Enterprise Strategy Group by TechTarget

TECHNICAL VALIDATION

Supercharge the SOC With Devo

AI-assisted SIEM/SOAR/UEBA at Speed and Scale

By Justin Boyer, IT Validation Analyst
Enterprise Strategy Group

December 2023

Contents

Introduction

This Technical Validation from TechTarget's Enterprise Strategy Group outlines the evaluation of the Devo Security Data Platform. We validated how Devo uses efficient data ingestion and artificial intelligence (AI) to provide full visibility into an organization's risk posture and enable security teams to efficiently respond to and prevent breaches.

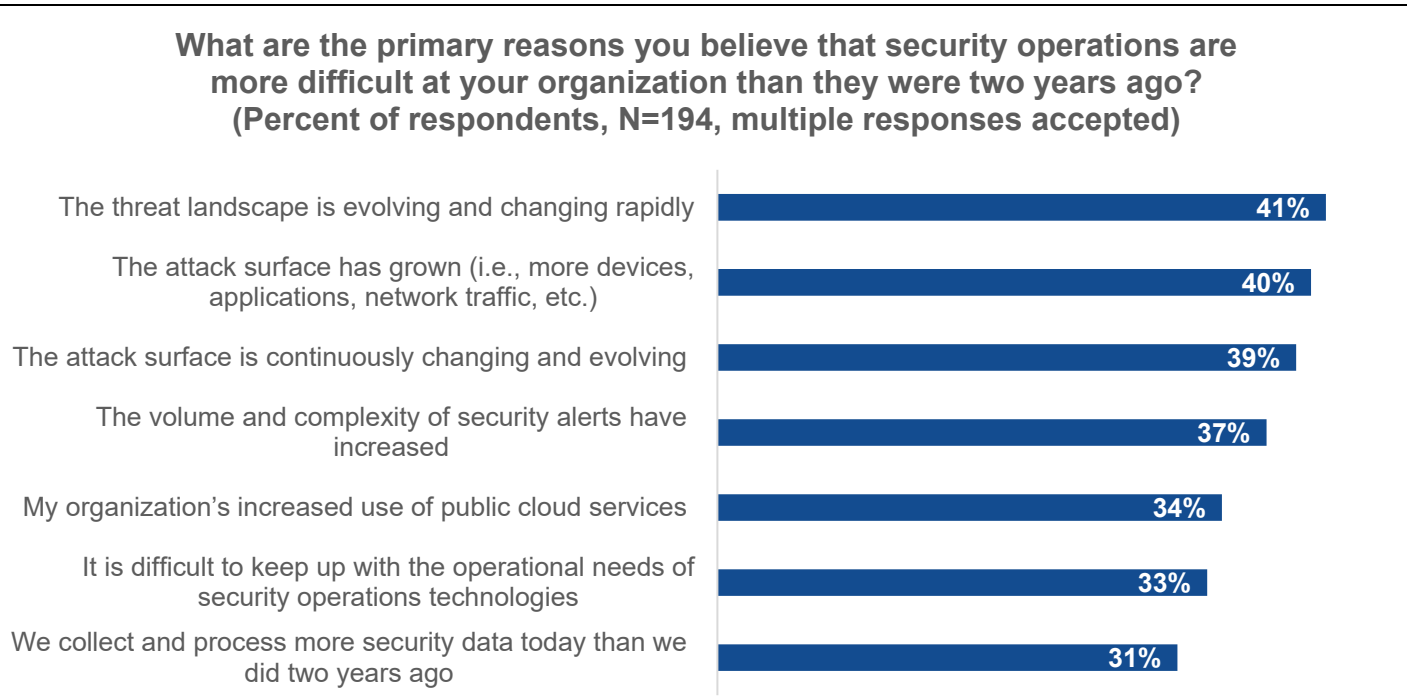
Background

Security operations teams are under increasing pressure. An explosion of data, expanding attack surface, and talent shortages tax security teams as they attempt to keep up with constantly evolving threats.

Budget constraints and regulations also contribute to that pressure at a time when organizations expand into the cloud and continue to use third-party tools alongside custom business applications. This shift has generated a deluge of data and potential threats, creating a challenge for the security teams working to detect and respond to threats and breaches.

According to Enterprise Strategy Group research, most organizations believe security operations are more difficult today than two years ago. Figure 1 shows the top seven reasons for this increased difficulty, with the three most commonly cited reasons involving the ever-increasing and evolving threat landscape and attack surface. Other reasons include an increase in the volume and complexity of alerts and more data being collected than was previously.[1]

Figure 1. Top 7 Reasons Security Operations Are More Difficult



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[1] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.

As these challenges mount, many companies are turning to AI-powered cybersecurity solutions. As AI technologies continue to improve, organizations look to them to help security operations teams make sense of the increasing volume of data, provide effective and actionable alerts, and help automate remediation.

The Devo Security Data Platform

Devo's solution is SaaS-based and cloud-native. The platform includes security information and event management (SIEM); user entity and behavioral analytics (UEBA); security orchestration, automation, and response (SOAR); and autonomous investigation and threat hunting (see Figure 2). Devo's embedded AI enables rapid detection of anomalous activities and comprehensive analysis of patterns across real-time and historical data, empowering organizations to maintain resilience while proactively safeguarding against threats.

HyperStream

The Devo Security Data Platform is powered by HyperStream, its data ingestion and analytics engine, with 400 days of hot data as standard, multi-tenancy support, real-time queries, alerts, and analytics.

Devo rapidly ingests diverse data at any scale, enabling it to deliver real-time results and analytics across the full data set, which improves analyst efficiency and reduces risk across the organization.

Devo Exchange is a curated marketplace where customers can extend Devo's functionality with vetted security and analytics packages that can be installed with one click. Devo Exchange provides security teams with on-demand access to expert-created security analytics, use case-based applications, Devo Activeboards, lookups, and content packs. These features connect security professionals so they can share threat intelligence and leverage the collective knowledge of the cybersecurity community.

Artificial Intelligence

Devo has invested heavily in AI through acquisition and organic research. Through the use of machine learning, Devo excels at analyzing large volumes of data and identifying and maintaining baselines for anomaly detection, such as UEBA. As the models improve, false positives decrease, helping security teams with decreased budgets and staff to keep up with emerging threats. Devo's behavior analytics has expanded to network and cloud behavior analysis, helping security teams adjust to the changing IT environment where more network requests are sent via microservice architecture and cloud-native applications.

The Devo Security Data Platform uses AI to receive feedback and subsequently improve models to provide more accurate results. Devo automates the process of attack tracing and task automation, building and sharing cases, verifying analyst responses, and learning from them. It then shares these lessons with the team and uses this information to inform future responses. This increases detection rates, improves decision experiences, and lowers mean time to repair (MTTR).

Intelligent SIEM

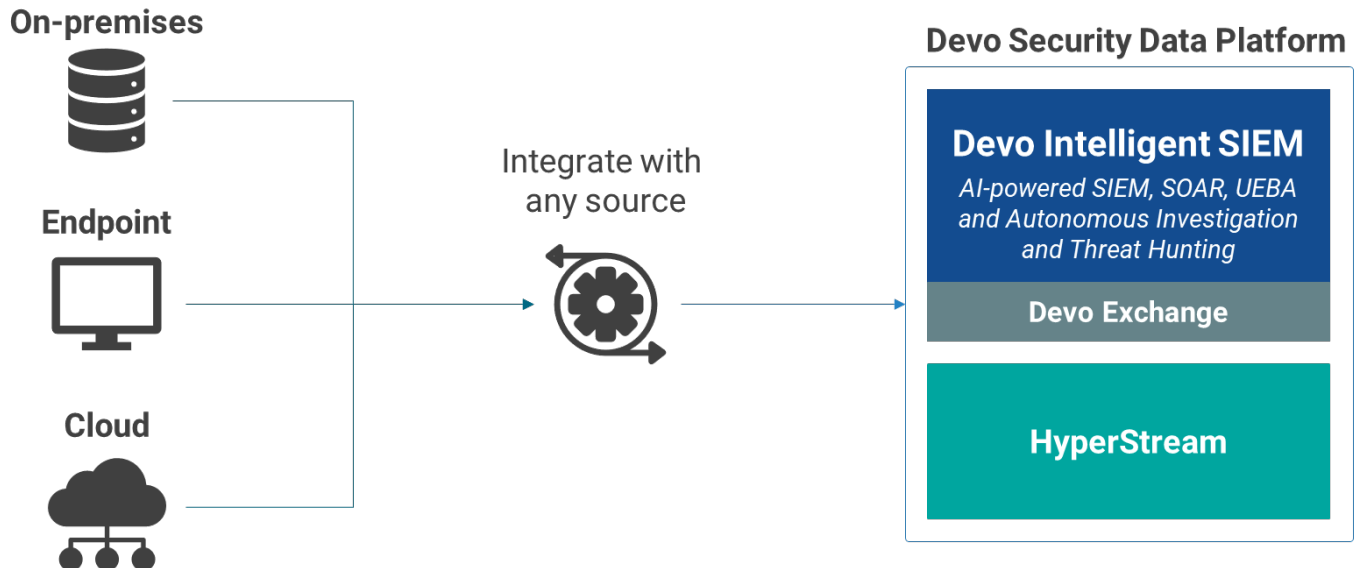
The Devo Security Data Platform's Intelligent SIEM solution is the security operations center (SOC)'s single source of truth. It delivers a singular view of risk posture, security operations, and threat detection, enabling proactive and automated response to real-time threats and alerts. The advanced UEBA engine identifies threats and anomalies across the enterprise, including cloud, network, and user behavior-driven events. Embedded AI, powered by HyperStream, enables rapid detection of suspicious activities and comprehensive analysis of real-time and historical data patterns, so organizations can maintain resilience and actively prevent potential attacks from occurring.

Devo DeepTrace delivers autonomous investigation and threat hunting. DeepTrace's attack-tracing AI improves SOC efficiency by building complete traces of suspicious activity, alleviating mundane, repetitive tasks. DeepTrace

autonomously queries data sets to dig deeper into specific alerts, saving analysts time and effort. It provides analysts with key insights around alerts so they can quickly respond without spending time writing and executing queries.

The Intelligent SIEM includes AI-powered SOAR that integrates with security operations to automate incident response throughout the environment. Devo integrates with more than 300 security and network response tools at the time of this writing. Analysts can create playbooks using a no-code, AI-driven editor that guides playbook development for automated remediation.

Figure 2. Devo Security Data Platform



Source: Devo Technology Inc. and Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group Technical Validation

Enterprise Strategy Group validated the Devo Security Data Platform to evaluate how Devo's data ingestion capabilities, coupled with a multilayered AI engine, helps security operations teams become more efficient and effective in threat hunting and incident management.

Data Ingestion at Speed and Scale

Enterprise Strategy Group validated Devo's data ingestion workflow to evaluate the speed and scale at which Devo can collect, analyze, and alert on data.

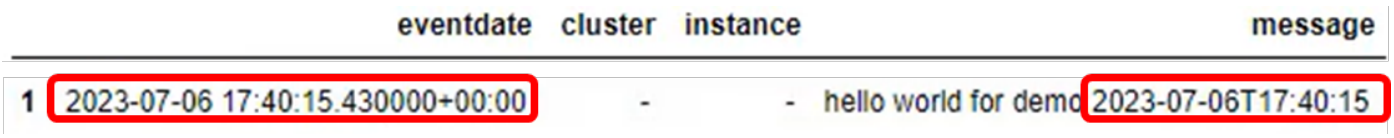
Enterprise Strategy Group Testing

With a highly optimized ingestion pipeline, Devo's HyperStream technology enables efficient data processing and analysis. Devo started as a data platform first before focusing on using that data for security operations. With a data focus, Devo was able to build a platform that optimized large-scale data ingestion and processing. It ingests raw data and uses efficient tagging and data organization to reduce the time it takes to store data and make it usable.

Enterprise Strategy Group observed the processing speed through a script written in the Python programming language run in a Jupyter notebook. The script crafted a "hello world" message with a timestamp within and sent it to Devo. It then printed the Devo transaction log. This test was built to demonstrate how quickly the Devo engine executed the code, compared to the event timestamp automatically generated when Devo processes an event. For

comparison, similar solutions may log an event but then take up to 30 minutes to perform an analysis and provide an alert. As shown in Figure 3, the time it took for Devo to process this request was less than a second. This speed scales to any amount of data, providing a fast pipeline for data processing.

Figure 3. Screenshot Showing Processing Speed of the Devo Engine



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

In an independent study, a Devo customer reported significant performance improvements while realizing cost savings. Table 1 outlines Devo's performance against a competitor the customer previously used in performing a series of common tasks that a SOC analyst may perform in their day-to-day work. This data showed that Devo saves significant time, not only in ingesting data but also in processing, analyzing, and querying it.

Table 1. Devo's Performance Metrics

Use Case	**Competitor**	Devo	Time Reduction
Find a specific host name	7.52 seconds	1.25 seconds	83%
Find anything in a hostname that has a specific text string	More than 5 hours	5.5 minutes	98%
Find a single event_id in the data with a sparse data set	4.48 seconds	.59 seconds	87%
Count proxy accesses by a user over a 24-hour period (over 31,000 users)	More than 5 minutes	20.68 seconds	93%
Count number of users in a 24-hour period	202 seconds	17.57 seconds	91%
Return statistics on client transaction time over a day	171 seconds	19.42 seconds	89%
Simple count of events in a day	40.37 seconds	11.19 seconds	72%

Source: Devo Technology, Inc.

Why This Matters

Modern security operations teams have a difficult task. They must analyze increasing data generated by hybrid IT environments while quickly reacting to possible threats. Tools such as SIEM platforms have been created to help with this task, but many take time to normalize and index data as it comes in before it's used, delaying the time between log ingestion and alerts. To be effective, machine learning models require large amounts of data delivered quickly.

Enterprise Strategy Group validated Devo's focus on speed and scale in data ingestion. Since Devo was founded with a focus on data ingestion and processing, it has an advantage in its ability to analyze and detect

threats. Devo's HyperStream technology forms the core of all its AI processing, and the fast data ingestion and processing capabilities provide the AI models with the amount of data required, at the speed required, to take full advantage of machine learning capabilities.

Devo's fast and scalable data ingestion significantly reduces time and effort for the security team. Additionally, its AI, fed with machine-speed data collection, enables better detections and less alert fatigue, helping even inexperienced analysts to find and remediate potential threats quickly.

AI-driven Investigation With DeepTrace

Enterprise Strategy Group validated DeepTrace, which is used for autonomous investigation and threat hunting.

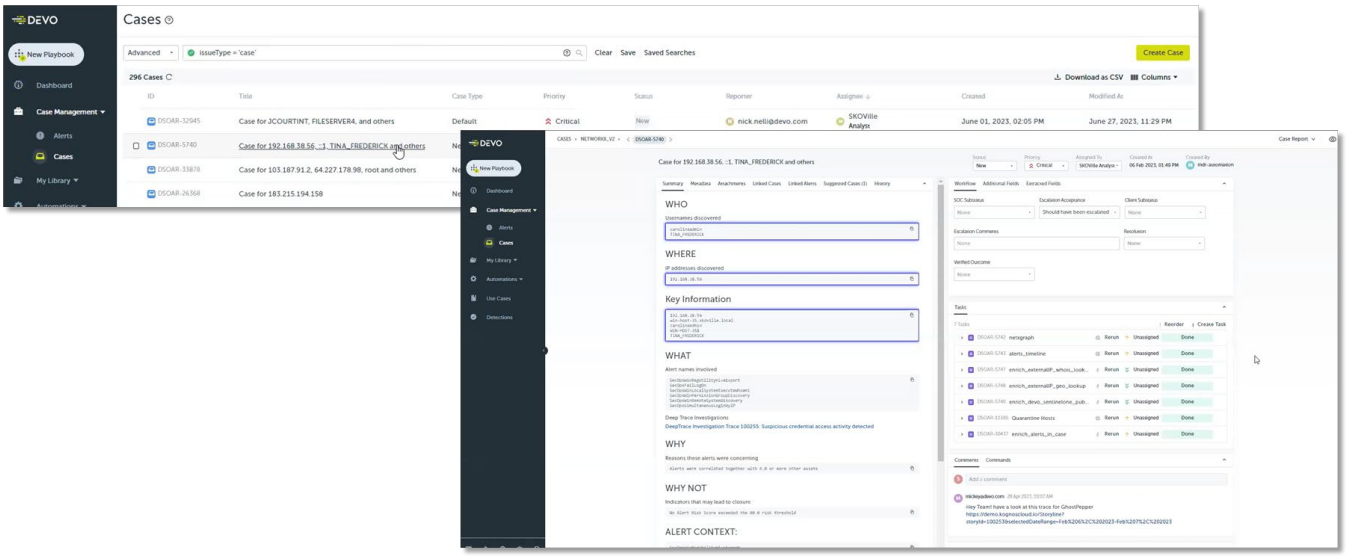
Enterprise Strategy Group Testing

Enterprise Strategy Group's testing was done via remote demo using a test environment to replicate a production application under attack. The simulated attack began when an end user executed a file called FinanceReport.pdf.exe, thinking it was a normal PDF file. Once executed, the exploit achieved privilege escalation, scanned the network to move laterally and find valuable data, and exfiltrated a secretrecipe.zip file with sensitive information within.

We selected a case from the Devo SOAR Case Management screen to analyze this attack. Devo SOAR's Case Management provides analysts with context for any incident, helping them understand what happened, identify which user account was used to perform the action, and decide whether the event indicates a malicious attack. After clicking the case, Devo displayed important details about the specific case, such as the usernames involved and the operations observed.

In this example, we see a failed logon attempt immediately followed by an execution of a "whoami" statement, used to discover the username currently being used to access the system. These were followed by attempts to discover permission groups and remote systems to move laterally. Devo also provides a "Why" section, detailing why this behavior was flagged. This case was also flagged because several different assets saw this strange behavior, indicating that an attacker could be moving through the environment in an attempt to find valuable data to exfiltrate (see Figure 4).

Figure 4. Key Details of a Simulated Attack in Devo's Case Management

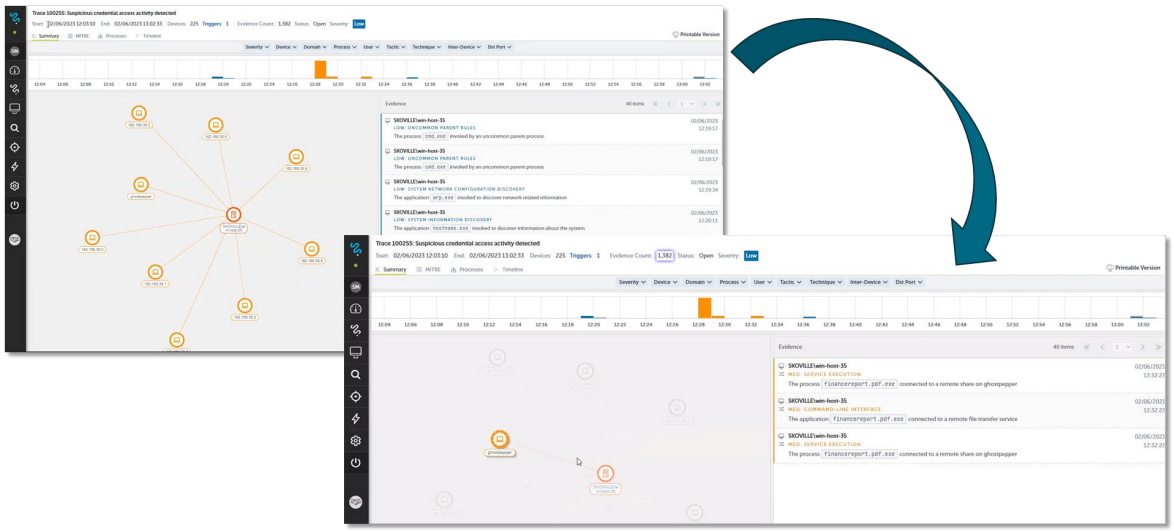


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Next, we viewed the DeepTrace investigation for this case. DeepTrace shows the timeline of the potential attack, the number of devices involved, and other details. It also displays a list of evidence gathered when DeepTrace executed around 1,500 queries without analyst intervention to determine if these alerts added up to an attack.

Finally, we viewed the trace summary window, which featured a trace diagram outlining all the assets the compromised computer connected to during the attack. Clicking on a specific machine (in this case, "ghostpepper") showed us the events that occurred on that specific server, where we were able to see that arbitrary code was executed (see Figure 5).

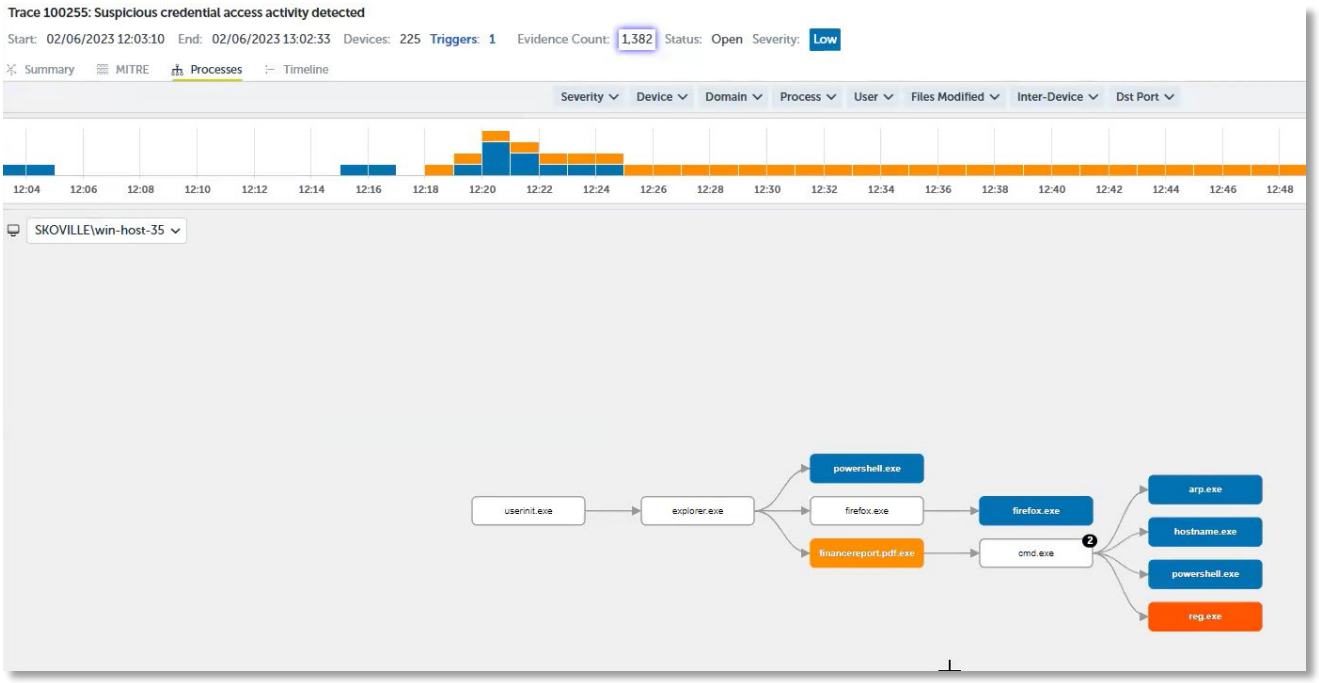
Figure 5. DeepTrace Investigation of Simulated Attack



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

We continued our investigation by selecting the "Process" tab in the navigation bar in the DeepTrace trace summary window. This presented a visualization of the processes detected on the machine during the incident. In this case, it showed a suspicious process called "financereport.pdf.exe" that launched a command line where several commands were run (see Figure 6). This level of detail helps analysts determine the root cause of an attack and take swift action to contain it.

Figure 6. Process Execution Path on a Single Host



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

The increase in the attack surface and the complexity of alerts have made security operations more difficult for many organizations, according to Enterprise Strategy Group research.[2] Gathering data isn't enough on its own. Effective security tools must help analysts find what's truly important within that data so that potential attacks aren't missed. Typically, analysts have to run many queries into the data to try to gather the incremental bits of information that may add up to an attack.

Enterprise Strategy Group validated how Devo DeepTrace simplifies investigation for security analysts. Using attack-tracing AI, DeepTrace autonomously queries all of the data related to a case and collects evidence on the analyst's behalf, greatly reducing the time and effort needed to complete investigations and determine if a series of events constitutes an attack.

DeepTrace works in the background to gather evidence and present it to analysts. This frees analysts to focus on important details and find potential threats instead of spending time querying large data sets. Thus, Devo enables the computer to do what it does best while helping analysts do the same.

[2] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.

Automating Incident Response

Enterprise Strategy Group validated Devo SOAR's playbook creation workflow, as well as how it helps analysts build automated responses into the platform.

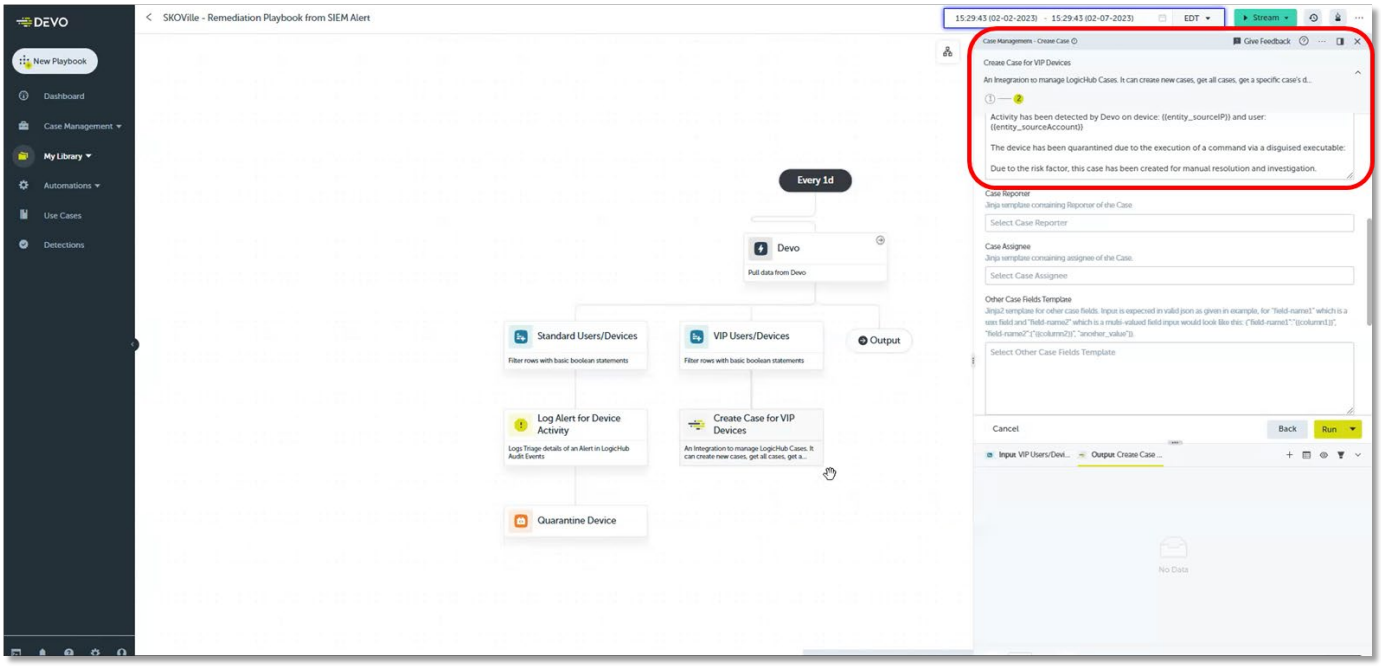
Enterprise Strategy Group Testing

First, we viewed the outcome of a simulated attack within the test environment, noting that it took about an hour to complete the attack.

Next, we viewed the playbook that would've prevented this attack (see Figure 7). The Playbook feature uses data from Devo to filter alerts and respond, in this case, either by quarantining the compromised device or creating a case for an analyst.

The simulated attack alert fired almost immediately after the attack began, which means the playbook would've created a case within seconds (since the attack featured an admin account takeover). This quick response would have allowed an analyst to respond and stop the attack before it reached critical systems.

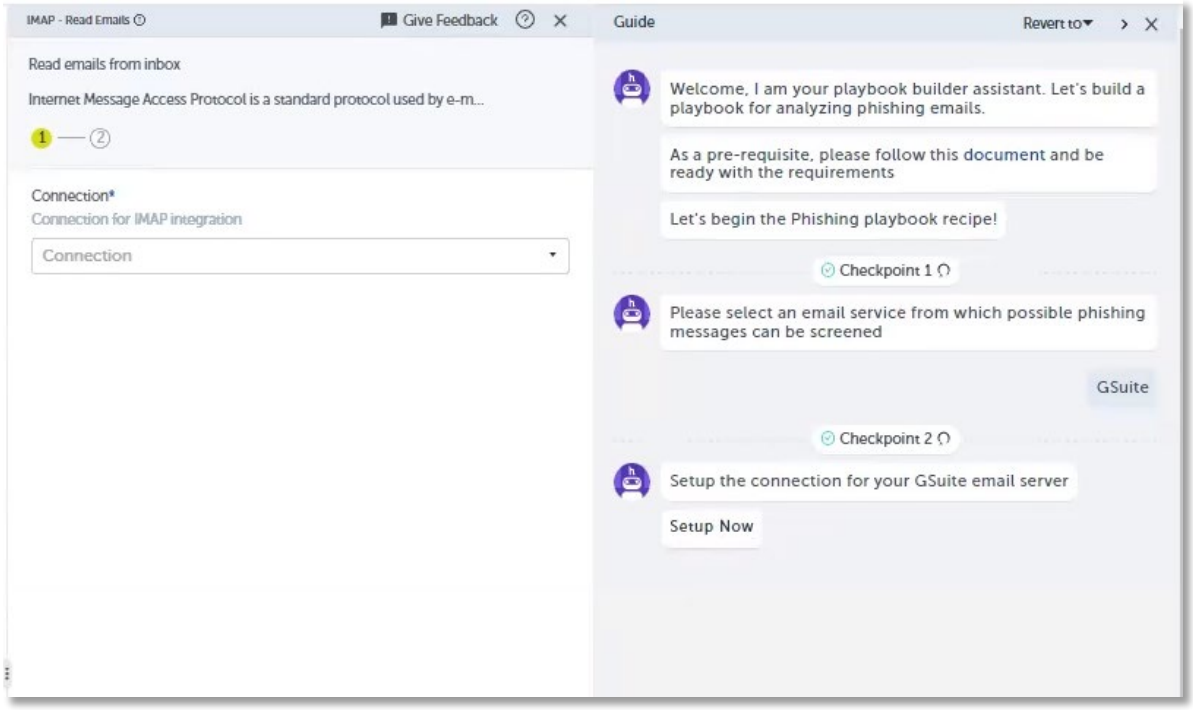
Figure 7. Remediation Playbook Responding to a SIEM Alert



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Devo SOAR also features a chatbot-style playbook creation assistant. Figure 8 shows how to create an email phishing response using the chatbot. By answering a series of questions and then providing configuration details, Devo walks the analyst through the playbook's creation from start to finish.

Figure 8. AI-assisted Playbook Construction



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

Responding to a potential breach quickly and effectively is critical to a security team's success. However, when it takes time to discover potential attacks, quickly finding them and responding becomes a challenge. SOAR solutions help analysts by stopping potential attacks automatically and then providing the necessary data to analysts to decide whether it's truly an attack.

Enterprise Strategy Group validated Devo's investigation and response capabilities. By taking advantage of Devo DeepTrace and the advanced AI within, Devo can find and stop potential attacks and alert security analysts within minutes of the attack's first steps. Additionally, Devo SOAR's AI-assisted playbook creation helps analysts of all experience levels create effective responses to various common threats.

By automatically stopping potentially malicious actions, Devo protects organizations while taking pressure off analysts to be perfect. Using Devo reduces an organization's risk and can help increase the morale and productivity of security teams.

Conclusion

Modern IT environments continuously change at a rapid pace. Modern application development emphasizes frequent updates to small microservices that interconnect to complete a business task. The growing number of tools and cloud services companies use increases the noise, making it difficult for analysts to pick through the data and find potential threats. These factors spread an organization's attack surface across the internet, forcing companies to protect on-prem resources and data in the cloud. Companies require a solution that ingests data quickly and has powerful AI to help find potential malicious activity, stop it, and alert the security team.

Enterprise Strategy Group reviewed the Devo Security Data Platform to determine how it can help organizations overcome these challenges. Devo's focus on cloud-native, high-performing data ingestion provides a lightning-fast pipeline to collect data from across the attack surface. UEBA then analyzes and maps potential attacks, finding behaviors that seem out of the ordinary. Devo DeepTrace saves time and effort by autonomously querying data to build evidence to support cases, helping analysts focus on investigation instead of data gathering. Devo SOAR automatically stops suspicious activity before it can do damage, alerting the security team within minutes of a potential attack. Devo's AI-assisted playbook builder helps analysts of all experience levels build effective playbooks for common scenarios.

The amount of data processing required for effective security across an organization's entire attack surface has become more than human analysts can handle. Devo's AI-driven Security Data Platform, powered by HyperStream, gives security teams confidence that an ally that thinks at machine speed is supporting them. If your security team is challenged by the complexity and size of modern IT environments, we recommend you seriously consider Devo.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com