M+E JOURNAL

The Future is Automated

The landscape ahead for M+E looks uncertain. Automation can ease the journey.

WORKFLOWS AND THE CLOUD
From cloud-based productions to unprecedented storage demands, the supply chain has never been more challenging

SMART CONTENT
The questions around AI, metadata, and analytics are endless. But we do have many of the answers already

SECURITY SOLUTIONS:
Cybersecurity and content protection in M&E is always on defense. Can automation can change that?

23.01

GET SMARTER WITH YOUR SECURITY RESPONSE TO SMART DEVICES

The adoption of IoT personal tech has opened up new avenues of attack

ABSTRACT: What happens when your “dumb” water bottle becomes a “smart hydration vessel”? There are services and functions that benefit consumers and our growing demand for new sources of information. Each of these new elements becomes a security risk, and only through automation can operators keep up with the growing threat landscape.

By John Jacobs, Field Chief Information Security Officer, Fortinet

What happens when a “dumb” water bottle becomes a “smart hydration vessel?” Growing adoption of IoT personal tech allows consumers to engage in immersive entertainment and powers greater business insights to drive personalized content, next best offers, and to continuously improve experiences that keep people coming back. But now the water bottle has an IP address, and the accelerated increase of IoT elements is a security risk. Only through automation can operators keep up with the expanding threat landscape.

Collecting high volumes of private information across a swath of IoT devices, such as fitness details or location information inside smart parks, drives service innovation but also complexities around data generation, transport, and storage as it’s shared between providers and services, creating new avenues for hackers to obtain and exploit that data or impact the online user experience.

A watch used to communicate zero bits of data. Now the devices we wear have embedded firmware and operating systems that transmit data to your phone and cloud-based services, meshing them into a giant software ecosystem. Often these devices are in constant sync, silently plugged into the larger ecosystem, posting data that’s no longer in a person’s control and extends beyond the walled garden—it’s sold, extracted, manipulated, and replicated—creating a data explosion.

Within media and entertainment businesses, security operators are struggling to maintain existing processes and procedures with the continuous rise in IoT data volume. But just as technology has transformed the consumer experience, the solution to manage your security response to that data is also technology. Security information and event (SIEM) platforms and services scale well as volume builds, but that can add cost, and without automation does not reduce the workload. Without the consideration of tooling and systems, the staffing for an around-the-clock SOC can hover near one million a year. Add to that investment the cost to manage growing assets and devices and you need to ask the question: how do you direct your resources for the best security effectiveness?

The typical SOC process involves four stages for a triggered event:

1. *Event classification and triage*
2. *Prioritization and analysis*
3. *Remediation and recovery*
4. *Assessment and audit*

SOC teams have previously had the ability to process event stages properly, adjusting time spent depending on severity. With the advent of IoT, operators are overwhelmed with events and notifications, making it difficult to act on what's truly important. This leads to setting less sensitive thresholds to trigger fewer events, or removing sources from the triage process, for example, ignoring failed admin logins. These and other attempts to reduce notifications can create risk.

This is where machine learning (ML) and artificial intelligence (AI) can help. ML can build historical records, such as learning that user logins are higher on Monday mornings, which can lead you to reduce the alert threshold during that window. But responses such as that can be quickly learned and circumvented by hackers. ML alone is not enough. But coupled with AI, you can refine your results and build a model of overlying information to reach more logical conclusions that reduce SOC overhead without compromising security. ML plus AI can help you take more parameters into account for nuanced responses that attackers struggle to respond to:

- *Has the user account logged in elsewhere?*
- *Does that account normally fail at attempts?*
- *What device is it being attempted from?*

> *THE ACQUISITION OF MULTIPLE SECURITY TOOLS has resulted in fragmented workflows, often stitched together by third-party systems, that can slow or interrupt notification and response.*

Applying this kind of logic processing as a service or added to a SOC solution can refocus analyst skills on the investigations that matter.

Another pillar of evolution to handle the influx of IoT data is task automation. The acquisition of multiple security tools has resulted in fragmented workflows, often stitched together by third-party systems, that can slow or interrupt notification and response. Security orchestration automation and response (SOAR) platforms offer several important features, including a user-friendly interface to conduct logical "if-this-then-that" workflow connections, often referred to as playbooks or runbooks. By grouping known actions with their workflow steps, a mundane task can be scripted once and run as long as needed with predictable outcomes. This reduces analyst workload so they can look at new automation opportunities or deeper event correlation. Other key SOAR features include ingesting different log or event sources and performing structured correlations, centralized reporting, and coordinated incident response. By eliminating manual processes, you can reclaim precious time to process additional workload or continue to improve procedures to better detect and block more complex attacks.

Layered security is the most effective means to prevent and detect breaches in your digital environment. As your ecosystem grows, remember that security operations are an important focus and can greatly benefit from modern advancements in ML/AI to better the user interface, accelerate effective triage, and act as a smart platform to help secure IoT ecosystems and incoming data from consumer devices. ⊞

John Jacobs serves as the field CISO for Fortinet. Before this role, he has held numerous technical leadership positions at Fortinet covering varied geography and industry exposures, including the formation of our cloud consulting services organization. jjacobs@fortinet.com @Fortinet