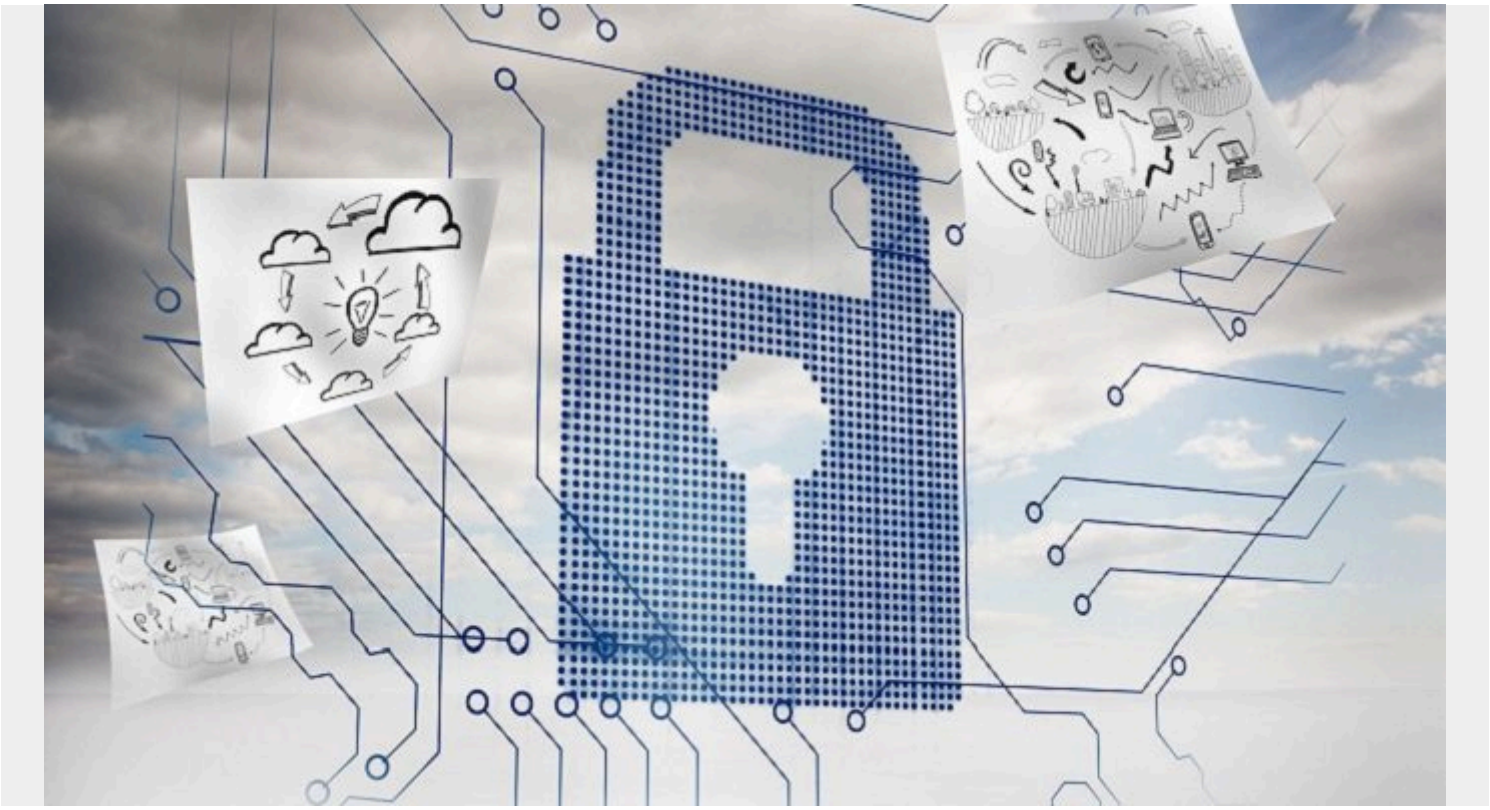
SECURITY AUTOMATION: A BEGINNER'S GUIDE



Security automation refers to machine-actions that monitor, detect, troubleshoot and remediate cyberthreats without human interaction. Security automation identifies threats, prioritizing the best actions to remediate them as they occur. This helps security teams remain focused on big-ticket security items as they don't have to solve each small remediation that would normally get escalated to security.

Automating security results in best practices for performing threat detection, systematically triaging identified threats, determining the next steps and resolving issues in a matter of seconds. It's no wonder more and more often, enterprise businesses that have undergone digital transformation are looking to automated security as an asset for their organization.

Using security automation, risk analysts can focus on proactively identifying security problems instead of remediating existing tickets. This allows these professionals to use their skills in a way that adds more value to the organization. In this article, we'll talk about the history of security automation, why it's important and then offer tips for implementing automated security protocols in your organization.

The Origin of Security Automation

The discussion about automating security was a direct result of the increase in cyberthreats and attacks facing businesses. Before the rise of security automation, risk analysts were responsible for identifying and resolving as many threats as possible. Unfortunately, that meant the vast majority of

minor threats went ignored because capturing and remediating all threats was an endless task. Security automation was a necessary response to the overwhelm that analysts were experiencing.

The first iteration of security automation was an automated incident response that helped make security queues more manageable and easier to service. Then came a more holistic approach to security automation that was sophisticated enough to find and resolve security issues without being prompted by analyst interaction. Today, another market has arisen from security automation called Security, Orchestration Automation and Response, or SOAR.

The Difference Between Orchestration and Automation

Security automation integrates machine-operated tasks that simplify essential processes for risk and security analysts. Orchestration takes security automation a step further, ensuring vital systems are carefully and securely integrated together to provide a full range of automated security and feedback tasks. Orchestration ensures that all parts of your security and threat detection infrastructure are able to work together, offering proactive threat protection and remediation to an entire architecture.

Automation is a component of orchestration, and orchestration is an evolution of security automation. There are almost a limitless number of IT tasks that can be automated. Security is among them. Doing so removes time-intensive aspects of security from the analyst, leaving them able to handle other issues while making proactive observations for security optimization. The goal of orchestration is to provide full-coverage management of the security of a large-scale infrastructure.

Why is Security Automation Important?

You already know security automation serves the primary role of assisting risk and security analysts so they can focus on essential components of the job. Now, here are some other key benefits of security automation:

Speeds up threat detection

Intelligence is the mechanism that allows a computing device to learn from patterns and plan from repetition. Intelligence in threat detection allows for security response to trigger based on learned behavior that signifies a threat. This allows for faster, more responsive threat protection that plays a critical role in security infrastructure.

Improves incident response

In the same way it speeds up threat detection, it also improves incident response. When analysts are overwhelmed with security alerts, they can only mitigate the most critical on the list. By taking a share of the workload from the security analyst, incident response becomes standard practice.

Increases visibility of security metrics

When you orchestrate your automated security, you integrate with tools that can help you track and report on security metrics. This leads to greater visibility of your security issues and processes.

Encourages standardization in security management

When fully orchestrated, you can have visibility of all infrastructure security from a centralized hub. This helps security departments standardize security management processes across departments to ensure consistently that goals are met.

Tips for Implementing Security Automation

Here are some tips for implementing security automation:

- **First, automate infrastructure:** By automating infrastructure first, you create an environment that is ready to scale with business growth, no matter how fast you grow. This should take place early and be subject to continuous improvement measures.
- **Shift payload of work to detectors:** Moving most of the work to detectors is essential since it's difficult for analysts to handle the existing workload.
- **Automate everything you can:** Alert collection, alert prioritization, tasks and processes can all be automated. You can also automate things like compliance checks, vulnerability management and more. Practice orchestration, centralizing your automation across departmental workloads.
- **Focus on continuous improvement:** Continuous improvement ensures you always have superior security measures in place no matter how your infrastructure changes.
- **Stay involved, always:** Automating tasks does not equate to being a hands-off security manager. When you automate your security framework you must still have human oversight and involvement to ensure enterprise assets are as secure as they can be.
- **Participate in an internal review of vendors:** In the world of multi-cloud technologies, it's not unlikely an enterprise business selects a cloud provider for an essential service they seek to inject into existing infrastructure. Before turning over your data and information to third party vendors, participate in an internal review.
- **Restrict access in automated systems:** Treat automated systems the way you would other manually-activated parts of your infrastructure. This means limiting access to essential employees and vital contractors.