Scaling cybersecurity through **automation**

Successfully managing a complex security landscape hinges on automated, orchestrated response

Chris Usserman
Principal Security Architect,
Infoblox

CYBERSECURITY RESOURCES ARE not growing at the scale of the enterprise or the scale of the threat. And that means security professionals are left with the challenge of managing what's happening inside their IT environments while keeping an eye on external activities that could have an impact on agency systems. And they still have to maintain the day-to-day functionality of their networks.

The only way to successfully do all that is with automation. To reap the benefits of automation, however, agencies' cybersecurity tools must support interoperability.

The value of integrated ecosystems

Specifically, open (RESTful) APIs and software development kits make it easy for customers to quickly link together different vendors' technologies in a repeatable, scalable, automated way.

In addition, an integrated ecosystem not only collects information from external sources, but also understands what to do with it. By automating existing manual processes, the ecosystem could inform agencies, for example, when a new device connects to the network so that it can be scanned for vulnerabilities. Integration has become simple enough that organizations have to willfully go around it to avoid making it part of their security process.

The next phase is putting repeatable manual processes and responses into an automated series of events that will be triggered by certain activities. Then agencies can start to move beyond automation to an orchestrated response policy that can grow at scale immediately.

Faster malware detection

As government systems move to the cloud and employees become more mobile, though, the security challenges continue to evolve and the attack surface continues to expand. Now that mobile employees are accessing cloud-based resources from anywhere on the internet, they inadvertently become potential gateways for adversaries. Encrypting data at rest and in motion and taking a zero-trust approach are exceedingly helpful tools to protect users and data.

When employees take their laptops home and connect to a local internet service provider, most of the investments the organization has made to secure its enterprise no longer provide protection. Antivirus will handle some threats, but adversaries will always change their game to attack enterprise systems and mobile devices.

One of the best ways to protect those systems is to control a device as soon as it reaches out to the internet. When malware starts to infiltrate a network, it typically makes a DNS query to reach its command-and-control server for instructions. If an agency can intercept malware at that point and immediately take action through automation, the agency has a much better chance of containing the threat.

As a result, agencies can reduce the current meantime-to-detection from months down to hours or even minutes, which is essential in this increasingly mobile, cloud-based world. ■

Chris Usserman is principal security architect at Infoblox.