Security Operating Procedure

|  |  |
| --- | --- |
| **Procedure Name** | Network Monitoring & Logging |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Approved By | Owner | Date Last Updated | Review Frequency | Next Review | Comments |
|  |  |  |  |  |  |  |

**Classification**: Confidential

This document should be restricted to those with a specific need.

**1. Purpose**  
The purpose of this procedure is to establish guidelines for the deployment, configuration, and management of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to protect [Your Organisation’s Name] network infrastructure from unauthorised access and potential threats.

**2. Scope**  
This procedure applies to all IDS and IPS technologies used within [Your Organisation’s Name], including network-based and host-based systems.

**3. Roles and Responsibilities**

* **IT Administrator:** Responsible for deploying, configuring, and maintaining IDS and IPS systems.
* **Network Administrator:** Monitors and manages IDS/IPS alerts and responses.
* **Information Security Manager:** Oversees the IDS/IPS process, ensures compliance, and reviews system configurations and alerts.

**4. Procedure**

**Step 1: IDS/IPS Deployment**

* **System Selection:**
  + Select IDS and IPS systems based on organisational needs and threat landscape. [Placeholder: List the IDS/IPS systems used]
* **Deployment Planning:**
  + Plan the deployment to ensure comprehensive coverage of the network. [Placeholder: Describe the deployment plan]
* **Installation and Configuration:**
  + Install and configure IDS/IPS systems according to vendor guidelines and best practices. [Placeholder: Specify installation and configuration steps]

**Step 2: IDS/IPS Configuration**

* **Signature Updates:**
  + Regularly update IDS/IPS signatures to protect against the latest threats. [Placeholder: Specify update frequency and methods]
* **Tuning:**
  + Tune IDS/IPS systems to reduce false positives and ensure accurate detection. [Placeholder: Describe tuning procedures]
* **Rule Management:**
  + Implement and manage rules to detect and prevent specific types of attacks. [Placeholder: Specify rule management process]

**Step 3: Monitoring and Alerting**

* **Real-Time Monitoring:**
  + Continuously monitor IDS/IPS alerts and network traffic for signs of intrusion. [Placeholder: Specify monitoring tools and methods]
* **Alert Configuration:**
  + Configure IDS/IPS to generate alerts for predefined security events and anomalies. [Placeholder: List the types of events that trigger alerts]
* **Alert Response:**
  + Define and document response procedures for handling IDS/IPS alerts, including escalation paths and responsible personnel. [Placeholder: Describe the alert response process]

**Step 4: Incident Response and Investigation**

* **Incident Identification:**
  + Investigate alerts generated by IDS/IPS to confirm and assess potential security incidents. [Placeholder: Specify investigation tools and methods]
* **Incident Containment:**
  + Take immediate actions to contain and mitigate confirmed intrusions. [Placeholder: Describe containment procedures]
* **Documentation:**
  + Document the incident, including the nature of the intrusion, affected systems, and response actions taken. [Placeholder: Specify documentation procedures]

**5. Security Controls**

* **Access Control:** Restrict access to IDS/IPS management interfaces to authorised personnel only. [Placeholder: Specify access control measures]
* **Encryption:** Use encryption to protect data transmitted between IDS/IPS components and central management systems. [Placeholder: Specify encryption methods]
* **Logging:** Maintain detailed logs of IDS/IPS activities, including alerts and responses. [Placeholder: Specify logging procedures and retention]

**6. Continuous Improvement**

* **Post-Incident Review:**
  + Conduct post-incident reviews to identify lessons learned and improve IDS/IPS configurations and response procedures. [Placeholder: Describe the review process]
* **Regular Audits:**
  + Regularly audit IDS/IPS systems to ensure they function correctly and effectively. [Placeholder: Specify audit schedule and methods]
* **Training:**
  + Provide ongoing training to relevant personnel on IDS/IPS management and incident response. [Placeholder: Specify training schedule and content]

**7. Monitoring and Auditing**

* **Continuous Monitoring:**
  + Regularly monitor IDS/IPS performance and effectiveness. [Placeholder: Specify monitoring procedures]
* **Periodic Audits:**
  + Conduct periodic audits to ensure compliance with this procedure and identify areas for improvement. [Placeholder: Specify audit schedule and methods]

**8. Review and Update**

* **Review Frequency:**
  + This procedure will be reviewed annually. [Placeholder: Specify additional review triggers, if any]
* **Update Process:**
  + The Information Security Manager must approve any updates or changes to this procedure. [Placeholder: Specify update process]

**9. References**

* **Information Security Policy**
* **Network Security Policy**
* **IDS/IPS Configuration Guide**
* **Incident Response Plan**