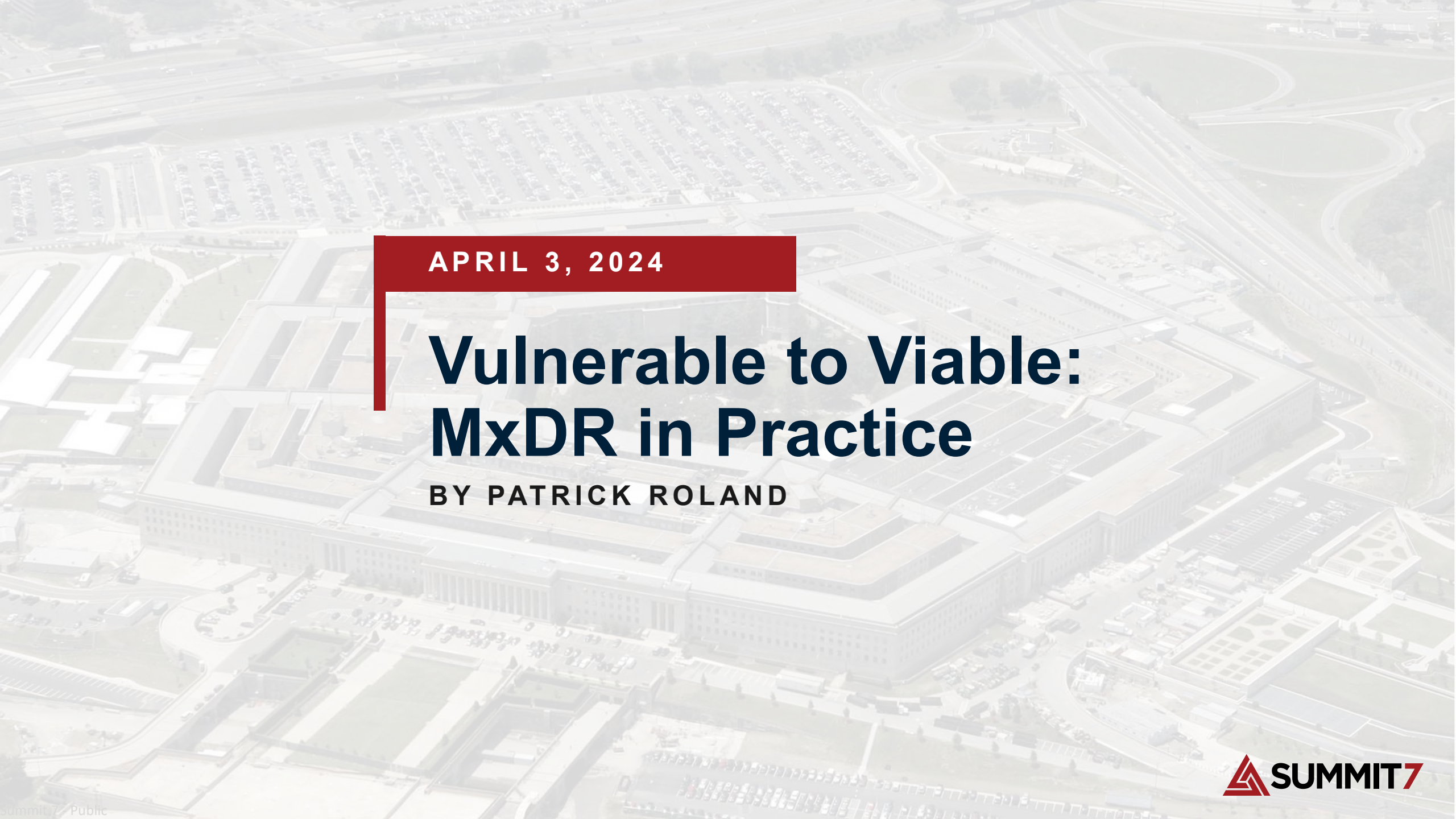


APRIL 3, 2024

# Vulnerable to Viable: MxDR in Practice

BY PATRICK ROLAND

SUMMIT7

# About the Speaker

GUARDIAN+ VIGILANCE

**The Managed IT (MSP) and Managed Security (MSSP) Solution for DoD Contractors**

## Patrick Roland

DIRECTOR OF VIGILANCE MXDR

M.Sc., Cybersecurity and Information Assurance, WGU
ISC2 Certified Information system Security Professional (CISSP)
CMMC Certified Professional (CCP)
SC-200: Microsoft Security Operations Analyst
BTL1(Gold): Aligned with NICE Cyber Defense Analyst framework



SUMMIT7

# Security Operations Center

SUMMIT7

# What Goes Into a SecOps Practice?

A FUSION OF MULTIPLE SKILLSETS

01

## Business Acumen

02

## Data Engineering

03

## Data Analysis

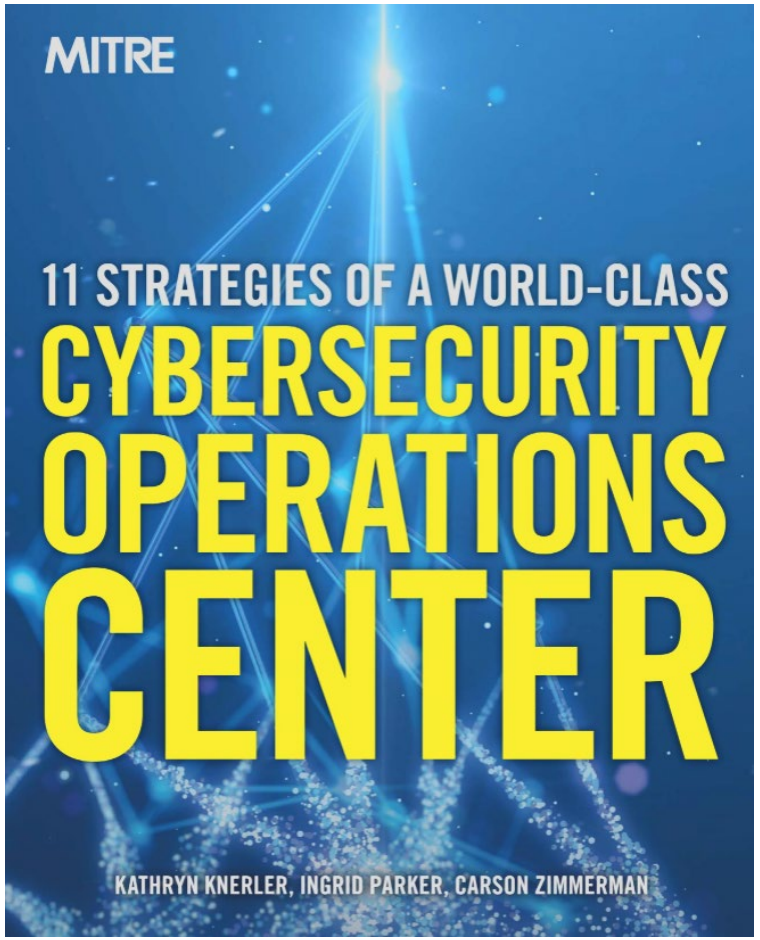
04

## Information Security



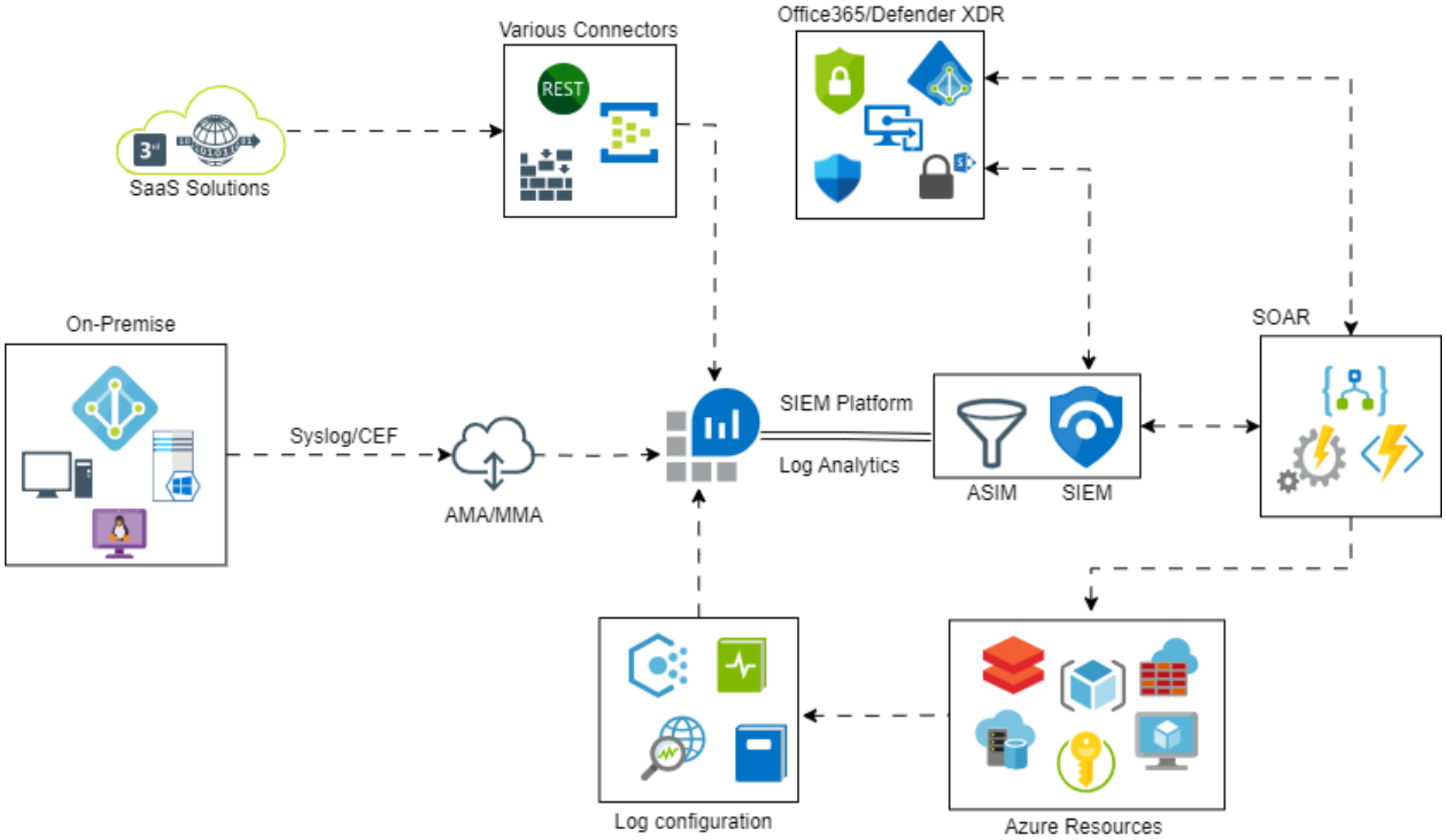
SUMMIT7


High Level Overview




SUMMIT7

# Vigilance MxDR



# Compliance & Security

Compliance is only the beginning

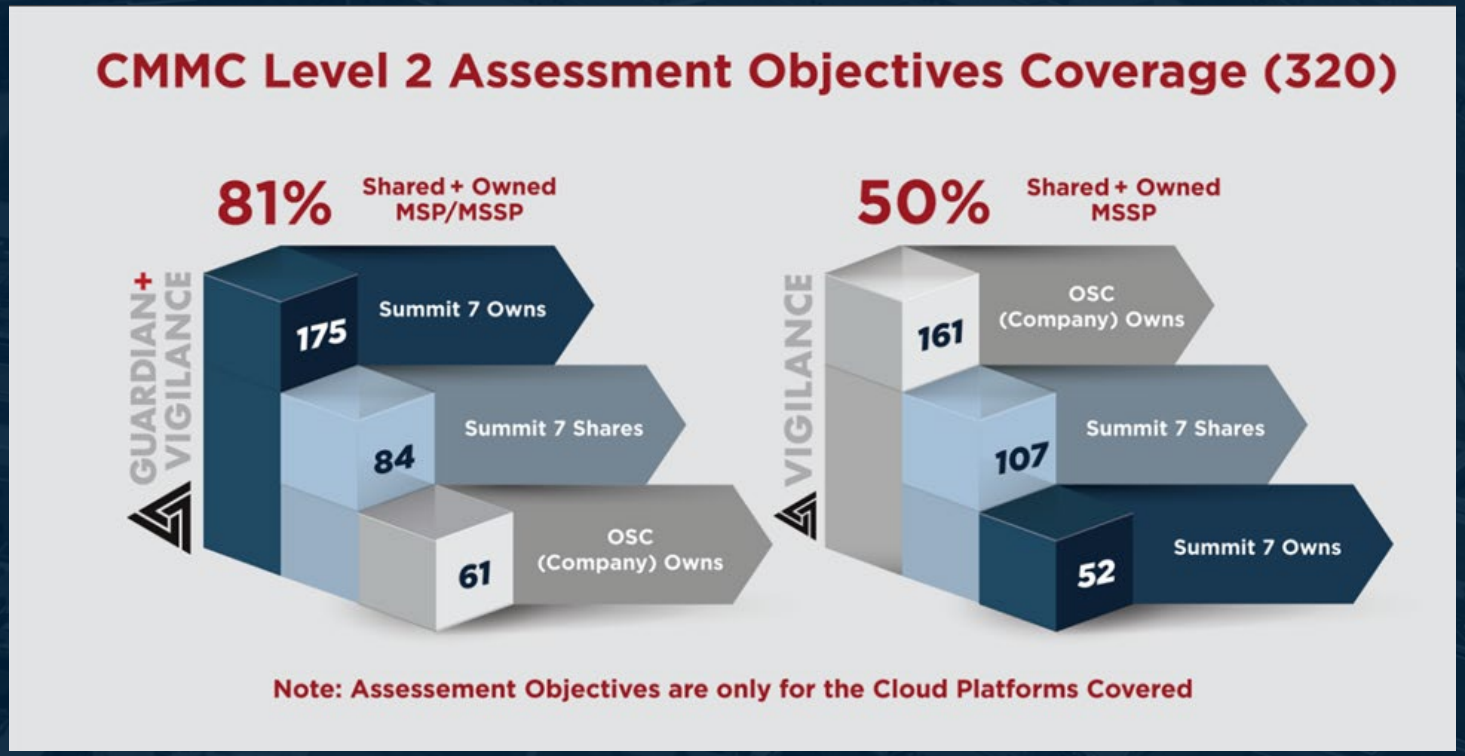
## MxDR Concentration

Section 3.3
Audit and Accountability (AU)

## MxDR Support

56 out of 110 Controls supported by a mature audit logging function.

The assessment methods define the nature and the extent of the assessor's actions. The methods include *examine*, *interview*, and *test*. The examine method is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities). The purpose of the examine method is to facilitate understanding, achieve clarification, or obtain evidence. The interview method is the process of holding discussions with individuals or groups






SUMMIT7

# 3.3.1

Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems.

## NIST 800-53

AU-2 Event Logging

AU-3 Content of Audit Records

AU-3(1) Additional Audit Information

AU-6 Audit Record Review, Analysis, and Reporting

AU-11 Audit Record Retention

AU-12 Audit Record Generation

| | | |
|---|---|---|
| **3.3.1** | **SECURITY REQUIREMENT**<br>Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | |
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.3.1[a]** | *audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.* |
| | **3.3.1[b]** | *the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.* |
| | **3.3.1[c]** | *audit records are created (generated).* |
| | **3.3.1[d]** | *audit records, once created, contain the defined content.* |
| | **3.3.1[e]** | *retention requirements for audit records are defined.* |
| | **3.3.1[f]** | *audit records are retained as defined.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing auditable events; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing control of audit records; procedures addressing audit record generation; system audit logs and records; system auditable events; system incident reports; other relevant documents or records].<br>**Interview**: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; personnel with audit review, analysis and reporting responsibilities; system or network administrators].<br>**Test**: [*SELECT FROM:* Mechanisms implementing system audit logging]. | |



SUMMIT7

# M-21-31

Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

*Table 1: Summary of Event Logging Tiers*

| Event Logging Tiers | Rating | Description |
|---|---|---|
| **EL0** | Not Effective | Logging requirements of highest criticality are either not met or are only partially met |
| **EL1** | Basic | Only logging requirements of highest criticality are met |
| **EL2** | Intermediate | Logging requirements of highest and intermediate criticality are met |
| **EL3** | Advanced | Logging requirements at all criticality levels are met |



SUMMIT7

# 3.3.2

This requirement ensures that the contents of the audit record include the information needed to link the audit event to the actions of an individual to the extent feasible. Organizations consider logging for traceability including results from monitoring…

## NIST 800-53

AU-2 Event Logging

AU-3 Content of Audit Records

AU-3(1) Additional Audit Information

AU-6 Audit Record Review, Analysis, and Reporting

AU-11 Audit Record Retention

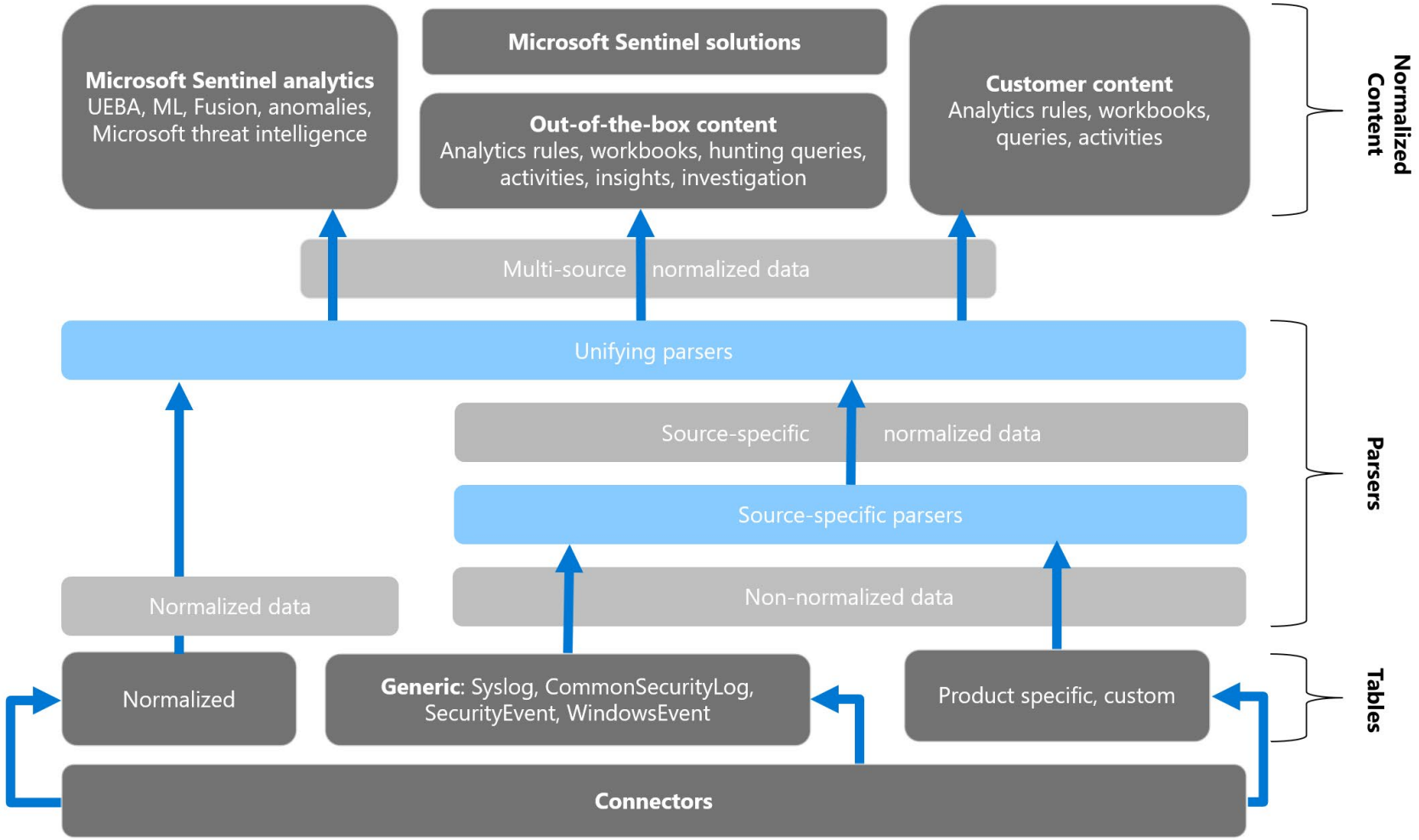
AU-12 Audit Record Generation

| | | |
|---|---|---|
| **3.3.2** | **SECURITY REQUIREMENT**<br>Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | |
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.3.2[a]** | *the content of the audit records needed to support the ability to uniquely trace users to their actions is defined.* |
| | **3.3.2[b]** | *audit records, once created, contain the defined content.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>Examine: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit records and event types; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing audit record generation; procedures addressing audit review, analysis, and reporting; reports of audit findings; system audit logs and records; system events; system incident reports; other relevant documents or records].<br>Interview: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators]. | |



SUMMIT7

# ASIM Architecture



# Tier EL 1, Rating - Basic

EL1 Basic Requirements (Implementation and Centralized Access)

**Requirements:**

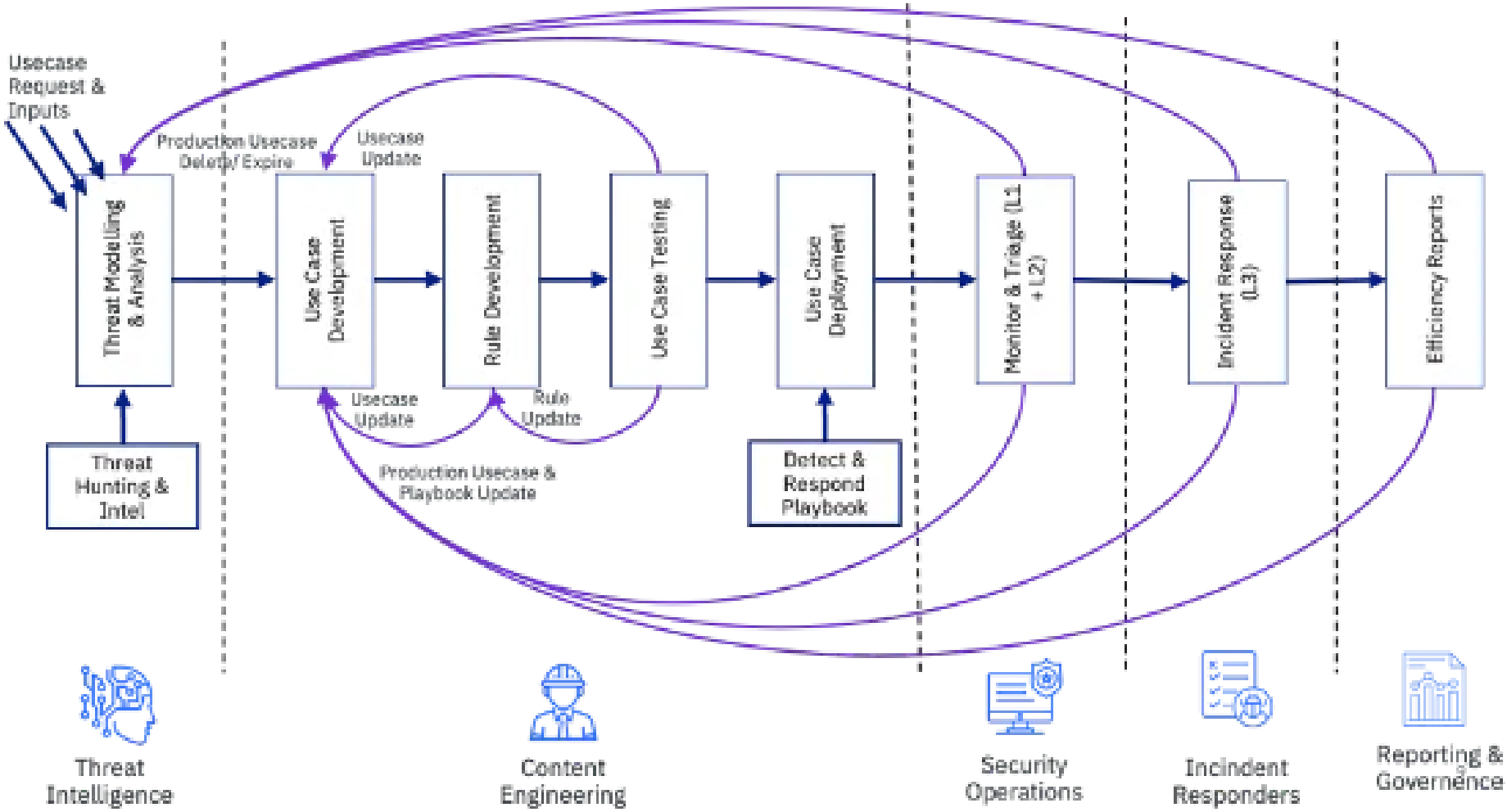
- ✓ Basic Logging Categories
- ✓ Minimum Logging Data
- ✓ Time Standard
- ✓ Event Forwarding
- ✓ Protecting and Validating Log Information
- ✓ Passive DNS
- ✓ Cybersecurity Infrastructure Security Agency (CISA) and Federal Bureau of Investigations (FBI) Access Requirements
- ✓ Logging Orchestration, Automation, and Response
- ✓ User Behavior Monitoring
- ✓ Basic Centralized Access

**Appendix A: Implementation and Centralized Access Requirements**

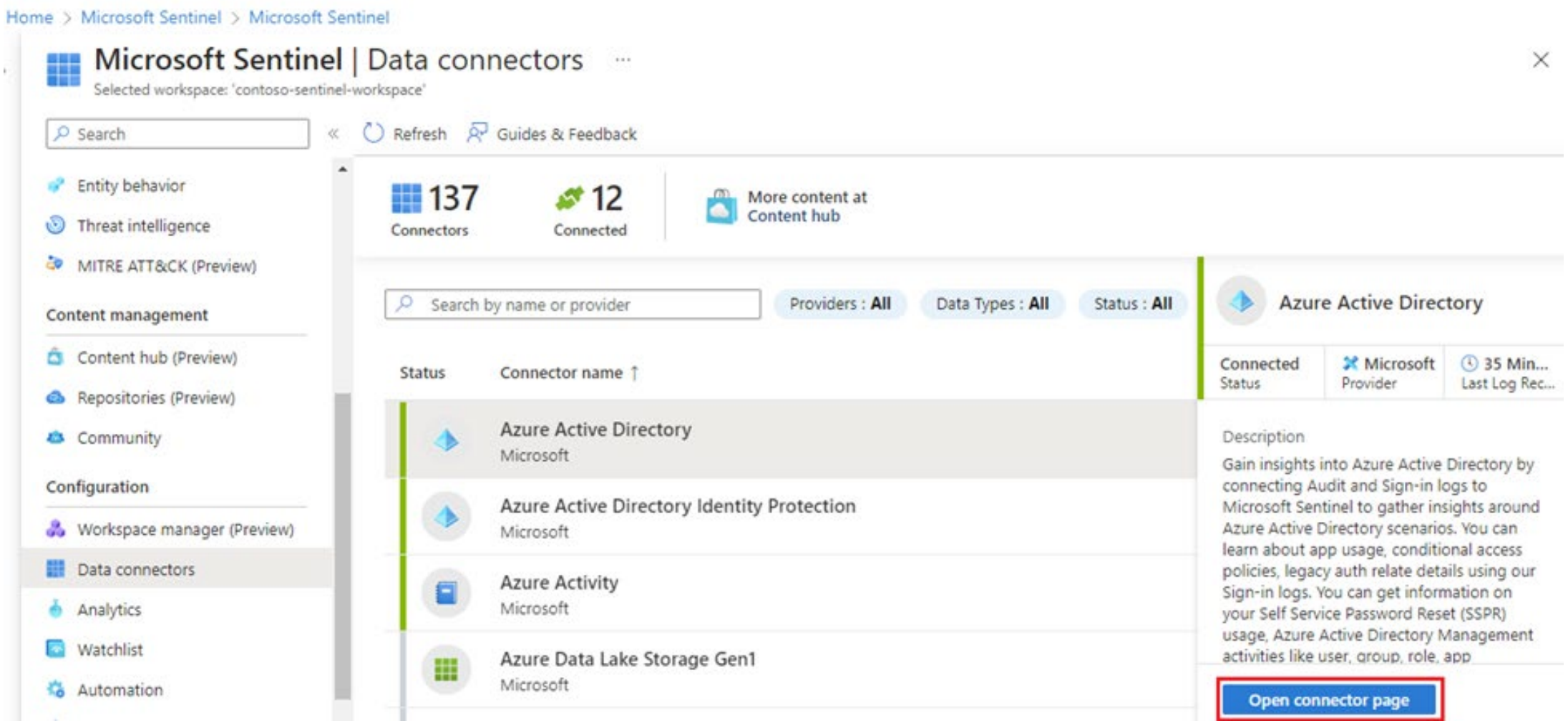
*Table 2: EL1 Basic Requirements*

| | |
|---|---|
| Basic Logging Categories | Ensuring that Required Logs categorized as Criticality Level 0 are retained in acceptable formats for specified timeframes, per technical details described in Appendix C. |
| Minimum Logging Data | At a minimum, agencies shall ensure that each event log contains the following data, if applicable:<br>• Properly formatted and accurate timestamp (see below for Time Standard Requirements)<br>• Status code for the event type<br>• Device identifier (MAC address[5] or other unique identifier)<br>• Session / Transaction ID<br>• Autonomous System Number<br>• Source IP (IPv4)<br>• Source IP (IPv6)<br>• Destination IP (IPv4)<br>• Destination IP (IPv6)<br>• Status Code<br>• Response Time<br>• Additional headers (i.e., HTTP headers)<br>• Where appropriate, the username and/or userID shall be included<br>• Where appropriate, the command executed shall be included<br>• Where possible, all data shall be formatted as key-value-pairs allowing for easy extraction<br>• Where possible, a unique event identifier shall be included for event correlation; a unique event identifier shall be defined per event type[6] |

# SIEM USE-CASE DIAGRAM



# Built-in SIEM Connectors



# NIST SP 800-53

## AU-11: Audit Record Retention

| | | |
|---|---|---|
| **Control Family:** | Audit And Accountability | |
| **Priority:** | P3: Implement P3 security controls after implementation of P1 and P2 controls. | |
| **CSF v1.1 References:** | PR.PT-1 | |
| **Baselines:** | Low | AU-11 |
| | Moderate | AU-11 |
| | High | AU-11 |
| **Next Version:** | NIST Special Publication 800-53 Revision 5: AU-11: Audit Record Retention | |

### Control Statement

The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

### Supplemental Guidance

Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention.

# Log Data Volume

MITRE 11 Strategies of a World-Class Cybersecurity Operations Center

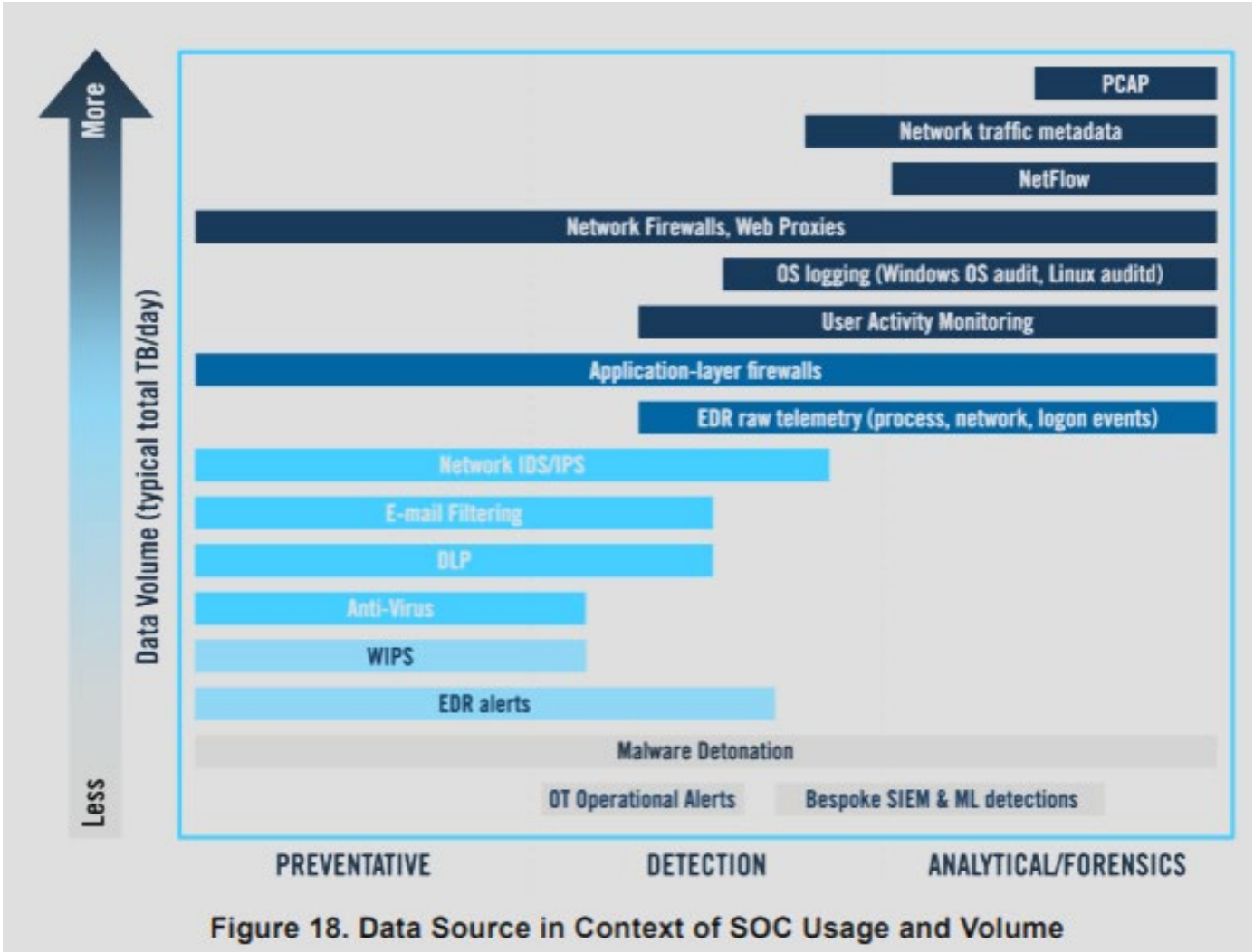



Figure 18. Data Source in Context of SOC Usage and Volume

# Suggested Log Retention

MITRE 11 Strategies of a World-Class Cybersecurity Operations Center

**Table 15. Suggested Minimum Data Retention Time Frames**

| What | SOC triage | SOC forensics & investigations | External Support |
|---|---|---|---|
| EDR, network sensor alerts, and SIEM-correlated alerts | 2 weeks | 6 months | 2+ years |
| NetFlow & traffic metadata logs | 1 month | 6 months | 2+ years |
| Full-session PCAP | as needed* | as needed* | as needed* |
| System, network & application audit logs | 2 weeks | 6 months | 2+ years |
| Emails | 2 weeks | 2 years | As needed |



SUMMIT7

# 3.3.3

The intent of this requirement is to periodically re-evaluate which logged events will continue to be included in the list of events to be logged. The event types that are logged by organizations may change over time.

Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.

## NIST 800-53

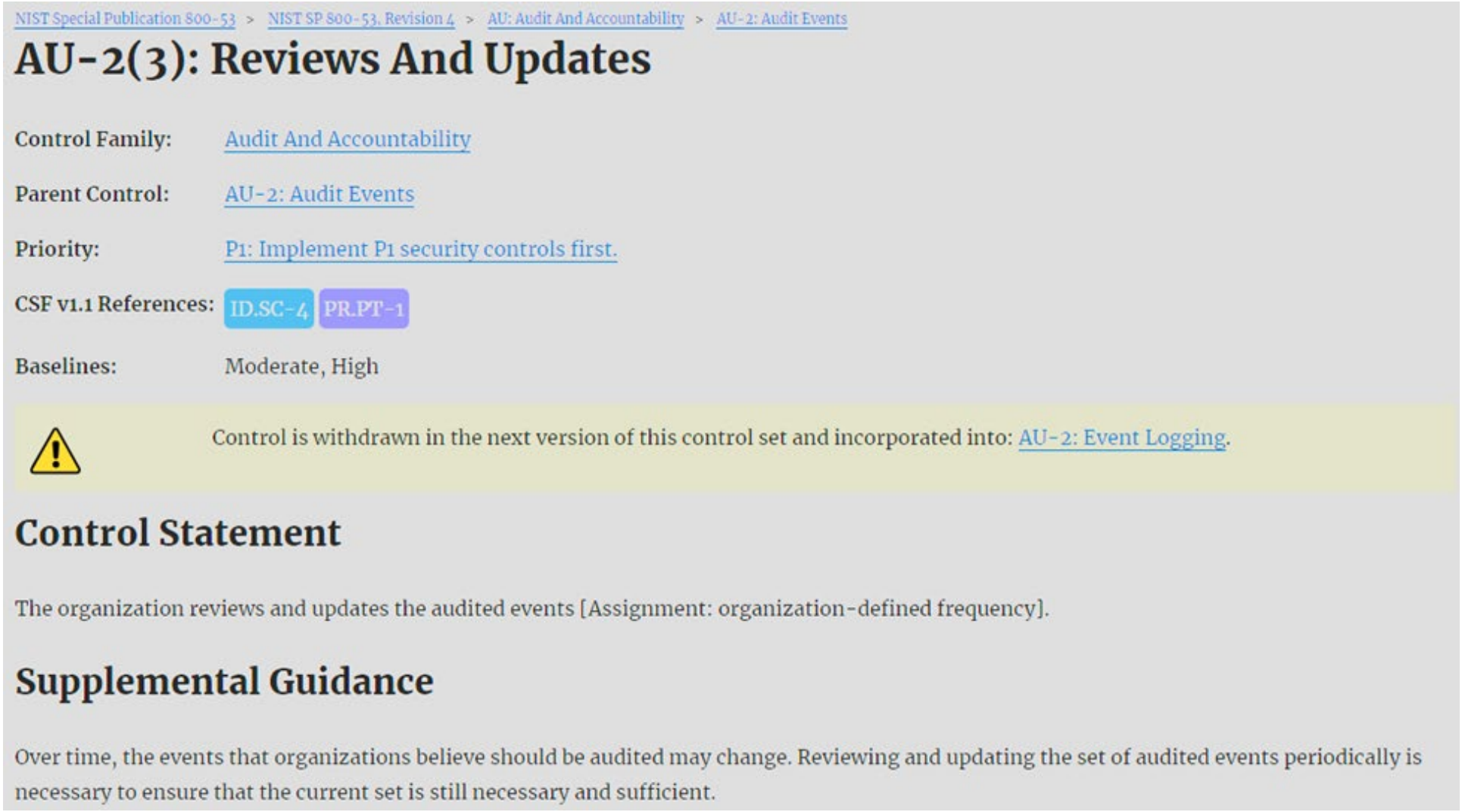
AU-2(3) Event Logging, Review and Updates

| 3.3.3 | **SECURITY REQUIREMENT**<br>Review and update logged events. | |
|---|---|---|
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.3.3[a]** | *a process for determining when to review logged events is defined.* |
| | **3.3.3[b]** | *event types being logged are reviewed in accordance with the defined review process.* |
| | **3.3.3[c]** | *event types being logged are updated based on the review.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>Examine: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit records and event types; system security plan; list of organization-defined event types to be logged; reviewed and updated records of logged event types; system audit logs and records; system incident reports; other relevant documents or records].<br>Interview: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities].<br>Test: [*SELECT FROM:* Mechanisms supporting review and update of logged event types]. | |



SUMMIT7

# NIST SP 800-53



NIST Special Publication 800-53 > NIST SP 800-53, Revision 4 > AU: Audit And Accountability > AU-2: Audit Events

## AU-2(3): Reviews And Updates

**Control Family:** Audit And Accountability

**Parent Control:** AU-2: Audit Events

**Priority:** P1: Implement P1 security controls first.

**CSF v1.1 References:** ID.SC-4 PR.PT-1

**Baselines:** Moderate, High

⚠ Control is withdrawn in the next version of this control set and incorporated into: AU-2: Event Logging.

### Control Statement

The organization reviews and updates the audited events [Assignment: organization-defined frequency].

### Supplemental Guidance

Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

# Cybersecurity Log Management Planning Guide

NIST Special Publication, NIST SP 800-92r1 ipd

**INV, Update Logging-Related Inventories** (Section 3):

Characterize the current state of your organization's cybersecurity logging.

**TS, Define Target State** (Section 4):

Define the target state for your organization's cybersecurity logging.

**GRC, Document Gaps and Their Root Causes** (Section 5):

Document the gaps between the current cybersecurity logging state and the target state, and identify the root causes of each gap.

**PMG, Develop a Plan to Mitigate the Gaps** (Section 6):

Develop a plan for addressing the root causes of the identified gaps in order to reach the target state.



SUMMIT7

# NIST SP 800-92

Compliance Objective Mapping

| Play | NIST SP 800-53, Rev. 5 [SP800-53r5] | CSF 1.1 [CSF11] | EO 14028 Security Measures [NIST-CRSW] |
|---|---|---|---|
| INV-1, Update the Inventory of Log Source Types | AU-2, AU-12, CM-2, CM-6, CM-8 | ID.AM-2, ID.AM-4 | SM 1.3, SM 2.1, SM 3.1, SM 3.3 |
| INV-2, Update the Logging Infrastructure Inventory | CM-8 | ID.AM-1, ID.AM-2, ID.AM-4 | SM 2.1, SM 3.1 |
| INV-3, Update the Logging Use Case Inventory | AU-1 | ID.GV-1 | SM 1.3 |
| INV-4, Update the Requirements Inventory | AU-1, AU-2 | ID.GV-3 | N/A |
| INV-5, Update the Work Role Inventory | AU-1 | ID.AM-6 | SM 5.1, SM 5.2 |
| TS-1, Forecast Future Changes to Logging Inventories | AU-1 | ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4 | SM 4.1 |
| TS-2, Define Target State for Log Generation | AU-1 | ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4 | SM 4.1 |
| TS-3, Define Target State for Log Storage and Transfer | AU-1 | ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4 | SM 4.1 |
| TS-4, Define Target State for Log Access | AU-1 | ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4 | SM 4.1 |
| TS-5, Define Target State for Log Disposal | AU-1 | ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4 | SM 4.1 |
| GRC-1, Scope and Plan the Assessment | RA-1 | ID.RM-1 | SM 4.1 |
| GRC-2, Conduct the Assessment and Document Findings | RA-3 | ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5 | SM 4.1 |
| PMG-1, Draft the Plan | AU-1, RA-7 | ID.RA-6 | SM 4.1 |
| PMG-2, Revise Affected Policies | AU-1 | ID.GV-1, ID.GV-4 | SM 4.1 |
| PMG-3, Address Feedback on Draft Plan and Policies | AU-1, RA-7 | ID.GV-1, ID.GV-4, ID.RA-6 | SM 4.1 |



SUMMIT7

# 3.3.4

Audit logging process failures include software and hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded.

This requirement applies to each audit record data storage repository (i.e., distinct system component where audit records are stored), the total audit record storage capacity of organizations (i.e., all audit record data storage repositories combined), or both.

## NIST 800-53

AU-5 Response to Audit Logging Process Failures

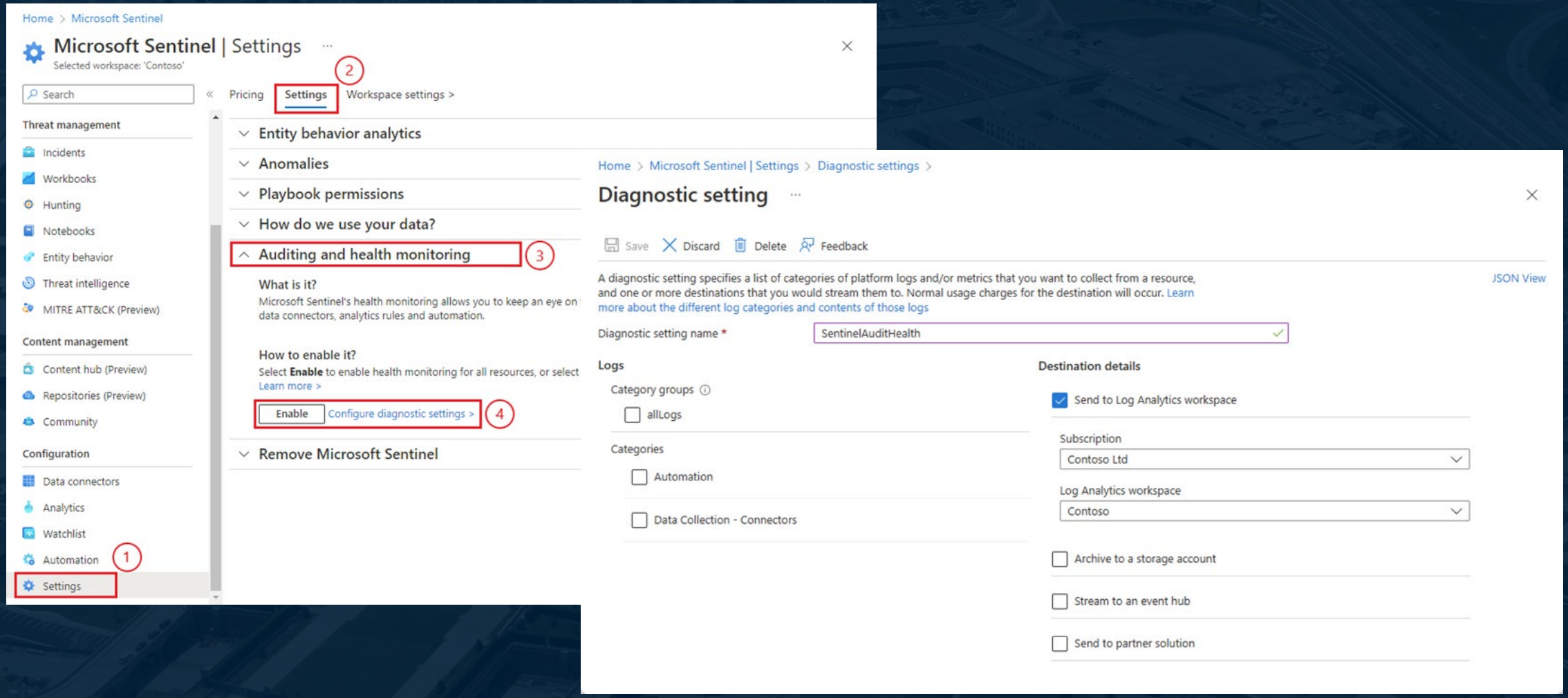
| 3.3.4 | **SECURITY REQUIREMENT**<br>Alert in the event of an audit logging process failure. | |
|---|---|---|
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.3.4[a]** | *personnel or roles to be alerted in the event of an audit logging process failure are identified.* |
| | **3.3.4[b]** | *types of audit logging process failures for which alert will be generated are defined.* |
| | **3.3.4[c]** | *identified personnel or roles are alerted in the event of an audit logging process failure.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>Examine: [*SELECT FROM:* Audit and accountability policy; procedures addressing response to audit logging processing failures; system design documentation; system security plan; system configuration settings and associated documentation; list of personnel to be notified in case of an audit logging processing failure; system incident reports; system audit logs and records; other relevant documents or records].<br>Interview: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators; system developers].<br>Test: [*SELECT FROM:* Mechanisms implementing system response to audit logging processing failures]. | |



SUMMIT7

# Sentinel Health Settings

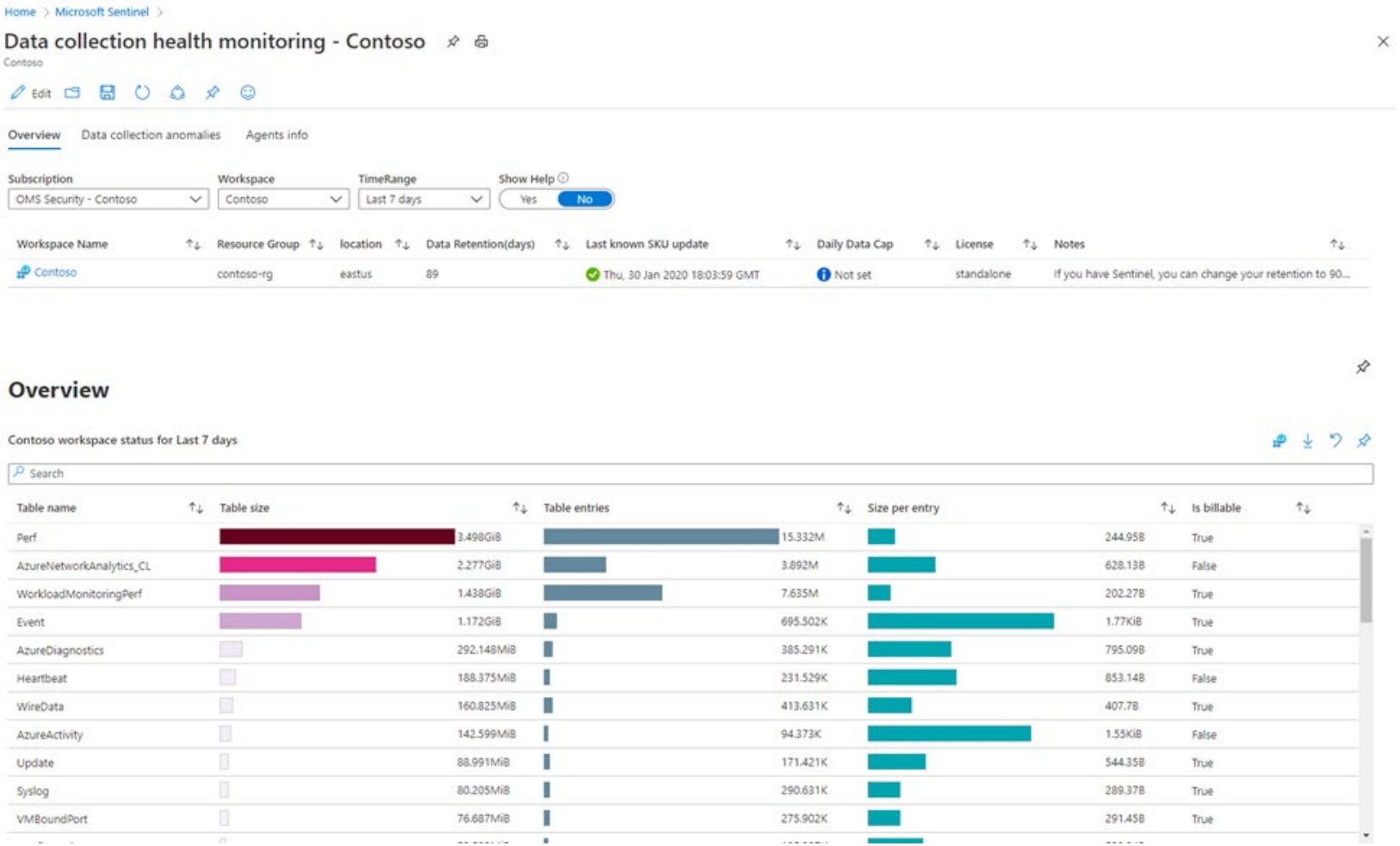
Configuration






SUMMIT7

# Sentinel Health Settings



# 3.3.5

Correlating audit record review, analysis, and reporting processes helps to ensure that they do not operate independently, but rather collectively.

Regarding the assessment of a given organizational system, the requirement is agnostic as to whether this correlation is applied at the system level or at the organization level across all systems.

## NIST 800-53

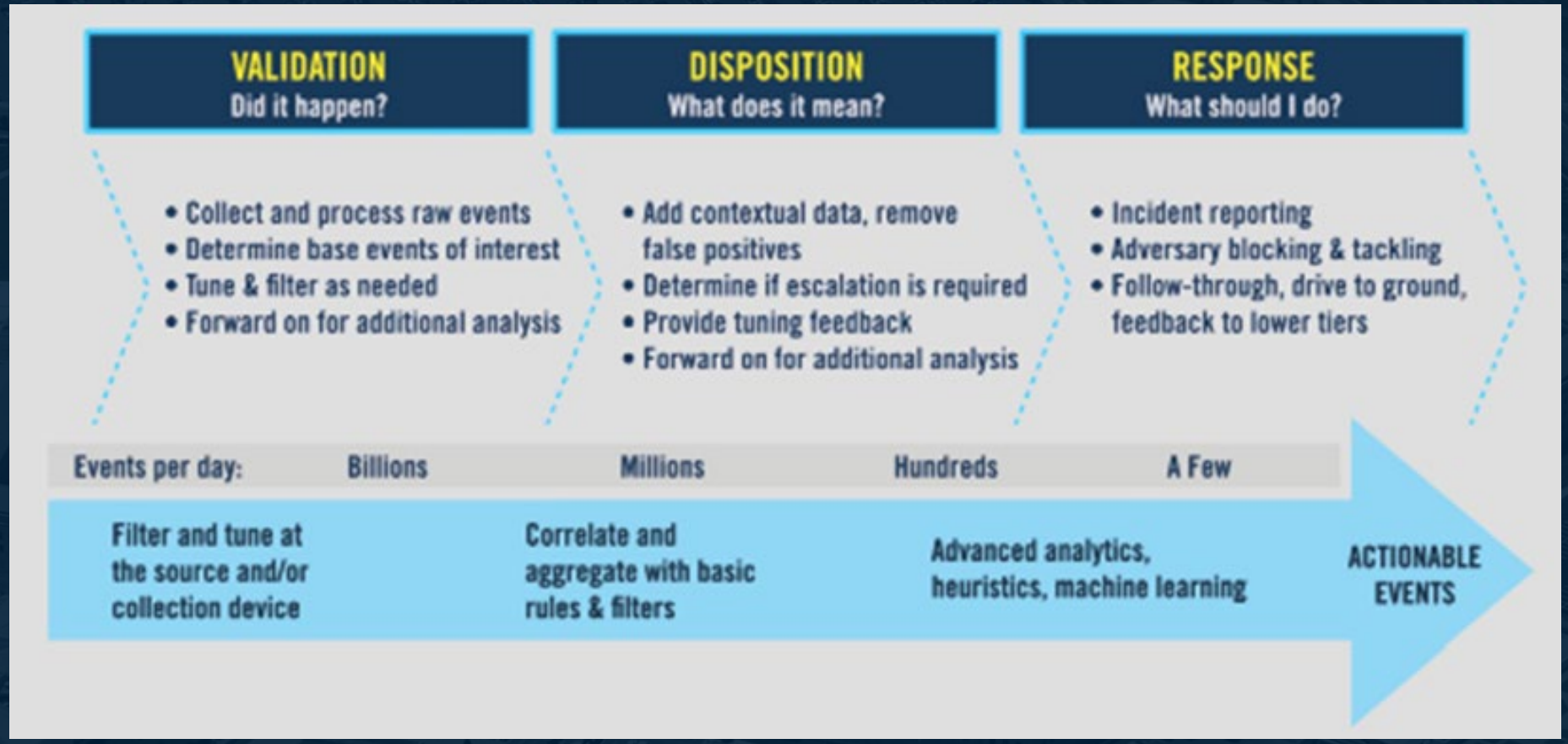
AU-6(3) Audit Record Review, Analysis, and Reporting
Correlate Audit Record Repositories

| | | |
|---|---|---|
| **3.3.5** | **SECURITY REQUIREMENT**<br>Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. | |
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.3.5[a]** | *audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined.* |
| | **3.3.5[b]** | *defined audit record review, analysis, and reporting processes are correlated.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>Examine: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit record review, analysis, and reporting; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing investigation of and response to suspicious activities; system audit logs and records across different repositories; other relevant documents or records].<br>Interview: [*SELECT FROM:* Personnel with audit record review, analysis, and reporting responsibilities; personnel with information security responsibilities].<br>Test: [*SELECT FROM:* Mechanisms supporting analysis and correlation of audit records; mechanisms integrating audit review, analysis and reporting]. | |



SUMMIT7

# SOC Analyst Process






SUMMIT7

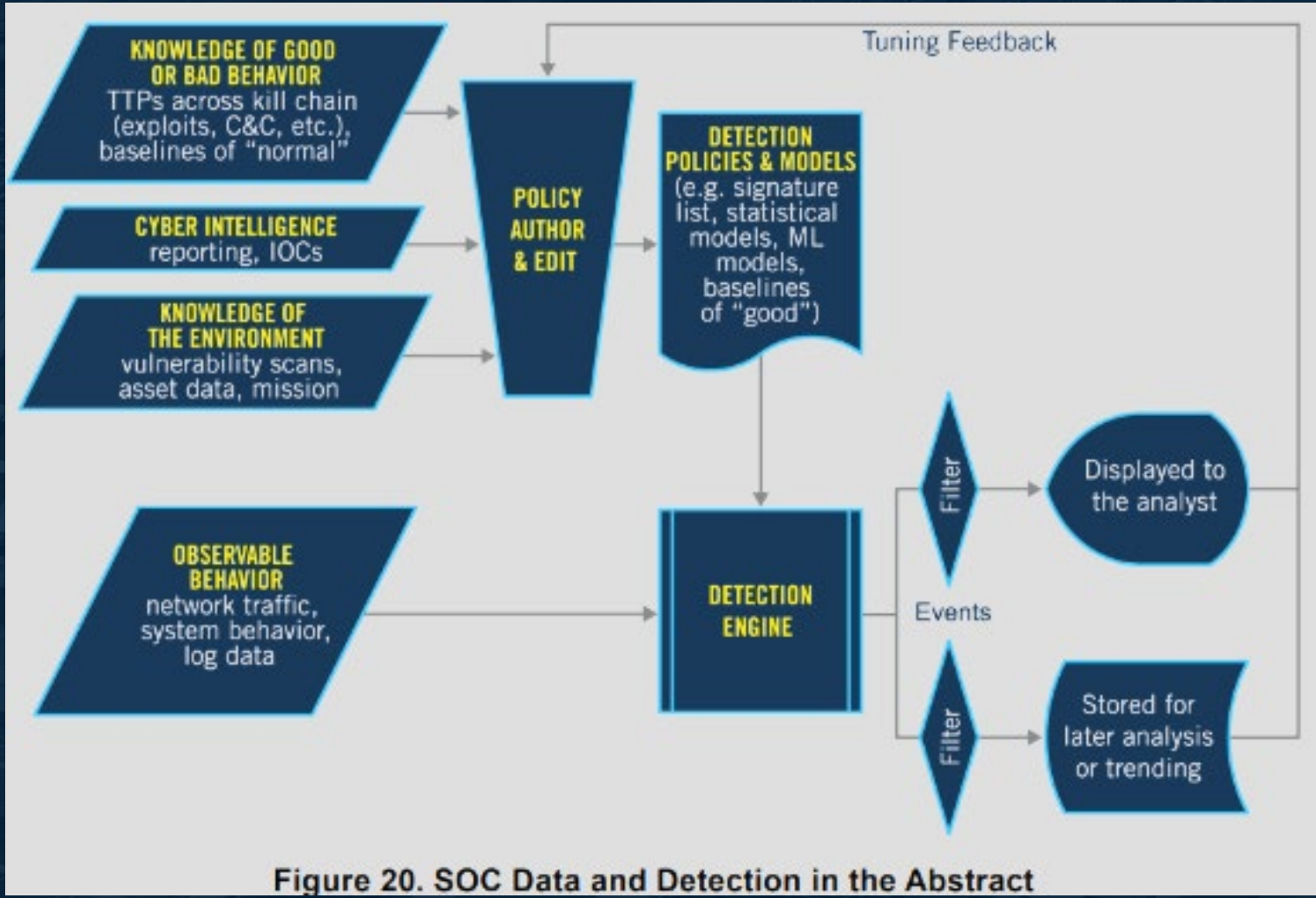



Figure 20. SOC Data and Detection in the Abstract




SUMMIT7

# 3.3.6

Audit record reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or organizational entities conducting auditing activities.

Audit record reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records…

## NIST 800-53

AU-7 Audit Record Reduction and Report Generation

| | | |
|---|---|---|
| **3.3.6** | **SECURITY REQUIREMENT**<br>Provide audit record reduction and report generation to support on-demand analysis and reporting. | |
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.3.6[a]** | *an audit record reduction capability that supports on-demand analysis is provided.* |
| | **3.3.6[b]** | *a report generation capability that supports on-demand reporting is provided.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>Examine: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit record reduction and report generation; system design documentation; system security plan; system configuration settings and associated documentation; audit record reduction, review, analysis, and reporting tools; system audit logs and records; other relevant documents or records].<br>Interview: [*SELECT FROM:* Personnel with audit record reduction and report generation responsibilities; personnel with information security responsibilities].<br>Test: [*SELECT FROM:* Audit record reduction and report generation capability]. | |



SUMMIT7

# 3.3.7

Internal system clocks are used to generate time stamps, which include date and time. Time is expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC…

Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

## NIST 800-53

AU-8 Time Stamps

AU-8(1) Synchronization with Authoritative Time Source

| | | |
|---|---|---|
| **3.3.7** | **SECURITY REQUIREMENT**<br>Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. | |
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.3.7[a]** | *internal system clocks are used to generate time stamps for audit records.* |
| | **3.3.7[b]** | *an authoritative source with which to compare and synchronize internal system clocks is specified.* |
| | **3.3.7[c]** | *internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>Examine: [*SELECT FROM:* Audit and accountability policy; procedures addressing time stamp generation; system design documentation; system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records].<br>Interview: [*SELECT FROM:* Personnel with information security responsibilities; system or network administrators; system developers].<br>Test: [*SELECT FROM:* Mechanisms implementing time stamp generation; mechanisms implementing internal information system clock synchronization]. | |



SUMMIT7

# 3.3.8

This requirement focuses on the technical protection of audit information and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by media protection and physical and environmental protection requirements

## NIST 800-53

AU-9 Protection of Audit Information

Access by Subset of Privileged Users

| 3.3.8 | **SECURITY REQUIREMENT**<br>Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | |
|---|---|---|
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.3.8[a]** | *audit information is protected from unauthorized access.* |
| | **3.3.8[b]** | *audit information is protected from unauthorized modification.* |
| | **3.3.8[c]** | *audit information is protected from unauthorized deletion.* |
| | **3.3.8[d]** | *audit logging tools are protected from unauthorized access.* |
| | **3.3.8[e]** | *audit logging tools are protected from unauthorized modification.* |
| | **3.3.8[f]** | *audit logging tools are protected from unauthorized deletion.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine**: [*SELECT FROM:* Audit and accountability policy; access control policy and procedures; procedures addressing protection of audit information; system security plan; system design documentation; system configuration settings and associated documentation, system audit logs and records; audit logging tools; other relevant documents or records].<br>**Interview**: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators; system developers].<br>**Test**: [*SELECT FROM:* Mechanisms implementing audit information protection]. | |



SUMMIT7

# NIST SP 800-53

AU-9 Protection Of Audit Information

## AU-9: Protection of Audit Information

**Control Family:** Audit and Accountability

**Threats Addressed:** Tampering | Information Disclosure

**Baselines:**

| | |
|---|---|
| Low | AU-9 |
| Moderate | AU-9 (4) |
| High | AU-9 (2) (3) (4) |
| Privacy | N/A |

**Previous Version:** NIST Special Publication 800-53 Revision 4: AU-9: Protection Of Audit Information

### Control Statement

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.

### Supplemental Guidance

Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.



SUMMIT7

# 3.3.9

Separation of Duties

Individuals with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit logging activities or modifying audit records.

This requirement specifies that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges

## NIST SP 500-53

AU-9(4) Protection of Audit Information, Access by Subset of Privileged Users

| | | |
|---|---|---|
| **3.3.9** | **SECURITY REQUIREMENT**<br>Limit management of audit logging functionality to a subset of privileged users. | |
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.3.9[a]** | *a subset of privileged users granted access to manage audit logging functionality is defined.* |
| | **3.3.9[b]** | *management of audit logging functionality is limited to the defined subset of privileged users.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine**: [*SELECT FROM:* Audit and accountability policy; access control policy and procedures; procedures addressing protection of audit information; system security plan; system design documentation; system configuration settings and associated documentation; access authorizations; system-generated list of privileged users with access to management of audit logging functionality; access control list; system audit logs and records; other relevant documents or records].<br>**Interview**: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators; system developers].<br>**Test**: [*SELECT FROM:* Mechanisms managing access to audit logging functionality]. | |



SUMMIT7

# NIST SP 800-53

AU-9(4) Protection Of Audit Information

## AU-9(4): Access By Subset Of Privileged Users

**Control Family:** Audit And Accountability

**Parent Control:** AU-9: Protection Of Audit Information

**Priority:** P1: Implement P1 security controls first.

**CSF v1.1 References:** PR.PT-1

**Threats Addressed:** Tampering, Information Disclosure

**Baselines:** Moderate, High

**Next Version:** NIST Special Publication 800-53 Revision 5: AU-9(4): Access by Subset of Privileged Users

### Control Statement

The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users].

### Supplemental Guidance

Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.



SUMMIT7

# False Claims Act Excerpt:

31. As a starting point, the assessors themselves were not qualified to determine whether a lab's practices actually complied with a given control. This, in and of itself, violates 800-171 3.2.2, which requires that the organization "[e]nsure that personnel are trained to carry out their assigned information security-related duties and responsibilities."

32. For example, in the Manos SSP (discussed below), the SSP listed FileVault (a MacOS disk encryption system) as an anti-malware control. However, as a properly trained auditor would know, FileVault does absolutely nothing to prevent the installation of malicious software and thus could not meet that control.

NIST 800-171 3.2.2
Critical enough as to be considered a starting point in the FCA document.



SUMMIT7

# Is your SOC trained on triage and remediation?

| | | |
|---|---|---|
| **3.2.2** | **SECURITY REQUIREMENT**<br>Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. | |
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.2.2[a]** | *information security-related duties, roles, and responsibilities are defined.* |
| | **3.2.2[b]** | *information security-related duties, roles, and responsibilities are assigned to designated personnel.* |
| | **3.2.2[c]** | *personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>Examine: [*SELECT FROM:* Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; system security plan; training records; other relevant documents or records].<br>Interview: [*SELECT FROM:* Personnel with responsibilities for role-based security training; personnel with assigned system security roles and responsibilities; personnel with responsibilities | |



SUMMIT7

# NIST SP 800-53

AT-3 Role-based Training

## AT-3: Role-based Training

**Control Family:** Awareness and Training

**CSF v1.1 References:** PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5

**PF v1.0 References:** GV.AT-P1 GV.AT-P2 GV.AT-P3 GV.AT-P4

**Baselines:**

| | |
|---|---|
| Low | AT-3 |
| Moderate | AT-3 |
| High | AT-3 |
| Privacy | AT-3 (5) |

**Previous Version:** NIST Special Publication 800-53 Revision 4: AT-3: Role-Based Security Training

## Control Statement

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:
   1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and
   2. When required by system changes;
b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
c. Incorporate lessons learned from internal or external security or privacy incidents into role-based training.



SUMMIT7

# What to look for in the MSSP

- ✓ Security
- ✓ A broad set of capabilities
- ✓ An individualized approach to your needs, budget, and environment
- ✓ Offers an MSP service that supports/augments the MSSP
- ✓ Offers a long-term consulting partner relationship
- ✓ Provides real-time detection and response capabilities that are tailored to your specific business needs (response methods, SLAs, etc.)



SUMMIT7

# What to look for in the MSSP

- ✓ What compliance expertise does the MSSP have?
- ✓ What federal compliance requirements experience does the MSSP have?
- ✓ What is the MSSPs level of understanding of CMMC?
- ✓ What are the credentials and qualifications of the MSSPs staff?
- ✓ What are the internal controls that the MSSP has in place around user access to customer systems/data?



SUMMIT7

# Provider Questions

- ✓ Are you currently CMMC L2 accredited? If not, are you actively working towards accreditation?
  - ✓ What is your timeline for completion?
- ✓ How do you implement the 110 controls and 320 organizational actions outlined in the NIST 800-171 framework?
- ✓ Are your personnel trained on the application of our Compliance frameworks or NIST 800-181(NICE)
- ✓ Can you describe your defense-in-depth approach to situational awareness for compliance needs?
- ✓ What experience do you have with CMMC and DFARS compliance, and can you provide examples of past work?



SUMMIT7

# Questions?