**📘 Summary: 07 Threat Management**

**1. Threat Management in the Organisation**

* Present in both:
  + **Operating Model**
  + **Organisational Model**
* Connects closely with:
  + **IR, Monitoring, Engineering, Risk, Intel, Business, App/Infra teams**

**2. Main Components of Threat Management**

**A. Threat Intelligence (TI)**

* **Gathers data on:**
  + Threat actors, campaigns, exploits
  + Sector-specific threats, TTPs
* **Sources**: feeds, articles, vendor intel, underground forums
* **Types of TI:**
  + **Strategic** (for execs)
  + **Tactical** (high-impact emerging threats)
  + **Technical** (IPs, hashes, IOCs)
  + **Operational** (active threats to the organisation)

**B. Threat Modelling**

* **Analyses system/data flow to:**
  + **Identify threats**
  + **Determine exposure paths**
  + **Recommend mitigations**
  + **Validate effectiveness**
* **Threat Modelling Techniques:**
  + **STRIDE**
  + **Attack Trees**
  + **PASTA, LINDDUN, Trike, Kill Chain, MITRE ATT&CK**

**C. Threat Hunting**

* Detect threats that evaded existing controls
* **Based on:**
  + Indicators of Compromise (IoC)
  + Indicators of Attack (IoA)
  + Adversary TTPs
* **Types:**
  + Structured (based on TTPs, MITRE)
  + Unstructured (event-triggered)
  + Situational (based on risk to high-value assets)
* **Tools**: SIEM, XDR, analytics, intel feeds

**D. Advanced Threat Management**

* **Deep technical work such as:**
  + Adversary emulation
  + Exploit Proof of Concepts (PoCs)
  + Honeypots / Honeynets
  + Red Team, Purple Team exercises
  + Advanced deception & disruption techniques

**3. Key Activities and Outputs**

| **Function** | **Activity** | **Output** |
| --- | --- | --- |
| **TI** | **Scan sources & assess impact** | **TI reports, guidance** |
| **TI** | **Create TTP profiles** | **Organisational threat profiles** |
| **TI** | **Find new intel sources** | **Improved threat visibility** |
| **Modelling** | **Map architectures, data flows** | **Threat model diagrams** |
| **Modelling** | **Identify/validate threats** | **Risk & mitigation plans** |
| **Hunting** | **Define attack scenarios, collect data** | **Threat hunting reports** |
| **Adv. Threat** | **Create honeypots, simulate attacks** | **Behavioural insights, mitigation strategies** |

**4. Threat Modelling Process**

1. **Analyse System**: Identify components, entry/exit points
2. **Create Model**: Data flow, trust boundaries
3. **Analyse Threats**: Use STRIDE, identify vulnerabilities
4. **Develop Mitigations**
5. **Validate Controls**

**5. Threat Hunting Process**

1. **Specify Threat**
2. **Formulate Hypothesis**
3. **Perform Hunt**
4. **Report Results**
5. **Assist with Mitigation**
6. **Service Maturity Levels**

| **Level** | **Scope** |
| --- | --- |
| **Foundation** | **OSINT, basic feeds, ad-hoc modelling** |
| **Advanced** | **Multiple TI sources, defined modelling, limited hunting** |
| **Optimised** | **Strategic TI, routine modelling, continuous hunting, adversary simulation, deception systems** |

**7. Red – Purple – Blue Teaming**

* **Red**: Offensive simulation (attacks)
* **Blue**: Defensive response (IR, monitoring)
* **Purple**: Collaborative testing/improvement of both sides

**8. Framework Mapping**

**NIST CSF**

* Identify: Threat Intel, Modelling, Advanced Threat Mgt
* Detect: Threat Hunting, Advanced Mgt
* Respond: Same as above

**ISO 27001**

* A12: TI, Threat Hunting
* A14: Threat Modelling for secure design
* A16: IR (supports Threat Hunting)
* A18: Compliance (through documentation and validation)

**MITRE ATT&CK**

* Provides full mapping for:
  + Threat Modelling
  + Threat Hunting
  + TTP tracking
  + Advanced Adversary Behaviour simulation