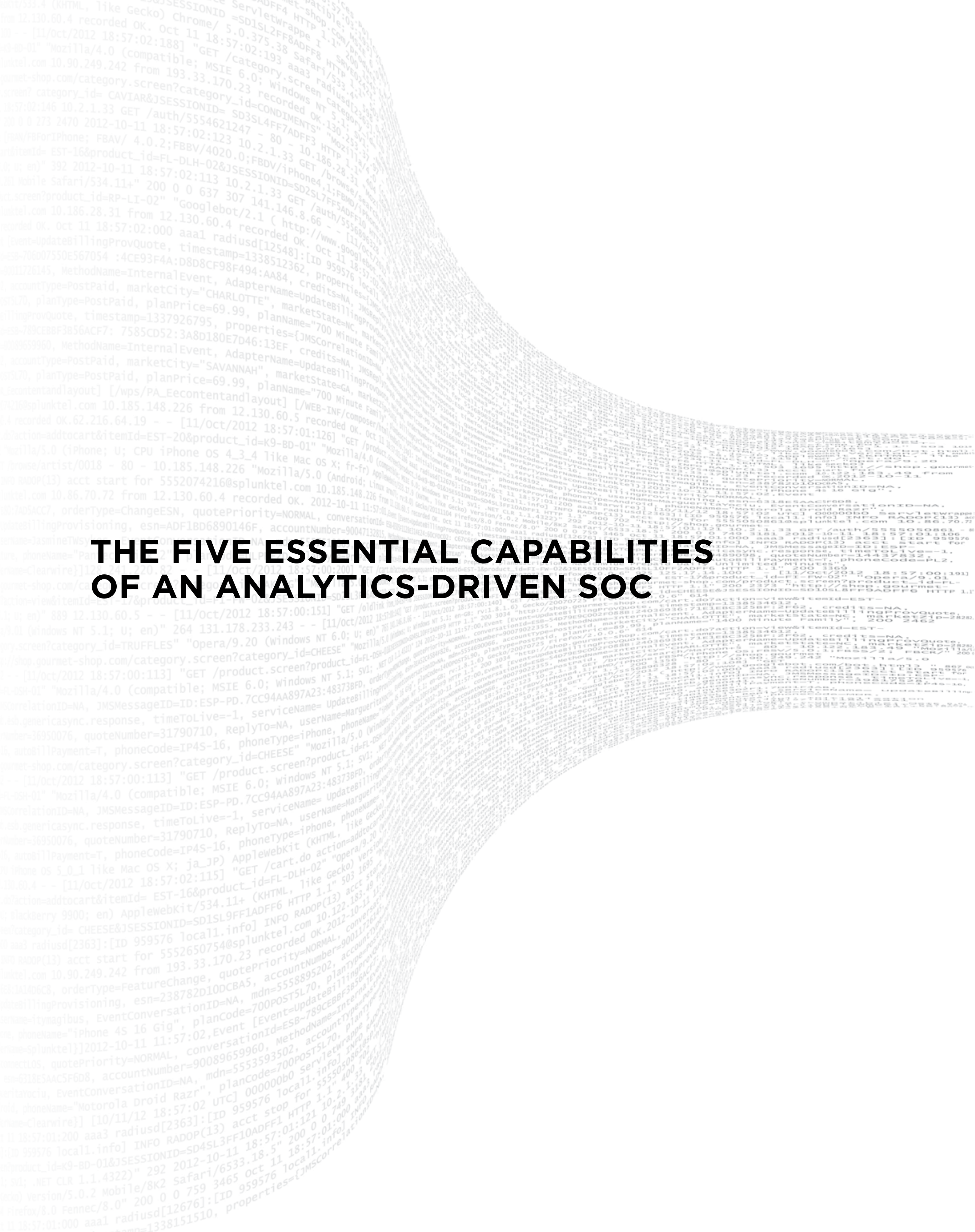
WHITE PAPER



THE FIVE ESSENTIAL CAPABILITIES OF AN ANALYTICS-DRIVEN SOC

As the volume and sophistication of cyberattacks accelerates, security operations centers (SOCs) have become the focal point for consolidating the necessary people, process and technology for an organization's defense and response. The trouble is that most IT and business leaders don't really know their real level of risk vulnerability. They have no real visibility into all the potential vulnerabilities that might be exploited, let alone a means to fix them.

But organizations can keep up with modern threats by adopting an analytics-driven SOC. A successful SOC can improve an organization's incident detection and response while accelerating and enhancing its security posture.

The legacy SOC

The role a SOC plays in preventing cyberattacks is relatively straightforward. Rather than respond to cyberattacks in an uncoordinated fashion, a SOC enables IT organizations to rapidly provide context by centralizing security management around a well-defined set of processes.

A SOC also builds on the change management and maintenance of security devices and monitoring log and events that are primarily handled by a security information and event management (SIEM) platform. Most IT organizations are already dependent on IT environments that have scaled beyond the ability of any manual management by humans – and security.

A recent Gartner study **found that an intelligence-driven SOC** significantly improves the overall security posture of any organization by adding threat intelligence, analytics, automation and investigation capabilities via an adaptive security platform.

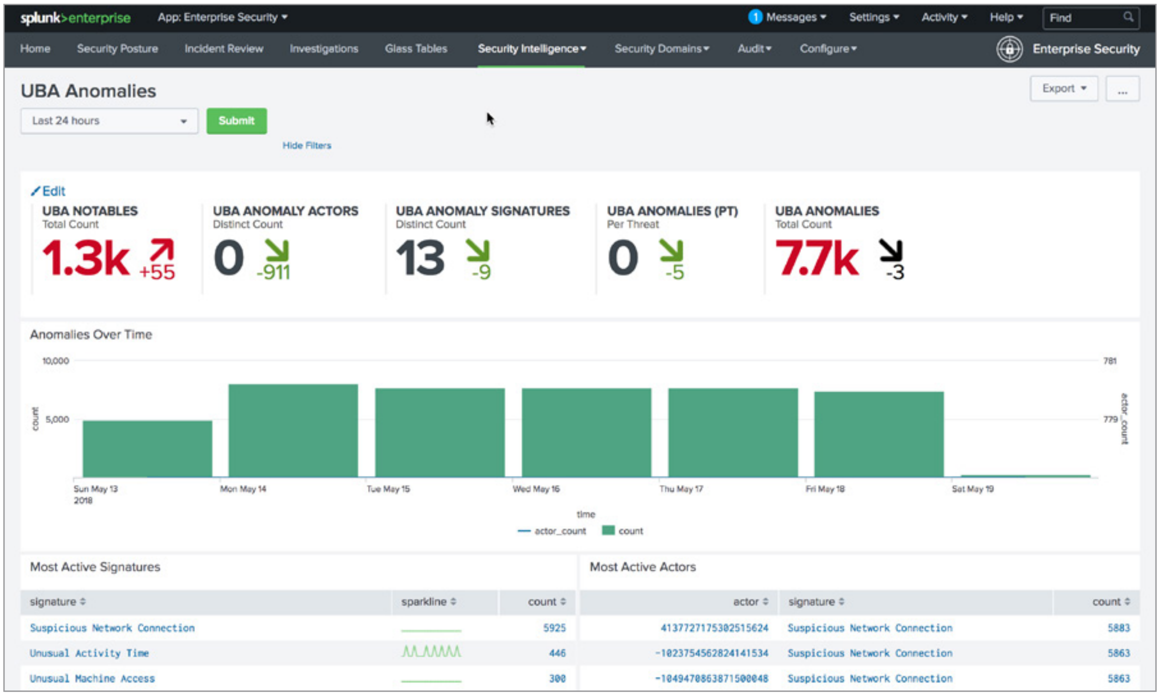
THE EVOLUTION OF A SOC	
Common Virtual SOC	A SOC made up of remote analysts without a dedicated facility.
Multifunction NOC/SOC	When organizations combine operations capabilities like NOC or helpdesk.
Command SOC	A SOC of SOCs often seen at multinational corporations.
Co-managed SOC	Common when an MSSP performs part of the SOC duties.
Crew SOC	This is set up like a volunteer fire department: When an incident occurs, a crew is gathered to analyze and respond.

The essential capabilities of an analytics-driven SOC

Gartner **defines the five essential capabilities** needed for an intelligent, or analytics-driven, SOC as advanced analytics, threat intelligence, automation, the ability to proactively hunt and investigate, and the adoption of an adaptive security architecture.

Advanced analytics and machine learning

Advanced qualitative tools based on machine learning algorithms, data mining tools, and simulations, coupled with traditional approaches to querying and interrogating data, are all critical hallmarks of a modern security intelligence platform. Security intelligence needs to be consistently and comprehensively applied to identify new emerging threats in context with any unusual changes in end-user behavior.



UBA Anomalies

UBA NOTABLES Total Count	UBA ANOMALY ACTORS Distinct Count	UBA ANOMALY SIGNATURES Distinct Count	UBA ANOMALIES (PT) Per Threat	UBA ANOMALIES Total Count
1.3k ↗ +55	0 ↘ -911	13 ↘ -9	0 ↘ -5	7.7k ↘ -3

Anomalies Over Time

Most Active Signatures

signature ⇕	sparkline ⇕	count ⇕
Suspicious Network Connection		5925
Unusual Activity Time		446
Unusual Machine Access		300

Most Active Actors

actor ⇕	signature ⇕	count ⇕
4137727175302515624	Suspicious Network Connection	5883
-1023754562824141534	Suspicious Network Connection	5863
-1049470863871500048	Suspicious Network Connection	5863

Splunk ES integrates advanced analytics via machine learning algorithms and techniques to identify anomalies and patterns that can speed investigations and discovery. Machine learning not only helps spot trends and outliers; it also can remove the "noise" generated by all the events occurring across massive amounts of data. These machine learning techniques can also be tuned using Splunk's Machine Learning Toolkit and Splunk User Behavior Analytics.

Splunk Enterprise Security™

Splunk User Behavior Analytics™

Splunk Machine Learning Toolkit

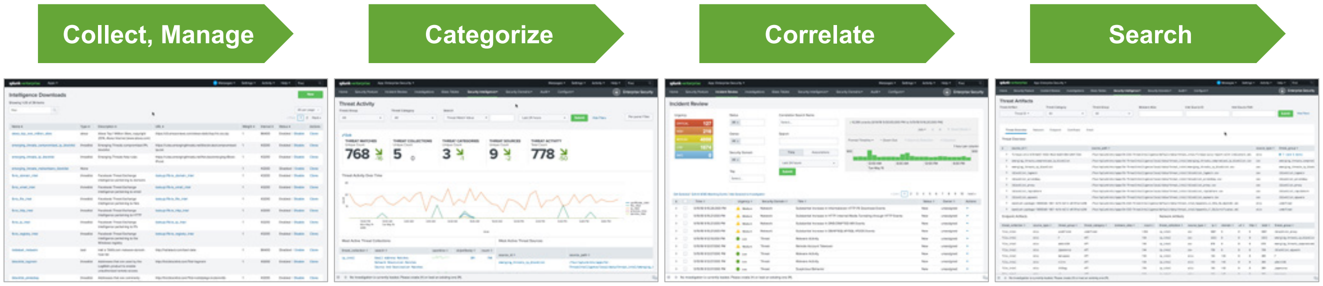
Threat intelligence

Security teams must be able to employ threat intelligence both tactically and strategically. It's not enough to collect threat intelligence information as part of a systematic effort to eliminate vulnerabilities.

Potential threat indicators such file hashes, IP addresses, registry values, service names, processes, URLs, email attributes, and certificate attributes, like common name or serial number need to be correlated against known vulnerabilities, threat sources, etc.

Splunk® ES includes a threat intelligence framework for gathering threat intelligence that automatically collects, aggregates and deduplicates threat feeds from a broad set of sources. The framework consists of modular inputs that collect and sanitize threat intelligence data and lookup-generation searches, to reduce data for optimized performance.

Threat Intelligence Framework



Data Management | Threat Activity | Correlation Data / Notable Events | Data Search

The framework also includes a number of audit dashboards that enable introspection into threat intelligence retrieval, normalization, persistence and analysis.

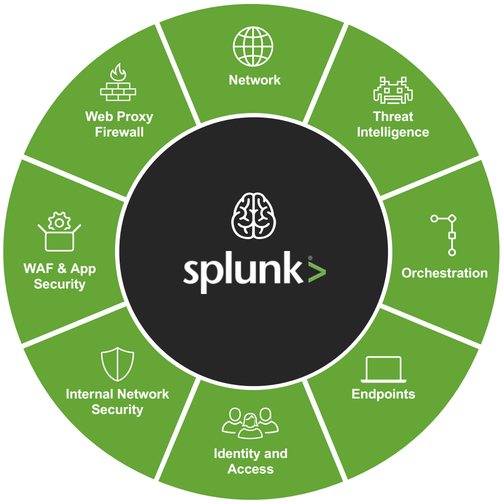
It includes access to more than 30 sources out of the box with support for STIX/TAXII, OpenIOC, and Facebook standards, as well as threat activity and threat artifact dashboards that can be deployed to quickly pinpoint specific types of threats.

Automation

IT organizations should automate security functions whenever and wherever possible depending on the risk profile of the organization. Semi-automation is sometimes necessary because a legacy SOC can require heavy staffing.

When it comes to cybersecurity, the choice of tools to use should not be discovered during a breach. The response to an attack needs to be initiated in a matter of seconds to prevent the loss of more data. Organizations need to be careful not to pollute the audit trail or invalidate evidence for legal purposes by relying on flawed manual processes alone.

Splunk Adaptive Response



Splunk ES includes a common framework for interacting with data and invoking actions.

The Adaptive Response Framework resides within Splunk Enterprise Security and helps optimize threat detection and remediation using workflow-based context. Analysts can automate actions or individually review response actions to quickly gather more context or take appropriate actions across multi-vendor environments.

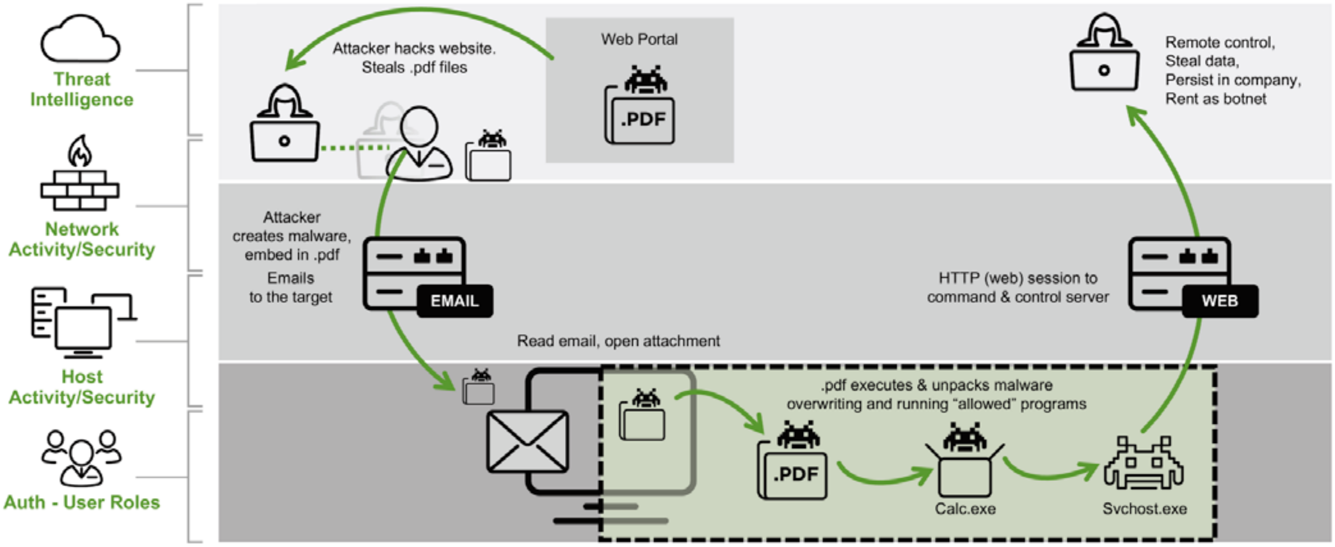
Adaptive Response can be used for automation to eliminate routine tasks, to accelerate detection and streamline their response times. The framework provides the ability to register and configure automated or assisted response actions, enabling organizations to effectively leverage their existing security products, including firewall, IDS/IPS, endpoint, threat intelligence, incident response and identity, with Splunk ES serving as the central security intelligence platform.

Analysts can also automate actions or individually review response actions so that they can quickly gather more context or take appropriate actions across a multi-vendor security ecosystem.

Proactively hunt and investigate

Assuming the perimeter defenses of the organization have already been breached, IT security teams need tools that make it simpler to discover malware wherever it lurks inside the organization. Hunting and investigating malware requires the ability to not only pivot from one dataset to another, but also the ability to cross-reference and correlate relationships with other entities – in addition to being able to view historical activity.

Depending on the organizational maturity, domain and product experience, Splunk ES can be used in combination with data collected from both third-party network and endpoint security software and hardware as well as from any number of security intelligence applications.


Threat Intelligence
Network Activity/Security
Host Activity/Security
Auth - User Roles
Attacker hacks website. Steals .pdf files
Web Portal
.PDF
Remote control, Steal data, Persist in company, Rent as botnet
Attacker creates malware, embed in .pdf
Emails to the target
EMAIL
HTTP (web) session to command & control server
WEB
Read email, open attachment
.pdf executes & unpacks malware overwriting and running "allowed" programs
.PDF
Calc.exe
Svchost.exe

CITY OF LOS ANGELES INTEGRATES REAL-TIME SECURITY INTELLIGENCE SHARING ACROSS 40+ CITY AGENCIES

To protect its digital infrastructure, the City of Los Angeles requires situational awareness of its security posture and threat intelligence for its departments and stakeholders. In the past, the city's more than 40 agencies had disparate security measures, complicating the consolidation and analysis of data. Los Angeles sought a scalable SaaS security information and event management (SIEM) solution to identify, prioritize and mitigate threats, gain visibility into suspicious activities and assess citywide risks. Since deploying Splunk Cloud and Splunk Enterprise Security (ES), the city has seen benefits including:

- Creation of citywide security operations center (SOC)
- Real-time threat intelligence
- Reduced operational costs

The city's integrated SOC does more than collect information; it also provides information. It translates data from Splunk Cloud into timely threat intelligence. The city shares its findings with its agencies as well as external stakeholders like the FBI, the Department of Homeland Security, the Secret Service and other law enforcement agencies. With this information, the city collaborates with federal agencies to identify risks and develop strategies for deterring future network intrusions.

By anchoring its integrated SOC with the rich SIEM functionalities of Splunk Cloud and ES, Los Angeles met its mayor's directive by transforming its patchwork of security measures into a cohesive, all-encompassing cybersecurity strategy.

Splunk ES can specifically help organizations with automatic threat intelligence gathering and information sharing between toolsets. The Splunk platform can also be used for operationalizing threat intelligence to implement an automated threat hunting and threat management platform. Splunk ES can take organizations from having zero visibility into threats to building a rich and sophisticated platform with the ability to automate threat hunting in a matter of weeks.

Adopt an adaptive security architecture

Traditional static security architectures based on security controls, preventative technologies and periodic strategy reviews are outdated and ineffective. An adaptive security architecture as outlined by Gartner needs to be able prevent, detect, respond and predict.

Security architectures typically involve many layers of tools and products that are not designed to work together, leaving gaps in how security teams bridge multiple domains. To successfully implement an adaptive security architecture, with the ability to prevent, detect, respond and predict, organizations need:

- Correlation across all security-relevant data
- Insights from existing security architectures
- Advanced analytics techniques such as machine learning
- Automation, wherever possible
- Integration with the security ecosystem with bi-directional context enrichment

SAIC BUILDS NEW WORLD-CLASS SECURITY OPERATIONS CENTER

SAIC is a leading technology integrator that specializes in technical, engineering and enterprise information markets. The company needed to build out a robust SOC and computer incident response team (CIRT) to defend against cyberattacks. Since deploying the Splunk platform, the company has seen benefits including:

- Improved security posture and operational maturity
- 80+ percent decrease in incident detection and remediation times
- Comprehensive visibility throughout the enterprise environment

After the original SAIC split into two companies in 2013 to avoid organizational conflicts of interest, SAIC needed to build a SOC as part of its new security program. Although it had most of the security tools it needed, SAIC lacked a SIEM solution to anchor its defenses. The traditional SIEM used by the original company as its core tool for security investigations had limitations. SAIC supplemented the SIEM with Splunk Enterprise, using the platform for incident detection via correlation searches, as well as for incident investigations. SAIC's IT operations staff is now also using the Splunk solution for network monitoring, performance management, application analytics and reporting.

Once SAIC began building its new SOC, the company decided to rely on Splunk as the single security intelligence platform for all of its SIEM-like needs, including incident detection, investigations and reporting for continuous monitoring, alerting and analytics. SAIC also purchased Splunk Enterprise Security (ES) for its pre-built correlation searches, incident review workflow, reports, dashboards and threat intelligence feeds. SAIC began indexing hundreds of GB a day of data into the Splunk solution from various data sources, including firewall, intrusion detection, anti-virus and vulnerability scanner systems.

The Splunk platform addresses these gaps with its **Adaptive Response** framework. The framework, a common interface for automating retrieval, sharing, and response in multi-vendor environments, is in Splunk Enterprise Security. To successfully implement an adaptive security architecture that enables SOC teams to prevent, detect, respond and predict security issues, Splunk ES makes it possible to correlate all security relevant data; derive insights from existing security architectures; access to advanced analytics; automate remediation; and bi-directionally share security intelligence with third-party security products and services.

A modern SOC to fight modern threats

Outdated SOCs based on legacy SIEM platforms are not up to the modern security challenge. Most existing SOCs are built on top of a legacy SIEM platform that can't cope with the amount of data that must be analyzed or keep pace with the rapid rate of change within a modern IT environment.

Given the complexity of the security challenges every organization faces today, having a SOC is critical. The issue many organizations wrestle with is whether to build and staff a SOC internally or rely on a managed security service provider to provide that capability on their behalf. The right answer will vary based on the size and nature of the risk each organization may face.

Regardless of the path chosen, every organization would benefit from evaluating its security posture based on the SOC characteristics outlined by **Gartner**. Many organizations will discover they are not as proactive with IT security as they had assumed. While that may be cause for concern, the time and expense required to build an analytics-driven SOC is not nearly as high as it once was. IT security capabilities that were once only the province of government security agencies and Fortune 100 companies are now affordable to every size company.

Do you want to learn more about how Splunk customers are using Splunk Enterprise Security to power their analytics-driven SOC and improve their security posture? Download our **free customer ebook**. **Or contact a Splunk Expert**.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com