XDR

Helps Mitigate Advanced Cybersecurity Threats for State and Local Governments

Cyberattacks against state and local governments can interrupt critical infrastructure, leak sensitive information, and cause significant financial damage. Agencies are using more security tools to thwart increasingly sophisticated attacks, but this has led to a level of complexity that overburdens security teams. MeriTalk recently sat down with Kenny Holmes, cybersecurity senior leader for government and education at Cisco, to discuss how integrated, automated solutions can help analysts quickly detect, prioritize, and remediate threats.

MeriTalk: A Public Technology Institute survey finds that nearly two-thirds of state and local IT officials believe their budgets are inadequate to support their cybersecurity programs. How can existing security solutions be leveraged to help IT teams do more with existing resources?

Holmes: State and local governments face a particular cybersecurity challenge in that cyberattacks put citizens at risk when essential services go offline. When you add in under-resourced security teams, agencies become prime targets for cyberattacks.

Security is becoming increasingly complex. To keep up with evolving attacker techniques, many agencies have added more point security solutions. But analysts are struggling to manage multiple security tools and platforms, and as a result, they are overwhelmed by alerts and unable to create a comprehensive view of their security posture. Alert fatigue is leading to staff turnover, which just makes these issues even more challenging.

Agencies need a solution that aggregates data from existing tools into a unified view – and they need to work with a vendor that doesn't require agencies to rip and replace the tools they already have in place.

MeriTalk: You noted that often, state and local government cybersecurity solutions are comprised of point security products. How can security teams evolve beyond their point security practices so detection and response are easier and faster?

Holmes: Security analysts report that they struggle to investigate advanced threats with point products. With each tool added, the time they need to remediate threats grows, because they struggle to prioritize alerts and can't gain a comprehensive view across siloed data flows.

And although Federal agencies have security operations centers (SOCs), not all state and local agencies have a SOC. By adopting automated solutions that integrate with existing tools, they can define and prioritize the most critical events and streamline responses. Unified, single pane of glass visibility, regardless of vendor or vector, is a key feature of advanced security practices.

MeriTalk: Security threats can target the network, cloud, endpoints, email, and applications. What do agencies need to enable effective security across multi-vendor, multi-vector environments?

Holmes: To protect today's complex environments, agencies need solutions that incorporate artificial intelligence (AI) and machine learning to correlate threats so they can act on what truly matters. And whether or not an agency has a SOC, automation and assistive guidance are key to increasing the productivity and confidence of security analysts.

Interoperability with vendors across the ecosystem is a key factor in extended detection and response (XDR) systems. At Cisco, we strongly believe in an open, collaborative approach. Multi-vendor integrations are at the core of strengthening an organization's overall security posture and increasing resilience.

MeriTalk: What are the advantages that Cisco XDR's cross-domain telemetry offers state and local government agencies? Where do automation and orchestration fit into this process?

Holmes: The data-driven Cisco XDR approach combines endpoint, network, cloud, and application telemetry to detect threats across all attack vectors and provide critical context, so analysts have a better understanding of security events, including where attacks start and how they spread through the network.

With our open approach, Cisco XDR also integrates telemetry from third-party security tools and threat intelligence, such as Cisco Talos, to strengthen detection capabilities. Built-in automation, orchestration, and guided remediation prioritize threats by impact and speed investigations and response.

MeriTalk: In some cases, analysts need to respond directly to remediate a threat or breach, but they may not have decades of experience and know exactly what to do. How does Cisco XDR help in these situations?

Holmes: Cisco XDR incorporates AI-guided response to help security teams optimize remediation tactics, expand visibility, and support decision-making. Guided response suggestions and recommendations help analysts take more effective actions. In addition, security teams can leverage pre-built and customizable orchestration workbooks to enable consistent, effective decision-making.

MeriTalk: Some attacks are difficult to detect because they do not involve the use of malware or other malicious software that would be flagged by traditional security solutions. How can analysts use Cisco XDR to monitor system processes and network activity to identify suspicious behavior?

Holmes: Security teams need to have comprehensive coverage of MITRE ATT&CK (adversarial tactics, techniques, and common knowledge) tactics, techniques, and procedures (TTPs). Cisco XDR detects and correlates anomalies found in system activities and network traffic patterns to quickly alert security teams of potential attacks.

In addition, Cisco Breach Protection protects against the constantly evolving techniques used by threat actors to provide a comprehensive understanding of attacks by mapping observed adversary behaviors to MITRE ATT&CK TTPs in real time.