All for One, One for All: Bringing Data Together with Devo

Matt Bromiley
It’s time for us to be honest about security tools. At many organizations, security programs—and their associated toolkits—were founded years or decades ago and were originally designed to deal with less-impactful threats. Since then, each year has seemed to be an uphill battle as analysts fight for visibility and better tooling with defensive capabilities. Meanwhile, the organizations they’re in charge of protecting have continued to grow in size, oftentimes leaving security concerns to languish as an afterthought.

The outcome of this struggle is often a security team that is forced to link multiple tools (sometimes dozens) in order to gain visibility into the environment. A recent SANS survey found that an overwhelming majority of organizations use multiple tools for endpoint management alone; some even reported using more than 20 tools. How can one possibly expect to defend an organization adequately with so many tools in use? Even worse to consider: Do these tools work together, and how is their output brought together?

In the past, the answer has been, “Send it all into a SIEM.” However, even if all data sources were piped into a common platform (a massive undertaking in itself), analysts must then sort through everything to find meaning, establish context and perform security investigations. The problem of data acquisition morphs into a problem of data normalization, correlation and action.
In this whitepaper, we will take a look at a platform that is designed to solve these problems: Devo Data Analytics Platform. In particular, we’re going to look at Devo Security Operations, a product built on top of the highly integrated and data-centric Devo Platform. Recognizing that security analysts often face data overload and “analysis paralysis,” Devo set out to bring together data points from a multitude of sources and tools while simultaneously performing correlations and enrichment.

Automated data handling on the back end enables analysts to get down to the job of investigating and protecting the organization. During this product review, our favorite parts of Security Operations helped us to do just that. Regardless of skill level, we were able to get right to the business of investigating. Standout features from our product review included:

- Devo brings multiple underlying tools into one, unified platform, which enables Security Operations to **provide enterprisewide insight from one dashboard**.
- Security Operations goes beyond simply combining data and firing alerts; it provides a way for analysts to **seamlessly investigate and hunt within the environment**.
- Data correlation and enrichment occur in the background, which **automatically adds invaluable context** to alerts, investigations and hunts.
- Devo quickly integrates into analysis and response workflows, providing **400 days of hot data and instant access to context**.

All of these features, brought together in one platform, provide a force multiplier for security analysts. Before you read further, we encourage you to take a quick mental stock of your security tool set:

- How many tools are in your security stack?
- How many tools do your analysts require to defend the organization?
- How is the data from all of these tools collected and correlated? Furthermore, are your analysts empowered or shackled by the data?

As you read through this whitepaper, keep those mental notes in mind. Security Operations enables you to realize the benefits of a security platform while maintaining your current tool set. Furthermore, platforms empower analysts and help them respond to threats quickly. This may just be the change your organization needs. Let’s begin.
Examining a security platform often comes down to one question:

**Will this tool make my analysts' lives easier or more difficult?**

Thus, we often focus on the initial dashboard to understand where an analyst would start the day. Sitting on a platform that is packed with data, the opening screen of Security Operations provides a lot of context at first glance. Figure 1 provides a screenshot of the initial dashboard, which includes multiple useful features:

- A quick display of the most critical and untriaged alerts
- Top investigations
- A self-titled pew pew map of network activity
- Alert metrics, including mapped MITRE ATT&CK techniques and types (observations vs. detections, and so on)

While at first the screen can seem overwhelming, the initial Security Operations dashboard is actually quite succinct and provides relevant data. If the job of an analyst is to assist in defending an organization, then these data points are going to enable them to assess the current level of threats to the organization quickly and accurately.

Another consideration during our review was the value of the tool for analysts of all skill levels and job descriptions. For example, some

**Takeaway**

Many tools do a great job of providing analysts too much data, hindering their ability to consume it effectively. We found that Security Operations provides the right amount of data, enabling analysts to gain context and insight quickly.
security tools provide an extreme wealth of data but require multiple years of training to use effectively. We can tell that Devo worked hard to make sure this was not the case for its product. Security Operations provides capabilities for analysts of all skill levels and job assignments.

Senior analysts or team leads may need to gain insight into the current state of the team's response efforts. By providing highly customizable panels, Security Operations enables them to access a single screen with updates on investigations and alert metrics within the environment. Junior analysts, who are responding to incidents or detections, will be quickly rewarded with context and enriched data points. We'll examine this functionality next.

**Analyst Workflow**

The initial Security Operations dashboard is extremely powerful for displaying data; however, we very quickly wanted to drill down into the relevant data points. The true power of navigating through the Security Operations product comes within the top navigation bar, which we've zoomed in on in Figure 2.

Security Operations breaks data analysis into three high-level categories:

- Triage
- Investigations
- Hunting

We absolutely loved this approach because it helped quantify the various roles that security analysts perform. These tasks often utilize the same data, but analysts consume them in a different manner. Security Operations recognizes this up front, and the quick links to task-specific dashboards enable analysts to get right to work. Note that this dashboard is entirely customizable by each analyst to cater to the data needed up front. For example, some analysts could craft a dashboard that features only alerts and no investigations (for quick triage). A senior analyst, on the other hand, could create an investigation and MITRE-centric dashboard. Figure 3 on the next page shows the Triage dashboard, which is where many analysts will typically start their day.

The Triage dashboard is an extremely insightful way to consume alerts. Notice that while our analysts are examining alerts, this is not simply raw data. For each alert, Security Operations provides the following context and enrichment:

- Source system and IP address
- Priority (Critical to Low or Unknown)
- Type (Model, Analytics, Detection or Observation)
- High-level description with succinct details
- MITRE ATT&CK tactic and technique
- Status
- Alert geography and timestamp details
Here’s what we love about this approach: Security analysts can begin answering questions immediately. Often, alert triage involves lots of data correlation and lookups. Triage may even require utilizing open source intelligence (OSINT) to understand what a particular alert means. However, with Security Operations, most of what analysts care about is up front:

- Where did this threat occur?
- How serious is it?
- When did it happen?
- What attacker techniques were observed as part of this alert?

Security Operations isn’t simply viewing data; it’s also adding enrichment from multiple sources. The Devo Threat Data Service, a service that is essential to Security Operations (and included with it), allows for retroactive and enterprisewide indicator matching sourced from an underlying MISP² instance. We won’t dig into the Threat Data Service in this whitepaper, but we will be reviewing data enriched by its context. Devo Security Operations also performs file analysis capabilities on the back end, via an instance of Viper³ or third-party integrations. Relevant data analysis output is kept within the case, “close” to the alert.

Security Operations also boasts a ridiculously large list of third-party integrations to enrich data beyond what’s included by default. From external threat intelligence to endpoint detection and response (EDR) tools to malware sandboxes, we found the list of available integrations to be wide-ranging and cover a good number of corporate

---

² www.misp-project.org/
³ https://github.com/viper-framework/viper
enterprises. Figure 4 provides a list of the enrichments that were available during our test instance, but this is not a conclusive list.

Having these details means that as soon as analysts begin their day, they can focus on certain severities or alert types. With the automatic mapping to the MITRE ATT&CK framework, analysts can also place investigative priority and value on an observed tactic/technique. For example, detecting Discovery activity may indicate earlier steps of a security breach, whereas Data Exfiltration may indicate a successful attacker was in the network for some time.

Drilling down into a single alert, as shown in Figure 5, provides us with more data and context about the observed activity.

It’s only natural that, when triaging alerts, analysts will want more insight into the detected activity. With some security tools, this can often be an unanswered question. Security Operations is quite the opposite. It provided so much context into an alert that we could triage right from the browser, without needing to acquire files from the suspect system.

Figure 4. Enrichment Options Within Our Test Instance

Figure 5. Details of a Single Alert
As shown in Figure 5 on the previous page, we’re examining a PowerShell Exec Bypass alert. This activity, common in modern attacker toolkits and playbooks, was detected when an external download was detected. Security Operations provides a timeline of the event and relevant command-line details. It’s worth noting that nearly every alert within the Triage dashboard is clickable or interactive, enabling us to drill down where appropriate. For example, as shown in Figure 6, we can hover over the command detection to get details on the full command executed.

A highly interactive alert menu with context and automatic enrichment allows for quick analysis reactions and decision making, while saving precious reaction time. Analysts are no longer forced to track down and correlate multiple data points. However, this is only for a single alert. Where Devo’s alert triage really shines is its capability to see into the past.

### Triage Through History

As we mentioned earlier, Devo comes equipped with a default 400-day history of hot data retention. This means that as analysts work their way through data, the historical context they need to mentally process an alert is readily available. For example, we looked at a detection for an Anonymous Connection, as shown in Figure 7.

![Figure 6. Snippet of Context Menu Showing Full Command Execution](image)

![Figure 7. Context for Detected Adversary Opsec Activity](image)
Figure 7 is not one alert but rather a series of alerts that have been brought together based on various commonalities, including matching connections that include a known TOR exit node. Alert enrichment tells us that this activity is likely Adversary Opsec, based on the types of connectivity observed. Analysts who are curious to see if this activity has been observed before can quickly adjust the date filter within the alert to gain results for a longer period of time, as shown in Figure 8.

This allows analysts not only to evaluate an alert on its severity and mapped attacker technique, but also to add historical context to their reaction decision. For example, how would your organization respond if an alert were fired once a week for the past four months versus an alert fired once every two seconds for two hours? Note that within Figure 7, we also have the option to view Related alerts, which provide entity-based relationships to the current data on-demand thanks to Devo’s fantastic default hot storage parameters. Historical context is extremely valuable when assessing alerts, and Security Operations made it very simple to view this history.

Another gem we saw in Devo Security Operations, which you may not have noticed in your reading, was consumption consistency. In the previous two examples (Figures 4 and 7), we examined host- and network-based alerts, respectively. Each alert came from a different reporting tool. However, because Security Operations sits on top of the Devo Platform, our ability to consume, discuss, analyze and react to alerts remained the same.

Within these two examples lies one of the greatest capabilities of a tool like Security Operations. When tools and data are disparate, analysts have to design workflows for each application or tool set. Although it’s not uncommon for endpoint and network data to be handled in different ways, almost as if they are exact opposites, this could not be further from the truth. Endpoint and network alerts are often generated in unison and provide immense value when analyzed together.

Bringing It Together with Investigations: A Case Study

Of course, simply viewing alerts doesn’t secure an environment. When a true incident takes place, the security and/or incident response team must swing into action to identify, scope and neutralize the attack. Security Operations is right there to meet this demand with Investigations. Investigations are a separate subdashboard of Security Operations, as well as a direct link from any alert being analyzed. You may have noticed in Figure 5 the Add to Investigation button at the top right, which allows analysts to add alerts to an existing investigation or start a new one. We’ll use this opportunity to examine an

Takeaway

Alert source shouldn’t matter to analysis workflows. With combined and correlated data in Security Operations, analysts are able to build a consistent pattern for investigating alerts regardless of source or type.
investigation fully, highlighting some of the additional benefits of the Security Operations product. Figure 9 provides a screenshot of the Investigations dashboard, showing all active investigations within our environment.

At the time of testing, we had three investigations open. Notice that Security Operations provides the most useful data points about an investigation up front: severity, labels and length of time. For this case study, we’re going to dig into a PowerShell execution. Figure 10 provides a screenshot of this investigation, which focused on PowerShell execution on the system 10.52.60.69.
We absolutely loved the way that Security Operations handles investigations. First, as shown in Figure 10, the Investigations dashboard includes key data points, investigation labels, observed attacker techniques and other high-level metadata that provide quick insight into what analysts have observed thus far.

Our favorite feature, however, is the focus on analyst collaboration. You may notice in Figure 10 that the Investigations tab for this case opens up directly into the Comments section, enabling us to see the latest activity in the investigation. We cannot stress this enough: **Whenever an analyst is jumping into a case, they should first read about what has been done.** Understanding what the team has already done and investigated is a crucial step in knowing what to do next. Security Operations allows for capture and retention of institutional knowledge to make multi-analyst investigations painless to execute.

After reviewing analyst comments, we found that all related data points are easily accessible and provided in a way that makes sense. The center panel (shown in Figure 10) is the fastest way to browse through data points, such as related detections, observations and analytics. Figure 11 shows an example of Observations associated with this investigation.

The power of Investigations within Security Operations enables artifacts from multiple data sources to be correlated and brought together in a single investigation. It’s hard to quantify the amount of time this will save some analysts, who may spend more time collecting data than analyzing it. With everything already in one place—as we’ve mentioned before—we were able to quickly consume the data points and walk through the investigation.

**Figure 11. Observations Tied to an Active Investigation**

**Takeaway**

One of the biggest pain points in many security platforms is the inability to foster collaboration between analysts. Security Operations begins with analyst collaboration and enables capture and retention of institutional knowledge.
Within the Investigations dashboard, Security Operations also has links to associated files and impacted entities. Analysts can also tie together related investigations, again allowing for crucial context to be added as alerts are discovered, attacker activity is mapped out and the pieces are tied together. Figure 12 provides a snippet of investigations related to our case study.

Security Operations doesn’t stop with text representation. Figure 13 provides a screenshot of an Investigation Timeline, which can be used to identify the key dates and activity from an entire investigation, stretched across multiple devices and data points.

Security Operations also provides link analysis from detections and observables, allowing for analysts to identify central pivot points or key attacker systems. Figure 14 on the next page provides a screenshot highlighting link analysis among all the evidence related to our investigation case study.
It’s easy to see that we were thoroughly impressed with Security Operations’ collaboration and investigation tracking capabilities. Years of security analysis and incident response capabilities have identified that these concepts—collaboration and tracking—are critical to preventing future threats. Organizations that don’t maintain institutional knowledge are bound to be attacked by the same attacker and/or techniques more than once. Furthermore, new analysts on a team have very little opportunity to consume data from previous incidents. Security Operations helps solve this problem.
Switching to Proactive with Hunting

The final dashboard in Security Operations is Hunting. Shown in Figure 15, the Hunting dashboard allows analysts to go beyond simple detections and begin proactively looking for threats in the environment.

In Figure 15, we crafted a search across endpoint data within the environment to find evidence of PowerShell within a process command line. Security Operations brought back the results, again loaded with tons of context and data points. You may also notice that you can add Hunting results directly into Investigations—yet another benefit to analysts actively responding to incidents.

The power of Hunting is in line with the rest of Security Operations' data-handling capabilities and cannot be understated. Similar to alerts and investigations, hunting within Security Operations allows for quick query crafting across multiple datasets. Notice in Figure 16, for example, the various data points available for querying. How many other platforms allow us to search all of these vendor data points at the same time? We love it!

Whether it's alert handling, incident response or threat hunting, we were amazed at how often Security Operations provided useful and actionable data. We found ourselves no longer concerned with data sources—this was handled on the back end for us. Instead, we simply focused on security analysis, understanding malicious activity and building out an investigative timeline.

Figure 15. Hunting Dashboard

Figure 16. Data Sources Available in the Hunting Dashboard
Closing Thoughts

In this whitepaper, we spent some time examining a solution to the problem of bringing multiple tools together: the Devo Security Operations product, which is built on top of Devo’s highly integrated and data-centric security platform (Devo Data Analytics Platform). In our experience, the capabilities of many organizations are often a hodgepodge of security tools that have been cobbled together over the years. Recognizing this problem, Devo offers an intuitive solution that actually empowers analysts to use their data, instead of simply drowning in it.

Overall, we thoroughly enjoyed getting hands-on experience with the platform. We found that when we, as analysts, were able to free ourselves from collecting and correlating data, we were able to focus on responding to incidents with ease and context. Devo offers an incredible 400-day hot data retention period, meaning we were able to extend our investigations into the past and gain valuable insight into contributing events. The customizations within Security Operations enabled us to tailor workflows as we saw fit and enhanced our analysts’ capabilities.

Bringing together multiple disparate datasets is no easy feat; this task often consumes the schedules of many security analysts, leaving little time for responding to actual incidents. Once data is brought together, it must then be processed and enriched before it can start providing security context. Security Operations made these struggles all but nonexistent and enabled us to focus on the business of securing the organization.

When evaluating a security tool, ensure that your analysts will benefit—not suffer—from implementation. Let your analysts get hands on, ask questions and put the tool to the test.
About the Author

Matt Bromiley is a SANS digital forensics and incident response instructor, teaching
FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and
He is also an IR consultant at a global incident response and forensic analysis company,
combining his experience in digital forensics, log analytics, and incident response and
management. His skills include disk, database, memory and network forensics; incident
management; threat intelligence; and network security monitoring. Matt has worked with
organizations of all shapes and sizes, from multinational conglomerates to small, regional
shops. He is passionate about learning, teaching and working on open source tools.

SANS would like to thank this paper’s sponsor:

All for One, One for All: Bringing Data Together with Devo
<table>
<thead>
<tr>
<th>Course Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Virginia Beach 2020</td>
<td>Virginia, VAUS</td>
<td>Aug 30, 2020 - Sep 04, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich September 2020</td>
<td>Munich, DE</td>
<td>Sep 14, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Australia Spring 2020</td>
<td>, AU</td>
<td>Sep 21, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Antonio Fall 2020</td>
<td>San Antonio, TXUS</td>
<td>Sep 28, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam October 2020</td>
<td>Amsterdam, NL</td>
<td>Oct 05, 2020 - Oct 10, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS FOR500 Milan 2020 (In Italian)</td>
<td>Milan, IT</td>
<td>Oct 05, 2020 - Oct 10, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas Fall 2020</td>
<td>Dallas, TXUS</td>
<td>Oct 19, 2020 - Oct 24, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Tel Aviv November 2020</td>
<td>Tel Aviv, IL</td>
<td>Nov 01, 2020 - Nov 05, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Rocky Mountain Fall 2020</td>
<td>Denver, COUS</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Sydney 2020</td>
<td>Sydney, AU</td>
<td>Nov 02, 2020 - Nov 14, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Krakow November 2020</td>
<td>Krakow, PL</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Gulf Region 2020</td>
<td>Dubai, AE</td>
<td>Nov 07, 2020 - Nov 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>APAC ICS Summit &amp; Training 2020</td>
<td>Singapore, SG</td>
<td>Nov 13, 2020 - Nov 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Diego Fall 2020</td>
<td>San Diego, CAUS</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich November 2020</td>
<td>Munich, DE</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam November 2020</td>
<td>Amsterdam, NL</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>