Plan**	2.1 Define objectives and scope.		
		2.2 Conduct risk assessment and BIA.		
		2.3 Specify RTO and RPO.		
		2.4 Develop recovery procedures.		
		2.5 Include testing and validation steps.		
		2.6 Allocate resources.		
3	**3: Incident Identification**	3.1 Describe incident detection techniques		
		3.2 List incident detection tools.		
		3.3 Implement system isolation procedures.		
		3.4 Establish communication protocols		

4	**4: Forensic Analysis**	4.1 Preserve evidence properly		
		4.2 Document and analyze the incident.		
		4.3 Reconstruct the event timeline.		
		4.4 Address legal considerations for evidence handling.		
	5.System and Data Restoration	5.1 Prioritize system and data restoration		
		5.2 Test and validate restored systems.		
		5.3 Communicate with stakeholders.		
		5.4 Set up post-restoration monitoring.		
		5.5 Provide user training.		
		5.6 Documentation is produced		

Further information to the trainer

Miller, R. (2021). *Network security monitoring and analysis: A comprehensive guide to intrusion detection systems and security information and event management*. Wiley.

Northcutt, S., & Novak, W. (2020). *Intrusion detection: A practical guide to the techniques and technologies*. Pearson Education.

Skoudis, E., & Liston, T. (2020). *Counter Hack Reloaded: A step-by-step guide to computer attacks and effective defenses*. Pearson Education.

Jones, A., & Sawyerr, K. (2021). *Cyber incident response and recovery: A comprehensive guide for businesses*. CRC Press.

Cisco. (n.d.). *Cybersecurity awareness month*.Cisco. https://www.cisco.com/c/en/us/products/security/cybersecurity-awareness-month.html#~additional-resources

National Cyber Security Centre. (n.d.). *Developing your plan*. National Cyber Security Centre. https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes/developing-your-plan

Palo Alto Networks. (n.d.). *Managed detection and response*. Palo Alto Networks. https://www.paloaltonetworks.com/unit42/respond/managed-detection-response

SANS Institute. (n.d.). *Cyber security courses*. SANS Institute. https://www.sans.org/cyber-security-courses/?focus-area=cloud-security,cyber-defense,cyber-security-it-essentials,digital-forensics

Veeam. (n.d.). *File-level restore before you begin*. Veeam. https://helpcenter.veeam.com/docs/agentforwindows/userguide/files_restore_before.html?ver=60

END

RTB | RWANDA TVET BOARD

October 2024