Evolving your **security posture**

Automation and orchestration are integral to maturing your cybersecurity program

Chris Usserman
Principal Security and Threat Intelligence Advisor, Infoblox

THREAT ACTORS' TACTICS are constantly changing, which means cyberspace is an increasingly dangerous domain. Among other traditional nefarious activities, hackers have begun hijacking organizations' computing resources to mine cryptocurrency, using fileless malware to bypass antivirus software and exploiting the Domain Name System that is central to most internet activity.

To survive in such an environment, agencies must take a proactive approach and must understand that emerging cybersecurity tools won't help if they don't first gain a comprehensive view into all aspects of their enterprise.

The need for actionable intelligence

The worst three words in cybersecurity: "I don't know." Many organizations in industry and government don't have a good understanding of what's within their enterprises at any given moment or what their mobile systems are doing on and off premises, nor have they incorporated threat actors' tactics, techniques, procedures, and motivations for conducting attacks.

Agencies should consider what their "crown jewels" are and what adversaries could do with them. Knowing how to respond to a cyberthreat requires understanding its intent and capabilities. Context is the key to appropriate response.

Although "actionable intelligence" is an overused term, the intention is to answer the question: Do adversaries consider the information valuable? Can they do something with it?

Automation and orchestration offer a powerful way to combine cybersecurity tools and strategies to truly embrace both the proactive and reactive functions of cybersecurity. Automation often involves sharing data between two or more security tools while orchestration embraces validated and effective processes linked with skilled people and capable technology in a way that allows the technology to respond without human intervention.

Harnessing the power of AI

Although AI modeling is still relatively immature in end-user environments, it holds the key to the discovery of advanced threats. An AI-enabled cybersecurity capability requires an ecosystem whose components play well together, either directly or through third-party security products. In addition, such systems must have enough of the right data from enough sources to process and evaluate, and it often takes cloud resources to do that.

To strengthen cybersecurity in the government space, we need better processes and more collaboration. For example, the IT branch needs to understand its

davooda/Shutterstock/GCN Staff

Knowing how to respond to a cyberthreat requires understanding its intent and capabilities. **Context is the key** to appropriate response.

role in the cybersecurity posture of the agency even if it's not part of the security organization. And the cybersecurity branch needs to understand its obligation to provide input into IT procurement activities so that security is not an afterthought.

Often, the IT or security branch will procure a "best-of-breed" product without considering whether and how it will interact with existing tools. If an agency buys the best tool for a problem but no one is watching the output or it cannot automate/orchestrate with the ecosystem, that tool is virtually useless.

In addition, cybersecurity teams often take a response role far behind the threat actor's activities instead of in near-real time. If a silent alarm at a bank is triggered but the alarm company never receives the signal, the security staff likely won't catch the criminals in the act or stop them before they leave with anything valuable.

When the IT and cybersecurity departments work together, however, they can move efficiently toward the common goal of creating the most mature, resilient and secure enterprise possible. ■

Chris Usserman *is principal security and threat intelligence advisor at Infoblox.*