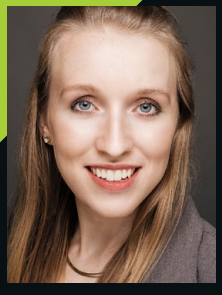
USING THREAT INTELLIGENCE TO STAY AHEAD OF CYBERATTACKS



The right threat intelligence rounds out the security arsenal so that state and local government agencies can stay ahead of threats. ***Sarah Geary,*** *manager of Intelligence for Executives at FireEye, explains how.*

Why are traditional defenses inadequate to protect against today's advanced cyberattacks?

Today's threat actors are very sophisticated. Many of them target state and local governments specifically, and if they're kept out one way, they'll try to evolve their tactics to get in through other means. Firewalls and other traditional defenses only focus on keeping the threat out. In today's environment, organizations need a more dynamic and sophisticated defense capability.

What is the key to addressing today's attacks effectively?

Intelligence. Technology by itself is not enough to protect the network. Focusing intelligence on the threat actor lets you see how the threat is evolving and stay ahead of the game. Take the recent Texas ransomware attack that targeted 20-plus cities. If that had been an espionage operation instead of a ransomware attack, the full extent of the targets would not have been so obvious, and the threat would potentially remain on their networks. Using intelligence to identify the source of the attack and understand the full extent of the problem would be key to remediating quickly and staying ahead of the threat.

What cybersecurity issues do state and local governments tend to overlook as they modernize their operations and services?

State and local governments usually have many disparate, decentralized systems that generate multiple alerts. This environment coupled with a shortage of cybersecurity staff who still need to deal with many alerts makes it difficult to prioritize response efforts. For example, the National Vulnerability Database annually ranks more than 1,000 vulnerabilities as critical — the highest level of severity — which makes prioritization difficult. Fortunately, the right third-party threat intelligence can act as a force multiplier that enables organizations to prioritize response efforts based on an analysis of how easily a vulnerability could be exploited, as well as what's being observed in other government networks and the global landscape.

How do technologies such as AI, machine learning and automation improve the detection, analysis of and response to security risks?

Coupled with intelligence, these technologies can be a game changer. To give you an example, our endpoint security tool recently alerted us to new APT34 malware on a customer's network. This sort of malware would have gotten past traditional defenses, but through behavioral monitoring, the tool enabled us to detect the malware. Over and above that, we used intelligence on top of that tool to explore the malware more. In doing so, we identified multiple completely new malware families associated with APT34. With that intelligence, we could protect the customer before the threat actor attempted to use the new tools to attack the organization.

Where should organizations start as they adopt new technologies such as AI and machine learning?

While these new technologies are very important, they are even more successful when integrated with an intelligence element that allows organizations to stay ahead of the threat. When state and local agencies know what threat actors are up to and what threats are coming, they can take a proactive posture.

FIREEYE™

BREACHES ARE INEVITABLE. BEING A HEADLINE ISN'T.

Secure your systems and manage your message with world-renown incident response services and cyber threat intelligence.

FireEye.com