The power of **real-time cyber intelligence**

Automation and ongoing collaboration can improve threat detection, incident response and overall security

Paul Kurtz

Splunk

Last year's Executive Order on Improving the Nation's Cybersecurity represents a powerful step forward, and it is already helping agencies prioritize their security needs. For example, the order directs agencies to improve their ability to log system activity over time, which is particularly important in the wake of the SolarWinds-based attack. At the time, agencies struggled to understand what was happening, what had gone wrong and how far back the problem went. Better monitoring and logging capabilities would have helped.

In addition, many agencies were already exploring the concept of zero trust, but the executive order's focus on that philosophy is pushing agencies to adopt it. The challenge is recognizing that zero trust isn't a single product. It's a suite of capabilities that are brought together and re-examined time and time again to ensure that as systems evolve, agencies continue to maintain zero trust.

At the end of the day, the goal is to drive down the time it takes to detect and respond to events.

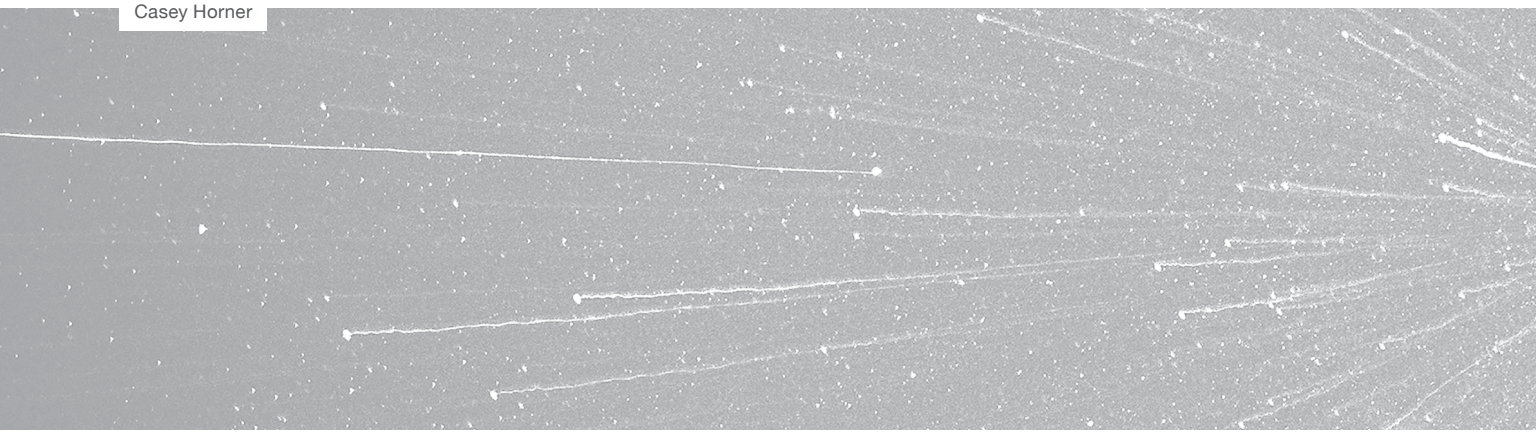
Why automation is a security imperative

Government agencies are realizing that if they are going to mitigate cybersecurity risks and respond to breaches more quickly, they need access to real-time operational intelligence. However, they also recognize that their security products and intelligence sources must be readily integrated. A security operations center (SOC) can't function when it has 50 products that don't talk to one another and whose data can't be easily fused and normalized.

Many organizations try to manually corroborate a notable security event with other data, such as external threat intelligence, feedback from an endpoint detection and response platform, or information from the Department of Homeland Security. A manual process is slow, inefficient and ultimately doomed to failure.

The solution is to move to an automated environment. Frankly, we are not going to make real progress on cybersecurity until we adopt greater automation. Agencies should have intelligence workflows that fuse together data in real time, automate the prioritization of that data and update defenses without necessarily having a human in the loop.

Furthermore, when agencies successfully integrate information from security tools and intelligence sources in real time, they develop valuable data that can be used to train machine learning models, and they can refine those models as more events are correlated. Then they will start to see patterns that allow them to identify



Casey Horner

> At the end of the day, **the goal is to drive down the time it takes to detect and respond to events."**

problems earlier and more easily predict what might happen in the future.

Shifting the focus from individual agencies

Most cybersecurity discussions focus on individual agencies and what they can do to improve their defenses. The prevailing wisdom has been that each agency must defend itself, which was appropriate in the past but is no longer a viable approach.

Now, with the growth of cloud technology, it is far easier for agencies to work together in a seamless fashion, and that is something that should happen automatically. In other words, let's stop thinking as individual SOCs and start thinking about how SOCs at different agencies can collaborate to share information in real time.

We have organizations like NATO because we are stronger together than we are individually. When agencies share what they're experiencing with one another in real time, they strengthen their ability to protect government systems on an exponential scale. ■

Paul Kurtz is chief cybersecurity advisor for public sector at Splunk.