How State and Local Agencies Can Beat the Cyber Staff Shortage

MARKET TRENDS REPORT

govloop

LUMEN®

Executive Summary

The security operations center (SOC) stands at the heart of security programs, with detection and response capabilities that aim to protect an organization from cyber intrusion. Faced with escalating threats, budgetary constraints and a limited talent pool, however, state, local, tribal and territorial (SLTT) governments face challenges to supporting an effective in-house SOC. In fact, according to ICMA, an association of professional city and county managers, more than half of SLTT IT leaders say they struggle with insufficient staff when it comes to cybersecurity.

In SLTT governments, the SOC typically must support security across dozens of disparate agencies, each with its own business needs, technology dependence, workforce and IT footprint. The level of complexity presents a challenge to state and local leaders trying to manage the cyber risk to support the overall business of government.

Often, SLTT government leaders find their efforts hamstrung by a range of constraints. It is hard to hire and retain the broad range of cybersecurity professionals needed to support an effective in-house SOC. It is difficult to fund such a complex operation and budget for it effectively in the face of a rapidly evolving cyber threat landscape, compounded by transformative initiatives in state and local government.

By leveraging industry partners providing SOC as-a-service, SLTT governments can effectively manage risk to their environment and minimize costs, while elevating their overall security posture. To learn more about this approach, GovLoop developed this report in collaboration with Lumen, which specializes in helping SLTT agencies address their security challenges.

At a Glance

51%

of states plan to close the cybersecurity competency gap by contracting with a security services provider.

53%

of local IT leaders say an insufficient number of cybersecurity staff is a top barrier to effective cyber security.

57%

of state and local IT leaders say ransomware is their biggest cyber threat today.

41%

of IT decision-makers say they are using a managed security service for cyber threat detection and response.

A Clear Consensus

Technology leaders across the board point to outsourced security services to improve security:

- "More city and county governments will ultimately turn to managed [service] providers, given the challenges in attracting and maintaining" competent security staff.
  — *CompTIA*
- "For some organizations, it is practically not possible to implement the security measures in-house due to lack of staff, expertise, technology, and time to attend to the evolving security issues."
  — *ACM*
- "If you can't hire enough experienced security professionals, why not outsource routine, repetitive tasks? Or activities that require special skills? Or jobs that someone else has figured out how to automate?"
  — *ISC2*

Tackling a Changing Cyber Landscape

Challenge: Resource Constraints, Threat Management

In the current threat environment, SLTT security teams face a range of key challenges in the management and operation of in-house security operations centers.

- **Limited talent** makes it hard to run an SOC effectively. SLTT governments struggle to hire and retain skilled security professionals in a highly competitive labor market, and this takes a toll on the ability to support an effective security operation.

  "Organizations are implementing so many new systems and applications every day, and each technology can have different behaviors that bad actors are trying to exploit," said Vinod Brahmapuram, senior director of security for State, Local and Education at Lumen. The competitive market for IT talent makes it hard for SLTT governments to assemble teams of sufficient breadth and depth.

- **Budget limitations** likewise present a challenge for an in-house SOC effort. It's hard to pay for an ever-changing and ever-expanding security toolset and hard to budget effectively for evolving costs around personnel, technology and operational enhancements.

  The federal government spends 16% of its IT budget on cybersecurity. Private organizations spend close to 10%, and states spend just 1% to 3%, according to the 2020 NASCIO cybersecurity study. There just isn't enough money allocated to really solve the problem of cybersecurity.

- **Threat detection and response** are a critical function of the SOC, yet many in state and local government may not have the ability to support that capability. They may lack the powerful analytics and threat management tools needed to proactively identify and respond to potential security issues before they cause harm.

  An in-house SOC, for example, may not have 24/7 response capability powered by an expert threat research and response team. The SOC may not be able to analyze alerts in time to stop threats.

The Solution: SOC-as-a-Service

In general, a managed security service (MSS) may help manage things like intrusion detection systems, firewalls, network detection and response systems, and endpoint detection and response. **SOC-as-a-Service (SOCaaS) solutions take this idea even further**.

SOCaaS typically does all that an MSS does, along with providing a team of analysts to resolve alerts, identify and analyze indicators of compromise, and analyze and respond to attacks in order to minimize the impact of security incidents, according to Kuppingercole Analysts. The team will also optimize an organization's protection, detection and response capabilities through continuous monitoring and reporting. As such, SOCaaS can be considered as an evolution of both MSS and managed detection and response (MDR).

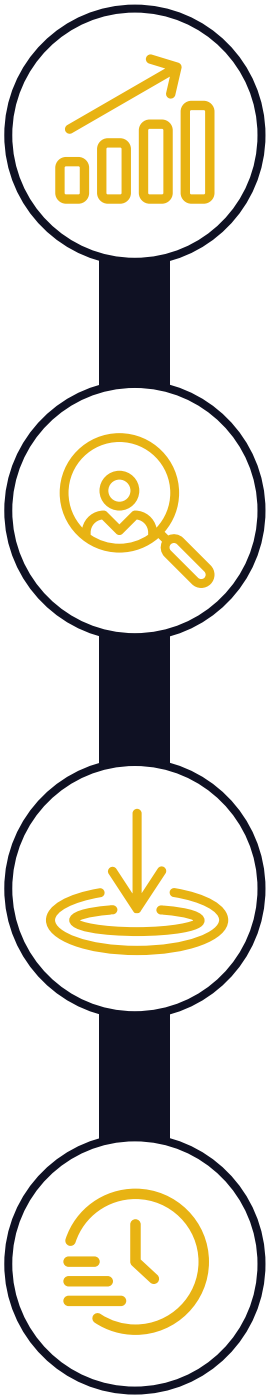
In support of improved detection and response, SOCaaS capabilities may include:

- **Threat detection:** SOCaaS leverages log data to rapidly identify potential anomalies. With access to the latest threat intelligence, an SOCaaS provider has broader reach, and the ability to spot potential problems to which an in-house SOC might not be privy.
- **Incident response:** With SOCaaS, skilled experts may work to rapidly identify potential anomalies and take immediate action in order to head off a threat, or the system may take automated action as defined in collaboration with the service provider and the government entity.

By leveraging an existing investment in security operations, SLTT organizations can access a ready pool of top-notch talent, with sufficient breadth and depth, employed within an existing operational model of proven procedures and processes. They can manage threats with less effort and can budget more effectively in an evolving cybersecurity landscape.

By freeing up SLTT resources, this approach also provides greater agility in the face of a rapidly shifting threat landscape.

Best Practices in SOCaaS for SLTT Governments



Measure Operational Improvements

While it can be difficult to assess return on investments (ROI) in the cybersecurity realm, it's possible to track another form of ROI: risk of intrusion. IT leaders can leverage the service provider's reporting capabilities to demonstrate success, pulling operational metrics to quantify potential threats mitigated.

Look for an SOCaaS provider that can deliver these metrics, both to track the progress of the cyber defense effort and to justify the ongoing investment in security-related services. "The metrics will help you to know whether you're making progress, how you are maturing in your detection and response capabilities," Brahmapuram said.

Hire Strategically

In support of SOCaaS engagement, it makes sense to be strategic in the types of in-house talent you hire, especially at a time when cyber talent is hard to come by. It can be helpful, for example, to bring in a security architect.

This individual can work at a high level to ensure the vendor understands the organizational ecosystem. A security architect can also work to align security services with specific business needs, collaborating with the service provider to decide what strategies and services will best support the SLTT needs.

Track Business Impact

The big-picture goal of security is to support and elevate government operations, including citizen satisfaction. "Here we're talking about business outcomes. Did we serve the citizens well, earn their confidence? Do more people trust our services? Are the citizens, and the government employees themselves, more satisfied with their experiences?" Brahmapuram said.

It's important to track this data as an overall indicator of the organizational impact of SOCaaS.

Look for Agility

The needs of SLTT governments change constantly as new laws, new regulations and new business circumstances arise. It makes sense to look for an SOCaaS provider that has the agility to adapt to these changes.

"The vendor should have processes in place to ensure they can keep up with your changing needs," Brahmapuram said. "Bad actors look to exploit change, and the service provider's agility will help to ensure there are no gaps as your business needs evolve."

How it Works: SOCaaS in Action

How might an SLTT entity leverage SOCaaS to improve its cyber protections? Here's how it typically works, using a hypothetical example of a state security program.

The organization runs an in-house SOC but is having trouble keeping up with the pace and severity of escalating cyber threats. There aren't enough experts on staff to run the dozens of security tools typically in use. There isn't enough money going around to support the latest-and-greatest solutions, nor does the organization have sufficient threat intelligence to take effective action.

By implementing SOCaaS, the organization gains instant access to a cadre of highly skilled professionals across a wide range of cyber disciplines. It also benefits from the service provider's deep threat intelligence, which helps to ferret out the noise and focus remediation efforts on the most pressing threats.

Meanwhile, automation tools free the IT team from routine daily tasks, thus boosting morale (and retention) while enabling them to focus their efforts on higher-level problems.

The SOCaaS brings a new level of agility to cyber detection and response, as the SLTT leverages the service provider's deep threat intelligence and experienced personnel to respond far more efficiently to changing threat vectors. Agility supports internal changes as well, with the provider working hand in glove with business leaders to adapt cyber strategies in response to their evolving needs.

The net result: a higher level of citizen service, and greater cyber security across the organization's ecosystem.

HOW LUMEN HELPS

With one of the largest, deeply peered IP backbones in the world, Lumen has unique visibility into the threats that emerge around the globe. The company leverages this network as a threat sensor to better detect and respond to malicious activities to protect their customers and the community at large.

Lumen has a long history of leveraging the threat intel on its network for cyber protection. As a founding member of the Cybersecurity and Infrastructure Security Agency's Joint Cyber Defense Collaborative (JCDC), among other working groups across the government, Lumen shares its cyber data and threat intelligence to warn agencies of the emerging risks that could impact our nation's critical infrastructure. The deep threat intelligence and sophisticated defensive capabilities built into the company's solutions have helped stop attackers in their tracks before they could gain a foothold.

In making its solutions available to SLTT entities, Lumen is helping elevate best practices across the public sector, empowering agencies to connect securely, monitor proactively and defend effectively against the full spectrum of emerging cyber threats. Its solutions are freeing SLTT technology teams to do more with less, automating network-integrated security to neutralize threats before they can do harm.

Conclusion

The challenges that face SLTT governments are not going away. Budgetary constraints, a chronic shortage of quality IT talent and the complexity of protecting SLTT systems against evolving cybersecurity threats will only make it more difficult to stand up and sustain an effective in-house SOC.

With SOC as-a-Service, these IT leaders can gain economies of scale, tapping into an existing, fully realized SOC infrastructure. In this way, SLTTs can gain instant access to a ready pool of qualified experts, along with both cutting-edge threat intelligence and a full suite of tools to support effective detection and response.

The cyber threat continues to evolve, and new business needs are always coming to the forefront in government. An SOCaaS approach gives IT teams the agility to respond to changing circumstances as they work in cooperation with the service provider to ensure solutions are always aligned with current agency requirements.

To learn more about Lumen® SOCaaS for Public Sector, click here.

govloop

LUMEN®

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 300,000 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 info@govloop.com.

ABOUT LUMEN

Lumen is guided by our belief that humanity is at its best when technology advances the way we live and work. With approximately 450,000 route fiber miles and serving customers in more than 60 countries, we deliver the fastest, most secure platform for applications and data to help state and local government deliver amazing experiences.

Learn more about Lumen's network, edge cloud, security and communication and collaboration solutions at lumen.com/sled

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop