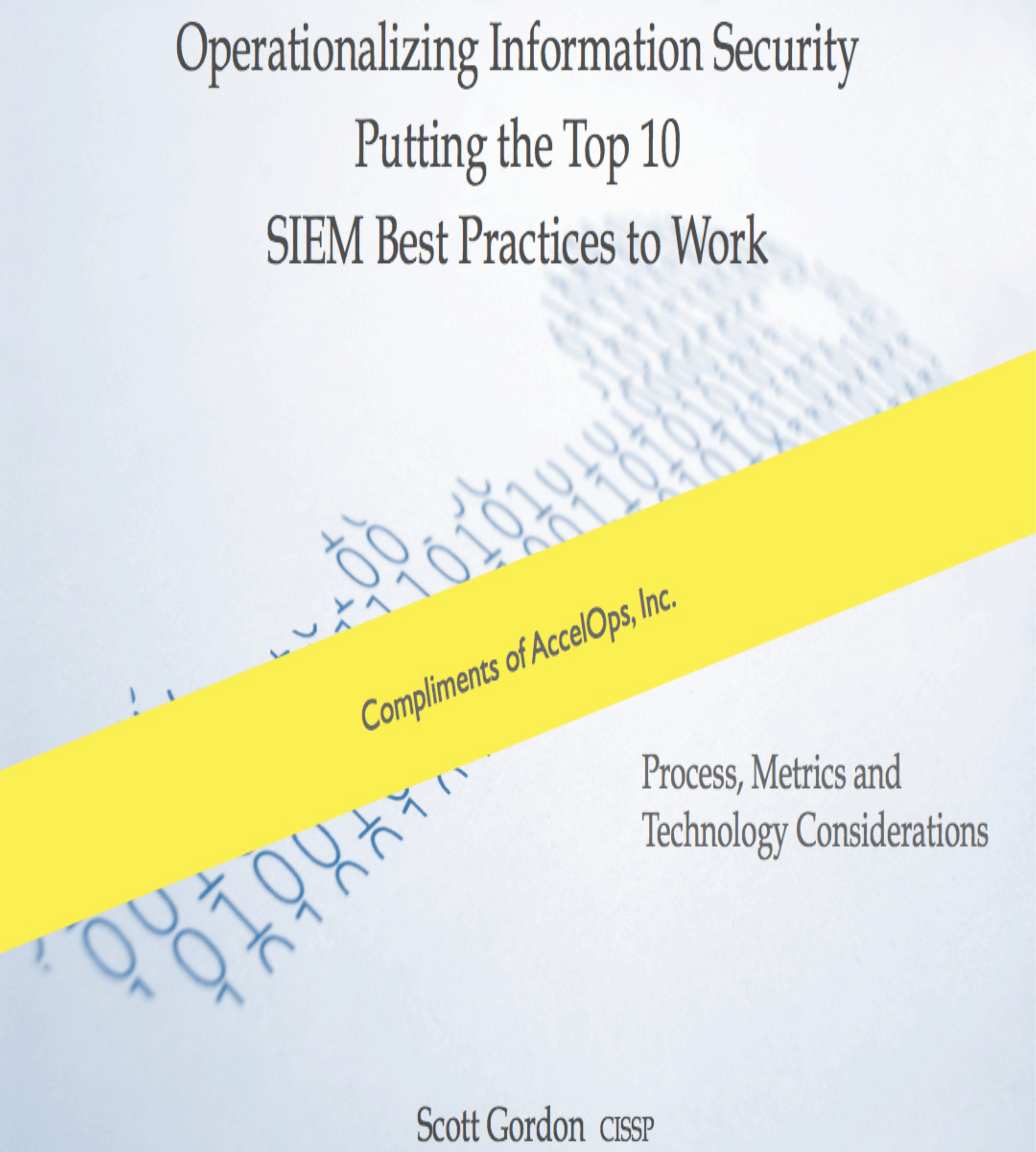
# Operationalizing Information Security
# Putting the Top 10
# SIEM Best Practices to Work



## Process, Metrics and Technology Considerations

Scott Gordon CISSP

# Introduction

**"Ask any security practitioner about their holy grail and the answer is twofold: They want one alert specifying exactly what is broken, on just the relevant events, with the ability to learn the extent of the damage. They need to pare down billions of events into actionable information. Second, they want to make the auditor go away as quickly and painlessly as possible, which requires them to streamline both the preparation and presentation aspects of the audit process. SIEM and Log Management tools have emerged to address these needs and continue to generate a tremendous amount of interest in the market, given the compelling use cases for the technologies.**
***Michael Rothman, Security Industry Analyst and President of Securosis***[1]

The use of Security Information and Event Management (SIEM[2]) as part of an integrated security management program is an information security best practice. The SIEM market category, beyond basic event logging, has been around since circa 1990's. Whether referring to security event management, security information management, log management systems or more modern combined industry solutions, SIEM user requirements and operational considerations have evolved. How can one ensure successful SIEM implementation and on-going improvement, while at the same time further optimize resources and accelerate return on investment?

This paper, provided as an e-book, provides guidance to operationalize security and put the top 10 best SIEM practices to work. Rather than an exhaustive examination of SIEM, the purpose is to offer pertinent insights and details with regards to how IT organizations and information security professionals can gain more assured value from SIEM.

Whether seeking to streamline incident response, automate audit and compliance processes, better manage security and business risks, or build out your deployed SIEM - this e-book presents process, metrics and technology considerations relative to SIEM implementation and security operations.

Each of the ten chapters referenced in the Table of Contents below offers:

- Overview and Highlight Processes: topic introduction, process considerations, exploring operational concerns, getting results, and avoiding common pitfalls
- Recommended Metrics: the more popular SIEM dashboards, reports, alerting and related operational measurements to support security operations, incident response and compliance
- Technology considerations: sources, controls and related SIEM functionality

### Table of Contents

Introduction ........ 2
What is a SIEM and What are the Top Ten SIEM Best Practices ........ 3
SIEM Best Practice #1 – Monitoring and reporting requirements ........ 5
SIEM Best Practice #2 – Deployment and infrastructure activation ........ 7
SIEM Best Practice #3 – Compliance and audit data requirements ........ 9
SIEM Best Practice #4 – Access controls ........ 11
SIEM Best Practice #5 – Boundary defenses ........ 13
SIEM Best Practice #6 – Network and system resource integrity ........ 15
SIEM Best Practice #7 – Network and host defenses ........ 18
SIEM Best Practice #8 – Malware control ........ 20
SIEM Best Practice #9 – Application defenses ........ 22
SIEM Best Practice #10 – Acceptable Use ........ 24
Conclusion ........ 26
About AccelOps ........ 28
Author, Acknowledgements, References, Use and Copyrights ........ 29

[1] *Securosis, "Understanding and Selecting SIEM and Log Management" August, 2010, www.securiosis.com*
[2] *Within this document, log management functionality and reference will be subsumed by the term SIEM.*

## What is a SIEM and What are the Top Ten SIEM Best Practices

A SIEM is a solution that aggregates, normalizes, filters, correlates and centrally manages security and other operational event log data to monitor, alert on, respond to, report, analyze, audit and manage security and compliance-relevant information.

Security Information and Event Management or SIEM systems (SIEMs) provide fundamental security operations management functionality that, like other product categories, differs by vendor, functionality and delivery mechanism - be it software, hardware appliance, virtual appliance or services. The general purpose of a SIEM is to aggregate and manage event log[3] data and to provide more efficient and useful analysis capabilities for the information security professional and IT organization for the purpose of monitoring, incident response, reporting, investigation and auditing.

SIEMs collect and centrally manage records of network, system, application, device, security and user activity from different infrastructure sources or "devices." The most common form of event log[3] data is an audit log file generated by a system that is commonly captured via syslog protocol. This requires the auditing functions of a given device to be activated. A device often produces event log data that may be stored in a log file or transmitted in real-time. Manually reviewing a large number of diverse log sources, while possible, has been long proven ineffective, slow, error-prone and frustrating to security personnel. The multitude of event log data that exists on each device within an extensive infrastructure would be cumbersome for organizations to maintain, arduous to consistently assess, and insurmountable to analyze by hand. In addition, at some point a given log file may be overwritten with newer data, whereby prior audit information will be lost.

Event log data can be obtained using a variety of common and vendor-specific protocols such as syslog, SNMP, WMI, network flow, databases and more. Since most event log sources have unique, vendor-determined event attributes that are conveyed in non-standard syntax (also called raw event log data), SIEMs employ normalization techniques to uniformly format all collected event log data for effective processing. As such, it is important to know what device sources in your operating environment must be supported and how your environment will support a SIEM's means to receive or pull necessary event log data. For example, even if a device's event log function is activated, some SIEMS or event log sources may require the use of agents or credentialed means of access to obtain event log data. SIEM vendors publish the devices they support and provide updates to maintain and expand device support. Some vendors also provide means for organizations to incorporate event log data from custom applications or as yet supported devices.

SIEMs offer the means to analyze event log data through real-time correlation and historic analysis. Once normalized, the event log data can be correlated in near real-time against pre-defined and custom rules. SIEM rules can serve to consolidate like events as well as quickly identify potential issues, problems, attacks and violations for which action may be required – typically called an incident. Incidents are derived from one or more events that have satisfied a rule's condition; or multiple rules and conditions. A given rule may be unique or reference an incident class. Rule logic can identify simple event conditions to complex pattern of events. Rules can also reference statistically derived event thresholds (sometimes called behavioral-based or profiling). The capacity for real-time correlation is often determined by two factors; (i) the amount of Events per Second (EPS) that the SIEM is able to sustain processing (normalize and analyze) and (ii) the breadth of attributes and logic that can be applied by the SIEM's "rule engine."

SIEMs ship with numerous rules out-of-the-box to provide upfront value. SIEMs offer a variety of means to refine, fully customize or create rules to help identify company-specific issues or scenarios of interest, extend operating controls and convey different level of severity. An event or incident will have a corresponding severity and notification method (alert). Incident severity can be related to the severity as reported by the device within the event log. Severity can also be automatically adjusted by the SIEM based on the rule, rule logic or rule customization. Some SIEMS also provide the means to convey the impact of an incident to IT and business services. A SIEM alert will provide the underlying event triggers that can be used to understand and further investigate a given incident. In addition, SIEMs possess different event consolidation, alert generation, alert suppression and case management capabilities to facilitate incident response.

SIEMs not only provide real-time correlation, but also have the means to historically search and report on aggregated raw, normalized and incident data. SIEMs ship with common security operational reports, as well as faculties to search for the proverbial "needle in a hay-stack." These pre-defined reports can be extended through different search or reporting constructs. SIEMs also provide query functionality, both real-time and historical, to produce custom reports. Search, report generation and the means to build-out executive, operational and audit dashboards will vary.

With regards to real-time correlation and historic analysis, SIEMs map pre-defined rules and reports to compliance standards and management frameworks for compliance monitoring and documentation - such as SOX, PCI DSS, HIPAA, COBIT and ITIL. By combining monitoring, reporting and case management functionality, SIEMs augment security situation awareness, incident response, investigation, forensics and compliance processes.

Having an overview and understanding of SIEM, IT organizations and information security professionals can apply the following top ten best SIEM practices to gain more assured value from SIEM implementations.

1. **Requirements.** Establish key monitoring and reporting requirements prior to deployment, which would include objectives, targets, compliance controls, implementation and workflow.
2. **Implementation.** Determine the scope of implementation, infrastructure audit targets, necessary credentials and verbosity, activation phases and configuration.
3. **Compliance.** Identify compliance requirements and automate compliance processes and the management of audit data including accessibility, integrity, retention, disposal and evidentiary requisites.
4. **Access Control.** Monitor and report on key status, violations and anomalous access to critical resources.
5. **Perimeter Defenses.** Monitor and report on key status, configuration changes, violations/attacks and anomalous activity associated with perimeter defenses.
6. **Resource Integrity.** Monitor and report on key status, configuration changes and patches, back up processes, vulnerabilities, threats and anomalous activity affecting network and system resources integrity and availability.
7. **Intrusion Detection.** Monitor, respond to and report on key status, notifications and incidents with regards to intrusion detection/prevention network and system threats, attacks and anomalous activity.
8. **Malware Defense.** Monitor and report on key status, threats, issues, violations and activity supporting malware controls.
9. **Application Defenses.** Monitor and report on key status, configuration changes, issues, violations and anomalous activity with regard to web, database and other application defenses.
10. **Acceptable Use.** Monitor and report on key status, issues, violations and activity regarding the acceptable use of resources and information.

While this chapter presents a general SIEM overview and introduces the top ten best SIEM practices, the next chapters offer insight into the top 10 SIEM best practices in terms of process, metrics and technology considerations relative to SIEM and security operations.

[3] *Within this document, event log data, beyond those specifically mentioned, will refer to the variety of audit log records, notifications (such as SNMP traps), network flow, database audit tables, vulnerability scans, identity and many various types and formats of operational audit data which may fall under the category of non-log and non-event. All of which are security and operational data that SIEMs may process and utilize.*

## SIEM Best Practice #1 – Monitoring and reporting requirements

Establish key monitoring and reporting requirements prior to deployment, which would include objectives, targets, compliance controls, implementation and workflow.

Subject covers: Objectives, prioritized targets, auditing, notification, reports, compliance control/proof matrix, system sizing in terms of Events Per Second (EPS) and storage, phased implementation, and workflow regarding accountability, assessment method, review frequency and incident response.

***Overview and Highlight Processes***

Achieving SIEM results has as much to do with human factors, people and processes, as it does technology. Human factors involve organizational (and individual) education, process commitment and accountability, and workflow with regard to a SIEM project and maximizing a SIEM's return on investment. Once preliminary policies and procedures have been established, it then becomes that much easier to apply a technical approach to outline key monitoring and reporting requirements prior to implementation. To that end, the IT organization will be better prepared to identify SIEM functionality gaps, as well as assess what is necessary to support deployment, incident response and compliance processes.

Organizations should establish requirements, objectives and responsibilities that are acceptable to respective constituents including IT management, IT security management, operations, finance, marketing and legal. Constructing SIEM technical requirements typically encompass:

- Defining a policy of what is to be monitored and the criteria for inclusion
- Comparing that policy to internal and external requirements (e.g. SOX, HIPAA, PCI DSS)
- Determining the types of monitoring dashboards and reports that are needed
- Outlining how classes of network devices, systems and applications can be monitored, and
- Assessing procedures to manage and respond to classes and severity of incidents, as well as to regularly review reports

The organization should also incorporate audit specifications with the means to verify source inputs and acceptable output. This will necessitate documenting operational procedures that should be reassessed from time to time.

Advanced planning would include objectives, prioritized source targets, defining attributes of what is to be monitored, internal and external audit requirements and frequency, notification and incident response processes, reporting as well as data retention requirements. Once device targets are mapped out and data retention is determined, then capacity requirements can be estimated in terms of Events per Second (EPS) processing capacity and storage capacity.

EPS is not equal among all devices, and depending on the vendor, may be measured differently. Generally speaking, an event is a raw record of infrastructure activity. In general, firewalls, network flow, IDS and the like can be more verbose than certain servers or applications. By classifying devices and the number of devices within each device class, one can start to build out a general estimate of EPS. Some application and SIEM vendors provide guidance, as well as event log EPS or data collection calculators. Another useful method in EPS calculation can be accomplished by gathering sample EPS data from live devices via a temporary logging server - for example, running syslog over a reasonably defined period, such as a few days up to a couple of weeks, to amass representative peak and non-peak event count. In most cases, conveying infrastructure details with SIEM vendors, the SIEM community or service providers will yield a good base estimate of EPS.

One of the benefits of a SIEM is to aggregate and centrally manage disparate event log data. A common misconception is a SIEM's ability to readily have on hand and use all managed data for the purpose of reporting, analysis or forensic investigation. In general, the way that a SIEM stores and analyzed raw, normalized and incident (alert) data can be employed using different technologies such as databases and other proprietary techniques. The extent to which a SIEM can historically analyze data is often determined by (i) how data is stored and managed, (ii) how much storage capacity is available, and (iii) the processing capacity to normalize incoming data and apply real-time correlation while at the same time executing searches and analyzing historical data.  For example, some SIEMs have all operational data online and available for analysis.  Other SIEMs may need to archive periods of data, which must be restored - potentially on a separate SIEM system - for forensics analysis.  Organizations should assess their organization's data retention, reporting and analysis requirements and understand how these requirements are addressed by the capacity constraints of the SIEM and respective operating platform.

SIEM workflow will consist of configuration, activation of new sources, SIEM management, customization and refinement, monitoring and incident management, reporting review, audit preparation and investigation requests. It is safe to assume that different reports will serve different groups.  By working together with respective business units on a frequent basis to accommodate their needs, one can ensure broader project support and operational adoption.

Defining success criteria for SIEM implementation is crucial.  By building out an initial implementation plan to satisfy the most immediate business critical requirements, an organization can ensure greater success and less costly on-going improvement.  This phased implementation approach will make SIEM deployment and management that much easier and faster. Monitoring and reporting requirements can then grow as appropriate.

If migrating from an existing log management or SIEM approach, you should document what you are currently capturing, monitoring and reporting.  It is expected that your infrastructure has grown, operating norms have changed and business requirements have evolved.  Interfacing with departments and business units will likely yield broader requirements and increased SIEM specifications – ultimately resulting in new purchase criteria.

***Recommended Sample Metrics***

- Percent of project achievement; requirements, objectives and responsibilities as verified by respective constituents
- Defined success criteria that have been met
- Verification of associated inputs and outputs e.g. source targets and desired reports
- Analysis of initial and near-term subsequent scope of device sources (type and number), operators, reports and data retention to enable estimation of capacity requirements
- Documentation of monitoring, incident response and auditing operating procedures

***Technology Considerations***

- Start with infrastructure and application sources that are security and business function critical and take a phased in approach towards implementation which can verify inputs and desired outputs
- Explore project management and collaboration software to complement tracking of SIEM implementation and processes
- Develop a SIEM procedure workbook incorporating requirements, processes, responsibilities, signoff, rules, reports, devices, etc.
- Track integration results and changes to rules, reports and procedures to identify shortcomings, etc.
- Use worksheet to estimate EPS performance capacity and data retention requirements

## SIEM Best Practice #2 – Deployment and infrastructure activation

Determine the scope of implementation, infrastructure audit targets, necessary credentials and verbosity, activation phases and activation.

Subject covers: Implementation options and considerations, node discovery, activation, verbosity, consistent capture, phased implementation, target device access and monitoring considerations, activation planning and coverage considerations.

***Overview and Highlight Processes***

Key to initial deployment and on-going operational success of a SIEM is:

(1) managing/maintaining the SIEM deployment,
(2) maintaining source activation and consistent delivery of event and log data, and
(3) refining the system to serve on-going needs.

At the core of any SIEM deployment is the identification and activation of a device's auditing functions, which includes network devices, systems and applications. Once respective device targets, device activation, event log capture, alerting and reporting requirements have been identified and documented, the process of expanding the scope of a SIEM project is simplified. As mentioned earlier, the best means to achieve SIEM implementation success is by phases. Rather than an "all at once" approach, organizations can start with monitoring the most security and business critical devices or those that address a specific set of controls. SIEMs can handle large projects, but breaking down the SIEM project into smaller phases - be in initial installation, expansion, upgrade or replacement - will better assure success.

SIEM deployment, scheduling and cost management, should consider:

- Procurement and overall deployment costs
- Delivery mechanisms, such as software, hardware appliance, virtual appliance (turnkey software application running on a Virtual Machine), or as hosted or managed service
- Necessary operating equipment (hardware, server, storage, backup or analysis systems, etc.)
- Installation and the scope of coverage such as site, multiple sites, or multiple divisions/clients
- Infrastructure preparation
- Personnel resource requirements including responsibilities, training and support
- Monitoring frequency, such as real-time or historic, by devices class or criticality of IT function

By calculating on-going maintenance and growth as part of overall implementation, organizations can obtain a true picture of the SIEM total cost of ownership (TCO).

The better the documentation, change management processes and initial preparation of the environment prior to SIEM deployment, the easier the implementation and ongoing maintenance of the SIEM will be. This involves an understanding of where and what devices, systems and applications are deployed; the technical or policy-based limitations to receive event log data or access the source; and the scope of work effort and timing for activating event logs and enabling device access. If one is migrating from an existing log management, SIEM or other monitoring solution, the redirection of event and log data can be an easier transition.

Some SIEMs offer infrastructure discovery capabilities and as well as the means to maintain credentials to access monitored resources. While many SIEMs can automatically process known event log data received via syslog, the use of SNMP community strings, activation of network flow, credentialed account access and possibly agents may be required by the SIEM as a function of the desired depth of operational monitoring. For example, configuration monitoring may require credentialed access.

Procedures should be in place to ensure the appropriate activation and access to event log data by source type and operating environment. Incorporating these procedures within change management processes will minimize monitoring and audit gaps. Once event log monitoring of a source is established, the SIEM should alert on terminated or anomalous event log communications so that an organization can initiate corrective action in a timely manner to assure consistent monitoring.

***Recommended Sample Metrics***

- Percent of deployment and event log activation complete to project scope
- Active to expected ratio of monitored device by category, network/site
- Active to expected ratio of monitored device by critical service or implementation phase
- Identification of device/source to SIEM event log feed anomalies
- Ratio of node discovery from SIEM to asset database or configuration management database (CMDB)
- Log and event volume by source, average and peak EPS rates
- Data retention capacity trends
- Report generation execution time trends

***Technology Considerations***

- Sources will include all event log sources prioritized by business function and security criticality
- Implementation option tradeoffs and total cost of ownership
- Process and tools for device event log activation (from syslog and network flow, to SNMP and credentialed access)
- Use of Discovery, Configuration Management Database (CMDB) and Configuration Management System (CMS) tools
- Frequency of credential updates and the means to maintain active credentials for the SIEM to access resources
- Use and support of inventory database or vulnerability scanning tools
- Establish thresholds or statistical profiling of event log by source to determine terminated or anomalous activity

## SIEM Best Practice #3 – Compliance and audit data requirements

Identify compliance requirements and automate compliance processes and the management of audit data including accessibility, integrity, retention, disposal and evidentiary requisites.

*Subject Coverage*
Accessibility, integrity, retention and storage considerations, transmission, data protection, access control, data disposal, accountability, and evidentiary requirements.

***Overview and Highlight Process***

The primary driver for most SIEM purchases is the support for compliance processes. Organizations must understand their applicable industry, regulatory and legal obligations for security and risk management. Given that many compliance standards, with regards to the types of controls that SIEM products can support, have overlapping mandates or guidance (e.g. monitoring access to resources and addressing malware) - it is best to establish a matrix of compliance requisites and SIEM "proof points." Some compliance mandates, such as PCI DSS (Payment Card Industry Data Security Standard) will offer more direct specifications than others. Once compliance requirements are assessed, respective audit policies and supporting documentation can be established to map and monitor source targets (infrastructure assets), monitor specific controls, respond to compliance-relevant incidents, and support audits.

While the majority of Governance, Risk and Compliance (GRC) solutions tend to monitor policies and compliance processes via attestation, SIEMs complement GRC by monitoring infrastructure controls supporting compliance mandates. Many SIEMs already cross-reference their rules and reports to support compliance standards and management frameworks. The organization's objective is to automate as many audit specifications as possible. This will not only necessitate capturing and reviewing event log data, but more often require the monitoring of configuration changes, infrastructure segregation, identity management, resource access, as well as documenting incidents and investigations.

SIEMs ability to address broad compliance requisites will vary based on the breadth of built-in functionality to support specific mandates, and the breadth of reporting devices and respective monitored controls that also serve to support compliance. Many SIEMs can monitor directory services to address privilege-based management requirements such as creation, modification and termination of user accounts. However, not all SIEMs monitor configuration changes and would therefore require the means to incorporate configuration data from other application sources. By correlating a broad set of operational and identity data, organizations can support more compliance-oriented controls. For example, SIEM rules can support identifying resources access with subsequent configuration changes outside of approved change windows.

Compliance dashboards, alerting and reporting frequency, and delivery targets will vary. As such, compliance reports and dashboards should be refined to support security analysts, internal and external auditors and the CIO or CSO. The use and availability of audit data is also vital to meeting compliance standards. The organization should know how much event log data, what type of data (raw, normalized, incident) and how long such data is readily available for use (as described in chapter 2). In addition, the organization should have processes to enable investigations / forensics. For example, some SIEMs have their event log data online and available for analysis while others may require archiving subsets of event data, or store the data in a raw format that must then be re-parsed. Depending on the investigation, the processing of historical data may also be beyond the capacity of a SIEM that is online and processing real-time information. As such, it would require a separate SIEM installation to fulfill analysis. Depending on the implementation, the organization and security analysts should know any technical constraints that may impact performing investigations.

Retention of raw and incident data can support a variety of compliance processes from fulfilling forensic investigations to satisfying compliance mandates and onsite auditor requests. For example, many states/provinces and countries have enacted data privacy laws that require that organization to pinpoint when a sensitive data breach or leakage has occurred and to notify those affected in a timely manner. This would require providing documentation to authorities or industry regulators. Without being able to trace back and analyze the necessary data, a firm's liability, penalty and notification exposure may be greater than actual. Depending on the compliance mandate, some auditors may want to validate the monitoring of compliance-relevant controls onsite. Here too, SIEMS can provide appropriate on-demand presentation of information to meet an auditor's request.

One size does not fit all when addressing audit data retention requirements. For example, one service organization may require adhering to SOX (Sarbanes-Oxley Act), HIPAA (Health Insurance Portability and Accountability Act), and COBIT (Control Objectives for Information and related Technology) mandates and only want retain one year of event log data. Whereas, another service organization that must address ISO (International Organization for Standardization 27001), NIST (National Institute of Standards and Technology SP 800-53 and SP 800-92) and DCID (Director of Central Intelligence Directive 6/3) requisites will require some access control data being retained for 5 years.

Other technical auditing obligations include event log retention, rotation and archival, clock/time synchronization, record integrity, data disposal (e.g. log deletion), transmission, incident response, and data storage requirements. Some additional considerations, depending on your audit and compliance requirements may include: the means to maintain SIEM audit records tracking access, use, administrative and system level activities, monitoring for event log transmission anomalies, documenting log review and incident management activities, options for secure event log data access, and offering user-definable means to adjust event log retention. These and other log management and audit practices are further referenced in NIST SP 800-52 and SP 800-92 guidance.

***Recommended Sample Metrics***

- Number of actual to recommended assets logging as prescribed by policy
- Trend any logging consistency
- Compliance classified threats, issues and violations and respective case/ticketing reference
- Daily alerts, monthly reports and quarterly reviews of material compliance policy violations (used for annual audits)
- Top compliance issues by category, severity, organization and asset in summary and trend
- Top compliance issues resolved in summary and trend
- Open compliance issues by month, quarter, compliance category
- Open to close ratio (and trend) compliance issues by month, quarter, compliance category
- Changes to current event log volume and sources by week, by month, by device type
- Time range of available monitoring records to support retention requirements

***Technology Considerations***

- Sources will include a variety sources, configuration management, identity management and incident management
- Document the number of audit control objectives via compliance control/proof matrix satisfied with SIEM monitoring, notification and case management capabilities
- Document product feature set and configuration attributes aligned with auditing requirements (e.g. integrity via MD5/ or SHA/Hash-MAC)
- SIEMs means to associate groups of assets related to compliance and the means to readily apply controls that automate compliance alerting and reporting functions
- Use of one SIEM or additional tools to support mandates (e.g. monitoring configuration standards, presenting topology, identity monitoring and host-based file integrity monitoring)
- Use of collaboration, business process or governance (GRC) tools to track process checks and attestation to adherence
- Consistency of collection, integrity and protection of raw and incident event log data to provide reasonable evidentiary quality of data.
- Assessment of SIEM capabilities with regards to: event log retention options, rotation and archival, clock/time synchronization, record integrity, data disposal (e.g. log deletion), transmission, incident response, and data storage, as well as SIEM audit records tracking access, use, administrative and system level activities.

## SIEM Best Practice #4 – Access controls

Monitor and report on key status, violations and anomalous access to critical resources.

*Subject Coverage*
AAA servers, VPN/RAS/NAS, Directory Services, privileged and administrative access, excessive failures, terminated account use, service account use, tracking 3rd party and consultant access, and monitoring access administration.

***Overview and Highlight Processes***
Monitoring resource access is critical to preserve system integrity and availability, as well as protect information assets, financial information, personal identifiable information (PII), and sensitive and proprietary business information. The creation of policies and procedures to manage and monitor user, and service account, resource access is also a requirement that is universal among numerous compliance mandates and IT management frameworks.

Authentication, authorization and accounting (AAA) mechanisms to control appropriate access to resources. Authentication identifies the user based on requesting unique attributes/factors prior to access such as user name, password and token. Authorization associates resource rights/privileges to the user or class of users based on the type of functions of the resource being accessed. Accounting, for this documents purpose, is the enablement and use of audit logs. Many organizations leverage directory services to facilitate the management of and access to resources by defining and maintaining user, system and group objects, and associating rights to said objects. Virtual Private Networks, Remote Access Servers and Network Access Servers, among other network access mechanisms, can then reference user, system and group object attributes maintained within a directory service.

SIEM can monitor directory services in terms of creating and modifying defined users, groups and respective resources access privileges. Centralizing and automating real-time monitoring and audit functions is especially important in organizations with multiple directory service. All hosts can have their audit logging capabilities enabled to record access and resource modification – as further described in chapter 6. SIEM rules and reports can consolidate the monitoring and review of access controls and authentication activity by aggregating and cross-correlating all respective AAA event logs. Beyond employing SIEMs to alert and record all access failure and excessive failed access attempts, SIEMs can more easily bring together all AAA; successful logins, subsequent secondary logins, and user / system activity to facilitate investigations.

Operators can use and refine the many built-in access monitoring rules and reports, or create new rules to support specific policies. For example, a SIEM could identify policy violations with regards to how and when privileged users can access specific resources. The broader the number of attributes and available logic that a SIEM rule exposes to the security analyst, the more expansive potential secondary controls can be implemented to prevent fraud, malicious activity and resource misuse. This allows operators the means to proactively identify threats and violations.

Incident response and report review procedures should be in place prior to activating SIEM rules and reports. It is also suggested to monitor for suspicious access activity, such as: high or unusual volume of directory account creation and termination, use of terminated credentials, use of resources outside normal operating hours, atypical access to resources using service account credentials, multiple logons from different locations, and atypical privileged user access to resources. In this regard, monitoring successful access is as important as failure. For example, monitoring and maintaining records of access to all resources can generate reports designed to investigate insider threats regarding privileged users and consultants.

***Recommended Sample Metrics***
- Top access failures by source, destination, user, business unit
- Access failure by prioritized logical grouping (e.g. payment processing resources)
- Top access destinations by users/groups and anomalous access
- Access login success and failure (internal); by user, system, by device class, by time (with details)

- Unusual access to prioritized logical grouping (e.g. financial reporting resources)
- Multiple account logons from different geographic locations
- Suspicious access attempts or failure followed by success from same source
- Privileged user access by access failure, by critical resource, by method, by different location/same time
- Top privileged user access follow by configuration changes
- Administrative changes to directory service user and group objects; by admin, by user, by group, by resource criticality
- Use of trusted and service accounts, by volume, by time of day, by domain
- User activations, privilege change and terminations by device class
- Remote access login success and failure (VPN, other); by user, by device class, by time with details
- Unusual service account, terminated account use, login success and failures

***Technology Considerations***

- Sources will include AAA, VPN, RADIUS, proxy and other authentication and access devices, directory services and host OS logs
- Where possible, physical security device logs, such as badge or bio readers should be incorporated as an event log source
- Maintaining baselines of location and access type for classes of users
- Note that the user/system identity reported in the system log is source-centric. As such, the use of non-unique/shared credentials (e.g. may users employing "Administrator" as their User Name) will be recorded in the source log. Unless the SIEM incorporates more automated means to track and resolve the "true identity" behind an activity, security personnel will need to investigate and cross-reference other source log data to determine the actual identity.

## SIEM Best Practice #5 – Boundary defenses

Monitor and report on key status, configuration changes, violations/attacks and anomalous activity associated with perimeter defenses.

*Subject Coverage*
Firewall, NAC, NAT, VPN, routers, proxy systems, wireless Access Point (WAP), attacks and violations, ports, anomalous request types, denial of service and false positives.

***Overview and Highlight Processes***

Boundary defenses, also known as perimeter countermeasures, such as firewalls, routers, VPNs and other means of network-based access controls, remain vital to defend against unauthorized access to network resources, as well as to prevent threats and attacks. While DMZs (demilitarized zone) serve as a checkpoint between the public network and company's private network, perimeter defenses in general serve to grant or prevent internal users or systems from accessing network resources within and outside the corporate network. Firewalls, and variations thereof, filter acceptable inbound and outbound connections, in terms of allowing or denying communications based on rules referencing computers, applications, services, ports or protocols.

There are multiple boundaries or perimeters in an organization. There are perimeters between users and systems; remote users and internal resources; business partners and extranets; and wireless access points and the corporate network. A level of understanding is necessary with regards to defining boundaries in terms of levels of risk, appropriate access grants, and monitoring interests. Once discrete perimeter controls have been configured and policies defined, whether comprised of firewall policies, router, VPN and RADIUS ACLs (Access Control Lists), wireless access points, as well as other forms of perimeter defenses, the respective logs and notifications from the devices must be activated and verified. SIEMs can serve as a centralized point to capture boundary state, changes and issues.

Some network devices, such as firewalls, can provide network flow information. Network flow is a record of network packet flow information, which contains details such as source and destination address, port (application) and amount of data. This type of information can be vital for incident response or monitoring for advanced persistent threats (APT). Network flow is produced by popular network firewalls, switches and routers, which disseminate the data according to vendor-specific protocols such as Cisco Netflow. Some SIEMS can process, analyze and manage network flow and use this information to understand network resource utilization. SIEMs can cross-correlate network flow with other operational data to identify suspicious behavior and potential security threats.

Virtualization presents additional potential challenges with regards to boundary defenses. The automated resource and network access provisioning and potential for dynamic VM movement (as describes further in Chapter 6 with regards to network and system integrity), does present the risk of a VM and respective guest host to leave one boundary and go into another. Attention should be paid to alleviate this condition by way of proper virtualization configuration management.

SIEMs can be used to consolidate the monitoring of access activity from various boundary defenses. It is suggested that organizations compile a prioritized list of key attributes to be monitored by business and operational risk, as well as assess frequency and type of required monitoring; be it daily, weekly, monthly, real-time correlation or historic report. Daily operational procedures should cover incident response, as well as incident and report reviews. Case management can track who and how specific incidents were investigated and resolved.

***Recommended Sample Metrics***

- Top access failures by source and destinations
- Top inbound connections to internal sources by system, user, bandwidth and time
- Top outbound connections to external sources by system, user, bandwidth and time
- Top outbound DMZ connections to external sources by system, user, bandwidth and time

- Top perimeter attacks by category
- Top dropped traffic from DMZ, FW
- Top blocked internal sources by port, by destinations
- Top blocked outbound connections by port, by destination
- Unusual DNS access and requests
- Changes to active and standby configurations by perimeter device class
- Daily or weekly alerts on top 10 connections from sites of concerns
- Top unusual peak bandwidth utilization sources and destination
- Top bandwidth by protocol, by connection, by source, by destination
- Configuration changes FW, VPN, WAP, Domain
- Failure FW, VPN, WAP, Domain
- Multiple login failures by FW, VPN, Domain
- Excessive VM movement by VM, by guest host
- Non-compliance VM movement by VM, by guest host
- Wireless network access by location, by user, by failed attempts

***Technology Considerations***

- Sources will include firewall, router, wireless AP, VPN, RADIUS, proxy systems, other authentication systems, NAC, NAT, and host OS logs.
- Most SIEMs have rule and report sets to monitor perimeter defenses, but not necessarily configuration changes, network flow nor statistical profiling to detect anomalous network and application activity. This can impact compliance monitoring and can require access to other types of IT management systems.
- Adjusting correlation rule severity by source IP, destination IP, user or asset grouping can help support prioritizing incident response and compliance mandates

## SIEM Best Practice #6 – Network and system resource integrity

Monitor and report on key status, configuration changes and patches, virtualization, back up processes, vulnerabilities, threats and anomalous activity affecting network and system resources integrity and availability.

*Subject Coverage*
Change management process, change control/ validation, vulnerability assessment, patch management, backup services, virtualization management, resources issues and restarts, availability and adherence to configuration standards.

***Overview and Highlight Processes***

Network device and system resource integrity have a direct impact on infrastructure and resource reliability. Given that corporate operating requirements evolve and vendors update their systems to address known issues or revise best configuration practices (sometimes expressed as RFCs/Request for Comment) - configuration changes are inevitable.

Understanding one's infrastructure, from deployed devices, systems, applications to configuration, vulnerability and patch details, is required in order to assure and maintain operating integrity. It is certainly necessary to make informed operational, budget, procurement and capacity planning decisions. Furthermore, understanding the criticality, dependency and relationships of devices, systems and applications with regards to their support of IT functions, business services and compliance relevance is imperative in order to meet service levels and gauge the impact of changes.

Change management processes provide the policies and procedures for provisioning, documentation, change review and maintenance. Standardized configurations eases provisioning and management, as well as reduces operational faults and improves fault triage. Depending on regulatory and industry standards, operating level agreements (OLA) and service level agreements (SLA), assuring system integrity and implementing change management processes are required for compliance such as PCI DSS, COBIT, ISO 27001 and ITIL (Information Technology Infrastructure Library). Once approved systems are deployed, respective configuration and subsequent configuration changes should be tracked and verified.

Setting and enforcing configuration standards is the standard to ensure service reliability. Unauthorized, inappropriate, accidental and malicious configuration changes are among leading causes of outages, performance degradation, data corruption and security issues. Since a configuration change can impact both network operations and security, having team collaboration on configuration issues and access to change details can speed up diagnosis and remediation.

SIEMs can provide a variety of monitoring, alerting and reporting mechanisms to support the maintenance of infrastructure integrity. Either directly or through data integration with other IT management systems, such as configuration management database/CMDB, they can be used to automate the means to identify unauthorized changes, identify systems out of compliance, resolve false positives, verify approved changes and assess the impact of a change to other systems and to the delivery of IT or business services. Security and compliance relevant configuration should be identified, escalated, tracked and resolved.

Virtualization software brings the tremendous benefits of provisioning ease, deployment ease, standardization on hardware architecture, and of course, server consolidation. A byproduct of virtualization is VM sprawl, VM contention and dynamic network architecture. This greatly intensifies data center management complexity by many levels of magnitude. Now with applications running in a guest OS that constantly moves to a different vSwitch or content switching port, due to load balancing, dynamic resource allocation or a security threat, pinpointing which layer having a problem is extremely difficult.

Is there an application problem that is causing the performance problem, or is it the OS layer? Is there a hypervisor management threat? How about the virtualization server layer? Is the problem in the vSwitch layer? Because VM images are stored in the enterprise network storage, assessing the scope of the problem would also need to consider the storage layer and the content switching layer.

Given the above virtualization management issues, it becomes more difficult to triage a virtualization issue in a timely fashion and readily know: what is the true problem and where is the problem? If the root cause is due to change, who and what trigged the change? Is there a VM configuration vulnerability that has been exploited? What resource limits have been reached? Where does the VM (and respective OS and application) reside and where/when did it move. And more importantly, what is the impact of VM resource contention, excessive VM movement, VM problems or hardware issues to the delivery of IT services. For example, has improper configuration and virtual management enabled a VM to migrate from a server within a compliant to non-compliant zone.

SIEMs, with virtualization intelligence, can cross-correlate information from all layers in the networking stack: information from applications, processes, guest OS, the virtualization server, the HW, network devices (e.g. a content switch), storage, etc. across performance, availability, security and change management. By doing so, SIEMS can help to monitor virtualized environments, bridge physical and virtual environments, and enable means to reduce potential security and compliance issues.

Ongoing product updates/releases, as well as the persistence of hackers to identify and exploit vulnerabilities have also necessitated the use of patch management and vulnerability management (vulnerability scanner) solutions. These vulnerability management systems can also feed SIEMs operational details to support security operations and incident response. Some SIEMs can directly monitor, verify and track configuration changes, as well as installed patches.

Operational resiliency measures typically relate to backup functions and disaster recovery capabilities. While usually addressed as an “availability” concern, for the purpose of this book, availability will constitute support for infrastructure integrity. While backup, snapshot and other replication processes are managed through various data protection solutions, SIEMs can serve to aggregate such processes and also highlight unscheduled and atypical processes requests. The same monitoring capabilities can be applied to monitoring the transfer of (and access to) virtualization datastores.

With regards to resource integrity, another necessity is having complete who, what, when and where information with regards to an approved, unauthorized or undocumented change. As a best practice, activating system audit log functions is critical to record access and changes to system resources. In some cases, this will involve procedures for operations or security personnel to retrieve data from network devices to obtain the “where.” It may require reviewing system logs to obtain the “who” and “when” details. However, problems arise when privileged users, employing shared credentials, perform configuration changes that need to be investigated. This would then require further assessment of various AAA logs detail to ascertain the “true user” behind the share credential. Some SIEMs incorporate identity and location management capabilities to provide complete change management records.

***Recommended Sample Metrics***

- Top critical system/device changes per user, per device class, per IT services
- Unauthorized changes, by criticality, as percentage and trend
- Changes to configurations by device class, by user, by criticality
- Systems outside configuration standards; by criticality, class, business unit, ratio and trend
- Percent of systems without approved patches
- Top attacks by exploited vulnerable systems
- Top inbound and outbound connections by system, user, bandwidth and time
- Unusual scanner / probe activities
- Non-standard port activity
- Actual and suspected systems with Peer-2-Peer software or communications
- Top system issue/incident by incident category

- Installation of unauthorized software
- Configuration changes outside approved changes (maintaining separate change reference data)
- Top devices with critical resource utilization (memory, processor, storage, fan…)
- Top business critical devices with critical resource utilization (memory, processor, storage, fan…)
- Top device / system restarts
- Top process start and failure (filtered)
- Object access denied
- DNS configuration changes
- DNS faults
- Account changes by critical resource
- Excessive VM movement by VM, by guest host
- Non-compliance VM movement by VM, by guest host
- High resource utilization by VM guest host, by resource types
- Devices with unauthorized or anomalous communications (SMTP, etc.)
- Vulnerability to incident ratio and open/closed vulnerability trends
- Attacks against vulnerable systems classified by criticality
- Device/device group availability percentage
- Failed backup services (or other similar services) by system, by time, by business unit/service

***Technology Considerations***

- Sources will include all infrastructure devices; beyond event log data, other means may be required to capture configuration and configuration change details
- Best to prioritize according to critical operational/business functions and security defenses
- Most SIEMs have rule and report sets to monitor system logs and security alerts, but not necessarily configuration change - this impacts compliance monitoring and can require integration or use of other types of IT management systems
- SIEMS can also identify those systems that have been compromised by way of automatically analyzing the infected systems' activity
- Integration with vulnerability management systems can be used to automatically or manually resolve false positives (the identification of an attack or malicious activity by an IDS/IPS that is actually benign)

## SIEM Best Practice #7 – Network and host defenses

Monitor, respond to and report on key status, notifications and incidents with regards to intrusion detection/prevention network and system threats, attacks and anomalous activity.

*Subject Coverage*
Network and host IDS/IPS, WIDS, network flow, false positives, anomalous network activity, Denial of Service attacks, and usual activity or requests (ICMP, TCP, IRC, Port availability/use).

***Overview and Highlight Processes***
Network and host security defenses more often include the combined use of firewalls and Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS), which serve to identify and prevent unwanted communications, known attacks and behavior-based malicious activity. While network and host defenses can also include anti-malware and many other security mechanisms, such as audit log activation, password management and other network segregation techniques, this chapter will focus on IDS/IPS in the context of SIEM best practices. Firewalls were examined in an earlier chapter as part of perimeter defenses.

Network intrusion detection systems typically work at the TCP/IP level, Layer-2 and/or Layer-3, to inspect traffic in real-time and apply detection methods (sometimes called rules) based on known patterns/signatures or traffic-flow behavior to discern network-based threats and attacks, such as: worms, spyware, peer-to-peer port scanning, denial of service (DOS) and buffer overflows. They can also use other mechanisms of stateful packet inspection, protocol and application context, site blacklisting and statistical profiling to identify protocol anomalies, zero-day threats and blended threats. WIDS (Wireless IDS) add wireless context such as alerting on WAP configuration, vulnerability, compliance, and failure as well as identifying rogue wireless access point alerts.

Host IPS/IDS can work in a similar manner in that they also examine traffic bound for a single host. Many vendors have also included additional features such as firewall, policy enforcement (e.g. current anti-virus or VPN client), scanning for spyware (registry, files and known rootkits) and application control (e.g. registry changes, file changes, system logs, process monitoring and approved applications). The difference between intrusion detection and prevention is the response options of alerting/logging versus blocking the offending network connection or system activity. Generally speaking, Network and Host IPS offer another beneficial security layer while at the same time generating a significant amount of notification events.

SIEMs can aggregate IDS/IPS alerting, conduct event consolidation on like alerts, filter IDS/IPS false positives and facilitate incident management. One useful way to examine IDS activation, refine IDS rules, test SIEM implementation and assess incident management processes is to generate offending test traffic to trigger alerts. Organizations can generate IDS alerts by either using traffic replay and test mechanisms within the IDS or by employing IDS test tools such as Tomahawk and Metasploit. Having incident response processes, such as prioritization, case management, investigation and escalation procedures in place, is as important as having daily and weekly incident review.

In some cases, IDS/IPS can generate false positive alerts - a detection of an attack or malicious activity by an IDS/IPS that is actually benign. Unfortunately, this results in an event that will require security staff to take some response. Essentially, the identification of the attack by the IDS is technically legitimate, but there is no security issue. In some cases, the IDS rule or statistical profiling is broad enough to identify attacks that are indeed non-issues.

SIEMs can alleviate this condition and respective administrative burden by offering the means to automatically tag certain IDS false positives (which all IDS users contend with) via event correlation and exception management. SIEMs can, and in real-time, identify false positive conditions which are comprised of: (i) attacks against invalid systems, (ii) attacks against systems that are patched and no longer vulnerable, or (iii) attacks that are non-threats such as scheduled vulnerability scans. For other cases of known false positives, such as scheduled scans or penetration tests, the SIEM/Log manager is also well positioned to handle exception management. Least of which, SIEMs can consolidate the often repeated or related IDS/IPS alerts which can consume conventional event log incident consoles.

***Recommended Sample Metrics***

- IPS/IDS events classified as incidents per month by network, by service
- Top incidents by attack type, by source, by destination
- Top attack sources and destinations by volume or destination criticality
- Attacks identified and resolved
- Top traffic by source by application, by source type, by business unit
- Unauthorized and suspicious network traffic by source, by destination, by type
- Suspicious behavior by source, by destination, by type
- Suspicious communications by source, by destination, by type
- Attack investigation open and close ratio and trends
- Wireless IDS alerts

***Technology Considerations***

- Sources will include network and host intrusion detection/prevention systems, firewall, network flow and other defense mechanisms, and host OS logs
- Activation, maintenance and refinement of IDS/IPS rule sets
- Use of SIEM real-time correlation and historic reports
- Means for SIEMs to suppress potential IDS/IPS false positives
- Integration into incident management / case management tools
- Generation of test traffic to test SIEM integration with IDS and incident response processes

# SIEM Best Practice #8 – Malware control

Monitor and report on key status, threats, issues, violations and activity supporting malware controls.

*Subject Coverage*
Tracking of virus, malware, spyware, spam, malicious website request, unusual resource activity, as well as detection, quarantine and remediation.

***Overview and Highlight Processes***
One of the more popular end point security tools is anti-virus. However, malware control is not limited to the use of anti-virus tools, but extends to managing additional threats, infections, scope of infection, outages and breaches related to a variety of malware risks and activity. Malware controls would comprise of identifying, mitigating and measuring: viruses, root kits, trojans and spyware issues, botnet, peer-2-peer activity, spam, and suspicious website and email communications.

The majority of information security compliance frameworks specify employing anti-malware tools. Best practices dictate that anti-malware implementation should be tiered from end point to perimeter (e.g. client, server and gateway). Processes should be established with regard to ensuring activation and standard use, monitoring and reviewing malware activity, and most importantly, responding to issues. This would include monitoring various anti-malware solutions for updates and failures. Procedures with regards to malware include management, incident response, infection or breach documentation, issue notification, quarantine of infected systems, and remediation.

Organizations should routinely monitor for critical anti-virus/malware issues; prioritized by system, type of issue, effect on operations, or the scope/probable spread of infection. SIEMs offer the means to centralize malware monitoring and reporting processing, measuring on overall malware infection, and assessing operational impact. One method to facilitate monitoring is to correlate event log data from anti-malware management systems rather than end point devices themselves. Keeping track of resolved infections or problems also helps justify security expenditures. For example, SIEMs can report spam and viruses prevented or mitigated at the MTA gateway.

SIEMs also provide the means to centralize malware incident response. One useful monitoring practice is to enable SIEMs to allow operators to focus on detection-only (rather than remediated) malware issues, as well as identifying difficult malware threats. Some SIEMs have the means to assimilate network flow data and establish baselines or profiles of traffic activity. Having this broader context allows the SIEM to identify suspicious application activity and network traffic bursts, such as identifying symptoms and direct activity related to botnets and worms. SIEMS can also facilitate processes to identify infected systems to quarantine and remediate, by correlating: unusual DNS requests, unusual port activity from the firewall log, unusual traffic spikes via network flow data, identified port scanning and outbound traffic attributed to zombies, or warnings from the IDS/IPS on outbound communications to a known malicious site.

***Recommended Sample Metrics***

- Top reported malware threats
- Anti-virus trends; prevented, detected, remediated
- Spam trends; identified and removed
- Top malware attacked sources, and by prior vulnerability issues
- Top unusual traffic to and from sources
- Top source and destinations of malicious connections
- Top systems with multiple infections / top systems re-infected
- Top systems with suspicious malware activity
- Anomalous network activity
- Atypical email or web communications

- Atypical port/application use
- Anti-virus stop, start, update failures

***Technology Considerations***

- Sources will include all anti-malware applications; anti-virus, anti-trojan, spam filtering, web filtering and website scanners
- For greater SIEM context, additional sources include DNS, IDS, VA and network flow operational data
- Leveraging the anti-malware manager, versus clients, as reporting sources

## SIEM Best Practice #9 – Application defenses

Monitor and report on key status, configuration changes, issues, violations and anomalous activity with regard to web, database and other application defenses.

*Subject Coverage*
Application availability, configuration changes, process monitoring, Web application server status, web application firewall security issues, database security including audit records, monitoring of users and tables activity…

***Overview and Highlight Processes***
Beyond perimeter, network and host security defenses, application security adds another layer of protection to improve service availability and address managing attack, fraud, data privacy and compliance risks. While secure application development within software development life cycle (SDLC), application scanning and "fuzz" testing are proven methods to reduce application risks, this chapter will limit the topic to areas more common to SIEM implementation. This would include application platform monitoring, resource monitoring, web application defenses and database activity monitoring.

The first line of defense for an application is to safeguard the application's operating platform. This would include maintaining the overall platform operational state, security and non-security configurations, and patches with regards to hardware, network interface, operating system (OS) and possibly the virtual machine. Since many applications write to an operating system's logging services, monitoring the application log file in addition to other performance and configuration changes is advised. Depending on SIEM functionality, many SIEMs can correlate broader application-monitoring context to facilitate rooting out non-security from security or compliance-relevant operating platform issues. Other areas of interest should examine: monitoring for newly installed and running applications, unusual application processes or those consuming a high amount of resources, or changes to communications from the operating platform – all of which can be symptoms of malicious software/activity.

Due to the increase of web and mobile applications, the use of web application firewalls (WAF) has also grown. Web application firewalls inspect and filter HTTP traffic at the application layer by applying rules (or policies) that are signature/pattern-based, learned or statistically derived to address a multitude of attacks. These vulnerabilities and attacks include injection flaws, cross-site scripting, authentication, encryption and session failure, insecure direct object references, and more (see http://www.owasp.org/index.php/Top_10_2010-Main). Beyond the functionality typically offered by conventional firewalls, application firewalls, whether network or host-based, can monitor and block unwanted inputs, outputs, web application access and subsequent service calls. SIEMs can aggregate and cross-correlate vulnerability and attack events from application firewalls to support incident response and purchase justification.

Databases, and database applications, are not attack-proof – they too require security measures including safeguarding from external and internal threats. Given the potential for IDS and even WAF to be blind due to encrypted traffic and internal operational risks (e.g. database privileged user), organizations should maintain their commercial databases' audit functions. SIEMS have the means to obtain, offload and utilize database audit logs, which are in the form of database tables, to complement overall security monitoring. Additional database security measure can include database firewall technology (which can be similar to web application firewalls but focusing on the SQL application level) and database security applications that employ a combination of database-centric configuration, access and transaction monitoring, vulnerability scanning, threat protection and auditing mechanisms.

The identification of SQL injections, buffer overflow, invalid input and denial of service attacks, exploits of unused database functions or poorly monitored privileges, and other security risks monitored by database-centric security applications should be incorporated into SIEMs. This information, such as monitoring for the use of specific SQL commands or alerting on activity above predefined thresholds, can be further correlated with a variety of security and availability issues, metrics and compliance requirements.

In general, application logs can be more diverse than device logs. With application logs, customers have the potential to monitor and correlate additional custom event attributes. Depending on the sheer number of applications, the focus of application monitoring can be prioritized for mission critical or high-risk applications. As with previous chapters, processes should be in place to review critical web server, database and application events with the means to escalate for investigation. In terms of investigations, the use of shared credentials with regards to database and application administration can hinder or lengthen the determination of who did what action (as discussed in chapter 6).

***Recommended Sample Metrics***

- Web application attacks per server and application
- Wed application attacks remediated
- Top web application attack by type, by source, by destination
- Web and database platform configuration changes
- Web and database platform outages due to configuration changes
- Application platform resource utilization anomalies
- Database application security issues / trends
- Database queries, inserts, deletes, creates that are atypical
- Excessive denied requests (e.g. file, record, page) by web application by source, destination
- Web application errors by web application by type
- Top Critical SQL commands by administrator
- Top monitored database table attribute changes
- Top and unusual Web and database application access
- Top Web application administrative changes
- Top or Unusual application process resource utilization by application server
- Web application outages associated with attacks or configuration changes

***Technology Considerations***

- Sources will include web server and web middleware application logs, database logs, operating system logs, web application firewalls, database firewalls, database security applications, directory services, web application vulnerability scanners
- Database logging can be problematic with regards to database performance and database audit table overwrites
- Use of shared administrative credentials

## SIEM Best Practice #10 – Acceptable Use

Monitor and report on key status, issues, violations and activity regarding the acceptable use of resources and information.

*Subject Coverage*
Resources and application access and use, web and email use, access rights management, use of encryption, data leakage prevention, network flow analysis, account use and policy enforcement.

***Overview and Highlight Processes***
Acceptable use monitoring (also known as Acceptable Use Policy or AUP) covers the appropriate use of infrastructure, application and data resources by authorized personnel according to defined policy.  This requires the publishing of policies from which users can understand when, where and how best to use and protect corporate assets and information – often conveyed in an employee handbook.  AUP is usually most concerned with the access and use of the Internet, applications, email, voicemail, physical business assets, as well as sensitive business data and information.

It is advised that information security professionals obtain legal advice to assure that:  (i) no individual privacy rights are at risk, (ii) the "duty of care" and respective consequence for violations are clear and appropriate, (iii) reporting and notification mechanisms are in place, and (iv) the potential liability for monitoring user activity is understood and addressed.  In addition, acceptable use monitoring requires consistency towards monitoring users for business purposes, teamed with periodic review, authorization, and investigation procedures.

To facilitate monitoring processes for AUP, organizations can develop watchlists for critical resources, user roles and specific AUP violation scenarios that align to policy.  Once defined, operating controls, such as event notification and event logs from systems, encryption applications and data leakage prevention solutions, can be incorporated into SIEM correlation and reporting functions.  In this respect, SIEMS can serve to fortify AUP policy to identify internal threats, material violations, potential fraud and malicious activity.  As mentioned earlier in chapter 3, the penalties for leakage of personal identifiable information (PII) can range from $200-$250USD per record leaked – and at least the highest amount averaged across all state regulatory violations (not including outside the United States).  By not having accurate records with regards to the scope of an incident, the resulting financial penalties and reputation risks can be significant.

Monitoring AUP is usually concerned with being able to answer who and what is accessing which resources, how and when are resources being used, is the access appropriate and necessary, and what actions are users taking within the context of business activity.  This applies to users and privileged users, consultants and other authorized third parties, and intermediary systems.  By obtaining events logs and defining rules within the SIEM to support AUP, SIEMs can automate the periodic review of suspicious activity or policy violations.  By limiting the monitoring scope to areas of interest such as management of key resources or remote access, organizations can minimize AUP enforcement expenditure.  While some organizations review activity conducted during business hours, it is advised to extend activity monitoring beyond normal business hours with special focus on critical assets or anomalous behavior.  To detect fraud and other potential violations can require analyzing statistical profiles of key user activity or establishing operational baselines to monitor thresholds.

There are a variety of AUP use cases which require reference device event log data such as:  the use of web filtering solutions to limit inappropriate internet use; the use of network flow to identify unusual network utilization patters; the use of encryption for network sessions as well as protecting sensitive financial and person identifiable information (PII); the use of data leakage prevention technology to identify sensitive information and unwanted disclosures; the use of configuration management systems to identify unauthorized installation and use of applications; and the use of email, directory service and database audit logs to identify unusual account or administration activity.  All of the aforementioned use cases can be derived from using built-in or creating customized SIEM rules and reports to support AUP.

***Recommended Sample Metrics***

- Top unwanted web sites visited by end user
- Systems with blacklisted software
- System access outside of business hours
- Top and atypical user access to critical resources (systems, directory, files)
- Consultant network resource use
- Top users with anti-virus, web proxy, email filter and DLP incidents
- Top traffic by application and user
- Top traffic to and from geographic locations
- Unusual traffic by application and user
- Administrative access to critical systems
- Authentication failures by privileged users
- Resource access failures
- User activations, privilege change and terminations by device class
- Use of terminated accounts
- Unusual access using service account credentials
- Unencrypted transmission of sensitive data
- Potential sensitive data disclosure violations by category

***Technology Considerations***

- Sources will include all AAA, system and applications logs, web filtering, spam filtering, network flow, data leakage…
- Customization of SIEM analytics (rules, dashboards and reports)
- For fraud, the means to baseline volume of network activity and resource use to identify excessive or anomalous activity
- Means to resolve identity, location and time of activity
- Use of case management functionality

## Conclusion

SIEMs offer the means to convey an organization's overall security posture and provide information security professionals more immediate security operational intelligence. By capturing, analyzing and managing the vast actionable details contained within an enterprise's event log data, SIEMs can help IT organizations:

- Better manage risks and proactively monitor issues
- Efficiently respond to incidents and violations with better collaboration
- Rapidly develop necessary operational reports and measure security program achievement
- Expose process gaps and validate security investments
- Identify potential fraud and facilitate forensics
- Complete investigations faster and with greater accuracy
- Fortify policy with complementary and compensating controls
- Automate compliance processes

and more.

As of the writing of this e-book, a few intersting trends in the SIEM industry are occuring. The first is the gradual adoption of cloud computing and the use of cloud-based elastic resources. With the volumes of security and operational data being captured, processesd and stored, it is likely that IT organizations and SEIM vendors alike will consider the use of cloud-based resources to potentially lower on-going capital expenses associated with SIEM. Depending on the type of data and data privacy restrictions associated with said data, as well as the means for vendors and their prospects to align security policy and guarantee availability requisites, the opportunity to migrate from on-premise to cloud-based SIEM resources will prove valueable. As a hosted SIEM service, organizations will need to well manage incident response and availability managmeent to ensure appropriate integration into IT processes.

Virtual appliances are another technological innovation that is being more widely applied by SIEM vendors. As mentioned earlier in this e-book, traditional hardware appliances, while offering the convenience of a turnkey system and relatively easy implementation, still have fixed processing, storage and scalability limitations. Customers also pay a premium for the SIEM hardware that at some point will need to be replaced. The introduction of virtual appliances allows for companies to leverage a common hardware platform and leverage existing virtualization platform capabilities such as provisioning SIEM resources and taking advantages of high availability options. This enables organizations to grow their SIEM implementation as needed and apply additional resources on-demand.

In cloud based, hosted and expansive data center environments, computing resources can be dynamically provisioned, which in turn can generate new and burst operational data. This is not unlike the condition that occurs when a company is under attack which can result in a dramatic increase in event log data generated by firewalls and intrusion detection system. In many cases, this will peak the events per second processsing load beyond the fixed capcity of a hardware appliance. The potential of dropped event log data, reduced event log data sampling and event SIEM platform failure can put an organization's security posture in jeaporday. The situation may also introduce liabilities in terms of failure to meet serices levels or compliance mandates. Here too, a virtual applicance approach offes the means to provide events per second elasticity to enable continuous monitoring with the flexibilty to handle peak loads due to dynamically provisioned resources or attack.

Managed services presents another popular and growing delivery innovation in the SIEM market. Managed security service providers (MSSP) offer the means to not only off-set SIEM application and capital expense, but also to off-load operational costs and expertise. Since information security personnels are in demand, augementing staff through the use of MSSP's presents a good SIEM implementation alternative for many organizations. The means for an independent third party to manage, respond, track and verify security provisions and incidents can also serve as a higher level of verification for compliance and business auditing. Similar data privacy, incident response, scalability and availability considerations will apply.

Given the ability to correlate massive volumes of data from diverse operational sources, the application of SIEM will advance well beyond security. By combining security-monitoring functionality, with the means to monitor network, system, application and virtualization performance metrics, configurations, events and state changes, corporations will be able to extend their data center visibility and realize benefits across IT functional domains.

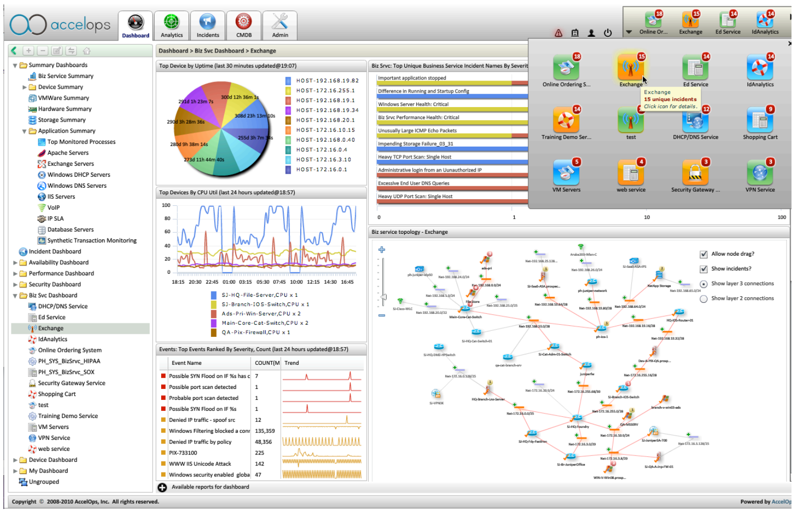
Like any IT automation tool, ensuring success and maximizing value derived from SIEMs will require: organizational endorsement and accountability; planning and alignment to objectives; assessing implementation and operational tradeoffs; policy and process development; appropriate training and support; appropriate deployment, infrastructure activation, tuning and maintenance; as well as feedback mechanisms to enable continuous improvement.

I hope this e-book has provided you, the SIEM novice to SIEM savvy user, some useful and pragmatic takeaways that can help you and your organization take full advantage of what SIEMs can offer.

## About AccelOps

AccelOps offers a seamlessly integrated, unified and service-oriented platform for the collection, monitoring, alerting, analysis and reporting on all IT event log and performance data that cuts through network devices, systems, application, virtualization, vendors and technology boundaries within data center, hosted and cloud environments.

AccelOps not only delivers complete SIEM functionality, it also provides the next logical evolution – a plug and play, scalable virtual appliance solution that gives security and IT professionals a single pane of glass for monitoring all aspects of data center and security operations business service insight.



Exchange
15 unique incidents
*Click icon for details.*

Events: Top Events Ranked By Severity, Count (last 24 hours updated@18:57)

| Event Name | COUNT(M | Trend |
|---|---|---|
| Possible SYN Flood on IF %s has c | 7 | |
| Possible port scan detected | 1 | |
| Probable port scan detected | 1 | |
| Possible SYN Flood on IF %s | 1 | |
| Denied IP traffic - spoof src | 12 | |
| Windows Filtering blocked a conr | 135,359 | |
| Denied IP traffic by policy | 48,356 | |
| PIX-733100 | 225 | |
| WWW IIS Unicode Attack | 142 | |
| Windows security enabled globa | 47 | |

Copyright © 2008-2010 AccelOps, Inc. All rights reserved.

AccelOps offers 360$^0$ intelligence, proactive monitoring, expedited incident response and robust reporting that puts the "who, what, why, when, how and where" at the operators fingertips. The fully integrated feature-set includes:

- Built-in, extensible knowledgebase of rules, dashboards and over 900 reports mapped to best practices
- Real-time correlation, historic analysis and enterprise search
- Compliance and standards-based reports
- Dynamic dashboards and topology maps; incident overlay, object drill-through and incident details
- Multi-factor infrastructure discovery and automated service mapping
- Event, log and network flow data parsing, consolidation and aggregation
- High-performance, layer 7 rules engine with extensive analytics
- Configuration Management Database (CMDB) and change monitoring
- Comprehensive network, system, virtualization and application status, change and incident details
- Multi-layer virtualization intelligence
- Automatic identity and location resolution
- Directory service integration and object monitoring
- Rich database security and performance monitoring
- Mainstream device support and XML-based parsing engine for rapid custom device integration
- Automated service and compliance-relevant grouping for rapid monitoring and reporting
- Real-time and long-term historic search with web-like query, and iterative filtering
- Intuitive and powerful rule and report GUI editor
- Fast report results with complete report generation, customization, distribution and format options
- Full dashboard customization applying any report template or search result
- Broad incident notification options with rich context
- Smart incident management; consolidation, filtering, suppression, exception and state management
- Automated IDS/IPS false positive tagging and exception management
- Built-in case management and trouble ticketing
- Event log data integrity and retention
- Optimized event repository for unlimited online data analysis and high-speed query
- Scalable, clustered virtual appliance architecture for on-demand performance and coverage capacity
- Multi-tenancy for multiple customer/division on-premise, off-premise and cloud monitoring
- Admin Wizards to streamline configuration, integration, maintenance and scale

and more.

Whether you are investigating log management systems, upgrading your present SIM, assessing compliance requisites, or exploring SOC/NOC convergence – explore the AccelOps' difference by taking a 14-day test drive at - http://www.accelops.net/eval-download.

# Author, Acknowledgements, References, Use and Copyrights

***About the author, Scott Gordon***

Scott Gordon is a seasoned enterprise systems and information security industry marketing executive who has worked with the best and brightest innovators over the past 20 years. Scott's SIEM knowledge stems from his work at AccelOps, SenSage and Protego. Protego had developed the once popular MARS security information event management appliance solution acquired by Cisco. Scott has advocated and contributed to the advancements of leading-edge products spanning business service management, event correlation, security information management, network security, anti-malware, penetration testing, encryption and risk management. Scott holds CISSP, ISSMP and ITIL certifications.

***Acknowledgements***

The author has compiled information from a variety of leading industry sources and lessons learned from the field. As with any body of knowledge, the topics conveyed in this book will evolve – keep in touch to obtain updates, as they are made available. To hear a live panel on this subject of “operationalizing security and putting the top 10 SIEM best practices to work,” visit: www.accelops.net or https://www.sans.org. Special thanks to the following industry experts whose prior webcast participation and interactive dialogue contributed content within this e-book:

Dr. Anton Chuvakin – Log management and security compliance expert, consultant and author
Randolph Barr (CISSP) – Chief Security Officer at Qualys and former CSO of WebEx Communications
Tim Mather (CISSP, CISM) – Cloud security expert and former Chief Security Strategist for RSA and CSO at Symantec
Bill Sieglein (CISSP) – Founder and CEO of the CSO Breakfast Club
Jamie Sanbower (CISSP, CSA) – Security CSE at Cisco and prior director of Cyber Security Practice at Force3

Additional sources and thanks to:

- SANS.org for their on-going contribution to the information security field and with specific reference to the “top cyber security risks” and “20 critical security controls”
- National Institute of Standards and Technology with regard to “SP 800-53 and SP-800-92”
- OWASP.org regarding application security risks, and
- Anton Chuvakin for his pragmatic ”Security Warrior” blog site.

***Resources***

For practitioners looking to further explore SIEM subject matter, the following is a short list of recommended sites:
http://www.sans.org/reading_room/whitepapers/logging/
http://www.sans.org/top-cyber-security-risks/
http://www.sans.org/critical-security-controls/interactive.php
http://csrc.nist.gov/publications/nistpubs/800-93/SP800-92.pdf
http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
http://chuvakin.blogspot.com/
http://securosis.com/
http://www.logmanagementcentral.com/files/LogMgmt_Checklist_Oct2010.pdf
http://www.accelops.net

***Use and Copyrights***

This document serves to amalgamate guidance from various industry sources and is for information purposes only. Content and respective accuracy within this document is subject to change. The author make no warranties, express, implied or statutory, as to the information in this document.