Simplifying Security Operations with XDR

With extended detection and response solutions, SLED security teams can respond to attacks, increase SOC efficiency and automate tasks.

A Scoop News Group Report

For more than a decade now, cybersecurity and risk management have led the list of state chief information officers' top **ten policy and technology priorities.** Yet, although state and local governments, as well as education leaders, recognize the importance of a robust cyber security posture, their organizations remain vulnerable due to the wealth of sensitive data they store, ranging from Personal Identifiable Information (PII), health records, criminal records, research, and financial records.

Cyberattacks are a growing threat to America's **critical infrastructure** and have the potential to severely impact citizens' day-to-day lives. According to a report released by the **Office of the New York State Comptroller**, the FBI received more than 800,000 cybercrime complaints nationwide in 2022, an "increase of 168 percent since 2016. In New York, reported incidents grew 53 percent within the same time period, with losses growing to more than $775 million.

A recent **Cisco blog** echoes the urgency in safeguarding the security of SLED entities and states, "Cyberattacks like malware, **ransomware** and phishing are increasing, and with 100,000 different local, state, law enforcement, tribal, townships, cities, municipalities, and county governments cyber criminals have a very big landscape to choose from in SLED... creating a situation where some of these entities are viewed as ripe for the picking by threat actors."

New resources to improve cybersecurity

It's no secret that the challenges faced by SLED organizations in bolstering cybersecurity measures reflect tight budgets and limited resources. Consequently, insufficient investments in robust infrastructure and personnel training have left these institutions' networks and systems more susceptible to malicious activities.

Moreover, the shortage of cybersecurity expertise—which has risen to under **4 million**, a 10% growth according to research from **ISC2**—can further impede efforts to develop and maintain effective defense mechanisms. The financial constraints and resource limitations not only hamper the proactive strengthening of cybersecurity protocols but also contribute to the organization's inability to respond adequately to incidents.

Fortunately, a new generation of extended detection and response (XDR) tools, like **Cisco's XDR solution** announced in 2023, provide a more comprehensive picture of an enterprise's security posture and the ability to respond to threats more quickly. These advancements, along with additional funding programs, are available to help public sector organizations.

Boosting cybersecurity attention

In August 2023, the Department of Homeland Security announced it would provide more than $370 million in grant funding for the **State and Local Cybersecurity Grant Program (SLCGP)**.

"Established by the State and Local Cybersecurity Improvement Act and part of the Bipartisan Infrastructure Law, the SLCGP provides $1 billion in funding over four years to support (state, local, and territorial) governments as they develop capabilities to detect, protect against, and respond to cyber threats," said a DHS **press release**.

> **"XDR offers a comprehensive way to stop ransomware, specifically for resource-limited SLED organizations," explained Javier Inclan, Cisco's product marketing manager. This method ensures minimal downtime and negates the need for ransom, aligning with budget-conscious operational needs.**
>
> - Javier Inclan, Cisco's product marketing manager.

The program is jointly administered by the Cybersecurity and Infrastructure Agency (CISA) and the Federal Emergency Management Agency (FEMA).

This year's funding allotment represents a significant increase (roughly twice the amount allocated in FY22), demonstrating the Administration and Congress's commitment to help improve the cybersecurity of communities across the nation," said DHS officials.

Indiana is just one of the states taking advantage of grant programs. In November 2023, **Governor Eric J. Holcomb** announced that the state was among the "first states awarded funding from the federal government's [first round of] SLCGP to support statewide cybersecurity programs." "Indiana is committed to leading the way by improving its cybersecurity posture and protecting our critical digital infrastructure," he said. Additionally, through no-cost cyber awareness training, the Indiana Office of Technology has provided more than $500,000 in value for local government.

Officials acknowledge the funding helps but only goes so far. A **survey** by the Public Technology Institute this year found that while 55% of local government IT executives reported their cyber budgets had increased over the previous budget, nearly two-thirds said their budgets are inadequate. An integrated security approach, like XDR, is crucial for SLED organizations that are often targeted by cybercriminals and face constraints in resources or budget. **Cisco's Automated Ransomware Recovery** within Cisco XDR preemptively backs up high-value assets, detecting potential threats by analyzing low-level network anomalies.

"XDR offers a comprehensive way to stop ransomware, specifically for resource-limited SLED organizations," explained Javier Inclan, Cisco's product marketing manager. This method ensures minimal downtime and negates the need for ransom, aligning with budget-conscious operational needs.

A game-changer in SLED security

XDR solutions streamline threat detection and response by offering centralized visibility across endpoints, networks, and cloud environments. The reduction of complexity, cost-efficiency and scalability can make XDR a compelling option for SLED entities, allowing them to enhance their cybersecurity posture without extensive upfront costs.

Additionally, the platform's real-time response capabilities and support for cloud integration enable organizations with limited resources to benefit from swift and adaptive security measures. The ability to share threat intelligence, with its integration of **Talos Intelligence Group**, across communities also empowers organizations. As an integral part of the platform, Talos enhances real-time response and cloud integration capabilities. Its rich, actionable threat intelligence, drawn from a global network of researchers and analysts, significantly enriches the platform's ability to respond dynamically to emerging threats.

Research from the **Enterprise Strategy Group** suggests that XDR contributes in many ways to improving security program objectives. According to their study participants, more than half of respondents said, "XDR will supplement current security operations."

"XDR set out to modernize detection and response automation, re-energizing SecOps teams to detect and mitigate complex threats more efficiently and effectively," reads another **report** from the group.

The role of XDR in SOCs

"Organizations are struggling around three major problems. One is the sophistication of attacks—the sophistication of attacks is increasing every day. The second is that it is difficult to identify which security alert should be addressed first, given the high volume," said Inclan.

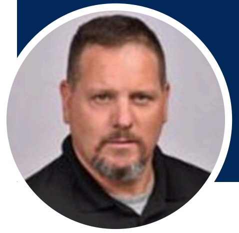
"And the third is that organizations have a siloed security approach where we have security tools or technologies that are not connected. One person cannot just wear different hats and defend the environment. Detection is key. If you can detect faster, you can stop attacks before they can cause any damage...XDR simplifies this." "The lack of security knowledge hinders SLED organizations, but Cisco XDR can help reduce the learning curve, providing steps or guidance by assisted AI effective incident management programs," Inclan added.

Norman St. Laurent, Cisco's federal product marketing manager, said that SLED entities need a "tool that can consolidate and pivot between different security products on a network, which is important." He metaphorically explained how Cisco's XDR solution was like "a pane of glass into different tools — doing a lot of the alerting, automation, orchestration, and filtration of data to make things easier."

The key to Cisco XDR's advanced capabilities lies in its ability to **integrate with an extensive range** of the Cisco Secure portfolio as well as third-party security products to share telemetry and streamline interoperability, delivering consistent outcomes regardless of vendor or technology. That includes endpoint detection and response, email threat defense, next-generation firewall, network detection and response and security information and event management.

Since the product's **release** in 2023, Cisco has expanded its capabilities to offer integrations with application, identity and device management, cloud security, and public cloud, providing what Norman St. Laurent described in the following **blog** as a SLED "SOC in a Box," due to its collaborative approach.

> **"Rather than relying on closed, proprietary systems, Cisco embraces interoperability. This means that SLED SOC environments can integrate Cisco XDR into their existing ecosystems, ensuring a seamless and efficient security framework that works harmoniously with other tools and technologies. SLED entities cannot afford clunky vender integrations that make It harder and more time consuming for SOC analysts to investigate."**



– Norman Lauren, Cisco Federal Product Marketing Manager

CYBERCRIME

800,000+
The number of cybercrime complaints reported by the FBI in 2022.

◆

168%
The increase of complaints since 2016.

◆

In New York, reported incidents grew by
53%
in the same time period, with losses growing to more than
$775 MILLION

– Cyberattacks on New York's Critical Infrastructure 2023 report

"Rather than relying on closed, proprietary systems, Cisco embraces interoperability. This means that SLED SOC environments can integrate Cisco XDR into their existing ecosystems, ensuring a seamless and efficient security framework that works harmoniously with other tools and technologies. SLED entities cannot afford clunky vender integrations that make It harder and more time consuming for SOC analysts to investigate."

And now, Cisco is augmenting human insight with AI-powered detection, said Jeetu Patel, EVP and general manager for security and collaboration **in a blog**. "We're using AI to give security analysts superpowers, helping your organization operate at machine scale," reads the blog.

"Within Cisco XDR—which correlates data across email, web, process, and network domains to detect a real attack with more accuracy—it works at scale to identify patterns and potential attacks that humans might miss because of alert fatigue or if they're only looking at one domain in isolation. Each small signal adds up to a bigger signal."

Sustainable security

Beyond better detection and response, **XDR is helping** enterprise IT and security leaders consolidate tools, improve team skills, efficiency, and effectiveness and support business growth and IT transformation initiatives.

A notable application of XDR can be seen in educational institutions, such as its implementation at the University of North Carolina – Charlotte. The Cisco security team demonstrated how successful XDR could significantly improve security efficacy and streamline threat-hunting processes. Such implementations often involve integrating XDR with existing systems, like Splunk, to create a more robust security environment.

"Securing the complex environments of hybrid work or multi-vendor is not an easy task— so it's also critical to empower teams with the tools and skills to cultivate a workforce capable of proactively addressing evolving threats," said St. Laurent.

Partners who leverage advanced **XDR solutions**, like Cisco's, can benefit from various integrations with third-party tools. Through turnkey, curated integrations with third-party security products as well as the extensive Cisco Security solutions portfolio, Cisco XDR delivers a seamless installation into existing architectures and delivers consistent outcomes regardless of vendor or solution.

While approaches will differ by state, SLED organizations should focus on ensuring the sustainability of their security approach beyond the current DHS funding window. That might include establishing partnerships to deliver cyber education, leading tabletop exercises to better prepare for breaches, or creating SOCs to provide security monitoring services for SLG or regional schools.

Partnerships could also share Incident Response Plans and Playbooks and help each other prep for Readiness Assessments and Compromise Assessments. St. Laurent notes, that to "properly protect your network, you must have a proactive approach to security."

By leveraging solutions like Cisco's XDR, SLED organizations can simplify, automate, and unify their SecOps—all while managing limited resources or budgets to build a more robust security posture.

Empower your SecOps teams to respond to threats with better insights and learn more about investing in XDR to protect sensitive data, minimize downtime, and build trust with constituents.

STATESCOOP EDSCOOP CISCO

*This report was produced by Scoop News Group,
for Statescoop and EdScoop, and underwritten by Cisco.*