splunk>

SOLUTIONS GUIDE

Splunk® for Security

Supporting a Big Data Approach for Security Intelligence

Security's New Challenges

Advanced threats have permanently changed how organizations think about cybersecurity. It's no longer enough to monitor for known threats or to just rely on security point products that provide a narrow view. Security teams need an infrastructure-wide view of activities in order to identify, understand and stop attackers.

There are four classes of data that security teams need to leverage for a complete view: log data, binary data (flow and PCAP), threat intelligence data and contextual data. If any of these data types are missing, there's a higher risk that an attack will go unnoticed. These data types are the building blocks for knowing what's normal and what's not in your environment. This single question lies at the intersection of both system availability (IT operations and application) and security use cases.

The amounts and types of data needed for making the most effective data-driven security decisions requires a solution that:

- Will scale to collect tens of terabytes of data per day without normalization at collection time and applies a schema to this data only at search (query) time
- Can access data anywhere in the environment, including traditional security data sources, personnel time management systems, HR databases, industrial control systems, Hadoop data stores and custom enterprise applications that run the business
- Delivers fast time-to-answer for forensic analysis and can be quickly operationalized for security operations teams
- Provides a flexible security intelligence platform that includes significant out-of-the-box content and apps that can maximize security infrastructure investments and the skills of your security team

Understanding advanced threats and business risk drives the need to make more data available for analysis and to see events in context. In this light, all data can be security relevant.

New Security Opportunities

Today's security professionals are looking beyond a basic perimeter defense. These teams and their business stakeholders want to better understand threats from malicious insiders and advanced threats from remote attackers. To fully understand the malicious insider, the security professional needs to watch for indicators in context. For example, seeing an increasing number and size of print jobs from a single person at odd hours coupled with large file transfers out to a cloud service may not reach the threshold of investigation; however, seeing this in the context of a dramatic change in the categories of websites being accessed by an individual, a 'pink slip' lay-off list or even a recent change in marital status could warrant the need for HR to remind the individual of relevant corporate policies.

A rules-based approach is not designed to catch advanced threats because it can't possibly predict all the conceivable threat vectors an attacker may choose or which data sources may be relevant in advance of the attack. In this case, determining what is and isn't "normal" is done through statistical analysis and watching for behavioral outliers. Once an outlier is discovered, the analyst can immediately see it in the context of threat data.

The newest security strategy against advanced attackers divides an attack into stages called the "kill chain" (see *Figure 1*). Defenders can use the kill chain as a way to break down and analyze events, with the goal of stopping attackers as early as possible. Splunk

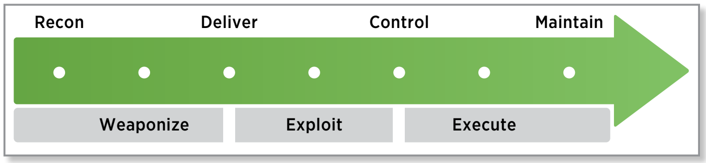
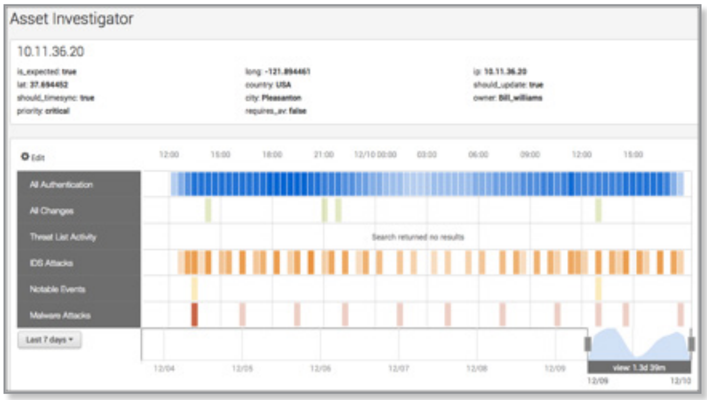


Figure 1: The stages of the kill chain.


Asset Investigator

10.11.36.20

is_expected: true
lat: 37.694452
should_timesync: true
priority: critical

long: -121.894461
country: USA
city: Pleasanton
requires_av: false

ip: 10.11.36.20
should_update: true
owner: Bill_williams

Figure 2: The Asset Investigator provides a comprehensive view of events.

software is ideally suited for this type of analysis. Correlation searches can be tagged to align with phases in the kill chain so that non-authorized scans, social media data or website data can be used to identify threats. For example, a sudden increase in hits to the business leadership page of the corporate website could be attackers in the recon phase of an attack. Once the searches are tagged with the appropriate phase of the kill chain, the phases are easily represented as a graphic in Splunk and can be prioritized by the organization.

Splunk: Stalking Cyber Criminals

An approach to security that applies pattern analysis to user activities around the most sensitive business data can also minimize business risk. More operational and security data results in better insight into business risk. Collecting and correlating data from the widest possible sources is the first step to gaining visibility into your infrastructure and improving your security posture.

Using behavior-based analysis is the next step in a security intelligence approach. Security teams need to work with the business to identify the most important digital assets. These can be data stores of personally identifiable information (PII), intellectual property, internal emails or other high value enterprise information. The final step is to apply an IT risk scenario approach to understand the modus operandi and methods of potential adversaries. Security intelligence analysts need to routinely ask:

- Who would I target to access 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?

Whether or not you map to the kill chain, a behavior-based approach that employs analysis to determine what's normal/what's an outlier and enables the discovery of threat activity patterns, is the best and most advanced approach to threat detection (see *Figure 2*).

It is important to note that having a big data approach for unknown threats doesn't supplant traditional methods for monitoring known threats. Watching for known threats using point solutions is still a requirement given the constant flow of less sophisticated attacks. A dual approach to known and unknown threat detection is optimal and also recommended by the Security for Business Innovation Council (see *Figure 3*).

	Conventional Approach (Known Threats)	**APT / Risk-based Approach (Unknown Threats)**
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 3: 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

Splunk software supports security teams with two approaches for security intelligence. Splunk Enterprise is the core Splunk software platform with thousands of successful worldwide security deployments, providing customers with scalability, analytics, visualization and alerting capabilities. The product allows you to ask scenario-based questions in real time and to create shareable reports based on your discoveries.

Running on the core Splunk Enterprise platform, the Splunk App for Enterprise Security supports traditional SIEM capabilities, watching for known threats and monitoring key security metrics. The app operates as a 'lens' into your security data. Designed for the security professional, it organizes data into specific security domains while collecting data from traditional security architectures automatically, delivering real-time dashboard visualizations. Unlike the traditional SIEM, the app can also act as a starting point for unknown threat detection by using statistical analysis to detect anomalies and outliers. Splunk Enterprise and the Splunk App for Enterprise Security are an integral part of a security intelligence strategy.

Splunk Enterprise is a platform for security intelligence, with over 80 apps available, including apps from leading security technology providers such as: Palo Alto, FireEye, Cisco and F5. Apps are available on apps.splunk.com.

Using Splunk for Security

Flexible, Scalable Security Investigations

Splunk Enterprise is software that is scalable and flexible enough to search across terabytes of data such as traditional security sources, custom applications and databases. Splunk automatically provides a timeline view of all collected data.

This timeline can focus on the precise moment in the past a security event occurred or be viewed in real time. 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, FISMA or HIPAA.

Real-time Forensics Operationalized

Once a forensic investigation is complete, Splunk Enterprise searches (queries) 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 Processing Language (SPL™).

Splunk SPL 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 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.

Make Data More Meaningful to More Users

Splunk Enterprise automatically extracts knowledge from your data. Additional knowledge and security context can be added by identifying, naming and tagging fields and data points. You can even add information from external asset management databases, configuration management systems and user directories. Expand the use of Splunk in your organization without having knowledge of the Splunk SPL by defining Data Models that describe relationships in the underlying machine data. Data Models can then be used to power the Splunk Pivot interface, which allows any user to easily build Splunk reports.

Metrics and Operational Visibility

Understanding business risk requires a metrics-based approach to measure effectiveness over time. The Splunk SPL contains over 100 commands that can help users 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 age them 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 6 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.