Automation and enterprise security

Moving from reactive to proactive security
Security personnel often don’t have enough time to consider and act on every threat, no matter how minor – but automated systems do.

With security tools increasingly capable of acting without human intervention, using automation is often the sign of an organisation with a mature cybersecurity posture.

Security teams have an increasing array of demands on their time, which means reacting to daily or even hourly alerts can feel like a never-ending battle.

Automated systems help organisations reduce teams’ workloads, freeing them up from repetitive day-to-day tasks. Security staff are then able to use their time in more valuable ways: getting up to speed with evolving threats and attackers, improving their own skills and taking a more proactive stance to protecting company systems.

While traditionally seen as the province of large enterprises, automated systems can have even bigger benefits for smaller organisations, which typically have fewer dedicated security staff: any task that can be automated gives another member of staff the chance to focus on other priorities.

Preventing fatigue and false positives

Nonetheless, automated systems have their own challenges. Their ability to act autonomously in response to security events can have unintended consequences, such as acting on a false positive, what the system blocks as a suspicious IP address might turn out to be linked to a developer’s cloud-based pilot project, for example.

However, good systems can be fine-tuned to suit the risk profile of the organisation and the preferences of its security team, addressing both false positives and alarm fatigue through selecting appropriate analytics and effective workflows.

And while staff may be concerned about handing control of their security environment to automated systems, well-configured tools enable a company not only to react to incoming threats faster but give personnel more time to spend on value-added tasks that improve the company’s defences. It’s also important for organisations to weigh up the hassle caused by a false alarm against the damage wrought by a successful cyber attack.
Automation holds the answer

Once the security tool has identified behaviour indicative of malware or other threats, the race is on to take action before that behaviour leads to a full blown incident.

APIs and integration with other security products can help not only identify behaviour but also take remedial actions when something doesn’t look right.

LogRhythm uses plug-ins to provide automated responses on its platform. These can take a pre-determined action, or SmartResponse™, when they detect a compromised user account or one still being used by a former employee: shutting down access immediately, for example.

There is a wide variety of SmartRespones available, including adding specific IP addresses to firewall blacklists or sounding a warning or alarm if certain behaviour is spotted. SmartResponse plug-ins are pre-built but can be adjusted if required to suit the individual organisation’s needs. In addition, SmartResponse can plug into other security vendors’ APIs.

How does automation work in practice?

Ask any IT professional and they’ll tell you they spend too much time concentrating on keeping the lights on, and not enough on driving innovation in their organisation.

It’s a problem that affects those working in security most acutely - the security skills shortage keeps growing, as does the number and complexity of the incidents they have to protect against.

Automation can help streamline some of the repetitive tasks in threat detection and remediation. Once a threat has been identified, a case can be created automatically containing information on the alarm, log data and more. The case can then be reviewed by personnel who can collaborate on the right response to deal with it.

Once the threat has been dealt with, security teams can examine the details of the incident and decide how to prevent a similar occurrence in future.
From detection to containment

Automation today can provide the means not only to detect, but also to respond more quickly to security incidents.

Security professionals often talk about the ‘golden hour’ – the key initial period after a breach is detected when the actions taken can make a massive difference to the disruption and damage caused.

Automated systems can give staff precious minutes to defend against attacks. Moving from detection to containment almost instantaneously can also mean the difference between a managed security incident and a damaging data breach. Security teams can focus on mitigating the damage and getting systems back to normal.

By automating workflows around typical incident response procedures, organisations can ensure the right actions are taken at the right time. Collaboration is a key part of successful incident response, and automated systems can make this process far easier to manage.

Such systems can also help create clear incident reports that can be used to improve future responses – an element that can be overlooked when an attack is underway. By managing incident response, collection of artefacts and even evidence, organisations can make sure they learn as much as possible from an attempted attack.

There’s no doubt that automation will play an increasing role in cybersecurity. Despite concerns over control and false positives, the threat landscape is changing so rapidly that organisations need the ability to respond instantly to new threats.

As the demands on security teams continue to increase, so does the need for the best tools to help them do their jobs.

LogRhythm can help organisations at all stages of the threat management lifecycle, from detection to remediation.

To free your security staff from manual tasks and empower them to be more proactive, contact LogRhythm.