**📘 Summary: 04 Operational Monitoring**

**1. Security Monitoring – Role in Models**

* Embedded in both:
  + **Operations Model**
  + **Organisational Model**
* Provides core **detection and response capabilities**

**2. Key Concerns**

* **SIEM Management** **(Security Information & Event Management)**
* **Log Ingestion**
* **Use Case Management**
* **Alert Monitoring & Incident Detection**
* **Incident Qualification & Triage**
* **Threat Intelligence Integration**
* **KPI Reporting & Dashboards**

**3. Key Activities and Outputs**

| **Function** | **Activity** | **Output** |
| --- | --- | --- |
| **Security Monitoring** | **Set up & manage SIEM** | **Documented system** |
|  | **Log feed onboarding (infra/app)** | **Connected log sources** |
|  | **Develop, test, tune use cases** | **Documented & updated use cases** |
|  | **Monitor & investigate alerts/incidents** | **Qualified alerts/incidents** |
|  | **Contact IR, support incident resolution** | **Tickets, evidence, info** |
|  | **Integrate threat & vulnerability intel** | **Ingested intel, enhanced visibility** |
|  | **Report KPIs** | **Dashboards, reports** |
|  | **Upgrade & evaluate SIEM platform** | **Recommendations, improved system** |

**4. Function Interactions**

* Works closely with:
  + **Incident Response**
  + **TVM**
  + **Security Engineering**
  + **Infrastructure, App, Network Ops**
  + **Risk & Security Architecture**
  + **Threat Intel Teams**
* Often **partially outsourced** (e.g., MSSPs)

**5. SIEM Architecture & Use Case Lifecycle**

**Use Case Phases:**

* **Identification & Selection**
  + **Based on MITRE ATT&CK, STRIDE, Kill Chain**
* **Creation & Testing**
* **Deployment & Operation**
* **Integration with IR**
* **Strategic and Operational Reporting**
* **Tuning and Optimization**

**6. Use Case Management Best Practices**

* **Define business/security needs**
* **Identify log/data sources**
* **Design correlation logic**
* **Establish baselines and thresholds**
* **Monitor performance and tune for:**
  + **False Positives**
  + **False Negatives**
  + **Noise reduction**

**7. Investigation Levels (Multi-Tier Model)**

1. **Level 1 Analyst** – Basic alert triage, resolves false positives
2. **Level 2 Analyst** – Deeper technical investigations
3. **Level 3 Analyst** – Critical threat handling, engages Cyber Crisis Team

**8. Service Improvement Focus**

* **Reduce false positives** to free analyst resources
* **Enhance automation and correlation**
* **Focus on advanced analysis and coverage**

**9. Service Maturity Levels**

| **Level** | **Description** |
| --- | --- |
| **Foundation** | **Perimeter, on-prem, OOTB use cases** |
| **Advanced** | **Cloud integration, critical infrastructure, partial automation** |
| **Optimised** | **Full coverage, custom advanced use cases, threat hunting, high automation** |

**10. Framework Alignment**

**NIST CSF**

* Detect: SIEM, analysis, threat hunting
* Respond: IR support
* Recover: Expansion of detection scope

**ISO 27001**

* A12: Operational Monitoring
* A16: Incident Management
* A18: Compliance

**MITRE ATT&CK**

* Aligned to monitoring:
  + Perimeter
  + Infrastructure
  + EDR
  + Access
  + Network & Security Services
  + Specialist & Advanced Use Cases