Commonwealth of Virginia

Enterprise Technical Architecture [ETA]

Event Log Management

vita.virginia.gov

January 25, 2024

Revision History

Event Log Management: Version History		
Revision	**Date**	**Description**
1.0	04/22/2022	Original. This document was adapted from Federal Executive Order 14028, *Improving the Nation's Cybersecurity* and the resulting OMB memorandum, *M-21-31 Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*.
1.1	05/27/2022	Adjusted per feedback from public comment.
1.2	06/15/2022	Adjusted per feedback from legal on log retention, and for coping log collection of SaaS solutions.
1.3	11/01/2022	Updated to address implementation schedule.
1.4	12/15/2022	Administrative edit to clarify ELM-25.
1.5	12/20/2022	Administrative edit to update Appendix B to amend the schema documentation requirement to add positions for Agency, Application, and Log Name.
1.6	1/25/2024	Administrative edit amend ELM-03 that removes the binding to Appendix A.

Review Process

This standards document was posted on VITA's Online Review and Comment application (ORCA). All agencies, stakeholders, and the public were encouraged to provide their comments through ORCA. All comments were evaluated, and individual commenters were notified of action(s) taken.

Requirements & Exceptions

The requirements included within this document are mandatory. Agencies and suppliers deviating from these requirements must request an exception for each desired deviation, and receive an approved *Enterprise Architecture Exception* via Archer, prior to developing, procuring, or deploying such technology, or not complying with a requirement specified in this document. The instructions for completing and submitting an exception request are contained within the *Commonwealth Enterprise Architecture Policy*.

Contents

Scope

This standard is applicable to all Executive Branch state agencies (hereinafter collectively referred to as "agencies") that are responsible for the management, development, purchase and use of information technology resources in the Commonwealth of Virginia. This standard does not apply to research projects, research initiatives, or instructional programs at public institutions of higher education

These requirements address logging, log retention, and log management, with a focus on ensuring centralized access and visibility for the highest-level enterprise Security Operations Center (SOC) of each agency. In addition, it establishes requirements for agencies to increase the sharing of such information, as needed and appropriate, to accelerate incident response efforts and to enable more effective defense of Commonwealth of Virginia (COV) information and executive branch departments and agencies.

Authority

- Code of Virginia, §2.2-2007. Powers of the CIO
- Code of Virginia, §2.2-2007.1. Additional duties of the CIO relating to information technology planning and budgeting
- Code of Virginia, §2.2-2009(A). Additional duties of the CIO relating to security of government information
- Code of Virginia, §2.2-2012(A). Additional powers and duties related to the procurement of information technology

General Provisions

Commonwealth Security Information & Event Management (COV SIEM)

ELM-01 COV shall implement a central SIEM platform for ingesting event logs from agency and supplier applications, capable of analyzing collected logs with User Behavior Analytics (UBA) and Security, Orchestration, Automation, and Response (SOAR) workflows.

ELM-02 The COV SIEM shall supply an Enterprise Log Manager (ELM) for the central aggregation of event logs for use by agencies and suppliers.

ELM-03 Event logs from all executive branch agencies and their suppliers for all criticality levels shall be configured and stored locally.

ELM-04 COV shall control the event logs that are forwarded to the COV SIEM for ingestion.

ELM-05 Agencies shall be able to view and search their log data in the COV SIEM, both real-time and historical.

ELM-06 Agencies shall be able to implement the UBA and SOAR capabilities available in the COV SIEM.

ELM-07 Logs ingested by the COV SIEM shall be multitenant, segregated by agency or supplier, so that each submitter only has access to their own logs.

ELM-08 Logs ingested by the COV SIEM across all agencies and suppliers shall be available to CSRM for forensic analysis.

ELM-09 The record copy of event logs are maintained by the originating agency; retention and disposition of event logs is the responsibility of the originating agency.

Commonwealth Security & Risk Management (CSRM)

ELM-10 CSRM shall assist and advise agencies in their assessment of logging capabilities.

ELM-11 CSRM shall define the set of tools to assist agencies in facilitating their assessment of logging maturity across the organization, and to develop automated hunt and incident response playbooks.

ELM-12 CSRM shall develop and publish guidance for documenting log schemas (see Appendix B).

ELM-13 CSRM shall create and maintain an implementation schedule for the adoption of the requirements identified in this standard

Agencies & Suppliers

ELM-14 Agencies and suppliers shall use the following event log tiers to characterize event logs used in any of the agency's event log categories, and for reporting and analysis.

Tier	Rating	Description
EL0	Not Effective	Logging requirements for Criticality 0 are either not met or are only partially met
EL1	Basic	Only logging requirements for Criticality 0 are met
EL2	Intermediate	Logging requirements for Criticalities 1 & 2 are met
EL3	Advanced	Logging requirements for all Criticalities are met

ELM-15 Agencies and suppliers shall implement EL3 logging maturity.

ELM-16 Agencies and suppliers shall assess the maturity of their event log management against the maturity model in this policy and identify resourcing and implementation gaps associated with completing each of the requirements within this document.

ELM-17 Agencies and suppliers shall employ the following event log categories for any event log communications including when managing event logs:

- Anti-Virus and Behavior-Based Malware Protection
- Application Level
- Authentication and Authorization
- COV Cloud Environments[1]
- Container
- Data Loss Prevention
- Database Level
- Email Filtering, Spam, and Phishing
- Identity & Credential Management
- Mainframes[2]
- Network Device Infrastructure
- Network Traffic
- Operating Systems
- PKI Infrastructure
- Smart Devices

[1] COV Cloud Environments means infrastructure stood up by COV within a cloud provider. ECOS (SaaS) applications fall under ECOS Oversight and the Vendors are contractually liable to perform continuous monitoring, with regular reviews meeting SEC-525, and provide monthly reporting through ECOS Oversight Services. ECOS vendor logs are available to COV upon request per contract.
[2] Mainframe logs stored in a binary format may require 3rd party software to be human readable

- System Configuration and Performance
- Virtualization System
- Vulnerability Assessment

ELM-18 Agencies and suppliers shall share log information with other COV agencies to address cybersecurity risks, vulnerabilities, investigations, and incidents when directed by CSRM.

ELM-19 All agencies shall adhere to the published implementation schedule for the adoption of the requirements identified in this standard.

Event Log 1 (EL1) Provisions

Agencies and suppliers shall comply with the following requirements to meet the EL1 maturity level. EL1 maturity is required to meet EL3 maturity.

ELM-20 Agencies and suppliers shall ensure that Required Logs categorized as Criticality Level 0 are retained in acceptable formats for specified timeframes, per technical details described in Appendix A.

ELM-21 Agencies and suppliers shall ensure, at a minimum, that each event log contains the following data, if applicable:

- Properly formatted and accurate timestamp (see ELM-19)
- Status code for the event type
- Device identifier (MAC address5 or other unique identifier)[3]
- Session / Transaction ID
- Autonomous System Number
- Source IP (IPv4)
- Source IP (IPv6)
- Destination IP (IPv4)
- Destination IP (IPv6)
- Status Code
- Response Time
- Additional headers (i.e., HTTP headers)
- Where appropriate, the username and/or userID shall be included
- Where appropriate, the command executed shall be included
- Where possible, all data shall be formatted as key-value-pairs allowing for easy extraction
- Where possible, a unique event identifier shall be included for event correlation; a unique event identifier shall be defined per event type
    - Software developed by agencies or by contractors on behalf of agencies must log unique event identifiers for each event in accordance with these requirements

ELM-22 Agencies and suppliers shall employ consistent timestamp formats across all event logs are necessary for accurate and efficient event correlation and log analysis. Timestamps shall be applied consistently to logs from all computing devices, routers, switches, and servers. Agencies shall maintain log timestamps in a format that meets the following requirements, based on both ISO 7 8601 and RFC 3339: Date and Time on the Internet:

[3] Agencies and suppliers should configure all hosts to have MAC randomization turned off; where possible, this configuration shall be maintained automatically.

- YYYY-MM-DDThh:mm:ss.mmmZ (Zulu time, UTC+0) and YYYY-MM-DDThh:mm:ss.mmm+04:00 (UTC+4)
  - YYYY = four-digit year
  - MM = two-digit month
  - DD = two-digit day of the month
  - T = a set character indicating the start of the time element
  - hh = two digits of an hour (00 through 23)
  - mm = two digits of a minute
  - ss = two digits of a second
  - mmm = three digits of a millisecond (000 through 999)
  - +|-= time zone designator (Z or +hh:mm or -hh:mm), the + or – values indicate how far ahead or behind a time zone is from the UTC (Coordinated Universal Time) zone

ELM-23 Agencies and suppliers shall ensure that their event logs do not capture sensitive data, such as Protected Health Information (PHI), Personally Identifying Information (PII), or financial information such as payment cards or accounts.

ELM-24 Software developed by agencies or by contractors on behalf of agencies shall log timestamps for each event in accordance with the timestamp requirements. If the software does not produce data in this format, COV agencies and suppliers shall transform records to conform to these standards before the data is ingested into the SIEM or stored in bulk storage.

ELM-25 Agencies and suppliers shall use the GPS master station clock at QTS Richmond as a baseline reference for timestamps used for logs and systems producing logs:

- ntp1.cov.virginia.gov
- ntp2.cov.virginia.gov

If GPS reference is not possible, agencies shall use the NIST Authenticated NTP Service.

ELM-26 Agencies and suppliers shall forward all required logging data, in near real-time and on an automated basis, to the COV SIEM.

- Data shall be encrypted in transit between its source and destination
- Agencies and suppliers shall ensure the original log can be replayed for future use per the retention period specified in Appendix A

ELM-27 Agencies shall protect and monitor the integrity of their logs and systems producing logs by:

- Verifying that event logging is enabled and active for system components.
  - Traps shall be put in place to monitor these data streams for disruption
  - These traps shall be monitored, and when triggered, the disruption shall be escalated and reported
- Ensuring that only individuals who have a job-related need can view, access, or modify log files.
- Documenting views and usage of log files and reviewing/auditing the resulting records every 30 days.
- Confirming that current log files are protected from unauthorized modifications via access control mechanisms, such as virtual or physical segregation.

- Ensuring that current log files are backed up to an authorized source every 24 hours, such as a centralized log server or write-once media. Using integrity-verification mechanisms to detect unauthorized changes to event logging configuration and log files that are no longer being written to or are considered closed.
- Conducting integrity checks every 30 days and upon access against the log hashes throughout their retention period.
- When logging stops unexpectedly, audit alerts shall be sent in near real-time to any parties responsible for monitoring. The responsible party shall investigate the cause of the disruption and take appropriate corrective actions and shall escalate and report disruptions.
- Monitoring across the enterprise for unexpected changes to files or configuration items, including changes to:
  - Credentials
  - Privileges and security settings
  - Content
  - Core attributes and size
  - Hash values
  - Configuration values

ELM-28 Traps for detecting data-stream disruption shall be monitored by the component-level SOC. The DNS logging system and accompanying analytics shall be monitored and triaged by the component-level SOC, who shall escalate and report disruptions.

ELM-29 Agencies and suppliers shall implement a Domain Name System (DNS) logging system that meet the requirements identified in Appendix A, including DNS requests made over encrypted DNS connections.

- Agencies and suppliers shall implement accompanying analytics that allow for rapid identification of the host that sourced each DNS query. This capability shall be monitored and triaged, and disruptions shall be escalated and reported.
- Agencies and suppliers shall automate the production of a list of hostnames that are frequently accessed or looked up by legitimate users within their agency but are not included in general top domain lists identified by CSRM or available publicly or via subscription.
- Agencies should make that list automatically accessible to CSRM or submit it to CSRM daily via a COV-accepted automated mechanism.

ELM-30 Agencies at EL1 stage shall start planning on how to best implement SOAR capabilities in their environment and develop automated hunt and incident response playbooks.

ELM-31 Agencies and suppliers at EL1 stage shall start planning on how to best implement a UBA capability in their environment, leveraging the logging requirements, in order identify potentially malicious or malicious activity.

Event Log 2 (EL2) Provisions

Agencies shall comply with the following requirements to meet the EL2 maturity level. EL2 maturity is required to meet EL3 maturity.

ELM-32 Agencies and suppliers shall meet all EL1 requirements.

ELM-33 Agencies and suppliers shall retain Required Logs categorized as Criticality Level 1 and 2 in acceptable formats for specified timeframes, per technical details described in Appendix A.

ELM-34 For all software developed by or on behalf of COV agencies that produces logs and is deployed in COV environments, agencies shall provide a document detailing the structure (schema) for those logs to CSRM.

- Agencies and suppliers shall refer to CSRM guidance when developing this documented schema (see Appendix B)
- Agencies shall also provide all updates to the schema to CSRM no later than one business day after finalization
- Schema and associated documentation shall be published to the Virginia Open Data Portal

ELM-35 Agencies and suppliers shall retain and store in cleartext form the data or metadata from Appendix A that is collected in their environment.

- If agencies or suppliers perform full traffic inspection through active proxies, they should log additional available fields as described in Appendix A and can work with CSRM to implement these capabilities.
- If agencies and suppliers do not perform full traffic inspection, they shall log the metadata available to them.
- In general, agencies and suppliers are expected to follow zero-trust principles concerning least privilege and reduced attack surface, and relevant guidance from CSRM relating to Zero-Trust Architecture.
- Data or metadata acquired shall be available to CSRM within one business day.

ELM-36 Required Logs categorized as Criticality Levels 0 and 1 shall be accessible and visible for the highest-level security operations by the head of each agency. Required Logs categorized as Criticality Levels 2 are retained, at a minimum, at the component level.

- Traps for detecting data-stream disruption should be monitored by the component-level and top-level enterprise SOCs, who shall escalate and report disruptions
- The DNS logging system and accompanying analytics shall be monitored and triaged by the component-level and top-level enterprise SOCs, who shall escalate and report disruptions
- The enterprise SOC shall ensure that cross-organizational analytics are established for use across agency components

Event Log 3 (EL3) Provisions

Agencies shall comply with the following requirements to meet the EL3 maturity level.

ELM-37 Agencies and suppliers shall meet all EL2 requirements.

ELM-38 Agencies and suppliers shall retain Required Logs categorized as Criticality Level 3 in acceptable formats for specified timeframes, per technical details described in Appendix A.

ELM-39 Agencies and suppliers shall finalize and implement automated hunt and incident response playbooks that include SOAR capabilities. Agencies shall also provide any updates to the playbooks and automation integrations to CSRM no later than one business day after they are finalized.

ELM-40 Agencies and suppliers shall have real-time access to automated hunt and incident response playbooks, and to view incidents in progress.

ELM-41 Agencies and suppliers shall implement UBA in order to allow for early detection of malicious behavior. This shall monitor all user and non-user accounts. This capability shall be monitored and triaged by component-and top-level agency SOCs, who shall escalate and report disruptions. At a minimum, User Behavior Monitoring should be configured to detect and alert on:

- Compromised user credentials
- Privileged-user compromise
- Unauthorized Access to systems or data
- Compromised system/host/device
- Lateral movement of threat actor
- Deviations from behavior baseline

ELM-42 Agencies and suppliers shall have access to view and query user behavior analytics, both real-time and historical.

ELM-43 Agencies and suppliers shall integrate their container security and monitoring tools with the COV SIEM to ensure container-related events are captured by the enterprise. Alternatively, in cases where the uses and privileges of containers are appropriately constrained by the orchestration layer, agencies may rely on SIEM tools present at that layer. In general, COV agencies shall ensure that their threat hunt and incident response teams have appropriate tools and training to identify incidents within a containerized environment.[4]

ELM-44 Agencies and suppliers shall ensure that Required Logs across all Criticality levels shall be accessible to the highest-level security operations by the head of each agency.

Compliance & Implementation

Understanding that the initial implementation of this logging standard will require a specific level-of-effort for agencies and suppliers to meet compliance, the following outline for tiered implementation is described.

ELM-45 COV agencies and suppliers shall undertake and deliver the following

- Assess logging capabilities against the model and identify resourcing and implementation gaps associated with completing each of the requirements
- Create plans for achieving EL3 maturity for all applications
- Document logs by application
- Document application logging schemas
- Publish documentation to the Virginia Open Data Portal

ELM-46 Agencies and suppliers shall maintain event log documentation as new solutions are consumed, old ones discarded, and existing ones modified.

ELM-47 Agencies and suppliers shall incorporate their intentions for achieving EL3 maturity for each application into their Information Technology Strategic Plans (ITSPs).

[4] NIST SP 800-191, Application Container Security Guide

ELM-48 All projects, procurements, and developed solutions initiated after the issuance of these requirements must meet EL3 maturity at the time of their implementation into the environment.

Definitions

As appropriate, terms and definitions used in this document are included in the COV ITRM IT Glossary.

Active storage	Refers to data that is stored in a manner that facilitates frequent use and ease of access.
Application monitoring dashboard	A system that provides information about the metrics, usage, and performance of an application. Agencies should use a dashboard suited to the version, type, and deployment method of each application.
Attachment	A file sent via email.
Behavior Monitoring	The analysis of electronic usage patterns such as destinations, frequency/periodicity of identified risk incidents, and/or volumes exchanged, which indicate whether the behavior exceeds a specified baseline and represents a threat.
Cold data storage	Refers to the storage of data in a manner that minimizes costs while still allowing some level of access and use.
Config	A configuration file used by various applications. It contains plain-text parameters that define settings or preferences for building or running a program.
Criticality	Each log category has an assigned criticality level based on its relative cybersecurity value. This cybersecurity value relates to the usefulness of the log data for threat detection, with the data of the highest value assigned a criticality of zero, and the lowest a criticality of 3.
Database Query	A request to access data from a database. Capturing the query allows for playback so that Hunt and IR teams can identify what data was exfiltrated or inserted.
Database Record	A set of database fields.
Enterprise Application	Applications that are owned by a COV service supplier or agency that are provided for use to other agencies or service suppliers, or which support shared business functions or processes. Examples • Cardinal • eVA • Archer • ServiceNow
Enterprise Mobility Management (EMM)	A set of technology, processes, and policies to secure and manage the use of corporate and employee-owned mobile devices within an organization.

Event Log Forwarding	A service that allows network administrators to forward events from multiple servers and collect them in one location.
File	A resource for recording data in a storage device.
International Mobile Equipment Identity (IMEI)	A number, usually unique, to identify 3GPP and iDEN mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone but can also be displayed on-screen on most phones by entering *#06# MMI Supplementary Service code on the dialpad, or alongside other system information in the settings menu on smartphone operating systems.
International Mobile Subscriber Identity (IMSI)	A number that uniquely identifies every user of a cellular network. It is stored as a 64-bit field and is sent by the mobile device to the network. It is also used for acquiring other details of the mobile in the home location register (HLR) or as locally copied in the visitor location register.
Log	A file that contains data about an event that occurred in an application or operating system.
Log Category	A classification of available event logs.
Mobile Device Management (MDM)	Software that allows IT administrators to control, secure and enforce policies on smart devices.
Mobile Threat Defense (MTD)	Dynamic protection against cyber threats targeted against smart devices.
Near Real-Time (NRT)	Refers to the time delay introduced by automated data processing or network transmission between the occurrence of an event and the use of the processed data, such as for display or feedback and control purposes. Also known as Nearly Real-Time.
Packet Capture (PCAP)	Results from the interception and copying of a data packet that is crossing or moving over a specific computer network.
Required Log	An event log containing data considered essential to the analysis and resolution of a cybersecurity incident, sourced from one of the following log types: • Perimeter device logs • Operating system event logs • Endpoint logs • Application logs • Proxy logs • IoT logs
Security, Orchestration, Automation, and Response (SOAR)	A stack of capabilities that enable an organization to collect data about security threats and respond to security events without human assistance. The goal of using a SOAR platform is to improve the efficiency of physical and digital security operations through security orchestration, security automation, and security

	response. Security orchestration connects and integrates with monitoring tools in the environment, such as vulnerability scanners, endpoint protection products, end-user behavior analytics, firewalls, intrusion detection and intrusion prevention systems (IDSes/IPSes), and external threat intelligence feeds. Security automation consumes the data from the orchestrated systems to automatically conduct vulnerability scanning and log analysis. Security response is a set of actions that are carried out once a threat is detected based on an incident playbook.
Script	A configuration file that lets users run or execute certain actions.
Security Information & Event Management (SIEM)	A software solution that aggregates and analyzes activity from disparate data sources from across an IT infrastructure. It provides real-time analysis of security alerts generated by applications and network hardware.
Simple Network Management Protocol (SNMP)	Exposes network data in the form of variables on the managed systems organized in a management information base (MIB), which describe the system status and configuration. These variables can then be remotely queried by managing applications.
Smart device	An electronic device capable of connecting to a network, or to other devices, via wireless communication protocols such as Bluetooth, Wi-Fi, 4G, or 5G, and which can operate interactively and autonomously to some extent. It includes devices that exhibit some properties of ubiquitous computing, such as artificial intelligence.
Security Operations Center (SOC)	A centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.
User Behavior Analytics (UBA)	A cybersecurity process about detection of insider threats, targeted attacks, and financial fraud that tracks a system's users. UBA looks at patterns of human behavior, and then analyzes them to detect anomalies that indicate potential threats.
Unified Endpoint Management (UEM)	A class of software tools that provide a single management interface for mobile, PC and other devices. It is an evolution of, and replacement for, mobile device management (MDM) and enterprise mobility management (EMM) and client management tools.
Zero Trust Architecture	A security framework requiring all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.

References

- Executive Order 14028, Improving the Nation's Cybersecurity
- M-21-31 Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

Appendix A – Log Category Definitions

The set of event logs of interest to COV are separated into log categories that distinguish the different types, which are further characterized by Criticality. They are ranked in order of usefulness, where the most useful data is assigned a criticality of zero, and the least a criticality of 3.

Criticality 0

Log Category	Category Target	Required Data	Format	Retention Period
COV Cloud Environments	General Events	Nearly all successful attacks on cloud services result from customer misconfigurations. With that in mind, the logging and monitoring focus should be on: • Any Activity on Breakglass Account(s) • Conditional Access Policy Changes • Changes to Environment Policies (e.g., Azure Subscription, AWS Services, Google Solutions, etc.) in Management Logs • Privileged Role Changes • Virtual Network (VNet) Changes • Deletions of Delete Locks • Changes to Logging Policies • Privileged Identity Management (PIM) and Identity Protection Changes • Changes to Alert Rules (Audit the Auditor) • Key Vault/Key Management Changes • Storage File Access Logs, File, File Hashes • Baseline Deviations for Prod App Tiers • Baseline Deviations for Prod Data Tiers	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
COV Cloud Environments	General Logging	• IDS / IPS / NTA / NDR / SIEM Logs • API Activity Logs • Authentication Logs • Firewall Logs • Web Proxy/WAF Logs • Service Metrics • Billing Data • Flow Logs • Remote Access/VPN Logs • System/OS Logs • DLP Logs • DNS Query/Response Logs	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage • 72 Hours Packet Capture

Log Category	Category Target	Required Data	Format	Retention Period
COV Cloud Environments	AWS	• AWS Cloudtrail • Amazon Cloudwatch Logs • AWS Config • Amazon S3 Access Logs • Amazon VPC Flow Logs • AWS WAF Logs • AWS Shield • AWS Guardduty • AWS Security Hub	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
COV Cloud Environments	Azure	• Azure Active Directory Logs • Activity Logs • Active • Unified Audit Logs (w/Advanced Audit Features)	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
COV Cloud Environments	GCP	• Access Transparency Audit Log • Admin Audit Log • Data Studio Audit Log • Drive Audit Log • Email Audit Log • Groups Audit Log • LDAP Audit Log • Login Audit Log • Devices Audit Log • Sail Audit Log • Token Audit Log • User Accounts Audit Log • OAuth Token Audit Log • Security Reports • sage Logs • Storage Logs • Data Access Logs For Organizational and Default Configuration Settings Enable: • Admin Read • Data Read • Data Write	• Log	• 6 Months Active Storage • 18 Months Cold Data Storage
COV Cloud Environments	OCI	• Audit logs • Service logs	• Log	• 6 Months Active Storage

Log Category	Category Target	Required Data	Format	Retention Period
		• Custom logs		• 18 Months Cold Data Storage
Email Filtering, Spam, and Phishing	NA	• IP and Domain Reputation (As Indicated by Mail Server Connection)	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage

Identity & Credential Management	NA	• Account Creation
		• Manage Credential Type
		  ○ (PIV or CAC) and Derived Credentials
		  ○ Cert
		  ○ MFA
		  ○ Password
		• Establish/Manage Attributes
		  ○ Organization
		  ○ Groups/Roles
		• Manage/Track Changes in Attributes & Credentials
		• Track Usage of Credentials
		• Account Deletion
			• Log
			• Script
				• 12 Months Active Storage
				• 18 Months Cold Data Storage

Identity & Credential Management	Privileged Identity	• Provisioning
		• Manage Credential Type
		  ○ (PIV or CAC) and Derived Credentials
		  ○ Cert
		  ○ MFA
		  ○ Password
		• Establish/Manage Attributes
		  ○ Organization
		  ○ Groups/Roles
		• Manage/Track Changes in Attributes & Credentials
		• Track Usage of Credentials
		• Deprovisioning
		• Establish and Manage Privileges (Privilege Credentials)
		• Isolate, Monitor, Record, Audit Privilege Sessions
		• Control Privileged Actions
		  ○ Commands
		  ○ Tasks
		• Track Privilege Escalation and Delegation
		• Monitor, Alert and Respond to Anomalous Behaviors/Activities
			• Log
			• Script
				• 12 Months Active Storage
				• 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
Network Device Infrastructure	For Devices with Multiple Interfaces: Interface MAC -If Correlated to the De-NAT IP Address	DHCP Lease Information, Including: • MAC • IP	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
Network Device Infrastructure	DNS -Source IP and Port, Destination IP and Port Date and Time	• Content of Query, Response, and Errors – All Record Types • Zone Transfers Request and Response (Audit Log) • Zone Transfers Request and Response (Content)	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
Network Device Infrastructure	Passive DNS Log	• Tuple (Rrname, Rrtype, Rdata) • Time_First • Time_Last • Count • Bailiwick • Sensor_Id • Zone_Time_First • Zone_Time_Last • Time_First_Ms • Time_Last_Ms • Origin • Count of Questions Asked by Source IP • Count of Questions Asked Overall • Count of Responses by Source IP • Query Size in Bytes • Response Size in Bytes • TTL per Record Returned • Request Was Made Via UDP, TCP or Both • Response Was Made Via UDP, TCP or Both • Passive DNS Source (Used to Identify Which Passive DNS Source Data Came From)	• Log • Database Record	• 12 Months Active Storage • 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
Network Device Infrastructure	DNS, DHCP, and Wi-Fi	• Wi-Fi Supporting Infrastructure Logs Including Security Logs at Info Level • Device Authentication Logs with User Agent • URL Browsing Logs + HTTP Methods (e.g., Post, Get, etc.) • User Authentication Logs • DHCP Lease Information Including MAC, IP • Roaming Logs • Timestamps	• Log • SNMP	• 12 Months Active Storage • 18 Months Cold Data Storage

Network Device Infrastructure	DNS, DHCP, and Wi-Fi	• Static Network Address Translation Table Mapping as Well as Port Forwards
		  ○ Date and Time
		  ○ Protocol
		  ○ Port
		  ○ Inside Local and Global IP and Port
		• Outside Local and Global IP and Port
			• Log
			• Database Record
			• Script
			• File
			• Config
			• SNMP
				• 12 Months Active Storage
				• 18 Months Cold Data Storage

Network Device Infrastructure	General Logging	• IDS / IPS / NTA / NDR / SIEM Logs • API Activity Logs • Authentication Logs • Firewall Logs • Web Proxy/WAF Logs • Service Metrics • Network Flow Logs • Remote Access/VPN Logs • System/OS Logs • DLP Logs • DNS Query/Response Logs	• Log • File • Packet Capture	• 12 Months Active Storage • 18 Months Cold Data Storage • 72 Hours Packet Capture
Network Device Infrastructure	Routers and Switches (For Devices with Multiple Interfaces: Interface MAC -If Correlated to the De-NAT IP Address)	• Routing Tables • Routing Changes (Logging All CLI Commands, BGP) • IP Addressing Schema and Implementation	• Script • File • Config	• 12 Months Active Storage • 18 Months Cold Data Storage
Network Device Infrastructure	Load Balancer / Reverse Proxy	Access Logs • Connection Type • Date and Time • Resource ID of the Load Balancer • Client IP:Port • Target IP:Port	• Script • File • Config	• 12 Months Active Storage • 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
		• Request Processing Time • Target Processing Time • Response Processing Time • Status Code from Load Balancer • Target Status Code • Received Bytes • Bytes Sent • Request • User Agent • SSL Cipher • SSL Protocol • SNI Domain • Matched Rule Priority • Actions Executed • Redirect URL • Error Reason • Target IP:Port List • Target Status Code List • Classification Reason Request Does Not Comply with RFC 7230 • Other Implementation Specific Fields		

Network Device Infrastructure	Proxies and Web Content Filters (For Devices with Multiple Interfaces: Interface MAC -If Correlated to the De-NAT IP Address)	Provides NAT, User, and Gateway IP Address to Provide Enhanced Reporting of Malicious Domains and IP Addresses. In the Case of Web, W3c Format.
		• Date and Time
		• Source
		  ○ Hostname
		  ○ IP Address and Port
		  ○ MAC
		• Destination
		  ○ Hostname
		  ○ IP Address and Port
		  ○ MAC
		• Web URL Methods / User Agent / Decoded Headers
		• URL Categories
		• URL
		• Permitted, Restricted, Denied
			• Log	• 12 Months Active Storage
				• 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
Network Device Infrastructure	Proxies and Web Content Filters	• Policy Updates • Software Updates	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage

Network Device Infrastructure	Access, Authorization, and Accounting	• General Information
		  ○ Date and Time
		  ○ Event, Status, or Error Codes
		  ○ Service/Command/Application Name
		  ○ User or System Account Associated with an Event
		  ○ Device Used (e.g., Source and Destination IPs, Terminal Session ID, Web Browser, etc.)
		• Operating System (OS) Events
		  ○ Start-Up and Shutdown of the System
		  ○ Start-Up and Shutdown of a Service
		  ○ Network Connection Changes or Failures
		  ○ Changes to, or Attempts to Change, System Security Settings and Controls
		• OS Audit Records
		  ○ Log-On Attempts (Success/Failure)
		  ○ The Function(s) Performed after Logging On (e.g., Reading or Updating a Critical File, Software Installation)
		  ○ Account Changes (e.g., Account Creation and Deletion, Account Privilege Assignment) • Successful/Failed Use of Privileged Accounts
		• Application Account Information
		• Application Authentication Attempts (Success/Failure)
		• Application Account Changes (e.g., Account Creation and Deletion, Account Privilege Assignment)
		• Use of Application Privileges
		• Application Operations
		  ○ Application Startup and Shutdown
		  ○ Application Failures
		  ○ Major Application Configuration Changes
		  ○ Application Transactions, For Example,
		  ▪ Email Servers Recording the Sender, Recipients, Subject Name, and Attachment Names for Each Email
		  ▪ Web Servers Recording Each URL Requested and the Type of Response Provided by the Server
			• Log	• 12 Months Active Storage
				• 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
		• Business Applications Recording Which Financial Records Were Accessed by Each User		

Operating Systems	Windows Infrastructure and Operating Systems	• User and Administrator Access to OS Components and Applications
		  ○ File and Object Access
		  ○ Audit Log Access (Success/Failure)
		  ○ System Access and Log Off (Success/Failure)
		  ○ Privilege Access and Log Off (Success/Failure)
		  ○ RDP Access and Log Off (Success/Failure)
		  ○ SMB Access
		  ○ Installation or Removal of Storage Volumes or Removeable Media
		• System Performance and Operational Characteristics
		  ○ Resource Utilization, Process Status
		  ○ System Events
		  ○ Service Status Changes (Start, Stop, Fail, Restart, etc.)
		  ○ Service Failures and Restarts
		  ○ Process Creation and Termination
		• System Configuration
		  ○ Changes to Security Configuration (Success/Failure)
		  ○ Audit Log Cleared
		  ○ Changes to Accounts
		  ○ User or Group Management Changes
		  ○ Scheduled Task Changes
		• File Access
		  ○ Transfer of Data to External Media or Remote Hosts
		• Host Network Communications
		  ○ Listening Network Port and IP Address
		  ○ Active Network Communication with Other Hosts
		• Powershell Execution Commands
		• WMI Events
		• Registry Access
		• Command-Line Interface (CLI)
		• Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware
		  ○ Version
		  ○ Created Date
		  ○ Installed Date
		• Manufacturer
			• Log	• 12 Months Active Storage
				• 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period

Operating Systems	MACOS (Or Other Apple Desktop and Server Operating Systems)	• User and Administrator Access to OS Components and Applications
		  ○ File and Object Access
		  ○ Audit Log Access (Success/Failure)
		  ○ System Access and Log Off (Success/Failure)
		  ○ Privilege Access and Log Off (Success/Failure)
		  ○ Remote Terminal or Equivalent Access and Log Off (Success/Failure)
		  ○ Samba/NFS/(S)FTP or Equivalent Access
		  ○ Installation or Removal of Applications
		  ○ Installation or Removal of Storage Volumes or Removeable Media
		• System Performance and Operational Characteristics
		  ○ Resource Utilization, Process Status
		  ○ System Events
		  ○ Service Status Changes (Start, Stop, Fail, Restart, etc.)
		  ○ Service Failures and Restarts
		  ○ Process Creation and Termination
		• System Configuration
		  ○ Changes to Security Configuration (Success/Failure)
		  ○ Audit Log Cleared
		  ○ Changes to Accounts
		  ○ User or Group Management Changes
		  ○ Scheduled Task Changes
		• File Access
		  ○ Transfer of Data to External Media or Remote Hosts
		• Host Network Communications
		  ○ Listening Network Port and IP Address
		  ○ Active Network Communication with Other Hosts
		• Command-Line Interface (CLI)
		  ○ System Log Folder: /Var/Log/*
		  ○ System Log: /Var/Log/System.Log
		  ○ Mac Analytics Data: /Var/Log/Diagnosticmessages/*
		  ○ Wi-Fi Log: /Var/Log/Wifi.Log
		  ○ System Application Logs: /Library/Logs/* and /Private/Var/Log/*
		  ○ System Reports: /Library/Logs/Diagnosticreports/ *
		  ○ User Application Logs: /Users/Name/Library/Logs/*
			• Log	• 12 Months Active Storage
				• 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
		○ User Reports: /Users/Name/Library/Logs/Diagnosticreports/* ○ Audit Log: /Var/Audit/* • Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware ○ Version ○ Created Date ○ Installed Date • Manufacturer		
Operating Systems	BSD (Linux)	• User and Administrator Access to OS Components and Applications ○ File and Object Access ○ Audit Log Access (Success/Failure) ○ System Access and Log Off (Success/Failure) ○ Privilege Access and Log Off (Success/Failure) ○ Remote Terminal or Equivalent Access and Log Off (Success/Failure) ○ Samba/NFS/(S)FTP or Equivalent Access ○ Installation or Removal of Storage Volumes or Removeable Media • System Performance and Operational Characteristics ○ Resource Utilization, Process Status ○ System Events ○ Service Status Changes (Start, Stop, Fail, Restart, Etc.) ○ Service Failures and Restarts ○ Process Creation and Termination • System Configuration ○ Changes to Security Configuration (Success/Failure) ○ Audit Log Cleared ○ Changes to Accounts ○ User or Group Management Changes ○ Scheduled Task Changes • File Access ○ Transfer of Data to External Media or Remote Hosts • Host Network Communications ○ Listening Network Port and IP Address ○ Active Network Communication with Other Hosts • Command-Line Interface (CLI) • Security Enhanced Linux (SELinux) AppArmor or Equivalent	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
		○ Warning Logs ○ Violation Logs • System ○ /Var/Log/Messages ○ /Var/Log/Dmesg ○ /Var/Log/Syslog ○ /Var/Log/Daemon.Log ○ /Var/Log/Cron ○ /Var/Log/Kern.Log ○ /Var/Log/Boot.Log • Access And Authentication ○ /Var/Log/Auth.Log ○ /Var/Log/Secure ○ /Var/Log/Faillog ○ /Var/Log/Btmp ○ /Var/Log/Wtmp or /Var/Log/Utmp • Applications ○ /Var/Log/Mail.Log or /Var/Log/Maillog ○ /Var/Log/Xorg.X.Log • Package Install/Uninstall ○ /Var/Log/Dpkg.Log ○ /Var/Log/Yum.Log • Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware ○ Version ○ Created Date ○ Installed Date • Manufacturer		

Criticality 1

Log Category	Category Target	Required Data	Format	Retention Period
Anti-Virus and Behavior-Based Malware Protection	NA	• Date and Time Source Hostname ○ IP ○ Port • Destination Hostname ○ IP	• Log • Email Attachments	• 12 Months Active Storage • 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
		○ Port • Description of Malicious Code or Action and Severity • Identity or (Hash) Identifier of the File(s) • Description of the Action Taken (Clean, Quarantine, Delete) • Signature Updates		
Anti-Virus and Behavior-Based Malware Protection	Indication of the Host that Connected to a Specific URL	• Date and Time • IP and Domain Reputation • URL • Categorization	Log	• 12 Months Active Storage • 18 Months Cold Data Storage
Application Level	Web Applications	• URL • Headers • HTTP Methods -Request with Body of Data[5] • HTTP Response with Body of Data	• Log • Log and PCAP of Plaintext HTTP Request and Response with Data	• 12 Months Active Storage • 18 Months Cold Data Storage
Application Level	Web Application	• Database queries • Response codes	Log	• 12 Months Active Storage • 18 Months Cold Data Storage
Application Level	Web Application Crashes	• Processes • Applications	Log	• 12 Months Active Storage • 18 Months Cold Data Storage
Application Level	Web Applications & Middleware	• Configuration • Version	Log	• 12 Months Active Storage • 18 Months Cold Data Storage
Authentication and Authorization	Administrative	• Authentication Logons (Success/Failure) • Authentication Logoffs • Privilege Elevation (Success/Failure) • Security Related System Alerts and Failures • User and Group ○ Additions ○ Deletions	Log	• 12 Months Active Storage • 18 Months Cold Data Storage

[5] Agencies shall evaluate this data to ensure proper protections are in place to encrypt the data at rest and in transit. Agencies shall also ensure that their tools are accredited to handle sensitive data and proper oversight controls are implemented to look for signs of inappropriate data usage

Log Category	Category Target	Required Data	Format	Retention Period
		○ Modification to Permissions • Unauthorized Access Attempts to Critical Systems and File		
Authentication and Authorization	Authorization	All Privileged Operations Including: • "sudo" or runas • Enabling CLI Access • System Administrative Commands • Powershell Execution Commands • Powershell Script Block Logging	Log	• 12 Months Active Storage • 18 Months Cold Data Storage
Container	Supply Chain	• Log Container Image Sources • Log Changes / Deltas Between Image Source Versions • Log Vulnerability Scan of Container Images, even if No Vulnerabilities Are Discovered • Log Where Containers Are Deployed and Which System They Support	• Script • Manual log entry	• 12 Months Active Storage • 18 Months Cold Data Storage
Database Level	NA	• Addition of New Users, Especially Privileged Users • Query Being Executed • Query, Status (Response), and Traceback ○ Method ○ Comments or Variables ○ Multiple Embedded Queries ○ Database Alerts or Failures ○ Time to Execute Query • Attempts to Elevate Privileges (Success/Failure) • Changes to the Database Structure • Changes to User Roles or Database Permissions • Database Administrator Actions • Database Logons (Success/Failure) • Failed Logons • Use of Executable Commands • CLI Commands against the Data Base • Database Configuration and Version • Access to Sensitive Information within the Databases such as Keys, Passwords, Privacy Related Data	• Log • Database Query	• 12 Months Active Storage • 18 Months Cold Data Storage
Email Filtering, Spam, and Phishing	NA	• Content Filtering Policy Updates	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period

Network Device Infrastructure	All Devices	• Hash of the Binary / Binaries Running on the Device
		• Hash of Configs
		• Firmware
		  ○ Version
		  ○ Created Date
		  ○ Installed Date
		• Manufacturer
			• Log	• 12 Months Active Storage
				• 18 Months Cold Data Storage

Network Device Infrastructure	All Devices: IDs / IPs Alerts and Events
	(For Devices with Multiple Interfaces: Interface MAC -if Correlated to the De-NAT IP Address)
		• Date and Time
		• Source
		  ○ Hostname
		  ○ IP Address and Port
		  ○ MAC
		• Destination
		  ○ Hostname
		  ○ IP Address and Port
		  ○ MAC
		• Signature Triggered and Associated Details Including:
		  ○ Signature
		  ○ Anomaly
		• Rate Threshold
		• Device Name
		• Type of Event and Category
		• In the Case of Fortinet Network IPs, Attack Context
		• (Web / Device) User Agent if Available
		• Wi-Fi Channel
		• Wi-Fi Extended Service Set Identifier (ESSID)
			• Log	• 12 Months Active Storage
				• 18 Months Cold Data Storage

Network Device Infrastructure	Firewalls
	(For Devices with Multiple Interfaces: Interface MAC -If Correlated to the De-NAT IP Address)
		• All Events from Firewall. At the very least, if access control lists (ACL) are enabled and the device is filtering traffic:
		  ○ Action Permit, Teardowns, Closes, Denies, and Drops
		  ○ Interface
		• Source
		  ○ Hostname
		  ○ IP Address and Port
		  ○ MAC
		• Destination
		  ○ Hostname
		  ○ IP Address and Port
		  ○ MAC
			• Script
			• File
				• 12 Months Active Storage
				• 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
		○ Protocol Type ○ Rule Name and Number Triggered ○ URL if Applicable, Associated User and User Agent • Date and Time		
Network Device Infrastructure	VPN Gateway – All Events (For Devices with Multiple Interfaces: Interface MAC -If Correlated to the De-NAT IP Address)	At the very least, for Accepts, Teardowns, Closes, Denies, and Drops: • Date and Time • Source ○ Hostname ○ IP Address and Port ○ MAC • Destination ○ Hostname ○ IP Address and Port ○ MAC • Source IP Address and Port, MAC (Inside Tunnel) • Destination IP Address and Port, MAC (Inside Tunnel) • Authentication Information (Success/Fail with Username and Device with User Agent) • Change in Status of Connections / Tunnel Status • VPN Certificate Status Validation	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
PKI Infrastructure	NA	All Events Related to: • Generation • Revocation • Access • Update • Expiry • Recover • Authentication Success • Authentication Fail • LDAP Logs	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
Smart Devices	Agent Logs	• General ○ Date and Time Device Data • Device Name ○ Device Manufacturer and Model ○ Serial # ○ Phone # ○ IMEI, IMSI, OS Version, OS Build	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
		○ Firmware Version ○ Device IP Address, Device Root/Jailbreak Status and Reasons ○ Developer Mode Enabled ○ Battery/Power Information ○ Hardware Info (Processor, Memory, Storage) ○ Last Time Device Synched with Enterprise • Application Data ○ Application Manifest (Installed Apps, App Version, Version History and Installation Timestamps), Installation and Data Storage Location ○ Application Permissions ○ Application Hash (e.g., SHA256) ○ Running Apps and Processes • Device Policy Settings ○ Enrollment Policies ○ Policies Successfully/Unsuccessfully Applied ○ Authentication Policies (Password, Pin, Biometric, etc.) • Device Configuration ○ Certificates end Related Information (Validity Period, Revocation, etc.) ○ Device Encryption Configuration ○ Android Enterprise Settings ○ System Integrity Status • Network Configuration ○ Allowed/Disallowed Networks ○ Currently Connected Network ○ Proxy/Tunnel and Per-App VPN Info ○ Telephony Info (Some of This Is Covered by Carrier Data) ○ Captive Portals ○ Wi-Fi SSID ○ Network MAC Address ○ Bluetooth • Event / Audit / Crash Logs ○ Event Type and ID ○ Event Date/Timestamp ○ Success/Failure of Various Services ○ User Authentication (Success/Failure) ○ Event Actor and ID (e.g., Admin, System, Device)		

Log Category	Category Target	Required Data	Format	Retention Period
		○ Event Change Type (CRUD) • MTD Agent Info ○ Agent Activation Status ○ Threat Detection of Variety of Vulns ○ Phishing Protection Status ○ Tampering of Agent, App, or System ○ Privilege Escalation ○ MITM Activities ○ Remediation Actions Taken ○ Last Time Device Synched with Enterprise		
Smart Devices	Server Logs	EMM (UEM)/MTD Alerts • Date and Time • Alert Type • Failure of Cryptographic Protocols • Failure of Device Cryptographic Capabilities (e.g., Trusted Boot Process) • Certificate Validation Failure (Defined in MDM Server Protection) • Alerts from Agent to Server Defined MDM Agent Protection	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
System Configuration and Performance	Configuration	Scripts or Database Changes Used to Configure Systems, Services on a System, or Applications	• Database Record • Script	• 12 Months Active Storage • 18 Months Cold Data Storage
System Configuration and Performance	Endpoint Detection & Response (EDR)		• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
System Configuration and Performance	Configuration Changes	• Management Action (Success/Failure) • Admin Login (Success/Failure)	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
Virtualization System	NA	• User Authentication ○ Logon (Success and Failure) ○ Attempts to Obtain Privileged Access (Success and Failure) • User and Administrator/Root Access and Actions of Components and Applications to File and Object Access ○ Audit Log Access (Success and Failure)	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
		○ System Access (Failure) • System Performance and Operational Characteristics of Resource Utilization, Process Status ○ System Events ○ Service Status Changes (e.g., Started, Stopped) • System Configuration ○ Changes to Security Configuration (Success/Failure) ○ Changes to Hypervisor o Changes to VMS ○ Changes Made within VMS o Audit Log Cleared • Creation and Deployment of VMS • Migration of VMS (e.g., Source and Target Systems, Time, Authorization) • Creation and Deletion of System-Level Objects		
Vulnerability Assessment	NA	• Date and Time • Hostname, IP Address, and OS • Open Ports • Installed Applications • Version of Installed Applications • Vulnerabilities Listed in Installed Applications • Source of Vulnerability and Severity	• Log[6]	• 12 Months Active Storage • 18 Months Cold Data Storage

Criticality 2

Log Category	Category Target	Required Data	Format	Retention Period
Application Level	Commercial Off the Shelf (COTS) and Custom Applications	• User Authentication (Success/Failure) • User and Administrator Application Use: ○ File and Object Access ○ Audit Log Access (Success/Failure) ○ System Access (Failure) ○ Application Transactions (Web Page Hits, Email Sent/Received, File Transfers Completed) • Transaction Logs • System Performance and Operational Characteristics ○ Resource Utilization ○ Process Status	• Log • Application Monitoring Dashboards	• 12 Months Active Storage • 18 Months Cold Data Storage

[6] Logs are kept for ALL assessments, even if there are 0 vulnerabilities identified during the assessment.

Log Category	Category Target	Required Data	Format	Retention Period
		○ Errors (Input Validation, Dis-Allowed Operations) ○ System Events ○ Service Status Changes (e.g., Started, Stopped) • Application Configuration and Version		
Application Level	General – Non-COTS	• User Authentication (Success/Failure) • User Access of Application Components ○ File and Object Access ○ Audit Log Access (Success/Failure) ○ System Access (Failure) ○ Application Transactions • Transaction Logs • System Performance and Operational Characteristics ○ Resource Utilization ○ Errors (Input Validation, Dis-Allowed Operations) and Exit Codes ○ Process Status ○ Service Status Changes (e.g., Started, Stopped) • Application Configuration and Version, Middleware Configuration and Version • Usage Information, if Applicable • User Request and Response Events, if Applicable	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
Container	Image	• Vulnerability Scan Log • Hash of the Binary • Hash of the Executables • Container-Aware Network Monitoring • Container-Aware Process Monitoring • Container-Aware Malware Detection • Filesystem Changes Log • Data Monitoring • Read and/or Writes to Well-Known Directories (e.g., /ETC, /USR/BIN, USR/SBIN, etc.) • Creating Symlink • Changes in File/Resource Ownership or Mode Changes (CHMOD) • Access Control Log • Runtime Vulnerability Scan Log Scan for Malware Log • Digital Signature Verification • Unexpected Network Connections or Socket Mutations	• Log • File • Script	• 12 Months Active Storage • 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
		• Spawned Processes Using Things Like <Execve> • Executing Shell and/or SSH Binaries		
Container	Engine (Management /Orchestration)	• Audit Log • Account Access Log • Active Storage • Account Permission Changes • Application • Configuration Log • Monitoring • Resource Allocation and Dashboards	• Log • Application Monitoring Dashboards	• 12 Months Active Storage • 18 Months Cold Data Storage

Container	OS	• User and Administrator Access to OS Components and Applications
		  ○ File and Object Access
		  ○ Audit Log Access (Success/Failure)
		  ○ System Access and Log Off (Success/Failure)
		  ○ Privilege Access and Log Off (Success/Failure)
		  ○ RDP Access and Log Off (Success/Failure)
		  ○ SMB Access
		• System Performance and Operational Characteristics
		  ○ Resource Utilization, Process Status
		  ○ System Events
		  ○ Service Status Changes (Start, Stop, Fail, Restart, etc.)
		  ○ Service Failures and Restarts
		  ○ Process Creation and Termination
		• System Configuration
		  ○ Changes to Security Configuration (Success/Failure)
		  ○ Audit Log Cleared
		  ○ Changes to Accounts User or Group Management Changes
		  ○ Scheduled Task Changes
		• File Access
		  ○ Transfer of Data to External Media
		• Powershell Execution Commands
		• WMI Events
		• Registry Access
		• Command-Line Interface (CLI)
			• Log	• 12 Months Active Storage
				• 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period

Data Loss Prevention	NA	• Date and Time
		• Source Hostname
		  ○ IP
		  ○ Port
		• Destination Hostname
		  ○ IP
		  ○ Port
		• Description of Malicious Code or Action and Severity
		• Identity or Identifier of the File(s)
		• Description of the Action Taken (Clean, Quarantine, Delete)
		• Signature Updates
			• Log
			• Email Attachments
				• 12 Months Active Storage
				• 18 Months Cold Data Storage

Email Filtering, Spam, and Phishing	Raw and Metadata - Filtering Events	• Date and Time
		• Sent from Sender, from Sender
		• Recipient
		• Subject
		• Email Headers
		• Rule Triggered – Log of Policies along with Actual Values Including but Not Limited to:
		  ○ DNS Records
		  ○ Phish Campaign Identifier
		• Domain URL
			• Log
			• Email Attachments
				• 12 Months Active Storage
				• 18 Months Cold Data Storage

Network Traffic	Full Packet Capture Data	• Decrypted Plaintext • Cleartext	• Packet Capture	• 72 Hours Packet Capture
System Configuration and Performance	System Status	• Resource Utilization • Performance	• Log • Database Record • Script	• 12 Months Active Storage • 18 Months Cold Data Storage

Criticality 3

Log Category	Category Target	Required Data	Format	Retention Period
Container	Cluster/Pod Events	• Container User and Service Logs • Container and Application API Audit Logs • Container Management Access Logs • Changes to Container Resources Across Containers and Container Management Environment	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage

Log Category	Category Target	Required Data	Format	Retention Period
Email Filtering, Spam, and Phishing	NA	• Spam Dictionary Modifications	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
Mainframes	NA	• Syslog & Syslog Data • Log4j Data • Sysout Data Resource Measurement Facility (RMF) Data • System Management Facility (SMF)16 • Output from Integrated Intrusion Detection Service	• Log	• 12 Months Active Storage • 18 Months Cold Data Storage
System Configuration and Performance	Software Updates	• User Agent	• Log • Database Record • Script	• 12 Months Active Storage • 18 Months Cold Data Storage

Appendix B – Documenting Event Logs

Document Format

Event Logs by Application and Event Log schemas will be transmitted to the Virginia Open Data Portal in .CSV format.

Event Logs By Application

Event Logs by Application and Event Log schemas will be transmitted to the Virginia Open Data Portal in .CSV format.

CSV Example for Event Logs By Application

```
Agency,Application Name,Event Log
VDOT,Adopt A Highway,Windows Application
VDOT,Adopt A Highway,Windows Security
VDOT,Adopt A Highway,Windows Setup
VDOT,Adopt A Highway,Windows System
```

Log Schemas

Data Elements within an event log shall be documented as follows:

- Agency - Name of the submitting agency
- Application Name - Name of the application supporting the custom event log
- Log Name - Name of the custom event log
- Data Element - Name of the column being tracked
- Data Type – Scope of the value that the Data Element accepts, such as string, integer, or datetime
- Format - Rules for display of the Data Element if any
- List Values - All possible codes and their definitions when the Data Element is a code

Log Schema Example

Agency	Application Name	Log Name	Data Element	Data Type	.	List Values
VDOT	Adopt A Highway	Custom Log	Source IP (IPv4)	String	x.x.x.x, where x is an octet and must be a decimal value between 0 and 255. Octets are separated by periods. Must contain three periods and four octets.	
VDOT	Adopt A Highway	Custom Log	Source IP (IPv6)	String	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx Each x is a hexadecimal digit, representing 4 bits. Leading zeros can be omitted. The double colon (::) can be used once in the text form of an address, to designate any number of 0 bits.	
VDOT	Adopt A Highway	Custom Log	Cache Warning Code	String		110-Response is Stale 111-Revalidation Failed 112-Disconnected Operation 113-Heuristic Expiration 199-Miscellaneous Warning 214-Transformation Applied 299-Miscellaneous Persistent Warning
VDOT	Adopt A Highway	Custom Log	Response Time	Decimal	0.0### ms	
VDOT	Adopt A Highway	Custom Log	Unique ID	GUID		
VDOT	Adopt A Highway	Custom Log	MAC address5	String	XX:XX:XX:XX:XX:XX	
VDOT	Adopt A Highway	Custom Log	Timestamp	Datetime	YYYY-MM-DDThh:mm:ss.mmmZ (Zulu time, UTC+0) YYYY-MM-DDThh:mm:ss.mmm+04:00 (UTC+4)	

CSV Example for Log Schema

```
Agency,Application,Log Name,Data Element,Data Type,Format,List Values
Virginia Department of Transportation,Adopt A Highway,Custom Log,Source IP (IPv4),String,"x.x.x.x,
where x is an octet and must be a decimal value between 0 and 255. Octets are separated by periods.
Must contain three periods and four octets.",
Virginia Department of Transportation,Adopt A Highway,Custom Log,Source IP
(IPv6),String,"xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
Each x is a hexadecimal digit, representing 4 bits. Leading zeros can be omitted. The double colon (::) can
be used once in the text form of an address, to designate any number of 0 bits.",
Virginia Department of Transportation,Adopt A Highway,Custom Log,Cache Warning Code,String,,"110-
Response is Stale
111-Revalidation Failed
112-Disconnected Operation
113-Heuristic Expiration
199-Miscellaneous Warning
214-Transformation Applied
299-Miscellaneous Persistent Warning"
Virginia Department of Transportation,Adopt A Highway,Custom Log,Response Time,Decimal,0.0### ms,
Virginia Department of Transportation,Adopt A Highway,Custom Log,Unique ID,GUID,,
Virginia Department of Transportation,Adopt A Highway,Custom Log,MAC
address5,String,XX:XX:XX:XX:XX:XX,
Virginia Department of Transportation,Adopt A Highway,Custom Log,Timestamp,Datetime,"YYYY-MM-
DDThh:mm:ss.mmmZ (Zulu time, UTC+0)
YYYY-MM-DDThh:mm:ss.mmm+04:00 (UTC+4) ",
```