



SIEM BUYER'S GUIDE

SECURITY INFORMATION AND
EVENT MANAGEMENT



DOMAINTOOLS®

SIEM: A BUYER'S GUIDE

TABLE OF CONTENTS

1. Introduction	1
2. What is SIEM	2
3. Who Uses SIEM Solutions?	3
a. SOC	3
b. CSIRT	3
c. Threat Hunters	3
4. How to Evaluate a SIEM Solution	4
5. How to Get Started with a SIEM Solution ...	5
6. How DomainTools Can Help	6

INTRODUCTION

Security Information and Event Management (SIEM) solutions have become an integral piece of IT and Security operations. SIEM solutions gather logs from applications and networks that includes end-user devices, servers, network equipment, firewalls, antivirus, and intrusion prevention systems. From these logs, events are fed to the console where Tier 1 and Tier 2 SOC analysts can sift through the noise and establish if the events are incidents to initiate the proper protocol. However, the proper collection of raw logs in a SIEM solution for aggregation and the ability to uncover abnormalities, create appropriate policies, and set rules for analysis can be overwhelming for most organizations.

According to the U.S. National Institute of Standards and Technology (NIST), “the most prevalent arrangement is for the organization to outsource 24-hours-a-day, 7-days-a-week (24/7) monitoring of intrusion detection sensors, firewalls, and other security devices to an offsite managed security services provider (MSSP). The MSSP identifies and analyzes suspicious activity and reports each detected incident to the organization’s incident response team”.

SIEM: SECURITY INFORMATION AND EVENT MANAGEMENT

WHAT IS SIEM

SIEM is an approach to security management that combines security information management (SIM) and security event management (SEM) functions into one security management system. The foundational principle of SIEM is the aggregation of data that is relevant to an organization from multiple sources. Certain organizations will leverage a SIEM solution to stop abnormalities and associate an action. Sophisticated organizations will leverage correlated data in conjunction with user and entity behavior analytics (UEBA) or security orchestration and automated response (SOAR).

According to Gartner, SIEM solutions need to meet the core capabilities of basic security monitoring, advanced threat detection, and forensics & incident response.

 splunk®

 exabeam

 graylog

 IBM Security

 RAPID7

 LogRhythm®

 McAfee™

 MICRO
FOCUS

 ArcSight
An HP Company

 SECURONIX

WHO USES SIEM SOLUTIONS?

SOC (SECURITY OPERATIONS CENTER)

The SOC is a unit within the larger information security group that is tasked with the identification of incidents through real-time monitoring. For most SOCs the event triage process looks for suspicious and potentially malicious activity within the networks and systems and analysts determine the scope of the incident. An integral solution for capturing log data, is crucial for analysts to be able to spot abnormalities and true-positive events.

CSIRT (CYBER SECURITY INCIDENT RESPONSE TEAM)






In larger organizations, there may be an established CSIRT but for the majority of organizations, the functions of a CSIRT exist without the formal labeling of a CSIRT. Ultimately, the Incident Response (IR) function would be responsible for the following in triaging an event; severity, solution/workaround, cross-departmental collaboration, dissemination of threat vectors, and the maintenance of incident and vulnerability data to refine the incident management process.

THREAT HUNTERS

As organizations reach a level of basic security hygiene and proper implementation of solutions, they often look to threat hunting as a way to cover additional threats to their network. Often times APTs (Advanced Persistent Threats) demand significantly more effort and attention from the SOC and CSIRT, but the foundational pieces to threat hunting can be firewalls, antivirus, endpoint management, network packet capture, and SIEM solutions.

HOW TO EVALUATE A SIEM SOLUTION

When looking to onboard a SIEM solution, organizations often look at the following:

 Threat Intelligence Feed	Does the solution push or pull from the feeds needed to maintain or improve an organization's security posture?
 Forensic Capabilities	When capturing events, can the solution capture the appropriate information to arm investigations?
 Integrations with Multiple Controls	Can the solution work towards triage and remediation by pushing or pulling actions to or from other solutions?
 Artificial Intelligence / Machine Learning	Leveraging the continuous data set, can the solution improve on accuracy through unsupervised or supervised machine learning?
 Compliance Reporting	Can the solution provide the organization with the needed regulatory compliance standard reports?

CHECKLIST

- How do you want to identify threats?
Raw log form vs. descriptive
- Can the solution integrate or pull from other data sources to establish risk levels to events?
Also, can they be weighted based on severity?
- Does the platform allow for measurement and reporting on configured changes to devices?
- Are you able to gather asset-based information for devices on your network?
- Can you track both server, application, and network behavior to look for anomalies based on communication?
- Does the solution provide alerting options, to adapt to how your team would like to be notified?
- Will the platform support the monitoring of user activity, logging in, applications usage, etc.?
- Does the solution provide the ability to track from the original source of an event to the destination?
- Can you establish policy enforcement for existing and updated defined policies?
- Will the platform integrate with SOAR platforms?
- Does the solution integrate with ticketing systems?

HOW TO GET STARTED WITH A SIEM SOLUTION

The core competencies of a SIEM take a significant amount of internal evaluation on how your systems currently run and what the changes/impacts to those systems are going to be when onboarding a SIEM.

SOME THINGS TO LOOK AT ARE:

AGENT VS. AGENTLESS

Agent - a software agent is installed on each host that generates logs, extracting, processing and transmitting data to the SIEM server.

Agentless - the log-generating host transmits its logs to the SIEM or there could be an intermediate logging server involved (ie. syslog server).

COST

The cost to implement a SIEM solution can be shocking to most organizations as it is established based on the following:

Data Collection	Storage of Data	Processing
Threat Intelligence Feeds	Hardware	Management

HOW DOMAINTOOLS CAN HELP

DomainTools enables organizations to take indicators from their network, including domains and IPs, and connect them with active domains on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.



PHISHEYE

Discovers newly-registered domain names with the ability to identify existing and new domains that spoof legitimate brand, product, organization, or other terms, for defensive or investigative actions.



IRIS

Combines enterprise-grade domain intelligence and proactive risk scoring with industry-leading passive DNS data to guide threat investigations and uncover connected infrastructure.



DOMAIN RISK SCORE

DomainTools Risk Score predicts how likely a domain is to be malicious, often before it is weaponized. This can close the window of vulnerability between the time a malicious domain is registered, and when it is observed and reported causing harm. The Domain Risk Score algorithms analyze a domain's association to knownbad infrastructure, as well as intrinsic properties of the domain that closely resemble those of known phishing, malware, and spam domains.



APIs

The DomainTools APIs bring a critical subset of capabilities to third-party products and custom integrations, enabling rapid in-context profiling of domain-based threats and effective pivots that help build comprehensive lists of malicious infrastructure.



To test the power of DomainTools or get pricing information:

WWW.DOMAINTOOLS.COM • SALES@DOMAINTOOLS.COM • 206.838.9020