splunk> a CISCO company | CND Ltd

Protect public services with modern security operations

Insights from Splunk and CND

Today, people expect every organization they interact with, including government agencies, to incorporate processes that can keep pace with our modern and increasingly connected world.

Whether they want to sign up for healthcare services, pay a parking ticket, or renew a business license, residents want the option to use the speed and convenience of digital services.

But with these digital services comes a wealth of resident data that attracts cyber criminals. In the public sector, upholding trust and ensuring national security are paramount, which means ensuring critical services and infrastructure remain up, running, and secure. With a mature security posture, the teams that safeguard government services can do just that: resolve issues faster or even avoid them altogether and take a proactive stance against threats.

Legacy systems, modern technologies, on-premises infrastructure, and cloud solutions often create an increasingly complex digital landscape that makes it challenging to get a full view of risks and vulnerabilities — and to detect, investigate, and respond to security threats at scale.

Unfortunately, sophisticated cyber threats like ransom-as-a-service and nation-state attacks are on the rise. In fact, our State of Security 2024 research found that over one-third (36%) of public sector respondents have experienced a data breach in the past two years. Another 33% had their system compromised by a bad actor via phishing, malware, ransomware, or similar types of attacks.

In major data breaches, bad actors may target high-profile individuals or government officials, collecting confidential data that leads to costly reputational damage. But it doesn't end there.

Data breaches can significantly impact operations, disrupt services, and even put lives at risk.

Consider a cyberattack that takes a government system offline. The effects can range from mildly inconvenient to devastating outcomes.

According to Splunk's Hidden Costs of Downtime Report, downtime for the public sector industry costs $193M annually.

Government agencies are also held to strict compliance standards, like ISO 27001 and NIST. This creates additional pressure for teams to adhere to standard guidelines and reporting requirements or risk funding consequences or regulatory action.

As government agencies strive to do more with less budget and team bandwidth, a mature security posture is key. The security operations center (SOC) of the future will enable teams to advance their security maturity with full visibility and control over their data so they're able to:

Detect threats at scale

With unified visibility and monitoring across all sources, and AI and machine learning (ML) capabilities that analyze data in one place and proactively prioritize threats, SOCs can unearth developing events and detect and respond to threats in real time.

Unify security operations

The modern SOC helps analysts get the information they need in a timely manner across siloed tools and systems. It also helps those same teams, frequently burdened with reporting on scattered information, to comply with the evolving global regulatory landscape.

Empower security innovation

As limited bandwidth and inflexible tool sets limit agencies' innovation, partner and tool selections play a pivotal role in modernizing the SOC so teams can increase productivity and outwit adversaries.

"Growing geopolitical tensions will continue to increase risks, even to organizations that are seemingly apolitical. A byproduct of our global supply chain is the inherited risk with every digital link.

Mick Baccio,
Global Security Advisor, Splunk

Safeguarding public services and data with enhanced cybersecurity

With Splunk and CND, government agencies gain comprehensive visibility that empowers accurate detection and fuels operational efficiency for more reliable digital services.

A holistic view of your digital landscape enables proactive threat detection and response across systems, networks, and services

Agencies' complicated digital footprints and complex environments make it difficult to identify threats and respond effectively if cyber events occur. Splunk helps government agencies achieve visibility across disparate data sources, creating resilient systems that safeguard critical information.

Automated compliance tasks and customized reports simplify compliance and auditing

Splunk automates data collection and continuous risk assessment for real-time insights that make compliance easier and lighten the load of audits to free up valuable resources.

Real-time insights prevent service disruption and help reduce fraud

Splunk unifies security operations, delivering real-time insights to prevent disruptions.

For example, Splunk worked with one state's public assistance programs to replace three separate legacy systems with a single cloud-based platform to make services more accessible. With the help of an IT services partner, Splunk created a system that collected data more efficiently and provided actionable insights that lowered costs and reduced security risks.

A similar approach can be effective in reducing public services abuse and fraud through quick search, detection, and investigation to identify constituent data anomalies and take action.

Powering the modern SOC with Splunk

With Splunk's Unified Security and Observability Platform, public sector organizations can overcome the complexities, threats, and disruptions that come between them and their mission.

Splunk has created a model to help security teams expand into new and complementary use cases that advance security operations. It takes organizations from gaining visibility to being more prioritized and proactive by integrating workflows in and between teams for safer and more resilient digital infrastructures.

Powering the SOC of the future

journey stages

Foundational Visibility

See across environments

Security SecOps

Search, monitor, and investigate for real-time security monitoring

Achieve visibility across your entire environment, enabling accurate threat detection and building towards a more resilient organization.

Guided Insights

Detect threats and issues with context

Reduce noise, detect more threats, and identify risk with AI/ML-powered detections

Detect and investigate holistically to prioritize analysis based on risk, leverage integrated threat intel, and stay ahead of the latest threats.

Proactive Response

Get ahead of issues

Accelerate incident investigations and response using automation

Use machine learning to detect anomalies and unknown and insider threats. Orchestrate and automate investigation and response to force multiply the SOC.

Unified Workflows

Collaborate seamlessly

Maximize SOC efficiency with integrated threat detection, investigation, and response

Coordinate workflows across detection, investigation, and response and build repeatable and automated processes rooted in resilience.

Accelerated by Splunk AI

Ready for tomorrow's challenges — today with Splunk and CND

In the public sector, people count on you. They expect public services to be efficient, effective, and always available, while also prioritizing their safety and protecting their personal information. You've risen to the challenge, working to stop disruption and deliver secure, enhanced citizen services. You've met important and evolving compliance regulations, adopted AI to improve process automation and decision intelligence, and invested in a growing cyber workforce.

With increasingly resilient digital systems enabled by a modern SOC, you'll be better able to overcome complexities, threats, and disruptions that come between you and your mission. That way you can keep doing what you're doing and keep doing it better. No matter what lies ahead.

96% of surveyed organizations say they will increase their spending on cybersecurity in the next one to two years.

State of Security, 2024

Are you prepared to protect your organization from future security threats? Contact our team today to learn how we can help.

Computer Network Defence Ltd
Lorna

lorna.dilieto@cndltd.com
+44 (0) 1225 811 806

splunk> a CISCO company | CND Ltd

Learn more: www.splunk.com/asksales

www.cndltd.com