SPONSORED CONTENT

CSO
FROM IDG

4 STEPS TO GOVERNMENT SECURITY:

INVESTIGATE, MONITOR, ANALYZE, ACT

IDG Communications, Inc.

splunk>

With the right strategy and mindset, organizations can turn a sea of chaotic security data into an asset and manage risk by continuously advancing their ability to detect, investigate and respond to threats in a pragmatic manner.

SEVERAL GOVERNMENT AGENCIES FIND THEMSELVES DROWNING IN AN OCEAN OF SECURITY ALERTS, WHILE LACKING THE CAPACITY TO EFFECTIVELY IDENTIFY AND PRIORITIZE THE CRITICAL ONES.

Cybersecurity professionals at government agencies face largely the same challenges, and share many of the same needs, as their commercial counterparts. The public sector security pros, however, must often deal with complicating factors that make their jobs especially difficult. Those factors — ranging from strict compliance mandates to budget uncertainties to staff shortages and skills gaps — arguably place government cybersecurity challenges in a class of their own.

For many cyber attackers, government agencies also make for especially attractive targets — these organizations hold lots of sensitive and valuable data, be it social security numbers, medical records, or military and diplomatic secrets. A more fundamental motivator for many attackers: they know their efforts to compromise government systems will likely prove worthwhile given the nature and value of the assets they are after.

The good news is that security-relevant data can provide key insights that help agencies with their security and risk management initiatives. In a way, all data is security-relevant, and can be found across the agency, including specialized security systems and controls, application and equipment logs, network traffic, physical security systems, and many other sources.

The problem, of course — and one that challenges security professionals working in every commercial and public sector — isn't a lack of security-relevant data. It's having the right synchronization of people, processes, and technology necessary to make sense of it all and act upon any findings.

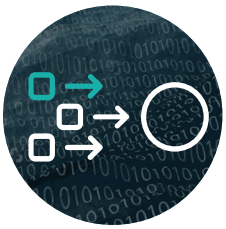
Several government agencies find themselves drowning in an ocean of security alerts, while lacking the capacity to effectively identify and prioritize the critical ones. This situation makes it difficult, if not impossible, to make fast, confident, and proactive decisions on how best to respond to threats, improve security posture, and manage risk overall — and to execute responses at speeds the mission demands.

Therefore, many agencies are adopting a risk-based approach, enabled by an analytics-driven foundation for security operations. This approach connects security teams with the right data and context at the right time to enable timely, objective analysis and decisions. As a result, security teams are able to more confidently manage risk.

An analytics-driven approach is based on the following design objectives:

- **Enable an agency-wide investigative methodology** based on centralized collection and enrichment of any and all security-relevant data
- **Show contextualized, priority security issues** based on a set of key metrics that include correlated, verified indicators across multiple IT domains
- **Drive fast, accurate analyses at scale,** regardless of data or incident volume, to support real-time incident and breach scoping, forensic analysis, threat hunting, and adversary profiling
- **Implement a set of standard procedures for security operations across the agency** that incorporate playbook-centric collaborative workflows as well as orchestrated, automated containment and remediation capabilities

Achieving these objectives doesn't happen overnight for government entities. But getting there can be accelerated by taking a pragmatic approach along four simplified stages of a data-centric security maturity curve. Those stages:



1. INVESTIGATE — establish an investigative data platform, and ask questions of that data

2. MONITOR — gain real-time situational awareness of risk posture through continuous monitoring

3. ANALYZE — enable machine learning (ML) and artificial intelligence (AI) for deeper analysis and proactive threat hunting

4. ACT — automate tasks and orchestrate workflows for fast response and countering threats

A primary challenge for many government agencies is their ability to understand where they stand in terms of these stages, as well as how prepared they are to adapt to an evolving threat landscape and a dynamic and often conflicting set of mission demands.

Government Cybersecurity at a Crossroads

The cyber attacks leveled at government agencies aren't inherently distinct from those made against enterprises and small-to-medium-sized businesses. Regardless of their industry sector or organization size, security professionals must be able to mitigate distributed denial of service attacks, insider threats, phishing and ransomware campaigns, advanced persistent threats, and a host of other threat activities.

Like their commercial brethren, government agencies have deployed a growing collection of security tools, systems, and services to mitigate these threats. This strategy aims to provide the broad coverage critical to a sound, multilayered defense, but most tools are not designed to work easily or well together. Too often, the result is an ad hoc, uncoordinated, and often manual security operation.

THE DEMAND FOR SECURITY PROFESSIONALS IS FAR OUTSTRIPPING THE SUPPLY, WHICH WILL RESULT IN 3.5 MILLION UNFILLED CYBERSECURITY JOBS BY 2021.

Source:
Cybersecurity Ventures

Even with formalized teams and processes, there is the challenge of maintaining skill levels. In addition to retaining skilled staff, agencies must help their teams relearn syntax and workflows associated with new technologies, as stack components and vendors get replaced or upgraded. This need can make it difficult to fully exploit new technical capabilities in a timely and effective manner.

One of the reasons for the distinct challenges government agencies face is tied to their IT and security budgets and resources. For example, in a recent survey[1] of more than 660 IT, security, and business decision makers, IDG Research found that 60% of the enterprise respondents expected their security budgets to increase over the following 12 months. By comparison, just 46% of the government respondents expected budget increases.

Intertwined with the budget issues is security staffing — a pain point for virtually every type of organization. The demand for security professionals is far outstripping the supply, which will result in 3.5 million unfilled cybersecurity jobs by 2021, Cybersecurity Ventures predicts.[2]

While an industry-wide problem, the security skills gap often hits government agencies especially hard. In today's competitive job environment, it can be challenging for agencies to retain highly skilled security experts when they are being lured by many more lucrative opportunities in the commercial sector.

Perhaps in a reflection of this reality, government agencies tend to rely much more heavily than private companies on contract security workers. When the IDG Research study asked respondents about their security hiring plans for the coming year, 37% of all respondents said they would be increasing their number of full-time equivalents. Among the subset of government respondents, only 26% said the same.

At the same time, 35% of the government respondents said they would be adding to their roles of outsourced and contract employees, compared to just 26% of the full survey base saying so. While contract employees may be highly skilled, it can be costly and ineffective for government agencies to establish and maintain security operations centers (SOCs) if they're unable to reach peak efficacy due to turnover.

How can often-lean government security teams, faced with multiple compliance mandates, not only detect out-of-compliance situations, but establish and implement repeatable methodologies to correct them?

One solution that has proven to work is for authorities at all government levels to adopt a data-driven, risk-based approach to help their departments and agencies build better cybersecurity defenses and protect their high value assets (HVAs). A good starting point for this approach is for agencies to make use of various federal guidelines, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the NIST Special Publication 800-series.[3]

Providing government agencies with these and other types of security guidance and best practices is an important and necessary foundation on which to improve their security postures. But, even with this type of assistance, government security professionals can better manage risk by taking a pragmatic approach along the four stages of the security maturity curve.

[1] Source: 2018 Security Priorities Survey (government callout version), slide 19

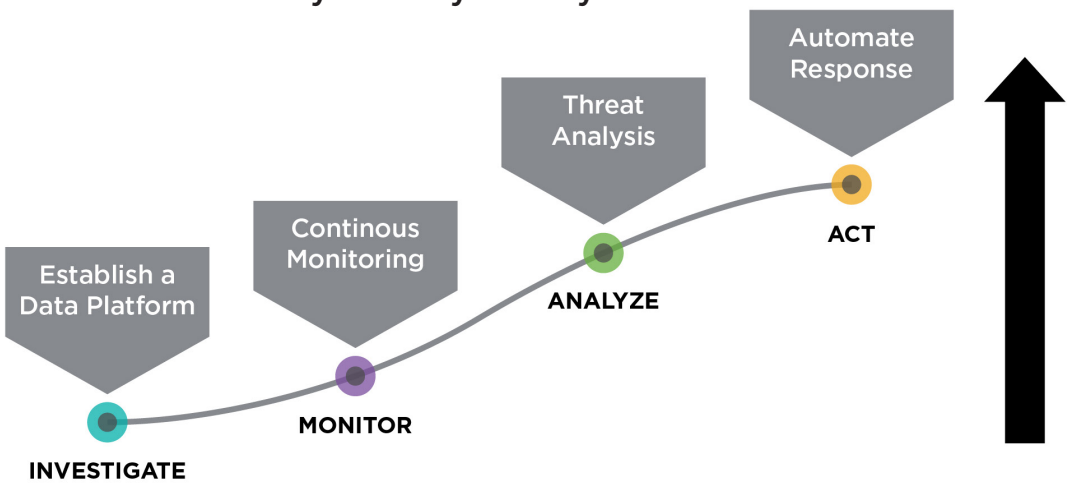
[2] Source: https://cybersecurityventures.com/jobs/

[3] https://www.nist.gov/itl/nist-special-publication-800-series-general-information

Finding Your Place on the Security Maturity Curve

To tackle the cyber threats they face and make sense of the massive volumes of security-associated data available to them, government agencies can follow a step-by-step journey along a four-stage maturity curve. They first need to determine their current position on the curve, and then move toward more secure operations. As noted earlier, the four stages are Investigate, Monitor, Analyze, and Act. More precisely, these stages are instantiated with the methods illustrated in Figure 1.

FIGURE 1. **The Security Maturity Journey**



Let's examine the elements of each maturity curve stage

INVESTIGATE

ESTABLISHING A DATA PLATFORM

As a starting point to an analytics-driven cybersecurity strategy, security professionals are often at a loss to determine which data they need, and which data their systems are able to ingest. When it comes to security, all data is security-relevant.

In today's digitally infused world, this includes data from any pertinent source including endpoints and servers, network routers, databases, cloud-based services, Internet of Things (IoT) devices, security tools, applications, and many other data sources (see "Tapping Data" box). Usually heterogenous and in silos, when brought together data can provide end-to-end visibility across a distributed IT environment.

The challenge facing many organizations — especially those with limited security staff and budget — is one of collecting, normalizing, and aggregating all of this diverse data in a single place. Building data models to accomplish these complex tasks is a skill beyond the reach of most organizations, government or otherwise. What's needed is an off-the-shelf data platform that can perform these functions with minimal IT effort.

The foundation of leveraging this data is the ability to ask questions and refine those questions in real-time. Such investigation is fundamental in security analysis. One of the main tasks of the security analyst is to figure out "what happened & why?"

MONITOR

CONTINUOUS MONITORING

An organization's risk posture is not a constant. Attacks are automated, system configurations change regularly, and updates to mission requirements can result in increased complexity in attack surface. Taking periodic snapshots of data, even if it's a wide-angle picture of data from many diverse sources, isn't a strategy for success in the dynamic, ever-changing security space.

To counter dynamic risk, organizations require systems that can continually monitor all relevant data streams and sources, and contextually enrich risk profiles in real-time to inform the organization of exposure. It's worth noting that continuous monitoring of this sort requires the ability to absorb and manage huge volumes of data. Only in this way, however, can IT and security managers obtain real-time situational awareness of what's happening across their organizations.

Especially important for government agencies: continuous monitoring is the only way to ensure that they're meeting the many compliance mandates under which they operate. If an agency's compliance posture begins to drift, the security team will know immediately, and can proactively respond to the situation.

ANALYZE

ANALYZING THREATS

Once the data platform and continuous monitoring regime are established, organizations can move to this stage of the security maturity curve. It's here that security teams and their systems seek to identify advanced threats, suspicious traffic patterns, anomalous activity that deviates from established baselines, and other threat indicators.

Technologies such as ML and AI can be leveraged for deep analysis of massive datasets to discover anomalies, hidden patterns, and future trends. Petabytes of data are now an asset instead of a roadblock — helping you gain a deeper understanding of your risk posture and how your organization operates.

A key objective at this stage is to bring only true cyber threats to the attention of security analysts to minimize the blizzard of false positives that can cause alert fatigue. Importantly, because this analysis is data-driven and therefore objective, analysts can have a high degree of confidence in the fidelity of an alert.

ACT

AUTOMATING RESPONSES (AND OTHER PROCESSES)

This fourth stage of the security maturity curve encompasses not just the automation of incident responses to breaches, but also the automation of other security processes and repetitive tasks. Automation, in fact, is an integral element of each maturity stage, given that the volumes and speeds involved in data collection, monitoring, and analysis long ago surpassed the abilities of people to keep pace unassisted.

Nowadays, automation is a requirement, not an option, for organizations that want to effectively counter threats once identified, or to minimize damage should an attack get through. With the ability of some malware to infect connected systems at blinding speeds, organizations need highly reliable systems that can shut down an infected server instantly once the threat is spotted. It goes without saying that security teams must have a high degree of confidence before letting an automated response system take a critical server offline.

WITH MANUALLY INTENSIVE TASKS AUTOMATED, ANALYSTS AND OTHER SECURITY STAFF CAN FOCUS ON HIGHER-VALUE TASKS AND STRATEGIC ANALYSES.

Automation that removes repetitive manual tasks from security analysts' shoulders may seem a less compelling application, but it can deliver significant benefits. With manually intensive tasks automated, analysts and other security staff can focus on higher-value tasks and strategic analyses.

Automation can also deliver something that many security teams typically have difficulty measuring — the return on investment (ROI) of security investments. Comparing the time requirements and efficiencies of manual security processes and tasks with the same processes once automated can produce quantifiable and impressive improvements. Documenting these benefits can help IT and security professionals justify spend.

As is true of every aspect of security — and each stage of the maturity model — security teams never reach an "end point" at which further improvement is impossible. In later stages of automation, for instance, discrete activities that have been automated will be orchestrated with one another into end-to-end processes. Ideally, security solutions in this space will deliver best-practice, out-of-the-box automations, while also giving organizations the ability to automate their own custom security processes .

SPLUNK AS A SECURITY PARTNER

The value and capabilities that Splunk brings to the table are built on a broad and diverse data foundation. Splunk's highly scalable portfolio of solutions — Splunk Cloud, Splunk Enterprise, Splunk Enterprise Security, Splunk User Behavior Analytics and Splunk Phantom — deliver end-to-end capabilities from detection to investigation to response.

With Splunk, security teams can efficiently minimize risk and avoid damage – Splunk enables security teams to collect and analyze any data, gain valuable security insights, investigate and prioritize quickly and accurately, and take remediation steps across their entire security architecture with confidence.

In the cybersecurity realm, these capabilities can be applied to address the entire cyber risk management lifecycle and its many discrete elements. That includes everything from security monitoring to advanced threat detection to incident response.

Splunk's ability to help organizations harness the full value of their data has won it thousands of customers around the world, including 90 of the Fortune 100 corporations. In the public sector, Splunk solutions are deployed within all three branches of the federal government, in all 15 cabinet-level departments, all four branches of the military, and within many state and local government offices. It is the security standard in more than 13 U.S. states.

SPLUNK GOVERNMENT CUSTOMERS INCLUDE:

THE CITY OF LOS ANGELES encompasses a broad infrastructure with more than 100,000 endpoints generating 14 million security events daily. Each city department had its own security tools, so the city had to manually gather and correlate logs from each agency to get a comprehensive view of its security status. LA deployed Splunk Cloud as its security information and event management (SIEM) solution, chosen not only for its out-of-the-box capabilities but also for its flexible customization options. The city is now able to share threat intelligence. Since deploying the solution, the city has been able to create a citywide SOC, share real-time threat intelligence among its various agencies — as well as with local and federal law enforcement agencies — and reduce operational costs.

"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, CISO, City of Los Angeles

THE STATE OF ALASKA faced a budget deficit due to falling revenues. That left the state's security team — consisting of just seven people and with vacant positions that would remain unfilled — in a tough spot. It turned to Splunk Enterprise, which was able to ingest log data from security devices, network devices, and other endpoints, catalog that data, and present it on dashboards that allowed the security team to immediately glean intelligence from it. The solution also serves as the underpinning for the many compliance and regulatory mandates that the security team must follow.

"WE REALLY NEED TO FOCUS ON BEING LEAN WITH THE TOOLS THAT WE HAVE, AND SPLUNK ENTERPRISE ALLOWS US TO DO THAT."

— Chris Letterman, CISO, State of Alaska

ONE LARGE U.S. CABINET-LEVEL DEPARTMENT includes 40 agencies that count 130,000 users and upwards of 200,000 hosts under its umbrella. The department was hampered by a legacy SIEM system that was expensive, slow, and unable to provide the straightforward and comprehensive log analysis required for security compliance. After replacing the legacy SIEM with Splunk Enterprise, the productivity of the 40 analysts in the department's SOC is greatly improved. Instead of spending 4-6 hours each week pouring through data logs, for example, the analysts now load a dashboard once a week to take a quick look for anomalies. By replacing the older system with Splunk Enterprise, the cabinet department is also saving $900,000 per year in maintenance costs.

A U.S. FEDERAL AGENCY TURNED TO INFOTEK, a consulting and systems integration firm, to help it overcome limitations of its existing SIEM solution. The legacy solution struggled to accommodate massive data sets, required costly hardware and engineering support, and was slow to identify and mitigate threats. In just one weekend, InfoTek installed Splunk Enterprise and Splunk Enterprise Security, and the software provided immediate ROI during its first day of operation by stopping a serious threat that could have forced a complete network rebuild. Thanks to its reduced hardware and management demands, the Splunk solution reduced costs by 75% compared to the prior solution.

"SPLUNK IS THE ONLY PRODUCT THAT WE HAVE FOUND THAT HAS BEEN ABLE TO TRULY TAKE ANY DATA SOURCE AND GO TO SCALE."

— Jonathan Fair, Senior Incident Handler and Security Engineer, InfoTek

Whether cloud, on-premises or for large or small teams, Splunk has a deployment model that will fit your needs: learn more now. Or if you are ready to try Splunk for yourself, download Splunk Free.