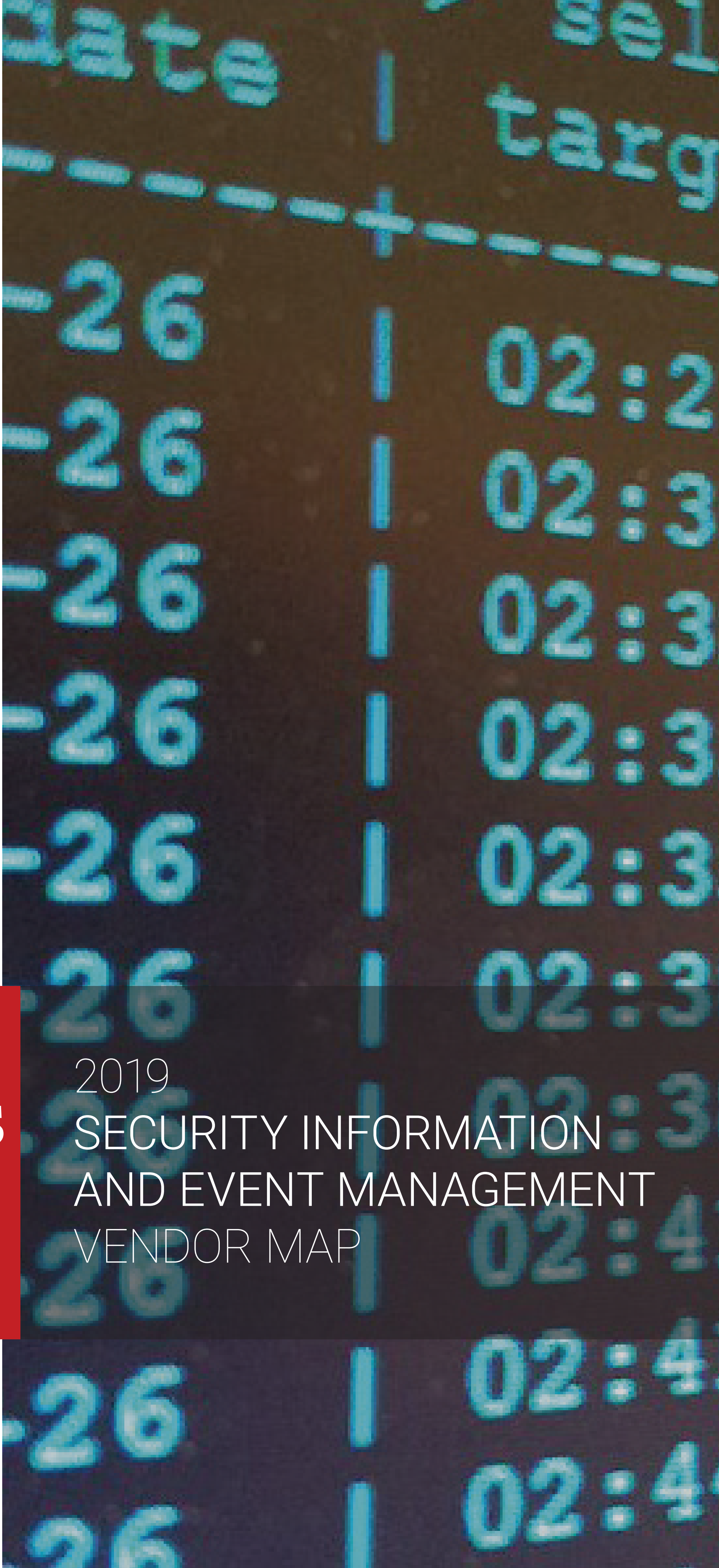
Solutions Review



2019

SECURITY INFORMATION AND EVENT MANAGEMENT

VENDOR MAP

Choosing the Right Security Information and Event Management Solution for Your Needs

Introduction

If any year indicated a shift in cybersecurity thinking, it was 2018. In the formative years of digital security, fortifying the perimeter was the key concern of enterprise-level InfoSec experts. Keeping digital threat actors and their malware from ever touching the inner recesses of the network was of the utmost importance. But those days are long gone.

Currently, the global average dwell time for a digital threat on an enterprise network is estimated anywhere between 99 days and 191 days. Every minute a hacker remains on your network unchallenged compounds the damage they wreak. The enterprise network has expanded beyond the scope of legacy prevention-oriented solutions, especially in hybrid or cloud architectures. And the global epidemic of hacks, cyber attacks, and malicious insiders shows no signs of abating. If anything, the infection rate continues to rise...escalating to a fever pitch.

With traditional preventative cybersecurity appearing to only offer token countermeasures against digital threats—and, with the rise of fileless malware, perhaps not even that—the paradigm is shifting to a detection and response-based strategy. No cybersecurity solution is more equipped to serve enterprises in this new paradigm than security information and event management—SIEM.

SIEM solutions, however, are as diverse as any other cybersecurity field. Different solution providers emphasize different key capabilities in security analytics: compliance reporting, threat intelligence/detection, and log management. Knowing which capability your enterprise should emphasize in its individual security platform, and which solution best fits your business needs, can prove a challenge.

Enterprises are distinct in their size, industries, and priorities. Each digital architecture, whether on-premises, hybrid, or cloud-based is unique. Therefore your SIEM solution must accommodate your enterprise as an individual use-case. What proportion of compliance, log management, and threat intelligence/detection do you need?

In this SIEM Vendor Map, we dive into the key SIEM capabilities and the specialists in each.

Threat Intelligence and Detection

As stated above, the digital perimeter is becoming more porous as the network expands to accommodate new endpoints, databases, and access demands. Threat detection capabilities enable enterprises to find digital threats dwelling on their networks. They cut down on attacker dwell time, prevent private data compromises, reduce recovery expenses, and improve customer trust. Threat detection is vital for improving network visibility and for supporting other cybersecurity initiatives. The latter is especially important for overtaxed IT departments. Threat detection can comprise of real-time correlation, analytical capabilities, and behavioral analysis.

Compliance

For much of its technological history, enterprises turned to SIEM solutions to fulfill their compliance reporting mandates for regulations as diverse as HIPAA and PCI DSS. Using its log management and normalization capabilities, SIEM can automatically compile reports to the correct specifications via out-of-the-box or customizable options. More recently, compliance has taken a backseat to SIEM's threat detection as the cybersecurity paradigm shifted from perimeter-focus. This change paved the way for smaller businesses to adopt SIEM in larger numbers and take advantage of its compliance capabilities. Compliance is still an important aspect of SIEM, but fulfilling a compliance mandate should not be confused with true cybersecurity protection. It should instead be considered as the bare minimum of one kind of cybersecurity.

Log Management

The typical large enterprise generates information on a staggering scale. A fortune 500 enterprise alone can generate 10 terabytes of plaintext data a month. These logs contain everything from data transfers, access requests, traffic, server activity, and user interactions. Log management capabilities by their nature will find evidence of security breaches or dwelling threats, but won't be able to distinguish between good and bad activity without an incorporated correlation capability. Log management can provide visibility and storage, facilitate compliance, and even provide search capabilities for finding specific events. Log management not only compiles security events and ordinary events—it also normalizes all of the data to make analysis consistent and easy to understand.

Conclusion

The major capabilities of SIEM work together via comprehensive enterprise-level solutions. None of these capabilities can be truly said to be superior or more vital to security than any other. Each of the key capabilities facilitates and strengthens the effectiveness of the others. None should operate on its own. The real question is one of emphasis and proportion.

What enterprises' should prioritize depends largely on the solution providers' technology and on their distinct needs. For enterprises, the primary concerns should be fulfilling their compliance and threat detection requirements. For smaller businesses, log management and threat detection might be more important. Selecting a SIEM solution should be a process of contemplation and true self-evaluation.

Does your chosen SIEM solution provide enough of an audit trail for your company to satisfy its necessary compliance mandates? Does it offer a smooth enough log management experience to provide adequate security controls? Can you balance the features of the toolset with the number of personnel required to make them work? That last question is not an idle one; SIEM is one of the most labor-intensive cybersecurity solutions on the market.

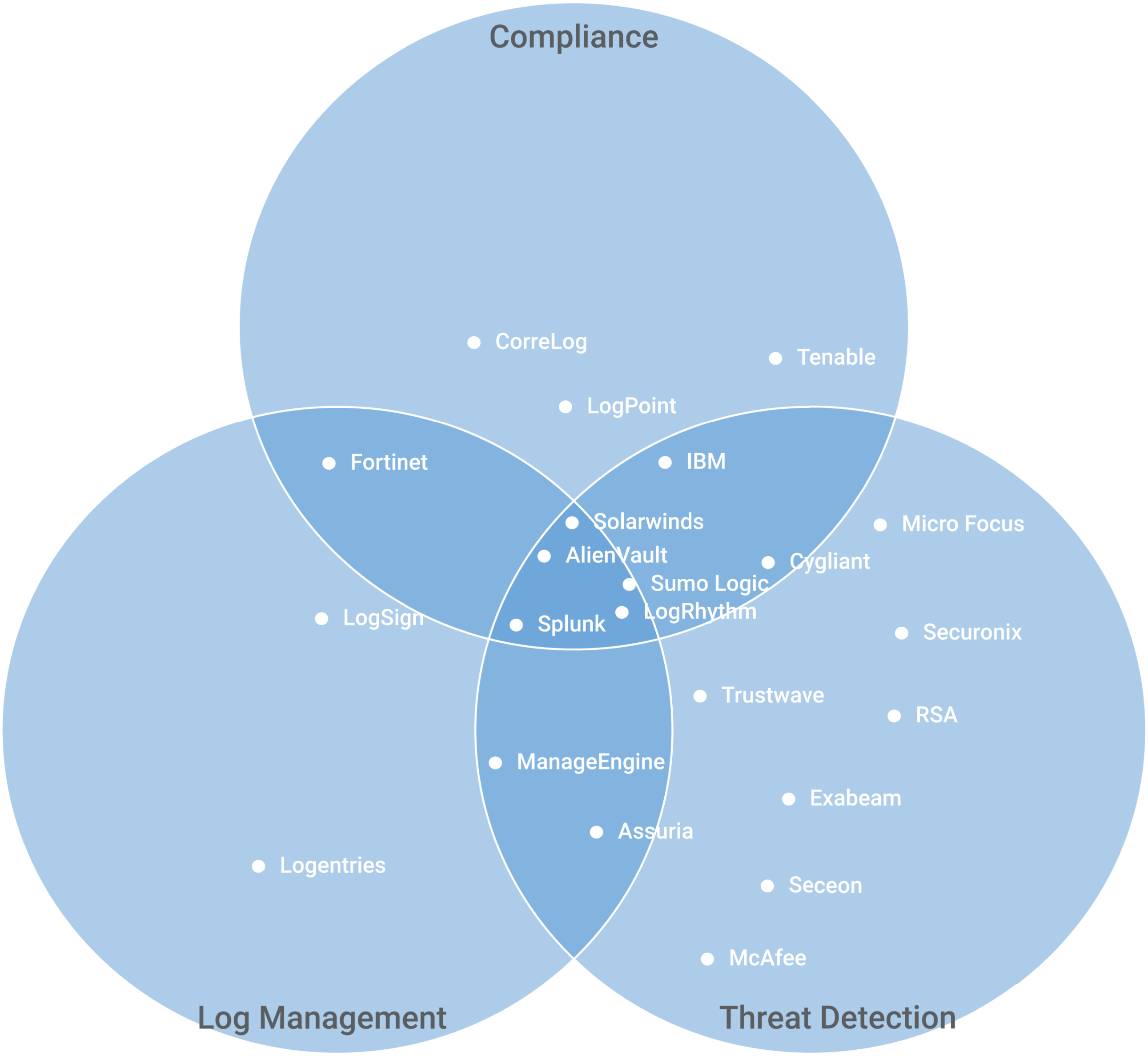
No enterprise is going to come to the exact same answer regarding the same product. The goal—and the difficulty—will be to minimize the downsides of your chosen solutions while maximizing its security coverage. It is difficult, but the rewards of success will provide reassurance and protection in an age of InfoSec uncertainty.

Vendor Comparison Map

Aimed at simplifying the time-consuming vendor selection and evaluation process, the following Venn diagram offers an at-a-glance reference guide for 22 SIEM players, the solutions they provide, and the markets they specialize in.

Vendors on the outside of the circles tend to offer highly-specialized solutions in the SIEM market, favoring certain capabilities or use cases. Vendors towards the center, on the other hand, offer more comprehensive platforms. They can address multiple needs but may not do so with the same depth and granularity as "point" solution providers.

Almost all of the vendors included in this resource offer various solutions addressing each of the capabilities concerned; SIEM is a well-defined and mature marketplace. We have therefore tried to reflect this in their positioning, taking into account each vendor's technological focuses to determine their positioning in the diagram.



Vendor List

AlienVault

AlienVault provides specialized compliance solution packages for GDPR, HIPAA, and PCI DSS among other regulatory mandates. Its USM solution draws from the Open Threat Exchange to acquire new threat intelligence. USM can draw from an extensive correlation rules library to strengthen its log management. Further, all log data aggregated by AlienVault can be stored in a specialized, certified compliant cloud environment. AlienVault can perform advanced threat detection across the cloud environments or in on-premise environments.

Assuria

Assuria provides distinct SIEM suites for public and private cloud security, supplemented by network traffic monitoring solutions for recognizing threats using bandwidth. It can leverage analytics, correlation, and anomaly detection. Assuria offers automatic monitoring, alerting and reporting of system changes in addition to file integrity monitoring. Assuria's ALM-SIEM product offers enterprise-wide log collection and management, as well as log cataloging in a secure storage environment. Its documentation may not be user-friendly to the layperson.

CorreLog

CorreLog provides a SIEM solution they define as "cross-platform."Their solution offers real-time notifications, collects all the system log messages created by your network, and parses them into industry standard Syslog protocols. CorreLog offers security compliance for GDPR, HIPAA, and many other regulatory mandates. Their solutions also provide sophisticated data aggregation: archiving functions, data searching ability, high-speed message correlation, and input filtering.

Cygilant

Cygilant defines their products as Security as a Service. They offer managed detection and response capabilities which draw from security technologies like firewall and antivirus. Cygilant has strong compliance capabilities, vulnerability assessment, incident detection and response, and log management incorporated into their threat detection. Their Log Management capabilities appear to supplement compliance and threat detection.

Fortinet

Fortinet's SIEM solution demonstrates detection and remediation of security events, offers asset self-discovery, rapid integration, and scalability. However, it does not provide out of the box threat detection. It emphasizes automated workflows, single pane of glass visibility, and a unified platform. Fortinet offers solutions for individual compliance regulations and security automation. It appears to not emphasize its log management capabilities as much as its overall threat detection.

IBM

IBM focuses on threat intelligence over the other key capabilities. Their solutions draw from global teams of researchers and from the IBM X-Force Exchange—a cloud-based threat intelligence sharing platform. IBM also offers IBM QRadar, a SIEM as a Service product, for threat detection. The IBM QRadar Log Manager is a scalable solution for collecting analyzing, storing, and reporting. IBM BigFix Compliance is their compliance solution; all of them are marketed as separate products.

Logentries

Logentries focuses on log management and analytics. It is capable of handling and providing data formats, instant centralization, easy to read results, infrastructure monitoring, and compliance. It does this via log management offering data filtering, PCI compliance, weekly reporting, anomaly detection, and team-wide notifications. It's threat detection is not as emphasized.

LogPoint

The list of LogPoint focuses and capabilities is staggering: detection and response, UEBA, GDPR compliance, and threat intelligence. LogPoint's risk management toolkit provides rapid analytic insight, big data analytics, forensic investigations, and a compliance management system for monitoring and automation. It provides automatic compliance alerts, out of the box compliance reports, protection of sensitive data, alerting of policy and compliance violations, and threat intelligence. LogPoint can normalize data compiled by data aggregation of events.

LogRhythm

LogRhythm performs broad-based collection, identifying threats with corroboration from one or more security-related activities or integrations. It aims to reduce the mean time to detect and mean time to respond to threats by using behavioral-based analytics. LogRhythm UEBA uses advanced machine learning to perform profiling and anomaly detection so your team can easily identify insider threats and more. Compliance is provided for, as is log management.

LogSign

LogSign offers all three capabilities: security intelligence, log management, and compliance reporting. It offers log management and automated compliance needs, focusing on maintaining a "good enough" security posture. Whether this enough for individual enterprises will depend on their priorities. LogSign's log management offers centralized collection and logging, rapid search among the massive amounts of data, and log filtration and normalization. Threat intelligence, security analytics, and outright SIEM are all available as individual solution areas.

ManageEngine

ManageEngine offers individual products and solutions for network and server performance management and integrated network management. Its Log360 product offers log management for Microsoft products. The Office 365 reporting product is also offered for Microsoft compliance. Cloud Security Plus allows for log data searches and management, as well as compliance reporting for public cloud environments. Its compliance appears a little more limited otherwise. The ManageEngine EventLog Analyzer does offer log management and IT compliance.

McAfee

McAfee offers the McAfee Enterprise Security Manager. This provides real-time visibility into all activity on systems, networks, databases, and applications. McAfes also provides the McAfee Enterprise Log Manager, which delivers automated log collection, storage, and management with flexible storage. It can integrate with your infrastructure, collect logs intelligently, store the right logs for your compliance, and parse them. In other words, it provides a SIEM foundation and advanced threat intelligence but not the same compliance emphasis as others.

Micro Focus

Micro Focus might be thought of as multiple individual solutions providing the core functions of a comprehensive SIEM solution. Sentinel offers SIEM with actionable intelligence, ArcSight Investigate offers security investigation and analytics, etc. Micro Focus also provides the NetIQ solution for day-to-day SIEM. NetIQ integrates identity information into its analytics and provides visibility via log management. Micro Focus allows for some customization options that can disrupt the optimal performance of its log management capabilities.

RSA

The RSA NetWitness Platform is their threat detection product which they designed as a unified security data platform. It features an analyst “workbench” for analyzing security alerts and works to improve network vulnerability in all environments. The RSA Netwitness is designed to combat advanced persistent threats—threats that bypass traditional SIEM log systems. The RSA Netwitness Logs is their log management product. RSA does offer some compliance solutions, especially for GDPR, but threat detection seems to be their primary emphasis.

Seceon

Seceon offers the Seceon aiSIEM—an integrated log management and threat detection product. It uses machine learning and big data analytics to adapt to the individual enterprise environment. Seceon aiSIEM also provides threat indicator scores for increased accuracy and improved threat elimination. They also offer products for Traffic Monitoring. Seceon does provide compliance reporting, but this is not as central to their products as their threat detection.

Securonix

The Securonix SIEM offering is called the Snypr Security Analytics. It features a library of threat signatures, UEBA functionality, and event collection. This enables it to support threat detection and incident investigation; the former is based on behavioral analysis coupled with peer group analysis. It also offers insider threat management. Some have noted Securonix’s case management can feel more basic than other SIEM solutions. Securonix also does not focus as heavily on compliance as other SIEM solutions.

Solarwinds

SolarWinds’ exclusive solution for SIEM balances all three of the key SIEM components: threat detection, log management, and compliance. It provides threat mitigation, demonstrable compliance reporting, and continuous security through an encrypted data transfer system. Other capabilities include log forwarding, IT compliance reporting, and active response. SolarWinds also offers individual threat monitoring products, log management for the Orion platform, and traffic analysis.

Splunk

Splunk's SIEM strength is its out-of-the-box availability. It provides pre-packaged dashboards, incident response workflows, and analytics. Splunk also offers both out-of-the-box security and compliance reporting templates. Both can support multiple threat feed sources. On the threat detection side, Splunk provides security analytics with optimization and remediation facilitated by machine data. Additionally, it is designed to fight fraud and ransomware as well as other breaches.

Sumo Logic

Sumo Logic's Security and Compliance Analytics aims to help enterprises maintain and streamline compliance through intricate log management and continuous monitoring. They position themselves as a next-generation SIEM or security analytics solution rather than a traditional SIEM product. Its log management is designed to facilitate troubleshooting and operational insights. Sumo Logic can automate security and compliance audits and provide machine learning analytics and threat intelligence.

Tenable

Tenable offers its Tenable.io product, which incliudes the Tenable.io Vulnerability Management product. It provides actionable insight into security risks and areas of potential focus. For overall solutions, Tenable offers specialized solutions for cloud infrastructures and industrieslike healthcare and retail. It also provides individual compliance solutions for GDPR, HIPAA, and others. Tenable is most fitting for enterprises interested in compliance and threat detection rather than log management.

Trustwave

Trustwave's solutions provide threat management, vulnerability management, and compliance management. It can identify and deploy security best practices and reduce risk with multiple compliance standards. Trustwave also offers continuous threat detection and response, advanced security solutions, and industry best practices. It does provide log monitoring—centrally collecting logs utilizing automated filtering and review for compliance purposes and reporting. It uses this log management as a baseline for its other SIEM services.

ABOUT SOLUTIONS REVIEW

Solutions Review is a collection of technology news sites that aggregates, curates and creates the best content within leading technology categories. Solutions Review's mission is to connect buyers of enterprise technology with the best solution sellers.

Over the past three years, Solutions Review has launched over 15 tech Buyer's Guide sites in categories ranging from Cybersecurity to Mobility Management, Business Intelligence, Data Integration, Cloud Platforms, and Content Management.

Information for this report was gathered via a meta-analysis of available online materials and reports, conversations with vendor representatives, and examinations of product demonstrations and free trials. Solutions Review does not endorse any vendor, product or service depicted in this publication and does not advise technology users to base their vendor selection entirely on this research.