Security Automation and Orchestration – delivering efficiency or risk?

Security professionals have learned to invest time with the utmost care. It is a resource that underpins some of our industry's most critical metrics, such as the time between threat detection and response.

As security operations teams attempt to manage risk and compliance across a growing number of disconnected point solutions, finding ways to increase efficiency within the SOC is high on most organizations' agendas. In particular, organizations are facing interconnected pressures including alert fatigue, a growing skills gap and heightened threat levels from attackers that are adept in the use of automated techniques such as 'burst bot attacks' (Mirai and the more recent variant Okiru malware, for example), brute-forcing credentials, domain generation algorithms (DGAs) and ransomware.

Many in our industry consider that Mirai's open source code (which compromised IoT devices in 2016 bypassing default credentials to conscript the devices into a botnet), changed the game in terms of real-time response. Although these attacks have mainly been successful in attacking consumer technology, hackers' ability to mutate and customize this type of code will potentially require automated mitigation to counter the staggering speed and variety of attacks.

But equally, our industry is not interested in shortcuts and is understandably cautious about adopting new practices that by reducing or even removing the input of skilled analysts, may introduce further business risk. Some argue that not only will automation never be able to replicate the decision-making of security analysts, but also that it will create more false positives and potentially lead to significant business disruption when an automated process gets it wrong.

So, what can Security Automation and Orchestration (SAO) offer in the balance between maximizing time and resources for security operations within a controlled, practical framework?

Are we ready to automate security operations?

In theory, security automation tools can help organizations eliminate manual tasks from almost every aspect of security operations. For example, they allow organizations to analyze certain types of the most frequent, labor-intensive attacks and respond immediately without analyst intervention – freeing up valuable resources to focus on more high-value tasks. Working with clients across the globe, our consultants observe considerable time being invested in the growing number of daily manual tasks that security teams perform. These resources are too often stretched by these essential, if low-level administrative tasks.

Typical drivers for organizations evaluating Security Automation and Orchestration

- A high volume of alerts and incidents stretching resources or reporting
- Desire to maximize the value of SIEM systems and reduce false positives
- Issues with patch management or firewall maintenance
- A diverse portfolio of third-party security detection products generating a growing number of alerts
- Planning for new compliance requirements for incident response and breach notification, such as GDPR
- Difficulty in recruitment or high employee turnover in security operations teams
- Drive for faster incident response to reduce risk and cost to systems availability
- Preparing to move to managed security services

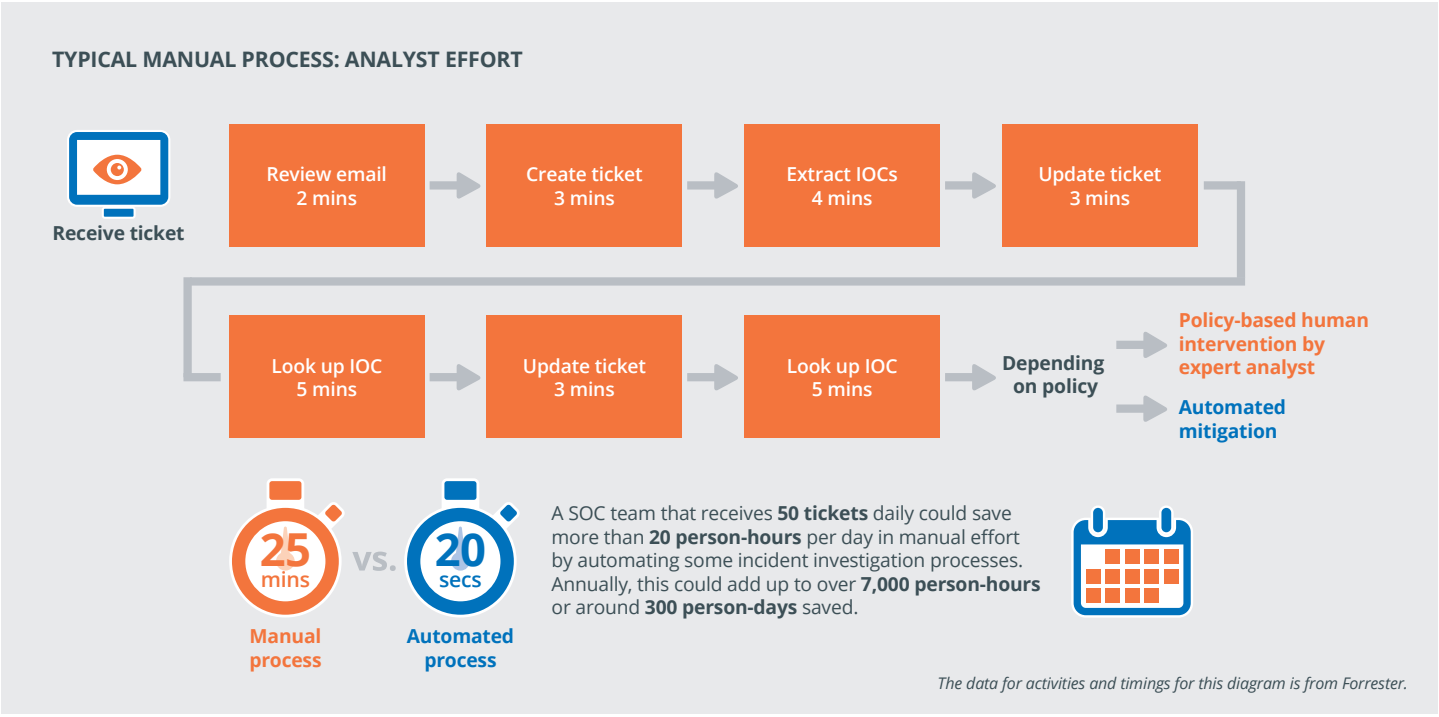
Ask yourself the following questions:

1. How much time does your team spend every day cutting and pasting queries between different tools?
2. Do you manually log into multiple sources during the day to access threat intelligence?
3. Do your analysts have to keep moving between multiple tools and screens suffering from what is referred to as the 'swivel chair' effect?
4. How much time and risk do you introduce by manually manipulating data in a spreadsheet when investigating and prioritizing events?
5. Do meetings with auditors result in days of repetitive reporting on standards and regulations?
6. When incident investigation is complete, do your analysts have to manually check if systems are remediated correctly?
7. Do you continually have to generate manual post-incident reports?

If any of this sounds all too familiar, automation could be a way to regain precious time invested in these repetitive, manual processes – time that security operations teams cannot afford to lose.

Automation is now confidently applied to a wide variety of business processes that are repetitive and predictable – such as inventory management, shipping, purchasing and generating invoices. Not only has automation accelerated these workflows and lowered the costs by eliminating human intervention, it has also dramatically reduced the risk of human error. This risk is something SOC teams are aware may creep into the application of well thought-out SOC playbooks when security events happen, as other pressures lead to vital steps being overlooked. Automation can help SOC teams apply best practice not only faster, but more consistently.

Figure 1 An example of how automating elements of the incident investigation process can reduce time spent by analysts on repetitive manual processes



Security Automation – saving time and managing the risk of manual tasks

Security operations are no stranger to automation – particularly in areas such as remotely deploying customer content or signatures from security vendors, blocking command and control to malicious IP addresses or removing rogue files. But when it comes to detection, there is still much work to do.

The NTT Security 2017 Global Threat Intelligence Report showed that nearly 21 percent of vulnerabilities detected in client networks were more than three years old. More than 12 percent were over five years old, and over five percent were more than ten years old. Results included vulnerabilities that were from as far back as 1999, making them over 16 years old. This is for vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 4.0 or higher. These findings not only demonstrate the scale of the security operations task, but also show the opportunity to re-focus resources from repetitive to higher impact tasks that would change an organization's risk profile.

Even in the face of increasing pressure on time and resources, some processes are rarely considered for automation. These include incident response tasks such as isolating infected machines from the network, shutting down systems and taking them offline. This may reflect the hesitation around the impact of automation on business as usual. For automation solutions to not only work, but to give confidence, they will have to follow exactly the same steps an analyst would take to analyze and action a cyber threat. This implies that if you can train a human to carry out an investigation, it should be possible to codify the same logic into an automation system and potentially perform it faster.

And when it comes to considering automation, we cannot ignore that there will be a 1.8 million shortage of information security workers by 2020.[1] The brutal fact is that without changing our resourcing model, very few organizations will have enough skilled people to analyze data and turn it into actionable threat intelligence.

1. More threats, fewer experts - there is a growing skills gap. How will you manage?

Security Orchestration requires standardization for better, faster decisions

Ironically, the challenge around getting the right information at the right time is one of the potential objections to security automation. SAO solutions are not plug-and-play. In our experience, in order to maximize the potential of security automation and avoid the potential risks of business disruption, organizations need to think carefully about how to standardize processes and plan how they want point solutions to work together. And this review is not just about technology processes.

Typical applications of SAO

Automated policy-based response

If a suspicious file is found on a laptop, the analyst can use the SAO tool to run a playbook that takes a hash of the file for investigation, stops the process from running, and scans the machine for malware.

Other examples:

- Blocking of indicators
- Malware analysis
- Phishing investigations
- Indicator enrichment
- Case management
- Alert/event triage

Organizations must consider that different security professionals, even within the same team, may take slightly different approaches to activities such as investigations. Automation is impossible without standardization. One risk within organizations is that different individuals are allowed to collect and interpret data manually and it is not unusual to see very different personal approaches to implementing defensive controls. Automation systems can help organizations address these manual process risks, but this does not mean that machines are consistently infallible.

So how can Security Orchestration help facilitate Security Automation?

Security Orchestration solutions are being used as a way to connect and integrate an organization's different security systems and processes. For many years security best practice has advocated bringing together people, process and technology and this perfectly describes the goal of Security Orchestration. By bringing security operations tasks onto a single platform, security teams can save precious time by stopping the endless movement from one technology solution to another. But again, the real benefits are using orchestration as an opportunity to refine configurations and standardize processes. In this way, orchestration also prepares the way for more effective automation.

In a study by leading German technology magazine Computerwoche and IDG research services, sponsored by NTT Security – 43% of participants reported that Security Automation delivered invaluable breathing space to both teams and individuals to complete more high value tasks.[2]

NTT Security Point of View: The fastest route to effective SAO

Here are five points we advise organizations to consider before investing in SAO:

1. **It is important not to forget people and process before investing in any SAO solution.** Working with a specialized security partner to perform an initial skills and process assessment of any areas where you wish to improve performance can highlight areas of risk, find the highest-impact use cases and lead to a faster, more effective implementation. Leading with a technology investment is unlikely to deliver the best results.
2. **Our consultants advise organizations to start by automating operational tasks rather than analytical or decision-making ones.** This approach not only delivers rapid time savings, but also builds confidence in the solutions.
3. **In the short term, it is unlikely any SAO solution will replace human analysis and contextualization for certain decisions.** Alert feeds need automation and orchestration as this is where the majority of breaches occur and a manual approach introduces risk. On one hand, implementing tried and tested monitoring solutions such as machine learning can help organizations take a more proactive approach rather than just reacting to events. On the other hand, it may be possible to automate shutting down a device in response to an alert, but if the device belongs to your CEO, you may need a second-level check.
4. **SAO can play a part in both data collection and security decision-making.** Investment in this type of technology is not about replacing people, but freeing up these experts to do what they do best. What we all hope as an industry short of skills is that by using SAO to offload some simple decisions to machines, your valuable analysts can use their business knowledge and security skills to react and advise where computers will always fall short.
5. **SAO solutions are still evolving.** As with any technology selection, it is imperative that new solutions are configured correctly in line with business goals, compliance requirements and industry best practice. Making your SAO investment work harder means seeking ways to reduce the complexity and cost of your existing security operations.

2. Computerwoche: Results of the 2017 Security Automation study

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies (NTT Communications, NTT DATA and Dimension Data) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.

For sales enquiries, please visit **www.ntt.com/en/index.html**, **www.nttdata.com/global/en/**, **dimensiondata.com**, or speak to your NTT account representative for more information.