Evolution of Security Information and Event Management (SIEM)

Security information and event management (SIEM) solutions were introduced at the start of the 21st century and combine two functions, SIM (security information management) and SEM (security event management), into one solution which gives organizations a holistic, real-time view of potential adverse activity within their data environments. SIEMs aggregate log and event data generated by organizational assets, such as security software and appliances, network infrastructure devices, and applications. The SIEM analyzes this data, identifies anomalous activity, and generates an alert.

Early SIEMs had limited functionality. Rules and analysis were entirely manual and dependent on a predefined set of correlation rules, which were effective against known threats but fell short against unknown threats and insider attacks. The ability to interface with downstream IT and security systems was limited or non-existent, historical data retention was limited, and dashboards and visualizations were primitive.

Modern SIEMs have been developed with advanced features such as smart analytics, full integration with downstream systems, long-term event storage, and comprehensive dashboards, visualizations, and reporting tools.

Why use a SIEM?

Since SIEMs were first introduced, organizations have used them to facilitate compliance; early adoption of SIEM systems was largely driven by PCI DSS compliance.

Modern SIEMs continue to play a major role in achieving and maintaining compliance by providing functions that are required by regulatory and industry compliance frameworks, including PCI, DSS, HIPAA, HITECH, GLBA, and FINRA.
SIEM Functionality That Help Meet Compliance Requirements

- Log management, review, and retention, including automated audit trails
- Log protection hashing, time-stamping, and encryption
- Tracking and monitoring of access to network resources
- File integrity monitoring and change detection
- Real-time alerts of anomalous activity
- User and device activity monitoring
- Asset discovery and inventory

Most SIEMs also include an out-of-the-box compliance reporting function, which makes audit reporting less onerous and time-consuming. Additionally, organizations are able to customize these reports for internal use cases, such as ensuring policy adherence, assessing vulnerability management, and designing incident response plans.

Effectively Monitor Today’s Complex Data Environments

The rise of cloud computing, the Internet of Things (IoT), and remote workers have made modern data environments highly complex, and organizational cyberattack surfaces are expanding significantly.

According to Flexera’s 2020 State of the Cloud Report, 93% of enterprises have a multi-cloud strategy, and 87% have a hybrid cloud strategy. The COVID-19 pandemic is driving further cloud migration; 40% of businesses report accelerating their cloud adoption plans due to the pandemic. Organizations are embracing IoT devices as eagerly as they are cloud computing. Gartner predicts that the enterprise and automotive IoT market will grow to 5.8 billion endpoints in 2020, up 21% from 2019.

Every cloud resource and IoT device in an organization is vulnerable to cyberattacks, and all of them need to be monitored in real-time.

A small SIEM deployment has up to 300 event sources, generates up to 1,500 events per second (EPS), and can store up to 800 GB of data.*

A mid-sized deployment has up to 800 event sources, generates up to 7,000 EPS, and can store up to 8 TB of data.*

A very large deployment has thousands of event sources, may generate more than 25,000 EPS, and offers over 50 TB of data.*

Most of this event data is harmless “noise.” SIEMs are designed to filter out the majority of this noise and alert SOC security personnel only to potentially high-risk situations that warrant further investigation.

A Note About SIEM Monitoring

While SIEMs are useful tools, they do not replace oversight by skilled security personnel. Even after filtering out noise, a SIEM installed in an average organization generates 10,000 alerts per day; larger organizations can receive 150,000 per day or more. Sifting through these alerts to identify and act on the real threats requires an enormous amount of work and time which results in SIEM oversight, comprising the highest cost component of using a SIEM solution effectively.

*Ponemon Institute
Defend Against Today’s Complex Cyberattacks

The cyber threat landscape is highly dynamic, and cybercriminals quickly adjust their attack methods to avoid new defenses and constantly look for ways to detect and take advantage of new vulnerabilities. Not surprisingly, cybercriminals were quick to seize on the chaos, confusion, and anxiety caused by COVID-19. In April 2020, Google’s Threat Analysis Group reported detecting 18 million COVID-19-themed malware and phishing attempts each day*. Many of these phishing attacks were laying the groundwork for ransomware attacks. Between Q4 2019 and Q1 2020, ransomware attacks rose 25% and became the most common type of cyber threat, surpassing payment card theft.**

Q1 2020 also saw rapid growth of a new ransomware tactic called double extortion, where cybercriminals publicly release or sell data stolen from organizations that refuse to pay ransomware demands. In one double extortion incident, cybercriminals using the REvil ransomware variant attacked the National Eating Disorders Association, downloaded sensitive files, and warned the organization that if it didn’t pay the ransom, their information would be published on a public blog. After the organization refused to pay, the attackers followed through on their threat and released confidential patient data.***

SIEM solutions are key tools in defending against complex cyberattacks. The real-time network monitoring provided by a SIEM enables organizations to assess and respond to threats immediately, when they can still be stopped or mitigated. After an incident has occurred, automated audit trails allow security personnel to reconstruct the event, identify any remaining advanced persistent threats, and harden network systems against future attacks. The advanced analytics feature enables personnel to conduct computer forensics investigations, gather evidence, and preserve this information for future presentation in court.

*Google: “Helping you avoid COVID-19 online security risks”, **ZDNet: "Ransomware is now the biggest online menace you need to worry about - here’s why", ***Tech Republic: “How ransomware attackers are doubling their extortion tactics”
Guidance for Evaluating Alternative SIEM Systems

All SIEMs collect, categorize, and store log and event data, correlate related events and interpret correlation results, generate security alerts, and run queries and reports. However, organizations need more than bare minimum capabilities to effectively secure their data environments and maintain compliance.

A Robust SIEM Solution Should Include:

- **User and event behavioral analytics (UEBA).** UEBA uses machine learning and deep learning to model the behavior of users and devices on organizational networks. This allows SIEMs to continuously refine their own accuracy, enabling SIEMs to detect threats that static correlation rules cannot. These include anomalous behavior with no set patterns or rules; and complex attacks spanning multiple users, IT devices and IP addresses. UEBA also makes it possible for SIEMs to monitor large numbers of cloud assets and IoT devices.

- **Real-time event monitoring, and real-time application of UEBA and correlation rules.** In today’s threat environment, “near-real-time” isn’t good enough. The ability of a SIEM to monitor, analyze, and apply rules and smart analytics in real time can make the difference between a successful cyberattack and an attack that was stopped.

- **Active Directory monitoring.** As cybercriminals evolve their methods to compromise credentials and data, it is essential that SIEMs monitor all changes to critical systems, such as Active Directory.

- **Privilege escalation detection.** Privilege escalation is a key component in advanced attacks. Once cybercriminals have compromised an account, they attempt to expand its privileges, either by increasing the privilege level of the compromised account (vertical escalation) or by seizing control of more accounts (horizontal escalation).

- **Long-term historical analytics and machine learning.** By analyzing past events and learning from them, SIEMs enable security analysts to detect subtle trends that are warning signs of a future attack.
A Robust SIEM Solution Should Include: (Cont’d)

**Search and reporting on both raw and normalized data.** Not all event data is “pretty.” A modern SIEM can aggregate data from nearly any source and use it to distill actionable intelligence. Security personnel must be able to search this data and use it to create alerts, data models, pivots, reports, and shareable dashboards.

**Forensics capabilities.** The SIEM should have the ability to ingest context data, such as headers and packet contents, for additional correlation and analytics.

**Out-of-the box compliance reporting.** In addition to built-in reports for common frameworks, the SIEM should allow the organization to customize standard templates and create custom compliance reports.

**Integration with downstream controls.** The SIEM should integrate with other enterprise security controls to prevent or stop attacks in progress.

**File integrity monitoring (FIM).** The SIEM should continuously monitor all files and generate real-time alerts for unauthorized access and changes to files, folders, and registry settings.

**SECNAP’s CloudJacketX Managed SIEM**

SIEMs were originally designed for the large enterprise market, and many SIEM vendors are still focused on these major clients. Because monitored SIEM services are cost-prohibitive for much of the SMB to mid-enterprise market, SIEM vendors frequently offer lower-tier packages that offload some or all of the monitoring activity (and cost) to the client.

Companies that decide to purchase a low-cost SIEM option usually regret this decision. SIEMs need to be monitored by human staff 24/7 so that identified threats can be responded to immediately. Most small to mid-market organizations lack the in-house expertise, staffing levels, and budget to provide round-the-clock SIEM monitoring and threat management.
SECNAP’s CloudJacketX Managed SIEM

SECNAP’s CloudJacketX Managed SIEM is a groundbreaking security-as-a-service solution that provides superior layers of detection and protection at a fraction of the price of competing solutions. Because early identification is of no value if a threat is not stopped, the CloudJacketX Managed SIEM combines our fully managed SIEM with managed detection and response (MDR) services, enabling SECNAP to respond immediately and block cyberthreats in real-time.

- **Real-time security monitoring** from our 24/7/365, U.S.-based SOC, staffed by U.S. citizens who are all SECNAP employees.

- **Incident response** in compliance with NIST SP 800-61, Computer Security Incident Handling Guide.

- **Threat intelligence.** SECNAP develops our own threat intelligence in-house through a network of globally deployed sensors and honeypots which tracks the spread of international threats and views hacking activities in different regions, including the development and testing of malware. This allows us to program our systems and create patches which can block emerging malware well ahead of it being released into the wild.

- **Behavior Profiling/Data & End User Monitoring.** Immediate investigation of anomalous activity, such as strange DNS lookups or a user logging in at odd times.

- **Application monitoring** allows SECNAP to alert clients if they are running outdated software that could leave them vulnerable to an attack, as well as notify them when their end users install or modify apps.

- **Forensic capabilities.** Logs are automatically sent to the SIEM so that analysts can analyze past events; these logs can also be presented as a defense in court cases. One year of archived log data is retained for all devices.

- **Active Directory Monitoring:** allows our SOC to monitor when modifications such as add, change, remove and escalation of privileges, are made to computers, groups, group members and policies.

- **Analytics.** One central dashboard allows clients and technology partners to view the same information our SOC does, including when users are logging on and off.

- **Flexible deployment options,** with the ability to receive logs in real time, on-prem or in the cloud, from any device that can export them.

- **Event collection rate suited for very large scale deployments.** SECNAP sizes our hardware and virtual machines based on each client’s individual needs, so that our hardware will never slow down a client’s network.

- **Highly intuitive log search,** with a web interface to search either current day or historical logs, retain, and retrieve them for compliance purposes, with reports to enhance visualization.

- Can be configured to meet any SIEM-related compliance requirements, including PCI DSS and HIPAA.
About SECNAP Network Security

Since 2001, SECNAP Network Security has been combining human intelligence with innovative technology to protect organizations of all sizes against cyber threats, including data breaches, ransomware, phishing, and advanced persistent threats (APTs). Our proprietary, patented and patent pending CloudJacketX managed security-as-a-service platform addresses common pain points faced by IT teams, such as alert fatigue, challenges with meeting regulatory compliance requirements, lack of resources, and hidden vulnerabilities.

SECNAP’s proactive cybersecurity approach combines ongoing network security assessments with managed detection and response (MDR) services, an advanced SIEM solution, and a patented intrusion detection and prevention system (IDS/IPS) to provide multiple layers of detection and protection, which are monitored 24/7 by our U.S.-based security operations centers (SOCs). SECNAP utilizes proprietary security technologies that were developed in-house.

Choose a managed security service provider that will secure your data and help facilitate compliance.