Elevaite365

Log Management and Monitoring Policy

Version 1.0

PURPOSE

This policy defines the requirements for managing and monitoring the logs generated on the organization's cloud infrastructure, safeguarding information assets' confidentiality, integrity, and availability.

SCOPE

This policy applies to Elevaite365 (herein referred to as "the Organization") and all its employees, contractors, and third parties. It encompasses all IT systems, applications, virtual machines (VMs), and network devices within the Organization's cloud platform, where logs are generated, stored, and analyzed. This includes, but is not limited to, services provided by AWS, Azure, and Google Cloud Platform (GCP).

DEFINITION

Incident: An event that indicates harm or has a high potential to cause damage to the organization in terms of security, confidentiality, or availability

CISO: Chief Information Security Officer

Virtual Machine: A virtual machine (VM) is a digital version of a physical computer. VM software can run programs and operating systems, store data, connect to networks, and perform other computing functions. It requires maintenance, such as updates and system monitoring

Audit Trail: A security-relevant chronological record, set of documents, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected a specific operation, procedure, event, or device at any given time.

SIEM: Security Information and Event Management

NDA: Non-Disclosure Agreement

Log: A file that records events, processes, messages, and communications within an IT system or network.

Cloud Platform: A suite of cloud services provided by cloud service providers (e.g., AWS, Azure, Google Cloud) that enable the deployment, management, and scaling of applications and services.

RESPONSIBILITIES

1. **IT Head**
    a. **Policy Ownership:** Owns the Log Management and Monitoring Policy and is responsible for its implementation and enforcement across the Organization.
    b. **Coordination:** Collaborate with the DevOps Head and ISG to ensure effective logging and monitoring practices.
    c. **Resource Allocation:** Ensure adequate resources for logging and monitoring activities, including tools and personnel.
    d. **Compliance Oversight:** Ensure all logging and monitoring activities comply with relevant laws, regulations, and organizational policies.
2. **DevOps Head**
    a. **Log Monitoring and Maintenance:**
    b. Monitor and maintain logs of network activity, including but not limited to the status of virtual machines, capacity, management events, and performance.
    c. Utilize the logging and monitoring services the cloud platform provides (e.g., AWS CloudTrail, Azure Monitor, Google Cloud Logging) to monitor and log network activity.
    d. **Tool Management:**
    e. Implemented and managed log monitoring tools to analyze logs for anomalies and generate alerts.
    f. Configure automated alerts within these tools to notify the DevOps Head when anomalies are identified in the event logs.
    g. **Log Review Frequency Review:**
    h. Conduct Monthly reviews of all logs to ensure compliance with the **Data Retention and Deletion Policy**.
    i. Ensure that logs are not edited or deleted by unauthorized users.
    j. **Incident Response:**
    k. Raise, investigate, and resolve incidents upon alerts of suspicious or security-related events.
    l. Maintain an audit trail of the investigation and actions taken by the **Incident Management Policy**.

m. **Secure Sharing:**
n. Ensure that any sharing of logs with external parties adheres to the organization's policies, including having NDAs in place, obtaining approvals, using secure transfer methods, and protecting passwords.

3. **Chief Information Security Officer (CISO)**
   a. **Oversight:** Provide strategic oversight for log management and monitoring activities.
   b. **Compliance:** Ensure log management practices comply with relevant laws, regulations, and industry standards (e.g., GDPR, HIPAA, ISO 27001).
   c. **Risk Management:** Assess and manage risks associated with log data, including data breaches and unauthorized access.
   d. **Policy Development:** Develop and update log management policies and procedures with the ISG and DevOps Head.
   e. **Incident Oversight:** Oversee the investigation and resolution of security incidents related to log data.
4. **Information Security Group (ISG)**
   a. **Implementation Support:** Assist in implementing and maintaining logging and monitoring tools and processes.
   b. **Training:** Train relevant personnel on effective log management and monitoring practices.
   c. **Audit and Compliance:** Conduct regular audits to ensure compliance with the Log Management and Monitoring Policy.
   d. **Continuous Improvement:** Identify areas for improvement in log management and monitoring practices and recommend enhancements.
   e. **Collaboration:** Work with relevant departments to ensure that technical and organizational aspects of log management are effectively managed.

POLICY

Log Collection and Management

1. **Comprehensive Logging:**
   a. **Support Across Systems:** Logs and audit trails shall support all systems and applications within the Organization's cloud platform. These logs must capture every addition, modification, and deletion of information to ensure a complete and accurate record of activities.
2. **Responsibilities of the** IT Support Lead
   a. **Monitoring and Maintenance:** The IT Support Lead, is responsible for monitoring and maintaining network activity logs. This includes but is not limited to, tracking the status of virtual machines, assessing capacity, overseeing management events, and evaluating performance metrics.
   b. **Utilization of Logging Services:** The IT Support Lead, will leverage the logging and monitoring services provided by the cloud platform (e.g., AWS CloudTrail, Azure Monitor, Google Cloud Logging) to monitor and log network activity effectively.
3. **Log Retention and Integrity:**
   a. **Adherence to Retention Policy:** All logs must be retained by the Organization's Data Retention and Deletion Policy.
   b. **Protection of Log Files:** Users are strictly prohibited from editing or deleting log files to maintain the integrity and reliability of audit trails.
4. **Log Review:**
   a. **Scheduled Monitoring:** The IT Support Lead, will monitor and review logs on a log review frequency basis to identify and address any irregularities or security concerns.
   b. **Error Log Management:** Error logs must be reviewed regularly and resolved promptly to prevent potential security breaches.
5. **Security Logs Monitoring Methods:**
   a. **Method 1:** Utilize services such as **CloudTrail**, **Azure Audit**, or **Google Cloud Logs** to monitor all actions within AWS, Azure, or GCP environments, enabling detailed auditing capabilities.
   b. **Method 2:** Employ a dedicated log monitoring tool to analyze these logs for anomalies and generate alerts. This tool should also collect and aggregate all server logs for daily review.
6. **Automated Alerts Configuration:**
   a. **Alert Setup:** Configure automated alerts within the chosen log monitoring tool to notify the IT Support Lead, when anomalies are detected in event logs.
   b. **Actionable Alerts:** Ensure these alerts are actionable and provide sufficient context to facilitate timely investigation and response.
7. **Incident Management:**
   a. **Incident Response:** Upon receiving an alert of a suspicious or security-related event, the incident management policy will raise an incident, investigate it, and resolve it

b. **Audit Trail Documentation:** Maintain an audit trail of the investigation process and actions taken to ensure accountability and traceability.

8. **Secure Sharing of Logs:**
    a. **External Sharing Protocols:** When logs or related information need to be shared with external parties to resolve, receive support, or mitigate the effects of an issue or incident, the Organization must ensure the following:
        i. **Non-Disclosure Agreement (NDA):** An NDA must be in place with the external party.
        ii. **Approval Requirement:** The DevOps Head and the CISO must approve sharing information.
        iii. **Secure Transfer Methods:** Utilize secure file transfer methods to protect the data during transmission.
        iv. **Password Protection:** Ensure that passwords or sensitive information within the logs are adequately protected.
9. **Log Deletion Procedures:**
    a. **Retention Compliance:** During the Monthly log review, any logs exceeding the retention period specified in the Data Retention and Deletion Policy will be requested for deletion.
    b. **Automated Log Cleaning:** Automated log cleaning must be logged as an incident and investigated by the Incident Management Policy.
10. **Audit Trail Generation:**
    a. **Comprehensive Documentation:** All log management and monitoring activities must generate an audit trail. These audit trails must be saved to ensure accountability and for future reference.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Aug 29 2025	Initial Release	Borhan	Linh	Borhan