Creating a More Resilient Future with Intelligent Cybersecurity Automation

State and local governments and education institutions, including K-12 and higher education, have modernized their organizations over the past few years to meet demands for hybrid learning, digital constituent services, remote work and more resilient operations. In embracing digital solutions, they have expanded their threat surface and increased operational complexity, opening the doors to more ransomware, phishing and other attacks.

Despite their best efforts to stem the tidal wave of threats, cybersecurity teams face significant challenges. They have accumulated a host of security tools that create thousands of alerts every day, but these tools may not be adequately integrated with one another. In many cases, IT teams have lost significant workforce talent and are left with skeleton crews that find it challenging to keep up.

To improve resilience, propel innovation and address staffing shortages, many government leaders are turning to intelligent security orchestration, automation and response (SOAR) technologies to manage threats, quickly respond to security incidents and automate security operations. When managed from a single platform, SOAR improves decision-making and reduces the time to triage and respond to alerts from minutes or hours to seconds.

Growing demands on cybersecurity teams

State and local governments, K-12 districts and higher education institutions face several challenges regarding incident management and response.

IT/cybersecurity workforce and skillset gaps. The Great Resignation, baby boomer retirements and competition from the private sector have made it difficult for governments to meet staffing and skillset needs. Competition with the private sector is fierce, and it can be difficult or impossible for government agencies to keep pace with private sector salaries.

Sheer scale of work required to monitor the digital organization. Security analysts must manage alerts coming from a plethora of siloed security tools. Many organizations want to increase visibility into threats, but when they do, they must deal with more alerts and incidents, which exacerbates alert fatigue and can overwhelm staff. Without a unified platform, they lack the visibility and context needed to make decisions quickly and accurately.

More targeted and damaging ransomware and other threats. State and local governments and schools (both K-12 and higher education institutions) continue to be prime targets for ransomware attacks. A recent ransomware attack on the Los Angeles Unified School District led to a shutdown of the district's computer systems and forced password resets for more than 600,000 students and other users.[1]

How intelligent automation can close the gaps

Many public sector organizations are using a cloud-based SOAR platform to alleviate staffing issues, increase resilience and mitigate risk. Indeed, 67% of government organizations are actively investing in SOAR technologies, according to a 2022 report from Splunk.[2]

Instead of having their cybersecurity teams physically manage alerts and manually execute incident response playbooks, organizations can use a SOAR platform to automate security and IT tasks across all their security tools within seconds. A SOAR platform connects and orchestrates disparate security tools and systems to monitor cybersecurity data, apply advanced analytics and context, and coordinate an endless variety of playbook automations.

A data-centric, machine-driven response improves cyber resilience and reduces risk by allowing organizations to resolve issues more quickly and decisively than if they had to assemble a response team and discuss case-by-case. By responding immediately, organizations can avoid or minimize downtime

Enabling flexible, equitable learning

Jefferson County Public Schools in Colorado set up a wireless network to make computer resources available to all its students and to support flexible learning. To combat account credential theft, unauthorized access and cyberbullying in this environment, it implemented a SOAR platform that correlates user activity across all its devices and systems. Doing so allows the district to protect students and sensitive data, while providing reliable access to support teaching and learning.[3]

and the high cost of remediation, data loss and potential fines. Automation of repetitive tasks also reduces stress and keeps staff more engaged by freeing them to focus on emerging threats and more meaningful work.

SOAR is ideal for automating investigation and response related to suspected phishing, ransomware or endpoint malware. During investigation of a phishing campaign, SOAR can present analysts with all the metadata about an email instead of analysts being required to manually check websites, domain names and other threat intelligence. The right platform can also automate the response, whether that's to mark and deliver the suspicious email or pull it from user inboxes. In the case of a ransomware attack, if an endpoint displays symptoms of infection, SOAR can automatically isolate that device to mitigate the impact of the attack.

While a SOAR platform is critical for strengthening cyber defense, many organizations are leveraging SOAR to meet other business needs beyond security. A water utility authority in the Southwest, for example, is using SOAR to automate the unlocking of certain user accounts after-hours. Repair crews fixing broken water supply lines sometimes lock themselves out of their computers, email or remote access VPN. Using SOAR, this water utility can receive a ticket through its normal service desk process and unlock the account using multifactor authentication. Crews can resume their work in about 10 minutes from the time the ticket is opened.

Preparing for success

The following best practices will help organizations successfully deploy a SOAR solution.

- **Understand the threat environment and the organization's threat profile.** Doing so enables project teams to prioritize goals and defend the organization appropriately.
- **Clearly define goals, strategies and processes.** Bring network, security, desktop and other IT teams together and be sure to include stakeholders from different areas of the business in discussions.
- **Start with a plan but be flexible.** Be prepared to adapt and fine-tune plans as requirements change, new opportunities emerge or real-world use reveals areas for operational improvement.
- **Establish communications and data literacy.** To build trust and a team culture, train on data literacy as a team. Use language that everyone understands to communicate with one another about data. Celebrate wins.
- **Use a "crawl, walk, run" approach — and get help**. To avoid overwhelming staff as they learn new technologies, start slowly. Professional services can help with implementation, training and getting staff up to speed. Don't stay in the crawl phase too long, though, or the project will stagnate. Iterations are key.
- **Use a platform approach, rather than disparate point solutions.** A platform approach gives organizations more visibility, context and control over the data coming from various security tools.

Today's security operations teams need as much support as possible to combat threats, protect their organizations and stay engaged. A SOAR platform will be critical to helping organizations and security operations staff work smarter, not harder.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Splunk.

1. www.npr.org/2022/09/07/1121422336/a-cyberattack-hits-the-los-angeles-school-district-raising-alarm-across-the-country
2. https://www.splunk.com/en_us/form/state-of-security.html
3. https://www.splunk.com/en_us/customers/success-stories/jefferson-county-public-schools.html

Produced by: CENTER FOR DIGITAL GOVERNMENT | DIGITAL COMMUNITIES

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com**.

Sponsored by: splunk>

Splunk is a technology company that provides the leading unified security and observability platform. For public sector leaders entrusted with mission success, Splunk offers the ability to provide real-time, data-driven insights that helps agencies unlock innovation, improve security and prepare for the mission ahead.
www.splunk.com/en_us/solutions/industries/public-sector