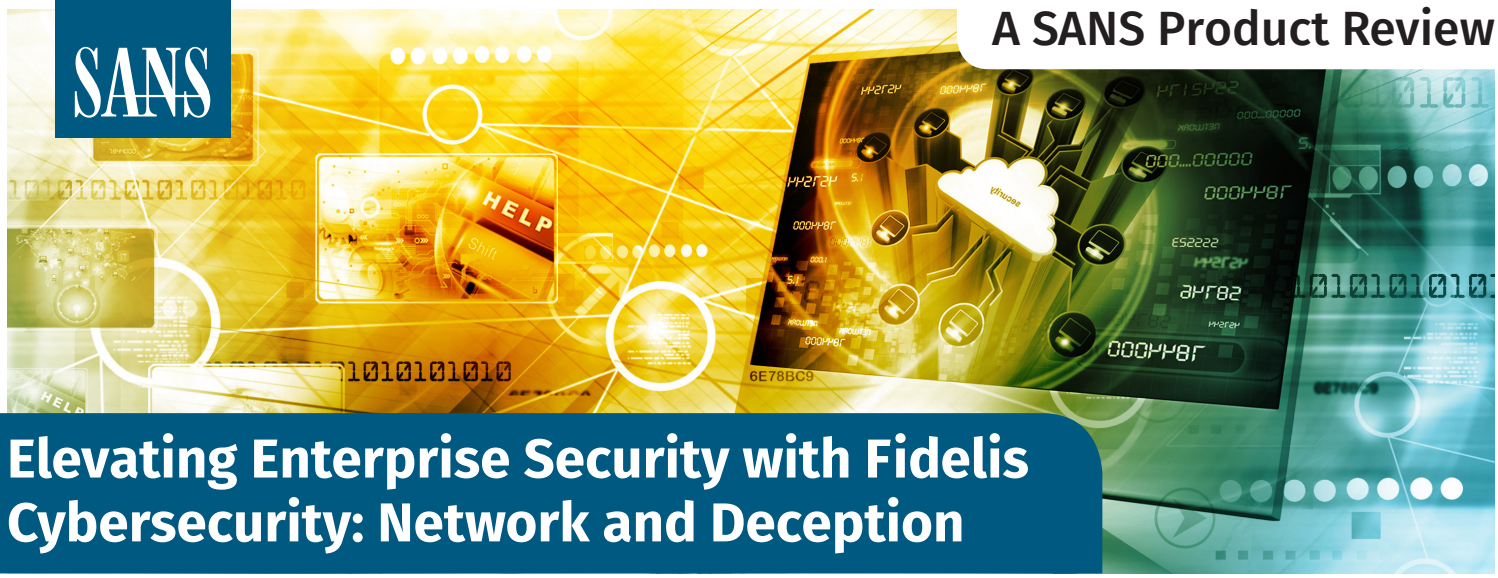
A SANS Product Review



Elevating Enterprise Security with Fidelis Cybersecurity: Network and Deception

Written by **Matt Bromiley**

September 2019

Sponsored by:

Fidelis Cybersecurity

Executive Summary

Securing a modern global enterprise is not easy by any stretch of the imagination. The list of technologies and requirements that contribute to the networks of large organizations is sometimes mind-boggling: cloud computing, on-premises systems, mobile workers, diverse data privacy regulations and laws, and cross-platform device support, to name a few. Over the past few years, these complexities have continued to drive one core concept: **Security teams cannot defend complex networks without holistic, correlative insight into the environment.**

Unfortunately, some organizations still think of their environments as multiple pieces that somewhat work together—user endpoints over here, servers over there. Network operations and desktop operations have unique teams and directives. Information security teams, on the other hand, should not have the luxury of thinking of an environment as piecemeal. Defending an organization requires an understanding that all the pieces work together—and doing so allows security teams to **view the organization's networks the same way threat actors see them.**

In this paper—the first of a two-part series—we take a look at how the Fidelis Elevate[1] platform rises to meet the demands of defending modern organizations. We had a chance to examine multiple aspects of the Fidelis Elevate platform, and in this paper, we focus on Fidelis Network and Fidelis Deception, the integrated components of

[1] Fidelis Elevate™, Fidelis Network® and Fidelis Deception® are trademarks of Fidelis Cybersecurity®.

Fidelis Elevate that allow for insight into network assets and traffic, threats, data loss prevention (DLP) and deception. Through one interface—CommandPost—security teams can review analyses performed by network sensors and activity captured by decoys. This same interface also acts as the interface for Fidelis' endpoint agent, the aptly named Fidelis Endpoint.

Overall, we were pleased with the platform and enjoyed using the interface to gain insight into threats and network activity, observing what Network and Deception were doing behind the scenes. Fidelis Elevate offers several features that make the life of a security team easier—which should be standard for modern, comprehensive platforms. The high points of our testing included:

- Fidelis Elevate offers true *holistic visibility*, with the capability to view the state of security of the entire organization from a single screen.
- Conclusions, derived from the confidence attributes of alerts, offer *correlative alert activity* that enables single-screen investigations.
- *Investigation decision options are available with each alert,* enabling immediate alert handling.
- Fidelis Elevate allows for custom tasks, playbooks and analytics, providing the capability to customize the platform to meet the *organization's needs.*
- Being network-focused, Fidelis Elevate provides the technology to *dig deep into packets,* identifying protocols and applications, and allowing for payload examination.

As you read through this paper, we challenge you to consider whether your security team has the ability to view your organization as a single entity and investigate accordingly. If your team finds itself like so many others—looking at the environment piece by piece—consider how changing to enterprise-level security visibility and security management might help defend your organization.

In the second paper of this two-part series, "Elevating Enterprise Security with Fidelis Cybersecurity: Endpoint Security Capabilities," we explore Fidelis Endpoint and review additional features in the interface as they pertain to endpoint and alert management.

Holistic Visibility

Security teams are extremely successful when they are able to view the networks and assets they defend holistically and in a correlative manner. Therefore, when looking at platforms such as Fidelis Elevate, we look for those capabilities. While our testing did not involve each of the following elements, Fidelis Elevate has sensors available for egress WAN, email, proxy and internal application traffic.

Upon taking the first steps into the interface, the analyst is greeted with multiple views that offer holistic insight. Figure 1 on the next page shows the initial Fidelis Elevate dashboard, which brings information of concern *directly* to the user.

As we look for insights into a *global* organization, we appreciate having the latest threats mapped out on a geographical map, with hover-over capabilities. Note that this is not one of the fabled "pew-pew" maps, which simply show data points between two nations; this map provides a real representation of malicious traffic.

Also included in the dashboard are details, as shown at the bottom of Figure 1, that report the numeric counts of:

- Conclusions with malware (513)
- Assets with malware alerts (34)
- Alerts with malware (14,843)
- Critical alerts with malware (941)

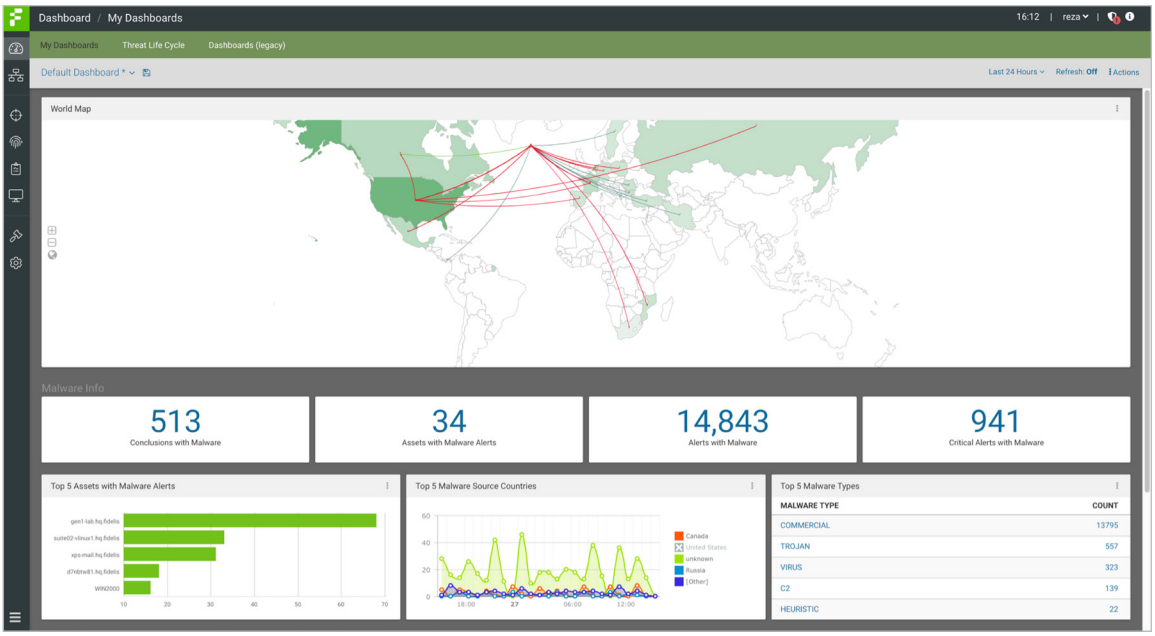


Figure 1. Fidelis Elevate Dashboard

Again, this dashboard brings pertinent information *right to the surface*. Here's what we expect when we load a dashboard: key insights up front. And the dashboard provides that to us. (We examine conclusions and alerts later in this paper.)

Continuing on the topic of holistic insight, just a single click away in the interface is Terrain, which provides analysts with the opportunity to drill down into their environment. Figure 2 shows the details of the malicious traffic we observed during our testing.

Terrain includes two parent categories: assets and analysis. Assets is fairly straightforward. Based on observed traffic, analysts can gain insight into operating systems, subnets and domains, as well as custom tags they can define. As this data is captured via analysis and classification of network traffic, it can provide real-time visibility into what is traversing the wire, as opposed to what the organization thinks is crossing the wire.

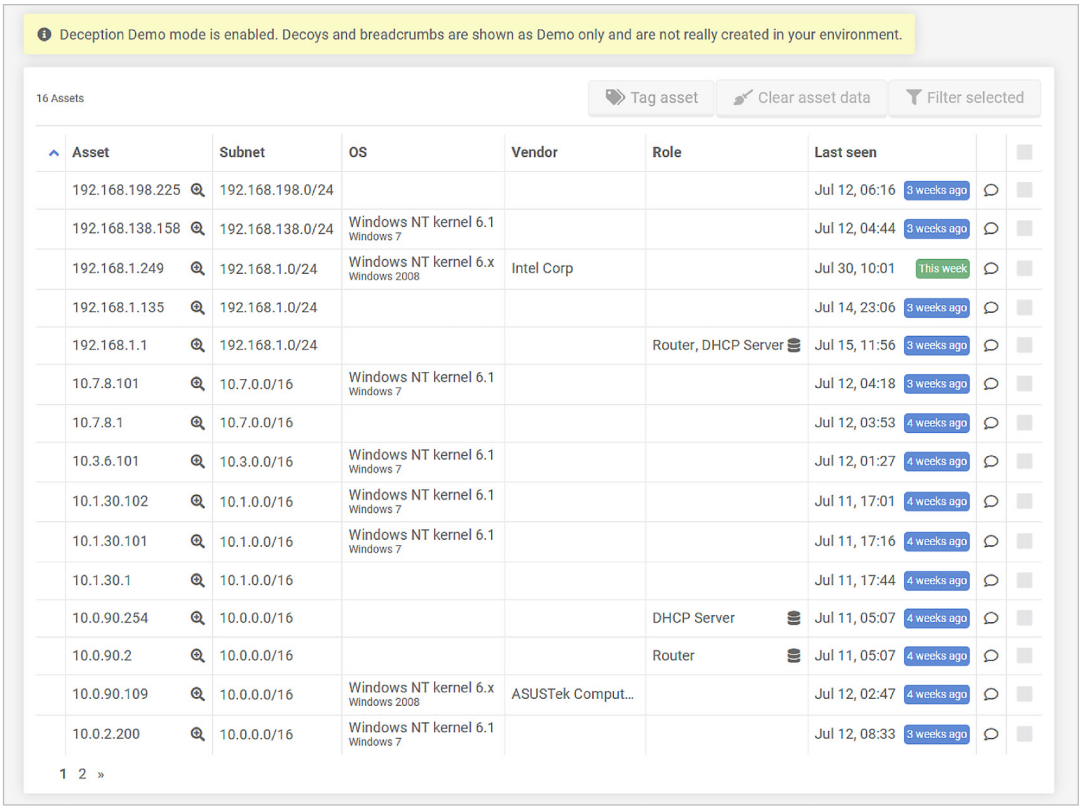


Figure 2. Drilling Down with Terrain

Assets

It's important to note why we consider up-front data to be so crucial to effective security operations. When an organization has immediate insight into its networks, it can make quick, confident decisions. The organization can also rest easier, knowing that all of its assets are represented in a single platform. Furthermore, knowing one's infrastructure is a huge advantage for the organization. Attackers breaching an environment have to spend time and resources discovering an environment, potentially slowing their approach. While automated tools can speed up this process, organizations that know their terrain are often faster at containment and remediation.

This means that analysis on one asset can quickly scale to many assets without leaving the same console. Having separate tools or multiple platforms to manage assets causes a loss of time and efficiency, both of which should be advantages for security teams.

All-in-one platforms also offer organizations the benefit of maturity. When organizations finally start to move from reactive to proactive practices—likely because of integrated and effective security—they can take on more mature and proactive security operations, such as threat hunting. When testing Fidelis Elevate, we found this platform can take an organization from reactive to proactive very quickly.

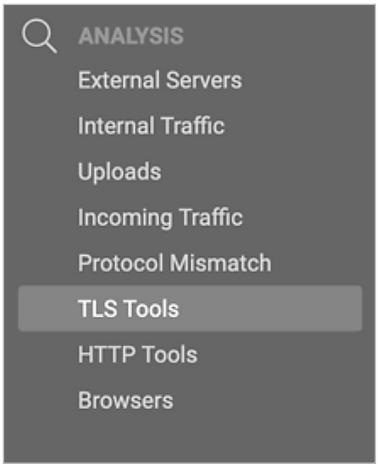


Figure 3. One-Click Insight

Analysis

Below Assets is Analysis, one of our favorite areas. As shown in Figure 3, Analysis offers deeper, one-click insight into multiple areas, including external servers, internal traffic and uploads. Network-centric visibility also includes protocol mismatches, Transport Layer Security (TLS) and HTTP tools, and browsers, which are offered from this menu.

The insight analysis begins with a look at evidence of malicious activities and their frequency in the environment. Figure 4 shows the TLS Tools analysis as an example. We can see that during traffic observation, Fidelis has automatically collected the JA3 Hash (a fingerprinting technique for encrypted web traffic) and performed correlative analysis to identify potential risks.

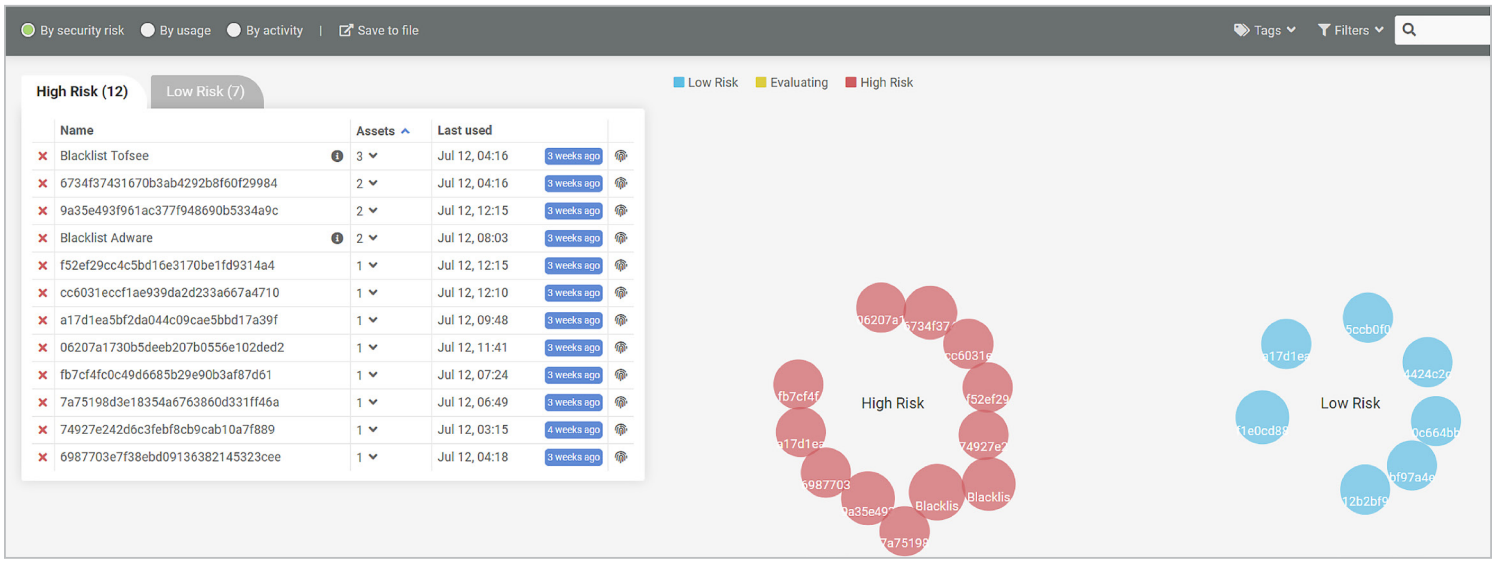


Figure 4. TLS Tools Analysis

But wait—there's more! Within this same section, analysts can also begin to examine the same content with respect to frequency. If we select the "By usage" option from the menu bar, the diagram updates to represent frequency in the environment. See Figure 5.

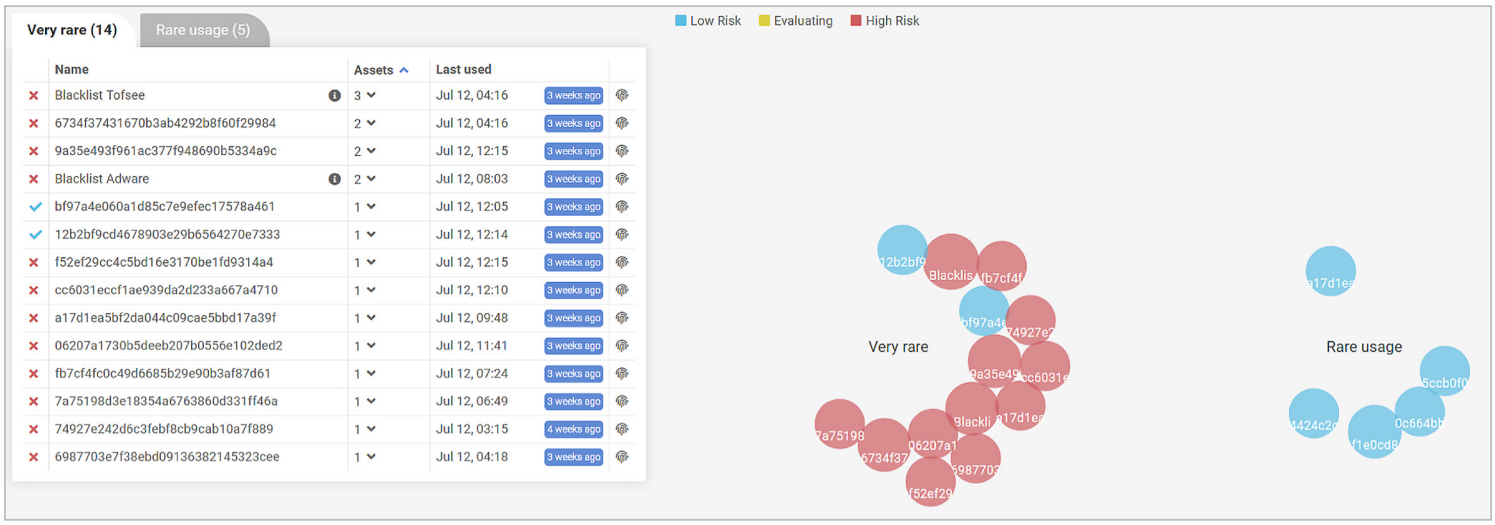


Figure 5. Frequency of Malicious Activity

This was our first step into Fidelis Elevate's capabilities as not only a response, but also a threat hunting platform. During testing we examined only a small environment and limited sets of data. Therefore, our frequency graphs are respective to that test. However, in a large environment, with tens or hundreds of thousands of endpoints, finding the needle in the haystack is often a laborious task. Fidelis simplifies that process, allowing your organization to be proactive rather than reactive.

Investigating with Focus and Determination

While the main dashboard and Terrain provide insight into the environment, as well as data points into frequency analysis in the organization, these features also provide quick links to view alerts. If holistic visibility is the top priority, an obvious second would be the ease with which analysts can move from visibility to triage. Fidelis Elevate makes that process extremely simple.

You may recall from Figure 1, shown earlier, that Fidelis Elevate provides the following three data counts:

- Conclusions with malware
- Assets with malware alerts
- Alerts with malware

These links bring you right to the forefront of suspicious activity that requires investigation. However, these are not unique events; they are instead alternative representations of the same data. Our favorite, from an investigation perspective, is Conclusions.

Conclusions and Alerts

Conclusions are an analyst's dream. The platform automatically searches for similarities among alerts and then collapses them into unified events, all in the background. In our testing, we had 85 alerts, but only 14 conclusions. This difference is due to the auto-collapse, which simplifies the investigation and presents the data with more confidence. Figure 6 provides a list of some of the conclusions we investigated.

In Figure 6, you can see that conclusions are shown with a confidence score of maliciousness, followed by summary details such as malware classification, impacted entities and timestamps. This information provides a high-level snapshot of "what's going on" in the environment. Analysts can use the confidence score to prioritize top conclusions for analysis and next steps.

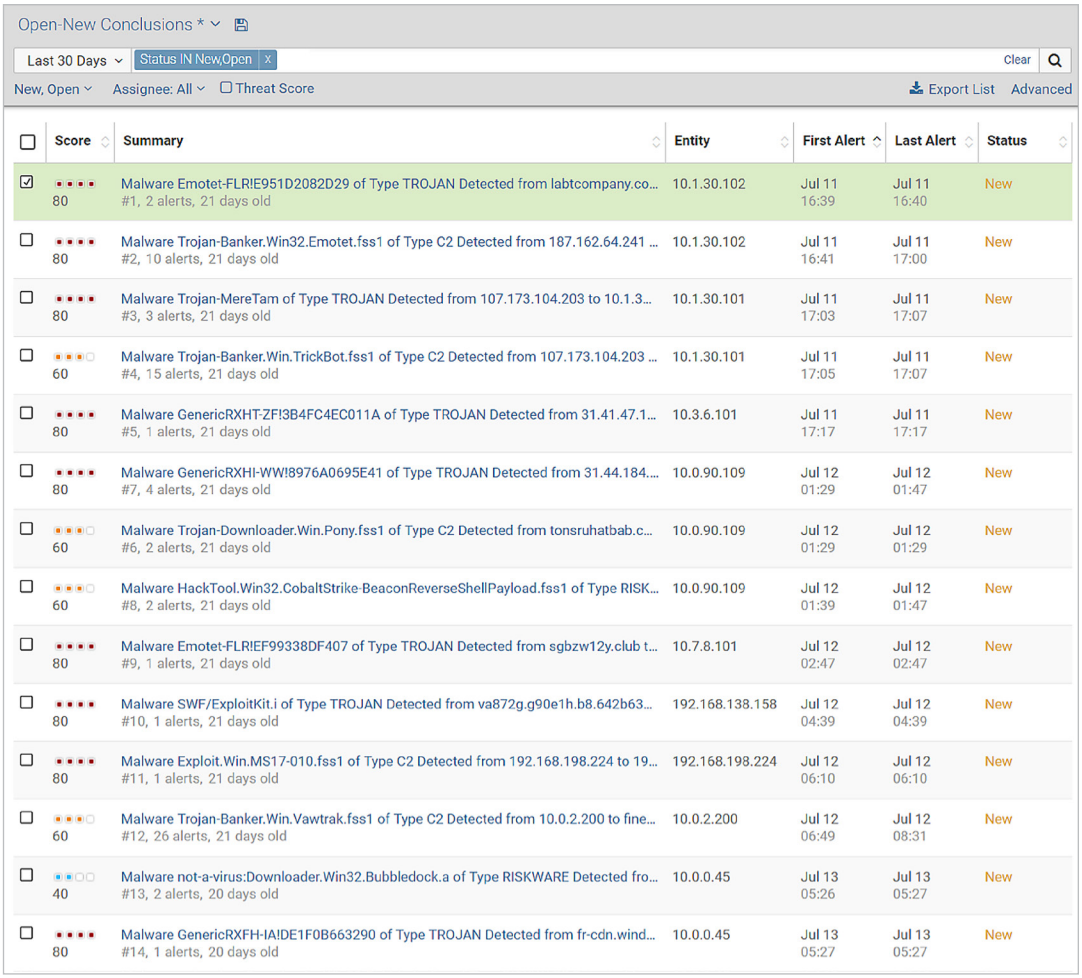


Figure 6. Conclusions

Technical Insights into Alerts

The second analysis section of Conclusions also provides technical insight into the alerts that were collapsed into each conclusion. As an example, let's dig into the first alert shown in Figure 7: a potential Emotet infection.

Notice that Fidelis collapsed two alerts associated with this activity. These alerts

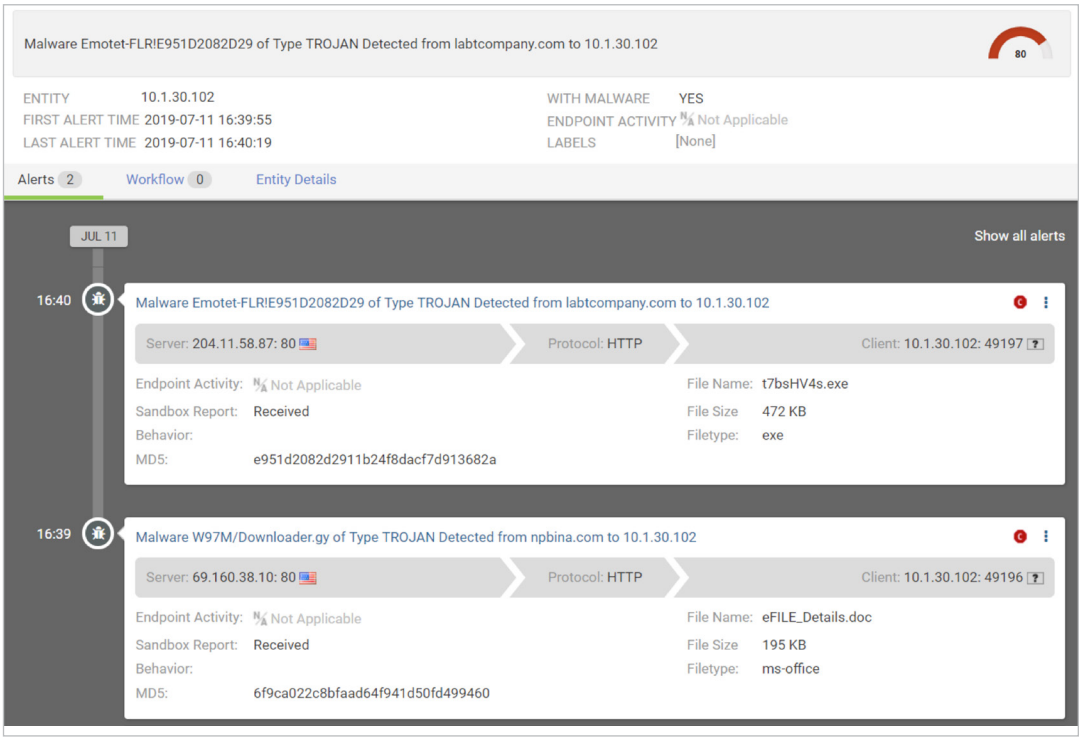


Figure 7. Insights into Alerts

include some common attributes, such as protocol and impacted client. However, the downloaded malware and external IPs differ. Despite this difference, the platform was able to correlate the two alerts and provide a succinct view into the activity. Let's dig further into one of the alerts.

Figure 8 is an expansion into the first alert, for the file **`t7bsHV4s.exe`**, which was downloaded from **`labtcompany[.]com`**. There's a lot for analysts to dig into here—we love this! Again, all the data is in one place, meaning analysts don't have to move far to draw conclusions and make effective decisions.

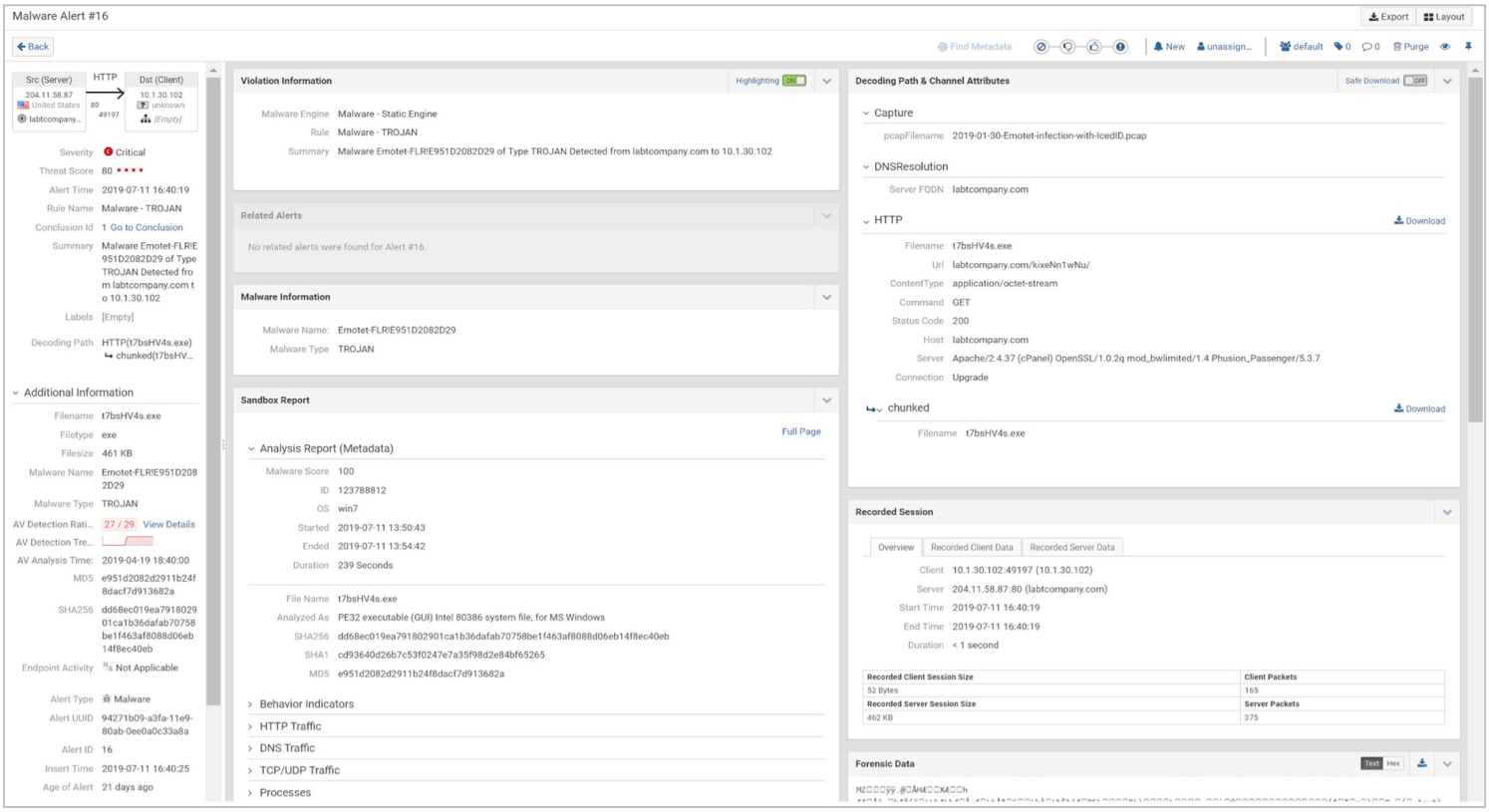


Figure 8. Technical Insights

A few key areas to call out within each alert page, working from left to right, include:

- **General Alert Details**
  - On the left side of Figure 8 are general alert details such as the observed traffic, severity score and conclusion details.
  - The results also include high-level details about the activity, in this case metadata about the file that was downloaded and flagged as malicious.
- **Sandboxing and Malware Details**
  - We enabled automatic sandboxing in our test environment, which allowed for malicious samples to automatically be sandboxed and results provided in the alert.
  - Sandboxing details included specific network and host observations during malware runtime. (We expand on this in the "Built-in Sandboxing" section.)

- **Network Observations**
  - The right-hand side of each alert dashboard provides related network observations. The dashboard captures and displays the URL, related server information and details about the recorded sessions.
  - Furthermore, by clicking the Recorded Session tab, analysts can view the client and server data recorded from the session. See Figures 9 and 10, respectively.

The amount of data contained in each alert stayed in line with the goal of making analysis and enterprise defense more streamlined for analysts. Typically, sandboxing and network artifacts are contained in different applications. This separation forces analysts to perform their own correlation to validate high-confidence threats. Fidelis Elevate brings everything together on one screen—returning that valuable time to analysts. Furthermore, with all the data in one place, analysts of all skill levels can gain more confidence about their threat and incident assessments. This can help them make faster decisions, such as whether to remediate, ignore or escalate.

We found another underlying system we really like: delegation and assignment of responsibilities. This feature includes a Status column (shown in Figure 11), which refers to activity around each conclusion—specifically, has someone opened the conclusion, and is it assigned to an analyst? We're huge fans of platforms that include ticketing and alert-handling capabilities. Upon determining the confidence of an alert, we were able to assign the alert to a specific analyst and track the status of how that alert was being handled. All in one place!

Built-in Sandboxing

As previously mentioned, we took advantage of sandboxing during our testing to determine the granularity of the results and whether they were useful to the analyst. Sure enough, Fidelis Elevate continued to deliver.

As shown in Figure 11, the platform successfully sandboxed the Emotet alert. Results of the sandboxing are provided in groupings such as network traffic, registry or file modifications, and processes. Figure 11 provides an example of host-based artifacts, for example, as they were captured by the sandbox.

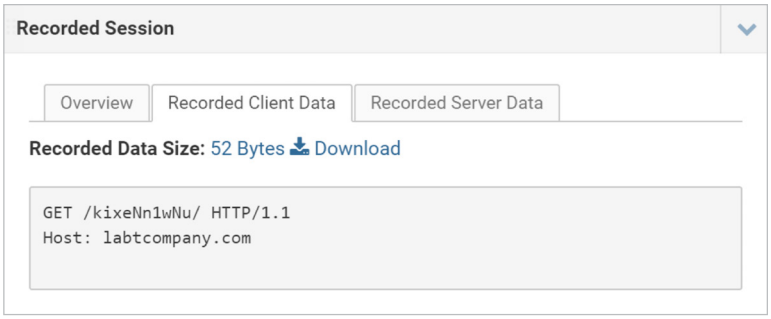


Figure 9. Recorded Client Data

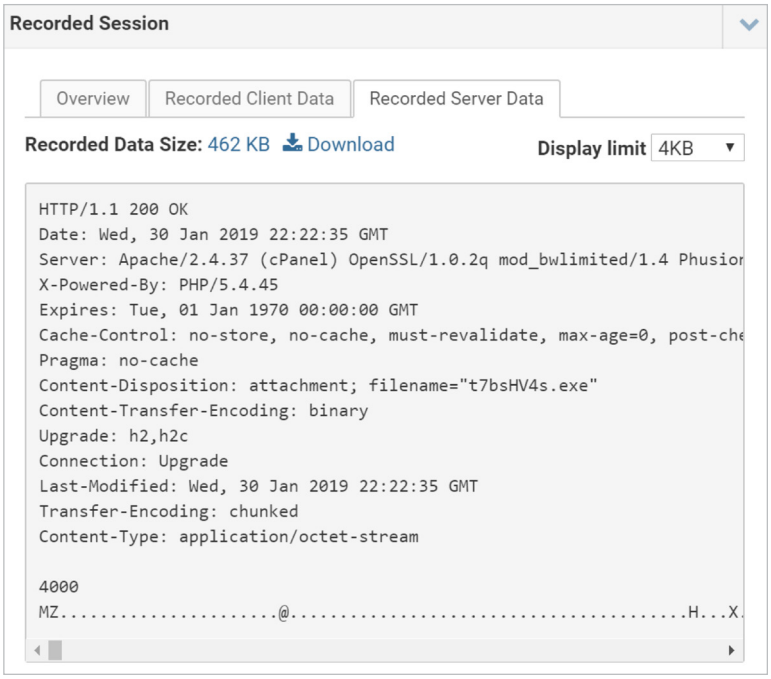


Figure 10. Recorded Server Data

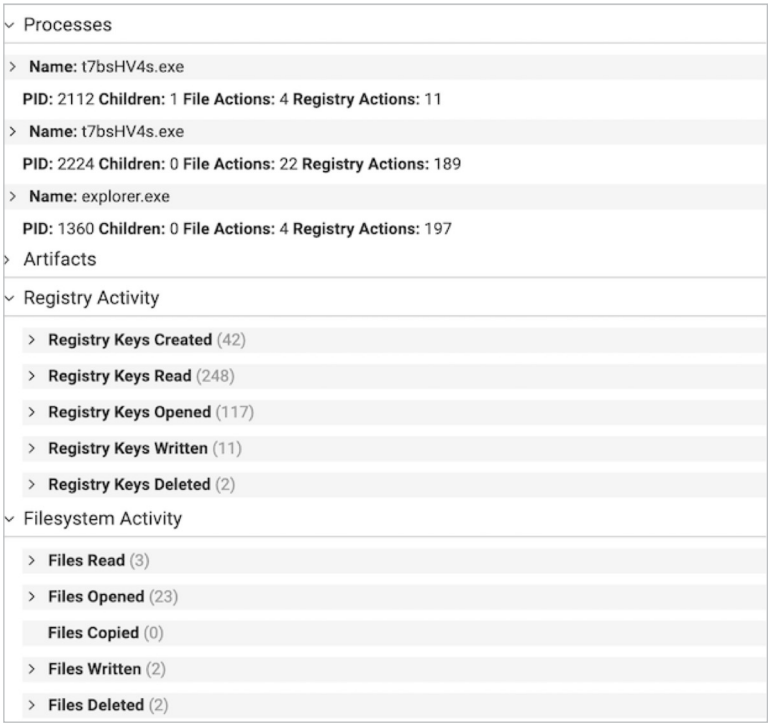


Figure 11. Host-based Artifacts

Focusing on efficient analysis, the significant, relevant forensic data points are provided directly in the console. This is yet another time-saver because analysts no longer have to manually perform or outsource sandboxing. This automation means that malware behavior and detections can be confirmed faster, allowing for better tuning and detection capabilities.

Custom Analytics

On the topic of detection capabilities, we found another benefit. Often, detections are scattered across multiple devices. Host-based detections may exist here, while network detections are over there. However, when an organization moves to holistic visibility, it's possible to combine powers and build detections all at the same time.

In Fidelis Elevate, a separate area that caught our interest was Analytics. Analytics offers two strengths that we loved:

- The ability to pivot off known-bad activity and write cross-environment detections
- The ability to utilize knowledge of the environment and write detections that may identify suspicious or malicious activity

Similar to the frequency counts we examined earlier, Analytics is yet another way for analysts to graduate from a reactive, fire-fighting approach to a proactive, threat hunting stance.

Analytics in Fidelis Elevate takes one of four possible initial designs:

- Event rate
- Event set
- Sequence
- Frequency

We loved the initial approach, given that so much malicious activity is often classified into one of these high-level categories. For example, a spearphishing email may lead to a specific process execution, which may lead to an external callout. Or, a frequency of 100 HTTP 404 errors within three seconds may illustrate an attack or scan on external servers.

When an analyst initiates any rule, Fidelis Elevate provides a simple, easy-to-follow template. In the platform, rules essentially then become fill-in-the-blanks. The events from which an analyst can pivot are barely restricted. We were able to write detections for data types we hadn't even ingested yet. We wrote a basic Sequence rule, as shown in Figure 12, that allowed us to look for evidence of a **`powershell.exe`**

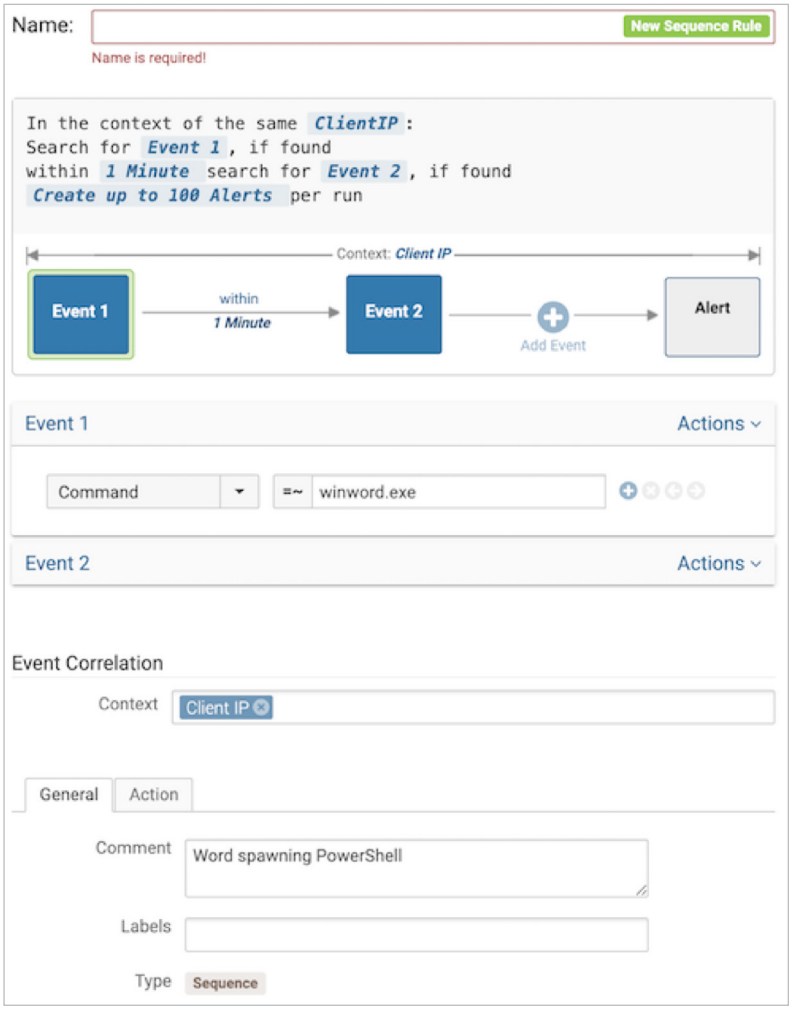


Figure 12. Example of Basic Sequence Rule

command spawning within 10 seconds of **`winword.exe`**—a sequence of events that may indicate that Microsoft Word is spawning PowerShell.

Each of the data points we discussed is customizable, allowing for wide flexibility in how stringent the analytics are. The preceding example, while extremely simple, can be tuned to catch a multitude of attacker activities that are described as "living off the land," or taking advantage of built-in system applications.

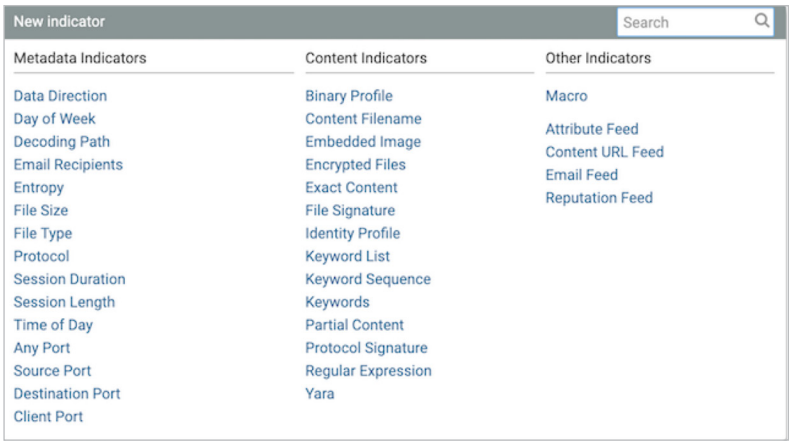


Figure 13. Indicator Sets Available

Analysts can also import more familiar, or cross-organization, detection sets. Within Fidelis Elevate, analysts can import a wide variety of indicators, as shown in Figure 13.

These indicators can be as simple as an email recipient or as complex as a Yara rule or a regular expression. The flexibility of crafting custom analytics combined with metadata or content indicators adds to the security teams' arsenals, giving them greater capability to detect and track attacker activity across their networks.

Hiding in the Shadows

Another feature set built into Fidelis Elevate, which we have not directly addressed, has been omnipresent in our review thus far. "Hidden" within is the capability to deploy and utilize deception technology in monitoring networks. Deception technology is yet another technique that security teams can use to stay ahead of threat actors, primarily by deploying assets that are true positive alerts if triggered—mainly because no legitimate user would ever find them.

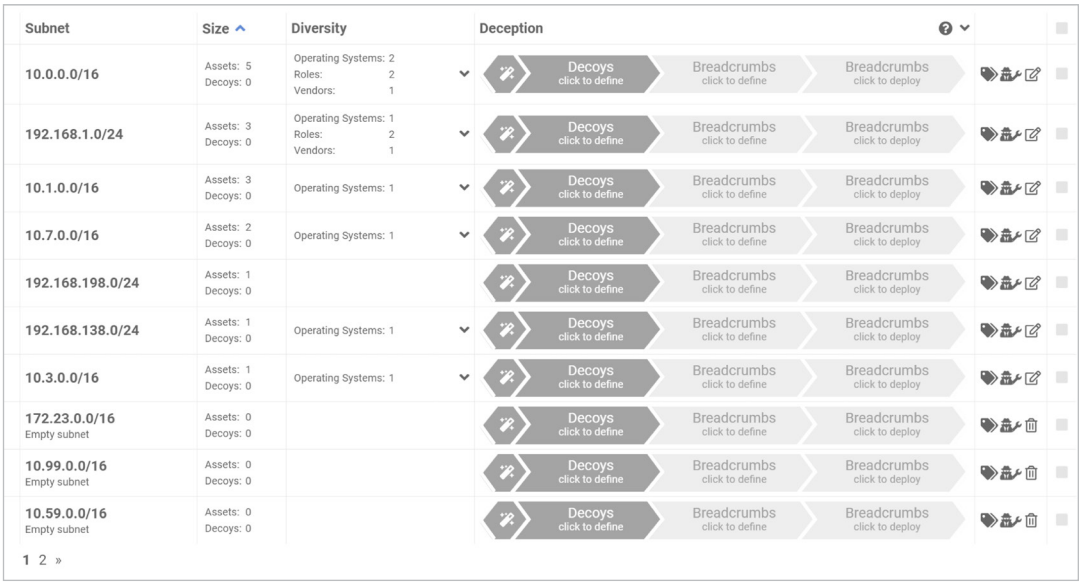
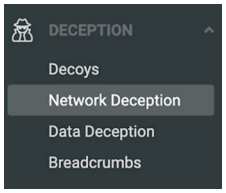


Figure 14. Decoy Deployment

Deception is nicely woven throughout Fidelis Elevate's capabilities. For example, when we were examining asset lists earlier, there were opportunities to deploy Decoys in specific subnets, as shown in Figure 14.

As we worked through multiple screens shared in this review focusing on concepts such as alerts and conclusions, the capability to quickly deploy decoys was available on most dashboard panels (see inset figure). But this is only the beginning. Fidelis Deception goes far beyond simple subnet decoys. In fact, it's a whole capability of the Fidelis Elevate platform!



Fidelis also allows for customization of network decoys, including Media Access Control (MAC) spoofing, man-in-the-middle (MITM) attacks, Address Resolution Protocol (ARP) poisoning and whether to respond to ICMP echo (ping) requests. Users can also, right from the console, perform decoy DNS validation, increasing their visibility to attackers.

From a data perspective, we can also begin to spread breadcrumbs in file systems and even prop up web servers in the environment, specifically looking for scanning and unauthorized access activity. Last, and perhaps the decoy that impressed us the most, was the ability to add a layer of deception to Microsoft Active Directory. Right from the platform's interface, we can add in users and user activity that attackers may target, but that users won't know about—thus eliminating false positives.

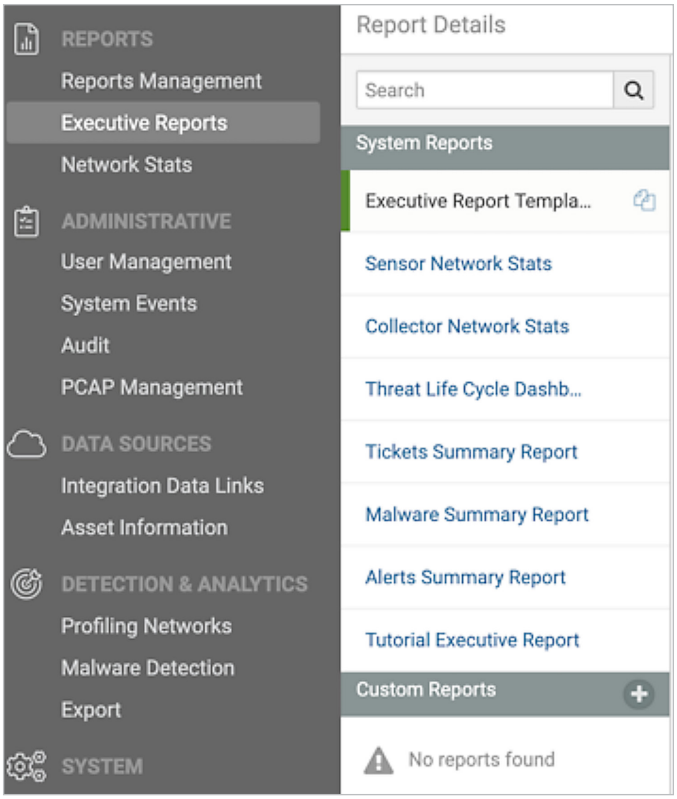


Figure 16. Custom Report Options

Metrics, Metrics, Metrics

One area of information security we are constantly trying to improve—and are urging organizations to do the same—is to track better metrics with respect to their security teams and the teams' detection and response capabilities. However, this is often easier said than done, primarily due to an inability to gain value from metrics. We found that Fidelis Elevate offered solutions to assist team leaders in this capacity as well.

Within the Administration tab, an area we have not covered in significant detail, the Reports option allows for generation of standardized reports provided by Fidelis. These reports include executive summary reports and device statistics for leaders and executives interested in high-level operations. Also available are more granular reports that allow for insight into alerts, malware and ticket activity by assigned analysts.

If the default options don't provide the insight your organization seeks, you can create custom reports (see Figure 16). The construction of a new report is quite complex, which we see as a benefit. This feature allows for extremely granular inclusion of various data points across the entire platform, meaning you can get access to the data you, your leaders and your security teams truly value.

In the same Administrative panel is an option for users to gain insight into the components in their Elevate platform. As shown in Figure 17, this includes a device-by-device breakdown of observed traffic, byte counts and protocols.

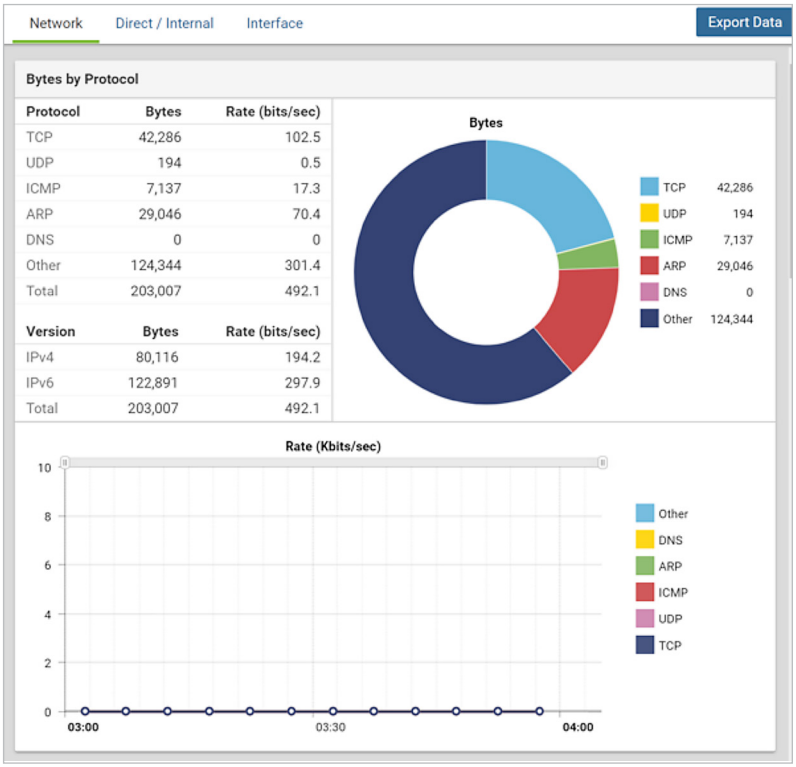


Figure 17. Network Traffic Breakdown

While this level of technical insight is great for network operators, security teams also need this knowledge. Providing this information to the security team has multiple benefits:

- Keeping tabs on devices ensures visibility is not lost and devices are not overloaded.
- As the security team matures and moves from reactive incidents to proactive hunting, metrics such as top-talking devices and protocols help establish baselines.
- Spikes in activity, easily represented in rate measurements, can act as a separate source of alerts for investigative teams.

With these metrics, security teams can think about more advanced tasks and opportunities to protect the environment, using datasets they might never have had access to before.

Conclusion

Defending enterprise networks requires tooling that enables security teams to operate faster and more efficiently. Hand in hand with efficiency is having a single point of view into the same large enterprise networks. Yet despite the benefits, many organizations still handicap their security teams with limited, subpar visibility and investigative ability.

In this first of two review papers, where we examined Fidelis Elevate and its capability of enhancing insight into network traffic, threats and deception, we explored how to combat and handle network-related threats and insight in an organization. We found the interface easy to use, the alerts insightful and—perhaps most important—the data we wanted was provided first. It's unlikely anyone could ever count the amount of time analysts have had to waste clicking through multiple screens and dashboards, performing their own correlations. Fidelis Elevate removes those steps, saving analysts time so they can refocus their efforts on keeping the organization secure.

One of our favorite takeaways from using a platform such as Fidelis Elevate was being able to exercise the concept of holistic visibility, meaning the environment is ingested, analyzed and treated as a single unit. Holistic visibility allows for threats to be analyzed and neutralized faster, and lets organizations make confident decisions that truly affect enterprise security.

Not only does the Fidelis platform allow for holistic visibility, but it also allows for your team to mature. Fidelis Elevate makes it easy for organizations to move toward threat hunting, shortening their time to detect and uncover intrusions.

Please join us for the next paper in this two-part series, "Elevating Enterprise Security with Fidelis Cybersecurity: Endpoint Security Capabilities," where we examine the Fidelis Endpoint component of the platform and how to gain expanded visibility across your estate and automate response.

About the Author

Matt Bromiley is a SANS digital forensics and incident response (IR) instructor, teaching FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and SANS FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. He is also an IR consultant at a global IR and forensic analysis company, combining 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.

Sponsor

SANS would like to thank this paper's sponsor: