**Cybersecurity Detect Policy**

Revision: 1.0

Approved:

Date: 05/06/2024

**1. Introduction**

1.1. Purpose: The purpose of this cybersecurity detect policy is to establish procedures and mechanisms for detecting cybersecurity events, incidents, and anomalies within the organization's information systems and networks, in alignment with the NIST Cybersecurity Framework (CSF) Version 2.0.

1.2. Scope: This policy applies to all employees, contractors, and third-party vendors who have access to the organization's information systems and networks.

**2. Event Logging and Monitoring**

2.1. Event Logging:

* All information systems and network devices shall generate and retain logs of security-relevant events, including but not limited to login attempts, access requests, configuration changes, and system activities.
* Log retention periods shall comply with regulatory requirements and industry best practices.

2.2. Log Monitoring:

* Logs shall be monitored regularly using automated tools and technologies to detect abnormal or suspicious activities indicative of potential cybersecurity incidents.
* Log monitoring shall include real-time analysis and correlation of events to identify patterns and trends.

2.3. Network Monitoring

* Network traffic will be monitored for abnormal or suspicious spikes indicative of potential cybersecurity incidents.

**3. Intrusion Detection**

3.1. Intrusion Detection Systems (IDS):

* Intrusion detection systems (IDS) shall be deployed to monitor network traffic and identify signs of unauthorized access, malicious activities, and security breaches.
* IDS sensors shall be strategically placed throughout the network to provide comprehensive coverage.

3.2. Anomaly Detection:

* Anomaly detection mechanisms shall be implemented to detect deviations from normal behaviour patterns within information systems, applications, and user activities.
* Machine learning algorithms and behavioural analytics tools may be used to identify anomalous behaviour indicative of security threats.

3.3. Anti-virus Detection

* Endpoints will, where possible, have antivirus software installed.

**4. Security Information and Event Management (SIEM)**

4.1. SIEM Deployment:

* A security information and event management (SIEM) system shall be deployed to aggregate, correlate, and analyse security events and logs from various sources across the organization's infrastructure.
* The SIEM platform shall provide centralized visibility into security incidents and enable timely response and remediation.

4.2. Threat Intelligence Integration:

* Threat intelligence feeds shall be integrated into the SIEM platform to enrich security event data with external indicators of compromise (IOCs) and known threat signatures.
* Threat intelligence shall be used to enhance the detection capabilities of the SIEM and prioritize response efforts.

**5. Incident Response Readiness**

5.1. Incident Detection Thresholds:

* Thresholds for detecting cybersecurity incidents shall be established based on predefined criteria, including severity, impact, and likelihood.
* Incident detection thresholds shall be reviewed and adjusted periodically to reflect changes in the threat landscape and organizational risk tolerance.

5.2. Incident Response Team:

* An incident response team shall be designated and trained to respond to cybersecurity incidents promptly and effectively.
* The incident response team shall consist of individuals with specialized skills in incident detection, analysis, containment, eradication, and recovery.

**6. Continuous Monitoring**

6.1. Real-time Monitoring:

* Continuous monitoring of information systems and networks shall be conducted in real-time to detect and respond to cybersecurity events as they occur.
* Automated monitoring tools and technologies shall be used to enhance the organization's ability to detect and respond to security threats promptly.

**7. Review and Revision**

7.1. Policy Review:

* This cybersecurity detect policy shall be reviewed and updated periodically to reflect changes in the organization's technology environment, business operations, and regulatory requirements.
* Reviews shall be conducted at least annually or more frequently as needed.

**Reference Documents**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |