Ministry of Communications & Information Technology

Log Management and Monitoring Standard

Table of Contents

1 Introduction

Robust logging and monitoring is important in serving to strengthen the oversight of the Government of Samoa (GoS) security posture by detecting, identifying and recording potential and realized attacks. This then enables us to promptly manage the events in our system and network, and ultimately to reduce the likelihood of them resulting in an incident and impacting GoS.

1.1 Purpose and Scope

This standard establishes requirements for collecting, monitoring, and analysing log data from GoS systems. This ensures there is accountability and traceability for all actions that occur on GoS systems, ensures that malicious and anomalous activity can be detected, that appropriate controls are applied to prevent future potentially damaging events, and an audit trail is maintained.

This standard applies to the environment monitored by the GoS Security information and event management system (SIEM) and its interrelated components.

No system within this environment is considered to fall outside the scope of this standard unless an exemption has been made and approved in accordance with the Ministry of Communications, Information and Technology (MCIT). A justification must be provided to the MCIT for a risk-based assessment, and subsequently approved by the CEO. It must then be recorded in the Government risk register.

1.2 Key Principles

Log where possible

- Where systems have logging available, this should be enabled. All GoS systems should strive to align with the logging requirements put forward in this standard.The GoS will be aware of requirements for retention periods for logs and act accordingly.

Review logs regularly

- The GoS will strive for consistency with conducting and maintaining records of log reviews across their systems. Log reviews should aim to identify as much details of events, commensurate to the criticality of that environment.

Maintain logs across their entire lifecycle

- The GoS strives to protect logs and logging systems through the use of controls across the entire logging procedure. It is important this be done to maintain the integrity and confidentiality of logs that then inform our perception of what has taken place in the GoS environment.

2 Requirements

2.1 Time Synchronisation

The following table outlines the requirement for how network time protocols are to be applied within the GoS environment for systems:

Requirement	Description
All systems must be time synchronised	• All systems in the GoS environment in scope must synchronise time from the same authoritative Network Time Protocol (NTP) source (as per the Samoa Government NTP server). • This will ensure there is a consistent time throughout the environment, which aids not only in the identifying relationships between events and the development of a timeline in an incident.

2.2 Log Analysis

The following table outlines the requirements for how logs collected by the GoS are to be analysed:

Requirement	Description
Log analysis rules must be clearly defined and catalogued	• Log analysis must be based on a defined and agreed Use Case Catalogue. At a minimum, this Catalogue must contain: ○ The Use Case focus ○ The Rules used to satisfy the Use Case ○ The rule logic, if not maintained as live content on a SIEM ○ The expected triggers ○ This applies to both basic log management and any SIEM deployments. • The Use Case Catalogue must be fully maintained and kept current. • This requires updates following an incident, when a rule changes, or when intelligence is received • Rules are to be assessed every three (3) months for suitability. • All changes to rules, alerts, reports, and playbooks/runbooks must be recorded. • The Use Case Catalogue is maintained by the MCIT ICT Team maintaining the SIEM and informed by SamCERT and any intelligence they may have.
Continuous Log Review	• Logs that are collected in logging servers must be analysed and reviewed in a timely manner for anomalous and suspicious activities. Where possible and within scope, this is to be centralised by the SIEM. • Log analysis must be conducted using automated log analysis and correlation functions where possible. Where this is not possible (e.g., on applications such as the threat intelligence platform and vulnerability management tools) this is to be completed by the MCIT ICT Team and SamCERT if deemed necessary. • The SIEM will conduct continuous log reviews for anomalous or suspicious activity.

Requirement	Description
Log analysis must inspect incongruous or unusual login act	At a minimum, log analysis must specifically examine the following: - User logins out of business hours - Unusual login source IP addresses, particularly from countries other than Samoa - Logins of the same account from multiple source IP addresses in a short period of time - A high number of failed login attempts (e.g., 5 attempts) - Unusual logins and / or interactive sessions for service accounts - Unusual logins for privileged accounts - Activity by inactive or deactivated accounts - Mass addition or deletion of accounts - Privileged / ‘pseudo’ activity on systems - Login attempts to components in the infrastructure (outside of routine maintenance). - Login attempts to recovery/privileged accounts - Other actions deemed critical
Log analysis must inspect account and file changes made	At a minimum, log analysis must specifically examine privileged accounts and other accounts deemed necessary across all critical infrastructure components for the following: - User accounts added, deleted, changed, and disabled - Privilege escalation to accounts and files - Passwords changes - Configuration changes
Log analysis must inspect error messages and alerts	At a minimum, log analysis must specifically examine the following: - Error messages generated for applications and systems which may affect the confidentiality, integrity and availability of systems. - Alerts of critical service failures - Alerts of potential infections by anti-malware software installed on systems
Log analysis must inspect system process activity	At a minimum, log analysis must specifically examine the following: - Alerts of critical system processes starting, stopping or restarting
Log analysis must inspect resource access requests made	At a minimum, log analysis must specifically examine the following: - Excessive attempts to access resources or files that users are not authorised to view - Large files being transferred - Malicious traffic allowed by firewalls and excessive deny packets being logged

2.3 System Specific Logging

The following table outlines the details of events that should be logged from all systems and applications in scope of the GoS SIEM and interconnected components:

Requirement	Description
All in scope GoS systems events must be logged	Events to be logged include: • All actions performed using administrator and/or privileged accounts • Successful and unsuccessful access attempts to all systems in the IT environment • Successful and unsuccessful access attempts to all audit logs • Initialisation, clearing and/or starting and stopping of audit log processes on the system • Creation, deletion, and disablement of system level objects
Operating Systems (OS) events must be logged	Operating System events to be logged include: • Logon and logoff events from all accounts configured in the in-scope environment (both successful and unsuccessful) • Any series of consecutive failed logon attempts. This is to be tracked following 5 logon attempts. • Changes to any accounts configured in the environment including but not limited to: ○ Privilege elevation from normal end-user account to privileged level access on a system or application ○ Modification (inclusion, deletion) of additional privileges or role(s)/group(s) to existing user accounts ○ Failed attempts to access information and/or system/application resources ○ Successful and unsuccessful attempts to use privileged accounts ○ Successful and unsuccessful attempts to manage accounts and groups on all systems ○ Successful and unsuccessful security policy change attempts in the operating system ○ Service starts, failures and restarts ○ System start-up and shutdown ○ Where able, the, copying, accessing and deleting of sensitive information in the operating system

2.4 Network and Security Infrastructure Logging

The following table outlines the details of events that are to be logged from network and security infrastructure systems in the GoS environment:

Requirement	Description
Firewall, router, and switch events must be logged	Events to be logged include: • Successful and unsuccessful login or logoff attempts for network and security device administrators and users • Device start up and shutdown • Changes to network device configuration parameters, particularly Access Control Lists (ACLs), Authentication and Management functions • Suspicious events triggering attack signatures where this feature is enabled on the device for both network and application-based attacks • Successful and unsuccessful additions and deletions of firewall objects • All connections that are rejected and dropped by the “deny all” rules for all ACLs • Successful and unsuccessful changes to administrative and/or privileged accounts • Successful and unsuccessful connection attempts made to management interfaces **Note:** Much of the logging of these sources may be more useful for infrastructure teams and/or for forensic ‘post-incident’ analysis. As such these logs may, or may not, be sent through to the SIEM if a lower cost logging alternative is available.
Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) – Host and Network – events must be logged	Where IDS / IPS have been established for the GoS, these should be monitored and logged: • Events to be logged include: ○ System start up and shut down ○ Successful and unsuccessful login or logoff of privileged user accounts ○ Successful and unsuccessful changes to administrative accounts and administrative functions in the device ○ Intrusion alerts ○ Heuristic anomalies ○ Matches to attack signatures ○ All blocking attempts where intrusion and attack signatures are matched

2.5 Log Security, Backup and Retention

The following table outlines the requirements to be observed in order to maintain the security of logs, have appropriate backup measures, and be retained as required:

Requirement	Description
User access to logs and logging environment must be restricted	The following controls to secure access to logs must be in place: • User access to the logging environment and logs must observe 'least privilege' (minimum level of access to perform their role) rules for access • Users not requiring privileged access to the log environment must only be provided time bound 'read' only access (e.g., where users only need to review logs) • Users who require privileged accounts to access the logging systems must only be provided with least privileges to complete their roles. Privileged accounts such as SIEM accounts must be approved by SamCERT or ICT Managers
Transmission of logs must be adequately secured	The following controls to secure log transmission must be in place: • Any attempts to edit configurations on the log transfer agents must be monitored • Transmission of logs between logging system components must occur using approved encrypted connections. This is mandatory if logs are to cross open networks or the internet to be collected. • Where transmission failure occurs, systems must re-attempt transmission of log data. Where transmission failure continues: • Logs must be stored on the generating host until communication is re-established. 'Read-only' access to the log files on each system must be restricted to authorised users only and any access to these logs must trigger a logging event • A report of the failed transmission along with cause of failure should be generated and sent to the MCIT ICT Manager who, where required, will escalate to SamCERT
Audits of logging systems must be conducted	Audit requirements for logging systems are as follows: • Audits must be conducted for the logging system every six months to ensure logging systems are secure and logging is being performed appropriately • Evidence of audits must be retained. This will include use case catalogues, data dictionary's playbooks and reports (or other documentation) produced from the audit
Log Retention and Backup	The following controls to manage log retention and backup must be in place: • Logs must be backed up and retained, with a minimum of 3 months of logs stored and immediately available for review in the event of a security incident • Access to 12 months of logs and alerts is a recommended retention plan • Logs must be protected from loss or tampering during the required retention period, including: • Restriction of access to the logs by staff with a business requirement for access • Read only access to logs for authorised staff members only • Logging all access to the logs and logging systems • File Integrity Monitoring (FIM) for all logs and logging systems

Requirement	Description
	• Archived log files must be protected using approved digital signatures to maintain integrity of the files once stored • Archived log files must be kept physically secure and access to these logs must not be permitted unless a business requirement related to their job role exists

Appendix A: GoS Future State Logging

The following requirements have been identified as future state goals for the GoS to log.

Log requirements established in the above document are minimum requirements, while the items detailed below are aspirational states that the GoS will strive to achieve with the appropriate resourcing.

Requirement	Description
Email Gateway Alerts must be logged	• Where secure email gateways have been established for the GoS, these should be monitored and logged. • Events to be logged include: • Successful and unsuccessful login or logoff attempts to the email gateway • Alerts generated by the email gateway • Alerts regarding spam campaigns • Phishing or Spear-phishing activity • Any email source spoofing attempt • Targeted email campaigns on VIPs, Senior Management, nominated critical infrastructure staff and others deemed at risk
Events from Web Applications must be logged	Events to be logged include: • Input and output validation failures • Session management failures and compromises • Application errors and events • Application start-ups and shutdowns • Use of cryptographic keys and any changes to the cryptography configuration • Configuration changes to web applications
Database Events must be logged	Events from the database server that must be logged include: • Database server start-up and shutdown • Creation, modification or deletion of database objects • Successful and unsuccessful modification of access controls to database objects • Successful and unsuccessful creation, modification or deletion of database users • Successful and unsuccessful modification to database user properties and privileges • All privileged user actions in the database both successful and unsuccessful • Successful and unsuccessful database user logon and logoff attempts • Successful and unsuccessful transaction journaling for databases containing ‘sensitive’ data
Anti-malware software events must be logged – All Endpoints, Server and Workstation	Anti-Malware software includes Event Detection and Response (EDR) platforms, File Integrity Monitors (FIM), Data Loss Prevention (DLP), as well standard Anti-Malware and Anti-Virus platforms and agents. Events from these systems to be logged include: • Successful and unsuccessful start up and shut down of anti-malware software • Detection of infected files and connections • Quarantining of suspect and/or infected files • Cleaning of infected files • Successful and unsuccessful system compromise attempts

Requirement	Description
	• Successful and unsuccessful updating of anti-malware software signatures • Successful and unsuccessful updating of anti-malware software • Successful and unsuccessful attempts to disable the software on the system

Version Management

Version	Date	Comments and Remarks
1.0		