Gaining the SITUATIONAL AWARENESS *needed to* MITIGATE CYBERTHREATS

splunk>

Industry Perspective

EXECUTIVE SUMMARY

To become more resilient against cyberthreats, agencies must improve visibility and understand events happening on their networks. With increased awareness, organizations will see operational benefits and save employees valuable time, improving productivity and morale.

To achieve these benefits, agencies need to deploy the right kind of infrastructure. They must look to a platform approach and be able to connect disparate data to gain the desired network visibility. Only by understanding data, and having a complete operational view of organizational data, can agencies improve their security posture.

In this industry perspective, GovLoop explores how Splunk, an operational intelligence platform and industry leader in government security, helps government agencies find value from their data to reduce the impact of cyber incidents.

Specifically, this report will:

- **Outline the challenges cybersecurity professionals in government face.**
- **Address the value of Splunk's holistic and data-analysis-based approach.**
- **Share a case study from the Nevada Department of Transportation.**
- **Provide best practices from industry expert Enoch Long, Public-Sector Principal Security Strategist/Client Architect at Splunk.**

Agencies need a cyber infrastructure that allows them to collaborate across teams and bring together all units to understand the role they play in crafting a more resilient and secure agency. This means capitalizing on any data, including that from log files, internal network devices and access points, that is relevant to keep an agency secure.

For government today, there is no challenge greater than cybersecurity. Our national security and way of life depend on safe, secure and robust cyber defense. But the unfortunate reality is that even with world-class technology, attacks and breaches are inevitable.

The Challenges of Cybersecurity

Cyber professionals face many challenges in mitigating cybersecurity threats. It's about more than having access to the latest information technology solution.

"One challenge is filling the high demand for cybersecurity personnel," Enoch Long, Public-Sector Principal Security Strategist/ Client Architect at Splunk said.

The cybersecurity community needs to reform the way it trains, recruits and retains the next generation of security professionals. Part of that process involves agencies having world-class IT infrastructure and deploying cutting-edge technologies. This will attract top talent, who can use the best tools and solutions to work toward protecting America's critical infrastructure.

But building the cyber workforce isn't the only challenge. Agencies also need to look at existing technology silos, because far too often cyber defense technology is focused only on point security solutions.

"From a technology standpoint, another challenge is that agencies often have dozens of different cyber technologies, all with their own specific silos. Agencies must learn how to combine those solutions so their personnel do not feel overwhelmed managing numerous different technologies," Long said.

"That's where Splunk can help a government agency," Long added. "Splunk is able to come in and give an overall situational analysis and help analysts, engineers, administrators, chief security officers and chief information officers feel more comfortable with the security of their entire technology portfolio."

A third challenge for cyber professionals is figuring out which is the most important data to collect, then accessing the data across departments — without inciting a turf war. Overcoming this obstacle is one of the most critical steps in improving an agency's cybersecurity posture, because a strong cyber defense first requires a keen understanding of an agency's data.

Long said that this understanding involves first being aware of what specific data is relevant for your security needs — then understanding if it is available and where it lives. "That is what agencies must focus on," Long said. "So even before you can protect data, you need to understand the relevance and importance of it."

"If you have all your personally identifiable data in a shared server and all revenue reports in another area, that's how you can start to put indirect blocks and keys on data, and then can understand where data is located to secure it," he said.

For security professionals, prioritizing data is not only important from a security perspective, it also provides clarity and improved network situational awareness.

Still, understanding your data can be tough, especially as the idea of a security perimeter evolves. Today, the perimeter can be anything that connects to the Internet and has access to agency resources. That includes enterprise devices or anything accessing information behind a firewall, such as phones, laptop computers, workstations, servers or data centers.

"When you talk about a security perimeter for a government agency, it starts with the employees and the multitude of devices accessing your network," Long said.

AS THE SECURITY PERIMETER CONTINUES TO GROW, ORGANIZATIONS MUST FOCUS ON WAYS TO GAIN MORE VISIBILITY INTO THEIR NETWORK. THEY MUST DEPLOY A PLATFORM APPROACH, HELPING THEM GARNER IMPROVED VISIBILITY, INCREASE SITUATIONAL AWARENESS AND SPOT ABNORMALITIES ON THE NETWORK TO IMMEDIATELY THWART ATTACKS.

This is where Splunk's real-time, analysis-based approach to cybersecurity becomes indispensible for protecting a network.

The Splunk Approach: A Real-Time 'Lens' into Your Data

Splunk offers the public sector the needed relief to mitigate cyberattacks via a holistic approach. The process involves fusing together datasets to provide a universal view of information across an agency. With this universal approach to data and threats, organizations can find new insights, patterns and trends that were previously unknown or that could be identified only through time-intensive and laborious processes.

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, visualizations and alerting capabilities. The product allows you to ask scenario-based questions in real time and to create shareable reports based on your discoveries.

Then, running on top of the core Splunk Enterprise platform, the Splunk App for Enterprise Security supports traditional security information and event management (SIEM) capabilities, watching for known threats and monitoring key security metrics. The app operates as a 'lens' into your security data. It organizes data into specific security domains while collecting data from traditional security architectures automatically, delivering real-time dashboard visualizations. Additionally it includes incident workflow management, predictive analytics, network protocol analysis and correlation and security logic development for your more advanced security analysts. The solution is designed to directly align to today's threats — online, slow and low attacks, and command and control communication.

"It's important to understand that our technology and our specific approach helps fuse everything together, because you have different personnel, different job titles, and different management structures," Long said.

"From my background as a security operations center (SOC) manager, it was very challenging to get the IT infrastructure managers, engineers and the admins to understand the need to share their data," he added. "But we're seeing government agencies start to be more receptive to having a technology that brings all data into the security fold."

A former federal contractor, Long is well versed in the challenges and obstacles that security officers face. During his time in the public sector, he was a Splunk customer and learned firsthand how the company's approach comes into practice.

"When I was a Splunk customer, one of the key challenges that I had as a security operations center (SOC) manager was that we didn't have enough personnel and security analysts for our third shift," Long said. "A lot of people don't want to work 11 [p.m.] to 7 a.m. With families and other obligations, it's tough to get top talent for that night shift."

What Long had to do was get more productivity out of the analyst working the late-night shift. That's when he decided to bring in Splunk to help consolidate data, build metrics reports and save his employees time.

"I decided to test if I could shift some of the day-to-day duties and operations of the late-shift to Splunk technology," Long said. "We tested metrics reporting and basic maintenance, hoping to pass this process over to the technology. We were able to create certain dashboards, reports, security logic and analytics, all pre-built by Splunk Enterprise, and schedule times for reports."

"So when the first shift comes in, they are getting a report handed over to them from Splunk technology, just as if it was coming from an analyst," he added. "We were able to leverage the technology as if it were two or three analysts."

Long's case study is a great testament to the power of Splunk and what organizations can do with it. Another exceptional use case comes from the state of Nevada.

"WE TESTED METRICS REPORTING AND BASIC MAINTENANCE, HOPING TO PASS THIS PROCESS OVER TO THE TECHNOLOGY. WE WERE ABLE TO CREATE CERTAIN DASHBOARDS, REPORTS, SECURITY LOGIC AND ANALYTICS, ALL PRE-BUILT BY SPLUNK ENTERPRISE, AND SCHEDULE TIMES FOR REPORTS."

— Enoch Long, Public-Sector Principal Security Strategist/Client Architect at Splunk

Will Keightley, CC BY-SA 2.0

Lessons Learned from the Nevada Department of Transportation

Splunk helps dozens of agencies combat cyberthreats. Here's how the **Nevada Department of Transportation (NDOT)** uses it.

Since 1917, NDOT has maintained, planned, constructed and operated the state's highway system. Located in Carson City, the division employs more than 2,000 professionals and is responsible for more than 5,400 miles of highway and more than 1,000 bridges. Additionally, NDOT administers the state's 511 system, which enables citizens to report and access information on delays, road closures and construction. NDOT also runs a statewide camera system that gives real-time feeds so people can check traffic levels prior to traveling.

Tasked with such an important mission, the department has huge amounts of critical data that it must protect. When an NDOT security official recently became worried the data was not properly protected, the department began to take preventive steps.

First, the division audited its system by attempting to hack into its own data to obtain documents. This allowed officials to assess network vulnerabilities and security gaps. And once they got in, they found that it was a very tedious process to understand how the attack occurred. The team had to sift through system logs, relying on a manual process that was mistake-prone. They realized they were losing precious time should a real cyberattack occur and that they needed an automated system to better combat attacks.

NDOT turned to the Splunk platform to aggregate data from disparate sources across the network's infrastructure. The team downloaded Splunk Enterprise for a trial and built two Splunk dashboards to present log data. The first dashboard captures logs from the department's web and File Transfer Protocol services, tracking cyber incidents. Another dashboard collects data from servers, switches, routers and firewalls throughout a network, informing managers about abnormal events on a network, such as crashes, timeouts and errors.

With this new system, NDOT immediately gained visibility into its network. Splunk took away and automated the laborious tasks, saving NDOT time and resources.

How Splunk Can Help

With Splunk, organizations can consolidate data, identify trends and work toward a more effective government. What differentiates Splunk is that, at its core, the company wants to empower security officials to make better insights, improve day-to-day operations and partner with agencies to achieve their goals, missions and objectives.

"We are deep in the trenches with government agencies," Long said. "Agencies look at us as a partner, and we care deeply about helping you achieve your mission and goals. We want to help you maximize Splunk. We're not trying to just obtain a license and then move on. We work with you to get the strategy in place, craft the right metric reporting and drive successful security outcomes."

Splunk is very much a platform for situational awareness. One of the ways it achieves this is by helping government agencies consolidate their endpoint technologies. The company helps combine data from various departments, data centers and locations into a central location. Once the data is centralized, Splunk provides the ability to run advanced analytics to identify trends and patterns from the data to spot vulnerabilities.

"We are able to give analysts and engineers analytic capabilities, like pattern detection, trend analysis and a lot of predictive analytics capability. We are able to provide different dashboards and a user interface to create visualizations, which is another key area that we help governments for different ideas they might have."

"We understand our role in security. When you talk about security, especially in this day and age, it's not just another technology term or a different aspect of IT," he added. "You have to have a sense of commitment. We have a different type of philosophy. We believe that securing is not just about going out to sell and talk capabilities. It is about understanding the customer's mission, goals [and] objectives, and then aligning our capabilities."

"We aren't going out forcing government agencies to fit into Splunk capabilities," Long said. "We are going out there and fitting into our clients' world, making sure our capabilities align to clients' goals."

WHAT DIFFERENTIATES SPLUNK IS THAT, AT ITS CORE, THE COMPANY WANTS TO EMPOWER SECURITY OFFICIALS TO MAKE BETTER INSIGHTS, IMPROVE DAY-TO-DAY OPERATIONS AND PARTNER WITH AGENCIES TO ACHIEVE THEIR GOALS, MISSIONS AND OBJECTIVES. SPLUNK WORKS WITH YOU TO GET THE STRATEGY IN PLACE, CRAFT THE RIGHT METRIC REPORTING AND DRIVE SUCCESSFUL SECURITY OUTCOMES.

About Splunk

Splunk Inc. provides the leading platform for Operational Intelligence. Splunk® software searches, monitors, analyzes and visualizes machine-generated big data from websites, applications, servers, networks, sensors and mobile devices. Organizations use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, improve service performance and reduce costs.

www.splunk.com

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 150,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to Catherine Andrews, GovLoop Director of Content, at **Catherine@govloop.com**.

1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501
www.govloop.com
Twitter: **@GovLoop**

govloop

1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
Twitter: @GovLoop