

Splunk for Security

Supporting a Big-data Approach for Security Intelligence

Security's New Challenges

The role of IT security is expanding, driven by new and evolving security use cases with risk implications for the business. Kevin Mandia of Mandiant estimates that there are “thousands of companies that have active APT (Advanced Persistent Threat) malware.” This malware is left behind through targeted attacks from persistent adversaries. The current conventional approach provides key reasons for the proliferation of security threats:

- In many organizations, perimeter defenses remain the primary focus for the security team;
- Signature and rule-based systems used by security teams are not able to keep up with the flood of new attacks
- SIEMs primarily set to collect data from signature-based or rule-based systems
- Security incidents identified in the absence of contextual data from IT operations
- Canned reports have given the impression that critical thinking and analysis are not necessary
- Systems that lack the scale and analytics needed to map potential threats against large data sets over long periods of time

This conventional security mindset and approach doesn't cover “unknown threats” from new more sophisticated malware that:

- Leverages data from social media sites supporting social engineering
- Obtains entry into the network via end users and end points
- Evades detection (redefined low and slow techniques)
- Uses unique attack patterns that allows the malware to be disguised as a “normal” application

With a much broader set of possible attack vectors and more innovative and targeted attacks coming from persistent adversaries, the amount and types of data analyzed must be expanded. A security intelligence approach is one that watches for known threats as reported by signature and rule based systems, and watches for unknown threats using extensive analytics on the behaviors of system users. Normal user activities needs to be monitored to understand time-based patterns of access, usage, and location.

Splunk: Big Data and Security Intelligence

An approach to security that applies pattern analysis to user activities around the most sensitive business data—aligns with business risk. The more operational and security data collected the better the insight into business risk. Collecting and correlating data from the widest possible sources is the first step to gaining visibility of your infrastructure and improving your security posture.

Behavior-based analysis is the next step in a security intelligence approach. In cooperation with the business, identify your most important digital assets. These could be data stores of personally identifiable information (PII), intellectual property, internal emails, or other information retained on systems that are of high value to attackers. The final step is to apply an “actor-based” approach to understand the modus operandi and methods of potential adversaries. Security intelligence analysts need to routinely ask:

- Who would I target to access data and systems that contain the highest value of collected data?
- What methods could I use to facilitate the stealthy spread of malware?
- How can I make sure my command-and-control communications are not detected?
- What changes should I make to the host to make sure my malware stays resident in the enterprise?
- What would abnormalities in my machine data look like in the event of an attempted email exfiltration or a transfer of PII outside the company?
- What host network services should be monitored for changes?
- What malware behaviors can be differentiated in log data based on time-of-day, length of time, and location of origin?

A behavior-based approach to advanced persistent threats using pattern analysis enables an advanced approach to threat detection, as recommended by the Security for Business Innovation Council.

It is important to note that having a big-data approach for unknown threats doesn't supplant the traditional approach for monitoring known threats. Watching for known threats using elements of a conventional approach to security is still a requirement.

	Conventional Approach	APT / Risk-Based Approach
Controls Coverage	Protect all information assets	Focus efforts on most important assets
Controls Focus	Signature-based preventive controls (AV, Firewalls, IPS)	Detective controls - data analytics
Perspective	Perimeter-based	Data-centric
Goal of Logging	Compliance reporting	Threat Detection
Incident Management	Find and neutralize malware and/or infected nodes (reactive)	Big Picture: Seek, find and dissect attack patterns (proactive)
Threat Intelligence	Collect information on malware	Develop deep understanding of attackers modus operandi in context of the organization's key assets and IT environment
Success Definition	No attackers get into the network	Attackers sometimes get in, but are detected quickly and impact (risk) is minimized

Figure 2 - When Advanced Persistent Threats Go Mainstream, Security for Business Innovation Council, 7/21/2011



“Rules-based SIEMs aren’t designed to detect polymorphic attacks or patterns from advanced persistent threats”

Splunk: The Platform for Security Intelligence

While the core Splunk Enterprise platform with its scalability, analytics, visualization and alerting capabilities allow you to ask scenario-based questions of your data, Splunk is also a platform for security apps (over thirty as of this writing). These are available on Splunkbase.com.

The Splunk App for Enterprise Security

The Splunk app for Enterprise Security supports SIEM capabilities and watches for known threats and monitors key security metrics. This app operates as a ‘lens’ into your security data. It is designed for the security professional organizing data into specific security domains while collecting data from traditional security architectures automatically, and delivers real-time dashboard visualizations. The App can act as a jumping off point into unknown threat detection, support identity correlation or manage a team of security experts who review incidents on a daily bases. The Splunk App for Enterprise Security is an important part of a security intelligence strategy.

Using Splunk for Security

Flexible, Scalable Security Investigation

Splunk is scalable and flexible enough to search across terabytes of data from any data source such as traditional security sources, custom applications, and databases. Splunk automatically provides a time-line view of all collected data.

This timeline can be used to focus on the precise moment in time a security event occurred. Any search result can be turned into a report for distribution. This is especially useful for ad-hoc queries in support of compliance initiatives such as PCI, SOX or HIPAA.

Real-time Forensics Operationalized

Once a forensic investigation is complete, Splunk searches can be saved and monitored in real time. Real-time alerts can be routed to the appropriate security team members for follow-up. Correlation across system data by vendor or data type is supported in Splunk’s easy-to-use search language.

Splunk’s search language supports correlations that can generate alerts based on a combination of specific conditions, patterns in system data or when a specific threshold is reached.



“Splunk allows us to quickly consolidate and correlate disparate log sources, enabling previously impractical monitoring and response scenarios.”

Splunk lets you see real-time information from security and network devices, operating systems, databases and applications, on one timeline enabling security teams to quickly detect and understand the end-to-end implications of a security event. Splunk watches for hard-to-detect patterns of malicious activity in machine data that traditional security systems may not register. This approach can also provide the building blocks for a variety of supported fraud and theft detection use cases.



“Our Security and Fraud teams detect and investigate fraudulent activity quickly.”

Metrics and Operational Visibility

Understanding business risk requires a metrics-based approach to measure effectiveness over time. Splunk’s built-in search language contains the commands needed to express search results as tables, graphics, and timelines on security dashboards. Key performance indicators (KPIs) can be monitored by business unit, compliance type, location and more.

Real-time Correlation and Alerting

Correlation of information from different data sets can reduce false-positives and provide additional insight and context. For long-term correlations, Splunk can write individual system events to internal files also monitored by Splunk and aged out over time. If the right group of events writes to the file, before it is aged out, the correlation is completed and an alert is issued. Splunk supports a rich set of alert creation criteria providing rule based alert suppression and thresholds.

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. You can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.