pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Security Information and Event Management Policy

ITP Number	***Effective Date***
ITP-SEC021	October 10, 2006
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	Annual

This Information Technology Policy (ITP) establishes enterprise-wide guidelines and standards for the procurement of Security Information and Event Manager (SIEM) solutions.

1. Purpose

This policy provides guidelines and standards that agencies must adhere to when procuring a Security Information and Event Managers (SIEM) solution. SIEMs are used to provide real-time analysis of security alerts which are generated by network hardware and applications. SIEMs automate the collection of event data from security devices, such as firewalls, proxy servers, intrusion-detection systems and antivirus software. The SIEM translates the logged data into correlated and simplified formats for real-time alerting and reporting capabilities.

In addition to guidelines to be followed in selecting an SIEM solution, this policy provides agencies with information on how to leverage the Office of Administration, Office for Information Technology (OA/OIT) SIEM solution that can provide agencies with the following services:

- Log collection and consolidation.
- Security event collection from multiple sources (firewalls, routers, servers, etc.).
- Identification of security related events and incidents.
- Some form of automated response/alerting capability when incidents are detected.
- Correlation of events from multiple sources.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Definitions

Event - An observable occurrence in a system or network. Events include, but are not limited to, a user connecting to a file share, a server receiving a request for a Web page, a user sending electronic mail (e-mail), and a firewall blocking a connection attempt.

Event Correlation - The process of monitoring events in order to identify patterns that may signify attacks, intrusions, misuse or failure.

Incident - A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of an incident are denial of service, malicious code, unauthorized access and inappropriate usage.

Incident Response - The manual and automated procedures used to respond to reported incidents (real or suspected), system failures and errors, and other undesirable events.

Log - A file that lists actions that have occurred.

Security Information and Event Managers (SIEM) – A SIEM is a set of tools used by IT professionals and system administrators to manage multiple security applications and devices, and to respond automatically to resolve security incidents and provides real-time monitoring and historical reporting of information security events from networks, servers, systems, applications and more.

4. Policy

Agencies that desire leveraging the Enterprise SIEM solution should contact the EISO Office at ra-ciso@pa.gov.

Agencies that have a SIEM solution or that are looking to procure a new SIEM solution must comply with the standards identified in the following section.

5. Standards

Agencies looking to procure a SIEM solution must ensure that it has the ability to provide the agency with the following critical capabilities:

Scalable Architecture and Deployment Flexibility: These are derived from vendor design decisions in the areas of product architecture, data collection techniques, agent designs and coding practices. Scalability can be achieved by:

- A hierarchy of SIEM servers — tiers of systems that aggregate, correlate and store data.
- Segmented server functions — specialized servers for correlation, storage, reporting and display.
- A combination of hierarchy and segmentation to support horizontal scaling.

During the planning phase, agencies should take into consideration the volume of event data that will be collected, as well as the scope of analysis reporting that will be required. An architecture that supports scalability and deployment flexibility will enable an agency to adapt its deployment in the face of unexpected event volume and analysis.

Real-time Event Data Collection: SIEM products collect event data in near real time in a way that enables immediate analysis. Data collection methods include:

- Receipt of a syslog data stream from the monitored event source.
- Agents installed directly on the monitored device or at an aggregation point, such as a

syslog server.
- Invocation of the monitored system's command line interface.
- Application Programming Interfaces (APIs) provided by the monitored event source.
- External collectors provided by the SIEM tool.

The technology should also support batch data collection for cases where real-time collection is not practical or is not needed. Filtering options at the source also are important methods of data reduction, especially for distributed deployments with network bandwidth constraints.

Agent-based collection options and virtualized SIEM infrastructure options will become more important as organizations move workloads to virtualized and public infrastructure as a service cloud environments. A large percentage of organizations that have deployed SIEM technology must integrate data sources that aren't formally supported by the SIEM vendors.

SIEM products should provide APIs or other functions to support user integration of additional data sources. This capability becomes more important as organizations apply SIEM technology for application-layer monitoring.

Event Normalization and Taxonomy: This is a mapping of information from heterogeneous sources to a common event classification scheme. A taxonomy aids in pattern recognition, and also improves the scope and stability of correlation rules. When events from heterogeneous sources are normalized, they can be analyzed by a smaller number of correlation rules, which reduces deployment and support labor. In addition, normalized events are easier to work with when developing reports and dashboards.

Real-time Monitoring: Event correlation establishes relationships among messages or events that are generated by devices, systems or applications, based on characteristics such as the source, target, protocol or event type. There should also be a library of predefined correlation rules and the ability to easily customize those rules. A security event console should provide the real-time presentation of security incidents and events.

Behavior Profiling: Behavior profiling employs a learning phase that builds profiles of normal activity for discrete event sources, such as NetFlow data, users, servers and so on. The monitoring phase alerts on deviations from normal. Profiling and anomaly detection are emerging capabilities in SIEM that complement rule-based correlation.

Threat Intelligence: Intelligence about the current threat environment exists in a variety of sources, including open-source lists, the threat and reputation content developed and maintained by security research teams within security vendors, and data developed by managed security and other service providers. Threat intelligence data can be integrated with an SIEM in the form of watch lists, correlation rules and queries in ways that increase the success rate of early breach detection.

Log Management and Compliance Reporting: Functions supporting the cost-effective storage and analysis of a large information store include collection, indexing and storage of all log and event data from every source, as well as the capability to search and report on that data. Reporting capabilities should include predefined reports, as well as the ability to define ad hoc reports or use third-party reporting tools.

Analytics: Security event analytics is composed of dashboard views, reports and ad hoc query functions to support the investigation of user activity and resource access in order to identify a threat, a breach or the misuse of access rights.

Incident Management Support: Specialized incident management and workflow support should be embedded in the SIEM product primarily to support the IT security organization. Products should provide integration with enterprise workflow systems, and should support ad hoc queries for incident investigation.

User Activity and Data Access Monitoring: This capability establishes user and data context, and enables data access and activity monitoring. Functions include integration with identity and access management (IAM) infrastructure to obtain user context and the inclusion of user context in correlation, analytics and reporting. Data access monitoring includes monitoring of database management systems (DBMSs), and integration with file integrity monitoring (FIM) and data loss prevention (DLP) functions. DBMS monitoring can take three forms — parsing of DBMS audit logs, integration with third-party database activity monitoring (DAM) functions or embedded DAM functions. FIM can be provided by the SIEM product directly or through integration with third-party products.

Application Monitoring: The ability to parse activity streams from packaged applications enables application-layer monitoring for those components, and the ability to define and parse activity streams for custom applications enables application-layer monitoring for in-house- developed applications. Integration with packaged applications, an interface that allows customers to define log formats of unsupported event sources, and the inclusion of application and user context are important capabilities that enable the monitoring of application activities for application-layer attack detection, fraud detection and compliance reporting.

Deployment and Support Simplicity: Deployment and support simplicity is achieved through a combination of embedded SIEM use- case knowledge, and a general design that minimizes deployment and support tasks. Embedded knowledge is delivered with predefined dashboard views, reports for specific monitoring tasks and regulatory requirements, a library of correlation rules for common monitoring scenarios, and event filters for common sources. There should also be an easy way to modify the predefined functions to meet the particular needs of an organization.

6. Responsibilities

Agencies are required to perform the actions outlined in this policy.

7. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

8. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	10/20/2006	Base Policy

Revision	5/9/2013	Updated the policy to reflect current standards making it easier for agencies to implement SIEM solutions. Rescinds STD-SEC021A and incorporates elements of OPD0SEC021B
	4/2/2014	ITP Reformat