A Unifying Viewpoint for Security

Automation of the easy stuff improves your information security efforts and makes the work that's left far more interesting for those who do it.

Jesse Trucks
Minister of Magic, Splunk

HIGHER EDUCATION HAS ALWAYS FACED TWO hurdles that make information security especially challenging. First, no matter what type of institution you're in – small or large, public or private – you will always have more work to do than you have people to do it. Second, churn will set you back. The human element plays a bigger role in technology success than any of us on the vendor side likes to admit. When people leave, you have to hire anew, which, in universities, is commonly those in early career. Once they've learned the ropes, they'll head off to somewhere else, often for more exciting work.

Automation of the easy security work – known threats, known responses, malware detection, cleanup – addresses both problems, and everybody wins. The campus gains better operational success. And when humans don't have to intervene with the ordinary, they're free to do more interesting work. They grow in their positions, because they're not just clicking buttons all day.

Automation is especially important in an era of remote status quo and zero-trust. IT has to assume that there's a high probability of any authentication request being nefarious. And that means being able to look at data in context: Is this person at a higher risk? Is the laptop or smartphone compromised? Should we let them on the network today? Have we scanned this device in the last three days? Then let's not allow them access to this HR data. If they get their machine scanned, then they can come back and try again.

While higher ed has long been predicated on allowing open access, now that can only happen when it's the appropriate thing to do. Users have to be classified – student, researcher, staffer – and access has to be controlled. When everything looks normal, they get unfettered access. But when their machine or account is compromised, the access should be denied.

Easier said than done, right?

Complex Uses for Simple Data Analytics

Splunk started out as a data analytics platform for IT operations and software development that is really simple to use. Users can shove anything they want in without having to predefine how the data is structured. It serves as a unifying viewpoint. Once the data is in Splunk, users can do various searches and analytics. But what really distinguishes the program is that users can also change data definitions on the fly and have the change retroactively apply to anything they've ever loaded. Because the data isn't structured in a particular way, users aren't limited by what they were thinking about the data at the time they loaded it.

What we as a company have learned is that our users are much more creative with uses for Splunk than we could ever have imagined. This data analytics platform for DevOps has found a ready application as a security information and event manager, handling all kinds of information security use cases – privileged user monitoring, detection of zero-day attacks, stopping data exfiltration, using DNS data to identify malware.

Splunkbase, our app exchange, offers more than 500 security applications from us, our many partners and the community at large, to extend the core functionality of Splunk and provide shortcuts for getting work done. That was the thinking for **Phantom**, a Splunk-created security automation and orchestration platform that integrates with existing security technologies in order to provide a layer of "connective tissue" between them.

Establishing a Security Nerve Center

Phantom streamlines security operations through the execution of digital "playbooks," which enable IT to achieve in seconds what might take minutes or hours to accomplish with all of those security products they use every day. Phantom doesn't replace existing security products; it makes the investment smarter and faster.

The program works like this: It gathers data from any and all sources, does deep analysis with predictive analytics, logs the results, and then transforms that information into actions it will perform. For example, based on the data it has

consumed, it may recognize the need to pull a machine off the network for reimaging. Rather than alerting IT to do the job, it can take the actions needed without human intervention. Or, if there's something more complicated that does require human input, Phantom can stop, send a message to a human, who can then decide what to do or not, and then it continues. It can trigger events, close networks down, generate help tickets and any number of other actions.

Phantom serves as the nerve center in the very middle of the entire security operation, where it can pull data from all the many tools, push data out and respond where it's needed. Organizations are able to improve security and better manage risk by integrating teams, processes and tools. On the incident response side, security teams can automate tasks, orchestrate workflows and support security operations center (SOC) functions including event and case management, collaboration and reporting.

One frequent story I hear from campus IT customers is how they use Phantom to block activities on the network that end up protecting students' machines in the residence halls. Even though those machines aren't being monitored directly, the network activity is. Splunk could detect botnet activities before they launched an attack in the dorms. Phantom could even be set to send out a notification informing the students with infected machines that their devices have been compromised and that they need to either do the patching themselves or bring their systems into the tech center for attention.

IT staffers no longer need to take training on all of the many security tools in use; they have to become conversant in just one. And because that one tool allows for deep analytics, level one folks aren't consigned to the simplest stuff; they too can dig into the raw data for forensic analysis, which makes the work far more intriguing. With the right automation, the churn may just wind down.

Jesse Trucks *serves as minister of magic at Splunk, where he specializes in security. He also hosts "Meanwhile in Security," a podcast covering cloud security for ordinary people.*