# VA Enterprise Design Patterns:

# 1. Privacy and Security

# 1.6. Enterprise Auditing

**Office of Technology Strategies (TS)**
**Architecture, Strategy, and Design (ASD)**
**Office of Information and Technology (OI&T)**

**Version 0.7**

**Date Issued: January 2016**

THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

**APPROVAL COORDINATION**

X Date: 01/29/2016

Rodney Emery
Director, Technology Strategies and GEAC, ASD
Signed by: people
ASD Technology Strategies

Date:

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

## REVISION HISTORY

| Version | Date | Organization | Notes |
|---|---|---|---|
| 0.1 | 09/08/2015 | ASD TS | Initial Draft/Outline |
| 0.3 | 10/30/2015 | ASD TS | Strawman Draft |
| 0.5 | 12/15/2015 | ASD TS | Updated Draft |
| 0.7 | 01/21/2015 | ASD TS | Final Draft |
| 0.9 | | | |
| 1.0 | | | |

## REVISION HISTORY APPROVALS

| Version | Date | Approver | Role |
|---|---|---|---|
| 0.1 | 09/08/2015 | Joseph Brooks | Brian James |
| 0.3 | 11/05/2015 | Joseph Brooks | Brian James |
| 0.5 | 01/07/2016 | Joseph Brooks | Dan Rockwell |
| 0.6 | | | |
| 0.7 | | | |
| 0.9 | | | |
| 1.0 | | | |

## TABLE OF CONTENTS


**1 INTRODUCTION ..... 2**

1.1 BUSINESS NEED ..... 2
1.2 APPROACH ..... 3

**2 CURRENT CAPABILITIES AND LIMITATIONS ..... 4**

**3 FUTURE CAPABILITIES ..... 7**

3.1 ENTERPRISE AUDITING DATA SOURCES ..... 9
3.2 ENTERPRISE AUDITING DATA TRANSFER ..... 10
3.3 ENTERPRISE AUDITING DATA REPOSITORY ..... 10
3.4 ENTERPRISE AUDITING DATA ANALYTICS ..... 10
3.5 ENTERPRISE AUDITING SOLUTION MANAGEMENT ..... 11
3.6 ENTERPRISE AUDITING GOVERNANCE ..... 11
3.7 ALIGNMENT TO THE TECHNICAL REFERENCE MODEL (TRM) ..... 12

**4 USE CASES ..... 12**

4.1 INSIDER THREAT INVESTIGATION ..... 13
4.2 ZERO DAY THREAT MONITORING ..... 13
4.3 FISMA AUDIT COMPLIANCE ..... 13
4.4 CUSTOM SOLUTION SECURITY MONITORING ..... 14
4.5 PRIVACY MONITORING ..... 14

**APPENDIX A. SCOPE ..... 15**

**APPENDIX B. DEFINITIONS ..... 17**

**APPENDIX C. ACRONYMS ..... 19**

**APPENDIX D. REFERENCES, STANDARDS, AND POLICIES ..... 21**


**FIGURES**


Figure 1: Enterprise Auditing Target Architecture ..... 9


**TABLES**


Table 1 Enterprise Auditing Design Goals ..... 2
Table 2 Enterprise Auditing Target State Benefits ..... 7
Table 3 List of Approved Tools or Standards for Enterprise Auditing ..... 12

# 1 INTRODUCTION

VA has many applications in use by numerous users from various locations at any point in time. VA is responsible for monitoring use of IT resources to prevent misuse. VA Enterprise Auditing is the review of audit log data to determine the appropriateness of authentication, authorization, and access. Due to the volume of data and variety of sources, a solution is needed to manage the analysis of these logs in an efficient and effective manner. This solution is referred to as a Security Information and Event Management (SIEM) solution and is the primary focus of this Enterprise Design Pattern. This includes the collection and storage of audit events for use in security monitoring, trending, and reporting.

## 1.1 BUSINESS NEED

This Enterprise Design Pattern establishes the official enterprise guideline for enterprise-wide auditing across all lines of business in accordance with Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) 800-53 and VA 6500 security policies (see Appendix D). Currently, NIST requires that VA must create, protect, and retain information system audit records needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. This approach ensures that the actions of individual information system users can be uniquely traced to those users, holding them accountable for their actions. The VA Office of the Inspector General (OIG) also audits that VA consistently reviews security violations and audit logs supporting mission-critical systems each year. Recommendations were included in the last FISMA audit for VA to audit access logs and perform centralized reviews of security violations.

Enhancements to VA's operational model described in this document will also provide the ability for business units across VA to perform security monitoring and analysis effectively for their area of responsibility. An enterprise-wide approach to Enterprise Auditing security provides the following benefits:

**Table 1 Enterprise Auditing Design Goals**

| Business Benefits | Description |
|---|---|
| **Greater value from investment in security technology** | • An Enterprise Auditing solution will enable more effective use of the security log and event information, thereby allowing VA Security Teams to realize more fully the potential of security systems. |

| Business Benefits | Description |
|---|---|
| **Comprehensive and efficient reporting** | • Developing and delivering reports to meet multiple assurance and regulatory requirements can be a daunting task; consolidating audit logs into a single solution can greatly reduce reporting tasks freeing security teams to better focus on higher priority responsibilities. |
| **Reduced capital and operational costs** | • Converging multiple existing tools into a single Enterprise Auditing solution with a shared architecture will enable VA to save time and money by reducing licensing costs and the amount of training and professional support needed for solution use. |
| **Reduced risk of noncompliance** | • During audits or investigations VA leaders will have a single source of information to demonstrate compliance and due diligence. |
| **Broader organizational support for information security** | • The Enterprise Auditing solution enable more stakeholders to evaluate events, create reports and take actions to perform security monitoring and reporting using the Enterprise Auditing solution. These activities will help break down organizational silos and create a broader and more consistent culture of security and overall risk management. |
| **More comprehensive detection of security incidents** | • Events will be captured, tracked, monitored and flagged in near real-time with fewer gaps created between monitoring groups. |
| **More efficient use of network resources** | • A single solution will prevent the same event logs from being transported to multiple locations for different business needs. |

## 1.2 APPROACH

The Enterprise Auditing Design Pattern provides a vendor-agnostic SIEM framework that can be applied to VA's Enterprise IT Systems. The integration of this framework will require the following steps to take place:

1. **Establish Governance-** In order to operate an enterprise SIEM solution, a single owner will provide governance and guidance over the deployment and use of the solution by all stakeholders.

2. **Systems analysis-** Analyze the ability of existing solutions to meet the requirements of an enterprise SIEM solution, the cost of each compliant solution and select a single path forward.
3. **Systems Design-** Describe desired solution architecture, features, and operations in detail, outlining business rules, process diagrams, and other documentation.
4. **Implementation-** Procure the solution and create a transition plan to move from disparate solutions to a single enterprise SIEM solution. Communicate the transition plan to stakeholders.
5. **Deployment-** Deploy the enterprise SIEM solution and transition existing solutions.
6. **Maintenance-** Operate the solution and integrate with stakeholders to allow access and meet business requirements.

## 2 CURRENT CAPABILITIES AND LIMITATIONS

VA currently has multiple solutions managed by separate groups that monitor a percentage of the available audit logs. The lack of an enterprise audit capability significantly increases VA's administrative burden and technology overhead; causing VA to manage multiple siloed, solutions which makes creating a comprehensive view of the enterprise very difficult. A lack of an adequate central repository for audit log retention also contributes to systems not generating or discarding events to preserve disk space on production assets.

---

**VA-NSOC SIEM capabilities:** The VA Network Security Operations Center (VA-NSOC) provides network and security incident management capability for the VA Enterprise. The NSOC monitors overall health of the WAN, in addition to performing Continuous Monitoring (CONMON) and Incident Response activities.
**SIEM Solution:** Splunk
**SIEM Licensing:** Finite amount of Indexed Data
**SIEM Scope:** VA-NSOC currently collects logs from the TIC Gateway security stack, WAN monitoring (Cisco, Solarwinds, MPLS) and some LAN monitoring such as IPS and NAC. More sources are in progress.
**Limitations:**

- VA-NSOC does not ingest logs for endpoints such as Windows logs, McAfee events or from other endpoint agents. Application, some server events and authentication logs are also not ingested.
- VA-NSOC has the ability to connect to Regional Splunk instances, but does not connect to other SIEM solutions.

---

**Field Security Service (FSS) SIEM capabilities:** FSS has deployed its own instances of Splunk to VA Regions for monitoring critical applications as part of the National Security Event Monitoring (NSEM) project.

**SIEM Solution:** Splunk
**SIEM Licensing:** Finite amount of Indexed Data
**SIEM Scope:** Logs include a very limited set of Windows events, some Linux events and syslog from network devices.
**Limitations:**

- Each Region has their own solution to maintain with licensing.
- Audited log scope if limited.
- VA-NSOC is dependent on the Regional deployments to ingest some logs.
- Log retention is 3 to 6 years and not aligned to an enterprise audit log retention plan.

---

**EOC SIEM capabilities:** The Enterprise Operations Center (EOC) provides security monitoring and vulnerability scanning services for five (5) VA data centers.
**SIEM Solution:** IBM QRadar
**SIEM Licensing:** Events per Second (EPS), Flows per Minute (FPM)
**SIEM Scope:** EO-managed data center assets only. Includes network firewalls, web application firewalls, IPS, Malware Protection and vulnerability scanning solutions.
**Limitations:**

- Preconfigured correlations are dependent on ingestion of required logs.
- Primarily for real-time correlation and not historical searches where performance lags or events must be resent to the SIEM.

---

**Compliance, Auditing and Reporting (CAR) SIEM capabilities:** VA Identity and Access Management (IAM) team currently provides an auditing solution which monitors user transactions. The IAM solution is called the Compliance, Auditing, and Reporting (CAR) Service which provides centralized monitoring, alerting, and auditing, as well as compliance reporting in association with the Access Services Solution (AcS). It establishes a compliance auditing framework that will provide the protections and security for the audit data as required. Currently, the CAR service integrates with multiple solutions that provide IAM services.

**SIEM Solution:** User Activity Reporting Module (UARM) from Computer Associates (CA) Technologies
**SIEM Licensing:** User-based volume licensing– Product End of Life (EOL) on 12/31/2017
**SIEM Scope:** Ingests events via logs and ODBC connections from nine (9) VA IAM applications.
**Limitations:**

- Does not perform real-time event monitoring.
- Uses a fixed schema database for event storage which restricts scaling. Events must be normalized for ingestion, which raises the level of effort for new data sources and does not store raw logs for compliance.
- Suffers from performance issues including query timeouts.

**Personal Identify Verification (PIV) SIEM capabilities:** The VA PIV project uses a SIEM as part of its Performance Monitoring Tools (PMT) for log management and event analysis.
**SIEM Solution:** LogRhythm
**SIEM Licensing:** Perpetual with annual support contract required for updates.
**SIEM Scope:** Ingests events from PIV servers and Nagios Appliance.
**Limitations:**

- Requires separate licensing and support contract
- Ingests logs that may be used by other stakeholders

---

**Office of Cyber Security (OCS) SIEM capabilities:** OCS has procured support to design and deploy a "Predictive Analytics" solution.
**SIEM Solution:** N/A, solution is still under evaluation.
**SIEM Licensing:** N/A, projected use of Open Source solutions.
**SIEM Scope:** "Big Data" solution will use data from OCS and VA-NSOC to perform analysis related to application layer attacks, zero day attacks, third party attacks, behavior patterns and anomaly detection. Includes real-time and historical analysis.
**Limitations:**

- Despite efforts to avoid redundancy, the nature of the desired results dictates the use of logs already in scope for other previously listed solutions.
- A "Big Data" solution alone may be insufficient for visualization of real-time analytics desired and require a different set of support skills to create queries and visualizations than other SIEM stakeholders.

# 3 FUTURE CAPABILITIES

An Enterprise SIEM tool will have the ability to collect, aggregate, filter, and store security events for triage, correlation, trending, reporting, and compliance, offering both real time and historical analytics. The Enterprise Auditing solution will be an Enterprise Shared Service (ESS) that can support the business requirements of multiple stakeholders throughout VA requiring security event analytics and reporting. Older SIEM strategy focused on reducing events for analysis. New SIEM strategy focuses on including more events for analysis to provide context and relationships for deeper insights. A centralized data repository will enable this potential for all stakeholders. The table below reviews some of the specific areas of projected improvement over the current state by adopting an Enterprise Auditing solution.

**Table 2 Enterprise Auditing Target State Benefits**

| Area | Current State | Future State |
|---|---|---|
| **Licensing** | • Multiple products using disparate or duplicative licensing models. | • A single or reduced set of licensing that takes greater advantage of volume discounting. |
| **Log Collection** | • Separate archives of logs in different locations. Not all events are collected. Not all collected events are retained in an unmodified (raw) state. | • A single repository of audit events that can be accessed by multiple stakeholders that retains all raw logs for compliance. |
| **Log Retention** | • Multiple log retention policies with different timeframes. | • A single log retention strategy that meets compliance and optimizes online storage. |
| **Reporting/Analytics** | • Some solutions only support real-time analytics while others only support historical reporting. Only a portion of the solutions support both. | • All stakeholders have access to real-time analytics and historical reporting capabilities using a common interface. |

| Area | Current State | Future State |
|---|---|---|
| **Scalability** | • Some solutions are not designed for a high volume of events and have performance issues. | • A scalable solution that can scale to the volume required by VA without using proprietary hardware making it cloud-ready. |
| **Compatibility** | • Some solutions are designed to ingest logs of varying formats while others require a high level of effort to normalize events. Third party agents may be needed. | • A consistent strategy is used to efficiently ingest events of all types and formats into the solution. |
| **Compliance** | • Creating artifacts for compliance requires multiple reports from disparate systems. | • Compliance can be demonstrated using reports from a single solution. |

The Enterprise Audit Solution will address five major areas.

- **Data Sources** – The source of events which need to be ingested by the SIEM solution in order to meet compliance requirements and provide the desired level of security monitoring. This area impacts the SIEM solution scaling and requirements for handling different types of logs and data.
- **Data Transfer** – Logs must be transported to the SIEM solution in some manner. This may include Syslog or require installed agents to collect and send logs. A distributed architecture may be required to control the aggregation and transport of events and to meet network management requirements.
- **Data Repository** – A SIEM solution must keep the "raw" event in its original state for compliance purposes. It may also normalize events for correlation or analytic purposes. While the SIEM supports the correlation of events in real-time as events are received, the data repository is required for historical searches or time-based analytics.
- **Data Analytics** – This is the core function of the SIEM. The SIEM is simply an application that performs analytics using security events often referred to as "correlations". This can be real-time correlations or historical trending. Simple correlations comparing two conditional events have been replaced by the need to perform more complex analysis of relationships between events, configurations, users, time, location, and other data.
- **Solution Management** – This is the component that provides governance over the SIEM solution. This should include access control, solution performance monitoring, workflows, data governance, and policy enforcement.

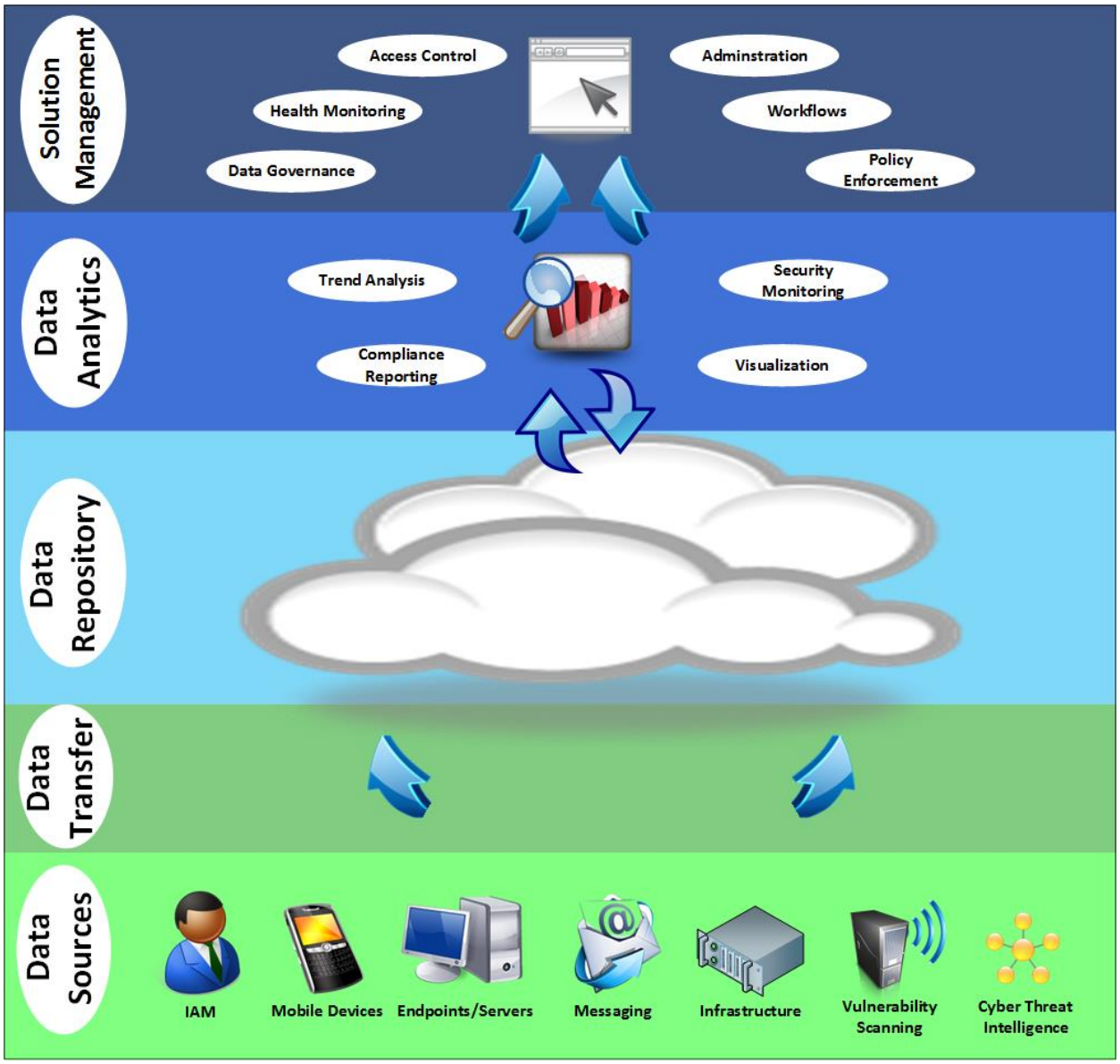


**Figure 1: Enterprise Auditing Target Architecture**

The following subsections will describe the best practice capabilities and Enterprise Audit design goals for each of the major areas in more detail.

## 3.1 ENTERPRISE AUDITING DATA SOURCES

*Establish an Enterprise Auditing solution that has the flexibility to use many data sources with a minimal Level of Effort.* The following capabilities represent the target features for supporting the many data sources that exist across VA:

- Ability to ingest audit events with minimal configuration needed for import
- Built in data classification that identifies relevant event fields

- Supports a wide range of audit events including security events, application events, network flows, full packet capture, audit logs, mobile data, threat intelligence, and other data formats such as unstructured data

### 3.2 ENTERPRISE AUDITING DATA TRANSFER

*Design a plan for data transfer of audit events that accounts for network bandwidth and prevents data loss.* Transferring all data across the network directly to a central repository may be impractical. In some cases, data loss can occur when the receiver becomes unavailable and the sending device is not able to compensate. The following areas should be addressed to ensure reliable data transfer:

- Distributed architecture for load balancing and event routing
- Management and reporting on status of audit event collection (success/fail)
- Prevention of audit event data loss due to solution downtime (High Availability architecture, redundancy, etc.)

### 3.3 ENTERPRISE AUDITING DATA REPOSITORY

*Establish a single, logical data repository to simplify governance and compliance.* Multiple stakeholders require access to overlapping sets of data to achieve their required business intelligence. A central repository will enable efficient stakeholder support and security monitoring while meeting VA and FISMA policy compliance. The following features will enable a robust solution:

- No logical limit to the ability to scale for data collection and retention
- Scalability of the solution is not reliant on hardware proprietary to the Enterprise Auditing software vendor which allows for future cloud migration
- Ability to design hot, warm, and cold audit event storage policies to maximize resources
- Maintains raw (not normalized) events for compliance. Events should be immutable (unaltered)
- Supports compression to reduce storage cost

### 3.4 ENTERPRISE AUDITING DATA ANALYTICS

*Select a SIEM platform that supports advanced analytics at the scale required by VA.* The ability to perform analytics efficiently is a core functionality of the SIEM. VA has a large enterprise which makes performance at scale a significant concern. Reports that take from minutes to hours to run could hinder security monitoring and investigations. This solution will also support multiple stakeholders of varying needs. Flexibility is needed to create visualizations and reports quickly. While out of the box rules and report templates are often provided, these should not be too heavily weighted as a decision factor as they may provide limited value because they are

designed based on expected event types that may not exist, may not match the target environment or contain very basic logic. The level of effort to customize the solution to meet stakeholder needs is important. Areas below are key considerations of the analytic function:

- Provides a single console that is easily accessible by users
- Supports real-time correlation and historical searching
- Enables High Availability (HA) design to minimize downtime
- Parallel processing is used to provide fast search results over large volumes of data
- Supports metadata tagging of audit events
- Supports machine learning
- Reporting options support customization achievable by the average solution user including creation of metrics and visualizations.
- Self-paced resources for user training are available up through an advanced level
- Extensible, if required to support advanced use cases
- Supports compliance against common technical controls such as FISMA, PCI, etc.

### 3.5 ENTERPRISE AUDITING SOLUTION MANAGEMENT

*Select a SIEM platform that supports data governance, access control, policy enforcement, solution management and workflow design.* As an enterprise solution used by multiple stakeholders, the Enterprise Auditing solution must provide the ability to govern who has access to which dataset to maintain least privilege required by VA policy. It should also simplify the monitoring and management of a complex solution to ensure data is not lost. Features required for this area are:

- Provides granular access controls to data for maintaining least privilege access for multiple stakeholders
- Customizable workflows for investigation and escalation that can integrate with external systems, as necessary
- Alerting that supports customizable actions
- Enables monitoring of the solution integrity from data collection to archive
- Supports policy compliance such as log retention, log integrity and others
- Supports compliance frameworks relevant to VA
- Has the capability to migrate to the cloud

### 3.6 ENTERPRISE AUDITING GOVERNANCE

*Establish governance for the Enterprise Auditing solution.* VA has at least six (6) stakeholders using a type of SIEM or log management solution that falls within the scope of Enterprise Auditing and there may be more. It is not possible for each stakeholder to track the technology in use by all the others and evaluate business needs that extend beyond their own. Responsibility should be assigned to provide governance over the deployment of an enterprise

auditing solution within VA to ensure all business needs are met while making the most efficient use of resources. The governance group should accomplish the following at a minimum:

- Audit the needs of all stakeholders and VA overall, selecting a solution with enough flexibility to meet VA needs
- Plan, communicate, and manage the transition to an Enterprise Auditing solution
- Enforce least privilege access and data governance by controlling access to the Enterprise Audit solution and the data sets available to each role
- Monitor the integrity and compliance of the Enterprise Auditing solution

### 3.7 ALIGNMENT TO THE TECHNICAL REFERENCE MODEL (TRM)

The Enterprise Auditing solution leverages approved tools and standards catalogued in the Technical Reference Model (TRM). The following table includes a mapping of technology categories to approved technologies or standards and indicates any mandated by ESS which are required by all VA projects.

**Table 3 List of Approved Tools or Standards for Enterprise Auditing**

| Technology Category | Example Technologies | Example Standards | Mandated ESS |
|---|---|---|---|
| **Monitoring** | CA User Activity Reporting Module, ElasticSearch Logstash, Microsoft System Center Operations Manager (SCOM), Splunk, SolarWinds Log and Event Manager (Requested) | | |
| **Security Event and Information Management** | QRadar, LogRhythm (Requested), Splunk Enterprise Security (Requested) | | |
| **Platforms and Storage** | Hortonworks Data Platform | | |

http://trm.oit.va.gov/TRMHomePage.asp

## 4 USE CASES

The following sections describe some general use cases that could apply to the use of security audit events via the Enterprise Auditing solution.

## 4.1 INSIDER THREAT INVESTIGATION

A business unit is concerned that a system administrator is leveraging their privileged access to collect sensitive information and share it with a third party with whom they are seeking employment.

- The business unit is able to gain support for the analysis as many users are trained on the Enterprise Auditing solution since it is used by multiple stakeholders.
- A query is made through the Enterprise Auditing Solution over the past 90 days to report on systems to which the user authenticated with their account using authentication logs archived by the solution.
- Firewall and Web Content Filtering event logs are used to report on related events of file transfers external to VA.
- An automated real-time alert is set up for the business unit to notify them if the user account is used to access a specific file server.

## 4.2 ZERO DAY THREAT MONITORING

The network security threat intelligence unit reports a credible new threat that exploits a vulnerability on web servers for which there is currently no patch.

- The security monitoring team creates a custom signature to detect exploit attempts within their web application firewall solution. This solution is already monitored by the Enterprise Auditing solution, so alerting is immediately possible and is configured to allow 24/7 support analysts to monitor for the signature to trigger until a patch is available and deployed.
- Web application events are logged to the repository. Security analysts perform a search over the past 30 days to determine if there was any evidence of unauthorized access or data loss.

## 4.3 FISMA AUDIT COMPLIANCE

The Office of the Inspector General (OIG) is conducting their annual FISMA audit. They have requested evidence that VA consistently reviews security violations and audit logs.

- VA creates a report for the OIG auditor that displays the types of audit events collected and the number of unique hosts being monitored. As all audit events are centralized, the report is comprehensive.
- VA is able to create a report on the number of queries created by all stakeholders across all VA for the purpose of monitoring security violations. The use of a single Enterprise Auditing solution across all stakeholders allows this report to be created efficiently.
- VA demonstrates a consistent retention plan for audit trails

## 4.4 CUSTOM SOLUTION SECURITY MONITORING

A business unit needs to audit the security of their service line and are concerned because their solution uses a custom platform where audit records are stored in a proprietary format.

- The business unit contacts the Enterprise Auditing Program Management Office (PMO) to coordinate a solution.
- A new solution is not needed as the Enterprise Auditing solution is able to ingest their custom log format.
- Their logs are ingested to the EA solution and the PMO provides access to their logs through the web-based console as well as login information associated with their system from the existing authentication logs.
- The business unit is able to gain support for their required analysis as many users are trained on the Enterprise Auditing solution since it is used by multiple stakeholders. Self-paced training is also available for their admins to learn to create their queries and alerts.
- Alerting is established to notify the business unit when conditions occur about which they are concerned.

## 4.5 PRIVACY MONITORING

A Veterans Affairs Medical Center (VAMC) would like to monitor access to medical records for Health Insurance Portability and Accountability (HIPAA) compliance to prevent unauthorized access.

- The VAMC contacts the Enterprise Auditing PMO to gain access to existing authentication logs.
- Authentication must be correlated against medical record access logs and patient discharge dates. This information is imported into the Enterprise Auditing solution and access to the data is restricted to only the VAMC authorized staff.
- Alerting is created to notify the VAMC of patterns of access that may be unauthorized. The alerts can be forwarded to their own system for investigation workflow and tracking.

# APPENDIX A. SCOPE

VA currently has a limited ability to capture/share, audit identification, authentication, and authorization data across enterprise boundaries. The lack of an enterprise audit capability significantly increases VA's administrative burden and technology overhead; causing VA to manage multiple siloed, incompatible, and logging solutions. Improving these systems will reduce cybersecurity risk, while improving business processes and achieving efficiencies. This Enterprise Design Pattern outlines the need for a robust enterprise auditing solution that will centrally store and interpret logs, enabling VA's security personnel to make defensive/preventive actions more effectively. The approach in this document will outline the following:

- Ensure that the system is able to collect data in a central repository for trend analysis and provide a mechanism to automate reporting
- Ensure that systems comply with FISMA, PCI, HIPAA, PII, PHI, sensitive data and legal requirements
- Automate and improve accuracy by certifying that relevant security data about VA's enterprise systems is being produced/shared/captured from multiple strategically placed locations
- Confirm that security data is readily available from a single point of view; consequently making it easier to locate trends and identify patterns
- Enable audit event data collection in a hierarchical manner throughout VA's enterprise to gather security-related event data from IAM / SOA systems, end-user devices, servers, network equipment, firewalls, antivirus and intrusion prevention systems.

This Enterprise Design Pattern will assist VA in establishing policy and methodology related to auditing and monitoring users across all VA IT systems. Although Enterprise Auditing relies on these areas, this Enterprise Design Pattern does not address configuration of audit policy settings on devices or time synchronization on systems that need to be monitored.

**Document Development and Maintenance**

This Enterprise Design Pattern was developed collaboratively with stakeholders from the ESS Security Group and included participation from VA's Office of Information and Technology (OIT), Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). In addition, the Technology Strategies team engaged industry, external government agencies, and academic experts to review, provide input, and comment on the document. This document contains a revision history and revision approval logs to track all changes. Updates need to be coordinated with the Office of Technology Strategies' lead for this document; they will facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

## APPENDIX B. DEFINITIONS

**Access** – Interaction with a computer system for instance VistA. Such interaction includes data retrieval, editing (create, update, delete) and may result from a variety of technical mechanisms including traditional user log on, consuming applications exercising middleware based connectivity, SOA service requests, etc.

**Accurate, unambiguous user identity** – Information that represents the actual human that is interacting with a computer system, including the initiation of that interaction.

**Application proxy –** Construct involving the use of a generic, non-human "user" entity to represent "machine-to-machine" interaction where appropriate for interactions that do not involve a specific end user.

**Auditing** – The inspection or examination of an activity based on available information. In the case of computer systems, this is based on review of the events generated by the system or application.

**Consuming application** – The application consuming services from a provider system. Generally used when discussing a front-end application supporting a user, but even service providers can themselves be a consumer of other services.

**Enterprise Service Bus (ESB)** – An SOA infrastructure device which manages message traffic, routing and a variety of other functions for instance orchestration, mediation, etc. The primary ESB at VA is the Enterprise Messaging Infrastructure (eMI).

**Enterprise Shared Service (ESS)** – A SOA service that is visible across the enterprise and can be accessed by users across the enterprise, subject to appropriate security and privacy restrictions.

**Identity attributes** – Characteristics which describe the user (e.g. name, National Provider Identifier, organization, etc.). Establishment of reasonably reliable "unique identity" is generally based on a combination of multiple identity attributes. Specific user identifiers include employee number and email address; may vary from organization to organization but identifier types ought to remain constant for all transactions from a specific organization.

**Machine-to-machine interaction** – In some cases, application processes resulting from workflow (not human interaction) will result in interaction with provider systems to download

data, initiate background processing, etc. These actions are not directly initiated by a specific human and the interaction would be attributed to an application, possibly via a service account.

**Provider system** – A system (e.g. VistA) which *provides* service at the request of a consuming application.

**SAML token** – An XML-based open standard data format for exchanging authentication and authorization data between parties.

**Service Oriented Architecture** – A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations

**User** – A person that interacts with a computer system application. In this context, a "user" is not limited to VA staff members and may include persons from external organizations, patients, beneficiaries, designees, etc.

**SSO and User Provisioning** – A services provided by Identity and Access Management (IAM) for authenticating users and providing user provisioning information to other systems.

**User types** – traditional types including VA staff, staff of non-VA agencies (e.g. DoD), staff of private sector organizations (e.g. Walgreens); nontraditional, non-staff types including patients, beneficiaries, designees, sponsors, caregivers, etc.

**VistA 'Visitor' record** – in conjunction with VistA Kernel, CPRS established an approach for recording "local" users on "remote" VistA systems so that had not previously had a user record (File 200, New Person file) record on file for that person. These records facilitate VistA auditing and role-based access logic as intended. However they do not have access/verify codes that would allow remote users to log on independently of the external application (e.g. CPRS) or exercise functionality that is not allowed by that application.

## APPENDIX C. ACRONYMS

| Acronym | Description |
|---|---|
| AD | Active Directory |
| API | Application Program Interface |
| ASD | Architecture, Strategy and Design |
| CDW | Corporate Data Warehouse |
| CPRS | Computerized Patient Record System |
| CSP | Credential Service Provider |
| eMI | Enterprise Messaging Infrastructure |
| ESB | Enterprise Service Bus |
| ESS | Enterprise Shared Service |
| FICAM | Federal Identity, Credential, and Access Management |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Management Act |
| HIPAA | Health Insurance Portability and Accountability Act |
| HTTPS | Hypertext Transfer Protocol over TLS |
| IAM | Identity and Access Management |
| MHV | MyHealtheVet |
| IdP | Identity Provider |
| JMS | Java Messaging Service |
| KAAJE | Kernel Authentication and Authorization for Java 2 Enterprise Edition |
| LDAP | Lightweight Directory Access Protocol |
| LoA | Level of Assurance |
| M4A | Minimum 4 Attributes |
| MDWS | Medical Domain Web Services |
| NIST | National Institute of Standards and Technology |
| PCI | Formally known as Payment Card Industry Data Security Standard (PCI-DSS) |
| PKI | Public Key Infrastructure |
| PIV | Personal Identity Verification |
| REST | Representational State Transfer |
| RPC | Remote Procedure Call |
| SAML | Security Assertion Markup Language |
| SDD | System Design Document |
| SPML | Service Provisioning Markup Language |
| SOA | Service-Oriented Architecture |
| SSOe/SSOi | Single Sign-On External/Internal |
| TLS | Transport Layer Security |
| TPM | Trusted Platform Module |
| TRM | Technical Reference Model |

| Acronym | Description |
|---|---|
| VHA | Veteran Health Administration |
| VistA | Veterans Health Information Systems and Technology Architecture |
| XML | Extensible Markup Language |

## APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This Enterprise Design Pattern is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, and are aligned to the VA ETA:

| # | Issuing Agency | Applicable Reference/Standard | Purpose |
|---|---|---|---|
| 1 | VA OIS | VA 6500 Handbook | Directive from the OI&T OIS for establishment of an information security program in the VA, which applies to all applications that leverage ESS. |
| 2 | U.S. Army | U.S. Army – Identity and Access Management (IdAM) Reference Architecture (RA) v2.0 | Provides guidance on Enterprise Auditing from an Army perspective http://ciog6.army.mil/Portals/1/Architecture/ArmyIdentityandAccessManagement(IdAM)ReferenceArchitectureV2.pdf |
| 4 | DOD | DoD IdAM Strategy | Provides guidance on Enterprise Auditing http://csrc.nist.gov/projects/abac/july2013_workshop/july2013_abac_workshop_howard.pdf |
| 5 | NIST | NIST Special Publication 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations | Provides guidance on Enterprise Auditing http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf |
| 6 | OMB | Federal Information Security Management Act (FISMA) of 2002 | For information systems to ensure compliance with the Federal Information Security Management Act (FISMA) of 2002 they needs to implement a foundational level of security controls outlined in the. FIPS 200 states that, “Organizations needs to identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.” |

| # | Issuing Agency | Applicable Reference/Standard | Purpose |
|---|---|---|---|
| 7 | OMB | Federal Information Processing Standard (FIPS) 200 and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 | Special Publication 800-53, Revision 4, provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber attacks and other threats.<br><br>http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf |
| 8 | NIST | NIST 800-63-2: Electronic Authentication Guideline standards | VA has adopted NIST risk management framework, NIST 800-63-2: Electronic Authentication Guideline standards for rating application Levels of Assurance (LOA) and aligning appropriate authentication protocols to the level of risk posed by those applications. |
| 9 | OMB | Approved Identity Services in US Government | Ihttp://www.idmanagement.gov/approved-identity-services |
| 10 | VA ASD | VA Enterprise Design Patterns, Office of Technology Strategies | Provides references to the use of enterprise capabilities as part of the integration with IAM services. These documents are intended to standardize and constrain the solution architecture of all applications in VA.<br>http://www.techstrategies.oit.va.gov/enterprise_dp.asp |
| 11 | VA ASD | Full range of technologies provided by the TRM | http://www.va.gov/TRM/ReportVACategoryMapping.asp |
| 12 | VA ASD | Enterprise Technology Strategic Plan (ETSP) | http://www.techstrategies.oit.va.gov/ETSP.asp |

| # | Issuing Agency | Applicable Reference/Standard | Purpose |
|---|---|---|---|
| 13 | NIST | Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules” | http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf |
| 14 | OMB | FIPS Pub 201, “Personal Identity Verification of Federal Employees and Contractors,” March 2006 | http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf |
| 15 | DOD | 10 U.S.C. § 2224, "Defense Information Assurance Program" | http://csrc.nist.gov/nissc/1999/proceeding/papers/o32.pdf |
| 25 | DHS | Homeland Security Presidential Directive (12) (HSPD-12) | http://www.dhs.gov/homeland-security-presidential-directive-12 |
| 26 | VA | VA Directive 6500, “Information Security Program,” August 4, 2006 | http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=637&FType=2 |
| 27 | VA | VA Handbook 6500, “Information Security Program,” September 18, 2007 | http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=637&FType=2 |
| 28 | VA | VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle | http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=637&FType=2 |

| # | Issuing Agency | Applicable Reference/Standard | Purpose |
|---|---|---|---|
| 30 | VA | Program Management Accountability System (PMAS) portal | https://www.voa.va.gov/) |
| 31 | VA | OED ProPath Process Methodology ( | https://www.voa.va.gov/) |
| 34 | VA | **Security Information and Event Management (SIEM) Solution** TAC Number: TAC-14-13183 | https://www.vendorportal.ecms.va.gov/ |
| 35 | OMB | The Office of Management and Budget (OMB) Circular A-130, Appendix III; Security of Federal Information Resources | https://www.whitehouse.gov/omb/circulars_a130_a130trans4/ |
| 36 | | **National Institute of Standards and Technology (NIST) Special Publication, (SP) SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations** | http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf |
| 37 | | **"Enhancing the Security of Federal Information and Information Systems", OMB Memorandum M-14-03,** | http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf |