splunk>

POCKET GUIDE

ANALYTICS-DRIVEN SECURITY IN GOVERNMENT: WHAT YOU NEED TO KNOW

TABLE OF CONTENTS

Foreword from Splunk 3

Executive Summary 4

Today's Threat Landscape 5

- Common Threats Facing Government 6

Government Security: Then and Now 7

What Analytics-Driven Security in Government Means Today 8

Industry Spotlight: Toward an Analytics-Driven Security Operations Model 10

Learning from Others: Advanced Security Investigations Case Studies 12

- **CASE STUDY 1:** Fairfax County Protects Citizen Data 12
- **CASE STUDY 2:** Better SIEM at a Federal Agency 12
- **CASE STUDY 3:** Los Angeles Integrates Real-Time Security Intelligence Sharing 13

Cheat Sheet: Analytics-Driven Security 14

- 5 Questions to Help You Prepare to Adopt an Analytics-Driven Approach to Security 14
- Key Mandates to Start With 14

FORWARD FROM SPLUNK

I often get asked, "What is the one thing that keeps you up at night?" — apparently a favorite question to ask CISOs. From my experience, many will say this is their least favorite question — and I am one of those CISOs.

Let me explain. As CISOs, our challenge is economic — we must ensure we're allocating scarce resources in the right way. Here's a better question — "why are you able to sleep at night?" And our answer —"since we're making the right investments in the right tools and people, and putting the right processes in place, I'm able to get a decent night's sleep."

Cybersecurity is a complex and sophisticated beast, but too many of us are trying to fight blindfolded. Visibility is not the only thing in cybersecurity, but it is definitely the first thing to get right.

Even if you could magically and instantly see all the critical issues across your heterogeneous, legacy, and — let's face it — sometimes poorly maintained environment — do you have enough funding and headcount to immediately address all the highest-priority ones? I'm betting "no". But that doesn't mean you don't take off your blindfold!

The key is practicing making positive economic decisions — whether in one area or another, but it must be forward progress. For example, do we now know where all source code repos and personally identifiable information are? Are we improving awareness, so we can make better decisions than before?

In government, this is especially difficult — I've spent time with SecOps teams focused on grading themselves on capabilities such as detection, in the context of NIST and other mandates — which is a great way to know where you need improvement. But to call it adequate — for example, giving yourself a "C" for being able to detect 70% of malware — well, this assumes that you can treat detection as a sequential or probabilistic problem set, of which it is neither. Stated simply, you just need to see more. Then you can make better decisions, period.

Here's an analogy — if you were a general in the US Army, you could hypothetically place soldiers everywhere on the battlefield for awareness. But if you were Special Forces — i.e., small, understaffed, and underfunded — then no matter how good you were, you would need as much intelligence as possible. Without that, you wouldn't be able to do much. More so, with the right intelligence, you can scale understaffed teams to perform well beyond what may seem feasible.

I'll conclude by circling back to the original question — what keeps CISOs up at night isn't what our teams see and know about — it's what they don't know that worries us. If we work to reduce those unknowns to a point where surprises are basically narrowed down to zero-days — wouldn't that be just fantastically boring again? Which I'm pretty sure makes for an excellent night's sleep.

— Joel Fulton, CISO, Splunk

Executive Summary

The threat landscape is rapidly changing. New sophisticated threats are creating new risks for agency cybersecurity. Attacks continue to increase in volume and sophistication, meaning that agency defenses also have to evolve.

The challenge is especially difficult for government agencies because they manage sensitive data that requires special handling, classification and heightened access monitoring for insider threats. Whether it's the Department of Energy keeping the latest U.S. oil and gas reserve data private, states and municipalities securing local election information, or the intelligence community safeguarding G-2 and tradecraft, the risks associated with sensitive data need to be understood and minimized.

In addition to confronting evolving cyberthreats, the public sector is burdened with tight budgets and resources, complex processes, and a need to keep up to date and educated on the latest mandates, attack methods, and technologies. Security teams within government agencies need more resilience, with fewer siloes and the ability to detect, investigate and respond to issues in real-time – even as they occur.

To become more resilient, agencies can start by gaining broader visibility and a deeper understanding of potentially suspicious activities. With this heightened awareness comes the ability to reduce risk, by investigating faster and more efficiently, and better aligning security staff to their strengths.

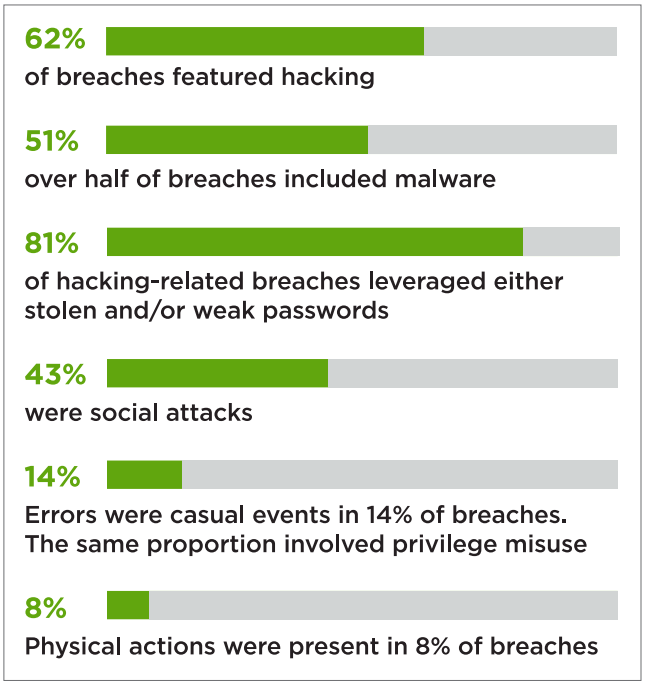
In order to achieve these results, agencies are moving toward a more holistic, analytics-driven approach. By gaining an end-to-end view of what is happening and performing more advanced investigations, many agencies are developing the ongoing resilience needed to evolve with the changing threat landscape while lowering turnover or burnout of skilled security staff.

To help clarify how agencies can better arm their cybersecurity teams to evolve, we've created this pocket guide. This new piece from GovLoop will give you an overview of the government threat landscape, describe a pragmatic model to follow, and explain the role that an analytics-driven approach to security can play in maturing operations. We also offer case studies, resources and how-tos that can help agencies move forward with better cybersecurity strategies.

Today's Threat Landscape

For government, there is no challenge greater than cybersecurity. Our national security and way of life depend on safe, secure and robust cyber defense, from federal agencies to townships.

But the unfortunate reality is that even with world-class technology, attacks and breaches are inevitable. And today, the public sector faces a more varied and alarming landscape of attacks than ever. Below are examples of threats and attack methodologies that are common in today's landscape.



STATISTICS ABOUT PUBLIC SECTOR ATTACKS IN 2017	
FREQUENCY	21,239 incidents, 239 with confirmed data disclosure
TOP 3 PATTERNS	Cyber-Espionage, Privilege Misuse and Miscellaneous Errors represent 81% of breaches within Public Administration
THREAT ACTORS	62% External, 40% Internal, 4% Multiple parties, 2% Partner (breaches)
ACTOR MOTIVES	64% Espionage, 20% Financial, 13% Fun/Ideology/Grudge (breaches)
DATA COMPROMISED	41% Personal, 41% Secrets, 14% Credentials, 9% Medical
SUMMARY	Almost one half of attacks resulting in confirmed data disclosure are state-affiliated. Timeline for breach to discovery is over 50% in the "years" category

Common Threats Facing Government

Account Takeover (ATO) – The act of impersonating someone to gain access and control over their account(s) (bank, credit card, etc.). The impersonation can be done online and/or in person.

Advanced Persistent Threat – A potential advanced cyberattack/exploit that uses multiple phases to break into a network, avoid detection and obtain information for business or political motives. Adversaries typically use that uses multiple attack vectors to obtain or change information. They can include phishing, infecting websites with malware, brute force attacks, social engineering to obtain trusted access, and targeted attacks that include zero-day exploits.

Malware - Malicious computer code used to corrupt, destroy or steal digital information. Malware includes viruses and worms, in addition to spyware the monitors user activities and ransomware that holds data hostage.

Worm - A standalone malware computer program that replicates itself in order to spread to other computer or systems.

Ransomware - A type of malware that prevents you from using your computer or accessing certain files unless some form of payment is made.

Remote Access Trojan (RAT) - A malware program that includes a back door for administrative control over the target computer; usually downloaded invisibly with a user-requested program—such as a game—or sent as an email attachment.

Rootkit exploit – Uses software designed to enable access to a computer or software that would not otherwise be allowed and often masks its existence or the existence of other software.

Man-in-the-middle - An attack where the hacker secretly intercepts, relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Zero Day Attack - Exploitation of an unknown vulnerability in software or hardware to instantly enter a platform or system without impediment.

Data Exfiltration - The unauthorized copying, transfer or retrieval of data from a computer or server.

Network Lateral Movement - A tactic used by hackers to progressively move through a network in search of key data and assets that are ultimately the target of their attack campaigns.

Botnets - An attack comprising multiple computers orchestrated for a single malicious purpose, such as denial of service or brute force attacks.

Brute Force Attack - A trial-and-error method where automated software is used to generate a large number of consecutive guesses as to the value of desired data; used to obtain information such as a user password or personal identification numbers.

Distributed Denial-of-Service - An interruption of network service, executed by sending such high volumes of traffic or data to a single network that it becomes overloaded, resulting in the targeted organization being unable to continue service.

Watering Hole Attack - A security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit.

Phishing - An attempt to extract sensitive information from an individual by masquerading as a trusted entity or person, usually via email or on websites.

Insider Threat - Employee use of government personnel, facilities, information, equipment or networks of systems to inflict harm.

SQL Injection - An attack in which malicious code is embedded in a poorly designed application and then passed to the backend database where it produces database query results or actions that should never have been executed.

These threats are complex, varied and getting more sophisticated every day. And they mutate to avoid detection, as evidenced by threats like polymorphic malware and other rapidly evolving threats. The good news is that security teams can combat these threats effectively with a strong cyber hygiene strategy. According to SANS, over 80 percent of incidents exploit known vulnerabilities. These trends point to the need to improve upon how well IT and security teams are handling the basics of security preparedness—referred to simply as cyber hygiene.

Government Security: Then and Now

The approach to security is evolving, across industries as well as in government. In the past, it was centered mainly around prevention, but as attack lifecycles continue to evolve, resulting in costlier and more destructive breaches, agencies have recognized the need to evolve with the threat landscape. Agencies are also coming to the realization that not all assets or targets are critical and are taking a risk-based approach.

A risk-based approach ensures that security teams classify assets, and then choose and implement measures based on the criticality of those assets. This approach is more pragmatic, and helps agencies to keep up with government mandates—a brief history of which is outlined below:

2002: Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), highlights the importance of information security to the economic and national security interests of the United States. It tasks NIST with responsibilities for standards and guidelines, including the development of standards, guidelines, and minimum requirements.

2003: California passed the Notice of Security Breach Act, which requires that any company that maintains the personal information of California citizens and has a security breach must disclose the details of the event.

2011: The DHS U.S. Computer Emergency Readiness Team (US-CERT) received more than 100,000 incident reports, and released more than 5,000 actionable cybersecurity alerts and information products.

2012: Then-Defense Secretary Leon Panetta stated in October 2012 that "a cyberattack perpetrated by nation-states or violent extremist groups could be as destructive as the terrorist attack of 9/11. ... Such a destructive cyber terrorist attack could paralyze the nation."

2012: The Office of Management and Budget identified continuous monitoring of federal IT networks as one of 14 Cross-Agency Priority (CAP) goals, established in accordance with the Government Performance and Results Modernization Act.

2012: To support federal departments and agencies in meeting the CAP goal, the Department of Homeland Security (DHS) established the CDM Program, an implementation approach consistent with the Information System Continuous Monitoring (ISCM) methodology.

2015: In June 2015, the United States Office of Personnel Management announced that it had been the target of a data breach targeting the records of around 18 million people.

2016: President Obama revealed his Cybersecurity National Security Action Plan (CNAP). This plan was made to create long-term actions and strategies in an effort to protect the U.S. against cyberthreats.

2017: President Trump released his cybersecurity executive order, titled Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which can be read in full **here**.

The sheer number of mandates, frameworks, and their revisions can seem daunting. The key is to start with a strong foundation. The National Institute of Standards and Technology (NIST) provides guidance in this area, including the following priority mandates:

- **FIPS PUB 199** – security categorization of federal information systems
- **Special Publication 800-53** – security and privacy controls
- **Special Publication 800-73** – Risk Management Framework (RMF) and guidance
- **Cybersecurity Framework (CSF)** – SP 800-53 and SP 800-73 form the basis of the CSF

Implementing a risk-based approach and adhering to the mandates from NIST are critical steps toward developing resilience in cybersecurity operations, based on sound cyber hygiene.

What Analytics-Driven Security in Government Means Today

In this section, we'll explain why and how an analytics-driven approach to security is critical to better cyber hygiene principles and handling of cyberattacks.

Security priorities are all too often centered around the "latest fire drill". Malicious activity will occur without warning and typically go undetected for long periods. The longer this "dwell time", the more serious the threat—meaning that by the time your security team is aware of an issue, there is a good chance your organization has already been negatively impacted, resulting in an all-hands-on-deck fire drill.

This "reactive" state is compounded by the difficulty and time-consuming nature of conducting investigations. Operational and data silos hinder end-to-end views and force teams to perform manual correlations, leading to inefficiencies. This makes investigations difficult, impractical and can lead to false positives.

A risk-based approach enables a consistent, agency-specific strategy to manage security challenges. Security teams can determine risk across the environment based on a number of tasks—from qualifying critical or high value assets, to implementing relevant controls, to continuously monitoring and validating their effectiveness by assessing security posture across the environment.

By doing these fundamental tasks well, security teams can monitor and assess risk on a continuous basis, and quickly determine whether any monitored activity has potential to be malicious and what impactful. Gaining key security insights from a single location is critical—such as where activity originated, where it spread, whom it targeted, how it is communicating, how frequently it has tried to access certain systems, and more.

This enables streamlined investigation and rapid response—critical for not only breach situations, but early detection of potentially severe issues. The right level of context allows for faster and better understanding of risk and associated decision making, and ultimately, a proactive mindset to managing risk, and finding and handling security issues.

An analytics-driven approach to security is a pragmatic model for government agencies to adopt to improve resilience to cyberthreats and attacks.

Adopting a Risk Management Approach

A pragmatic model for managing risk and ensuring cyber hygiene is to take an analytics-driven approach. Agencies can adopt this model to facilitate their journey toward improved resilience to cyberthreats and attacks. An analytics-driven approach enables security operations to evolve and mature toward more efficient and advanced detection, investigation, and response methods based on a "single source of truth".

1. Adopting a risk management framework

The first step in ensuring a risk-based approach is adopting a risk management framework (RMF). NIST has developed several publications to assist agencies in implementing a consistent approach and ensuring they mature as needs evolve. FIPS PUB 199 offers guidance on categorizing systems based on criticality and impact. Based on this categorization and identification of high valued assets (HVAs), agencies can select the controls defined in the NIST 800-53 publication. Once controls are selected, NIST 800-37 offers guidance on implementing a risk management lifecycle. To further guide agencies on bridging the gap between selecting controls and implementing them along the risk management framework, NIST has developed the Cyber Security Framework (CSF), which is now mandated by the President's Security Executive Order. This approach is essential for a robust foundation and ensuring cyber hygiene.

2. Central log management and compliance

Once controls are selected and implemented it is important to monitor them, as part of the risk management approach, on a continuous basis. Take for example the FISMA compliance framework and its supporting standards. FISMA must by law be followed by all executive- and legislative-branch agencies including the DoD. Within this framework, any deviations can be noticed and corrective action taken to ensure compliance. This requires data from all the relevant systems to be brought together to be measured against the controls being monitored. With silos of data and operations and heterogenous systems across the agency, this can be a tedious task and an activity that has proven to be time-consuming, error prone and costly. The practical solution is to automate the log data collection process and ingest them in real-time, bringing them together in one place for correlation and analysis. This gives information

assurance managers granular visibility, on adherence to controls. Additionally, the end-to-end visibility provides hard to find real-time insights like hidden patters or statistical outliers. Staff across the stack, from operators to executives can have views into the metrics based on their needs. Self-reporting to auditors eases the audit burden making it painless.

3. Security Investigation and Incident Response (IR)

By aggregating logs in one place, agencies now have end-to-end visibility into what is transpiring across the organization. With this strong foundation in place, security staff can enrich their investigations with contextual enrichment sources such as threat intelligence and other data, to support the processes and activities associated with investigating, containing and remediating the full extent of an incident or breach. This allows security teams to better minimize attack damage by managing security incidents, leveraging information uncovered in real-time during scoping and investigation to make informed decisions on how best to contain and reduce or even eliminate impact. Adding context helps cut down irrelevant alerts and helps prioritize the most critical issues for investigation, in turn enabling security analysts to respond to incidents faster. With an end-to-end view, pinpointing root cause is quicker and more accurate, helping minimize damage in case of an incident.

4. Proactive security and threat hunting

End-to-end visibility into the agency, in real-time, enables security staff to hunt for threats. And once incident management processes are operationalized, these can be applied to not only respond to incidents, but to proactively search for anomalous behavior and any unusual, potentially suspicious activity. Formal and standardized threat hunting processes can be implemented—to develop specific hypotheses based on diverse sets of events and other activity occurring in the environment. Supplemented buy machine learning algorithms, these processes help identify specific changes in user or device behaviors that could indicate a breach or other high severity issue. Applying this methodology, security teams can glean insights quickly to understand intent, quickly and confidently disrupt attackers from meeting their objectives, and develop threat actor profiles over time, to better understand the adversaries they are facing.

Industry Spotlight: Toward an Analytics-Driven Security Operations Model

An interview with Jae Lee, Product Marketing Director, Security Markets, and John Stoner, Security Strategist for Splunk Public Sector

The reality today is that adopting an analytics-driven approach to security does not require a massive investment and forklift "re-do." Rather, it can be as straightforward as rethinking the overall approach and aligning to trends in how security operations are evolving across the industry.

To understand how and why this is important in government, GovLoop sat down with Jae Lee, Product Marketing Director, Security Markets, Splunk, and John Stoner, Security Strategist for Splunk Public Sector.

Stoner said that today's government faces challenges unlike any era before. "Everything around cybersecurity is more complex today—there's bigger threat surfaces and more complicated attacks," he said. "And there are more mandates and cyber-hygiene requirements to keep up with, too."

Additionally, many legacy security technologies and approaches by themselves are only telling one piece of the story with the rate and sophistication of modern-day threats. Government IT professionals can still fall prey to old-fashioned approaches and a mentality of "set it and forget it," which doesn't take a proactive approach to discovering cyberthreats. Finally, IT departments are often beset with such a variety of tools that they're overwhelmed.

"The main obstacle government is often facing is not that they don't have the right tools," Lee said. "It's that they can't get context and insight from all those different tools quickly enough and all in one place to perform an efficient investigation."

This is a primary reason why adopting an analytics-driven security approach can help improve security, cyber hygiene and compliance. Threat detection, monitoring, incident investigation and response and forensic analysis can all be greatly accelerated and enhanced as a result.

"An analytics-driven approach to security enables better prioritization, handling, and response of the most critical threats, faster resolution of threats, regardless of the size of the security team, and longer-term, the ability for that team to grow, adapt, and standardize the operational aspects of handling and remediating security incidents," Lee said.

Today's security operations are evolving to be ever more proactive and nimble. A traditional SOC is more "tiered," meaning there are traditional escalation paths and very specific capabilities per each tier, and most tasks are handled via a specific set of procedural guidelines that encompass a combination of different monitoring, investigative, and other tools.

The current trend in security operations is moving toward a combination of virtual, managed services, multi-tiered approaches, and more lightweight teams or "crews" who respond to an incident in a more agile manner.

In order to accomplish this level of agility, security architectures—including the "landfill" of multi-vendor security architectures—must somehow work together. The multi-layered defense consists of many layers of tools and products, leaving gaps in how security teams bridge multiple domains.

A modern and evolving security operations model must take an analytics-driven approach to cybersecurity if it hopes to keep pace with the evolving threat landscape. For security operations, advanced analytics is the foundation that enables capabilities such as threat and vulnerability management, incident prioritization, advanced threat detection, and threat hunting and investigating.

"With an analytics-driven approach you can build a stronger security posture and improve cross-department collaboration," Stoner said.

Another key advantage can come in the form of implementing an adaptive approach to security. An adaptive security architecture can enhance the ability to prevent, detect, respond and even predict threats—at machine speeds. By proactively gathering additional insights, including enrichment from threat intelligence feeds and security teams can more effectively minimize risk, quickly detect and respond to internal and external attacks, simplify threat management, and gain continuous organization-wide visibility.

"Splunk solutions can also improve accuracy for even the most complex security problems with the advanced use of machine learning. It provides security analysts a way to stay ahead of and more quickly respond to cyberattacks and insider threats," Lee said.

"Security is not about a silver bullet," he concluded. "This has never been truer than today. You just don't throw technology at it and say it's secure. It's about deriving insights and establishing a codified way to handle issues, knowing what's happening and the associated risks, and over time working toward a more proactive stance. And when you can do that, you'll be better prepared to evolve and adapt with the threat landscape."

Splunk for Analytics-Driven Security

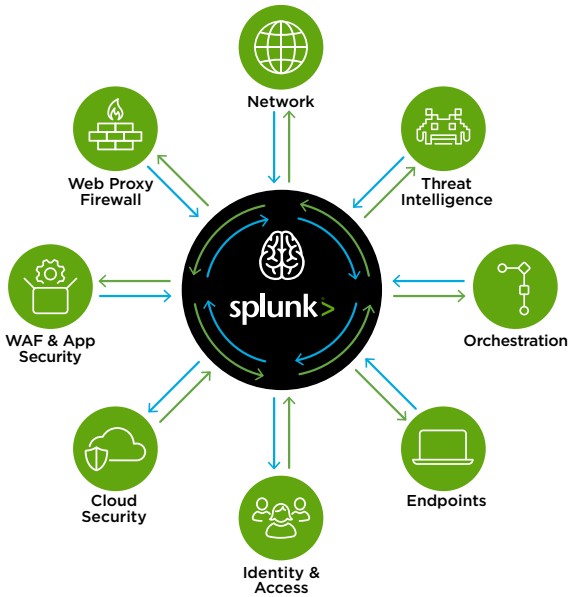
Splunk helps security teams navigate unchartered waters and quickly identify, investigate, respond and adapt to threats in dynamic, digital environments.

Splunk security solutions provide valuable context and visual insights to help security teams make faster and smarter security decisions. Security teams in government agencies use Splunk software to:

- better protect their most critical assets
- improve security posture and reduce false positives
- anticipate the unknown within the rapidly changing threat landscape

5 WAYS TO USE SPLUNK FOR CYBERTHREAT ANALYSIS

1. Perform research on adversarial threats posed to systems, operations and missions
2. Analyze collected data to derive facts, inferences and projections concerning attacks
3. Use content to more accurately determine false-positives and false-negatives
4. Identify attackers by piecing together snippets of abnormal behavior spread over time and across systems
5. Contribute to profiling adversarial behavior



Toward the "Security Nerve Center"

By bringing multiple IT areas together, Splunk software enables collaboration and efficient implementation of security best practices—including how security teams interact with data and automate actions to address modern cyber threat challenges. With Splunk as the "security nerve center", teams can optimize people, process and technology. Security teams can leverage statistical, visual, behavioral and exploratory analytics to drive insights, decisions and actions.

Learning From Others: Advanced Security Investigations Case Studies

Now that you've learned the basics of advanced security investigations, here are three examples of it in action to inspire you and help you build a case for it at your organization.

CASE STUDY 1: Fairfax County Protects Citizen Data

Fairfax County, Va., a stone's throw away from the nation's capital, employs 12,000 people across more than 50 agencies and serves more than 1.1 million citizens. Its government is regarded as a leader in cybersecurity and IT, enabling it to serve the needs and protect the data of its IT-savvy and high-profile citizens.

Challenge: More than 200 IT professionals support more than 50 county agencies, each with unique business and security requirements, said Mike Dent, chief information security officer (CISO) for Fairfax County. In the past, one of the major challenges Dent and his team faced was centered on the numerous disparate systems from which it had to pull event logs. What's more, its previous SIEM tool could not keep up with the more than 3.9 petabytes of data the county must control, access and secure.

Solution: Fairfax County turned to Splunk's Operational Intelligence and sees benefits in several key ways, including elasticity, security and scalability, without the operational effort. Dent said that the county is also enjoying cost savings from a hardware perspective because there is a smaller data center footprint. What's more, only one individual is required to manage the Splunk implementation, which enables the county to maximize its resources. "Previously, reporting to leadership was difficult because everything was manual. My staff would spend countless hours, probably two weeks' worth of work, to get me a summary report of our cybersecurity stance," Dent said. "Now, with the Splunk platform, I have real-time access and can give an overall security posture to my leadership to let them know when we have issues."

"My top priority is to protect the citizens' data. Making sure that these citizens can trust the government they have with the data that they have entrusted us with is our mission."

— Mike Dent, CISO Fairfax County, Va.

CASE STUDY 2: Better SIEM at a Federal Agency

Many organizations depend on security information and event management (SIEM) software to monitor, investigate and respond to security threats. But at one U.S. government agency, its mission was hampered when its legacy SIEM software failed to live up to expectations. The agency turned to InfoTeK, a leading cybersecurity, software and systems engineering firm that partners with Splunk, to replace its SIEM tool.

Challenge: This particular federal agency was finding that it was too difficult to glean actionable intelligence about threats. Identifying anomalies that could indicate vulnerabilities or an attack in progress required seasoned security engineering skills—and even for those who had them, it was a time-consuming puzzle. Gaining insight wasn't the only issue: As the volumes of data that needed to be searched and analyzed grew considerably, its legacy SIEM simply couldn't keep pace. Scaling performance meant more hardware and more expense.

Solution: With Splunk Enterprise and Splunk Enterprise Security (ES), the agency has an analytics-driven SIEM that provides the IT team with actionable security intelligence at an affordable cost. InfoTeK deployed Splunk software over one weekend for the customer. Starting the very next day, the software proved its value. The IT team was able to search security events and immediately thwarted an attack vector. "Something that used to take hours, days or even weeks with other products or jumping between multiple tools can be done in seconds, minutes or hours with Splunk," said Jonathan Fair, senior incident handler and security engineer at InfoTeK. "We were able to provide a ROI before the product was even fully purchased because the customer successfully stopped a threat that would have required a complete rebuild of the network."

"Splunk truly stretches across all data, and you can search across any data set at any time. An expanded view is necessary to truly look at an event, either in real time or for post-mortem analysis."

— Jonathan Fair, senior incident handler and security engineer at InfoTeK

CASE STUDY 3: Los Angeles Integrates Real-Time Security Intelligence Sharing

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.

Challenge: Los Angeles is a vast metropolis with critical infrastructure like airports, seaports, water and power, as well as 35,000 employees and over 100,000 endpoints generating 14 million security events daily. Its departments had their own security tools, requiring the city to gather and manually correlate logs from each agency for broad views of its network security. This process was cumbersome, imprecise and slow to address threats. "Our mayor issued an executive directive to improve cybersecurity," said Timothy Lee, chief information security officer for Los Angeles. "This meant collecting and evaluating all of our logs in real time. We needed a scalable SIEM to drive an integrated, citywide security operations center (SOC)." Mindful of the city's budget, Lee wanted a cloud-based SIEM to avoid the administrative burdens of onsite platforms.

Solution: Splunk Cloud provides Los Angeles with holistic views of its security posture. Splunk forwarders send raw logs and other data from the city's departments to Splunk Cloud, where they are normalized and returned to the integrated SOC, and then analyzed and visualized in Splunk dashboards. Using pre-built, easily customizable dashboards in Splunk ES, executives and analysts have always-available, real-time situational awareness of security events across the city's networking infrastructure. With all security data in one continuously updated database, Lee's team views and compares any machine-generated data, including disparate logs and both structured and unstructured data, to extract all-inclusive, actionable security intelligence.

"Our Splunk SIEM is like having video cameras on every block; it provides visibility into what's happening on the network, which is foundational to safety."

— Timothy Lee, chief information security officer for Los Angeles

Cheat Sheet: Analytics-Driven Security

This takeaway section gives brief tips and questions to help you think about your journey toward analytics-driven security.

5 STARTER QUESTIONS TO HELP YOU PREPARE TO ADOPT AN ANALYTICS-DRIVEN APPROACH TO SECURITY

1. Has your organization prioritized the task of inventorying and classifying the highest-priority assets in your environment?
2. Are you able to triage priority alerts in an efficient and effective manner, with adequate context to verify that an issue needs to be investigated further?
3. Is your security team making headway in demonstrating compliance to key mandates, and putting a cyber-hygiene policy in place—one that evolves and does not require a massive lift with each audit, report, or iteration of a mandate?
4. Are your security teams able to investigate quickly, in an ad-hoc manner when needed, and feel confident that remediation steps will help improve overall security posture?
5. Does your security process allow for more?

An analytics-driven approach to security can help government agencies more effectively deal with complex, sophisticated attacks and evolve along with the cyberthreat landscape.

Key Mandates to Start With

Once the security operations team has established reliable central logging, they can take advantage of that foundation to implement cyber hygiene and follow NIST guidance for compliance mandates. Three NIST publications are especially noteworthy.

Federal Information Processing Standards (FIPS) Publication 800-199 – Standards for Security Categorization of Federal Information and Information Systems

This publication establishes security categories for both information and information systems, based on the potential impact a breach other intrusion could cause to an agency's ability to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

Special Publication 800-53 – Recommended Security Controls for Federal Information Systems and Organizations

This publication provides a catalog of security and privacy controls for organizations, as well as a process for selecting controls to protect organizational operations, organizational assets, individuals, other organizations, and the United States from a diverse set of threats including hostile cyberattacks, natural disasters, structural failures, and human errors (both intentional and unintentional).

Special Publication 800-37 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach

This publication provides guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.