**📘 Summary: 05 Vulnerability Management**

**1. Vulnerability Management in the Org Model**

* Integrated within:
  + **Operational Model**
  + **Organisational Model**
* Collaborates across:
  + IR, Security Monitoring, Engineering, Infra, App & Network Ops, Risk, and Threat Intel

**2. High-Level Threat & Vulnerability Management (TVM) Process**

1. **Asset Management**
2. **Vulnerability Scanning**
3. **Threat Intelligence Integration**
4. **Vulnerability Classification**
5. **Remediation Planning**
6. **Compliance & Reporting**

**3. Key Concerns**

* **TVM Scanner Management**
* **Vulnerability Research**
* **TVM Standards Development**
* **Support to Security & Business Functions:**
  + **Scanning, Qualification, Reporting**
  + **Remediation Tracking**
  + **Compliance Verification**
  + **Vendor Advisory Integration**
  + **Threat Hunting Support**

**4. Key Activities and Outputs**

| **Function** | **Activity** | **Output** |
| --- | --- | --- |
| **TVM** | **Set up/manage scanners** | **Documented system** |
| **TVM** | **Maintain and share TVM standards** | **Published standard** |
| **TVM** | **Perform scans (regular, authenticated, etc.)** | **Scheduled activities** |
| **TVM** | **Analyse scan results** | **Reports** |
| **TVM** | **Qualify vulnerabilities** | **Analysis summary** |
| **TVM** | **Create management & governance reports** | **Operational/strategic reports** |
| **TVM** | **Engage remediation teams** | **Action plans** |
| **TVM** | **Track remediation progress** | **Progress dashboards** |
| **TVM** | **Validate compliance** | **Reports** |
| **TVM** | **Correlate threat intel** | **Remediation plan** |
| **TVM** | **Run ad-hoc scans for threat hunting** | **Validation support** |

**5. TVM Standard – Key Elements**

* **Purpose:** Define TVM scope and processes
* **Scope:** Covers all applicable assets
* **Includes:**
  + - * + **Scan conditions, frequency, and types**
        + **Vulnerability classification criteria**
        + **Reporting & remediation expectations**
        + **Penetration testing rules**
        + **Stakeholder roles**
        + **Compliance requirements**
        + **Exception handling procedures**

**6. TVM Architecture**

* **Hybrid Model:**
  + **Cloud + On-Prem**
  + **Data flows between TVM tools, SIEM, and Asset systems**

1. **Service Maturation Levels**

| **Level** | **Scope** |
| --- | --- |
| **Foundation** | **Perimeter, DMZ, unauthenticated scans** |
| **Advanced** | **Corporate LAN, cloud, authenticated scans** |
| **Optimised** | **Most systems, high compliance, integrated threat hunting** |

**8. Framework Alignment**

**NIST CSF**

* Identify: Vulnerabilities
* Detect: Analysis, threat hunting
* Protect: Standards, governance
* Respond: IR integration
* Recover: Expansion and improvements

**ISO 27001**

* A12: TVM, operating procedures
* A14: Vulnerability detection in system acquisition
* A16: Incident Management (TVM supports)
* A18: Compliance via scanning & reporting

**MITRE ATT&CK**

* Aligns with:
  + Pen Testing
  + Authenticated/Discovery Scanning
  + Detection and Exploitation Simulation