Security Information and Event Management (SIEM)

Navigating the security maze with AI

2025 CONSTELLATION SHORTLIST

The Constellation ShortList™ presents vendors in different categories of the market relevant to early adopters. In addition, products included in this document meet the threshold criteria for this category as determined by Constellation Research.

This Constellation ShortList of vendors for a market category is compiled through conversations with early adopter clients, independent analysis and briefings with vendors and partners.

ABOUT THIS SHORTLIST

In today's threat-filled landscape, organizations generate a tsunami of security data from diverse sources. Manually navigating this sea of information to identify and respond to threats is akin to finding a needle in a haystack. Security Information and Event Management (SIEM), a critical tool powered by Artificial Intelligence (AI), helps to centralize, analyze, and gain actionable insights from your security data.

The plethora of security alerts generated by various tools can overwhelm security teams, leading to "alert fatigue" and potentially causing them to miss critical alerts. AI algorithms go beyond simple rule-based analysis, meticulously sifting through log data to identify even subtle anomalies and predict potential security incidents with remarkable accuracy. This allows you to proactively address threats before they escalate. AI-enabled tools learn from past incidents and threat intelligence, continuously evolving its understanding of cyberattacks. This enables predictive security measures, identifying potential threats before they materialize and allowing you to proactively bolster your defenses.

The SIEM market, fueled by the ever-growing need for intelligent security solutions, is expected to reach a staggering $20+ billion by 2030. This robust growth reflects the immense value AI brings to SIEM, transforming it from a data aggregator to a cognitive security hub.

11 SOLUTIONS TO KNOW

Constellation evaluates more than 30 solutions categorized in this market. This Constellation ShortList is determined by client inquiries, partner conversations, customer references, vendor selection projects, market share and internal research.

- EXABEAM
- FORTINET
- GURUCUL
- IBM
- MANAGEENGINE
- MICROSOFT
- OPENTEXT
- RAPID7
- SPLUNK
- SECURONIX
- SUMO LOGIC

LIKE WHAT YOU SEE?

Consider partnering with Constellation Research on your go-to-market-strategy. Email **ShortList@ContellationR.com** for more info.

To learn more about Constellation Research Shortlists visit: **www.constellationr.com/ShortList**

THRESHOLD CRITERIA

Constellation considers the following criteria for these solutions:

- Log Management: Collects and centralizes logs from diverse sources, providing a historical view of your security posture.
- Security Event Monitoring (SEM): Correlates and analyzes log data, identifying suspicious activity and potential security incidents.
- Incident Response: Provides tools and workflows to investigate and respond to security incidents quickly and effectively.
- Compliance Reporting: Generates reports to demonstrate adherence to security regulations and standards.
- Threat Intelligence Integration: Integrates with threat intelligence feeds to enrich analysis and identify emerging threats.
- User Behavior Analytics (UBA): Monitors user behavior to detect anomalies and potential insider threats.
- SOAR (Security Orchestration, Automation, and Response): Automates incident response workflows, streamlining resolution and reducing manual effort.
- Open APIs: Enables integration with other security tools and platforms for a holistic security ecosystem.

ABOUT CONSTELLATION RESEARCH

As an award-winning Silicon Valley-based strategic advisory and futurist analyst firm, Constellation Research serves leaders and organizations navigating the challenges of digital strategy, business-model disruption and digital transformation. Constellation works closely with solution providers, partners, C-suite executives, board of directors, and its Constellation Executive Network of buy-side leaders to lead the way in research coverage and advise clients how to achieve valuable business results.

FREQUENCY OF EVALUATION

Each Constellation ShortList is updated at least once per year. Updates may occur after six months if deemed necessary.

EVALUATION SERVICES

Constellation clients can work with the analyst and the research team to conduct a more thorough discussion of this ShortList. Constellation can also provide guidance in vendor selection and contract negotiation.

BUSINESS THEMES

Digital Safety, Privacy and Cybersecurity

Chirag Mehta
VP & Principal Analyst

Chirag Mehta is Vice President and Principal Analyst focusing on cybersecurity, next-gen application development, and product-led growth. With over 25 years of experience, he has built, shipped, marketed, and sold successful enterprise SaaS products and solutions across startups, mid-size, and large companies. As a product leader overseeing engineering, product management, and design, he has consistently driven revenue growth and product innovation. He also held key leadership roles in product marketing, corporate strategy, ecosystem partnerships, and business development, leveraging his expertise to make a significant impact on various aspects of product success.