State of California

Department of Technology

Continuous Security Monitoring and Event Management Standard

Statewide Information Management Manual – 5335-B

August 2025

Table of Contents

Document History

Revision	Date of Release	Owner	Summary of Changes
v.1	August 2025	Office of Information Security (OIS)	Initial Release

Introduction

Purpose

Continuous security monitoring and event management are vital for robust information security defenses. This proactive approach allows state entities to detect and respond to threats and vulnerabilities in real time, significantly reducing the potential for damage. It also ensures compliance with various regulatory requirements, which mandate constant vigilance over information security and privacy practices.

This standard specifies the requirements for continuous monitoring and event management to ensure the security and integrity of information assets across all state departments. It adheres to the guidelines set by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, 800-53B, and 800-137 and incorporates specific operational protocols to enhance statewide cybersecurity efforts.

Scope

This standard applies to all California state entities, including agencies, departments, divisions, bureaus, boards, and commissions, as defined in Government Code Section 11546.1.

Compliance

As outlined in Government Code (GC) Section 11549.3, the Office of Information Security (OIS) is entrusted with creating, issuing, and maintaining policies, standards, and procedures, overseeing information security risk management for agencies and state entities, providing information security and privacy guidance, and ensuring compliance with State Administrative Manual (SAM) Chapter 5300 and Statewide Information Management Manual (SIMM) section 5300.

State entities must adhere to OIS-issued information security and privacy policies and all relevant laws, regulations, rules, and standards governing their state entity. Compliance may be reflected in audit findings and maturity scores. Non-compliance will

be addressed according to the Office of Information Security Policy Compliance and Enforcement Standard (SIMM 5330-H).

Definitions

Security Information and Event Management (SIEM): A comprehensive security solution that provides real-time analysis of security alerts generated by applications and network hardware. It primarily aggregates, analyzes, and reports on security data, helping organizations detect, monitor, and respond to cybersecurity incidents. SIEM's key functions include data aggregation, event correlation, alerting and notifications, compliance reporting, forensic analysis, and threat detection and response.

Minimum Continuous Security Monitoring and Event Management Requirements

This standard aligns with NIST Cybersecurity Framework 2.0 and the MITRE ATT&CK Framework. It sets the baseline minimum functional capabilities that each continuous monitoring program within the state must meet.

SIMM 5335-C, MITRE ATT&CK Framework, aligns the NIST controls below with corresponding MITRE ATT&CK coverage of Tactics, Techniques, and Procedures (TTPs). This mapping underscores the significance of each NIST control in addressing real-world threats, enhancing the framework's applicability in practical scenarios.

Details on how the following NIST controls demonstrate the minimum MITRE ATT&CK coverage of TTPs required for each entity are provided in SIMM 5335-C.

Minimum Requirements	
NIST 800-53	**CSF 2.0**
Access Control (AC)	
AC-04 Information Flow Enforcement • A Security Information and Event Management (SIEM) system must be configured to log the flow of information from information assets with internal and external systems, including East and West Traffic.	DE.CM
AC-07 Unsuccessful Logon Attempts • IAM (Identity & Access Management) Logs must be collected to analyze unsuccessful logon attempts. • Limits on invalid login attempts must be enforced by automatically locking accounts or nodes when the maximum number of unsuccessful attempts is exceeded in accordance with organization defined limits.	PR.AA
AC-17 Remote Access • IAM Logs must be collected to analyze remote access.	PR.AA
AC-18 Wireless Access • Wireless network traffic must be collected to analyze anomalous activity.	PR.AA
Audit and Accountability (AU)	
AU-02 Event Logging • All logs are aggregated and correlated in a SIEM • All Priority 1 and Priority 2 log types are collected and analyzed. • Meaningful analytic rules are defined and created, which align with MITRE ATT&CK framework and, at a minimum, cover detection categories of Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense, Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control,	PR.PS

Exfiltration, and Impact with a target of 60% coverage of subcategories.	
AU-03 Content of Audit Records • Audit records must include logs from Priority 1 and Priority 2 log types.	PR.PS
AU-04 Audit Log Storage Capacity • Logs must have 6 months of retention.	DE.CM
AU-05 Response to Audit Processing Failures • Audit process failures must be collected and analyzed from Priority 1 and Priority 2 log types.	DE.CM
AU-07 Audit Reduction and Report Generation • Must have the capability to manipulate collected audit log information and organize and/or generate summary capabilities for meaningful analysis.	PR.PS RS.AN
AU-08 Time Stamps • Logs must have time stamps following requirements in SIMM 5300-A, State Defined Security Parameters.	DE.CM
AU-12 Audit Generation • SIEM must be able to produce a system-wide audit trail composed of audit records in a standardized format.	DE.CM
Assessment Authorization and Monitoring (CA)	
CA-07 Continuous Monitoring • Anomalous behavior is tracked in an Incident Management or Governance, Risk Management, and Compliance (GRC) system. • Staff and/or Automation must continuously monitor for anomalies 24x7x365, including holidays. • Notification is required 24x7x365, including holidays and customer notification when detected events require attention.	DE.CM ID.RA ID.IM DA.AE

• Adequate coverage of day, swing, and graveyard shifts, including weekends and holidays.	
Identification and Authentication (IA)	
IA-02 Identification and Authentication (Organizational Users) • IAM Logs are required to detect anomalous behavior	PR.AA
IA-03 Device Identification and Authentication • IAM Logs are required to detect anomalous behavior	PR.AA
IA-08 Identification and Authentication (Non-Organizational Users) • IAM Logs are required to detect anomalous behavior	PR.AA
Incident Response (IR)	
IR-05 Incident Monitoring • Sensors, agents, and security monitoring software are placed at strategic locations throughout the network. • Security event notification (SEN) response timeframes and escalation protocols, outlined in SIMM 5335-A, are adopted for security event notifications and response upon discovering anomalous behavior triggers within the organization of the implemented analytical rules. • Upon discovering anomalous behavior, events shall be timely documented in a separate Incident Management or Governance, Risk Management, and Compliance (GRC) system and assigned a criticality level outlined in SIMM 5335-A. Correlated timeframes in SIMM 5335-A are immediately activated thereafter. Entities must report a True/False Positive incident into Cal-CISRS in compliance with SIMM 5340-A, Incident Reporting and Response.	DE.AE RS.MA
IR-06 Incident Reporting • Anomalous events must be analyzed, confirmed as incidents, and submitted to Cal-CSIRS compliant to SIMM 5340-A upon immediate discovery.	RS.CO RS.MA RS.AN

• Entity must be able to produce evidence which shows that network level alerts are tied to the entity's incident management system.	
IR-07 Incident Response Assistance • Documented process and procedures for requesting assistance from CDT and the California Cybersecurity Integration Center (Cal-CSIC) which include partnering with Cal-CSIC to share confirmed incident metadata.	RS.CO RS.MA
IR-08 Incident Response Plan • Documented process and procedures for Identification, Remediation, and Incident Response	ID.IM DA.AE RS.MA RS.AN RC.RP
Planning (PL)	
PL-07 Concept of Operations • Must have a Concept of Operations (CONOPS) for continuous monitoring describing their choice of system and how they intend to operate the system from the perspective of information security and privacy.	GV.OV
PL-08 Security and Privacy Architectures • Entity has a documented network defense architecture and network diagram depicting network security technologies in the entity. •	DE.CM
Program Management (PM)	
PM-09 Risk Management Strategy • Continuous Monitoring and Event Management is to be integrated into the risk management strategy (e.g. searching for risky users and endpoints)	GV.OC GV.RM GV.OV GV.SC ID.RA

	PR.IR DA.AE RC.RP
PM-14 Testing, Training, and Monitoring • Must ensure training is available for analysts to know how to identify, monitor, and analyze security events.	PR.AT
PM-31 Continuous Monitoring Strategy • Develop an organization-wide continuous monitoring strategy and implement continuous monitoring program with established organization-wide metrics, organization-defined effectiveness, correlation and analysis of information generated, and response and reporting actions. • All systems are baselined using NIST SP 800-53B and SIMM 5300-A controls.	GV.OV GV.SC ID.IM
Risk Assessment (RA)	
RA-03 Risk Assessment • Review collection of logs and event correlation tied to critical systems and/or sensitive data to make risk-based decisions, prioritizations and threat hunting activities.	ID.IM GV.SC ID.RA
RA-05 Vulnerability Monitoring and Scanning • Must employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process.	ID.IM GV.SC ID.RA
RA-10 Threat Hunting • Must have the capability to threat hunt indicators of compromises provided by trusted third-party authorities.	DE.AE

System and Communications Protection (SC)	
SC-07 Boundary Protection • Monitor communications at the external managed interfaces to the system and at key internal managed interfaces for, but not limited to, gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels	DE.CM
System and Information Integrity (SI)	
SI-04 Information System Monitoring • Monitor to detect attacks and indicators of potential attacks, including unauthorized local, network, and remote connections. • Monitor to detect incident types as defined in SIMM 5340-A. • Document procedures for how firewalls and intrusion detection/prevention systems (IDS/IPS) are used in the environment. These procedures include how the devices are tuned for the environment.	ID.RA ID.IM PR.DS DE.AE DE.CM
SI-05 Security Alerts, Advisories, and Directives • Must ingest a minimum of three different types of threat-intelligence feeds, including CDT, Cal-CSIC, and MS-ISAC. • Must be able to send and export logs to CDT and Cal-CSIC.	ID.RA

SIMM 5335-A Security Event Notification and Response Standard

Continuous monitoring and the resulting critical notification processes require a timely exchange for the benefit of all involved parties. SIMM 5335-A, Security Event Notification and Response Standard, establishes definitions of security events and incidents and classifies security events according to how fast an entity needs to respond

after receiving notification. It also establishes the format of notifications and their distribution protocols, timelines for responding to security event notifications, and escalation protocols and timelines.

Log Value Prioritization

Log value prioritization ensures that state entities focus on the most critical and actionable log data to enhance security, compliance, and operational effectiveness. The table below categorizes log sources by priority level based on their relevance to risk management, regulatory requirements, and business objectives.

Log Type	Telemetry	Priority
IAM (Identity & Access Management)	• Single Sign On • MFA • Host-based Collection (e.g. Windows Servers)	Priority 1 Logs
Security Controls	• IDS • IPS • Email Quarantine • Endpoint Detection Response (Anti-Virus, Anti-Malware) • Data Loss Prevention • VPN • Firewalls	
Network Infrastructure	• Routers • Switches	Priority 2 Logs

	• Domain Controllers • Wireless Access Points • Application Servers • Databases • Intranet Applications	
Non-Log Infrastructure Information	• Configuration • Locations • Owners • Network Maps • Vulnerability Reports • Software Inventory	Priority 3 Logs
Non-Log Business Information	• Business Process Mapping • Points of Contact • Partner Information	

References

- MITRE ATT&CK Framework https://attack.mitre.org/
- NIST Cybersecurity Framework 2.0: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- NIST SP 800-53B Control Baselines for Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

- NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf
- SAM 5335 Information Security Monitoring: https://www.dgs.ca.gov/en/Resources/SAM/TOC/5300/5335
- Statewide Information Management Manual (SIMM) Section 5300: https://cdt.ca.gov/policy/simm/#5300

Questions

Questions regarding this standard may be sent to:

California Department of Technology

Office of Information Security

Security@state.ca.gov