Global Edition Privacy & Security

Need a better cybersecurity process for healthcare? SOAR is king

SOAR solutions gather event and alarm data from across platforms and organize them into a single location or case.

Atos | September 11, 2019 | 11:52 AM

Security orchestration, automation and response (SOAR) is receiving more and more print these days—and with good reason.

The advances that SOAR offer are particularly relevant to healthcare because patient data is some of the most valuable data—to hackers—that there is. At the same time, healthcare organizations often operate highly distributed systems and networks, making them particularly vulnerable to attack.

First of all, SOAR is not security information and event management (SIEM), although SOAR can be seen as an enhancement to SIEM. SOAR goes further than SIEM by improving case management and reactivity of security personnel.

Any single hospital may, by itself, have 20 to 30 security products. The fundamental purpose of these products is to find and eliminate threats. That goal is quickly obscured by the sheer volume of alerts, the complexity of having so many products, and by security engineers having to manage such an infrastructure.

Here is how SOAR helps:

1. It consolidates multiple sources of threats and other information into a single case. SOAR solutions gather event and alarm data from across platforms and organize them into a single location or case. This single feature saves valuable resource time and uncovers hidden threat data. Important security and other information is brought together into a single case, which means analysts don't spend precious time hunting in various tools to find information.
2. Unlike SIEM, SOAR focuses on response—the 'R' in SOAR. Arguably, this is SOAR's greatest benefit. It enables security teams to create complex automated workflows that can help improve response times—while possibly lowering costs. SOAR establishes and documents workflows to deal with specific threat situations. These workflows can be practiced, updated and used for training—saving time and money.
3. SOAR enables the creation of multiple playbooks to deal with a wide variety of threats. Each step within a playbook may be automated and include integration with a variety of security products.
4. Automated administration can be built into daily threat intelligence gathered from tool sets to perform the tasks of gathering information, analyzing and opening a case. It can also deploy fixes and monitor the effects, carrying the automation through the close of the case.

More subtly, SOAR can help with healthcare's ongoing security labor shortage. As threats become more complex, the time it takes for people to process, analyze and respond to those threats increases. One of the fundamental benefits of SOAR is that it allows security staff to focus less on repetitive tasks and more on digital surveillance and threat hunting.

With SOAR tending to the tedium, healthcare organizations are better positioned to retain valuable security staff by allowing them to focus on more challenging and interesting work.

For more information about cybersecurity in healthcare, visit https://atos.net/en/industries/healthcare.

Topics:
Privacy & Security