SOC AUTOMATION

When we refer to automation in SOC, we're talking about:

- **Security Automation and Orchestration (SAO) or**
- **Security Automation, Orchestration, and Response (SOAR)**

And as an SOC analyst, you're likely to encounter some type of security automation within an organization. Let's dive into maturity models to learn how those relate to automation.

First, though, let's define security automation.

What is SOC Automation?

Simply stated, **automation** is the machine implementation of low-level security-related actions, which are smaller pieces of a larger task.

A **task** is made of a number of actions that are partially or fully automated. Their goal is to reduce human intervention in security operations.

From there, a **process** encompasses a number of tasks.

Orchestration is closely tied to automation, but it takes advantage of multiple automation tasks across multiple systems or platforms. Additionally, orchestration is used to automate or semi-automate more complex workflows and processes.

Now, some SOC analysts and others in the security community criticize automation. They seem mostly concerned that automation will take their job. I mean, if a machine can do it faster and more efficiently, what's an analyst to do?!

Let me present it like this. *Automation should be a springboard to an SOC analyst, not a limitation or replacement.*

We want analysts to continue detailing events, which takes a great deal of time and just isn't possible with the numbers of events coming in daily. Additionally, we need SOC analysts to look for trends, examine data over time, and find reasons the events are occurring. They should ask themselves, "Is the reason I have to respond to 50 events per day because the web server is vulnerable?" They should take that information to their SOC leadership and show initiative to patch the vulnerability.

Automation is a positive addition for any SOC. Let's look at why

Why Automate?

SOC analysts are incredibly valuable resources who will always be needed to perform jobs that machines simply cannot.

Think of it this way. SOC leadership is often tasked with new requirements and additional services--but with the same (or fewer!) resources. They're being pressured to deliver more, and combined with a shortage of skilled cybersecurity professionals, automation becomes more appealing and necessary.

You can see where this is going. Automation helps analysts with the flood of events coming on a daily basis.

Imagine how automation can free up **analysts** from monotonous tasks. They can instead spend more time on higher-level analysis of events. In addition, senior analysts can spend more time training junior analysts.

Consider, too, that automation can streamline existing processes.

For one, automation reduces analyst fatigue. For the amount of day-in and day-out information that must be collected, categorized, analyzed, and interpreted by an SOC analyst, it's easy to see why analysts start to feel brain-fried. By relieving this fatigue and stress, the SOC is a more challenging and fun place to work. With that in mind, automation can promote morale and create a healthy workplace environment.

The second reason for automation is to **reduce mistakes**. It's easy for analysts to make errors during the constant document checking and console switching. By automating these tasks, the likelihood of mistakes is far less. And it also increases consistency, which is key in security operations.

A third reason to automate is to **reduce information bias**. Analysts may create false positives or take off down a rabbit hole. Unfortunately, it's simple for one wrong attribution to skew a full dataset. Automation, therefore, ensures consistency.

Finally, automation allows operations to **keep up with the speed at which attackers** are evolving. Every few months, there seems to be a new attack pattern with more complex threats. Automation and orchestration can help reduce the mean time to detection **(MTTD)** and **mean time to response (MTTR)**. These can save time that adds up and leads to significant time savings.

Metrics decreasing will also satisfy senior management, and happy senior management is always a good thing.

SOC Maturity

Truly, there's no way to automate all processes in an organization, which simply gives you job security.

There are just too many situations when a real-life analyst is needed. Automation has led to horror stories in the past, leading to catastrophic effects on businesses--and their reputations.

As such, there must be checks and balances in the automation process. And those measures require human interaction and approval before being implemented.

Now, the topic of this chapter is SOC Maturity, so let's get to it. Or at least a shallow dive into determining an SOC's maturity.

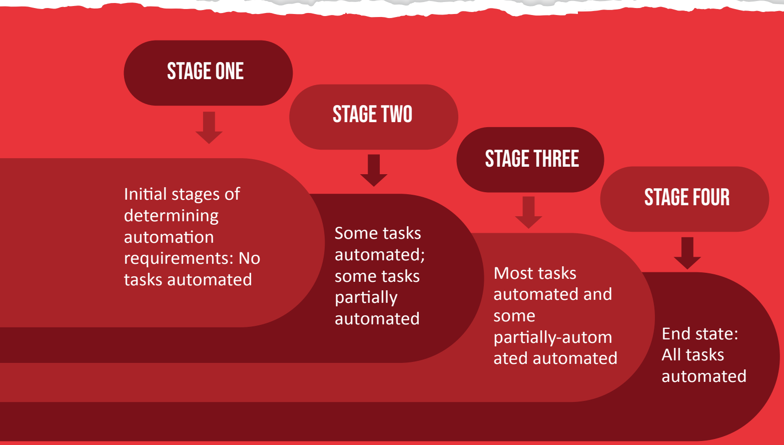
STAGE ONE
Initial stages of determining automation requirements: No tasks automated
STAGE TWO
Some tasks automated; some tasks partially automated
STAGE THREE
Most tasks automated and some partially-autom ated automated
STAGE FOUR
End state: All tasks automated

FIGURE 7-1: AUTOMATION STAGES

As shown in figure 7-1, you can begin with a staged approach to assess the maturity of an SOC's automation. You can see that once you've completed an inventory of your SOC today, then you can map your current state and measure your progress toward established goals.

You can start with small goals. And you can start anytime. Just start! Because automating actions gets you closer to your goals.

Now, as a junior analyst, you'll start to see areas for improvement in the processes used by you and your team every day. Keep an eye out for gaps, and look for actions that can be automated. Take your time and gather the proper data. Then do an analysis.

Ask yourself, can any of these actions be automated? What benefits do you see it providing to the team?

Being able to articulate process improvements or resolutions will set you up as a leader among your colleagues. Additionally, SOC leadership will view you as a real deal problem solver.

That right there is worth its weight in gold.

How to Start Automating

As with most things, there really isn't a one-size-fits-all approach. Here are our recommendations:

1. Someone who is intimately familiar with the organization's processes and procedures should spend some time analyzing the work they do each day. Before long, this will be you!
2. Categorize the tasks by the amount of time they take. Focus on the simple tasks because automating them can make a sizable amount of progress. Check out Figure 7-2.

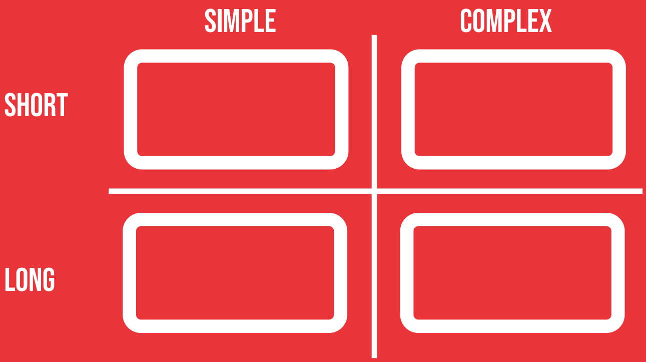

FIGURE 7-2: AUTOMATION MATRIX

3. Now, look for repetitive actions with complex conditions. Make every effort to break it down into the smallest possible steps.

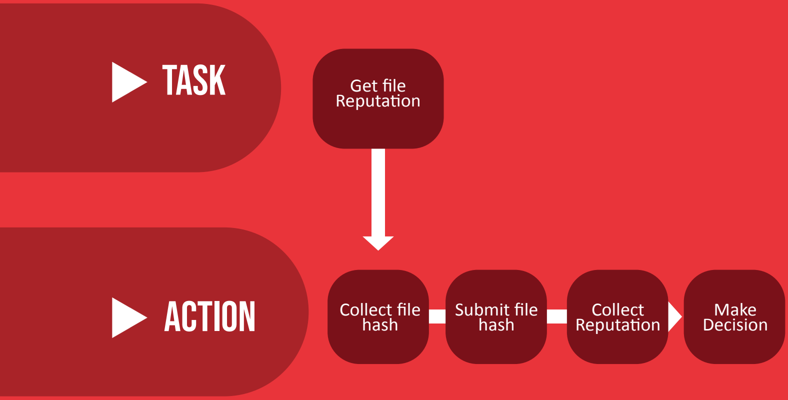

FIGURE 7-3: GET FILE REPUTATION

Review Figure 7-3. Let me break down the tasks for you as a future analyst:

- **a.** Gather the file hash.
- **b.** Open a web browser.
- **c.** Paste the hash into the browser and submit it.
- **d.** Make a decision based upon the file reputation

The decision made upon the file reputation might then feed another action or process flow further downstream.

A playbook can be this small, and it's also possible to have a playbook that calls other playbooks synchronously, waiting for the first one to complete before calling another.

I know. It may not look like much time will be saved by automating this task. But it sure might reduce the number of tickets you respond to! *SCORE.*

Sample Use Cases

Part of the SOC automation journey is realizing that what works for other platforms might not work in your environment. That's to be expected.

Bearing this in mind, I'll share a couple of use cases that might act as a starting point for your future automation endeavors. They likely won't be an exact fit, but they're good scenarios to consider.

1. If you haven't already started your automation journey, talk with your team about the benefits.
2. Do a full inventory of the tasks your SOC performs.
3. Break them down into the time required and complexity demanded.
4. Define your use cases before automating any actions. Focus initially on tasks that are simple and fast, providing you some quick wins.
5. Don't write long, complex playbooks. As much as possible, break them down into specific tasks. Also remember the option to use a parent playbook to call multiple child playbooks.
6. Don't fear challenging the status quo. Beginning an automation process will often reveal a new and better way to do something. Allow automation a chance to show its value to your organization.

It's true that security automation is still in its infancy, but it can be implemented to improve your SOC's operations. Take the lead! Show your team that automation isn't a limitation but a force multiplier for everyone to become better analysts.