IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Overcoming the Barriers to Automating Your Cybersecurity

Yann Le Borgne

Yann Le Borgne
International Vice President of Threat Intelligence Engineering
ThreatQuotient

Biography

Yann Le Borgne, International Vice President of Threat Intelligence Engineering, ThreatQuotient (https://www.threatq.com/) and is a specialist in Cyber Security with over 15 years of experience. He joined ThreatQuotient in January 2016.

Before ThreatQuotient, Yann was in charge of a technical team of 12 people across Southern Europe at Sourcefire which have been acquired by Cisco.

Yann blogs at https://www.threatq.com/resources/

Keywords Automation, Cybersecurity, XDR, Orchestration, Detection, ThreatQuotient, Threat intelligence
Paper type Opinion

Abstract

The phrase "automation" has gained traction in the cybersecurity community. However, the benefits of automation are not being realized by businesses due to a lack of money, time, and trust in the results. In this article, the author explores these issues and looks at how confusion around the meaning and potential of "automation", "orchestration" and "XDR" may be a barrier to implementation and offers insight for organizations on where to start so they can resolve pain points and achieve cybersecurity automation success.

Introduction

"Automation" has become a buzzword in cybersecurity circles. That is not surprising in an environment where security specialists are in short supply and under intense pressure to defend the business against a huge variety of threats from innumerable different sources. Using technology to do at least some of the work seems like a no-brainer. Nevertheless, it seems that organizations are finding it hard to get the right approach to cybersecurity automation.

ThreatQuotient conducted research last year that found resources, time, and a lack of trust in outcomes are preventing companies from realizing the benefits of automation. In a recent webinar, myself, Nabil Adouani, CEO of Strange Bee and co-founder of The Hive Project, and our Global VP of Threat Intelligence


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Engineering Chris Jacobs discussed the current state of automation, the expectations around what automation can achieve, and what this means for implementation in the real world.

From automation to orchestration and XDR – all sides of the same coin?

One of the challenges around automation is defining what we mean by the term, and where it differs from orchestration. Really, automation is anything that replaces a manual human-driven activity with a computer-driven alternative. It has applications across the technology sector wherever there is a repetitive manual task that would be better done by a machine that never gets bored or makes mistakes.

In the incident response area of cybersecurity, automation can be used at any stage of the process. Examples include ingesting alert data, enriching alerts, and even automating elements of response.

Often automation and orchestration seem to be used interchangeably, but there should be a distinction. Automation is the conversion/adaptation of a single manual process to be completed by machine, whereas orchestration is applied to a multi-stage workflow involving multiple different tools, which are automated and brought together to execute a process.

When it comes to XDR, there is further uncertainty around what this means. Analyst company Gartner suggests that XDR should have a minimum of three elements, such as endpoint detection and response, security incident and event management, and incident response capabilities on your platform. This would

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

constitute XDR and orchestration could also be part of coordinating a series of automated actions based on the technology capabilities of the platform.

However, despite all the buzz around automation, orchestration, and XDR the path to implementation has not proved easy.

Orchestration is not a silver bullet

On the face of it, orchestration is a no-brainer, lifting the burden of repetitive tasks and saving time so cybersecurity teams can focus on higher-value activities. Yet adoption remains limited. Industry observers have even seen examples where businesses shifted from having no orchestration, straight to full orchestration, and then back to no orchestration again because they found they were spending all their time and resources fixing the automated workflows to function properly. They concluded that a simple script could work just as well for their use case.

Chris Jacobs advises that teams shouldn't assume that by buying and installing a platform they'll suddenly find themselves "magically" capable of doing things they weren't doing before. Firstly, they need to look at what processes they currently undertake manually and identify how these will benefit from orchestration into an automated workflow on the platform.

Nabil Adouani suggests that another reason for low adoption relates to the number of existing tools already in use. When there are already a lot of tools in play, adding an orchestration platform that must be maintained increases the pressure on teams – the exact opposite of the desired effect. If security professionals who want to be focusing on security need to frequently add new use cases, update workflows and work on integrations, this may lead to task avoidance and low adoption of the tool.

Deciding where to start

Organizations can feel overwhelmed when faced with the potential scale at which they could automate cybersecurity detection, management, and response, so where is the best place to start?

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

First, decide what types of incidents you want to handle with the tool. Then look at what you are already doing and where you are doing it when an incident occurs. So, for example, you might be using spreadsheets, one note, and emails to record and handle incidents, following a manual playbook. Look at that process and work out which elements could be automated, and then orchestrated into a multi-stage process in the platform. This approach has the added benefit of overcoming lack of trust in the outcomes of orchestrated processes. If you know what your process outcomes typically look like before you orchestrate them, you will find it easier to rationally accept a similar outcome from the orchestration tool.

Detection and vulnerability management are strong use cases for automation, and we recommend businesses put most of their focus here initially. Network detection, email security, and endpoint detection are all areas where, once issues are identified, multiple automated actions can be launched, such as informing the relevant stakeholders, enriching the alert data, and prioritizing the actions needed to mitigate the issue. In the case of vulnerability management, scanning identifies the weaknesses, and an automated workflow can share it with the people that need to action remediation.

It is also important to understand that the level of automation and orchestration that is appropriate will depend on the use case. Very few organizations will want to remove human oversight entirely from a process. For example, in patch management, it's not advisable to automatically patch all your servers because the tool has identified a vulnerability and an available patch; there must be human input. Instead, you can use automation to find the right combination of compensating controls, so when the tool identifies a vulnerability, it automatically sends alerts to the relevant stakeholders so compensating controls can be put in place before the patch is implemented.

One of the major advantages of using a centralized platform is that all teams are using the same data and starting from the same point. This helps get cross-disciplinary IT and security teams working together and starts to break down the siloes that often exist between departments.

In conclusion

In summary, when starting out with automation, first identify the repetitive, time-consuming workflows you already undertake that can be orchestrated. Then design the workflow with the appropriate balance of automation and human input for the use case, focusing initially on the detection phase before determining what aspects of response can or should be automated. Finally, explore how access to the tool can go further to break down siloes between departments and get all teams working effectively together on a unified security mission.

This approach should reduce some of the pain points around implementing automation and ensure organizations are realistic in their expectations of what they can achieve.