UNIT - V

Deliverable: The Deliverable, The Document, Overall Structure, Aligning Findings, Presentation.

Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion**.**

Deliverable and Integration

1. Deliverable

Definition

A deliverable is the final output or report provided after completing a security assessment, penetration test, or network analysis.

It contains:

- Findings
- Vulnerabilities
- Risk analysis
- Recommendations
- Solutions

The deliverable helps organizations understand:

- Current security status
- Existing weaknesses
- Required improvements

1.1 The Deliverable

Purpose

The main purpose of the deliverable is to communicate technical findings clearly to:

- Management
- Security teams
- Clients
- System administrators

Characteristics of a Good Deliverable

- Clear
- Accurate
- Well-structured
- Professional
- Action-oriented

Example

After a penetration test, the security team submits a report showing:

- Weak passwords
- Open ports
- SQL injection vulnerabilities
- Suggested fixes

1.2 The Document

Definition

The document is the written report containing all assessment details.

Main Sections of the Document

1. Executive Summary
2. Scope of Testing
3. Methodology
4. Findings
5. Risk Levels
6. Recommendations
7. Conclusion

Example

A company security audit document may include screenshots of vulnerabilities and remediation steps.

1.3 Overall Structure

A security report should follow a logical structure.

Standard Structure

1. Title Page

Contains:

- Project name
- Organization name
- Date
- Author

2. Executive Summary

A short overview for management.

Example

"Three high-risk vulnerabilities were identified in the company web server."

3. Scope

Defines:

- Systems tested
- Time period
- Testing limitations

4. Methodology

Explains:

- Tools used
- Techniques applied

Examples:

- Port scanning
- Vulnerability scanning
- Password testing

5. Findings

Detailed vulnerabilities and observations.

6. Recommendations

Suggested mitigation methods.

7. Conclusion

Final assessment summary.

1.4 Aligning Findings

Definition

Aligning findings means organizing vulnerabilities according to:

- Risk level
- Business impact
- Priority

Categories

High Risk

Requires immediate action.

Example:

- Remote code execution vulnerability

Medium Risk

Moderate security impact.

Example:

- Weak password policy

Low Risk

Minor issues with limited impact.

Example:

- Information disclosure banners

Importance

Helps organizations:

- Prioritize fixes
- Allocate resources efficiently

1.5 Presentation

Definition

Presentation is the process of explaining assessment results to stakeholders.

Goals

- Make findings understandable
- Explain risks clearly
- Recommend actions

Good Presentation Features

- Simple language
- Charts and diagrams
- Screenshots
- Risk ratings

Example

A security analyst presents:

- Attack paths
- Vulnerability severity
- Recommended mitigation plan

using slides and demonstrations.

2. Integration

Definition

Integration means combining all security findings and applying them into organizational security planning and operations.

2.1 Integrating the Results

Purpose

To combine:

- Technical findings
- Security policies
- Risk assessments
- Defensive measures

Activities

- Updating security controls
- Improving monitoring
- Patching systems
- Training employees

Example

If multiple systems use weak passwords, the organization introduces stronger password policies company-wide.

2.2 Integration Summary

Definition

A concise overview of all combined findings and actions.

Includes

- Key vulnerabilities
- Risks
- Solutions implemented
- Remaining concerns

Example

Summary:

- Firewall misconfigurations fixed
- Critical patches installed
- Monitoring enhanced

2.3 Mitigation

Definition

Mitigation means reducing or eliminating security risks.

Common Mitigation Techniques

1. Patching

Updating vulnerable software.

Example

Installing security updates for Windows Server.

2. Access Control

Restricting unauthorized access.

3. Encryption

Protecting sensitive data.

4. Firewall Configuration

Blocking malicious traffic.

5. Employee Awareness

Training users about phishing and attacks.

2.4 Defense Planning

Definition

Defense planning is designing strategies to protect systems and networks from attacks.

Components

Preventive Controls

- Firewalls
- Antivirus software
- Access control

Detective Controls

- Intrusion detection systems
- Log monitoring

Corrective Controls

- Backup recovery
- Incident response

Example

An organization deploys:

- Firewalls
- Multi-factor authentication
- Network monitoring systems

to strengthen defense.

2.5 Incident Management

Definition

Incident management is the process of handling security incidents effectively.

Phases of Incident Management

1. Preparation

Developing policies and response teams.

2. Identification

Detecting incidents.

Example:
Malware detected on a workstation.

3. Containment

Preventing spread.

Example:
Disconnecting infected systems.

4. Eradication

Removing the threat.

Example:
Deleting malware files.

5. Recovery

Restoring normal operations.

6. Lessons Learned

Analyzing the incident to improve future security.

2.6 Security Policy

Definition

A security policy is a formal set of rules and guidelines for protecting organizational resources.

Purpose

- Define security responsibilities
- Enforce proper behavior
- Protect data and systems

Types of Security Policies

1. Password Policy

Rules for strong passwords.

2. Access Control Policy

Defines who can access resources.

3. Internet Usage Policy

Controls acceptable internet use.

4. Backup Policy

Specifies backup procedures.

Example

A policy may require:

- Passwords with minimum 12 characters
- Regular password changes
- Multi-factor authentication

2.7 Conclusion

Definition

The conclusion summarizes the overall assessment and security posture.

Includes

- Major findings
- Security improvements
- Future recommendations

Example

“The organization has improved security after patching critical vulnerabilities, but continuous monitoring is recommended.”

Overall Flow of Deliverable and Integration

1. Conduct Assessment
2. Document Findings
3. Prepare Deliverable
4. Present Results
5. Integrate Security Improvements
6. Apply Mitigation
7. Implement Defense Planning

8. Manage Incidents
9. Enforce Security Policies

Short Summary Table

Topic	Description
Deliverable	Final security assessment report
The Document	Written report of findings
Overall Structure	Organized format of report
Aligning Findings	Prioritizing vulnerabilities
Presentation	Explaining findings to stakeholders
Integration	Applying findings into security operations
Mitigation	Reducing security risks
Defense Planning	Designing protection strategies
Incident Management	Handling security incidents
Security Policy	Rules for organizational security
Conclusion	Final summary and recommendations