Document Reference:	ISMS	Effective Date:	07/05/2024
Document Name:	Monitoring & Log Analytics	Expiry Date:	07/05/2025

Monitoring & Log Analytics

SIT374 Team Project A

Redback Operations

Document Owner:	Daniel McAulay	Last Modified By:	Daniel McAulay
Next Review Date:	07/05/2025	Last Modified on:	07/05/2024

Version	Modified By	Approver	Date	Changes made
V0.2	Daniel McAulay	Daniel McAulay	07/05/2024	Document Creation

Contents

Scope

The Monitoring & Log Analytics Cyber Security Policy will apply to all IT systems and networks owned or operated by Redback Operations.

Monitoring in the context of this policy refers to the continuous oversight of IT infrastructure, which includes servers, networks, applications, and systems, to ensure operational stability and security. It involves the real-time scanning and analysis of data to detect, alert, and respond to potential performance issues or security threats.

Log Analytics is the process of using tools to collect, aggregate, normalize, and analyse log data from various sources within the IT environment. This practice is essential for understanding the behaviour of systems, diagnosing problems, ensuring compliance with regulatory standards, and maintaining security across all operations.

Log analytics supports the identification of trends, unexpected occurrences, and potential security breaches by analysing the historical data provided by logs.

Note: This policy is a high-level policy that refers to a theoretical future deployment of a SIEM/SOC solution for Redback Operations.

Purpose

This monitoring and log analytics policy is designed to support Redback Operations in achieving and maintaining high standards of security and compliance throughout its operations. The purpose of this policy is multi-faceted and supports our commitment to maintaining the integrity, confidentiality, and availability of our data and systems.

Objectives

The objectives that this policy intends to achieve are:

- Enhance Security Posture
  - Proactively identify, assess, and mitigate risks and threats to our infrastructure and data assets.
- Achieve Compliance and adhere to Regulatory Requirements
  - Guarantee that all monitoring and log analytics practices strictly adhere to applicable legal, regulatory, and contractual obligations, thereby safeguarding the organization against legal and financial repercussions.
- Achieve Operational Excellence
  - Monitor and analyse system performance and reliability continuously to ensure optimal operation, system availability, and ensure business continuity.
- Enhance and Allow for Incident Management and Response
  - Establish and maintain a proactive, structured approach for timely detection, thorough analysis, and effective response to security incidents to minimize their impact and prevent recurrence.
- Provide Forensic Capabilities
  - Ensure detailed and accurate logging practices are in place to support forensic investigations and establish accountability and traceability within our systems.
- Ensure Confidentiality, Integrity, and Availability (CIA) of company systems, applications, infrastructure & operations.
  - The policy, in alignment with the Redback Operations Information Security Management System, aims to safeguard the “CIA” of all operational and sensitive data across the organization.
- Threat Detection and Analysis
  - Establish standards, guidelines and control processes to actively monitor and analyse data traffic and usage patterns across all systems and networks to quickly identify and mitigate potential security threats and breaches.

This policy is essential not only for achieving technical and operational goals but also for fostering a culture of security and compliance at all levels of the organization. It serves as a foundational security policy for guiding and securing technical systems implemented within Redback Operations.

Common Terminology

This sub-heading refers to common terminology, components, KPI & KGI indicators covered under this policy:

Definitions

The table provided below presents the expanded definitions and components list relevant to the Monitoring & Log Analytics Cyber Security Policy:

Term	Definition
Logs	Data records that systematically capture events or actions within an IT environment, providing a traceable and chronological sequence of activities.
Log Management	The process of collecting, storing, archiving, and disposing of logs in a secure and controlled manner, covering the entire lifecycle from log creation to destruction.
Monitoring	Continuous observation of real-time or recorded logs to identify patterns, anomalies, and potential security threats, aimed at proactive threat detection and system health monitoring.
Audit Trails	Records that provide documentary evidence of the sequence and context of activities that have affected specific operations, procedures, or events, crucial for compliance and forensic analysis.
Event Correlation	A technique used to identify relationships between various events logged across different systems, aiding in pinpointing security incidents by connecting related anomalies.
Anomaly Detection	The process of identifying patterns in log data that do not conform to expected behaviour, key in spotting potential security breaches or system failures early.
Threat Intelligence	Information used to understand the capabilities, infrastructure, motives, goals, and actions of potential attackers, integrated into monitoring tools to enhance threat detection.
Data Retention	The policy and process determining how long log data should be retained based on legal, regulatory, and operational requirements, ensuring compliance while minimizing storage overhead.
Security Information and Event Management (SIEM)	A solution that aggregates and analyses activity from many different resources across your IT infrastructure, used for real-time analysis of security alerts generated by applications and network hardware.
Forensic Analysis	The detailed investigation of logs and other data following a security incident, aimed at understanding the actions that led to the incident and gathering evidence.

Guiding Principles

Here's a table that details the guiding principles relevant to the Monitoring & Log Analytics Cyber Security Policy:

Principle	Description
Comprehensiveness	Ensures all relevant data is captured, providing a detailed and complete view of system and user activities.
Security	Mandates that logs and their management processes adhere to the highest standards of data protection.
Accessibility	Balances the need for security with the requirement that logs be easily accessible to authorized personnel.
Integrity	Guarantees that logging information remains accurate, complete, and unaltered except by authorized processes.
Efficiency	Encourages the design of logging and monitoring processes that maximize resource use and operational performance.
Scalability	Ensures that log management systems can scale with organizational growth or an increase in data volume.
Resilience	Aims to maintain continuous operation of logging and monitoring systems, even in the face of failures.
Comprehensiveness	Ensures all relevant data is captured, providing a detailed and complete view of system and user activities.
Security	Mandates that logs and their management processes adhere to the highest standards of data protection.

General Obligations:

Here's a table that details the obligations that Redback Operations adheres to through the Monitoring & Log Analytics Cyber Security Policy:

Principle	Description
Comprehensiveness	Ensures all relevant data is captured, providing a detailed and complete view of system and user activities.
Security	Mandates that logs and their management processes adhere to the highest standards of data protection.
Accessibility	Balances the need for security with the requirement that logs be easily accessible to authorized personnel.
Integrity	Guarantees that logging information remains accurate, complete, and unaltered except by authorized processes.
Efficiency	Encourages the design of logging and monitoring processes that maximize resource use and operational performance.
Scalability	Ensures that log management systems can scale with organizational growth or an increase in data volume.
Resilience	Aims to maintain continuous operation of logging and monitoring systems, even in the face of failures.
Comprehensiveness	Ensures all relevant data is captured, providing a detailed and complete view of system and user activities.
Security	Mandates that logs and their management processes adhere to the highest standards of data protection.

Key Assets and Data Categories

For Redback Operations, identifying the critical systems, applications, and data sets that require monitoring and logging is crucial. This includes any sensitive information that needs heightened security measures. Here are typical IT assets and data categories that are critical:

- **IT Assets**:
  - Servers (web, application, database)
  - Network devices (routers, switches, firewalls)
  - End-user devices (laptops, smartphones)
  - Cloud services and storage solutions
  - Critical software applications (CRM, ERP, custom applications)
- **Data Categories**:
  - Customer data (personal identification information, payment details)
  - Employee data (personal details, HR records)
  - Intellectual property (trade secrets, proprietary technology)
  - Financial data (transaction records, financial reports)
  - Operational data (logs, configuration files)

These assets and data types require robust monitoring to ensure they are protected from unauthorized access, modifications, or any other cyber threats.

Framework References

The Monitoring and Log Analytics Policy leverages the following framework controls to ensure a robust approach to information security and risk management:

ISO 27001:2022 Controls:

- **A.12.1 Operations Security**: Involves correct and secure operations of information processing facilities to enhance the overall security of operations.
- **A.12.4 Logging and Monitoring**: Ensures that events are recorded and analysed to detect, prevent, and recover from security incidents.
- **A.12.7 Information Systems Audit Considerations**: Manages the audit of information systems to ensure compliance with security policies and standards without disrupting business processes.
- **A.16.1 Management of Information Security Incidents and Improvements**: Focuses on ensuring a consistent and effective approach to the management of information security incidents, including communications on security events.

CIS Controls:

- **Control 3: Data Protection**: Protects data through controls that enforce confidentiality and integrity, ensuring availability as required for monitoring and logging purposes.
- **Control 6: Audit Log Management**: Focuses on the collection, management, and analysis of audit logs to help detect and understand security incidents.
- **Control 8: Malware Defences**: Ensures that devices are monitored and protected against malware infections and activities.
- **Control 16: Account Monitoring and Control**: Involves managing the lifecycle of user and service accounts, including monitoring the use of these accounts to detect unauthorized access.
- **Control 19: Incident Response and Management**: Provides a structured method for managing the aftermath of security breaches or attacks, including establishing processes to ensure timely response to incidents.

These controls have been specifically selected to enhance the effectiveness of the Monitoring and Log Analytics Policy by aligning it with recognized best practices for security monitoring, data protection, and incident management. This alignment not only improves security posture but also ensures regulatory compliance and operational efficiency in handling security threats and incidents.

Roles and Responsibilities

For Redback Operations, clearly defined roles and responsibilities are essential to maintain an effective monitoring and log management system. Here are the typical roles involved and their respective duties:

Chief Information Security Officer (CISO)

- Oversees the cybersecurity strategy, including monitoring and log analytics policies.
- Ensures that all monitoring and log management practices comply with internal and external regulations.

IT Security Manager

- Manages the daily operations of security systems and ensures the effective implementation of the log analytics policy.
- Leads the security team in developing and maintaining security protocols.

Network Administrator

- Responsible for the management and monitoring of network devices including routers, switches, and firewalls.
- Ensures that all network configurations align with the security standards.

System Administrator

- Oversees the monitoring of all server and end-user devices.
- Manages the collection, storage, and maintenance of log data from servers and other critical systems.

Database Administrator

- Monitors database operations and ensures that access logs are maintained and reviewed.
- Responsible for the security and integrity of database assets.

Application Manager

- Ensures that all application logs are collected and analysed.
- Monitors the performance of business-critical applications and ensures they meet the required standards.

Security Analyst

- Analyses log data to identify, investigate, and respond to potential security threats.
- Acts quickly to mitigate any detected threats or breaches.

Compliance Officer

- Monitors compliance with legal and regulatory requirements pertaining to log management and cybersecurity.
- Coordinates internal and external audits of cybersecurity practices.

IT Support Staff

- Provides support to end-users on security best practices and assists with incident response.
- Assists in the management of monitoring tools and systems.

RACI Chart

A RACI chart is a valuable management tool used to delineate the roles and responsibilities across different team members for specific activities within a project or process. It clarifies expectations, enhances communication, and ensures clear ownership of tasks, aiding in project and process management.

Role	CISO	IT Security Manager	Network Admin	System Admin	Database Admin	Application Manager	Security Analyst	Compliance Officer	IT Support Staff
Develop and update security policies	A	R	-	-	-	-	-	C	-
Implement security measures	-	A	R	R	R	R	-	-	-
Daily monitoring of systems	-	-	R	R	R	R	R	-	R
Manage security incidents	C	A	-	C	C	C	R	-	C
Compliance and audits	C	C	-		C	-	-	A	-
Policy training and updates	-	C	-	-	-	-	-	-	R
Log data management	-	-	C	R	R	C	C	C	C

Legend

- R (Responsible): Performs the activity or does the work.
- A (Accountable): Ultimately accountable for the correctness and thoroughness of the activity. Only one Accountable per task.
- C (Consulted): Provides information and feedback during the process; two-way communication.
- I (Informed): Receives information about the process; one-way communication.

Types of Digital Assets Covered Under the Log Analytics Policy

This structured list of assets defines (but is not limited to) the broad scope of the Log Analytics Cyber Security Policy, ensuring that all critical systems and infrastructure are monitored in alignment with this policy.

Web-facing Applications and Services

- **Public Websites, Gateways, and Portals**
  - Includes main websites, customer portals, and blogs hosted on domains owned by Redback Operations.
- **Web Applications**
  - Online applications providing services or interactions to users, such as web-based email systems, CRM platforms, custom business applications, and APIs.

Network Infrastructure

- **DNS Servers**
  - Servers responsible for resolving domain names into IP addresses.
- **Firewalls and Edge Devices**
  - Devices at the network boundary protecting against external threats, including Next-generation firewalls (NGFWs) with intrusion prevention systems (IPS).
- **VPN/Remote Access Gateways**
  - Endpoints for VPN access that allow secure remote connections to the internal network, like SSL VPN appliances.

Cloud Services and Infrastructure

- **Cloud-based Web Hosting**
  - Services used for hosting websites and web applications on cloud platforms.
- **Cloud Storage**
  - Publicly accessible cloud storage solutions, such as Microsoft Azure Storage accounts.
- **IaaS, PaaS & SaaS Services**
  - Cloud-based applications accessed over the Internet, including Salesforce CRM, Google Workspace, and cloud infrastructures like Google Cloud Platform and Microsoft Azure.

Email and Communication Servers

- **Email Servers**
  - Servers handling incoming and outgoing email communications, including SMTP, IMAP, and POP3 servers.
- **Unified Communications Systems**
  - Systems providing services such as VoIP, video conferencing, and instant messaging, e.g., Microsoft Teams or Zoom.

Remote Access Services

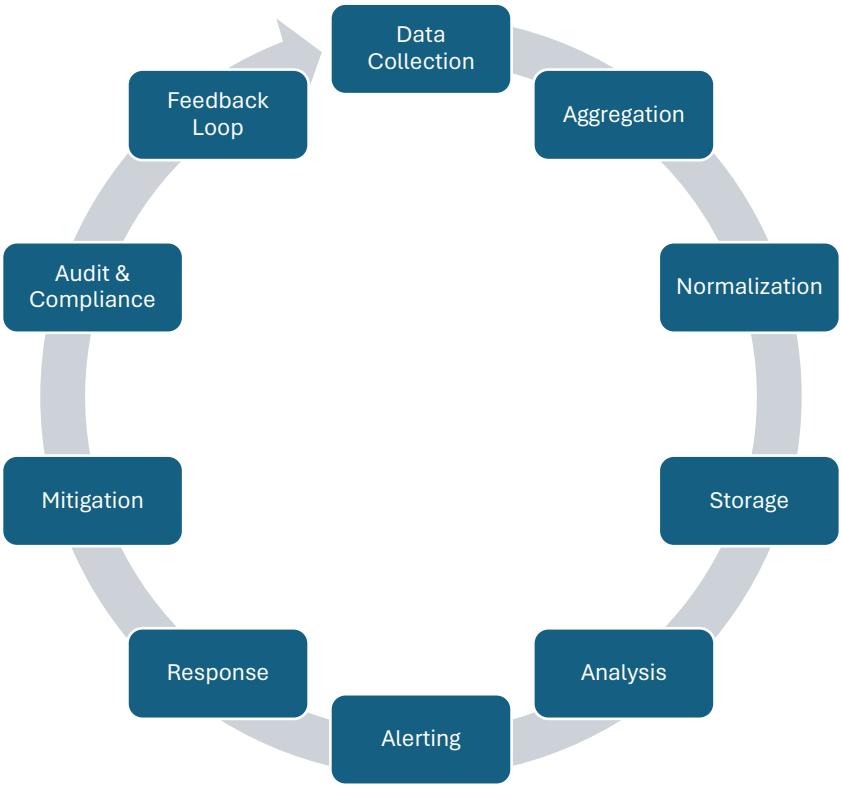
- **Remote Desktop Services**
  - Services allowing remote control of desktops or servers, such as Remote Desktop Protocol (RDP) endpoints.
- **Network Management Systems**
  - Tools and systems for managing and monitoring network infrastructure, including SNMP interfaces on network devices.
- **Privileged Access Management Platform**
  - Platform used for managing identities and facilitating privileged access to sensitive systems.

IT Assets

- **Servers**
  - Includes web, application, and database servers.
- **Network Devices**
  - Routers, switches, and firewalls.
- **End-user Devices**
  - Laptops, smartphones, and other personal devices used within the organizational network.
- **Critical Software Applications**
  - Enterprise applications such as CRM, ERP systems, and other critical software.

Monitoring & Log Analytics Lifecycle

The typical Monitoring & Log Analytics Lifecycle for effective systems can be defined as:



Data Collection	• Gathering logs from various sources such as servers, applications, and network devices.
Aggregation	• Combining logs from multiple sources into a unified format.
Normalization	• Standardizing log data to ensure consistency and facilitate analysis.
Storage	• Securely storing logs for retention and accessibility.
Analysis	• Analyzing logs to identify patterns, anomalies, and potential threats.
Alerting	• Generating alerts based on analysis outcomes to signal potential issues.
Response	• Addressing alerts by taking appropriate actions to resolve issues.
Mitigation	• Implementing measures to prevent future occurrences of detected issues.
Audit & Compliance	• Ensuring log management practices comply with relevant standards and regulations.
Feedback Loop	• Using insights from the lifecycle to improve data collection and analysis processes.

Log Collection Management, Practices & Activities

Redback Operations subscribes to a comprehensive framework for the collection, formatting, management, and analysis of log data across all IT systems and networks. This framework is designed to ensure the integrity, availability, and confidentiality of log information, which is crucial for maintaining security, facilitating incident response, and complying with legal and regulatory obligations.

Data & Log Types

User Access and Authentication Logs

Track all user login, logout, and authentication attempts to monitor unauthorized access attempts and user activity.

System and Application Changes

Record all updates, configuration changes, and software installations to ensure system integrity and audit system changes.

Network Activity Logs

Capture all data related to network traffic, including firewall logs, intrusion detection system logs, and network access logs, essential for detecting potential threats and malicious activities.

Data Access and Usage Logs

Document access to sensitive data and actions performed on the data, critical for protecting data privacy and detecting data breaches.

Log Formats

Standardized Formats

Logs are standardized to JSON or XML formats, which simplifies parsing and integration with various log analysis tools, aiding in automation and rapid response by SOC teams.

Detailed Elements

Logs incorporate essential elements like timestamp, user ID, event type, source IP, destination IP, and action details, providing comprehensive traceability and context for security analysis.

Encryption and Secure Streaming

All logs are encrypted during transmission and at rest. This ensures the confidentiality and integrity of log data, protecting it against unauthorized access and tampering.
Utilize secure channels (e.g., TLS/SSL) for log transmission to ensure that data is securely streamed in real-time to the log management systems without interception or data loss.

Security Operations Centre (SOC) Activities

Real-time Monitoring and Analysis

SOC teams utilize real-time log data to identify and respond to incidents swiftly, employing advanced tools for anomaly detection and threat hunting.

Incident Response and Forensics

The following rules apply to Incident Response & Forensics:

- Logs should provide crucial evidence and aid in forensic investigations to understand attack vectors and mitigate threats effectively.
- Real-time log analysis must be conducted for identifying security incidents, operational issues, and compliance anomalies.
- SIEM systems must be configured to generate alerts based on predefined criteria for critical events such as unauthorized access attempts, system failures, or significant changes to sensitive systems.
- In the event of security incidents, logs must be used to perform root cause analysis, identify indicators of compromise (IoC) and to aid in remediation efforts.
- Logs related to any identified incident must be preserved beyond the standard retention period until the incident is fully resolved and closed.

Refer to the Incident Response Policy & relevant playbooks for further information.

Log Collection Frequency & Retention

Log Collection Standards

The following rules apply in relation to Log Collection, Retention & Storage requirements:

- All systems must transmit logs securely to centralized log management solutions using encrypted channels (TLS 1.2 or higher).
- Log collection agents must be configured to capture all log entries without filtering, to ensure comprehensive data capture.
- Logs must be stored in encrypted form using AES-256 encryption to ensure their confidentiality and integrity.
- Access to logs must be controlled via role-based access controls (RBAC), ensuring that only authorized personnel have access based on their specific roles and needs.
- Critical systems and security logs are collected in real-time to facilitate immediate analysis and response to potential security threats.
- Application and system logs are configured to capture data per session or transaction, while network logs are typically collected at regular intervals, adjusted based on traffic volume and risk assessment.

Retention Duration

The following rules apply in relation to Retention requirements:

- Log retention periods are defined based on legal, regulatory, and operational needs. Log retention may extend up to several years based on the sensitivity of the target system.
- All logs must be retained for a minimum of 12 months, subject to target source criticality. Critical systems such as financial or personally identifiable information (PII) handling systems must retain logs for a minimum of 24 months.
- Logs must be archived in a secure manner at the end of their active life and must be readily accessible for audit purposes for an additional 12-month post-retirement.

Secure Storage and Destruction

Logs are securely stored in encrypted formats with access controls strictly limiting access to authorized personnel only.

Note: Procedures for the secure destruction of data are referenced in the Data Classification & Data Loss Prevention policy within the ISMS. Refer to this policy for further information.

Compliance with Standards & Controls

The log management practices defined in this policy align with CIS Controls for effective log management and ISO/IEC 27001 standards for information security management, ensuring data governance and compliance adherence with global cybersecurity industry standards.

By enhancing the log collection practices as outlined, Redback Operations strengthens its cybersecurity framework, ensuring that log management not only meets compliance requirements but also supports proactive security monitoring and incident management effectively. This detailed approach facilitates a secure, compliant, and efficient operational environment.

Auditing & Review

Compliance audits of log management practices must be conducted **annually** to ensure adherence to this policy and relevant legal or regulatory standards. Audit trails must be maintained for all access and changes to log data, to provide accountability and traceability.

Documentation and Training

All procedures related to log management must be fully documented and updated annually or following significant changes to the IT environment. Staff involved in log management must receive regular training on their responsibilities under this policy and on the secure handling of log data.

SIEM/SOC Logging Protection

To ensure the confidentiality, integrity, and availability of log data at Redback Operations, it is critical to implement security measures. Here are the minimum high-level requirements for protecting the integrity of the Redback Operations SIEM/SOC platform:

Data Encryption:

- Utilize strong encryption standards such as AES-256 for log data at rest and TLS for log data in transit to protect against unauthorized access and interception.

Note: Refer to the Cryptography Policy within the Redback Operations ISMS for further detail.

Access Control:

- Implement strict access controls using role-based access control (RBAC) to ensure only authorized personnel have access to log data.
- Use multi-factor authentication (MFA) for systems accessing log data to add an additional layer of security and adhere to common industry framework controls such as CIS.

Log Integrity:

- Apply cryptographic hashing to log entries to detect and prevent unauthorized changes.
    - Any alteration of the log data will result in a different hash value, indicating tampering.
- Use log management solutions that support log immutability (such as write-once-read-many (WORM) storage) to prevent alteration or deletion of log data.

Regular Security Assessments:

- Conduct regular security assessments of the log management infrastructure to identify vulnerabilities.

Note: Refer to the Attack Surface Management policy referenced in the Redback Operations ISMS for further detail.

Redundancy and Backup:

- Regularly backup log data to secure, geographically dispersed locations to prevent data loss from local disasters or system failures.

Note: Refer to Redback Operations Business Continuity & Disaster Recovery Policy for further detail.

Policy Review

Regular reviews and timely updates to the Monitoring & Log Analytics Cyber Security Policy are essential for keeping it relevant and effective at Redback Operations.

Note: Company layout and infrastructure does not reflect the standards outline in this policy at the time of this document's creation and is considered a long-term strategy to implement when company maturity has improved.

Responsibility for Reviews

The Chief Information Security Officer (CISO) is designated as the primary initiator of the reviews for the cyber security policy at Redback Operations. A review committee assists in evaluating the effectiveness and relevance of the policy.

Frequency of Reviews

Reviews are scheduled to occur at least annually. However, more frequent reviews are conducted if there are significant changes in technology, business practices, or compliance requirements. Ad-hoc reviews are also permitted in response to security incidents or major failures in the existing policy.

Proposing and Approving Changes

Any member of the review committee can propose changes during the review process. These proposals should be supported by a rationale and, where possible, data to substantiate the change. After a thorough discussion within the committee, the CISO presents the proposed changes to senior management for approval.

Communication Plan for Updates

Once changes are approved, the updated policy is communicated to all stakeholders through internal memos, meetings, and training sessions. It is crucial to ensure that all employees understand the changes and how they impact their roles and responsibilities. Regular training sessions are updated to reflect the new policy standards.

Documentation and Record-Keeping

Detailed records of all review meetings, discussions, decisions made, and the reasoning behind changes are maintained meticulously. The version history of the policy is documented to track changes over time and provide context for future amendments.