2023

seceon

THE MSP & MSSP INSIDER

BUYER'S GUIDE TO SIEM PLATFORMS

Look inside for requirements lists and sample questions to ask your shortlisted vendors.

Executive Summary:

MSP/MSSP -

Building a successful Managed Services Provider (MSP) or Managed Security Service Provider (MSSP) business is challenging, and over the decades, new technologies, new processes and new business practices have come and gone.

Whether you are working to add more managed security services to your MSP or you are an MSSP responsible for the people, process, and technologies needed to drive an effective, efficient, and profitable service, you are likely to be making some key strategic decisions in your technology and delivery stack.

One of the most fundamental choices that a successful managed services provider makes, is the stack they use to run their security services. And the most fundamental component of any stack has always been the SIEM. MSSPs fully understand this, and for years many MSPs have avoided a SIEM as legacy SIEMs built a reputation as giant databases of logs that required expert security analysts to query and derivative value from.

Legacy SIEM and even their new incarnation as “Next-Gen SIEM” - continue to add weight and cost to a team without truly adapting to today’s zero-day threat world and expanding attack surfaces.

And today, as more service providers search for newer ways to tackle the core challenges MSPs/MSSPs are being courted by MDR, XDR, SOC as a Service, and legacy SIEMs claiming to have a new approach, the fact remains - building a successful and profitable service provider business remains hard.

WHY SIEM:

Security Information and Event Management (SIEM) software helps organizations manage security by filtering and prioritizing security alerts.

SIEM software can (but not all do this complete list):

- Aggregate data from multiple sources, such as logs, network devices, events, identity, endpoints, and application data
- Identify unusual activity
- Alert security personnel of potential threats
- Identify an attack path across an attack surface
- Identify compromised sources
- Provide automated mechanisms to stop attacks in progress
- Collect and analyze log data from all digital assets in one place
- Provide the evidence and reports needed for auditors
- Make it easier for teams to monitor and troubleshoot IT infrastructure in real-time

History:

While SIEM has been deployed across many enterprises for years, its effectiveness in detecting potential threats and cyberattacks has been questioned across many quarters. Legacy and even NG-SIEM platforms were primarily designed to serve the threat vectors of yesteryear, relying mostly on expert security analysts to write effective rules for detection. Also, rules were designed to raise alerts that an IT Admin could monitor for operational continuity and generate reports for senior management. For the same purpose, central to legacy SIEM was the process of gathering “information” and “events”, deemed valuable for audit and discretionary compliance. Analysis of underlying threat indicators with the objective of honing in on the kill chain was subject to a security analyst’s interpretation of search results. Legacy SIEM thus remained lackluster in effect, as the insights below outlines some of the critical challenges.

Challenges:

Today’s Threats Are Different

Today’s threats are coming from threat actors that are AI-powered - every attack targeted or in mass is transformed to be unique, and clearly, the signature-based detection tools of the past are completely ineffective. Many attacks are also taking advantage of a far larger attack surface, think about the networks, devices, endpoints, and an explosion of locations where your users are working from. The tools of the past, like VPNs are more now more of an expressway into the backdoor than what they were designed for in legacy implementations.

Cybersecurity teams are too small and too fatigued to be effective 24/7

With the cybersecurity talent crunch (3.7M unfilled positions) to the simple fact that the average tenure of analysts and you can see why the number of incident responders have been falling for years. The daily grind of responding to alerts and hunting for evidence and correlation across dozens of systems continues to drive down both team morale and results. Combining this with the complexity of the attacks and the requirements from the frameworks and regulations has grown to make preventing attacks and keeping blast radius small feel like an almost impossible task for security teams.

SIEM Costs

SIEM costs are rising fast. With the massive growth in attack surfaces (More devices, more applications, more locations) and the lower costs of hardware, many organizations are discovering that the outdated method that SIEM vendors price and license their software is driving up costs for long-term storage of audits.

Legacy SIEM	Challenges/Gaps	Impact
Heavy reliance on Static Data (event logs)	Event logs stored in a database aren't suited for real-time indicators of cyber attacks or compromises	Misses out key threat indicators crucial for protection against cyber attacks and data breach
Correlation rules are mostly generic -requires trial and error cycles with frequent changes	Results in a high percentage of false positives and negatives	Reduces reliability on SIEM and increases the burden on Security Operations (SecOps)
Search operations on raw and normalized logs are critical to anomaly detection	Even simple search conducted on gigabytes (sometimes terabytes) of log data can take hours and days to return result	Delays investigation where time is of essence in blocking kill chain and limiting damage
Malware detection is often desgined on the signature of threat vectors	While signature may work for known malware, it isn't viable for zero-day threats and fileless vectors	Any new malware (absent in the database) can go undetected
User Behavioris not used as a key parameter for anomaly detection	Crucial context -that separates a normal user from a threat actor -is missing and can lead to flawed analysis	Inadequate context results in inaccurate and incomplete alerts
Advanced analytics leveraging AI/ML is missing	Without AI/ML based threat detection model, precise anomalies related to Indicators of Compromise (IoCs) would be a hit or miss.	Failure to detect modern threats with precision can result in significant risk to business
Limited to on-premises deployment	Many businesses and enterprises prefer Managed SIEM, hosted as SaaS in public cloud or semi-private (colo-based) with hybrid option	High cost of ownership and operational challenges make Legacy SIEM a difficult proposition

Buyer's Guide:

In this balanced buyer's guide you'll learn how to assess a SIEM vendor's ability to meet the needs of a modern SOC. Each section is defined by key process or factor in making an informed decision on the value of a SOC. Each section has a similar structure to make it easy for you and your team to put together your own requirements list or RFP. Required features, a list of the SIEM features that are best-in-class for 2023, "Evaluation Criteria" factors that you will want to quantify or measure, and finally, a set of questions to ask a potential vendor.

Ingestion

Ingest Logs, Flows, and Identities from across the large attack surface today.

Required Features

- Ingestion of network flows (NetFlow, sFlow, IPFIX) from on-premises network devices like firewalls and routers
- Ingestion of cloud flows from IaaS clouds like Amazon AWS, Microsoft Azure, Google Cloud, Oracle Cloud
- Ingestion of event logs from productivity applications like Microsoft 365 and Google Workspace and Email Systems
- Ingestion of identity providers like Active Directory and LDAP
- Ingestion of logs from endpoint protection and endpoint detection platforms like SentinelOne, BitDefender, VMware, Blackberry, CrowdStrike
- Ingestion of network flow metadata from IoT and OT devices

Evaluation Criteria

- Deployment complexity (agentless, agent, sensor, collector
- Deployment cost
- Integration list
- Time resolution

Questions to Ask

- Can the required installs be automated on the endpoints?
- Is there a method to monitor ingestion failures?
- What are the requirements for bandwidth and CPU for any data transfer from agents or collectors?

Enrichment

Enrichment of ingested metadata and events.

Required Features

- Ability to apply identities and context from sources like Active Directory or AWS security groups
- Enrichment data with threat intelligence feeds
- Enrichment of data with vulnerability scans
- Capability to bring your own threat intelligence feeds via STIX and TAXII

Evaluation Criteria

- Number of open-source and commercial threat intelligence feeds
- Source of the depth of vulnerability scans
- Speed of enrichment

Questions to Ask

- Do the threat intelligence feeds cover your industry?
- Can the identity be applied and maintained for devices when not connected to the identity provider?
- What is the method to attach additional feeds?
- Can manual enrichment be applied via CSV files?

Detection

Detections - detection of cyber threats, indicators of compromise, non-compliant postures

Required Features

- Ability to apply threat intelligence feeds (both native to the platform and 3rd party feeds via SITX and TAXII APIs).
- Ability to perform UEBA (user-entity-behavior analysis) across logs, flows, events, and identities
- Ability to apply network behavior analysis with UEBA and threat intelligence to factor in anomalies.
- Ability to detect data exfiltration, unusual network activity, compromised credentials, suspicious logins, password spraying, dictionary attacks
- Ability to detect and block malware and ransomware early - before they execute
- Ability to detect web and email exploits, including SQL Injection, directory traversal, remote file execution, business email compromise
- Ability to detect drift from policies and security posture architectures.
- Ability to detect DDoS attacks including volumetric, protocols, ICMP, SYN attacks and amplification.

Evaluation Criteria

- Machine-learning, is essential for rapid analysis and scoring across dozens of threat indicators, vulnerability assessments, and identity at near real-time speeds.
- Easy to configure and apply threat intelligence, UEBA, NBAD, NTA, in real-time to DETECT threats in the early stages without any limitation to context time.
- Comprehensive detection of attacks and threats in these categories: Cybercrime, insider threats, cloud and container security, vulnerability exploits, brute force, DNS, Web/Email, compliance/posture drift.

Questions to Ask

- Does the platform require 3rd party threat intelligence feeds?
- Does the platform provide transparency for its detections, including correlation across networks, endpoints, vulnerabilities, identities etc.?
- Is the platform built on a “true machine learning” model and big-data streaming architectures or a far more simple big data laake, signature and inference model?
- Explain how TI, UEBA, NBAD, NTA are combined to provide detection capabilities.

Correlation

Correlation - Provides evidence across devices, detection types, and the sources for the data to provide situational awareness to incident responders

Required Features

- Ability to capture all logs, network flow metadata, events/alerts from OS, Firewalls, IDS/IPS, Identity, M365/Google Workspace
- Ability to apply 40+ threat intelligence feeds (open source and commercial) and additional feeds via STIX and TAXII
- Ability to apply vulnerability assessment data
- Ability to apply context labels to machine IDs, Apps, Networks
- Ability to store relevant indicators of compromise or suspicious behaviors
- Ability to apply Machine Learning based UEBA, NTA, NBAD in-real-time to provide a “risk scoring” methodology to telemetry.
- Ability to show all “alert” creation signals (correlation) in a single screen with the ability to “drill down” to the details
- Mapping to alerts to the MITRE ATT&CK framework TTPs

Evaluation Criteria

- SIEM-based capture and correlation of telemetry
- UX is designed for analysts to have the context and relevant indicators visible from a single dashboard
- Mapping of alerts to MITRE ATT&CK TTPs

Questions to Ask

- Does the platform include or integrate with all of the telemetry signals from the required sources like: Networks, Firewalls, Endpoints, OS, Clouds, Applications, Identity, and IoT and OT devices?
- Does the platform store all of these logs, flows, and events in a way that provides context and situational awareness for alerts?
- Are all alert telemetry “clickable” to discover sources, times and other relevant details?
- Does the platform map alerts to the MITRE ATT&CK framework?

Response Automation

Response Automation - How are detected threats handled?

Required Features

- Customizable orchestration and response for threats that meet specific policy or risk tolerance postures
- Easy to edit, save, and share response automation
- Easy alert to response automation templating
- “Drag and Drop” multiple-step visual playbook designer.
- Options for manual “review first” vs. automated blocking, stopping, and quarantine of an attack
- Ability to apply “calendar” settings for automation ie. run on weekends after 6pm before 6am in a timezone
- Ability to support response on a wide variety of Firewalls, routers/switches, endpoints
- Ability to implement responses rapidly, for example, a library of standard responses to common threats

Evaluation Criteria

- Are the networks, applications and endpoint security and management solutions you and your team use today or have planned covered?
- Ease of use
- Transparency and ability to audit responses taken

Questions to Ask

- What types of detection/alerts can have automated or “push-button” level ability to respond?
- How many and what types of template responses are available?
- How many and which Switches, Routers, Firewalls, and Endpoints are supported?
- How does the user interface assist in the creation of responses? Is there a “drag and drop” visual version?
- Does configuring the response require deep programming and scripting skills?

Security Operations & Deployment

Security Operations - What does it take to deploy, configure, and run the SIEM?

Required Features

- Permissions for and audit trails for all staff from “create” to “edit” to view for interfaction
- Comprehensive “notes and comments” for actions reviewed and taken by SOC team
- Easy, documented integrations with key Network, Cloud, Identity, Endpoints, IoT, OT and beyond
- Sensors, Agents, API Endpoints for passing logs, events, flows securely to the platform
- Storage flexibility - on-premises, cloud, hybrid

Evaluation Criteria

- Number of existing point solutions consolidated
- Number of potential staff needed to run the platform
- Number of supported integrations, rate at which new integrations are added
- Onboarding training & certification for team
- Documentation for implementation, deployment options and overall usage and management

Questions to Ask

- On average, how many users and devices can be managed from a Level 1, Level 2, Level 3 analyst and incident responder perspective?
- Does the platform feature audit logs and notation for analysts and incident responders to track and note their work and actions?
- What are the deployment models for collectors, sensors and agents?
- What are the deployment models for SIEM storage?
- What are the Virtual Machine, Cloud or Hardware Deployment requirements?
- What are the agent requirements?

Licensing

Licensing - How is the license structured, what is included and what is optional?

Questions to Ask

- How is the software licensed?
- How is usage measured and reported?
- What is included and what features, integrations are included or optional.
- Does the platform feature:
    - Ability to ingest flows, logs, events, identity?
    - Included or optional threat intelligence feeds?
        - Which?
    - Included or optional vulnerability assessment
    - UEBA
    - NBAD
    - NTA
    - NDR
    - EDR
    - EPP
    - SOAR
    - Reporting
    - Risk Scoring
- Does the vendor have a program for ‘jumpstarting” a modern AI/ML-powered SOC with SOC as a Service?
- How is the SIEM priced and metered- events/flows per second, devices, users?

MSP/MSSP Use Cases:

XDR/MDR - With Seceon, many MSPs and MSSPs are able to offer a co-managed or fully-managed cybersecurity service that provides lower risk with detection across the full attack surface and endpoints and subsequent response for threats that are detected.

SOC/Service - With Seceon, many MSPs and MSSPs are able to offer a full 24/7 SOC (Security Operations Center) reduce cyber threat risks, and provide the requirements for insurance or compliance and framework requirements.

Compliance as a Service - Seceon's comprehensive detection and response, and posture monitoring, and threat remediation capabilities, plus reporting capabilities, enable organizations to produce the reports that compliance and insurance auditors require.

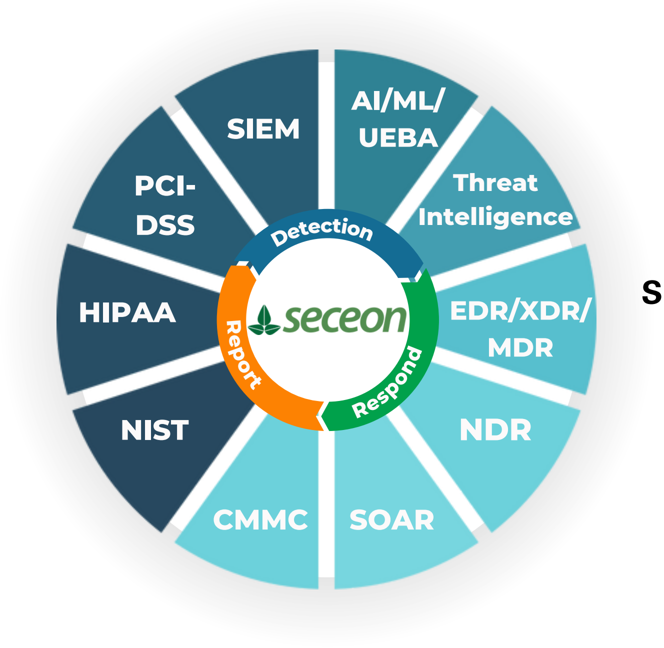
Seceon Approach:

Seceon:

Seceon enables MSPs and MSSPs to reduce cyber threat risks and their security stack complexity while improving their ability to detect and block threats and breaches at scale.

Seceon's aiSIEM platform augments and automates MSP and MSSP advanced security services. With a SIEM-based detection and response platform. It delivers continuous coverage by collecting telemetry from logs, events, identity management, networks, endpoints, clouds, and applications. It is all enriched and analyzed in real-time by applying threat intelligence, AI, and ML models built on behavioral analysis and correlation engines to detect and alert reliably. Today, over 300 plus partners are reselling and running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 7,500 clients.

Also available is Seceon aiXDR. It takes a holistic approach to cybersecurity by gathering deep insights from endpoints, servers, clouds, network devices, applications, IOT, and OT and applying user identity, threat intelligence, and vulnerability assessment to establish threat profiles, generating threat indicators, raising essential alerts, and offer remediation path – automated or triaged. In essence, the solution ensures multi-layered threat detection and response, relying on EDR, Network Behavior, Advanced Correlation (SIEM), Network Traffic Analysis, UEBA (ML-based), and SOAR for an All-In-One platform that is organically and seamlessly fused together.



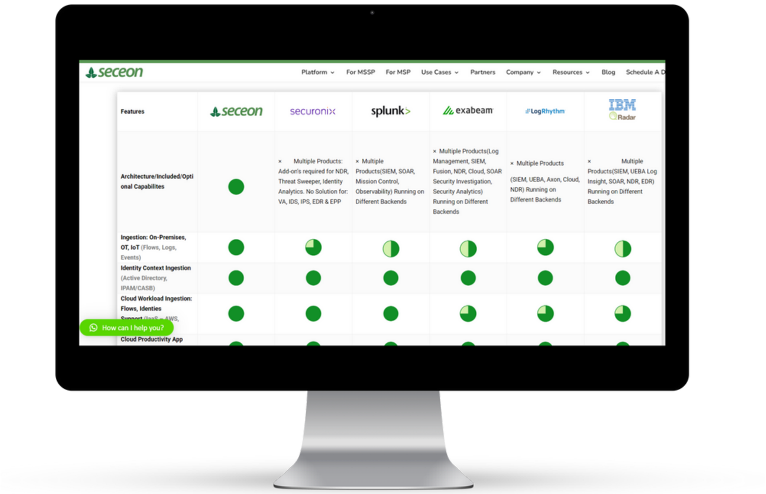
Seceon's aSIEM and aiXDR combine to create a powerful platform for cybersecurity teams.

> *"Seceon's aiSIEM platform is a foundational component of our managed security services platform and enables our SOC to deliver SIEM logging with 24x7 monitoring and alerting. The powerful combination of: ingest everything, and ML-based dynamic threat models and subsequent alerting and response automation continues to enable us to provide our clients with less downtime, less risk, and maintain higher compliance standards. Seceon is that rare solution that provides value from on-premises to the cloud and beyond, enabling us to offer top-shelf products for small and medium sized businesses due to its efficiency and licensing models,"*
>
> **-Tammy Jutras, Director of Cybersecurity Services, Visory**

About Seceon

Seceon enables MSPs and MSSPs to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 300 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 7,500 clients.

Learn more about Seceon and schedule a demo today. We also have a comparison page on our website where we compare SIEM solutions from various vendors.



Features	seceon	securonix	splunk>	exabeam	LogRhythm	IBM Radar
Architecture/Included/Optional Capabilites	●	× Multiple Products: Add-on's required for NDR, Threat Sweeper, Identity Analytics. No Solution for: VA, IDS, IPS, EDR & EPP	× Multiple Products(SIEM, SOAR, Mission Control, Observability) Running on Different Backends	× Multiple Products(Log Management, SIEM, Fusion, NDR, Cloud, SOAR Security Investigation, Security Analytics) Running on Different Backends	× Multiple Products (SIEM, UEBA, Axon, Cloud, NDR) Running on Different Backends	× Multiple Products(SIEM, UEBA Log Insight, SOAR, NDR, EDR) Running on Different Backends
Ingestion: On-Premises, OT, IoT (Flows, Logs, Events)	●	◕	◑	◑	◕	◑
Identity Context Ingestion (Active Directory, IPAM/CASB)	●	●	●	●	●	●
Cloud Workload Ingestion: Flows, Identies Support (IaaS – AWS,	●	●	●	◕	◕	◕
Cloud Productivity App						

Also, we recommend that you visit our SIEM feature and licensing comarison page:
https://www.seceon.com/siem-alternatives/

Learn more about Seceon aiSIEM and

Schedule a Demo www.seceon.com/contact/