splunk>

TECH BRIEF

Using Splunk® Software as a SIEM

Replace a Security Information and Event Management (SIEM) solution with Splunk.

HIGHLIGHTS

- Splunk is used for security by thousands of customers
- A proven, integrated, big data security platform
- Enables a wider range of security and non-security use cases than traditional SIEMs
- Traditional SIEMs lack the scalability and flexibility to deliver on the promise of SIEM

SIEM Requirements

SIEMs should enable the use cases and have the capabilities listed below. Splunk software can handle these plus much more.

- Real-time aggregation of security-relevant data
- Ability to add context to security events
- Incident investigations/forensics
- Security reporting and visualizations
- Real-time correlations and alerting for threat detection
- Advanced/unknown threat detection
- Compliance reporting

Industry Trends

Three SIEM trends call for a big data SIEM:

All data is security relevant and should be indexed. For IT security teams to properly investigate security incidents and identify threats, the data indexed for SIEM use cases needs to include more than security data from traditional security products such as firewalls, IDS or anti-malware. The data indexed also needs to include "non-security" data from sources such as OS logs, LDAP/AD, badge data, DNS, NetFlow and email/web servers. This is because traditional security products can only reliably detect "known" threats for which signatures exist. They cannot detect the advanced threats of today, whether they are nation states, cybercriminals or malicious insiders, which are "unknown" threats for which no signature exists. The minute fingerprints of these advanced threats are often only in the "non-security" data. The diagram in Figure 1 illustrates this.

Automated anomaly and outlier detection is needed. To detect advanced threats, all non-security and security data must reside in a single repository that is monitored in real time. This represents a massive amount of data and will provide a repository to baseline normal user and traffic activity. Using this baseline, real-time 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 off the norm. Correlations can also help by detecting combinations of events that are rarely seen and are suspicious.

Need to reduce IT security costs and raise efficiency. IT security is constantly facing budget pressure and is being asked to do "more with less." This includes finding flexible security products that:

- Address multiple security and compliance use cases
- Realize a fast time-to-value and are easy to deploy
- Accelerate incident investigations and automatically detect advanced threats, reducing labor costs
- Do not require purchasing costly physical appliances

The Limitations of Traditional SIEMs

Many IT security teams have made a significant investment in both money and people to support a traditional SIEM, only for the SIEM to fall short of vendor promises and never be fully deployed.

The reasons for the broken promises are numerous. They are often tied to the dated architectures of traditional SIEMs, which typically use a SQL database with a fixed schema. This database is a single point of failure with scale and performance limitations. Customers with failed SIEM deployments commonly complain that it is difficult to get data into the SIEM and that queries can take hours to run, often never finishing. To get around performance issues, SIEM vendors often sell one product for raw logs and yet another product with a SQL database containing a subset of this raw data for SIEM use cases. This "data reduction" process inevitably hampers future incident investigations or advanced threat detection, when all the original data is needed to get to the root cause or to find the tiny fingerprints of an advanced threat. Lastly, the vendor often requires expensive physical appliances to try to improve performance.

Delivering a New Approach for SIEM

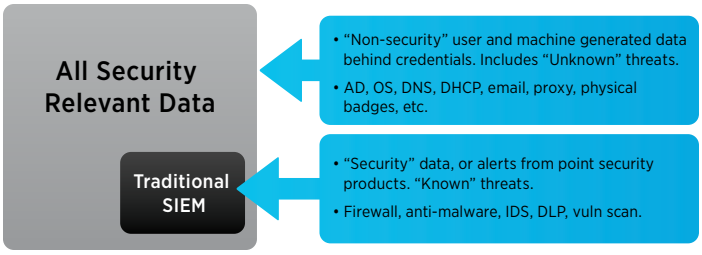

Figure 1

Splunk has quickly emerged to be a leading SIEM vendor. Over 2,000 customers use Splunk software for security use cases and Splunk has won numerous industry awards including placement as a leader in the 2013 Gartner Security Information and Event Management (SIEM) Magic Quadrant, and SC Magazine 2013 global awards for "Best SIEM Solution - US" and "Enterprise Security Product - EMEA."

Key to the Splunk success is a big data architecture and flexibility. Splunk software is not hampered by a SQL database and instead uses a flat file data store to make it possible to quickly index all the original, raw data from any source at massive data volumes. Our largest license is 100 terabytes of data indexed per day. The Splunk product scales out horizontally using commodity hardware, not costly physical appliances and Splunk uses an implementation of Google's MapReduce search technology to enable fast distributed searching.

Splunk software also offers powerful and flexible search and reporting capabilities in contrast to traditional SIEMs. In Splunk it is easy to get to the data you are after and then turn the results into a wide range of interactive reports and visualizations. These visualizations can also be used for measuring technical controls associated with compliance use cases.

The table below lists some of the limitations of traditional SIEMs and how the Splunk approach differs:

Traditional SIEM Limitations	Splunk Advantages/Differentiators
Multiple, discrete products (Logging and SIEM)	One platform (Splunk Enterprise)
Often costly, physical appliances	Software-only. Can be installed a wide range of OS's
Difficult to deploy; long time-to-value	Fast time-to-value. Customers often see value in hours or days
Reliance on vendor collectors or custom collectors	Not reliant on Splunk for "collectors." And if Splunk does not have the "collector" you need, it can easily be created
Database schema and normalization limits investigations and correlations	Flat file data store with no schema or normalization. All the original data is retained and can be searched on
Scalability and speed issues due to SQL database	No SQL database and uses Google's MapReduce for fast, distributed searches
Lack of search flexibility limits the ability to find outliers/anomalies	Splunk search language can do automated baselining and the calculation of outliers/anomalies, as well as advanced correlations
Limited flexibility in modifying or creating reports	Easy to create new reports or modify existing ones. Data can be visualized in many ways including tables, charts or scatterplots
Specializes in 'known threat' detection	'Known threat' detection, and can also index "non-security" data to identify the outliers that may be "unknown threats"
Closed products lacking APIs, SDKs, apps	Rest API with several SDKs exposes all the features and data in Splunk. Over 400 free apps on Splunkbase. Splunk UI and all configuration files are exposed for easy modification
Only security/compliance use cases	Other use cases include compliance, application security, fraud detection, IT operations, application management, web intelligence and business analytics. Results in more cross-department collaboration and stronger ROI

Using Splunk Software for SIEM

Splunk offers two products that support SIEM use cases, Splunk Enterprise and the Splunk App for Enterprise Security.

Splunk Enterprise is the core Splunk platform. It provides the core collection, indexing, search and reporting capabilities. Many Splunk security customers use the core Splunk Enterprise product to build their own real-time correlation searches and dashboards for a SIEM-like experience.

For Splunk customers looking for pre-built, SIEM-like content, there is the Splunk App for Enterprise Security which runs on Splunk Enterprise and contains pre-built correlation rules, alerts, reports, dashboards, incident review/workflow functionality and third-party threat intelligence feeds.

Additionally, there are over 40 other security-related apps on Splunkbase with pre-built searches, reports, and visualizations for specific 3rd-party security vendors, including Palo Alto Networks, Blue Coat, FireEye, Symantec, Cisco, Nessus, Websense, Sourcefire and Microsoft.

Migrating from a Traditional SIEM to Splunk Software

There are several ways to migrate from a traditional SIEM to Splunk software. Please contact Splunk sales to learn more. Splunk has technical resources, including dedicated security strategists, who can work with you to determine the best migration path.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

250 Brannan St, San Francisco, CA, 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.splunkbase.com

Item # TB-Splunk-SIEM-107