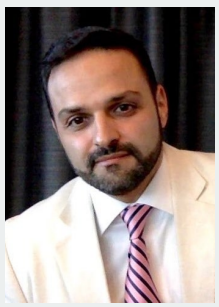
USING DATA AND MACHINE LEARNING TO ADDRESS VULNERABILITIES



Adilson Jardim, area vice president for public sector sales engineering at Splunk, discusses analytics-driven security and the importance of a defense-in-depth approach in today's hyper-connected enterprise.

How has cybersecurity management become more complex as organizations move toward a more connected future?

Before the internet took off, our focus was on whether a single system or application complied with general security practices. Since then, the attack surface has exploded. We now have internet-facing applications, microservices, IoT devices, mobile phones and other elements that have to be interconnected to exchange data. Given the value of personal data and the ways that bad actors can use that information, the imperative to protect data — to secure access to the data, systems and services — comes with this complexity. Some of these elements didn't exist even 10 years ago.

How can organizations leverage machine learning, AI, automation and other tools to improve their cybersecurity stance?

There are a number of basic considerations. You need to gather and save log files and other data that's generated by devices across your enterprise about what's going on. Then you must implement ways to identify the low-hanging fruit, like using statistical methods to establish basic anomalies of behavior inside your environments. You want to be able to "template" activities so that you can automatically orchestrate an operation or response. Then you can move into a machine learning framework where you consider how those large data sets inform your cybersecurity operations.

What do organizations need to put in place to unlock the power of analytics-driven security?

You need a lot of data to support machine learning and ultimately AI. Organizations must capture and understand the machine data coming from all the systems, services and devices connected to their networks. They need a historical view into what has happened, as well as the capability to use that data for a more real-time response to threats. To establish the basis for machine learning, they also need that historical set of data to teach algorithms what to look for and what outcomes to enable.

But organizations can get started right away with applying analytics to aid their security mission. For example, do you have a good handle on trusted identities in your enterprise? How about known devices? Analytics can answer these types of questions quickly to help agencies prioritize and take action on security enhancements.

What questions should organizations ask as they assess their vulnerability to cyberattacks?

There are lots of levels where an organization might be vulnerable. With so many unknowns, the question is never are you 100 percent secure, but rather how do you respond to incidents and breaches, given certain conditions. This requires a defense-in-depth approach that uses multiple layers of controls to address security on every front: Do we have the right visibility; do we have the data to support decision-making when we respond to an incident; do we have the right automation, processes and standard operating procedures to address different families of vulnerabilities, threats or incidents; and so on. Organizations also have to ask what their risks are if, given their budget, they can't address certain actions or responses. They may have to make tradeoffs, but they should only do so when they understand what's going on in their environment and what exposure at different layers looks like.

WEAPON OF A SECURITY WARRIOR.

Machine data is the key to having happy customers and avoiding costly cybersecurity incidents. Like we do for more than 16,000 customers around the world — let Splunk turn your data into real-time visibility and insights that will streamline operations and provide a foundation for a robust security posture.

→ splunk.com/get-value