splunk>

SOLUTIONS GUIDE

Splunk® for Enterprise Security

Defending against the next generation of cyber-attacks & threats

HIGHLIGHTS

- A new generation of cyber-attacks called Advanced Persistent Threats (APTs) has proven destructive and very costly.
- Traditional security technologies lack the data-driven techniques to thwart highly sophisticated, human-driven APTs.
- Splunk for Enterprise Security delivers the intelligence and analytics needed to detect and deter these and future exploits.

Today's Evolving Threat Landscape

Costly cyber-attacks are routinely in the news and many more go unreported. Many enterprises assume it's only a matter of time before they're hit. More troubling, victims are often large companies that amply invested in up-to-date security. Their defenses proved ineffective against a new generation of exploits called *Advanced Persistent Threats* (APTs).

These attacks are launched by criminal syndicates, nation states, and disgruntled insiders who have replaced joy-riding hackers and automated worms. These are cunning, resourceful and patient people who probe for vulnerabilities and learn from failures. They use valid credentials, making them very difficult to detect, and dynamically adapt to changing environments and defenses. Moreover, they're determined, exploiting new technologies, refining their techniques and innovating new ones.

An APT is not a single event or a rote technology exploit, but an attack transaction comprised of people, technologies and processes. It's a series of actions stealthily orchestrated across the IT infrastructure. The median number of days before an intrusion is detected is 229 and 67 percent of victims were alerted not by internal staff and tools but by customers, partners and even the FBI. The risks are great, the stakes high and the adversaries more formidable than ever.

The Kill Chain

Attackers follow a general pattern called the "kill chain." In Zeus attacks, for example, which are used to steal financial data, they start with *reconnaissance* to find weaknesses. In this case, they steal a vulnerable corporate PDF on a company's web portal. In the *delivery* phase, they embed executable code in the PDF and use phishing techniques until an employee opens it, thinking it's a legitimate file. *Exploitation* follows when the malware installs programs that establish communications with the intruders' *command and control* server. They're now inside and can move about freely to explore the environment. Finally, there are *actions on intent* as the criminals identify their targets and exfiltrate data that they conceal in routine outbound web traffic.

Nor does it end there. The environment remains compromised. The hackers will lurk about with valid credentials, prowling for targets that can be monetized on international black markets.

Until, and if, they are detected and expelled.

100% Percentage of attackers using valid credentials	**40** Average number of systems accessed
229 Median number of days before detection	**67%** Percentage of victims notified by an external entity

Table 1: Characteristics of Advanced Persistent Threats.

Connecting the Dots

In today's threat landscape, enterprises require data-driven, operational intelligence to evaluate events holistically rather than disparately. Pre-defined rules won't detect dynamic relationships of actions along the kill chain. Isolated, low-severity events, when correlated, could be a high-severity incident demanding immediate attention. Correlating data reveals the artifacts and evidence of infections, particularly when infected elements act normally or when stolen credentials are used. Noting a login after multiple failures is useful, but static rules won't reveal if malware was downloaded. Only when the entire security stack and other data sources are integrated will attributes, actions and interactions be revealed. Correlations must go beyond time- and event-based information to include location, phase and other data types. Rules-based SIEMs fail to discover next-generation exploits because APTs operate outside their functionality.

Visibility, Analysis & Action

Hardening the enterprise begins with *visibility* across the space where intruders might enter. Data from the network, endpoint and payload analysis components of the security stack are primary for analysis. To provide context, however, these data must be enriched with threat intelligence, asset and identity management to see who logs in and owns assets, and data from outside the stack. Data must be inclusive; don't filter out false positives. Amidst all the user- and machine-generated data lie the attacker's footprints.

As befitting the adversary, investigations call for depth and agility. For *analysis*, organizations must access data as needed, enrich this information and bring in historical data for baselines and perspectives. They need to pivot across multiple events or domains, from proxy to endpoint logs. They have to correlate any kind of information, including metadata and data from external sources. Lookups are critical, but the data sources are many and their output voluminous in both structured and unstructured formats. Cybercriminals leverage this complexity.

Only once events are connected and the attacker's processes and targets revealed can *action* must be taken to protect the enterprise. This will include changing endpoint and network configurations, blocking IP addresses, reimaging systems, changing policies, and sharing tactics and other intelligence.

Comprehensive Security Analytics

Enterprises that defend against APTs use security analytics platforms to unify visibility, analysis and action. They integrate all data types and enable searches, enrichment, contextualization, statistical analysis and reporting. They promptly respond when alerts notify them of unusual behavior. They have the tools,

Copyright © 2014 Splunk, Inc.
250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.splunk.com

resources and knowledge to adapt to evolving threats and detect and disrupt any criminal processes across the kill chain.

Enter Splunk

Splunk for Enterprise Security is a scalable framework for countering current and future exploits like APTs. Its core platform is Splunk Enterprise, which collects and indexes machine-generated data—structured and unstructured—from any source or location. Data sources from real-time feeds to historical information can be accessed, searched, correlated and visualized in dashboards for analysis and sharing.

Splunk for Enterprise Security is an entire ecosystem of over 80 security-focused apps for specific use cases or products. You can enhance Splunk Enterprise precisely to your IT and business needs. The Splunk App for Enterprise Security, for example, delivers such functionality as automated correlations searches, reports and security metrics, and a threat intelligence framework. Moreover, you can use Splunk API and SDKs to further extend the platform. These are some of the data sources that the Splunk security platform can integrate for visibility, analysis and action:

- Network (firewalls, web gateways, intrusion detection/prevention, packet capture, deep packet inspection and DNS events)
- Endpoint (Endpoint Threat Detection & Response [ETDR], endpoint event data, and application and services data)
- Payload analysis (dynamic, static and sandbox)
- Asset and Identity Management (asset databases, Active Directory and LDAP)
- Threat Intelligence (blacklists, reputation feeds, malware feeds, hashes and indicators of compromise).

The Splunk security platform is a critical part of the measures deployed by enterprises and governments worldwide. It indexes all machine data without modifying the events for deep visibility to map the kill chain. This visibility is easily extended with non-event sources on the fly, such as asset and identity information or threat intelligence from spreadsheets and web feeds. Time-based correlations identify relationships based on time, proximity or distance. Transaction-based correlations track related events as a single transaction to measure duration, status or other analysis. Lookups correlate machine data with data sources outside of Splunk Enterprise.

Drill down, pivot and search data for anomalies and linkages. Switch between data sources, building context and weaving through the kill chain. Because the Splunk platform automatically extracts fields from data sources, you can build the event sequence by mapping and correlating disparate data sources.

Event Correlation

To identify malevolent behavior in your environment, the Splunk security platform lets you view events in context of each other and enriched with other data. For example, someone logs in with a rarely used default administrator name. Anti-malware software detects malware running on a machine. A data loss prevention tool sees unencrypted credit card numbers leaving the enterprise. Event correlation connects the dots by revealing all three events are linked by the same IP address. The endpoint is compromised and you're in the latter stages of the kill chain. Using indicators and attributes from these and related events, you can determine appropriate remediation and containment. You can look back into the kill chain to determine how the attacker got in. You also can discover if the intruder moved laterally to infect other systems and maintain a presence in your environment. With the Splunk security platform, in-depth analysis is done quickly and easily. Additionally, the solution can detect and/or alert on correlations in real-time or on a scheduled basis.

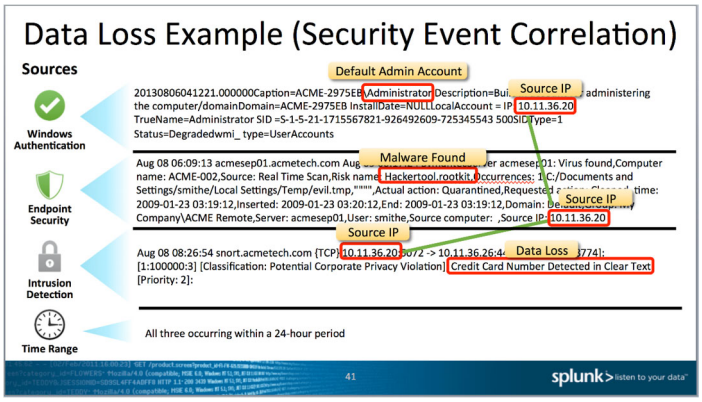

Figure 1: Event correlation reveals data loss.

Extract Intelligence & Insight from All Your Data

With the Splunk security platform, you can correlate data from non-security sources when threats are unknown to traditional products because no signature exists for them. For example, an employee receives an email from a mysterious email domain and goes to a never-visited web site. An unknown service then starts on the employee's machine. Splunk software can correlate all three events and issue an alert indicating a spear-phishing exploit. By correlating other data, you can rapidly determine if these events are the start of an ill-intentioned transaction and then take appropriate corrective measures.

Detect Insider Threats

With visibility across your IT infrastructure, you'll detect malicious insiders who have trusted credentials. Detecting these perils requires both traditional security information and non-traditional indicators like HR, personal and other "people-oriented" data. You can correlate data like changes in web surfing or activities at unusual times with such personal data as dropping credit scores or demotions, and activities like the use of default accounts and access to network diagrams and code. With Splunk, you have the insight to understand what's happening in your environment.

Listen to Your Data

Your security operations must match the high levels of attackers. Relying only on point technologies is a primary reason criminals can enter organizations. Their attacks utilize people, processes *and* technology. With Splunk for Enterprise Security, you can respond in kind. You'll reveal all processes and actions in your IT infrastructure, identify those that are malevolent, and quickly take the right countermeasures. With Splunk security solutions, you'll see better, learn faster and make more effective decisions.

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.

Copyright © 2014 Splunk, Inc.