SANS Institute
Information Security Reading Room

An Evaluator's Guide to NextGen SIEM

Barbara Filkins

SANS

A SANS Whitepaper

An Evaluator's Guide to NextGen SIEM

Written by **Barbara Filkins**
Advisor: **Chris Crowley**

Sponsored by:

LogRhythm

December 2018

Introduction

A SIEM system provides a central console for viewing, monitoring and managing security-related events and log data from across the enterprise. Because it correlates data from multiple sources, a SIEM system can enable an analyst to identify and respond to suspicious behavior patterns faster and more effectively than would be possible by looking at data from individual systems. Log data represents the digital fingerprints of all activity that occurs across a networked infrastructure—it can be reviewed to detect security, operations and regulatory compliance problems.

To be effective, a SIEM must remain relevant in the face of new threats as well as changes in both the technical and support infrastructures of an organization. Yet, legacy SIEMS are notorious for being difficult to configure and maintain. The average shelf life for a traditional SIEM is 18 to 24 months.[1] Because a traditional SIEM often lacks the capability to produce actionable information, the security team may be unable to justify to management ongoing investment costs such as license renewal, ongoing system management, integration of additional data sources and continued training of personnel.

A modern SIEM should be viewed as a central nervous system, capturing data and generating information that security teams can use as intelligence to detect potentially malicious activity before any damage is realized, providing a safety net that can catch potential threats that might slip through traditional defenses.

[1] www.cmsdistribution.com/top-5-siem-challenges-for-the-mid-market-enterprises

Because of these issues, demand arose for tools that can provide actionable information while optimizing current and future security investments and reducing risk. Next-generation SIEM augments traditional capabilities (automated log management, correlation, pattern recognition and alerting) with emerging and agile technologies (cloud-based analytics; security orchestration, automation and response [SOAR]; user and entity behavior analytics [UEBA]; machine learning and artificial intelligence). Table 1 shows a comparison of the needs of today with "next-generation" capabilities.

Table 1. Core Tenets of NextGen SIEM

Need	NextGen Capabilities
Manage and monitor the modern hybrid infrastructure (e.g., cloud, on-premises, in the hands of users) as a single entity.	• Permit quick integration into an enterprise infrastructure via open architecture. • Meet operational demands of complex, global environments both in terms of performance and maintainability due to scalable architecture.
Visualize related security events across disparate datasets for accurate incident identification and threat detection.	• Curate standard taxonomy of activities from log and machine data. • Employ real-time visualization tools that help gain insight into the most important, high-risk activities.
Detect, classify, escalate and respond to threats in real time.	• Use scenario- and behavior-based analytics to capture well-understood scenarios and indicate significant changes in behavior. • Integrate with and use threat intelligence gathered from commercial, open source and custom sources.
Search efficiently against massive amounts of data captured from a variety of sources, quickly honing in on the data most pertinent to forensic investigation.	• Provide precise and rapid access to data through high-performance and centralized searches on both structured and unstructured data. • Rely on high-scale indexing and storage of forensic data for months or even years. • Use big data architecture to allow storage of source data in its historical or original form. • Enable Elasticsearch capabilities.
Manage and improve repetitive workflows, adjusting to changing organizational needs, policies and systems (e.g., guide incident response more rapidly and accurately after threat detection occurs).	• Support SOAR capabilities. • Provide flexible framework that allows custom workflow implementation for key organizational use cases (e.g., Secure DevOps, incident response).
Represent and manage business risk in terms of organizational compliance and other mandates.	• Measure current status against a regulatory and/or other policy-based framework for risk prioritization and management via a rules engine. • Provide standard (e.g., PCI DSS, HIPAA, SOX) rule sets that are customizable and extensible.

The goal of this guide is to help you develop an actionable procurement process that enables your organization to feel confident in its selection of next-generation SIEM as a key component in the protection and defense of its business and critical assets.

An Evolution of Terms

SIEM technology combines the log management capabilities of what used to be standalone security information management (SIM) systems and security event management (SEM) tools.

- **Log management system (LMS):** A platform that collects and stores log files from multiple hosts and systems in a single location that allows centralized access.
- **Security information management (SIM):** Built on LMS. A type of software that automates the collection of event log data from security devices, such as firewalls, proxy servers, intrusion detection systems and antivirus software.[2]
- **Security event management (SEM):** An LMS targeted toward security managers that addresses security events as opposed to system events. Includes aggregation, correlation and notifications for events from security systems (e.g., antivirus, firewalls, IPS/IDS).
- **Security information and event management (SIEM):** An application which gathers security and event data from information system components and presents that data as actionable information via a single interface.[3]

[2] https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

[3] https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

Visualizing NextGen SIEM: A Reference Architecture

The term *security information and event management (SIEM)* was coined in 2005 by Mark Nicolett and Amrit Williams of Gartner.[4] Since then, organizations have looked to SIEM solutions to help:

- Address compliance requirements, such as PCI DSS, HIPAA and SOX, by capturing and retaining system logs, automating the log review process and providing reports that meet regulatory audit requirements.
- Support operations by pulling together data from disparate systems, allowing for more efficient collaboration among various IT teams, the network operations center (NOC) and the security operations center (SOC).
- Support investigations by storing and protecting historical logs, along with the tools to quickly navigate and correlate the data.

The high-level reference architecture shown in Figure 1 displays the basic requirements needed to fully evaluate a next-generation SIEM.

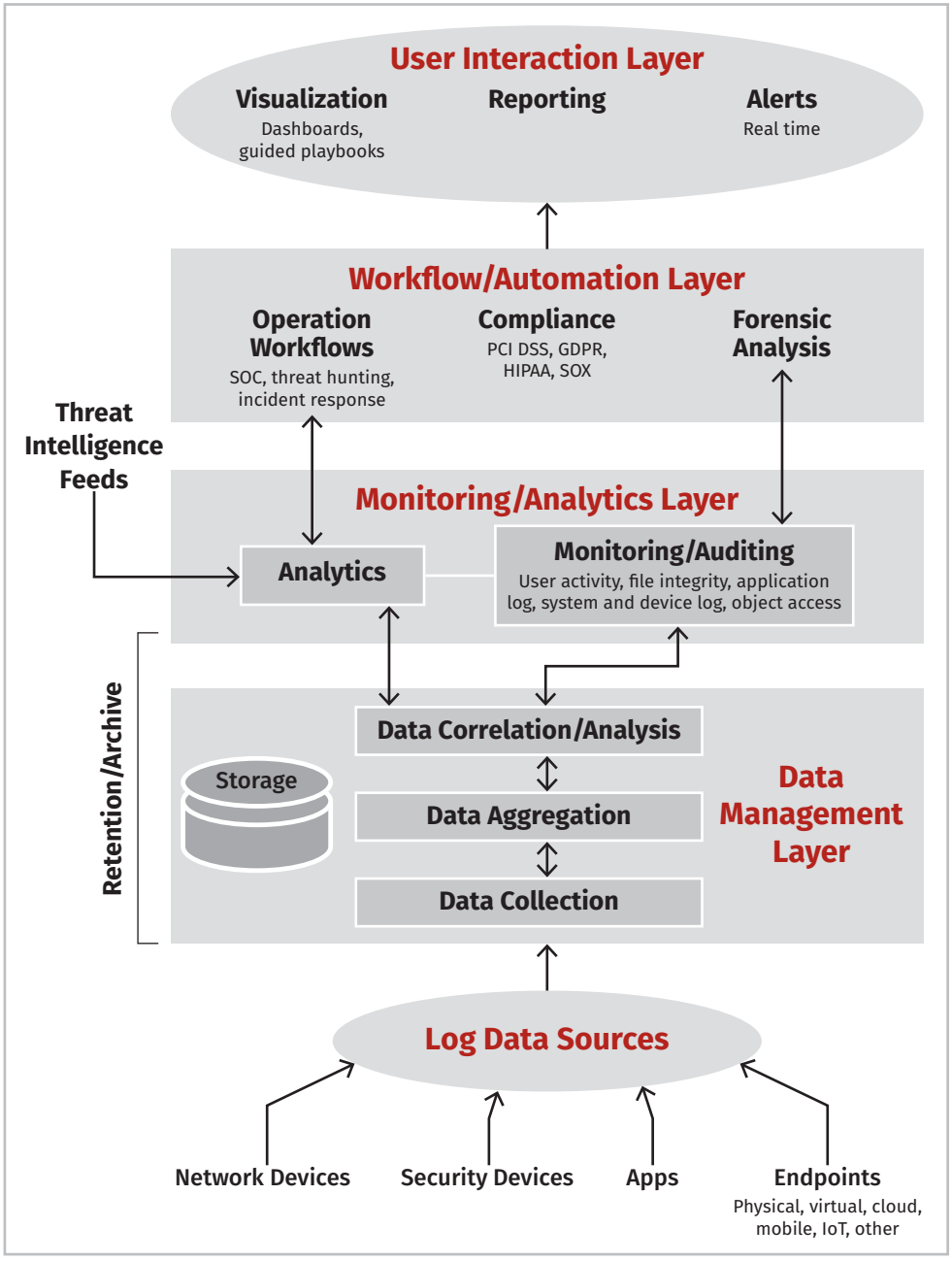

Figure 1. NextGen SIEM Reference Architecture Visualization

[4] www.gartner.com/doc/480703/improve-it-security-vulnerability-management

Table 2 explains each layer in more depth, with the key differences identified in the blue rows.

Table 2. NextGen SIEM Capabilities

Data Management Layer A next-generation solution is built around a big data storage architecture, a compute-and-storage architecture that collects and manages large security data sets for indexing and search, enabling real-time data analytics.	
Capability	**Description**
Data collection	Gathers log data from multiple sources, including network and security devices, applications and various endpoints (e.g., mobile devices, physical servers, virtual servers)
Data aggregation	Gathers and normalizes collected data
Data correlation and analysis	Links events and related data to security incidents, threats or forensic findings
Storage	Provides online access to current and archived log data, and additional artifacts such as reports and visualization snapshots
Retention	Stores long-term historical data, used for compliance and forensic investigations
Monitoring/Analytics Layer Next-generation advanced analytic capabilities are key to identifying hidden threats. They include both complex scenario detection and behavioral modeling to identify and prioritize threats.	
Capability	**Description**
Monitoring/auditing	Provides automated means to detect anomalous behaviors such as those related to user or network activity; works with analytics tools Audits various logs for compliance with standards such as PCI DSS, GDPR, HIPAA and SOX
Analytics	Uses statistical models and machine learning to identify deeper relationships between data and behavioral elements, and presents information in context
Threat intelligence feeds	Combines internal data with third-party data on threats and vulnerabilities and attack patterns
Workflow/Automation Layer A next-generation SIEM can automate and prioritize actions that allow workflow and productivity improvements to organizational security. Positive impacts can be expected in any area in which actions can be orchestrated (e.g., incident response, better triage of alarms or reducing alarm fatigue).	
Capability	**Description**
Operations: Automation	Integrates with other security solutions using APIs, defining automated workflows that should be executed in response to specific incidents Compatible with SOAR tools
Operations: Threat hunting/investigation	Enables security staff to run queries on both structured and unstructured log and event data to proactively uncover threats or vulnerabilities
Operations: Incident response	Helps security teams identify and respond to security incidents, bringing in all relevant data rapidly through case management
Compliance	Builds on audit data to generate reports for compliance with regulations and standards such as PCI DSS, GDPR, HIPAA and SOX
Forensic analysis	Enables exploration of log and event data to discover details of a security incident
User Interaction Layer Next-generation tools provide real-time insight into patterns, trends and correlations that can translate directly into the timely exposure and recognition of troublesome issues or events that might otherwise have gone unnoticed.	
Capability	**Description**
Alerting	Analyzes events and sends alerts to notify security staff of immediate issues
Visualization	Creates visualizations based on real time or historical event data to allow staff to more quickly and accurately identify patterns and anomalies
Reporting	Generates standard and ad hoc reports to support the appropriate workflow, as well as meet specific business requirements

Evaluation Strategy for NextGen SIEM

Acquisition and deployment of a SIEM is an enterprisewide project. The evaluation and procurement should be managed as a project in its own right with a dedicated project manager and team, assigned resources, budget and schedule.

Step 1: Establish the Business Case

Lack of stakeholder involvement is often cited as a reason for project failure.[5] SIEM can affect many workflows that require cooperation across all areas of the organization. Ensure that you include all appropriate stakeholders in the successful use of next-generation SIEM: the operational teams (IT, security and support), audit and compliance, application development, business owners and all levels of management.

Treat the evaluation process as part of the discovery and planning phase of the larger SIEM implementation project that will follow.

To focus the project and ensure continued commitment from all stakeholders, consider developing a project charter, such as the partially completed example shown in Figure 2.

Step 2: Strategize on Requirements

A SIEM is a platform that must be configured to meet the needs of the organization. The actual requirements (and the evaluation of possible solutions) depend on three key, interrelated factors:

- **Operational requirements.** Understand how the platform will fit into your management processes related to operations, compliance, incident and threat response, and risk management. Consider also how easy the platform will be to manage, whether it can meet your performance demands, and if it will scale appropriately as your infrastructure expands.

Project Title: *XYZ Global NextGen SIEM Implementation Project: Procurement Phase*			
Project Sponsor: CIO of XYZ Global		**Project Manager:** (You)	
Estimated Cost: $1,250,000 (variable)		**Project Category:** Strategic Business Need	
Date of Request: 2/1/2019 (variable)		**Target Completion Date:** 10/1/2019 (variable)	
Project Purpose (high level): Improved security posture for critical operation that complies with XYZ Global policies			
Project Description (high level): Remediate IT audit findings to reduce risk level to comply with XYZ Global Enterprise IT Security standards.			
Project Objectives (what project is meant to accomplish): Implement a SIEM that 1) meets the requirements of XYZ Global policies; 2) allows XYZ Global to identify and remediate deficiencies identified in regulatory compliance audits; and 3) brings operations in line with security best practices.			
Critical Success Factors: Commitment from XYZ Global leadership Committed project resources and staff (e.g., project workforce retention) Confidence in selected next-generation SIEM and vendor(s)			
Project Milestones (with key dates): Evaluate and choose SIEM solutions Purchase or design solution Negotiate final price and statement of work Award			
High-Level Risks: Other internal project-consuming resources Lack of participation by stakeholders: 1. PMO for guidance 2. Operational staff (IT and security staff) for evaluation, including proof of concept Inadequate scoping of requirements and business needs Not identifying all stakeholders Inadequate evaluation and proof of concept			
Business Justification for Project: This project is being undertaken for mandatory business reasons, to meet XYZ Global minimum IT security standards. These standards have already undergone business case justification and have become mandatory after the business risks for not complying with them have been reviewed. This project represents the first step in meeting the minimum level of risk acceptance for IT security-related issues for XYZ Global and its subsidiaries.			
Other Important Information (as needed):			
Approval Signatures	*Name*	*Signature*	*Date*
Project Sponsor			
Project Manager			
Funding Approval			

Figure 2. Sample Project Charter (Partially Completed)

[5] www.pmi.org/learning/library/project-scope-statement-skills-tools-7981

- **Technical requirements.** Understand technically how the proposed SIEM solution will integrate with your enterprise infrastructure. Plan on documenting your technical infrastructure in enough depth that the vendor understands your environment and you have a solid basis on which to evaluate the vendor response.
- **Business requirements.** Gather the business requirements (and assumptions), such as cost versus terms of coverage, support and training, and regulatory compliance. Consider the appropriate SIEM deployment model for your organization as well as any additional vendor services you may need.

Define the Operational Requirements[6]

Starting with the initial business case that was presented for next-generation SIEM, evaluate your organization's current security posture and how the SIEM deployment will affect it, taking into account all tasks that must be performed to complete the initial implementation and to support ongoing maintenance and operation. These tasks can range from policy development to workflow modification to planning for increased personnel expense, such as additional training and/or support staff.

First, review and prioritize current security policies and workflows according to the following set of rules:

- Which are important to the business of the organization?
- Which are important for the organization's compliance with regulations or other mandates?
- Which are best practices for maintaining a secure environment?

Next, perform a gap assessment. Are your current workflows and controls actually performing according to plan? Use this "as-is" picture to expose any issues for two reasons: 1) to remediate any critical gaps that an effective SIEM implementation will depend upon, and 2) to identify those issues that a next-generation SIEM can most effectively address. You now have a basic picture of what the daily "to be" environment should look like with a next-generation SIEM in place.

This security policy and workflow analysis can help to target your initial deployment strategy. You know your highest priority business need/use cases. Use this information to implement the next-generation SIEM on the representative subset of your existing infrastructure, gathering critical information to advise on making additional changes and improvements prior to a more complete rollout.

Document the Technical Infrastructure

Gather and organize information about your infrastructure, both to provide to potential vendors and for your team to evaluate vendor responses. At a minimum, you should provide:

- A detailed description of your infrastructure, including the configuration, location and business ownership of computing assets, security controls in use, and the underlying network topology. Sources for this information can include your asset management system, software inventory database, network maps and vulnerability reports.

[6] This section presents only a quick overview on how to develop operational requirements. For more information on developing use cases to support SIEM deployment, see the following presentation: www.sans.org/cyber-security-summit/archives/file/summit-archive-1533050405.pdf

- Acceptable performance expectations and constraints, such as available network bandwidth and latency
- Sizing information, such as number of users and projected growth over the next one to two years
- Data sources for logs and alerts, encompassing both infrastructure assets and security controls (see Table 3)

Table 3. Potential Data Sources for Logs and Alerts[7]

Infrastructure Assets	Security Controls
• Routers • Switches • Network services (e.g., email, DNS) • Physical and virtual servers (e.g., domain controllers, application, database, web) • User endpoints, both fixed and mobile	• Firewalls, IDS/IPS • Endpoint security • Data loss prevention • VPN concentrators • Web filters • Honey pots

Determine the Business Requirements

Selecting the organizational model can help determine your implementation budget as well as shape a draft statement of work (SoW). Table 4 outlines four organizational models that range from fully in-house to fully outsourced.

Self-hosted, self-managed is the primary deployment model for legacy SIEMs. This model can prove complex and expensive to maintain, even if the organization has committed the proper resources and budget. Today, however, there are a variety of options that allow your organization to select a model that best fits operational, business and financial needs. It's important for your organization to evaluate your approach and select the best model based on a realistic assessment of how you plan to support your SIEM into the future.

Table 4. Organizational Models for NextGen SIEM Implementation and Workflow

Model	Your Organization	Managed Security Service Provider (MSSP)
Self-hosted, self-managed	Host SIEM in organization's data center (e.g., dedicated SIEM platform, maintain related hardware and storage systems, manage SIEM with trained security personnel).	Not applicable.
Self-hosted, hybrid-managed	Purchase and maintain software and hardware infrastructure. Co-manage SIEM event collection/ aggregation, correlation, analysis, alerting and dashboards.	Deploy and co-manage SIEM event collection/ aggregation, correlation, analysis, alerting and dashboards.
Cloud SIEM, self-managed	Handle correlation, analysis, alerting and dashboards, and security processes leveraging SIEM data.	Receive events from organizational sources; handle collection and aggregation.
SIEM-as-a-service (totally outsourced)	Handle security processes leveraging SIEM data.	Handle event collection, aggregation, correlation, analysis, alerting and dashboards.

Key Questions to Determine Your Organizational Model

- **Is there an existing SIEM infrastructure your organization wants to maintain?** Consider leveraging the expertise of an MSSP to jointly manage the SIEM with your internal team.
- **Is your organization willing or able to move data off-premises?** A cloud-based SIEM or SIEM-as-a-service can reduce costs and management overhead. If not, self-hosted, self-managed is probably best, with hybrid-hosted as a possible augmentation for lack of SIEM expertise.
- **Does your organization have security staff with SIEM expertise?** If there is no trained staff, consider obtaining analysis services via a hybrid-managed or SIEM-as-a-service model.

[7] These are potential sources. Keep in mind both cloud and additional mobile assets as you develop your actual list.

Document all expectations regarding the services your next-generation SIEM vendor must provide. The SoW should list both required and optional services the vendor or MSSP will provide. Required services should include assistance with implementation (initial and key phases), along with testing and tuning to ensure the product is working as designed and configured for your organization. Other required services, such as security and compliance monitoring, will depend on the organizational model selected.

Optional services include ongoing consultation (remote and on-site) and configuration services. Consulting provides customized assistance to your organization in related activities such as assessment of business risks, key business requirements for security, and the development of policies and processes. Configuration services may address assessments of the deployed SIEM architecture for suggested updates and improvements as well as the integration of additional products.

Step 3: Develop the Evaluation Instrument

The next step is to develop your evaluation instrument and process. Use the next section, "SANS Evaluation Guide," as a guide for developing your requirements. These tables can help you to develop a formal statement of requirements you can use to score vendor technical responses.

You will first define a rating scale that can account for how a vendor's solution will meet your requirements, as well as other important factors, such as whether the feature is demonstrable now or in a time frame defined by the vendor's product road map for its solution.

You should determine what requirements you feel are mandatory versus optional and assign a weight to each requirement based on the importance of the requirement to your organization. Because next-generation SIEM solutions are commercial offerings, vendors may offer some product features or support services that were not accounted for in your requirements. The SANS evaluation process can account for this in the weighting process by considering whether a business need exists for these available features.

Build a numeric scoring sheet, ideally spreadsheet-based, to establish an overall score for how well a vendor responds to organizational requirements.

Next, construct a request for proposal (RFP) structure allowing each vendor to provide additional, supporting product information plus actual pricing and support information in a manner that easily establishes alignment with your requirements. Table 5 shows a sample outline for the RFP to the vendors, what the expected response should be, and the scoring for that section of the vendor response.

Consider requesting each vendor (or at least the top two or three) to walk you through the use cases/scenarios you included in the narrative section of the technical response. You should warn your potential vendors that this walkthrough may be an option. Plan on at least half a day, and if possible, have the meeting face-to-face. Be prepared with a detailed script and questions.

Step 4: Evaluate Potential Vendors

Select the vendors you want to send your evaluation instrument to. Establish a timeline for the responses and wait for them to roll in.

Evaluate and score the responses. Use the scoring results to select your top one or two vendors for an initial product demonstration. From here, you can determine your top vendor and whether (strongly recommended) you want to invest in a proof of concept (POC) with that vendor.

Step 5: Conduct Proof of Concept

A POC allows your organization to get hands-on experience with the product. You will be working with the product in a test environment that simulates your production.

Table 5. RFP Outline and Scoring for Vendor Response

Section	Description/Contents	Scoring (Points Awarded)
General Information	Presents the goals and objectives for the deployment of a next-generation SIEM in your organization.	Not applicable
Organizational Background	Provides background information to allow a vendor to get a feel for your environment, into which its product will be deployed. Include type of business, geographical location of offices, high-level network topology, number and type of data sources, key security policies and workflows, regulations that your organization must comply with, number of users, and other pertinent information.	Not applicable
Vendor Technical Response: Narrative Requirements	Outlines how the vendor should comprehensively describe the solution and how it plans to address the specific needs of your organization. The vendor response should describe: • Which of its product characteristics make it next-generation SIEM, including its specific differentiators • The solution architecture, emphasizing its capability to support and integrate with your current environment and existing assets • Performance limitations and how to overcome them. Ask about sizing, even if the platform is cloud-based! • How the solution will scale to match your projected growth • The process to be used to integrate a new data source into the infrastructure, including a timeline • How the solution operates for one or more use cases that you define. Examples include: - Incident response based on a recent attack scenario - Preparing for a compliance audit, including samples of critical reports - Conducting a forensics investigation based on your sample data	500 total points
Vendor Technical Response: Requirements Matrix	Provides a spreadsheet-based evaluation matrix to be completed by the vendor that delineates how it intends to meet each operational and technical requirement. Spreadsheet should be self-scoring. For example, each requirement will be assigned a point value such as: 0 = Not available 1 = Not available in current release; planned within six months 2 = Available, requires third-party interface 3 = Available, native capability The numerical score for this portion will be based directly on how the vendor completes the spreadsheet.	500 total points
Vendor Management Response: Business Details	Outlines how the vendor will support the solution. The vendor response should include: • A copy of the vendor's standard contract and an SLA tailored to meet your requirements for support and/or service • Summary of vendor's background • Contact information for at least three customer references	500 total points
Pricing	Provides structure for vendor to follow in describing the pricing structure for its product and service offering. The vendor response should include: • Pricing/licensing model for enterprise solutions, including any discount tiers • Any and all limitations to its enterprise pricing	Not scored, but will be used during negotiations

Consider the following when creating the POC.

1. Prepare for your POC.
   a. Ensure that the POC scripts reflect one or more well-defined scenarios. Consider modifying the scenarios you used for the vendor's written response and/or detailed initial demonstration.
   b. Establish evaluation criteria based on your requirements and use cases.
   c. Create a scorecard that evaluates operational requirements and the functionality needed on a 1–10 basis.
2. Establish a lab environment that is a representative subset of your infrastructure and based on the use scenario(s).
   a. Choose a representative sample of the production assets involved in that user scenario. Include configuring one or more custom data sources to see how those procedures work.
   b. Set up equipment to visually capture the information you need to evaluate POC results. For example, you might use screen capture or video technology to remember what the tools did and how they did it.
3. Familiarize yourself with product features, taking advantage of vendor training and support during the POC.
4. Perform the evaluation, keeping in mind you can't fully test scalability during the POC. Focus on the stuff you can see, feel and touch. Evaluate it from the viewpoint of your primary users. Focus on visualization and how the product provides visibility into the infrastructure. Play with the dashboards and the reports.
5. Create appropriate evaluation documents and scripts based on the scenario(s) and previous product evaluation results. You will use this information again when you start deployment.

If evaluating more than one product, maintain consistency across all products being evaluated by using the same process and artifacts developed for the POC with the first vendor.

Step 6: Select Recommended Vendor

At this point, evaluation should be considered complete—a final vendor has been selected. Your organization needs to negotiate the final pricing and SoW along with any legal terms and conditions and support/service levels.

SANS Evaluation Guide

This section lays out the specific elements belonging to the three interrelated requirements described earlier: technical, operational and business.

What features should you look for in a next-generation SIEM solution? How will it integrate into your operational environment? What should you look for in a vendor?

Technical Requirements

Table 6 provides a guide for evaluating the inherent functionality and capabilities of next-generation SIEM solutions.

Table 6. Product Features/Capabilities

Data (Log) Management ***Objective:*** To determine that the data is collected, managed to enable analysis, and retained for historical/archival purposes		
Short Title	**Capability**	**Evaluation/Criteria**
Data Collection	What is the method for collecting data? Select all that apply. • Agent on device • Directly connect using a network protocol or API call • Accessing logs from storage (e.g., syslog server) • Streaming protocol (e.g., SNMP, Netflow, IP Flow Information Export [IPFIX]) Is the SIEM integrated with common cloud systems? Select all that apply. • AWS • Azure • DreamHost • Rackspace Other (Please describe.)	Do the data collection methods meet your organizational requirements?
Data Management	Is all data stored and managed seamlessly, whether located on-premises, in the cloud, or both? Is the data optimized and indexed for efficient analysis and exploration? Does the product allow retention of full source data at reasonable cost? (This enables deep behavioral analysis of historical data, with the capability of catching a broader range of anomalies and security issues.)	Do the data management methods meet your organizational policies for devices and cloud?
Log Retention and Storage	Does the on-premises storage solution follow a tiered model? (Here, "hot" data [needed for immediate use] is on high-performance storage, whereas "cold" data (needed for historical analysis) is relegated to high-volume, inexpensive storage media.) Does the SIEM use data lake technology, allowing practically unlimited data access at low cost? • Amazon S3 • Hadoop • Elasticsearch • Other (Please describe.) Is the SIEM capable of retaining logs and data according to regulatory mandates? • PCI DSS • HIPAA • SOX • Other (Please describe.) What strategies does the SIEM use to reduce log volumes? Select all that apply. • Syslog • Log filtering by source system, times or other rules defined by the SIEM administrator • Summarization that imports only important data elements (e.g., count of events, unique IPs, etc.) is maintained	Bear in mind that the use of data lakes creates new considerations for implementing next-generation SIEM: • Nearly unlimited, low-cost storage based on commodity devices that allows data storage to grow linearly as needed • New tools in the big data ecosystem, which enable fast processing of huge quantities of data, while still enabling traditional SIEM infrastructure to query data via SQL • Retention of all data across a multitude of new data sources, including cloud applications, IoT and mobile devices

Short Title	Capability	Evaluation/Criteria
Logging Data Sources	What systems can feed logs to the SIEM? Select all that apply. • Intrusion detection systems • Endpoint security (antivirus, anti-malware) • Data loss prevention • VPN concentrators • Web filters • Honey pots • Firewalls • Network logs • Routers • Switches • DNS servers • Wireless access points • WAN • Data transfers • Private cloud networks • Applications and devices • Application servers • Databases • Intranet applications • Web applications • SaaS applications • Cloud-hosted servers • End user laptops or desktops • Mobile devices	Does the solution meet your needs as far as which organizational systems feed their logs to the SIEM?
Data Logging for Cloud Infrastructure	Can the SIEM access log and event data from your cloud infrastructure and/or applications? • AWS • Azure • Salesforce • Google Apps • Other (Please describe.) Does the solution provide prebuilt connectors and SIEM integrations with modern cloud technology?	Validate that the product supports needed security monitoring of your cloud infrastructure.
Monitoring/Analytics ***Objective:*** To determine how the vendor supports traditional and next-generation capabilities through big data processing and advanced analytics		
Short Title	**Capability**	**Evaluation/Criteria**
Extensible Analytics	Incorporate new and evolving technologies into the product offering through the cloud to aggressively identify and block attacks.	Validate that the vendor delivers detection, intelligence and analytic capabilities through the cloud and that cloud updates have an immediate impact on SIEM efficacy.
Use of Threat Intelligence	Use threat intelligence to identify malicious behavior and increase endpoint protection over time.	Verify how threat intelligence is incorporated into the product, including how it supports the identification of malicious behavior and demonstrates improved endpoint protection over time.
Threat Intelligence Sources	Gather threat intelligence from multiple sources for integration into SIEM.	Gather the following information: • Number and types of data sources used, both internal and external • Methods by which intelligence information is disseminated • Methods used to evaluate and reuse new threat data

Short Title	Capability	Evaluation/Criteria
Monitoring/ Auditing	Does the SIEM support—whether natively or through interfaces to third-party tools—the following activities in support of monitoring and auditing? Select all that apply. • Asset discovery (Track hosts, services and installed software and services present in the entire environment for improved correlation and context.) • Software inventory (Conduct full binary-level inventory of software packages running on key assets.) • Vulnerability assessment (Identify vulnerabilities across the infrastructure; track historical record for compliance purposes.) • Intrusion detection (Monitor environment for threats; identify known attack vectors and patterns.) • Behavioral monitoring (Track ongoing behavior of observed systems and users.) • Event correlation (Aggregate and analyze information from all security controls to correlate behavior and provide platform for forensic investigation.) • File integrity monitoring (Monitor changes to critical files to identify potential security issues on critical hosts.) • Service availability monitoring (Detect disruptions in availability that indicate a successful attack or compromise.) • Security operations workflow metrics to better understand operational bottlenecks	Are required capabilities provided, either natively or via third-party interface? Which of these capabilities are available on a continuous basis via the SIEM? Can the SIEM use information from asset discovery and software inventory capabilities to correlate with the latest known vulnerability feeds to identify vulnerable services without active scanning?
Automation	How does the SIEM leverage SOAR technology? For example, do SOAR capabilities provide a consistent tool to respond throughout the incident response process?	Can workflows be easily designed and documented, such as automating repetitive steps in an incident response process?
Data Exploration: Query Development	Does the SIEM enable security staff to freely explore data to actively hunt for threats or investigate known security incidents? Are there customizable queries and reports related to activity across the entire organization?	Determine whether the SIEM has the capability to easily: • Collect activity for all binaries (e.g., processes, file changes, registry access, network connections). • Query and report across the entire organization based on custom elements, such as specific events, indicators of compromise (IoCs) and anomalous activity detection.

User Interaction (Visibility and Context)

Objective: To determine how the product provides visibility into security events and attack context

Can the product provide answers to key questions related to detection, response and remediation, such as:

- How did the attack start?
- What happened prior to detection?
- Where else does this attack apply?
- What could the impact have been?
- Should I do anything to recover?
- Are there gaps that should be closed to prevent further attacks?

Short Title	Capability	Evaluation/Criteria
Detection Logging	Log all results from detection of malware/malicious behavior.	Determine what the standard (e.g., minimum) set of data elements is for both activities. Determine whether the administrator can customize (e.g., easily add additional data elements) to this minimum set as needed.
Response Logging	Log all resulting actions taken in response to detection of malware/malicious behavior.	
Logging Formats: Readability	Present all logged information in human-readable format, independent of the administrative interface.	Request a representative sample of logs normalized by the SIEM system.
End-to-End Process Logging	Reveal the full chain of processes affected by the malware/ malicious behavior.	Determine whether the presentation provides insight into the spawning process (for earlier detection on future occurrences), as well as subsequent lateral movement to know where and when to block such malicious behaviors.
Visualization	Provide visualization tools, using both graphical and plain language presentations, for real-time visibility and retrospective analysis of events. Provide role-based access to SIEM data and information that allows visibility for organizational stakeholders.	Review report output to determine ease of interpretation for real-time dashboards and/or reports for both endpoint users and administrators. Determine whether the product has sufficient tools to configure role-based visibility for dashboards, reports that cover details for specific incidents, and/or integration into workflows needed for decision support. Prioritizes alarms (e.g., by risk levels) and provides guided workflows to ensure visibility of the most pertinent activities.
Integration of Visibility and Context Functionality	Provide interface capability (e.g., API) for integration with other tools and data sources for broader detection and response support.	Determine whether the product has a demonstrated integration with external third-party tools and data sources (e.g., use of APIs).

Operational Requirements

Operational requirements go beyond product features. For example, they encompass how a user interacts with the SIEM product at the endpoint, as well as how an administrator manages the product within the organization. Table 7 provides a guide to key requirements and evaluation criteria.

Table 7. Operational Requirements

Performance and Sizing ***Objective:*** To deploy a solution that meets organizational performance requirements and avoids connectivity, hardware, and availability constraints		
Short Title	**Feature**	**Evaluation/Criteria**
Overall Scalability and Growth	Will the product adequately support current event volume and projected growth?	Review whether there will be any product-related performance limitations related to event volume and dependencies on growth of the infrastructure (e.g., number of endpoints in the organization). Determine whether the product will scale to meet growth projections without issue.
Velocity	Does the SIEM meet events per second (EPS) benchmarks?[8] • Normal time • Peak time (e.g., during an attack) Does the SIEM allow for growth with an additional 10 percent for headroom and another 10 percent for growth? Is there a need to encrypt/decrypt data?	Does the solution meet these benchmarks, especially critical for on-premises solutions? Can the network infrastructure support the overhead, or will it limit performance? What is the performance overhead that comes with the need to encrypt/decrypt data?
Storage Demand	Determine the storage requirements by asking: • What storage formats are in use (e.g., flat file format, relational database, unstructured data store such as Hadoop)? • Can data be moved to the cloud to take advantage of lower storage costs? • What technology is used to compress log data? What is the compression ratio? (Many SIEM vendors advertise compression ratios of 8:1 or more.) What is the projected growth in storage and the drivers behind the growth?	Hardware sizing is more important for on-premises storage, but cloud-based services also have a cost related to data volumes. Make sure your sizing reflects both your current needs and future growth for at least two years.
False-Positive Rate	Minimize false-positive events and noise.	Validate that protection meets goals on diverse system environments, including developer systems, which contain a lot of internally produced and/or third-party software; and servers that are tightly controlled and rarely change. Does the SIEM recognize activities with a high degree of accuracy and minimal tuning?
Failover and Redundancy	What are the methods used to provide a high-availability, redundant SIEM architecture?	Is there a business continuity plan in place that demonstrates that the proposed architecture is feasible?

[8] www.sans.org/reading-room/whitepapers/analyst/benchmarking-security-information-event-management-siem-34755

Interoperability and Interfaces ***Objective:*** To determine the capability of the product to integrate with existing tools/security tools in the organization		
Short Title	**Feature**	**Evaluation/Criteria**
Standard Integration: Third-Party Products	Have standard methods to interface/integrate with other external tools or platforms.	Determine whether the vendor currently supports standard interfaces allowing integration with external enterprise tools or platforms used in the organization.
Custom Integration: Third-Party Products	Have standard specifications for interfacing the product with other enterprise workflow and security tools defined in your environment (e.g., IT ticketing and Microsoft Windows AV systems).	Determine capabilities (e.g., API for SIEM systems) for developing custom interfaces and whether professional services are available to develop these if needed. If your organization is an application software provider, make sure that any custom programming will work with the SIEM product.
Enterprise Management ***Objective:*** To determine whether the product's approach to enterprise management fits organizational expectations concerning ease of use, customization and interoperability with other enterprise tools		
Short Title	**Feature**	**Evaluation/Criteria**
Management Console: Configuration	Support one or more of the following management console configuration options: • Cloud-based console that runs on vendor servers • Server-based console that runs on the organization's server Virtual appliance-based console (preconfigured by manufacturer)	Determine which console configuration is best for your organization and whether these requirements can be met better with an on-premises, cloud or hybrid (cloud and on-premises) environment.
Management Console: Usability and Customization	Provide a well-designed, easy-to-use and (if required) customizable user interface to the management console.	Evaluate overall console design for overall ease of use, simplicity of navigation, access to major features in an emergency and richness of integrated help functions. Evaluate the capability of the management console to customize the user interface and reporting features to meet your specific needs.
Rules Management	Provide support for rules management, including ease of use for preconfigured rules and capability to quickly develop new rules as changes are made to the infrastructure.	Evaluate ease of use for preconfigured rules and the development of new rules by administrators with various skill levels. Evaluate how long it takes for rules to be updated based on changes to the infrastructure.
Status Monitoring	Support status monitoring, which includes: • Dashboard that reflects the overall status of the infrastructure, including integration of information that is external to security operations • Status of individual endpoints • Alerts and warnings with risk-based prioritization related to the detection of malware/malicious behavior	Review capabilities for monitoring overall status (a dashboard that reflects all endpoints), as well as the capability to quickly drill down on a given endpoint if there is an issue. Determine how the console alerts the admin to the details of problems on an endpoint (e.g., client out of date, unresolved malware detection, protection disabled). Determine whether the product provides any mechanisms to remediate the problem identified in an alert or warning (e.g., remove, deactivate or reactivate a device from the management console).
Audit Logging	Monitor and collect system health statistics to provide proof of agent uptime and show policy compliance.	Validate that appropriate audit logs are created and accessible in accordance with policy.

Business Requirements

Finally, consider the business requirements—those factors directly tied to what the product will cost to deploy and the potential to accrue benefits. Table 8 provides a look at the features and criteria for evaluating your long-term relationship with the vendor, especially in terms of support and responsiveness to your organization's evolving needs.

Table 8. Business Requirements

Complies with Regulatory Requirements ***Objective:*** To ensure that the product can meet any regulatory or corporate compliance requirements		
Short Title	**Feature**	**Evaluation/Criteria**
Compliance Validation	Support the needs of the business relative to compliance mandates or directives.	Confirm the product is in compliance with all relevant regulatory or organizational policies.
Deployment and Licensing ***Objective:*** To determine overall costs associated with SIEM		
Short Title	**Feature**	**Evaluation/Criteria**
Deployment Model	Support one or more of the following organizational deployment models: • Self-hosted, self-managed • Self-hosted, hybrid-managed • Cloud SIEM, self-managed • SIEM-as-a-service (total outsource)	Evaluate the trade-offs (e.g., costs/benefits) of the organizational models offered by the vendor. Determine staffing requirements for each model, for example, and compare those needs with your staffing goals. Also determine which model best supports the way your endpoints are deployed and the business functions they're performing. Determine whether initial deployment will require the vendor to use third parties or professional services. Find out how long initial deployment will take and whether the process will disrupt any production services in your organization.
Licensing	Provide various licensing options, including a description of what is included in the maintenance and support agreement for each.	Use this information to determine the overall ROI or TCO for the SIEM solution based on the business requirements of your organization. These requirements may shorten your list of potential SIEM vendors to be considered.
Support ***Objective:*** To determine the best support approach for SIEM		
Short Title	**Feature**	**Evaluation/Criteria**
Support Structure	Provide various support tiers: • Standard business hours • 24x7, excluding or including national holidays • Expedited service	Before making a decision on support levels, evaluate vendor responses to the following questions: • What are the hours for each support level? • Is either local support or support provided by a third party available? • Can you reach a live person when you need help?
Product Training	Provide product training: • Course(s) for both end users and administrators • Variety of delivery options (e.g., web-based, electronic media-based, instructor led, on-demand and/or custom training)	Evaluate the training available. • Who provides training? • How well does training meet organizational expectations and skill levels? • Do the delivery options support organizational needs? • Can the training be recorded to support a "train the trainer" approach?
Service Level Agreements (SLAs)	Provide standard SLAs that include: • Service desk responsiveness • Professional services	Determine whether the vendor provides a guarantee on software performance or supports SLAs. Can the vendor's SLAs be tailored to meet organizational business needs?
Professional Services	Describe professional services available that are associated with SIEM, such as: • Project planning/management • Interface development • MSSP or SOC services	Evaluate services that can enhance the effectiveness of the SIEM deployment.

Documentation ***Objective:*** To evaluate vendor-provided documentation		
Short Title	**Feature**	**Evaluation/Criteria**
Documentation	Provide documentation for: • End user • Administrator • Technical specifications • API guides for integration Provide documentation in one or more of the following formats: • Electronic media • Paper • Online	Consider the following in evaluating documentation: • Is the external documentation (manuals and online knowledge base vs. built-in help) clear, correct and understandable? • Does your organization have the right to copy or record documentation? • Can your organization tailor documentation to its specific needs, such as customization for organizational workflows? • Are there additional costs associated with documentation or customization?
Vendor Background ***Objective:*** To verify vendor experience and statements related to SIEM		
Short Title	**Feature**	**Evaluation/Criteria**
Vendor Stability	Confirm that vendor has been in business for several years with an established client installed base. Consider the factors your organization routinely uses to assess vendor stability and background.	Ask the vendor for several client references. Contact them and consider their experiences as they relate to your business requirements.
Product Road Map ***Objective:*** To determine whether the vendor's growth path for the product aligns with your organizational needs		
Short Title	**Feature**	**Evaluation/Criteria**
Product Road Map	Confirm that vendor has a product road map for its SIEM product, both standalone and in conjunction with other vendor-provided tools, if appropriate.	Does the vendor product road map align with your business needs? Does the road map address key elements, such as: • Segmented security policy • Threat detection • Application control • Incident response • Threat hunting • Security analytics

Conclusion: Beyond Procurement

Your evaluation and procurement project can provide a strong foundation for your implementation of a next-generation SIEM solution. But, remember, the investment by your organization does not stop with the initial deployment. Hackers never stop developing more sophisticated methods of attack, so you must continue to evolve to remain one step ahead of your would-be foes. In other words, you have to keep on top of change. Your organization needs to adopt a culture of continuous improvement.

Next-generation SIEM allows you to concentrate on the key factors that can measure the security maturity of your organization and provide guidance on how to improve across all areas—people, processes and technology. Use the key features of next-generation SIEM to keep on top of that needed change.

About the Authoring Team

Barbara Filkins, a senior SANS analyst, holds several SANS certifications, including the GSEC, GCIH, GCPM, GLEG and GICSP, the CISSP, and an MS in information security management from the SANS Technology Institute. She has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, plus the legal aspects of enforcing information security in today's mobile and cloud environments, particularly in the health and human services industry, with clients ranging from federal agencies to municipalities and commercial businesses.

Christopher Crowley (advisor), a senior SANS instructor and course author for SANS courses in Managing Security Operations and Incident Response Team Management, holds multiple certifications. He received the SANS 2009 Local Mentor of the Year award for excellence in providing mentor classes to his local community. Chris is a consultant based in Washington, D.C., who has more than 15 years of experience in managing and securing networks. His areas of expertise include network and mobile penetration testing, mobile device deployments, security operations, incident response and forensic analysis.

Sponsor

SANS would like to thank this paper's sponsor:

LogRhythm®
The Security Intelligence Company