WHITE PAPER

Adopting Splunk's Analytics-Driven Security Platform as Your SIEM

Improve your security posture by using Splunk as your SIEM

splunk> turn data into doing™

Highlights

- **Splunk software can be used to build and operate security operations centers of any size**
- **Support the full range of information security operations,** including posture assessment, monitoring, alert and incident handling, CSIRT, breach analysis and response, and event correlation
- **Out-of-the-box support for SIEM and security use cases**
- **Detect known and unknown threats, investigate threats,** determine compliance and use advanced security analytics for detailed insight
- **Proven integrated, big data-based security intelligence platform**
- **Use ad hoc searches** for advanced breach analysis
- **On-premises, cloud, and hybrid on-premises and cloud deployment options**
- **Improve operational efficiency** with automated and human-assisted decisions by using Splunk as a security nerve center
- **Actionable guidance** on how to investigate and take action on threats detected in your environment using Analytic Stories

Early detection, rapid response and collaboration are needed to mitigate today's advanced threats. But these needs impose a significant demand on security teams. Reporting and monitoring logs and security events is no longer enough. Security practitioners need broader insights from all data sources generated at scale across the entire organization from IT, the business and the cloud. In order to stay ahead of external attacks and malicious insiders, companies need an advanced security solution that can be used for rapid response detection, incident investigation and coordination of CSIRT breach scenarios. In addition, companies need the ability to detect and respond to known, unknown and advanced threats.

New Criteria for Today's SIEM

Enterprise security teams must use a security information and event management (SIEM) solution that not only solves common security use cases, but advanced use cases as well. To keep up with the dynamic threat landscape, modern SIEMs are expected to be able to:

- Centralize and aggregate all security-relevant events as they're generated from their source
- Support a variety of reception, collection mechanisms including syslog, file transmissions, file collections, etc.
- Add context and threat intelligence to security events
- Correlate and alert across a range of data
- Detect advanced and unknown threats
- Profile behavior across the organization
- Ingest all data (users, applications) and make them available for use — monitoring, alerting, investigation and ad hoc searching
- Provide ad hoc searching and reporting from data for advanced breach analysis
- Investigate incidents and conduct forensic investigations for detailed incident analysis
- Assess and report on compliance posture
- Use analytics and report on security posture
- Track attackers' actions with streamlined ad hoc analyses and event sequencing
- Centrally automate retrieval, sharing and responses across the security stack
- Assess threats from the cloud, on-premises and hybrid apps and data sources

All Data Is Now Security Relevant

The evidence of an attack, as well as its activities, exists in an organization's machine data. For security teams to properly investigate security incidents and identify threats, all data, including more than security data from traditional security products such as firewalls, IDS or anti-malware should be brought into the SIEM. Organizations are often missing the data needed to see the real-time status of their security posture.

The activities of these advanced threats are often only in the "non-security" data, such as operating system logs, directory systems, such as LDAP/AD, badge data, DNS, and email and web servers.

Machine data often needs to be supplemented with internal and external threat context, such as threat intelligence feeds and other contextual information to aid during incident response and breach detection.

Keeping Pace With the Volume and Scale of Data

The amount and types of data needed for making the most effective data-driven security decisions requires a solution that will scale to index hundreds of terabytes of data per day without normalization at collection time and applies a schema to this data only at search (query) time.

Automated Anomaly and Outlier Detection

To detect advanced threats, all non-security and security data must reside in a single repository. This represents a massive amount of data and will provide a repository to baseline normal user and traffic activity. Using this baseline, analytics can detect the anomalies and outliers that may be advanced threats. Statistics can help with this detection by looking for events that are standard deviations of the norm. Correlations can also help by detecting combinations of events that are rarely seen and are suspicious.

A New Approach to SIEM

While many SIEMs purport to meet the new criteria, it may not be suitable for your organization. The table below lists the key capabilities to consider while evaluating a new SIEM or re-evaluating a legacy SIEM against new requirements:

Key Capability	Benefit
Single platform	One product to install and manage, which simplifies operations
Software	Providing cost effective scaling–hardware options can match requirements and expand as needed. Hardware costs are minimized since commodity hardware can be used
Index any data using variety of mechanisms	Fast time-to-value. Customers should realize value from their SIEM in hours or days
Large number of pre-defined data sources	A rich partner ecosystem reduces reliance on SIEM vendor and custom collectors
Flat file data store providing access to all data values and data fields with no schema or normalization	All values and fields from all data sources can be searched, reported on, and correlated as predefined alerts or for ad hoc investigation. All the original data is retained and can be searched, as compared to legacy SIEMs that requires transforming different log formats into single "taxonomy" to facilitate.
Single data store with distributed indexing and searching for scale and speed	Scalability and speed issues are non-existent

Key Capability	Benefit
Flexible search for automated base-lining and advanced correlations	Enhances the ability to find outliers and anomalies
Visualization of data and incidents in multiple formats and renderings	Ability to use, create and edit existing tables, charts or scatterplots provides much needed flexibility that is suited to diverse customer environment
Out-of-the-box support of APIs and SDKs	Interface with third-party apps to extend the capability of SIEM
Support of common IT use cases such as compliance, fraud, theft and abuse detection, IT operations, service intelligence, application delivery and business analytics	As security teams work in concert with other IT functions, the visibility from other use cases results in a centralized view across the organization with cross-department collaboration and stronger ROI
Operate on-premises, in the cloud and in hybrid environments	Operate a single logical solution that allows users to search, report and operate when data is stored in either on-premises or the cloud
Cloud deployment option (BYOL and SaaS)	Helps you consolidate your business in the cloud
Hybrid deployment with on-premises and cloud options	Optimize your business needs using SaaS or on-premises deployments—without sacrificing visibility
Response Actions	Improve operational efficiency with automated and human-assisted decisions
Threat intelligence operationalization	Security teams can quickly and effectively translate threat information into intelligence that can be actionable to detect threats and protect your organization
Risk scoring	Know the relative risk of a device or user in your network environment over time
Ad hoc searching over extended periods of time	Identify breaches and conduct detailed breach analysis by drilling down into machine data to get deep, precise insight
Supports applying the kill chain methodology of investigation	Gain visibility into an attack, understand adversary's objectives, monitor activities during an attack, record key information and use it to defend your organization
Support analysis of the five styles of advanced threat defense	Helps identify advanced targeted attacks, also known as advanced persistent threats from the network, payload and endpoint, in near real time and post-compromise

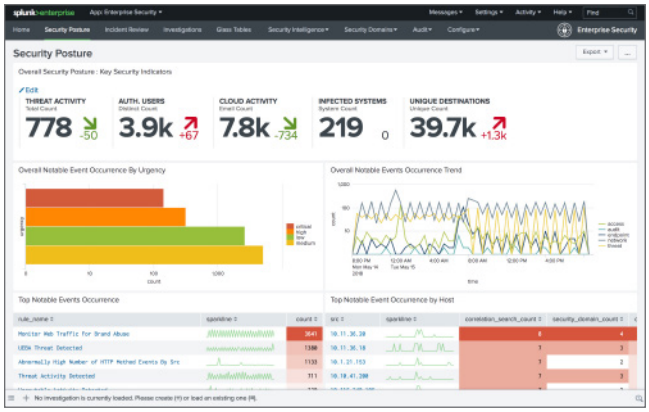
The flexibility and architecture of the platform plays a key role in determining if the SIEM can scale to meet the needs of an organization. It's important that the SIEM software can scale and is able to quickly index all the original, raw data at massive volumes – from several hundreds of terabytes to petabytes of data indexed per day.

Scaling horizontally, using commodity hardware, provides the flexibility and compute scalability that expensive physical appliances are unable to meet.

The use of distributed index and search technology with fast searches, reporting and analytics enables the quick transformation of results into a wide range of interactive reports and visualizations.

Splunk as Your SIEM

The Splunk security platform meets the criteria for a modern SIEM solution but it also delivers security analytics capabilities, providing the valuable context and visual insights that help security teams to make faster and smarter security decisions.



Adaptive Response actions provide provides the ability to register and configure response actions, enabling customers and partners to use their existing capabilities with Splunk Enterprise Security (ES) as an analytics-driven SIEM solution. The visibility into the capabilities and actions of each Adaptive Response entity helps customers view the list of actions available, select appropriate actions, and deploy and manage the entities and their actions in ways best suited to their environment, deployment and security operations. Analysts can take suggested response actions to quickly gather more context or take action when reviewing notables in the Incident Review dashboard. Analysts can also execute any action from a notable event context, so they can gather information or take action such as "block," "unblock," "open" or "close" to remediate an incident.

Splunk offers several options for enterprises looking to deploy their first SIEM solution or to migrate from their legacy SIEM, and offers the choice of on-premises, cloud or hybrid deployment options.

Customers can solve their basic SIEM use cases using Splunk Enterprise and Splunk Cloud, which are core Splunk platforms, providing collection, indexing, search, and reporting capabilities. Many Splunk security customers use Splunk Enterprise or Splunk Cloud to build their own real-time correlation searches and dashboards for a basic SIEM experience.

Splunk offers a premium solution, Splunk ES, which supports advanced SIEM use cases with ready-to-use dashboards, correlated searches and reports. Splunk ES runs on Splunk Enterprise, Splunk Cloud or both. In addition to pre-built correlation rules and alerts.

Splunk ES also improves visibility and responsiveness for security analysts with focused threat detection to better accelerate incident investigation. It also reduces risk by enabling faster detection and incident response to newly discovered and ongoing threats. And Splunk ES also includes a feature called the Investigation Workbench that helps analysts better understand the full scope of incidents and make real-time decisions to get ahead of threats.

For security teams of all sizes and maturity levels, the Splunk Use Case Library makes it possible for security analysts to proactively stay current with the changing threat landscape by leveraging additional knowledge from the Splunk Security Research team. Within Use Case Library, subscribers get regular updates to help security practitioners of all skill levels stay current with the latest cyberthreat trends and defense tactics in order to quickly address those threats.

Additionally, there are over **800 other security-related apps** on Splunkbase with pre-built searches, reports and visualizations for specific third-party security vendors. These ready-to-use apps and add-ons provide capabilities ranging from monitoring security, next generation firewall, advanced threat management and more. These increase the security coverage and are provided by Splunk, Splunk partners and other third-party providers.

There are several ways to migrate from the legacy or complex SIEMs to Splunk. Please **contact Splunk sales** to learn more. Splunk has technical resources, including dedicated security specialists, who can work with you to determine the best migration path.

Thousands of customers use Splunk software for SIEM and advanced security use cases. Splunk has won numerous industry awards including placement as a leader in the Gartner Security Information and Event Management (SIEM) Magic Quadrant.but there's very little that can be done to prevent cybercriminals from launching these attacks. Worse yet, most IT organizations simply don't have the manpower to keep up with those attacks on their own. The difference between that attacks being a routine annoyance versus a catastrophic event invariably comes down to the robustness of an organization's SIEM platform.

The good news is that setting up an analytics-driven SIEM is easier than ever. Add to that the sophistication that a modern SIEM can now apply to defending the IT environment and it quickly becomes not a question of whether an IT organization needs a SIEM, but rather how quickly can it be implemented before the next wave of cyberattacks get launched.