Buyer's Guide for Intelligent Security Automation

eBook

DEVO

Table of Contents

Introduction

This guide is intended to help IT and security buyers evaluate security automation products. It begins with an overview of uses and benefits of intelligent security automation for enterprise Security Operations Centers (SOC). Then it explores the individual capabilities that make up security automation—both generally and for the Devo SOAR platform specifically. Following an in-depth discussion of these capabilities and their applications for threat detection and threat hunting, the guide concludes with a checklist of intelligent security automation features and capabilities.

For more information about security automation and the Devo SOAR platform, visit devo.com.

Why Security Automation?

A shortage of cybersecurity skills, an increasingly overwhelming volume of data, the preponderance of multiple security tools, and the growing sophistication of attackers has given rise to the need for automation in security operations.

As an industry, we know these problems all too well:

ALERT TRIAGE

It is common for a security team to receive hundreds, if not thousands of alerts each day from SIEMs and other security systems that generate alerts. Because these systems typically use fixed rules to define the parameters that generate the alerts, in practicality anywhere from 80-99% of these alerts turn out to be benign or false positives. The problem for SOCs is that it takes too many security analysts to process all these alerts, not to mention the natural human tendency to miss a real incident in such a large volume of noise. It also leads to high levels of job dissatisfaction with security analysts.

Security automation with SOAR can help alleviate the above challenges by automatically collecting and correlating multiple sources of information to remove false positives and increase the productivity of the SOC team by many orders of magnitude.

INCIDENT RESPONSE

Once a security team has verified a breach or a threat that has penetrated their organization's systems, it becomes imperative to rapidly respond and remediate the damage. Typically, this requires numerous manual and repetitive tasks such as creating service tickets, coordinating across multiple tools and with multiple teams, and implementing policy changes and enforcement to stop and prevent similar future attacks.

SOAR tools that integrate with other systems and tools can remove much of the repetitive work, helping incident response teams focus on the most important and critical tasks first.

THREAT HUNTING

Once considered the domain of the elite security analyst, threat hunting is rapidly become a must-have capability for any organization. Attackers are increasingly successful in masking their footsteps and hiding from detection for months at a time. Manual threat hunting is the task of looking through security data on a hunch or an assumption that your organization has been breached, but without any alerts to clue you. This involves an exploratory process of starting with a hypothesis, testing it, moving to another hypothesis, and so on. With an increasing number of threat actor tactics, techniques, and procedures, it has become impossible for even the most skilled analyst to keep up with this process, yet this was traditionally the only effective approach for detecting advanced and unknown threats.

Advanced security automation with SOAR can help correlate billions of security events in a much shorter time and provide security analysts with a much needed boost for threat hunting.

Are you ready for Security Automation?

Many organizations understand the value of security automation but wonder if they are ready to implement a solution in the near term, given their existing IT staffing and workload.

Here's a checklist to help you determine if your organization is ready for security automation now:

ALERT TRIAGE AUTOMATION

- Do you have a SIEM or log aggregation in place?
- Do you have documented playbooks for how to investigate each type of alert?
- Are a lot of the steps in your playbooks repetitive?
- Do you have security analysts in-house manually looking at each alert?
- Can you calculate how much time automation would save you?

INCIDENT RESPONSE AUTOMATION

- Do you have documented playbooks for how to respond to incidents?
- Can you identify steps in your incident response playbooks you would want to automate?
- Do you have an inventory of key systems you would need to integrate with?
- Can you calculate how much time automation would save on incident response?

THREAT HUNTING AUTOMATION

- Do you have any senior security analyst(s) who manually threat hunt?
- Is there a process to capture and codify the techniques used in threat hunting?
- Can you document the techniques?
- Have you considered or tried automating any of the threat hunting processes?

If you answered "yes" to at least three of the Alert Triage questions, three of the Incident Response questions, and two of the Threat Hunting Automation questions, then your organization is most likely ready for security automation.

If you answered "yes" to fewer questions, then you might want to invest in building playbooks, creating documentation and hiring staff before investing in security automation. Organizations vary, and it could be that security automation will still help you address specific challenging areas of your SOC team's operations.

What is Intelligent Security Automation?

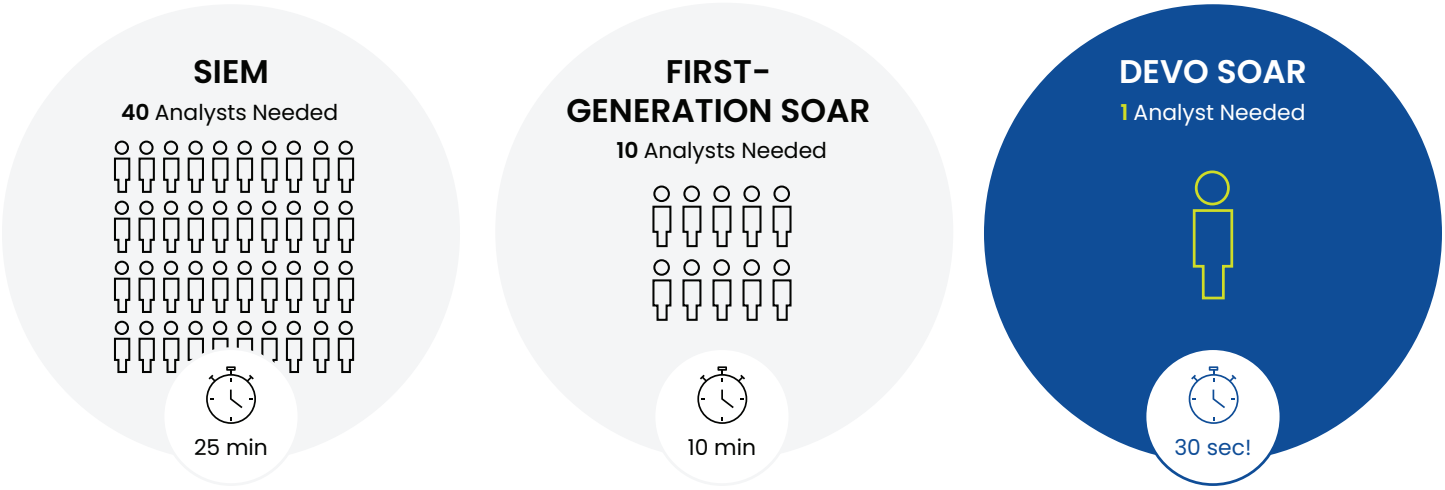
There are many types of security automation products on the market today. Each of them automates some portion of the work of a SOC, the command center for an enterprise IT organization's security operations. The products differ in what specifically they automate and how that automation benefits the SOC and the enterprise overall.

Intelligent Security Automation is a solution that can automate not only the routine steps required for data enrichment and threat remediation but also decision analysis.

To be comprehensive, a security automation solution needs to address two key components:

- SOAR (Security Orchestration, Automation, and Response) automates the performance of routine, low-complexity tasks, such as gathering and enriching data and performing actions to respond to attacks or potential attacks, including closing ports, running anti- virus scans, and adding IP addresses to a blacklist.
- Decision Automation accelerates and improves threat analysis, threat detection, and analyst decision making. Compared to SOAR, decision automation applies machine learning and data science techniques that are far more sophisticated and adaptive. It fully automates alert triage and determines which remediation steps, if any, should be performed in response to a potential threat.

Compare the Effort and Resources Required with SIEM, 1st Generation SOAR, and Intelligent Security Automation with Devo SOAR



First generation SOAR security products began to introduce robotic automation in the SOC. These systems integrate with multiple security tools and use that integration to automatically execute routine tasks, saving security analysts the time and hassle of moving from tool to tool when investigating or mitigating a threat. Security analysts are still required to perform their own threat analysis to triage alerts, but their data collection and threat mitigation activities are streamlined.

One main objective is to automatically perform a list of tasks that a SOC playbook prescribes for investigating or mitigating a possible threat. For example, instead of requiring a security analyst to manually look up the reputation of an IP address and then update a firewall rule if the address' reputation is bad, a security automation product can perform both these steps in a matter of seconds (or less). This automation saves security analysts time and reduces the SOC's Mean Time to Response (MTTR) for this particular type of threat.

While first generation SOAR tools help alleviate some of the pain of processing SIEM alerts, they don't go far enough.

Intelligent automation adds a decision engine to the SOAR approach and automates analysis of gathered data for threat detection and threat mitigation. Comparisons and deep correlations that analysts normally have to do themselves, sometimes over hours or days, are automatically performed in a fraction of the time. Analysis can be performed instantly, not just for a few incidents but for thousands at a time. By analyzing alerts and eliminating false positives, intelligent automation fully automates the end-to-end alert triage process, requiring far fewer resources, and significantly improving threat detection efficacy while reducing the MTTD or "Dwell Time".

Intelligent automation also improves the morale and efficacy of SOC teams, especially those who struggle to process alerts from multiple security systems such as SIEM systems, UEBA (User and Entity Behavior Analytics) systems, Phishing inboxes, and any other systems that generate large volume of alerts.

Key benefits of Intelligent Security Automation

Intelligent security automation delivers these key benefits:

- **10x Force Multiplication**
  Compared to reliance on SIEM or first-generation SOAR tools, Intelligent Security Automation can process 10x the volume of alerts in a fraction of the time required and free Level 1 analysts completely from the drudgery of alert triage. Automating the decision analysis is a key component that enables end-to-end automation and frees analysts to focus on more critical, creative and thoughtful tasks.

- **More Effective Threat Detection**
  Deep correlation and other AI techniques enable SOC teams to detect threats that traditional manual investigations overlook. In addition, threat detection techniques leveraging Machine Learning become more accurate and effective over time by automatically refining algorithms based on success and error rates and applying input from security analysts. Intelligent Security Automation enables SOCs to make the most of their security analysts' expertise, while automating work for speed and efficiency.

- **Improved Job Satisfaction**
  Intelligent automation also benefits any person or organization responsible for recruiting, training, and retaining skilled security analysts. Why? Because it transforms the daily work of analysts, eliminating the time-consuming work of investigating countless alerts that turn out to be meaningless, and freeing them to spend more time on intellectually engaging work such as threat hunting.

- **Automate Complex Processes**
  First-generation SOAR solutions, which rely on basic "If-Then" logic, are incapable of automating processes that require sophisticated logic and analysis. By supporting more complex analysis, Security Intelligent Automation solutions provide a more powerful automation engine that addresses the complexity and sophistication of real-world situations and processes.

The 3 key pillars of Intelligent Security Automation

How do Intelligent Security Automation systems work? There are three key pillars of functionality that an Intelligent Security Automation platform must provide:

Data Enrichment **Decision Analysis** **Response & Remediation**

Let's discuss each of these areas in turn.

DATA ENRICHMENT

Enterprises are awash in security data. Nearly every IT system produces a log file. All those log file entries can be collected and correlated for analysis.

In addition, there are Intrusion Detection Systems (IDS) monitoring network traffic for suspicious events and raising alerts of their own. And there are other security systems — everything from Data Loss Protection systems monitoring email and other network protocols for the unauthorized transmission of protected content to firewalls and User and Entity Behavior Analytics (UEBA) systems.

But event reporting and log files are merely a first order of security data. To make sense of all these events and log entries, the SOC needs context. Analysts need to know not just an IP address, but an IP address' reputation. They need to scan email attachments for malware. They need to scan network transmissions and files for malware, comparing data patterns to known signatures for viruses and other malware.

When data is enriched with context like this, it becomes much more useful to SOC teams. That's why data enrichment is a key capability of true SOAR and intelligent security automation systems.

To achieve this enrichment requires a rich library of integrations, as well as open APIs and a framework to easily create new integrations. For example, to check IP address reputations in real time, a network monitoring system or a SIEM system needs to be integrated with an IP address monitoring service. Similarly, to scan email attachments for threats requires integration with malware scanning services.

Data enrichment ultimately depends on the breadth of integrations available and the ease with which new, valuable integrations can be built.

DECISION ANALYSIS

Decision analysis is a capability unique to the Devo SOAR platform, distinct from other SOAR solutions. The Devo SOAR platform is a state-of-the-art SOAR system married to an ML-powered decision engine to perform intelligent automation in the SOC.

Decision analysis means analyzing security data in real time and determining whether or not a genuine threat exists. Decision analysis improves the decision-making capabilities of the SOC in three ways:

- **Depth of Analysis**
  Automating threat analysis enables the SOC to analyze hundreds to thousands more threats per day. In large enterprises, literally billions of IT events are captured every day, far too many for human security analysts to inspect manually. Applying AI techniques, a decision analysis engine can deeply analyze and correlate relevant security events and alerts, removing false positives and detecting threats that would have otherwise gone unnoticed.

- **Speed**
  Running at machine speed, a decision analysis engine can analyze data and correlate thousands of disparate events in real time, buying the SOC valuable time for remediating threats.

- **Accuracy**
  A well-designed decision analysis engine can detect and diagnose threats far more accurately than an analyst, who often has to fall back on intuition. In practice, a decision analysis engine is capable of recreating the expertise of a Level 3 analyst (the most knowledgeable and experienced level of analysis in most SOCs). To achieve this accuracy, the engine needs to understand what is normal user, system, and network behavior in a specific enterprise. Analyst input can help refine the engine's understanding of normal behavior. Then, using sophisticated algorithms and self-refining learning techniques, the engine can analyze data and quickly identify threats, reducing both false positives (benign events that have been flagged as potential threats) and false negatives (true threats that have been mistakenly flagged as benign).

RESPONSE AND REMEDIATION

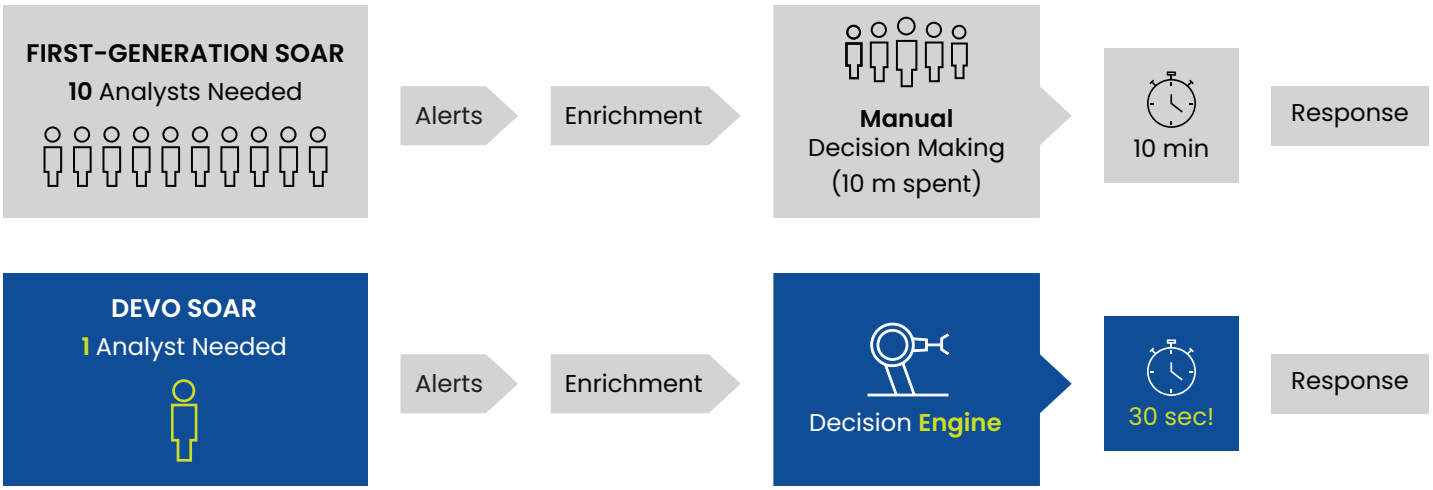
The work of SOCs is responding to and containing incidents. Response and remediation features can help automate this important work.

Typically, a response playbook contains a series of steps and decisions to be followed in response to a particular type of alert or violation of a rule. Originally, most of these steps were manual operations. As recently as five or ten years ago the playbook itself might have been a printed document. Today, playbooks are digital, and many steps are performed automatically by SOAR systems.

However, without an intermediary decision analysis phase between data enrichment and response, these automated responses may misfire, causing more harm than good. Not recognizing patterns that AI-driven analysis would have detected, they might misconstrue benign activity as a threat and shut down business-critical services. Or they might quarantine important files, wrongly suspecting that they might be dangerous.

SOCs can trust automated responses more easily when the most advanced decision analysis available has been applied to guiding those responses, supporting business-critical services while accurately flagging and shutting down malicious activity, no matter how carefully disguised by attackers.

The Devo SOAR platform automates the decision making that is missing from first-gen SOAR solutions.



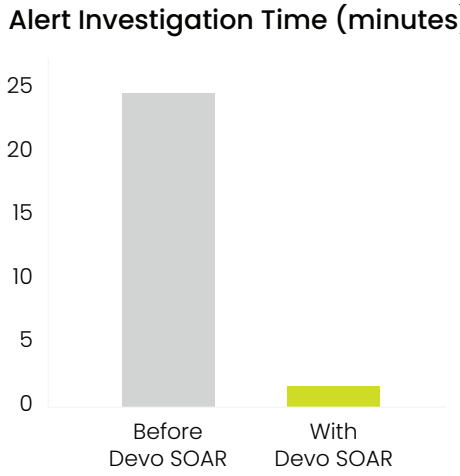
Case study: Top 10 Bank

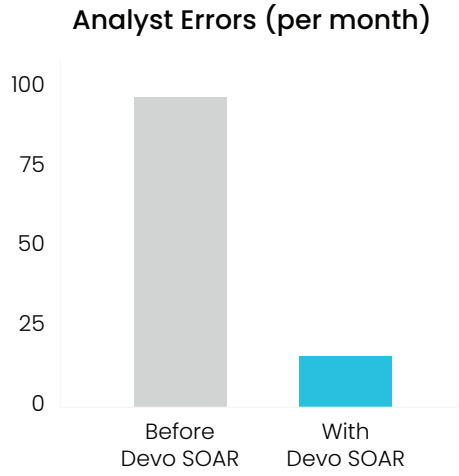
A top 10 bank's experience with Devo SOAR demonstrates the benefits of Intelligent Security Automation for reducing the workload in a SOC and improving the overall security resilience of an enterprise.

Each month, a single playbook generates about 700 malware alerts for the SOC at this bank. Of these 700 alerts, on average only 3 turn out to be indications of real attacks. The remaining 697 alerts are false positives.

False or not, an alert typically takes about 24 minutes of a SOC analyst's time to investigate. In the course of these investigations, security analysts made 98 mistakes (a 14% error rate), mischaracterizing threats or their severities.

Once this bank deployed Devo SOAR, the pace of investigations increased 12X, dropping from 24 minutes to just two. Most importantly, error rates dropped as well, from 98/month to 21/month (a 3% error rate).





Adopting Devo SOAR made the SOC much more effective at detecting true positives, and saved the SOC 256 hours of security analyst time–about a month and a half of a full-time security analyst's workload.

> *Devo SOAR is helping us automate security threat detection processes with decision science automation, using advanced analysis and correlation that is unique and powerful.*
>
> ***- Top 10 Bank***

Common use cases for Intelligent Security Automation

SOCs can apply Intelligent Security Automation to address any type of security threat. However, some types of attacks are more common than others. Here are popular applications of intelligent security automation.

PHISHING

Phishing[1] is a growing problem for SMBs and enterprises. In 2016, 91% of all cyberattacks and data breaches began with a phishing attack[2]

Phishing attacks are popular with attackers for two reasons. First, they require little effort to set up. They can be configured using toolkits with ready-made email message templates. Second, they work. A staggering 7.3% of business and government users were successfully phished in 2016—that's millions of users worldwide. Worse, 3% of users fell for phishing attacks twice, and 1% succumbed three times.[3]

Payoff is quick. Launch a phishing campaign against a company, and the first user usually succumbs in 16 minutes.[4] Attackers can download a phishing toolkit, configure it, and begin harvesting login credentials and possibly ill-gotten funds within hours.

How does intelligent secure automation help thwart these attacks? Typically, organizations have set up a central inbox where employees can forward suspicious emails.

A security analyst then has to manually look at each email and determine if it is truly a phishing attack, and if so take the appropriate response actions.

Intelligent security automation is able to automatically investigate each email, gather relevant enrichment data, and perform deep analysis and correlation to automatically determine whether it is a true positive or something benign.

The Devo SOAR platform has been proven to detect 5 times as many phishing attacks as other SOAR systems. This superior threat detection reduces the chances of a phishing attack compromising login credentials or installing malware. It also reduces the workload of analysts who might have to spend time manually inspecting email for indications of phishing attacks.

1 Phishing is the practice of sending fraudulent email in order to trick recipients into clicking links, revealing credentials, or downloading malware

2 https://www.csoonline.com/article/3268109/phishing/the-rise-of-mobile-phishing-attacks-and-how-to-combat-them.html

3 https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report

4 https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report

Phishing Playbook Example

ENRICHMENT

Local Contextual Scoring
Reduce false positives. Score domains with baselines of YOUR environment.

File Attachment Metadata
Flexible platform used for file attachment parsing and YARA rule execution for limitless metadata.

Detect Look-like Domains
Access powerful data science analytics to detect domain squatting.

Reputating Services
All the integrations you'd expect to include DomainTools, VirusTotal, malware sandboxes and more.

\+

DECISION

Work in tandem with AI
Built-in AI can remember recent analyst decisions to automatically make future triage decisions.

Decision Trees Simplify Complexity
Multiple iterations of enrichment, scoring, and logic can identify special cases like VIP / Executive treatment workflows.

Built-in Machine Learning
Replicate seasoned analyst intuition with custom models to detect malicious and benign URLs.

\+

RESPONSE

Automate Remediation
Update case log while removing malicious emails, blocking domains, creating service tickets or sending communications to users.

VIP / Executive Workflow
Initiate special workflows like sending custom email templates to special support groups.

Phishing Awareness Tests
Automatically enroll confirmed victims in corporate phishing training.

MALWARE

Malware includes all kinds of malicious code, including Trojans, rootkits, and viruses. Malware is delivered primarily by web servers (92.4%) and email (6.3%).[5] This software can attack all kinds of systems, including mobile devices, laptops, desktops, servers, and Internet of Things (IoT) devices, many of which have been designed and deployed with little or no thought to security.

Not only are there more devices than ever to attack, but attackers are becoming more sophisticated in designing their attacks. Knowing that firewalls and other IT security systems can recognize malware content by their "signatures" (digital patterns) within hours, attackers are modifying malware signatures almost immediately after initial use. In 2016, IT security companies were discovering new variants of malware every 4 seconds.[6] Attackers are also creating new file-less attacks (also known as non-malware) that work primarily by injecting malicious code into RAM, often using Powershell or Windows Management Instrumentation (WMI) tools.[7]

Because it can detect subtle variations from normal behavior in an enterprise IT environment, the Devo SOAR platform helps security analysts detect malware attacks and remediate the effects of those attacks quickly.

RANSOMWARE

Ransomware—malware that encrypts data or cripples systems until ransom funds are transferred to a remote account—is now the most prevalent form of malware.[8]

Its popularity makes sense. It's a low-risk activity for attackers that, like other forms of malware, can be leveraged using toolkits, and it promises direct monetization. Instead of luring users into divulging credentials and then eventually gaining access to financial accounts, ransomware cuts to the chase: if users want their data back or their IT systems to be operational, they need to pay up quickly.

Because healthcare systems literally save lives, healthcare organizations have a strong incentive to pay up when they fall victim to ransomware attacks. For this reason, healthcare organizations are now incurring the majority of ransomware attacks.[9] But ransomware is a widespread problem, affecting all industries as well as consumers.

Devo SOAR can help by detecting ransomware before it strikes and spreads through an enterprise. Devo SOAR also helps automate rapid responses to ransomware attacks.

SUSPICIOUS LOGIN ALERTS

Phishing and suspicious login alerts are common at large enterprises, including colleges and universities. A typical attack will masquerade as an official notice from the IT department instructing college or university faculty, staff, or students to re-enter login credentials to update user profiles. The recipients click links and unknowingly enter their credentials in a portal designed to harvest user information. Their accounts can then be used to gain access to other systems or to perpetrate additional phishing attacks, eventually leading to financial payoffs for the attacker.

The Devo SOAR platform can analyze suspicious login alerts far more quickly and accurately than security analysts. By integrating Devo SOAR with enterprise email systems, third-party SMS and messaging systems, and corporate directories, SOCs can gain a powerful tool for detecting and stopping phishing attacks before they compromise login credentials or cause other types of damage.

5 https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report

6 http://www.slate.com/articles/technology/future_tense/2017/02/why_you_can_t_depend_on_antivirus_software_anymore.html

7 https://www.darkreading.com/perimeter/fileless-malware-attacks-hit-milestone-in-2017/d/d-id/1330691

8 https://www.csoonline.com/article/3268109/phishing/the-rise-of-mobile-phishing-attacks-and-how-to-combat-them.html

9 https://healthitsecurity.com/news/healthcare-industry-takes-brunt-of-ransomware-attacks

Case study: Maricopa County Community College District

Maricopa County Community College District (MCCCD) is one of the largest community college systems in the nation, comprising of 10 regionally accredited colleges that serve a diverse study body in the greater Phoenix, Arizona area. Approximately 196,000 students took credit or non-credit courses in MCCCD colleges in 2016-2017.

With a user community that large, MCCCD needs an IT organization that can respond quickly and efficiently to security threats. Phishing attacks, including phishing attacks harvesting login credentials, and brute-force login attempts were becoming a problem for the university.

Every day, the IT organization was receiving suspicious login alerts for about 50 faculty and staff and about 200 students. Each alert took about 5 minutes to investigate. Investigations involved contacting users if they remembered their most recent activity or to confirm that they had tried to connect via proxy or from an unusual location. If students didn't respond within a brief period, administrators would take the safest course of action and reset credentials.

All this activity was time consuming for the two full-time employees (FTEs) in the MCCCD SOC.

To address this problem, accelerating response times to login alerts, reducing IT workloads, and improving security overall, the MCCCD SOC deployed the Devo SOAR Platform, along with the SumoLogic SIEM service for alerts and integration with Google GSuite APIs, CrowdStrike threat intelligence for malware assessment, and Twilio for automated text generation and transmission to users' mobile phones.

Now when the SOC receives a suspicious login alert through SumoLogic, the Devo SOAR platform automatically runs a playbook that analyzes the alert and generates a text sent through Twilio to the user. If the user confirms that he or she was responsible for the suspicious behavior, the SOC doesn't need to take any further action. Without this confirmation, the SOC automatically resets the user's password as a precaution.

By automating these responses to threats, the Devo SOAR platform delivered a 100% ROI within two months. In addition, the SOC benefited from having its two FTEs available for threat hunting and other valuable work, instead of devoting their time to responding to login alerts.

How to evaluate security automation solutions

It should be obvious now that security automation systems need to address all three phases of security analysis:

- Data enrichment
- Decision analysis
- Response and remediation

How should enterprises go about evaluating the capabilities of security automation solutions in these three areas?

One way is to look at their measurable results. Here are suggestions for metrics to be collected and compared

KEY METRICS FOR THE SOC

- **Reduction in Staffing Requirements**
  By completely automating key processes, the security automation platform should be able to exponentially reduce staffing requirements for the SOC or other IT departments.
- **Reduction in False Positives**
  Since false positives consume most security analysts' time, reducing false positives is obviously a critical goal of security automation.
- **Reduction in False Negatives**
  False negatives are lack of alerts in the presence of true threats. By reducing false negatives, a security automation platform is able to alert analysts to important threats that would otherwise be missed.
- **Reduction in Mean Time to Detection (MTTD)**
  MTTD is also known as dwell time. It measures how long an attack was able to dwell undetected on an enterprise network. According to the Ponemon Institute Cost of a Data Breach Study, the average dwell time for data breaches in 2017 was 191 days.[10] That's more than six months of time lingering on a network, giving attackers time to search for other targets, document IT infrastructure, and exfiltrate valuable data.
- **Reduction in Mean Time to Remediation (MTTR)**
  Remediation is the elimination of a threat and the undoing of its damage once the threat has been detected.
- **Reduction in Analyst Workload**
  Like any automation product, a security automation platform should reduce the workload of the department using it.

SCOPE OF AUTOMATION

It's worth measuring the reduction in time spent on various types of SOC activities. Most SOCs and help desks classify tasks according to three levels:

- **Level 1 (L1):** routines tasks that can be easily automated
- **Level 2 (L2):** tasks that require analysis by mid-level analysts
- **Level 3 (L3):** tasks that require analysis by experts

First-generation only automation platforms might be able to automate many L1 tasks but will probably have minimal effect on L2 and L3 tasks.

Because it applies intelligent automation, the Devo SOAR platform is able to automate 95% of analysts L1 tasks, 75% of L2 tasks and 50% of L3 tasks.

10 https://securityintelligence.com/media/2017-ponemon-institute-cost-of-a-data-breach-study/

AUTOMATION SERVICES AND SUPPORT

Many organizations lack the resources and skills to build and automate their own playbooks. It's important to consider the expertise available to help a SOC build end-to-end automation that spans across the three regions of enrichment, decision analysis, and incident response.

The best-of-breed vendors offer a complete "automation on demand" service. Such services are ideal because they provide a complete offering to build all elements of any given playbook, including the decision analysis logic, any required integrations, and all necessary steps for enrichment and response. As long as the SOC team can provide a documented playbook, the vendor will deliver a completely automated playbook in return. This is the best option as it requires the minimal time investment from the SOC team, generally only about an hour of an analyst's time.

In addition, vendors must provide a customer success team to ensure the SOC team is able to make the most of their investment during their use of the platform. This ensures the vendor doesn't leave the customer stranded on their own after the initial deployment.

While many vendors provide some professional services, most do not provide the full automation-on-demand type service described above. These require significantly more investment from the SOC team in terms of both time as well as fees for the services.

TIME TO AUTOMATION

Organizations should determine how much time and effort is required before a security automation platform delivers results.

- How long does it take to build and deploy an automated playbook?
- How quickly can the platform be integrated with security tools and begin delivering analysis that aids with threat detection, threat remediation, and threat hunting?
- How much training and trial-and-error work is required before analysts can begin using the platform productively?

Buyer's checklist of security automation capabilities

ENRICHMENT

- ☐ **Automation Engine**
  Automate manual steps for fetching intelligence.
- ☐ **Visual Playbook Editor**
  Enable easy creation of automation flows, without any coding.
- ☐ **Ingestion Framework**
  Easily intake security events data from SIEMs, UEBAs, log aggregators, cloud logs, and dozens of security products.
- ☐ **Integration Framework**
  Connect to any application or service, including your own custom-built apps.
- ☐ **Agentless Deployment**
  Easy installation and setup by leveraging open APIs.
- ☐ **Reusable Modules**
  Create modules for commonly used steps to easily re-use across playbooks.

DECISION ANALYSIS

- ☐ **Deep Correlation**
  Apply multi-level analysis across dozens of data points to correlate scoring of alerts and events.
- ☐ **Machine Learning**
  Apply cognitive automation to mimic the expertise and intuition of skilled analysts.
- ☐ **Full Explainability**
  Any automated analysis should be fully documented with visibility into the how and why.
- ☐ **Feedback Loop**
  Improve efficacy by easily providing context and expertise via an intuitive human feedback loop.
- ☐ **Analysis Building Blocks (Modules Library)**
  Provides out-of-the-box functions for data analysis such as baselining, spike detection, random string detection, classification, and more.
- ☐ **Customizable Scoring**
  Provides a flexible platform to specify your own scoring logic, rather than a "black-box" approach.
- ☐ **Threat Ranking**
  Ranks alerts and events after analysis and presents a prioritized list.
- ☐ **Scalable Architecture**
  Performing big data analysis requires a strong underlying platform such as Apache Spark.

RESPONSE

- ☐ **Integrations**
  Out-of-the-box integrations are available to connect to any system you need to orchestrate response across. Also see Integration Framework above.
- ☐ **Available Integrations**
  Apply cognitive automation to mimic the expertise and intuition of skilled analysts.
  - **Security tools**
    Such as firewalls, identity management systems, application security, etc.
  - **Case management/ticketing solutions**
    Such as Jira, PagerDuty, Zendesk, RSA Archer, and ServiceNow.
  - **Messaging**
    Such as SMS, email, instant messengers, etc.
- ☐ **Ease of Creating Connections**
  Ability to easily create new integrations to new systems such as custom-built apps.

THREAT HUNTING

- ☐ **Unknown Threat Detection**
  Detecting advanced hidden threats by reducing complex events, filtering out the known good, and ranking the resulting IOCs.
- ☐ **Continuous Detection**
  Automatically evaluate security events 24/7, thoroughly and consistently.
- ☐ **Classification**
  Automate complex classification of data into buckets.
- ☐ **Contextual Configuration**
  Encode domain knowledge and local context easily for more accurate analysis.
- ☐ **Big Data Analysis**
  Explore large volume of data, slice and dice the data from multiple angles.
- ☐ **Smart Operators**
  Easily reuse advanced machine learning and data science algorithms.
- ☐ **Visual Decision Playbooks**
  Visually map and define decision engine playbooks to mimic investigation the way an expert security analyst would do.

Common pitfalls to avoid

- **Integrations that don't work or cannot be customized**
  Ensure that integrations advertised by vendors will work in your environment and can accomplish what you want them to perform.
- **Having to write a lot of Python code**
  Ideally your team should have to write little to no python to get automation up and running. Of course, it is a good option to be able to add your own custom scripts if needed, but this should be the exception rather than the norm.
- **Pricing by number of actions or data volume**
  Any pricing that is predicated on number of actions executed or data volume is bound to become a monumental cost very quickly, something that is hard to predict and budget. Instead look for pricing that's easier to digest and budget for, e. g. based on number of playbooks or users.
- **Playbook libraries that don't work for you**
  Some vendors like to advertise having a large number of community playbooks. Since every environment is unique, it is highly unlikely you'll be able to leverage any playbooks from a "library". Look for vendors that can deliver fully-automated custom playbooks built for you, either as part of their customer on-boarding process or through expert professional services.

Conclusion

It's obvious to CSOs, CISOs, and SOC teams that security threats are increasing in number, sophistication and risk of harm, and that enterprises need to respond with strategic and effective tools and practices for detecting and remediating threats.

First-generation SOAR systems provide useful features for enriching data and performing rote responses to identified threats, but they lack the critical decision analysis that's at the heart of threat detection and threat response. A complete Intelligent Security Automation platform does it all:

- Data enrichment
- Decision automation
- Automated responses

The Devo SOAR platform provides the comprehensive security automation that SOCs so desperately need. The platform automates the sophisticated analysis of L3 security analysts and ensures that playbook remediation work is focused and on target. By providing the decision automation missing from other SOAR systems, the Devo SOAR platform dramatically reduces the workload of security analysts, eliminating up to 95% of false positive alerts and freeing analysts to engage in more productive work including threat hunting.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.