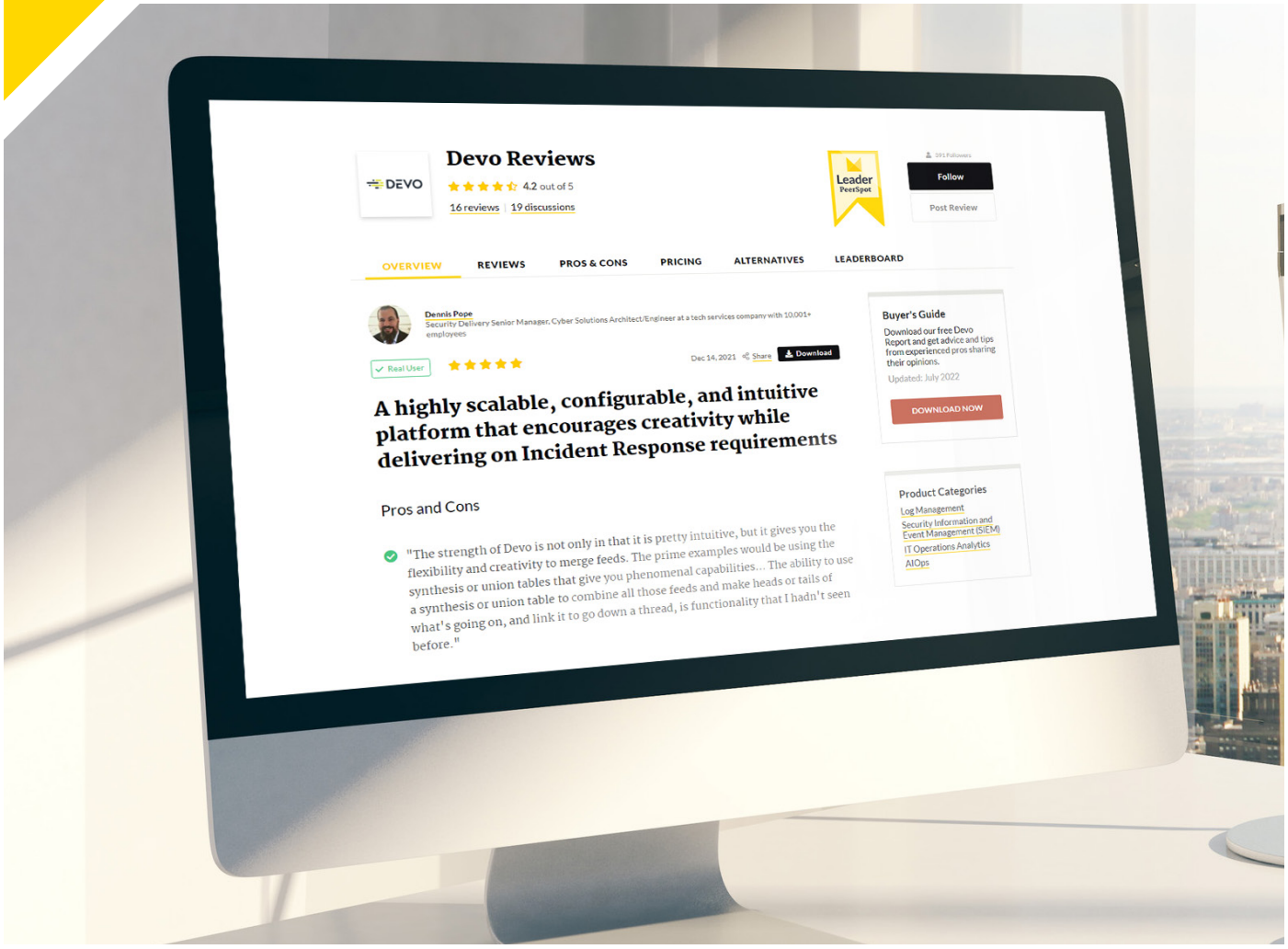
PeerPaper™ Report 2022

Based on real user reviews of Devo

Elements of the Autonomous SOC



PeerSpot

Contents

Introduction

When it comes to running an effective Security Operations Center (SOC), security managers are caught in a difficult balancing act. They need to secure complex infrastructures and applications as they shift to the cloud, achieve digital transformation and manage risk—all while attracting and retaining the best cybersecurity talent. Add in today's fast-evolving threat landscape, with its increased volume of sophisticated attacks, and there is what amounts to a perfect storm: A lack of visibility into complex operating environments, the inability to analyze cloud-scale volumes of data, and the struggle to enhance team performance, which results in lower productivity and higher security risk.

This paper explores how the autonomous SOC is reinventing the way security professionals work. It is based on PeerSpot user reviews of Devo's cloud-native logging and security analytics platform. Combining sophisticated automation capabilities with unlimited data, AI-powered analytics, and access to security expertise and content, the autonomous SOC gives analysts the ability to move from reacting to alerts to proactively identifying the threats that matter most to the business.

Drivers and Benefits of the Autonomous SOC

The need for cybersecurity talent is critical as infrastructure has become more complex and threats grow more advanced. Yet, it has become nearly impossible to find enough people to handle the number of alerts that are generated on a daily basis. In addition, the manual processing of security alerts and investigations is no longer viable.

The SOC's automated processes help to address these challenges by eliminating repetitive tasks, improve analyst efficiency, and reduce the attacker's dwell time. (Dwell time is the amount of time an attacker is allowed to sit on a system after it is compromised and discover more data—then compromise more systems on a network or expand what they currently have.) However, human intervention is needed throughout the process. The autonomous SOC takes automation a step further by utilizing AI to make decisions and determine behavior based on the conditions that exist at the time. In a continually changing attack surface, this is ideal because the system can analyze and process thousands of routine alerts and false positives that bombard the SOC every day.

The autonomous SOC enables security analysts to shift from the role of risk commentators to business risk experts. With more in-depth automation and access to community expertise, security teams gain access to new insights, better detection capabilities, and attack stories that enhance security. This also enables the security organization to keep up with the latest threats while reducing burnout and attrition within the organization.

100%
fidelity in my data

Elements of the Autonomous SOC

The autonomous SOC enables organizations to keep up with the exponential increase in data, the continued shortage of skilled analysts, and the ever-increasing volume and severity of cyberattacks. With an autonomous SOC, teams can focus on their top priority: keeping the organization safe and secure.

A fully autonomous SOC has the following elements:

- **Data:** Instant access to always-hot data at any scale, from any source, which provides high-quality, actionable information about the attack surface
- **Analytics:** AI and real-time analytics help teams identify advanced attacks, accelerate detection and investigations, and reduce response times
- **Community:** Expands user knowledge with access to industry-sourced content and on-demand expertise, strengthening SOC teams' performance and improving the organization's overall security posture

The autonomous SOC provides SOC leaders with access to the proper tools, workflows, and expertise, enabling them to provide an environment that fosters excellence and employee well-being — all while protecting the business.

Devo has made things more efficient

Data Access and Integration

PeerSpot has interviewed many Devo customers about how they utilize the Devo Platform. These reviewers discussed the importance of having unlimited data access and integration in a solution that supports autonomous SOC functionality. For example, the CEO of a tech vendor with over 10,000 employees explained, "We take all that raw data for events, essentially enriching it with the classification service that we have as a unique part of our own service." The automatic enrichment adds classifications that help human analysts respond more quickly and effectively to alerts.

This process is necessary because there is a lot of telemetry in their case. He added, "The telemetry is integrated with a lot of data. You need to look at it in real-time because if you are under attack, then you need to see that immediately: What's going on, where it's coming from, where is the zero patient, etc. This is all the while that you're conducting threat detection. The performance is amazing."

Detections are within seconds

He then remarked, “Devo is a powerful interface and platform which will ingest our data coming from an endpoint protection solution, putting it in a format and dashboard, then connecting tools where you extract them into an intelligence platform, oversight, or security. That’s essentially what we do.” Figure 1 offers a simple representation of this process.

Figure 1 - Data ingest from multiple sources, followed by analytics, enrichment, filtering, and forwarding of selected alerts to SOC analysts.

"The most powerful feature is the way the data is stored and extracted," said a Director of Security Architecture & Engineering at a software company with more than 50 employees. "The data is always stored in its original format and you can normalize the data after it has been stored." This company had previously used McAfee ESM on-premises, but switched to Devo because McAfee had limited correlation engine capabilities compared to Devo and it was difficult to segment customer data.

This user offered a detailed analogy that illustrates the nuances of data management. He said, "If you have ever taken a text file and inserted it into a spreadsheet, the individual fields within that text file now belong in individual cells in the spreadsheet. If a particular set of data should have been in a single cell but was split into two cells, searching for it as a whole becomes difficult. The way Devo stores its data, it never gets separated. It's always stored as original data."

"The way Devo stores its data, it never gets separated. It's always stored as original data."

Read review »

> "All those logs are in one place and we can use one pane of glass to query all of that data."
>
> Read review »

This approach gives his team complete control over how their SOC data is parsed or normalized. He shared, "I don't have to worry about data being mangled as it's being collected and that gives me confidence that I always have 100 percent fidelity in my data." The switch to Devo helped reduce blind spots for his team, having "a very good effect on our ability to protect our organization." With the limitations removed on how data is inserted and extracted, they are able to set alerts on things they were never able to focus on before.

Data integration is what mattered most to a Director of Security at a tech company with more than 50 employees. Devo enables his team to investigate incidents from a single platform. As he put it, "Before Devo, we had to go to individual platforms. For example, if we suspected something was happening, we'd have to go to tool A's logs, and tool B's logs, and tool C's logs. Now all those logs are in one place and we can use one pane of glass to query all of that data. Especially when it comes to security investigations, Devo has made things more efficient."

For a SOC Director at a tech company with over 10,000 employees, what stood out in Devo was the ability to segregate data and perform analytics across multiple data sets. They did not find that capability in other products. He elaborated, saying, "Either everything is mashed into one set of data, and you don't have true separation of that data so you can't, in turn, give customers view sets into that; or it's all separated and you have to do all the work against each silo rather than having a unified view, which is something we have within the Devo platform."

The ability to view data from separate sources in a single view helps with incident response, according to a Security Analyst at a comms service provider. He commented, "We can now get quite detailed data about communication between different nodes. Sometimes you don't see security incidents right away, and sometimes you have to go back. Now, we can go back three months to a specific date and do a really detailed analysis of what happened. Before, we would have to go to five, 10, or 15 different sources, extract the data and then put it together in a different platform."

If the team is looking for abnormalities, having a historical data set and a rich, detailed model of "normal behavior" means they have a greater chance of detecting anomalies that might suggest the presence of a threat or an attack.

"We can go back three months to a specific date and do a really detailed analysis of what happened."

Read review »

Data Analytics

The data analytics process is where the autonomous SOC comes to life. As the software company Director of Security Architecture and Engineering shared, "Devo's cloud-native SIEM [Security Incident and Event Management] has helped improve visibility into threats with its data analytics." This is important to his organization because, as a Managed Security Services Provider (MSSP), they need to be able to analyze the data for their customers and spot anomalies. He added, "The Big-Data analytics features included with Devo are allowing us to write some advanced alerting mechanisms that were not available to us in the past."

For analytics to be effective, they need to be generated in real-time or near real-time. A comms services Security Analyst stated, "We use its [Devo's] real-time analytics, which are very good. It sends alerts; we have some alerts that update every five minutes, or whenever the data comes in. It's really fast."

A Director of Worldwide Security Services at OpenText, a software company, concurred. He said, "Devo provides high-speed search capabilities and real-time analytics, which is important to us because we have built 30-minute SLAs [Service Level Agreements]. In reality, our detections are within seconds and we allow for 30 minutes as a buffer to ensure that we are successful for our clients. To this point, we haven't found any type of dataset or any data ingestions that has prohibited us from meeting our SLAs."

> "Devo's cloud-native SIEM has helped improve visibility into threats with its data analytics."
>
> Read review »

> "We are able to stop the attacker sooner during the attack lifecycle and before it becomes a problem."
>
> Read review »

A Director of Cyber Threat Intelligence at IGT, a computer software company with more than 500 employees, said, "It [Devo] provides high-speed search capabilities and near real-time analytics. These things are extremely important. It's also very easy to pull data into it from various log sources, even if they're custom homegrown apps. The parsers are also very easy to use."

"The solution's real-time analytics of security-related data does incredibly well," said an SVP of Managed Security at Critical Start, a tech vendor with over 1,000 employees. For context, he added, "I think all the SIEM solutions have struggled to be truly real-time, because there are events that happen out in systems and on a network. However, when I look at its overall performance and correlation capabilities, and its ability to then analyze that data rapidly, it has given us performance, which is exceptional."

He elaborated on this capability by saying, "It is incredibly important in security that the real-time analytics are immediately available for query after ingest." This is critical because of attacker dwell time. He related, "For us, having the ability to do real-time analytics essentially drives down attacker dwell time because we're able to move quickly and respond more effectively. Therefore, we are able to stop the attacker sooner during the attack lifecycle and before it becomes a problem."

This user also commented on the importance of historical analytics. He said, "With over 400 days of hot data, we can query and look for patterns historically. We can pivot into past data and look for trends and analytics, without needing to have a change in overall performance nor restore data from cold or frozen data archives to get answers about things that may be long-term trends. Having 400 days of live data means that we can do analytics, both short-term and long-term, with high speed."

A Product Director at an insurance company with over 200 employees also spoke of the importance of historical data retention. He revealed, "Those 400 days of hot data mean that people can look for trends and at what happened in the past. And they can not only do so from a security point of view, but even for operational use cases. In the past, our operational norm was to keep live data for only 30 days. Our users were constantly asking us for at least 90 days, and we really couldn't even do that. That's one reason that having 400 days of live data is pretty huge. As our users start to use it and adopt this system, we expect people to be able to do those long-term analytics."

"We haven't found any type of dataset or any data ingestions that has prohibited us from meeting our SLAs."

Read review »

In many cases, practical analytics in security means data correlation. Threat hunting and attack detection often involve correlating security data from multiple sources. A solution supporting the autonomous SOC should provide for robust data correlations. This is what a comms services Security Analyst found with Devo. He said that Devo "centralizes all our data, enabling us to correlate it and see issues we had never seen before." They use Devo as a SIEM, which in their case translates into Devo functioning as a big-data platform. Figure 2 depicts how this correlation works.

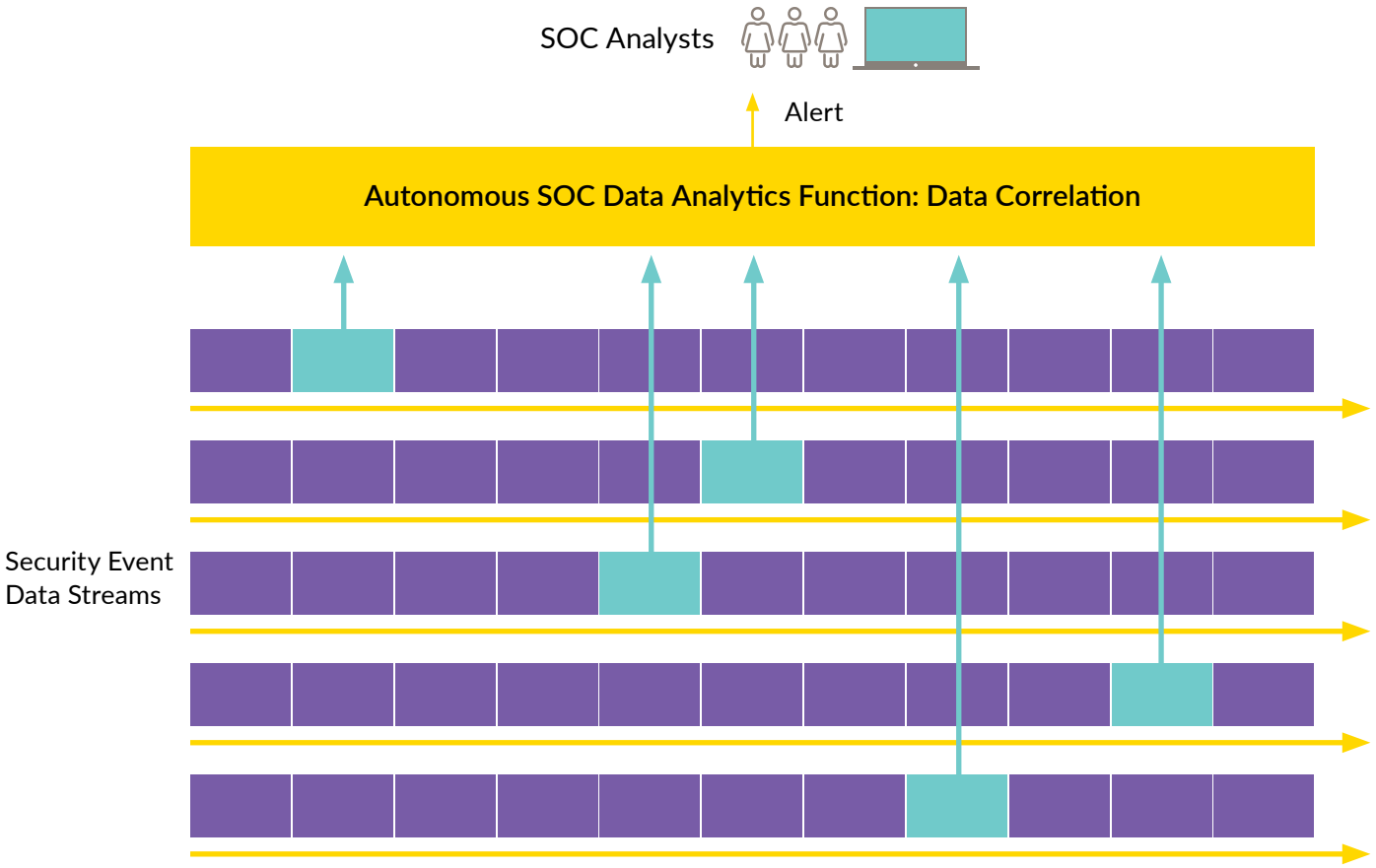


Figure 2 - Data analytics enables the autonomous SOC to detect threats occurring by correlating elements of a threat in multiple event data streams.

"We do store a lot of data centrally, using the solution, and then we analyze it," he said. "The main purpose of the analysis is for security, to detect attacks, abnormalities, and to get an overall view of the health of the network." They did not have a proper SIEM before. Now, they can "look at the data differently because we can access it really fast and with ease. We can experiment. We can also create long-term use cases. We were not able to do that before because we didn't have the correlation and the data in the same place."

Community and Threat Intelligence Capabilities

Managers of the autonomous SOC rely on external information from the broader cybersecurity community. Intelligence about threats, for example, provides crucial context for alerts while strengthening the SOC teams' performance and improving the organization's overall security posture. Devo Exchange extends the capabilities of security teams by providing them with on-demand access to a catalog of content created by Devo, its partners, and the greater community.

high-speed search capabilities and near real-time analytics

The SVP at Critical Start acknowledged the importance of Devo Exchange when he said, "The integration of threat intelligence data absolutely provides context to an investigation. Threat intelligence integration provides great contextual data, which has been very important for us in our investigation process as well."

He went further, explaining that the way the data integrated and made accessible in Devo is useful for his security analysts. He said, "The ability to have the integration of large amounts of threat intelligence data and provide that context dynamically with real-time correlation means that, as analysts, we are seeing events as they're happening in customer environments." Working this way, the analysts have the context of whether an event is related to something that they're also watching from a threat intelligence perspective. This awareness, in turn, helps shape their investigation.

over 400 days of hot data

"I'm all about the Devo Exchange," remarked the tech company's SOC Director. He is particularly pleased that Devo has integrated their community interface directly into their product. He described that as "absolutely fabulous."

Conclusion

The autonomous SOC makes security organizations more efficient, freeing analysts to concentrate on addressing the threats that matter most. The autonomous SOC enables fast, massive data ingestion and management. Working in real-time, or near real-time, the autonomous SOC is able to run AI-based analytics on diverse data sets. Therefore, the SOC can enable rapid, accurate responses to threats that might have previously gone unnoticed. The autonomous SOC also obtains input from the wider security community, augmenting the role of the analyst with additional expertise. As these elements come together, the autonomous SOC provides security teams with the capabilities and talent they need to power more effective cybersecurity operations.

About PeerSpot

PeerSpot (formerly IT Central Station), is the authority on enterprise technology. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

About Devo

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.