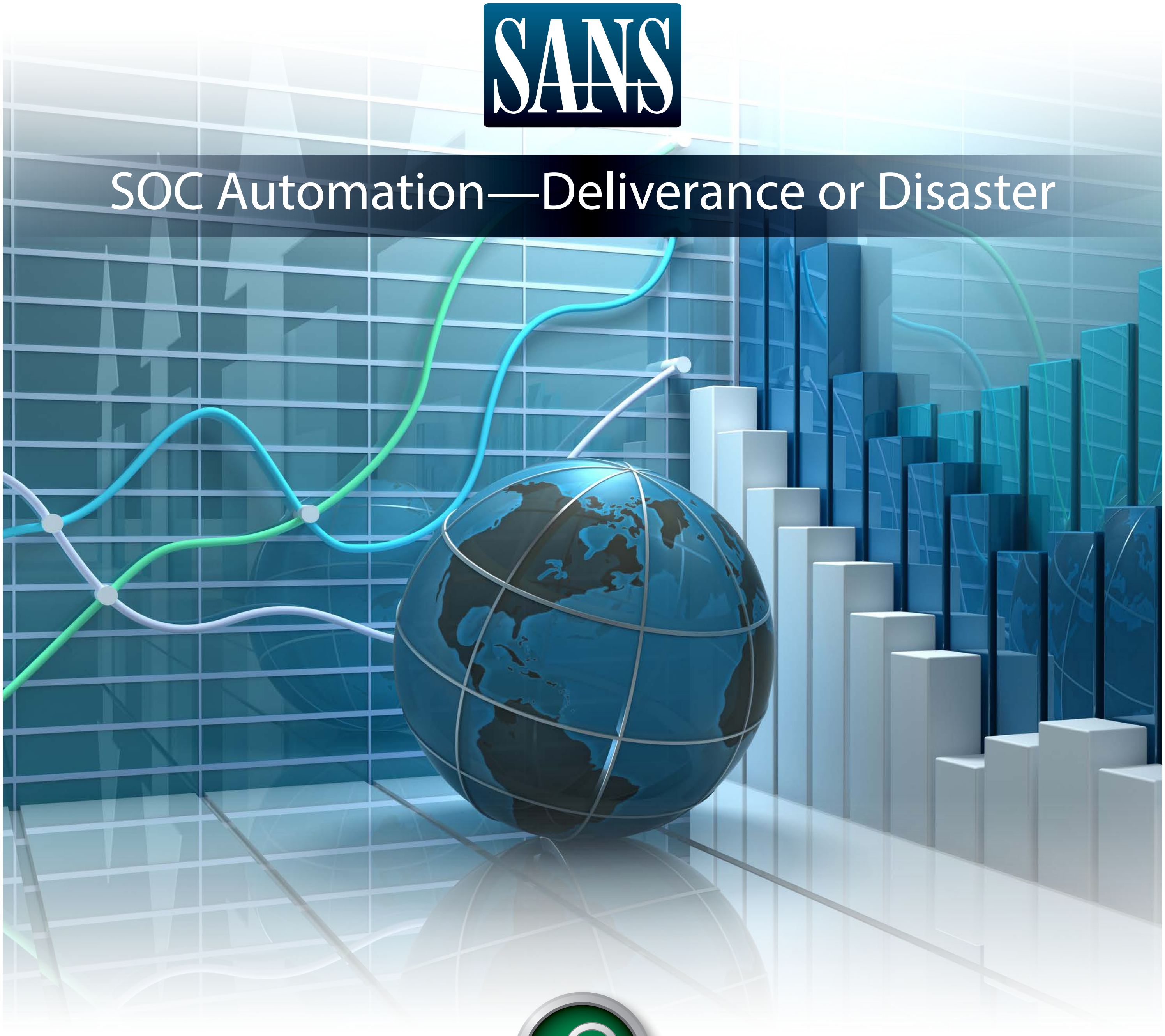
SOC Automation-Deliverance or Disaster

Eric Cole, PhD



SOC Automation—Deliverance or Disaster

A SANS Spotlight Paper

Written by Eric Cole, PhD

December 2017

Sponsored by
DFLabs

In almost every security incident, the same problem keeps recurring: Security devices alert practitioners about the attack, but there are too many alerts and not enough analyst time or expertise to handle them. As a result, alerts that truly matter get buried in the noise.

In most security operations centers (SOCs), the number of devices generating alerts is increasing at a much faster rate than the number of staff. Most organizations look at this problem and think there are only two solutions: 1) decrease the number of alerts (or in some cases organizations just choose to ignore a large percentage of alerts because they do not have the staff to respond), or 2) increase the number of staff. In reality, there is a third option to maximize the efficiency of the analysts' time: automation.

If you study the work of SOC analysts closely, you will realize there are really two types of activity that they perform: 1) routine analysis in which they essentially follow a script that has them performing tasks in a repeatable manner and 2) tasks that require expertise and analysis in order to respond and resolve the issue. The big difference between the two tasks is the amount of time required for the amount of analysis required. With routine analysis, a script is followed with minimal to no deviation. This paper will focus on the first task and how to improve the outcome.

Routine analysis is very repeatable and can be systemized and automated, but that same automation also creates potential risks. The risks are associated with false positives wherein legitimate traffic is either blocked or categorized as an attack. Either outcome could affect operations. Consequently, many organizations have avoided automaton. In the face of ever-growing threats, however, ignoring automation is no longer an option. For example, the Target[1] and Home Depot[2] breaches triggered attack alerts, but there weren't enough people to properly prioritize and respond to the alerts.

Although automation has been viewed as an all-or-nothing approach, companies can implement some elements of automation to balance risks while maintaining control over how they monitor and react to alerts. The idea is to strike a balance between alerts that can be automated with minimal impact and the higher-risk alerts that need to be handled by analysts.

[1] "Target Ignored Data Breach Alarms," www.darkreading.com/attacks-and-breaches/target-ignored-data-breach-alarms/d/d-id/1127712

[2] "Case Study: The Home Depot Data Breach," January 2015, www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367

Pros of Automation

With the large amount of traffic going across networks, organizations will never be able to hire enough people to handle all of the alerts. One method is to tune the devices to reduce the number of alerts, but that will also reduce the number of attacks detected.

The alternative solution is to automate. Many of the tasks performed by SOC analysts are very repetitive and can be automated with computers. The big benefits of automation include the following:

- More consistent response to alerts and tickets
- Higher volume of ticket closure and response to incidents
- Better focus by analysts on higher priority items
- Improved visibility into what is happening
- Coverage of a larger area and larger number of tickets

Automation has typically been favored in low-impact environments, but it has been frowned upon in high-impact environments such as utility and healthcare because of the negative impact false positives can cause.

Cons of Automation

False positives happen when the system interprets legitimate traffic as an attack and blocks it. In some industries, a false positive could result in an annoyance such as a denial of service attack. In other organizations, though, it could cause detrimental events, such as shutting down critical components in utility companies, hospitals or air traffic control. Some of the dangers of automation include the following:

- Shutting down operations
- Misclassifying an attack so the wrong action is taken
- Automating tickets that should have been handled manually
- Missing key information or data
- Making the wrong or inappropriate decision

Organizations have typically looked at the potential downsides of automation and then avoided it because that approach seemed safer. However, today's organizations are realizing that if automation is not used, there is a greater chance of missing an attack, which could cause more damage than the negative effects of automation. Given this scenario, practitioners should look at automating some tasks under specific circumstances to reduce the attack risk.

Ideal Tasks/Tickets to Automate

One of the key rules of security is to always avoid extremes. Let's look at what tasks can be automated while maintaining acceptable levels of risk—both on the operational side and the security side. Avoid taking automation to the extreme, automating everything and justifying this decision by claiming analysts cannot keep up with the tickets.

The solution is to find a balance in which you would automate tasks/tickets that create a lot of work, are highly repeatable in their process and are currently a distraction. The trick is to manage and control false positives, not eliminate them. False positives include the following:

- Scans of the network and system
- Noisy attacks/scans against services that are not running on a system
- Attempts of attacks that are not successful
- Low-priority systems that would have minimal impact if compromised

Organizations should stay away from automated alerts that could have a major impact to the organization if not addressed. These include the following:

- Missing critical applications or systems
- High-impact systems that could have a detrimental impact
- Any systems that contain large amounts of sensitive data
- Large-scale compromise indicators

Given the number of threats compared to the number of alerts, consider some automation to help increase the efficiency of SOC operations.

The trick is to manage and control false positives, not eliminate them.

Mini-Case Study

In this case study, we use a hospital to show the proper balance of automation. Even if you do not work in healthcare or hospitals, the logic and reasoning is applicable to almost any organization.

Typically, hospitals have avoided automation because of the concern that mission-critical systems could be blocked or taken off the network as a result of false positives. If an attack is miscategorized and a life support system is taken offline, the impact to patient safety could be too risky. The problem with this logic is that a small subset of systems is used as an example for the entire organization.

This approach has proven to be problematic with hospitals in light of ransomware attacks, which move so quickly that it is almost impossible for manual methods to respond fast enough to control the damage. The only possible way to manage and control damage from these rapidly emerging kinds of attacks is via automation. Now, after ransomware attacks have crippled hospitals by making 70 percent of their data unavailable, hospitals are learning to utilize a balance of automation on the business network with manual methods for patient-critical networks. This type of attack happened in the UK in May 2017 when 16 hospitals were shut down after they were hit with ransomware.[3]

[3] "U.K. Hospitals Hit in Widespread Ransomware Attack," https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack

The Future of Automation

Based on the speed at which attacks occur and change, organizations that ignore automation will fall further behind and be on the losing side of most attacks. An SOC will never be able to hire enough people to respond to all alerts. That leaves two options: 1) reduce the number of alerts generated, which could lead to missed attacks, or 2) automate most of the alerts and have analysts focus only on the most critical alerts or the ones that have been escalated up from automation. The second option is the most beneficial to most organizations.

TAKEAWAY

Balancing risk is key. Determine high-risk areas and use SOC analysts, but consider automation for cases where volume is high but risk is low.

As we have demonstrated above, successfully implementing automation requires finding a balance. Start with some automation on low-priority items not only to show the value to executives, but also to demonstrate the benefits of automation—and to show that automation will not take down the enterprise. As confidence builds, additional automation can be added, but remember it is unrealistic to think you will get to a point where everything can be automated.

Conclusion

As you consider automation in an SOC, ask yourself two questions: 1) Are you currently winning or losing the cyber battle? and 2) Do you want to continue to lose? As the means and methods of compromise change, our techniques for dealing with adversaries must also change. The rate at which organizations are attacked is increasing, as is the speed at which those attacks compromise a network—and it is not possible for a human to keep up with the speed of a computer. The only way to beat a computer is with a computer.

TAKEAWAY

The rate at which organizations are attacked is increasing, as is the speed at which those attacks compromise a network—and it is not possible for a human to keep up with the speed of a computer. The only way to beat a computer is with a computer.

In utilizing automation within an SOC, it is important to have a well-thought out strategy addressing the following key questions:

- What areas generate the most alerts?
- What alerts take up most of the analysts' time?
- Which responses are very structured and which ones do the analysts respond to in a predictable way?
- Can a playbook or runbook be used for Security Automation Orchestration to handle certain events?
- What events would have minimal to no impact if they had a false positive?

By utilizing this set of questions, an organization can start to identify the areas that can be automated within their organization.

About the Author

Eric Cole, PhD, is a SANS faculty fellow, course author and instructor who has served as CTO of McAfee and chief scientist at Lockheed Martin. He is credited on more than 20 patents, sits on several executive advisory boards and is a member of the Center for Strategic and International Studies' Commission on Cybersecurity for the 44th Presidency. Eric's books include Advanced Persistent Threat, Hackers Beware, Hiding in Plain Sight, Network Security Bible and Insider Threat. As founder of Secure Anchor Consulting, Eric puts his 20-plus years of hands-on security experience to work helping customers build dynamic defenses against advanced threats.

Sponsor

SANS would like to thank this paper's sponsor:

DFLABS
CYBER INCIDENTS UNDER CONTROL