SANS

A SANS Product Review

Elevating Enterprise Security with Fidelis Cybersecurity: Endpoint Security Capabilities

Written by **Matt Bromiley**

September 2019

Sponsored by:

Fidelis Cybersecurity

Executive Summary

Oftentimes the most crucial insight into any environment comes from the endpoints—the systems that are being interactively used or providing services to the environment. Given the wealth of artifacts that can be collected from endpoints, they are excellent resources for providing a comprehensive view into the activities of users and active attackers.

In this paper—the second in a two-part series—we continue our examination of the Fidelis Elevate[1] platform, with a specific focus on the endpoint portion: Fidelis Endpoint. While technically part of, and accessible from the CommandPost interface, Fidelis Endpoint provides a unique platform for monitoring endpoints, tracking behaviors and threat hunting, to name only a few of its many capabilities. As we examine the overall Fidelis Elevate platform, you can expect to see mentions of how the technologies discussed in the first part of this two-part series[2]—including deception—can be incorporated into Endpoint analysis.

[1] Fidelis Elevate™ and Fidelis Endpoint® are trademarks of Fidelis Cybersecurity®.

[2] "Elevating Enterprise Security with Fidelis Cybersecurity: Network and Deception, September 2019, www.sans.org/reading-room/whitepapers/analyst/elevating-enterprise-security-fidelis-cybersecurity-network-deception-39145

Fidelis Endpoint provides a wide range of impressive features that add to the strength of the Elevate platform. Some of our favorite features, which we believe are designed to make analysts' lives easier, include:

- Behavioral monitoring, which captures *endpoint activities from end to end*, simplifying triage and investigation activity
- Quick *links to post-analysis analyst activities*, such as indicator tracking or enterprise scanning
- Built-in threat hunting capabilities, including *real-time* and *historical* data searches and tasking
- Threat intelligence and scanning capabilities to *easily integrate third-party data* into your organization
- A s*olid inventory* of the devices, applications and key vulnerabilities in the organization

While this second paper focuses specifically on Fidelis Endpoint, our overarching goal for a platform such as Fidelis Elevate does not change: **We want organizations to strive for holistic visibility.** This concept means treating the entire organization as one functional unit, just as threat actors do. Network- and host-based artifacts are *naturally intertwined*, and analysis should be performed the same way. Security teams should launch a reactive investigation or initiate a proactive threat hunt **from the same platform**.

As you read this paper, we encourage you to assess whether your security team can gather the same metrics or perform the same analytics that we did with Fidelis Endpoint. Furthermore, keep in mind that at any point we can revert to the CommandPost interface and add more context to investigations and alerts. The focus of this series is **holistic visibility**—we hope you can achieve the same analytics, hunting and detections *across your own enterprise*. If not, it may be time to start working toward it!

Automated Endpoint Data Collection

We begin our assessment of Fidelis Endpoint where analysts would begin their typical day: within the initial dashboard. One thing we look for when assessing an initial, post-login screen is how easily the dashboard presents relevant data. After all, the seconds or minutes analysts spend tracking down information needed to perform their job duties can significantly slow down their security team over time. As shown in Figure 1 on the next page, Fidelis Endpoint serves up alert details first, providing high-level insight into the type of alert, the endpoints in question, the source and other key details.

In this initial dashboard, analysts can quickly pivot and address critical alerts without significant digging. Another feature we enjoyed when using the Fidelis Endpoint user interface—consistent with the unified CommandPost interface—is a robust, customizable search feature. Typing into the search bar allows for a simple text-based search.

However, as shown in Figure 2, analysts also have the option of modifying their search by focusing on a variety of variables, including endpoint, severity details, artifact name or intel-associated. While the concept of searching may seem trivial for an analysis platform, making key fields accessible allows for adaptable analysis and prevents analysts from needing to memorize complex search parameters to drill down into activities of interest.

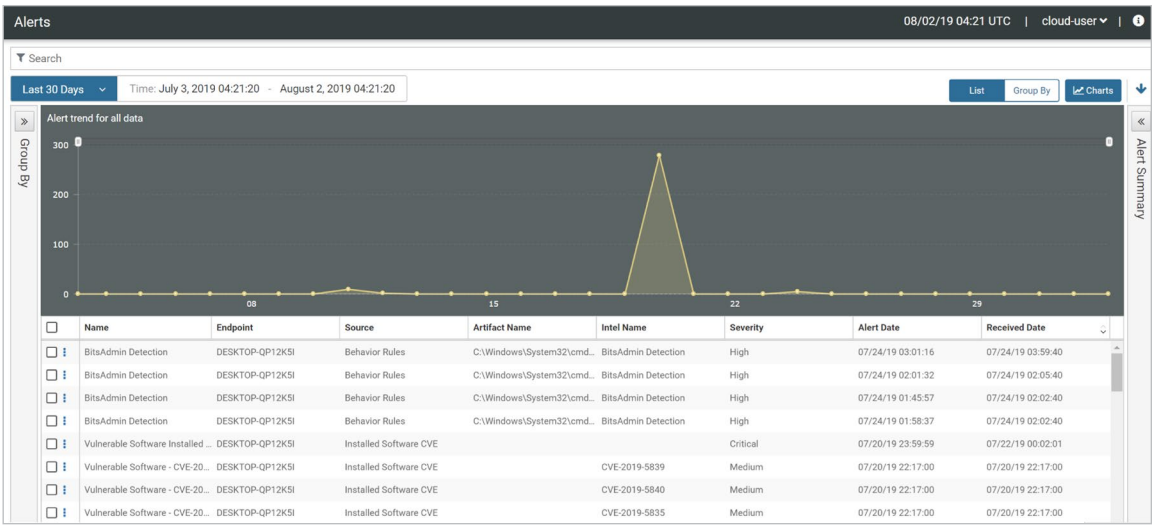

Figure 1. High-Level Insight into Alerts

During our examination of Fidelis Endpoint, we spent most of our time analyzing two types of alerts: targeted behavioral activity and automated "environmental metadata" collections. Let's address behavioral monitoring first.

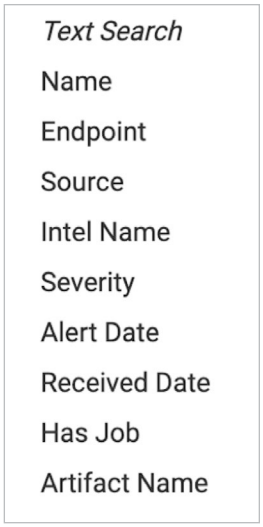

Figure 2. Search Customization Options

Targeted Behavioral Monitoring

Behavioral monitoring is one of our favorite features in Fidelis Endpoint because it provides the data necessary to *raise the confidence and accuracy* with which analysts can triage alerts. While our testing yielded fewer than 300 alerts total, large enterprises could potentially throw hundreds or thousands of alerts per minute. At that volume, security teams don't have time to manually run down the details from each alert. In such instances, behavioral monitoring is the first step in cutting down response times. In keeping with our theme of *holistic visibility*, behavioral analysis provides analysts with endpoint-specific visibility across multiple, correlated artifacts.

Behavioral monitoring works because *malware and threat actors do not exist in a solitary, technical bubble*. The infection or compromise of a system typically leaves traces of network activity and footprints all over the host. Modern malware is often network-dependent, requiring external access to download code or send a beacon back home. Threat actors have to find a way to get to a host, which also leaves unique traces on those systems.

Behavioral monitoring takes many of these dependencies into account, monitoring endpoints to watch for correlated process details, modifications to the disk and the operating system, and keying in on user activities. Correlated activity, as opposed to single-indicator triggering (such as an MD5 hash or strings in a binary), provides higher fidelity on severity scores and alert tracking.

While the concept of searching may seem trivial for any analysis platform, making key fields accessible allows for adaptable analysis and prevents analysts from needing to memorize complex search parameters to drill down into activities of interest.

In Fidelis Endpoint, behaviors are accessible either directly from the Alert console (assuming an alert was triggered) or the Behaviors tab. By accessing the Behaviors tab directly, shown in Figure 3, we can see the overall behavior tracking for the environment, not just suspicious or malicious detections. (We return to the Behaviors tab when we discuss threat hunting in the section "Executable and Script Code Analysis" later in this paper.)

Correlated activity, as opposed to single indicator triggering, provides higher fidelity on severity scores and alert tracking.

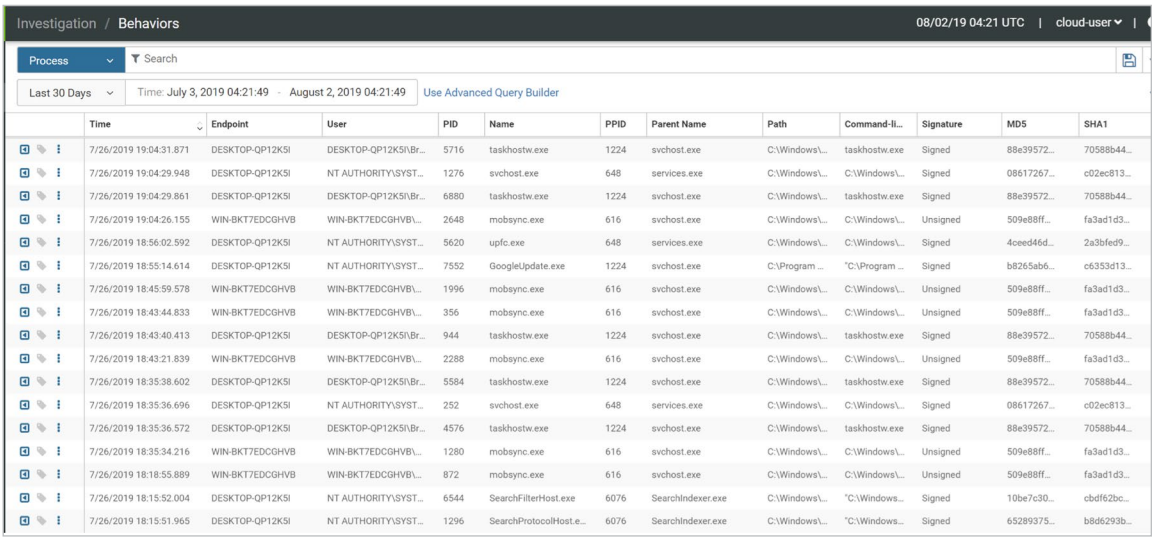

Figure 3. Behavior Tracking Across the Environment

Navigating back to the Alert console, analysts who want to drill down on any available alert are only a single click away from high-level alert details. Figure 4 shows a summary of one of the high-severity alerts Fidelis Endpoint detected during our testing.

Also with a single click, analysts can drill down into the specific behavior activity. Clicking the View Behavior link allowed us to get into the granular details of what triggered this potential alert. This is where we believe Fidelis Endpoint truly shines as a comprehensive analysis platform. As shown in Figure 5, there is a ton of data for analysts to dig through, *all presented in a single analysis screen.*

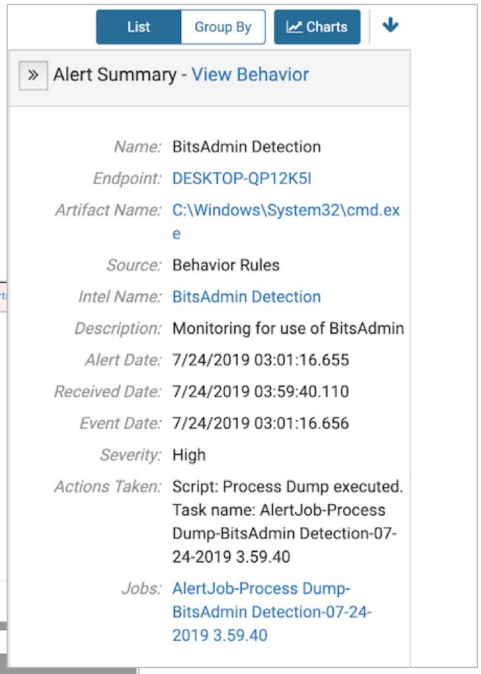

Figure 4. Details of a High-Severity Alert

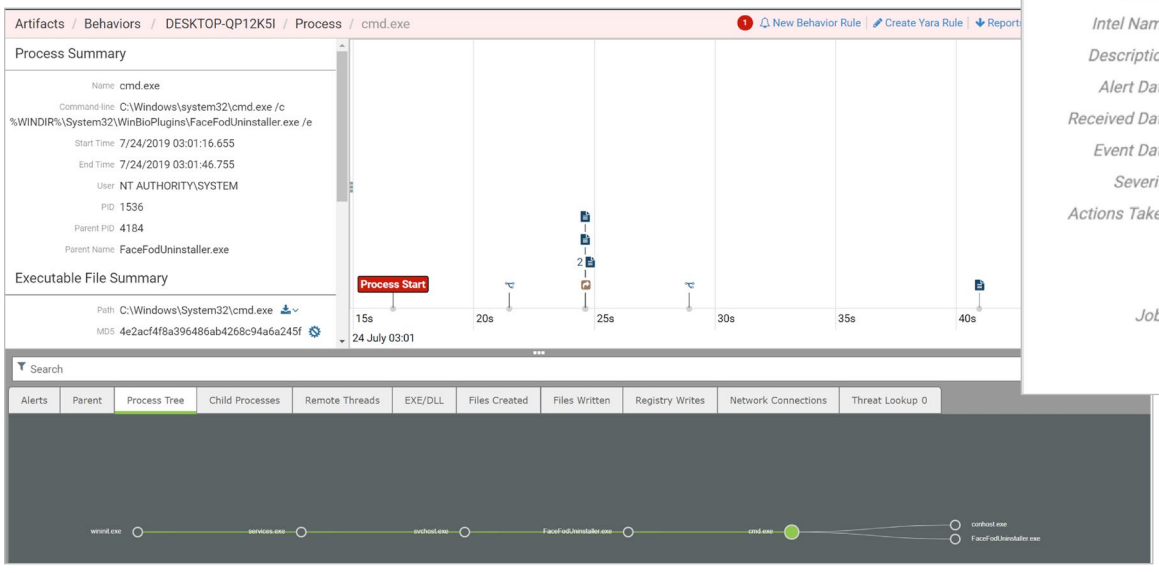

Figure 5. Granular View of Alert Triggers

Fidelis Endpoint tracks multiple data points, including process trees, files created or written to, network connections, registry modifications and **EXE/DLL** details, and presents them in the same screen (see Figure 5). Furthermore, where appropriate, Fidelis builds in various visualizations to provide additional context, such as a chronological sequence of events or a graphical representation of parent/child process relationships.

It's worth noting that not only does Fidelis Endpoint present a fantastic amount of data with this alert, but nearly all the data points in these analysis screens are interactive. The chronological timeline, as shown in Figure 6, provides single-click insight into each sequence, with links to additional details where appropriate.

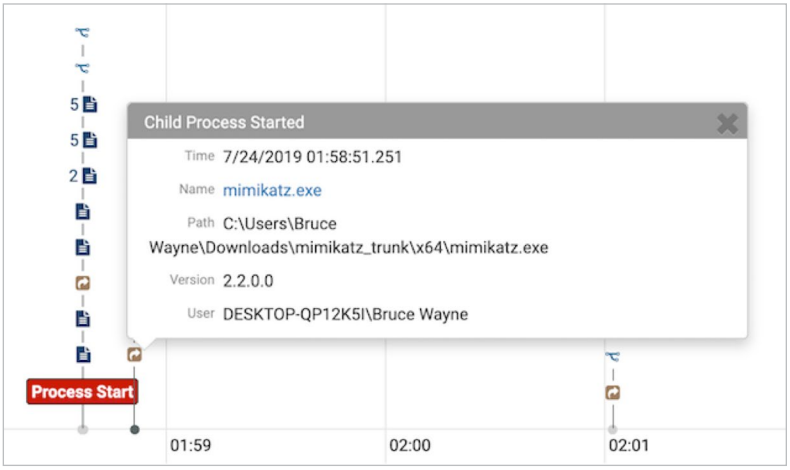

Figure 6. Interactive Insight into Sequences

By examining the tabs at the bottom of each behavior, we were able to switch between various data points to identify what activity took place and triggered an alert. Selecting the Child Processes tab from within Alert data, for example, allows for a succinct view into related processes. (See Figure 7.) This tab also provides "traditional" file details, such as the full path and various hashes.

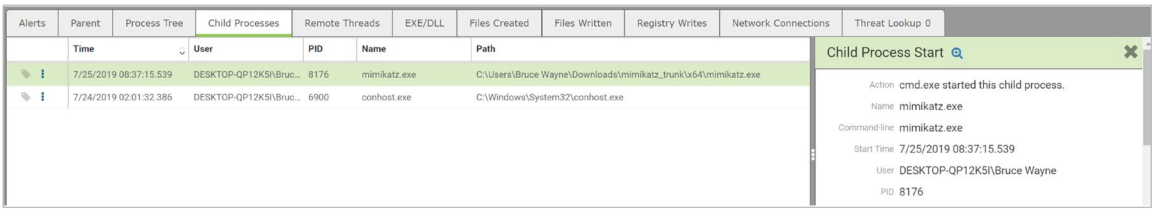

Figure 7. Concise View of Related Processes

We can view a graphical representation of the same data by clicking the Process Tree tab, shown in Figure 8.

Fidelis Endpoint provides details such as parent/child relationships, network connectivity, and registry and file interaction up front and makes them easily accessible. As previously mentioned, the more correlated data that analysts have access to, and the *greater the ease with which they can obtain that data*, the faster they can do triage and investigation or resolution. However, these data points are sometimes considered to be the norm for detection and response. We appreciate that Fidelis Endpoint consolidated multiple data points into a single screen.

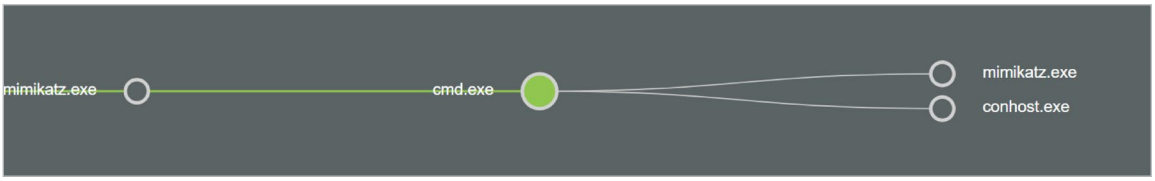

Figure 8. Graphical View of Related Processes

But Fidelis Endpoint doesn't stop there. Fidelis has clearly considered what analysts must do *after* they resolve alerts. Many of the data fields have drop-down menus that enable analysts to pivot from a file, behavior or finding directly into scanning, alerting or tasking (see Figure 9). Behavioral monitoring provides not only a unique, holistic investigation point of view, but also the ability to craft richer, multistep detections.

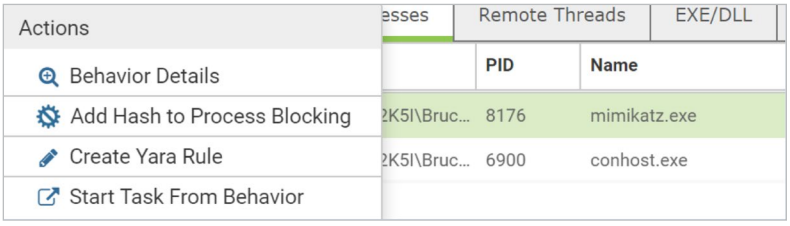

Figure 9. Drop-Down Menus for Data Fields

From the same console where we performed alert triage on a suspected credential-harvesting tool, Fidelis Endpoint offered a one-stop jump to:

- Implementation of a hash-based process block
- Creation of a Yara rule
- Start of a task from the particular observed behavior

These are some of the best features organizations can ask for in a security platform. These tools essentially allow analysts to go from one alert to the entire environment (a massive zoom out), depending on the severity of the confirmed activity. For example, if a particular executable is confirmed malicious, there may be a business justification to prevent further execution *anywhere else in the environment*. Process blocks can also be implemented via Yara rules, allowing for more flexibility and robust signatures. Attackers can easily change a hash, but other indicators or executable metadata are harder to reset.

If an executable is confirmed malicious, there may be a business justification to prevent further execution anywhere else in the environment.

Another feature worth mentioning, and accessible from the Alert and Behavior analysis screens, is the direct download of an offending executable or script, as shown in Figure 10.

This helpful screen once again is a display of bringing data pertinent to analysis directly to the analysts, so they don't waste time digging for it.

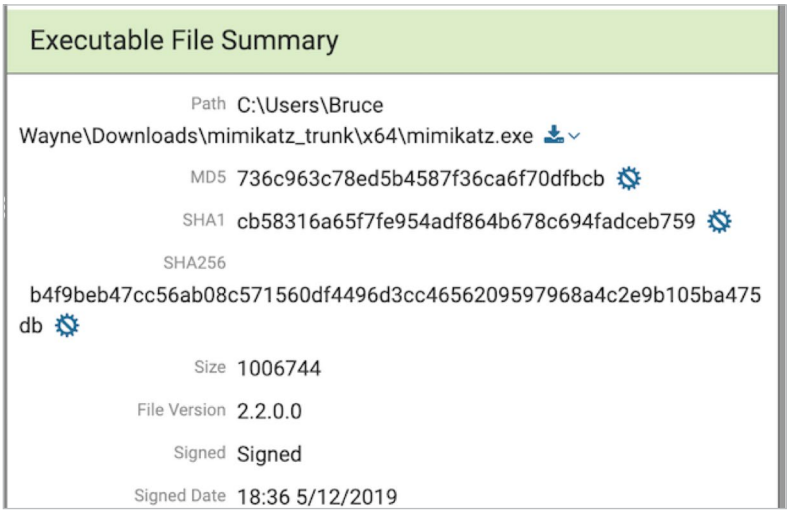

Figure 10. Direct Download of an Executable

Automated Collection

Another useful feature that Fidelis Endpoint offers is the automatic collection of executables and scripts at runtime. This provides organizations with a two-fold advantage:

- If an attacker tries to delete a file, the analyst team still has access to the raw data for subsequent analysis.
- Upon acquisition of the data, Fidelis Endpoint is able to inspect and provide various metadata elements about a particular sample. Analysts can, in turn, use these metadata points to craft additional detections or searches throughout the environment.

We're always a fan of features that take away threat actors' anti-forensic capabilities, especially because these threat actors continue to develop techniques to hide and mask their binaries from the operating system.

Switching from Reactive to Proactive

Thus far, we've examined a significant number of Fidelis Endpoint features from a *reactive* perspective, meaning an organization is responding to and handling alerts and investigations. However, as an organization's security program matures with a platform such as Fidelis Elevate, security teams can shift into a *proactive* stance, where they have the time and capabilities to *discover the threats they weren't aware of*. Fortunately, this is all possible in the same platform.

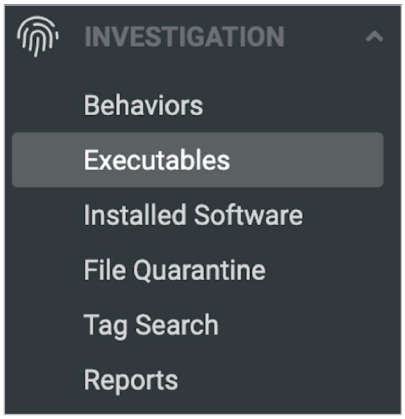

Figure 11. Investigation Tab Features

Executable and Script Code Analysis

In the Investigation tab of the main dashboard, analysts have access to more data than the Behaviors detail described previously. Fidelis Endpoint captures additional metadata simply by running and observing host activity. See Figure 11.

One key option, and perhaps a light introduction to some suspicious executable hunting, is provided in Executables. This feature provides insight into the various executables and scripts, such as PowerShell, detected in the environment, as well as related metadata. See Figure 12.

As mentioned earlier, Fidelis Endpoint captures executables and scripts and makes them readily available for download. Furthermore, each executable offers a direct link to behavioral activity, in the event that analysts want to drill down for additional information.

Date First Reported	File Name First Reported	Type	Size	Endpoint First Reported	Path First Reported	MD5	SHA1	SHA256
07/24/19 04:00:14	fodhelper.exe	Executable	45.0 kB	DESKTOP-QP12KSI	C:\Windows\System32\fodhelper.exe	1d1f9e564472a9698f1ba3f9feb9864b	84c1de94e002de58009973f5dd1624...	b52fbb99308493a27aac725cf70721
07/24/19 04:00:12	ngentask.exe	Executable	82.6 kB	DESKTOP-QP12KSI	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ng...	aa98e294a0213bda5f79a7288f91b78c	86dd2a5845c2ef0960a704b71a4926...	36576db25877fa5ecbf8e1e91d640a
07/24/19 04:00:11	ngentask.exe	Executable	83.1 kB	DESKTOP-QP12KSI	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngent...	ed7f195f7121781cc3d380942765b57d	aee93c4d84c2035c2fb20e45506722...	ca003ecd9a6caae17824816d1d869
07/24/19 04:00:08	mcbuilder.exe	Executable	89.0 kB	DESKTOP-QP12KSI	C:\Windows\System32\mcbuilder.exe	01d97c929881e231c51a11922c75c6a	d99cb75764194b56c180cbeb50ee5f...	6d91cfbdb5363bd3370ca3244a6f62
07/24/19 04:00:06	4ed1b7d4e99db4c711322406...	Script	9.5 kB	DESKTOP-QP12KSI	4ed1b7d4e99db4c711322406523991e38a8824e3c	9b010d27c4fe60e19341d872426797...	4ed1b7d4e99db4c711322406523991e...	4ebee677269f15eaa37b6dd47e22c2
07/24/19 04:00:05	414df3742beff253b4f898b407...	Script	23.4 kB	DESKTOP-QP12KSI	414df3742beff253b4f898b40751ce2af6656	b98ecc31e0b04197f9cfdc29f10287708	414df3742beff253b4f898b40751ce2...	20a87180de77648b3a04cab37e24e
07/24/19 04:00:03	GoogleUpdate.exe	Executable	151.3 kB	DESKTOP-QP12KSI	C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	b8265ab60d731fa7a1705f829a64ca32	c6353d1350e416fd64e5cefab0c0264...	3435cdd3d1975191ea2542f9b2a1fb
07/24/19 03:59:59	sdiagnhost.exe	Executable	24.5 kB	DESKTOP-QP12KSI	C:\Windows\System32\sdiagnhost.exe	22e56a1a980252b8880ed1a12561f0...	b969cfd894a554ed1721eabcc0854d...	165968286bd97d87e360e006cc0ca
07/24/19 03:59:58	lpremove.exe	Executable	42.0 kB	DESKTOP-QP12KSI	C:\Windows\System32\lpremove.exe	2db5526a2abc04bf2dfb02d404ddf5a9	e0e0154866db67db4a29898f61584...	9a20da8a4585f795cc8199501e1517
07/24/19 03:59:56	VSSVC.exe	Executable	1.5 MB	DESKTOP-QP12KSI	C:\Windows\System32\VSSVC.exe	c7053d974a35eab81f153ff33c883613	07d46e46e2180693a045d784043e82...	9d89dc644971f93931d0e59d42ade
07/24/19 03:59:42	cleanmgr.exe	Executable	214.5 kB	DESKTOP-QP12KSI	C:\Windows\System32\cleanmgr.exe	062ec57fe7f4463161d9e6ef400b2a3e	2eb3900399f8f0e518ad937db120b87...	aa5016a3f28f312e00679bfb9a6b66
07/24/19 03:59:39	tzsync.exe	Executable	61.0 kB	DESKTOP-QP12KSI	C:\Windows\System32\tzsync.exe	1c46a81ea1ea413a4fbde1fdbf71becc	bb97061b5256add7a6cc924feff090d...	9bef963b003092 1f70c3ddf46ef6e3
07/24/19 03:59:32	FaceFodUninstaller.exe	Executable	427.0 kB	DESKTOP-QP12KSI	C:\Windows\System32\WinBioPlugIns\FaceFodUninstalle...	9c30acd6aa83bde68329941d37e3b4...	210830a72ebef693fc5e4b85af1f49b...	9e370fedbdcbd4645683566b648dbz
07/24/19 03:59:29	sc.exe	Executable	67.5 kB	DESKTOP-QP12KSI	C:\Windows\System32\sc.exe	d79784553a9410d15e04764aab77fc...	72785e3068aa52ca223da466595d38...	aeb241959f4a7b7c29f45d27fd65c5
07/24/19 03:59:28	MpCmdRun.exe	Executable	446.8 kB	DESKTOP-QP12KSI	C:\Program Files\Windows Defender\MpCmdRun.exe	9f2c791ed4801f09ca2d56d265cd4bc5	c3864f7c57c2cf8e9be5d4401c36e74...	f9186a3236918316a453da67d6798
07/24/19 03:59:25	dstokenclean.exe	Executable	12.5 kB	DESKTOP-QP12KSI	C:\Windows\System32\dstokenclean.exe	9746f6f8866ce90c5186d69ec2a1d0b8	b790cb9c4ff3d19252dd085e6ae2fa...	45b6afcd58c1d27f3f09b68f86c68d8
07/24/19 03:59:23	DiskSnapshot.exe	Executable	89.0 kB	DESKTOP-QP12KSI	C:\Windows\System32\DiskSnapshot.exe	dcdfa656550edf320fe9a127739ea645	50e59c18cd4493e2f15ba7a944e139...	01e0d4ffe6f18299b0f33065dcc4009
07/24/19 03:59:21	Defrag.exe	Executable	181.5 kB	DESKTOP-QP12KSI	C:\Windows\System32\Defrag.exe	f52552d225c325a08de585a188b7ff6b	20103c9e3f0b40ae402446e286d13e...	14bd3078ad7f3aab8feb6fa157de11
07/24/19 03:59:19	SpeechModelDownload.exe	Executable	165.0 kB	DESKTOP-QP12KSI	C:\Windows\System32\Speech_OneCore\common\Spec...	08f71705ca28ba0a5d15e2019a26e9a3	3f9e7783f4821cffc1f0f601361ea2b6f...	b1fa6cc2f1f1563d9f1e048ea0bcaa2
07/24/19 03:59:17	AdobeARM.exe	Executable	1.1 MB	DESKTOP-QP12KSI	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\A...	50b17d217f07d5968b34f42311638f74	de0c092e9e157288c661f3471301fc5...	9ad7c808374331 2c9742f5844f6eff3
07/24/19 03:59:14	dasHost.exe	Executable	92.0 kB	DESKTOP-QP12KSI	C:\Windows\System32\dasHost.exe	fd83c3389817c5246fe544eee63e4115	4bd17fc26e5a1d2db41155300248 3c...	8d6881e9bfba065692e7b8de209903
07/24/19 03:59:06	SearchFilterHost.exe	Executable	111.0 kB	WIN-BKT7EDCGHVB	C:\Windows\System32\SearchFilterHost.exe	52d56d1013d4f1b99102679314cc53...	904a3b130e3db7cea97f31cc40d64d...	f8f6c41fec774c71a85c91dfeb05707
07/24/19 03:59:04	SearchProtocolHost.exe	Executable	244.0 kB	WIN-BKT7EDCGHVB	C:\Windows\System32\SearchProtocolHost.exe	42ec9065d9bf266ade924b066c783a56	a8dcf7d63a8bb5abef8787775957a5b...	4ac002e90a52cb0998da78f2995294
07/24/19 03:59:01	mobsync.exe	Executable	100.0 kB	WIN-BKT7EDCGHVB	C:\Windows\System32\mobsync.exe	509e88ff7b257885775791faf0965d6a	fa3ad1d38856416077d53c0bebe26e...	fecd6785984dbb61c6c0ea8a3d8daf
07/24/19 03:58:26	WinSAT.exe	Executable	2.7 MB	DESKTOP-QP12KSI	C:\Windows\System32\WinSAT.exe	7e222296267cb43d95ba8c376d937d...	bc9abebbc326b9d1fb81e2fc9bc783b...	8b2163756295f0f17e242a4d2a962c
07/24/19 03:58:20	SrTasks.exe	Executable	55.5 kB	DESKTOP-QP12KSI	C:\Windows\System32\SrTasks.exe	743a4f2dca5d3bfb771ea67a157c6cce	867952dc8a6df18b5a881170d016e3...	3cb58f649a9686b33f4b14765c9c2a

Figure 12. Detected Executables and Metadata

The ability to pivot through script data allows for greater insight into the environment. PowerShell has become a staple in modern attacker toolkits and is something that all defenders should be watching for. PowerShell presents a unique problem, however, as it's also a favorite of system administrators! Having Fidelis Elevate's insight into executable/script collection and code analysis can help your analysts identify what's approved versus malicious in the environment.

Software Inventory

Another inventory-related tab provided by Fidelis Endpoint includes an inclusive list of installed software, depicted in Figure 13.

Name	Publisher	Version	Highest CVE Score	CVE Count	Endpoint Count	Last Install Date
Adobe Acrobat Reader DC MUI	Adobe Systems Incorporated	19.012.20035	10 - Critical	79	1	07/20/19
Google Chrome	Google LLC	67.174.32910	9.3 - Critical	194	1	07/20/19
VLC media player	VideoLAN	3.0.7.1	7.5 - High	3	1	
MobaXterm	Mobatek	11.1.0.3860	6.8 - Medium	1	1	07/20/19
bzip2		1.0.6-8.1ubuntu0.2	5.1 - Medium	7	2	07/12/19
bash		4.4.18-2ubuntu1.2	4.6 - Medium	1	1	07/12/19
bash		4.4.18-2ubuntu1.1	4.6 - Medium	1	1	06/17/19
accountsservice		0.6.45-1ubuntu1	1.9 - Low	1	2	06/17/19

Figure 13. Inventory of Installed Software

Software inventory is not a new concept and is quite commonplace among endpoint platforms. However, as we've seen with other data points, Fidelis takes it a step further with Fidelis Endpoint. You may have noticed in Figure 1, shown earlier, a series of alerts categorized as *Installed Software CVE*. This feature ties directly to the *Installed Software tab* and is a really neat feature in Fidelis Endpoint.

Not only does Fidelis Endpoint keep track of software versions of various endpoints, but it performs lookups and comparisons to determine whether you are running any vulnerable software on those systems. Fidelis Endpoint categorizes and ranks common vulnerabilities and exposures (CVEs) accordingly, with vulnerabilities making their way into the Alerts tab so security teams can act on them. Furthermore, Fidelis Endpoint can also integrate with Active Directory, allowing you to bring these data points together with AD enrichment.

This might seem like a trivial data point, but many threat actor entry vectors, exploits and persistence mechanisms are based on outdated/unpatched software. This is often a key pain point for many organizations: out-of-date software details are hard to identify. Fidelis Endpoint helps solve this problem by allowing analysts to handle alerts and vulnerabilities *within the same screen*—remember, **we want holistic visibility!**

Constructing Tasks

Let's be frank about one thing: Looking at executable metadata or known vulnerabilities would hardly classify as efficient approaches to hunting through an environment. To gain unique, granular insight into key artifacts in the environment, we switched over to Tasks, another of our favorite features in Fidelis Endpoint and the Fidelis Elevate platform.

Figure 14 shows the initial Tasks screen, which contains a list of the various jobs and data points we can request from our environment. Whether we are chasing an adversary in incident response mode, or seeking to establish proactive threat hunting, data packages exist that allow for either to be easily executed. Note that this list is not comprehensive; our test instance included 98 built-in packages, with an easy option to create additional packages in the administration panel.

Name	Type	Platform	Tags	Description	Created Date
Administrators	Script	Windows 32 | Windows 64	User, Accounts, Administrator, System Management	Lists all users with Administrator rights. Use the optional parameter to filt...	05/10/19 16:08:1
Agent Log	Script	Windows 32 | Windows 64	System Management, Agent, Log	Returns log entries from the Fidelis Agent.	05/10/19 16:08:1
All User Accounts	Script	Windows 32 | Windows 64	Investigation, Volatile, Users, Accounts	Displays information about any created users on an endpoint. Use the Opt...	05/10/19 16:08:2
All User Accounts (WMI)	Script	Windows 32 | Windows 64	User, Accounts, System Management	Lists all the user accounts. Use the optional parameter to filter the results ...	05/10/19 16:08:2
AntiVirus Information	Script	Windows 32 | Windows 64	AntiVirus, System Management	Shows the AntiVirus and AntiSpyware products installed on client comput...	05/10/19 16:08:2
ARP Cache	Script	Windows 32 | Windows 64	Investigation, Volatile, Network	Displays information from the Address Resolution Protocol Cache. Use th...	05/10/19 16:08:2
Autoruns	Script	Windows 32 | Windows 64	Autorun, Startup, System Management, Investigation	Returns all windows Autoruns. Use the optional parameter to filter the res...	05/10/19 16:08:2
Certificates	Script	Windows 32 | Windows 64	Certificates	Lists all the certificates. Use the optional parameter to filter the results to t...	05/10/19 16:08:2
Computer Uptime	Script	Windows 32 | Windows 64	System Management, Uptime	Returns the time in minutes it has been since the computer started	05/10/19 16:08:2
Configure Agent	Script	Windows 32 | Windows 64	System Management, Configuration, Deployment	Allows you to set various configuration options for the Fidelis Agent.	05/10/19 16:08:2
Configure Agent Proxy	Script	Windows 32 | Windows 64	System Management, Configuration, Deployment	Allows you to set proxy configuration options for the Endpoint Agent servi...	05/10/19 16:08:2
CPU Load	Script	Windows 32 | Windows 64	CPU, Performance	Returns the CPU load percentage. Use the filter to specify a minimum retu...	05/10/19 16:08:2
CPU Usage Per Process	Script	Windows 32 | Windows 64	Process, CPU, Performance	Returns the CPU usage for each process currently running. Use the filter t...	05/10/19 16:08:2
Create Local User Account	Script	Windows 32 | Windows 64	Users, Accounts, System Management	Creates a local user account.	05/10/19 16:08:2
Current File-sharing Sessions	Script	Windows 32 | Windows 64	Network, Sessions, Investigation, Volatile	Displays information about the current inbound remote sessions connecte...	05/10/19 16:08:4
Delete Registry Value	Script	Windows 32 | Windows 64	Registry, Registry Value	Deletes the specified registry value. WARNING: This may break the target ...	05/10/19 16:08:2
Disk Image (Cancel/Throttle)	Script	Windows 32 | Windows 64	Disk Acquisition, Disk Image, Data, Investigation	Cancel or Throttle a currently running disk imaging task. 0 means to canc...	05/10/19 18:20:0
Disk Image (Filestore)	Script	Windows 32 | Windows 64	Disk Acquisition, Disk Image, Data, Investigation	Creates an image of an endpoint's disks or volumes and stores it on Endp...	05/10/19 18:20:0
Disk Image (Windows File Share)	Script	Windows 32 | Windows 64	Disk Acquisition, Disk Image, Data, Investigation	Creates an image of an endpoint's disks or volumes and stores it at the sp...	05/10/19 16:08:4
Disk Space	Script	Windows 32 | Windows 64	System Management, Hardware, Disk	Lists all the hard drives with respective size and free space. Use the para...	05/10/19 16:08:2
Disk Volumes	Script	Windows 32 | Windows 64	Investigation, Volatile	Displays the information about the volumes mounted on the endpoint. Us...	05/10/19 16:08:2
DNS Cache	Script	Windows 32 | Windows 64	Investigation, Volatile	Displays the data from the DNS cache on the endpoint. Use the Optional Q...	05/10/19 16:08:2
Drivers	Script	Windows 32 | Windows 64	Investigation, Volatile	Displays information about the drivers on the endpoint. Cerberus Stage O...	05/10/19 16:08:2
File Collection	Script	Windows 32 | Windows 64	File System, Data, Investigation	Search the filesystem returning the metadata of the files that matched the...	05/10/19 16:08:2
File Copy	Script	Windows 32 | Windows 64	File System, Data, Investigation	Copy a file from one location on the Endpoint to another. File must exist at...	05/10/19 16:08:2
File Delete	Script	Windows 32 | Windows 64	Data, File System, Incident Response, Remediation	Delete a file or folder at the specified path.	05/10/19 16:08:2

Figure 14. Job and Data Points that Can Be Requested

The various tasks Fidelis Endpoint offers enable organizations to comfortably walk the line between reactive and proactive investigations. For example, let's say an organization wants to conduct a hunt by digging through `prefetch` files. In simple terms, these files offer evidence of execution on Microsoft Windows systems and are often used to identify the current or previous execution of a file on a system.

Constructing a task that reaches out and pulls Windows **prefetch** files is so easy in Fidelis Endpoint that we almost wondered whether we forgot to include a particular field. In fact, the scripts that power the various tasks are quite complex, but much of this can be abstracted away from the analyst, if the organization chooses. Initiating a pull of **prefetch** data in the environment simply involves setting priorities, naming the job and selecting a target host set, as shown in Figure 15.

Once initiated, the tasks we launched ran quickly and pulled back data almost immediately. However, Fidelis Endpoint was just getting started.

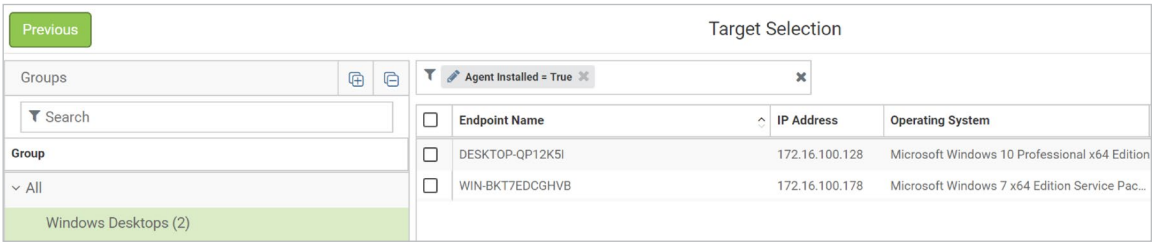

*Figure 15. Pulling **prefetch** Files*

When data started to return to the Fidelis Endpoint console, it automatically rendered in a columnar format that is *adaptive to the artifact being interrogated*. As shown in Figure 16, the **prefetch** data is displayed and parsed according to the relevant **prefetch** data points, such as creation time and reported file size.

If we change up our task and instead pull back **DNS** caches from all systems, notice that the columnar rendering changes, based on the requested data type. See Figure 17 on the next page.

In Task analysis, Fidelis Endpoint has built a truly adaptive data return dashboard, providing for artifact-specific analysis. For many organizations, this feature is a game changer. We often see endpoint monitoring platforms that can pull back various artifacts, but they are delivered as raw data that analysts must subsequently parse and/or make sense out of. Fidelis, once again looking to save analysts time and make holistic security possible, automatically parses returned data and provides it in a searchable, easy-to-consume format.

Endpoint	File Name	Creation Time	Reported File Size
DESKTOP-QP12K5I	UNSECAPP.EXE-72B9DDB3.pf	2019-07-24T01:55:00.978898	3931
DESKTOP-QP12K5I	FEP_CONSOLE.EXE-28100973.pf	2019-07-24T01:54:58.561897	9642
DESKTOP-QP12K5I	PROTECT.EXE-5213992F.pf	2019-07-24T01:54:48.913895	17515
DESKTOP-QP12K5I	DISMHOST.EXE-B53E4677.pf	2019-07-24T01:49:47.408326	6491
DESKTOP-QP12K5I	USOCLIENT.EXE-4ADC110B.pf	2019-07-24T01:49:45.799054	3681
DESKTOP-QP12K5I	NETSH.EXE-8174DA63.pf	2019-07-20T22:21:11.031857	9521
DESKTOP-QP12K5I	FIDDLERSETUP.EXE-710A367A.pf	2019-07-20T22:21:11.008856	9873
DESKTOP-QP12K5I	FIDDLERSETUP.EXE-4A647097.pf	2019-07-20T22:21:11.006356	21140
DESKTOP-QP12K5I	SETUPHELPER-BFF8ECCB.pf	2019-07-20T22:21:10.960856	7209
DESKTOP-QP12K5I	GIMP-2.10.12-SETUP.EXE-753E228C.pf	2019-07-20T22:19:52.400196	5984
DESKTOP-QP12K5I	GIMP-2.10.12-SETUP.TMP-802F8FE8.pf	2019-07-20T22:19:43.861357	34033
DESKTOP-QP12K5I	MAINTENANCESERVICE_INSTALLER.-6BEC36FF.pf	2019-07-20T22:15:11.319905	11830
DESKTOP-QP12K5I	MAINTENANCESERVICE_TMP.EXE-6A746806.pf	2019-07-20T22:15:11.288694	3922
DESKTOP-QP12K5I	SETUP.EXE-3A96EE15.pf	2019-07-20T22:15:10.351202	30109
DESKTOP-QP12K5I	THUNDERBIRD SETUP 60.8.0.EXE-1C4E5D8E.pf	2019-07-20T22:15:08.460665	19746
DESKTOP-QP12K5I	PIDGIN-2.13.0-OFFLINE.EXE-734FE682.pf	2019-07-20T22:14:49.796402	25056
DESKTOP-QP12K5I	HEXCHAT 2.14.1 X64.EXE-18041913.pf	2019-07-20T22:14:31.785635	6425
DESKTOP-QP12K5I	HEXCHAT 2.14.1 X64.TMP-7202B95C.pf	2019-07-20T22:14:31.785635	38868
DESKTOP-QP12K5I	WINPCAPINSTALL.EXE-04E99DDA.pf	2019-07-20T22:14:15.895455	11676
DESKTOP-QP12K5I	AUTOHOTKEY.EXE-9290C316.pf	2019-07-20T22:14:15.864207	6149
DESKTOP-QP12K5I	AUTOHOTKEY.EXE-5A35085F.pf	2019-07-20T22:14:13.551771	7684
DESKTOP-QP12K5I	REG.EXE-A93A1343.pf	2019-07-20T22:13:41.274183	2140
DESKTOP-QP12K5I	PRUNSRV-AMD64.EXE-2611112A.pf	2019-07-20T22:07:21.550739	32017
DESKTOP-QP12K5I	JAVA.EXE-6791F41A.pf	2019-07-20T22:07:20.268816	8945
DESKTOP-QP12K5I	CODE.EXE-12F1BED5.pf	2019-07-20T22:07:19.839728	37401

*Figure 16. Relevant **prefetch** Data Points*

As we mentioned previously, Fidelis Endpoint includes dozens of tasks. Furthermore, most tasks are cross-platform where appropriate, allowing analysts to consider hunting and investigative activities from an environmental perspective, instead of an OS-based approach. Deep-dive tasks are also available, allowing analysts to pull and triage a full memory image from a system, if they need to go to that depth.

Endpoint	Name	Time to Live	Section	Record Type	Data Size	Host Name	IP	Matches
DESKTOP-QP12K5I	desktop-qp12k5i.mshome.net	86400	Answer	A	4		192.168.233.113	0
DESKTOP-QP12K5I	1.0.0.127.in-addr.arpa	86400	Answer	PTR	4	view-localhost		0
DESKTOP-QP12K5I	checkin-5026278.fidelisclOud.com	4	Answer	A	4		54.158.15.170	1
DESKTOP-QP12K5I	113.233.168.192.in-addr.arpa	86400	Answer	PTR	4	DESKTOP-QP12K5I.mshome.net		0
DESKTOP-QP12K5I	view-localhost	86400	Answer	A	4		127.0.0.1	0
WIN-BKT7EDCGHVB	checkin-5026278.fidelisclOud.com	4	Answer	A	4		54.158.15.170	1

Figure 17. Adaptive Data Returned, Based on DNS Cache Data

Reaching Higher: Extending Fidelis Endpoint

While we found numerous areas in Fidelis Endpoint that we truly enjoyed and believe can improve the security capabilities of many organizations, one of our favorite takeaways is keeping the overall environment in mind. While we were looking at data points collected from endpoints in our test environment, at any point we could easily have zoomed out to CommandPost and viewed related network activity. The correlation of host- and network-based activity only strengthens the confidence with which one can analyze alerts, on top of the already ultrarich behavioral reporting.

In the first paper in this series, we pointed out Fidelis Elevate's capability of deploying deception technology to detect additional malicious activity in the environment. Fidelis Endpoint also becomes a critical player in deception technology, as it can be deployed to various endpoints and used to trigger custom alerts.

If your organization wants to extend Fidelis Elevate's capabilities, both CommandPost and Endpoint allow for integration of third-party sources. As shown in Figure 18, Fidelis Elevate allows for simple integration of threat intelligence feeds, in addition to the built-in feeds that Fidelis itself already overlays on the data.

Another way for security teams to level up their defensive capabilities is via signatures that can also easily be ingested into Fidelis Endpoint.

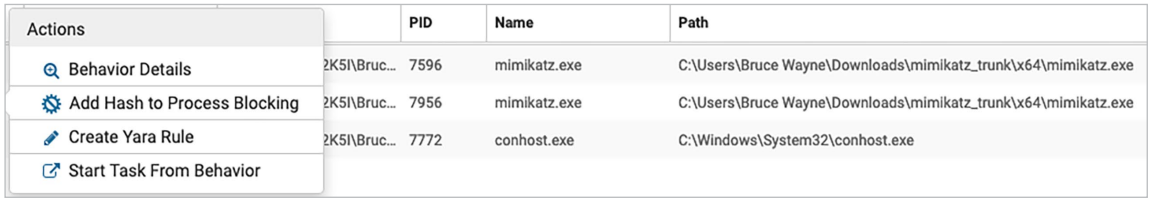

Figure 18. Integrating Threat Intelligence Feeds

Provided in the *Threat Intelligence tab*, Fidelis Endpoint maintains a Scanning Indicator Library, a collection of indicators of compromise (IoCs) and Yara signatures that can subsequently be roped into Detections and Tasks. OpenIOC is also supported. As shown in Figure 19, our instance came preloaded with multiple signatures.

Uploading your own signature and indicators is a simple two-click process. Those steps allowed us to craft and utilize custom signatures that may be

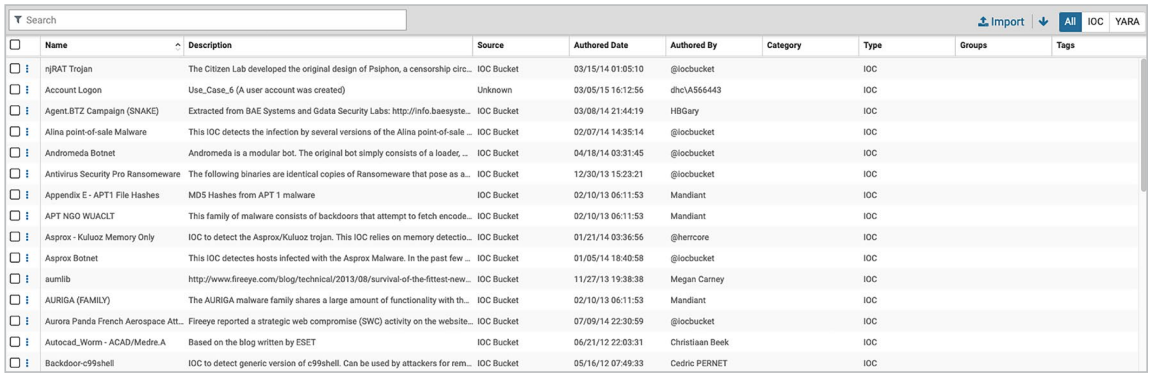

Figure 19. Preloaded Signatures

unique to our environment. This represents another area where security teams can effectively protect their organization—by using signatures relevant to the activity they are observing. Signatures can subsequently be used to scan filesystem and in-memory objects, allowing for greater reach and visibility into the environment.

Conclusion

Enterprise security and defense are best done when organizations are able to monitor and analyze their entire environment as a *single—albeit complex—landscape*. Many organizations get stuck applying defense in a piecemeal fashion, rarely considering how the various pieces of a large organization communicate with one another constantly. This stance is likely handicapping your security team and preventing your organization from achieving a *truly effective and efficient defense*.

In this second and final product review of the Fidelis Elevate platform, we examined Fidelis Endpoint, the aptly named product that provides endpoint insight and response. We found that Fidelis Endpoint offers organizations a robust capability for gaining high-level insights into the state of their various endpoints, while also offering drilldowns into key granular details that are crucial for effective detection and response.

Some of the key highlights from our review include:

- Behavioral monitoring and detections that track a *series of events*, as opposed to single events
- Enterprisewide threat hunting capabilities, allowing for mass collection and analysis of host-based artifacts
- Ease of response automation, allowing organizations to collect artifacts pertinent to an investigation before they have a chance to slip away
- Insight into the organization's applications

But perhaps our biggest highlight, across both papers, has been the ease with which Fidelis Elevate brings network and endpoints together. Our focus during this two-part review of Fidelis Elevate has been ***holistic visibility***—treating all the pieces of your environment as a single entity; combining monitoring, detection and analysis into a single platform. Our testing showed that Fidelis Elevate was able to deliver on this focus, ultimately making the life of an analyst—and the job of defending an enterprise-level network—easier and more empowered. A platform such as Fidelis Elevate makes the job of securing a modern global enterprise significantly more achievable, truly making the lives of threat actors more difficult and organizations ultimately more secure.

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:

Fidelis® Cybersecurity