BROADCOM

Taking threat detection and response to the next level

Agencies can disrupt attackers by creating networks that are secure by default and using innovative tools that make the most of machine learning

Eric Chien
Broadcom

A successful strategy for detecting and responding to cyber incidents requires focusing on multiple areas. The first step is to develop a comprehensive understanding of the agency's IT environment through an asset inventory, vulnerability assessment and penetration testing.

Good threat models are another key element. The government has limited resources so agencies should focus on the threats of highest impact and likelihood for their particular organizations. It's important to continuously refine those threat models using real-world intelligence.

Once agencies have gotten their IT environments under control, they can begin to look at security tools and architectures. The goal is to have a solid foundation that will make a network secure by default. That typically means embracing zero trust principles, adopting micro-segmentation, reducing the attack surface and requiring the use of multifactor authentication.

Flipping the model of security from one-size-fits-all

To limit the damage that attackers can do, all devices should be isolated by default and only allowed to connect to the network or services as necessary. However, no human can understand everything every user is doing on a network, and it can be difficult for the average IT administrator to deploy security policies across a diverse network without blocking some legitimate activities.

Fortunately, artificial intelligence and machine learning can give us that kind of fine-grained control. Broadcom's Symantec Adaptive Security technology, for example, flips the model of security from one-size-fits-all to an approach that is dynamically tailored to the organization's environment and uses machine learning to block everything except the normal business processes that a user or device may need to do. No organization using Adaptive Security has reported a successful breach, demonstrating the tool's real-world efficacy.

However, even with a well-designed security architecture, oversights such as unpatched vulnerabilities and unmanaged devices can lead to a breach, which means remediation plans are crucial. Most security products tell administrators and analysts what has already happened—for example, that the attacker used a specific tool—and in response, the analyst may block and remove that tool. Although necessary, such actions are not sufficient because the attacker has already used the tool and remains one step ahead of the defenders.

Many organizations are left with draconian measures that have a big impact on productivity, such as temporarily shutting down a database, service, website or entire network. Meanwhile, administrators still don't

know where the attackers are or how to kick them out.

Blocking an attacker's next move

To take remediation to the next level, Broadcom has created Incident Prediction. It is based on large language models (LLMs), the same technology generative AI uses to perform tasks such as writing essays by predicting the next word in a sentence. We realized that an attack chain is essentially a sentence and each event in that chain is a word. By training our own analogous LLM on half a million attack chains collected in just the previous six months, we developed a tool that can predict the next four or five steps an attacker will take with 100% confidence.

Incident Prediction can also identify what an attacker might do in response to those defensive actions so the security team can block those as well. The tool's targeted approach eliminates the need to shut down entire networks while administrators track down the attackers.

> "IT CAN BE DIFFICULT FOR THE AVERAGE ADMINISTRATOR TO DEPLOY SECURITY POLICIES ACROSS A DIVERSE NETWORK WITHOUT BLOCKING SOME LEGITIMATE ACTIVITIES."

Innovative tools like Adaptive Security and Incident Prediction are vital components of a robust security architecture that enables agencies to prevent and stop attackers without harming productivity. ■

Eric Chien *is a fellow on the Threat Hunter Team at Broadcom.*

ADOBE STOCK // SKIMP ART