USING AI, ML AND OTHER EMERGING TECHNOLOGIES TO PROTECT DATA AND INFRASTRUCTURE

Jon Ramsey, chief technology officer at SecureWorks, discusses new technologies that can improve an organization's security posture.

What challenges do state and local governments face in securing data and infrastructure as they move beyond traditional data center models?

We think about risk in terms of threats, vulnerabilities and assets. State and local governments provide a lot of critical infrastructure, and they have non-public personal information that is very attractive to adversaries. As for vulnerabilities, their infrastructure tends to be dated and frail. Much of it is decentralized, so there's poor visibility into vulnerabilities. In addition, it tends to be non-segmented, so once adversaries get inside the infrastructure, they can go wherever they want. In terms of threats, adversaries can now automatically scan the internet for opportunity. Because government infrastructures have such a large attack surface with many entry points, threat actors can often find a way in. When it comes to mitigating these risks, organizations often don't have the talent or can't scale to defend such a large, diverse environment.

How can a managed security service (MSS) help agencies meet these needs?

There is no faster way to improve your cyber maturity than to hire someone who does this day in and day out. An MSS provides a very skilled labor force that helps organizations fight threat actors and adversaries, reduce the attack surface and mitigate vulnerabilities so that if an attack occurs, exposure is limited. An MSS also helps identify and prioritize assets in your environment so you can focus on defending the most critical assets.

How can AI and ML improve threat intelligence and security services overall?

With AI — and machine learning, in particular — instead of us having to continuously tell the system what's malicious, the security monitoring systems themselves are gaining the capability to tell us what they think is malicious. That software-driven versus people-driven approach enables speed and scale and is an extremely important pivot point for the security community overall.

What other emerging technologies will help agencies improve their security posture?

There are a lot. Software-defined data centers provide greater visibility, so you can see the network and its assets and then understand what terrain needs to be defended. Sensoring capability that allows monitoring is also really important to gain visibility into the infrastructure and detect availability, integrity and confidentiality issues. Lastly, federated machine learning is going to have a huge impact on defending municipalities. That means taking what you're learning from one infrastructure, from a security perspective, and applying it to defend another infrastructure; so once one city or region is hit, you can automatically learn from that compromise to help inoculate or defend other areas.

What advice can you give for integrating ML and AI into an organization's security strategy?

First, identify a specific security use case and then decide whether data science or ML can help you in that use case. Avoid trying to impose data sciences simply for the sake of using them. Second, rich data and simple algorithms win the day, so be cognizant of the quality and breadth of your data. That's more valuable than trying to infer or guess something because you don't have a piece of data. Lastly, computer security personnel usually aren't data scientists. It takes someone with data science capabilities to generate the algorithms needed for true machine learning.

Conversely, software developers or data scientists are not cybersecurity experts. In order to create and apply cybersecurity analytics effectively, you need to know what the security use cases are, determine what data you need and identify what data sciences techniques will provide the most value.

Secureworks®

Detect faster, respond smarter, and predict and prevent more threats altogether.

Learn more about Managed Detection and Response Services at **https://carah.io/SecureWorks-5-16**