AI Hunting with the Cybereason Platform: A SANS Review

SANS reviewed Cybereason's AI hunting platform, which offers a lightweight, behavior-focused model of host-based protection that can help intrusion analysis and investigations teams more rapidly and efficiently prevent, detect and analyze malicious behavior in their environments.

A SANS Product Review

AI Hunting with the Cybereason Platform:

A SANS Review

Written by **Dave Shackleford**

July 2018

Sponsored by:

Cybereason

Introduction

The threat landscape becomes more daunting by the day. Increasingly sophisticated attacks are being spotted in the wild, and security teams are scrambling to keep up with attacks targeting end users. More than ever, the attacks targeting our endpoints and servers alike are stealthier, harder to detect with traditional tools and more likely to focus on persistence and longer term damage.

In the 2018 SANS "Endpoint Protection and Response" survey, 42 percent of respondents indicated that at least one of their endpoints had been compromised in the previous 12 months, primarily through browser exploits and social engineering.[1] Sixteen percent of those who experienced a compromise noted that they discovered it via third-party notification, which suggests that many endpoint security tools and tactics in use today are inadequate and we really need better prevention and detection tools right now. Almost 60 percent of respondents also indicated that they would like to see artificial intelligence (AI) and machine learning capabilities implemented in their endpoint protection tools but don't currently have them.

The previous generation of signature-based detection tools is failing us. Many attacks don't leverage malware at all: Attackers are using memory-resident techniques, compromised credentials and built-in system tools such as PowerShell to avoid detection by many of the traditional endpoint security platforms. Many endpoint tools also consume significant system resources.

[1] "Endpoint Protection and Response: A SANS Survey," www.sans.org/reading-room/whitepapers/analyst/endpoint-protection-response-survey-38460

SANS had the opportunity to review Cybereason's AI hunting platform, which offers a lightweight, more behavior-focused model of host-based protection that can help intrusion analysis and investigations teams more rapidly and efficiently prevent, detect and analyze malicious behavior in their environments. The company recognizes that most enterprises are lacking analytics experts and don't have enough time to train tier 1 analysts on the job, so one of the primary goals of the platform is to help overcome today's security skills gap. By emphasizing ease of use, built-in intelligence and search tools, rapid event triage, and highly capable hunting methods, Cybereason is a capable, intelligence-driven system that many security operations center (SOC) teams could leverage immediately to prevent or analyze attacks more quickly. Our review environment was set up with real exploits and malware in a testbed operated by Cybereason, and we fully analyzed numerous examples of the product in action.

Ease of Use

The first area we focused on was the platform's overall usability and ease of use. After logging in, we were presented with a main dashboard that has two primary tabs. The first, the Discovery board, is a breakdown of detected events by attack phase or type: Infection, Privilege escalation, Scanning, Lateral movement, command and control (C&C), Data theft, and Ransomware, as shown in Figure 1.

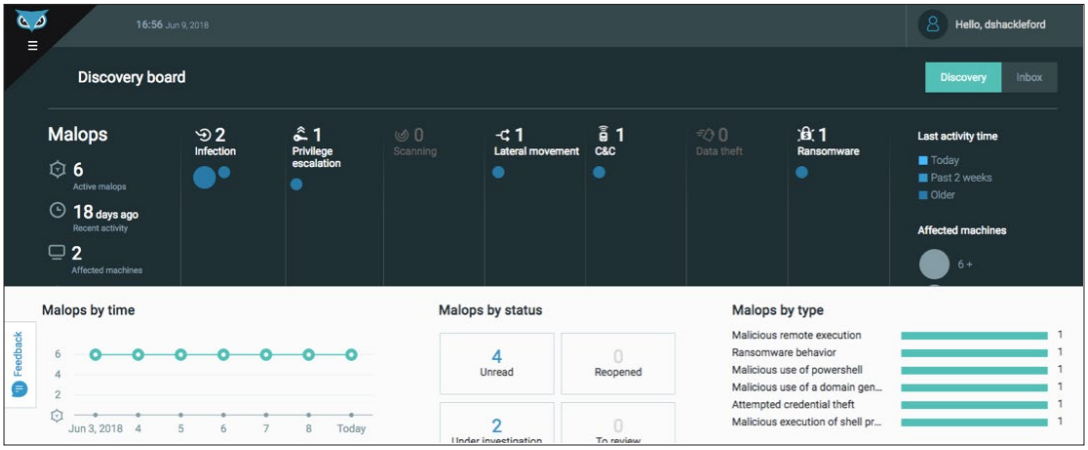

Figure 1. The Cybereason Discovery Board

This screen also lists the number of affected systems, the number of malicious operations (called "malops" in the interface and discussed in more detail later in this review) and most recent activity. Malops are high-fidelity alerts of active malicious operations that are detected and presented in the Cybereason platform when attack details are aggregated and correlated across the environment. The second dashboard is the Malops Inbox, which lists the current malops found in the environment, breaking them down by affected system and category with more immediate detail visible, as seen in Figure 2.

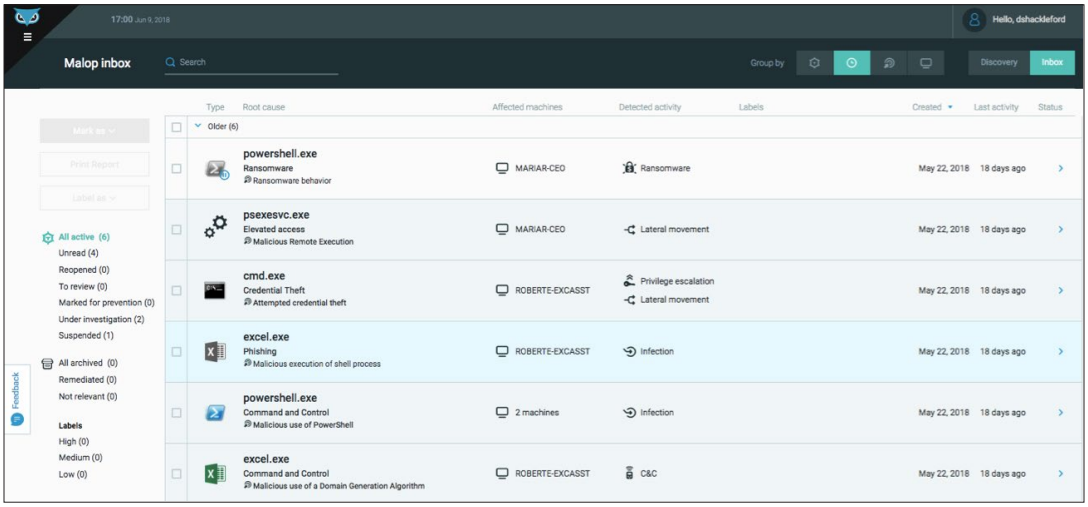

Figure 2. The Cybereason Malops Inbox

From both of these primary dashboards, we could easily click into any observed event

and begin investigating. Other areas of the product we could reach from the primary menu include malware alerts, where any critical alerts regarding malware appear; investigation, where analysts can build and call hunting and other queries; and security profile, where they can configure the product's enabled features (covered in more detail shortly). You can readily access system administration, user accounts and other settings from the same primary menu. Getting around the system was easy, and we were comfortable with the location of all major features and how to find them quickly. Given how quickly we learned our way around, we felt that this interface would allow level 1 analysts to quickly perform fundamental SOC tasks while also providing more advanced analysts with tools to easily perform deeper hunting activities as needed. Saving SOC analysts time is a critical endeavor, and having tools that are easy to navigate and use is vital.

Use Cases

Cybereason's platform readily supports the full spectrum of prevention, detection, triage and threat hunting, and remediation. Let's look at each capability.

Prevention

Prevention is the first area we decided to explore, and Cybereason's static prevention capabilities include both signature-based (dependent on traditional AV attributes or known malware indicators) and signatureless prevention, where malware is exhibiting unusual behaviors even though no signature is known. Malware alerts can break down the types of attempted execution events into prevention and detection categories, as shown in Figure 3.

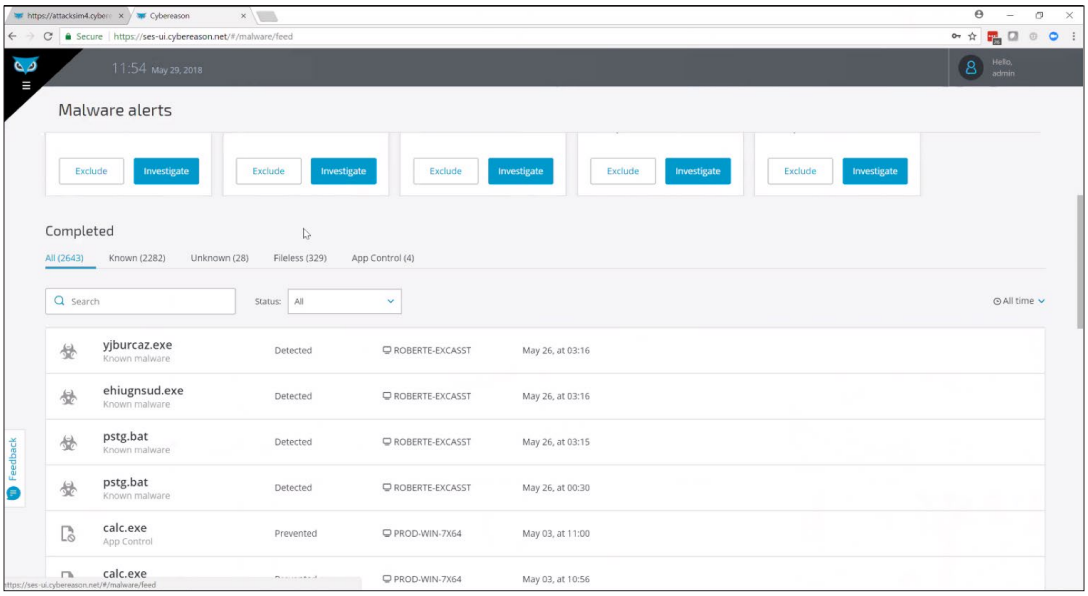

Figure 3. Malware Alerts

Cybereason's dynamic prevention is sophisticated. It relies heavily on context and Cybereason's AI engine, which correlates behavior and indicators within the environment to determine whether an application is acting unusually, whether file-less attacks can block activity if system tools like PowerShell are being used in a malicious fashion, or whether ransomware behavior is being exhibited. This information allows the platform to perform more generic prevention, which can help eliminate the root cause of many more advanced threat scenarios that may start with seemingly normal behavior in the environment. We found that Cybereason caught quite a range of malicious activities within the testbed, including executable malware, ransomware, malicious PowerShell use and embedded exploits in "normal" application files.

Ransomware

While not necessarily a phase in its own right, ransomware attacks exhibit very specific behaviors in infecting systems and seeking out new targets.

Cybereason has an excellent visualization engine that shows all aspects of the malops behavior, including the root cause event, subsequent events and any communication attempts the attack manifests. The company has built an AI engine that continually analyzes huge numbers of events and threat scenarios to produce malops behaviors and outcomes. This engine can significantly increase the efficiency and effectiveness of the hunting activities security analysts need to perform. The company also uses what it calls its "in-memory graph database" to map the memory activity of each system it protects, monitoring for suspicious or unusual behavior and mapping this back to AI-derived patterns that could be correlated with other noted activity. This mapping can occur across the entire enterprise simultaneously, providing very fast analysis and detection, along with a wide scope for quick hunting. In other words, analysts can reach any data point from any other data point within the interface because they are all correlated on the Cybereason platform. Cybereason's variety of graphic dashboards extends to full breakdowns of the attack scenarios being analyzed, including an attack tree model. In Figure 4, the dashboard depicts a command shell running the **`cscript`** command, with outbound communication involved as well.

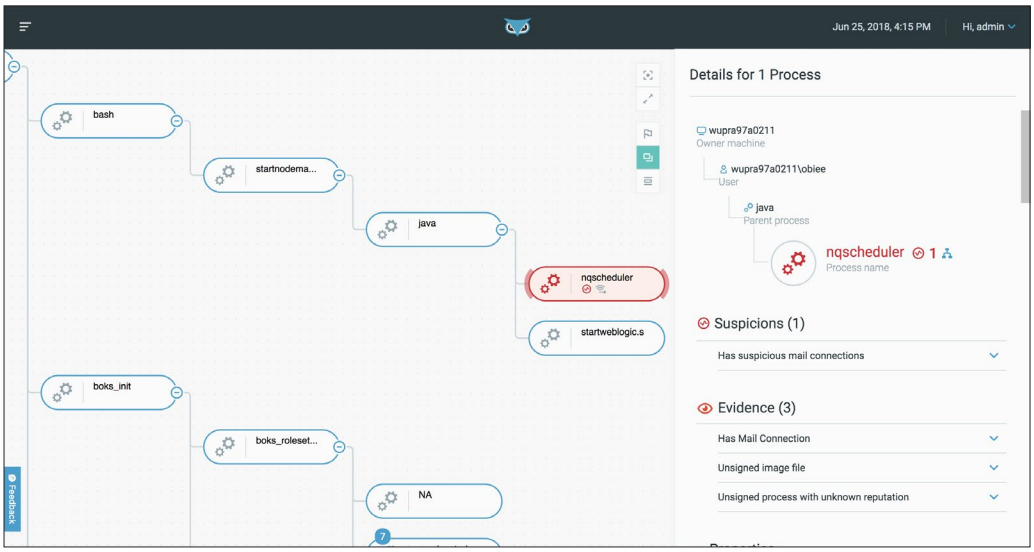

Figure 4. Attack Tree Visualization

AI Hunting

An area where Cybereason has always exceled is in detection and threat hunting. *Malops* are the entire set of stages within an attack scenario correlated together in real time. Cybereason breaks down the attacks it detects into a number of stages, which we followed through during our review of threat hunting.

The infection stage includes malware being dropped on systems, discovery of suspicious files and execution of unusual code. Cybereason detected numerous infection scenarios during our review, ranging from malicious execution of shell processes stemming from a malicious Microsoft Excel file to a malicious PowerShell used for command and control. Figure 5 shows the malicious Excel file executing in a suspicious manner.

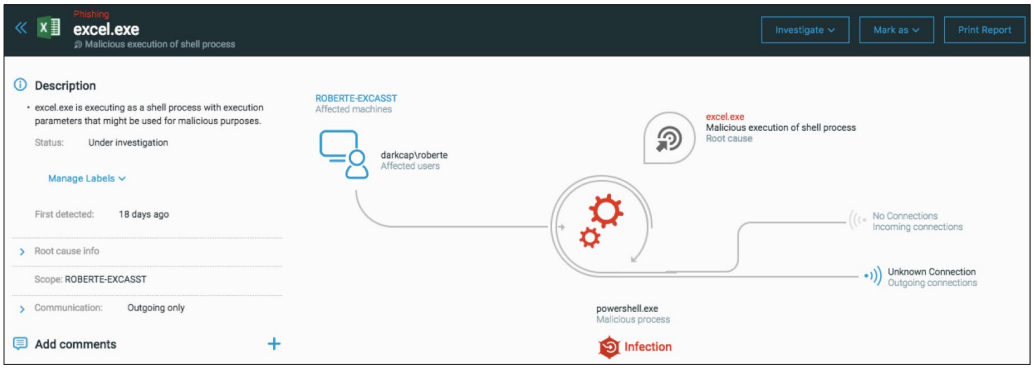

Figure 5. Malicious Excel Infection

Figure 6 shows a more detailed breakdown of the entire attack's processes, including invocation of PowerShell, dropping or loading DLLs and local modules, and outgoing connections.

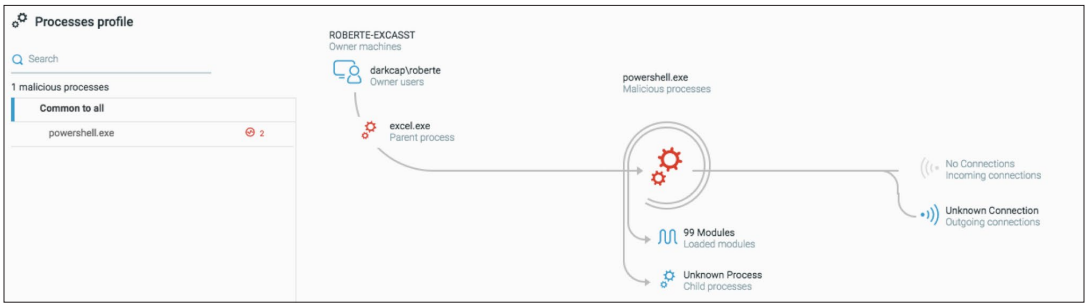

Figure 6. Excel Infection Process Flow

Privilege escalation involves attack elements that seek to access and compromise credentials or other tokens that could be used to perform administrative actions. We saw privilege escalation with attempts to access credentials from a browser exploit that accessed the Windows command shell. In Figure 7, we viewed the timeline of this attack, including shell command execution from the Firefox browser, C&C traffic and attempts to steal credentials.

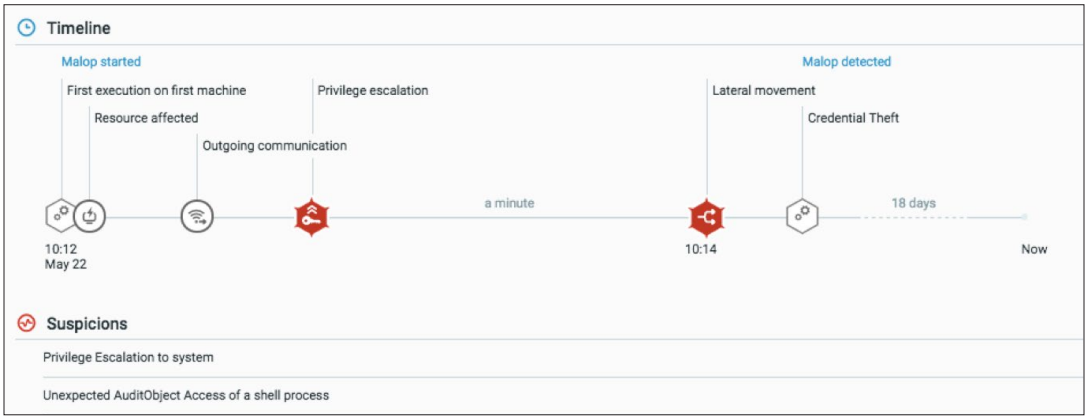

Figure 7. Privilege Escalation Attempt

Cybereason's attack timelines were automatically generated for all activity and very helpful in following through each attempted action within the context of a malicious operation. Analysts could easily leverage these visualizations to drill into any part of an investigation and perform additional detection and response actions.

Scanning activity would include a compromised system trying to communicate with other systems, likely looking for new targets. Most malware performs some sort of network scanning to look for other live systems in the local subnet, and these types of scans are detected due to seemingly random connection attempts to ports and services, as well as system-to-system communication patterns that are highly unusual in most enterprise environments.

An attacker actively trying to access a neighboring system or service in the environment would indicate lateral movement. An example from our test environment included the use of shell commands and the **`PsExec`** service to run a new command shell. Figure 8 shows suspicious PowerShell processes executing, with additional communications on the affected system.

Figure 8. Lateral Movement

C&C attack phases include attempts to communicate outbound to connect to control systems, usually by malware that is seeking new commands to execute from a remote attacker. These types of indicators are detected in numerous ways. Sometimes, the behavior of the affected endpoint may be unusual, communicating with new or unknown domains, at unusual times of day or in unusual patterns of network traffic. The detection of unusual domain names or known malicious IP addresses or network ranges is also common.

Exfiltration of data from the environment is what's happening in the data theft stage and often the ultimate goal of an attacker. These attempts may be detected through content matching in the outbound traffic or simply by the volume or patterns of the outbound traffic sent. Access to local data that contains sensitive information or patterns may be an indicator of imminent data theft as well.

Investigation and Manual Hunting

The Cybereason platform lends itself to a variety of investigation and hunting activities. Hunting within the Cybereason platform is very fluid, and analysts can initiate investigations quickly from any of the malops console dashboards we used (coming from either the Discovery board or the Malops Inbox). From each entry in the threat dashboards, analysts can click the *Investigate* button from the top right and choose one of several options. One option is to simply search Google for the keywords associated with the attack (such as **`powershell.exe`**). Another option is to leverage Cybereason's threat intelligence capabilities, which are spread across a diverse set of customers and environments. The third, and most common, option for many organizations will be the *Investigate root cause* type of investigation, which allows an analyst to dig deeper into the events in the Cybereason dashboard.

Queries

By selecting the root cause investigation option, analysts can access the query screen, which allows for custom filter creation or the use of built-in filters, all using natural language to select key indicators related to the event(s). During this review, SANS performed a number of investigations related to events in the dashboard. All of them were fast and returned responses quickly, due to the use of Cybereason's in-memory monitoring system. The main investigations screen is shown in Figure 9.

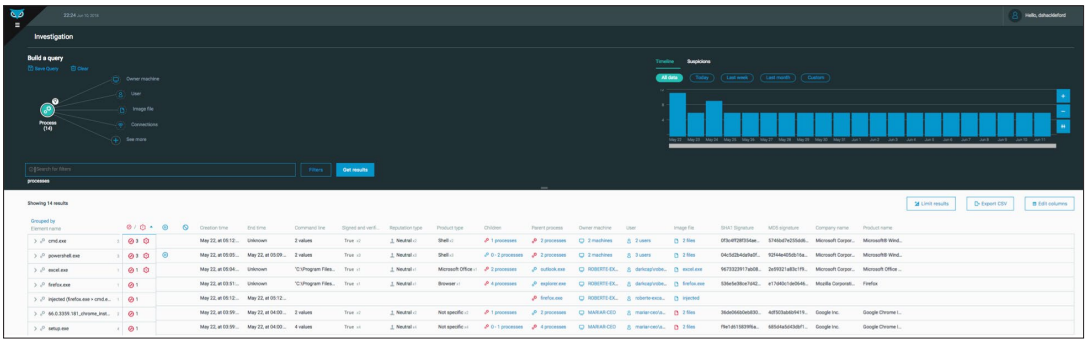

Figure 9. Cybereason Investigations

Everything in this investigations screen is clickable, allowing an analyst to discover more avenues of investigation and keep following indicators and detected events. For more targeted investigations, analysts can use the query functionality of the platform. The query interface has an intuitive search box that prompts analysts

for keywords and information based on what is entered, making this an ideal way for more junior analysts to quickly discover interesting avenues of investigation. Building a query is simple and very granular. Analysts can enter certain keywords and then build out information from a single aspect of the events (processes, users and more). As Figure 10 shows, we can build a simple query from any process where Cybereason suspects malicious activity.

The product also makes it easy to leverage saved queries that have proved useful. During our analysis, we saved queries related to process execution, persistence, privilege escalation, data theft and more (see Figure 11).

With saved queries, organizations can coordinate more efficient detection and investigation by letting more experienced analysts design queries and save them, and then tier 1 analysts can execute the queries to look for issues. Search queries also can include filenames, making it easy to quickly look for known malware variants across the entire set of systems in the environment, as shown in Figure 12 (where we are looking for the **`PsExec`** file).

Any files detected will also include **`SHA1`** hashes, file path on the system and much more.

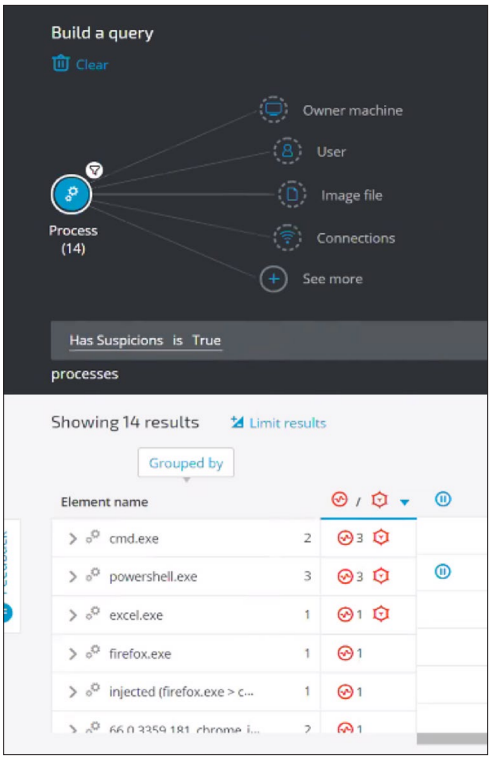

Figure 10. Suspicious Process Query

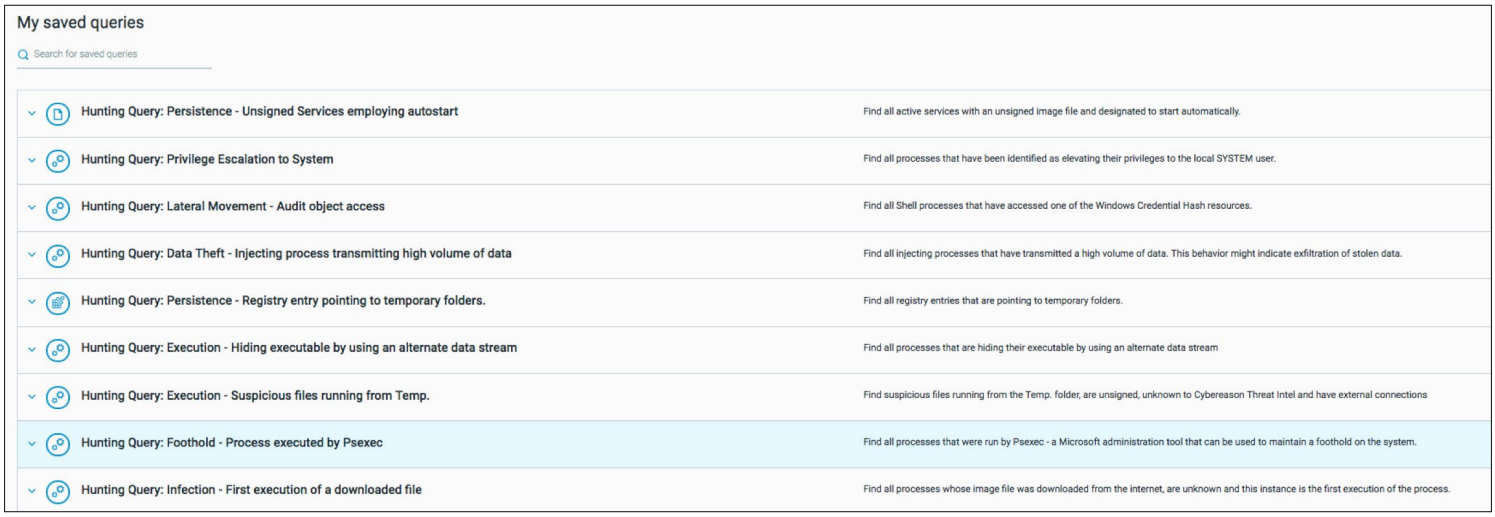

Figure 11. Saved Queries

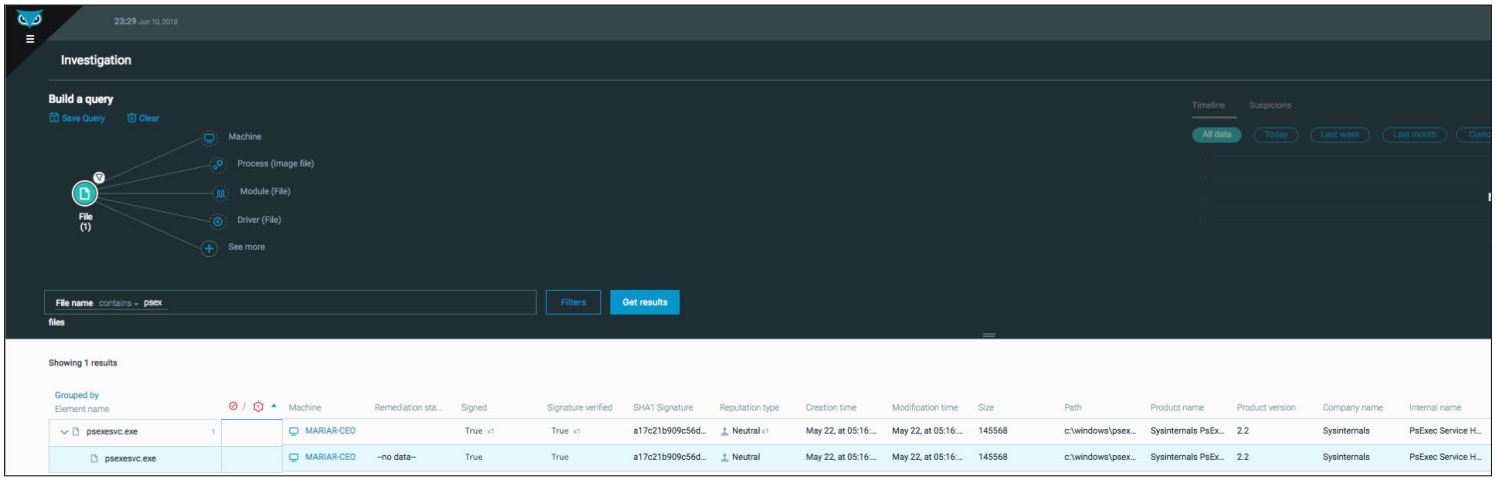

Figure 12. PsExec Search

Remediation

Remediation of attack scenarios is another key feature of the Cybereason platform. Many endpoint detection tools today can search for indicators of compromise (IoC) and potentially alert on issues. But having a single tool that can also help remediate problems when an IoC is found is a major benefit and, in many cases, can empower analysts with IT-level capabilities without needing IT personnel to be involved.

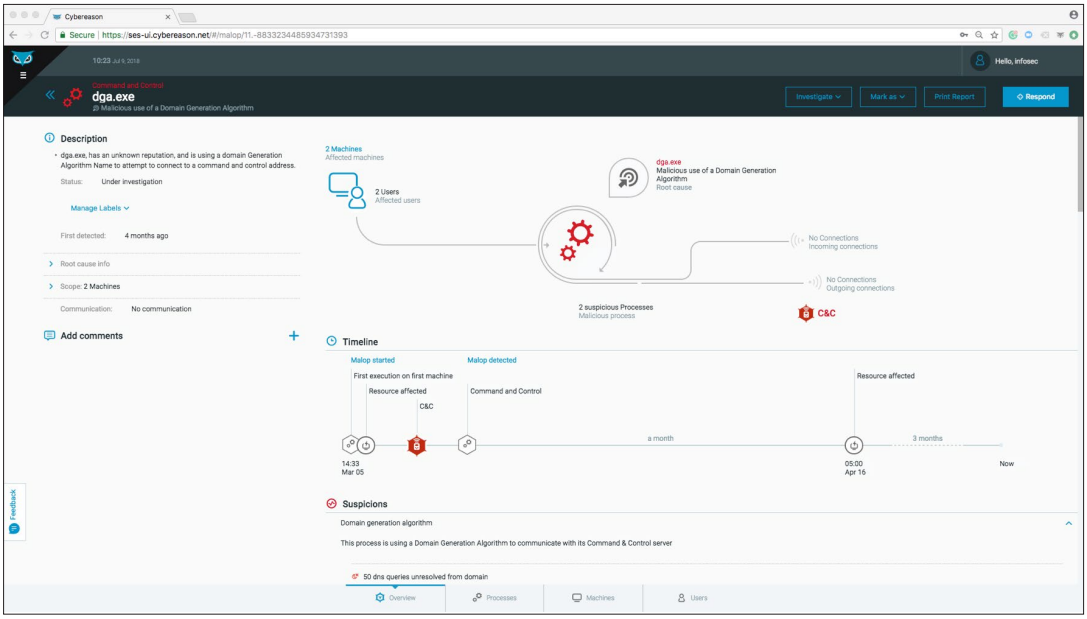

Figure 13. Malop with Response Button

We explored numerous response options during the course of our testing. To make this action simple, Cybereason includes a *Respond* button in the detail screen of every discovered malop. Clicking this button gives the analyst the opportunity to remediate the issue by cleaning up the files or processes detected and prevent the issues from happening again by "teaching" all machines in the environment that it was malicious in the first place. See Figure 13 for an example.

This capability provides true single-click remediation across affected machines, not machine by machine, which can greatly simplify and expedite response activities in large organizations. The Cybereason platform is also flexible in its approach to remediation, with several options depending on the circumstances. First, the platform can isolate systems that are potentially infected. Remediation actions can also include killing processes, removing files, and/or quarantining files, depending on the security analyst's preference. Figure 14 illustrates the Response pane shown after an analyst clicks the Respond button.

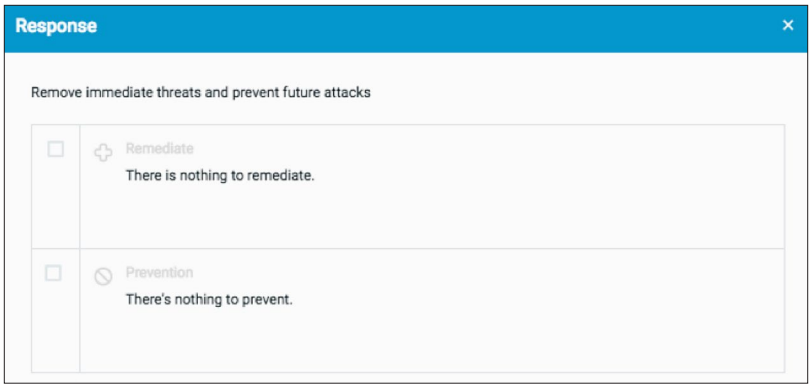

Figure 14. Response Pane

Administration and Security Profiles

The final section of the Cybereason console we explored was the Administration area. Here, we could configure sensor profiles for any agents we wanted to deploy and manage. Cybereason supports Windows, Mac OS X and Linux. Although we did not observe it in our review, Cybereason can scale to significant numbers of sensors in this single dashboard (500,000 or more).

The platform also supports the addition or creation of reputation filters, behavioral whitelisting for malops, and exceptions for isolated systems on specified ports (to allow for very specific monitoring use cases). Anti-malware options allow for prevention and detection-only models of operation, as well as sensitivity ranges for AI operations. Analysts can create exclusions and scheduled scans. Cybereason has a number of configuration options for protecting PowerShell on Windows systems, too. Prevention and detection options are available for execution of code and downloads. We liked the overall granularity of these options, which give analysts more direct and manual control of critical settings where desired. The platform is also flexible in creating exclusions and analyzing scripts (see Figure 15).

Another customizable set of policies relates to ransomware. Cybereason can create "canary" files that detect ransomware activities early and trigger alerting and response actions. This function is a unique approach to ransomware detection that is much more sophisticated than most. In addition to leveraging deception tactics, Cybereason monitors specific behavioral patterns of access to the canaries once they exist, providing an even higher degree of accuracy, which is invaluable to any SOC analyst who has battled false positives. Cybereason can also detect shadow copy and Master Boot Record (MBR) modifications, as shown in Figure 16.

The second major section of the Admin area is the user configuration, where we created specific users and assigned roles. We found that Cybereason is more granular in its role categories than most other products we've seen, with options ranging from executives and user/system admins to SOC analysts (tiers 1 through 3). These roles are customizable, too, and Cybereason also has a number of predefined roles, such as the SOC lead or super-user. The user creation screen is seen in Figure 17 on the next page.

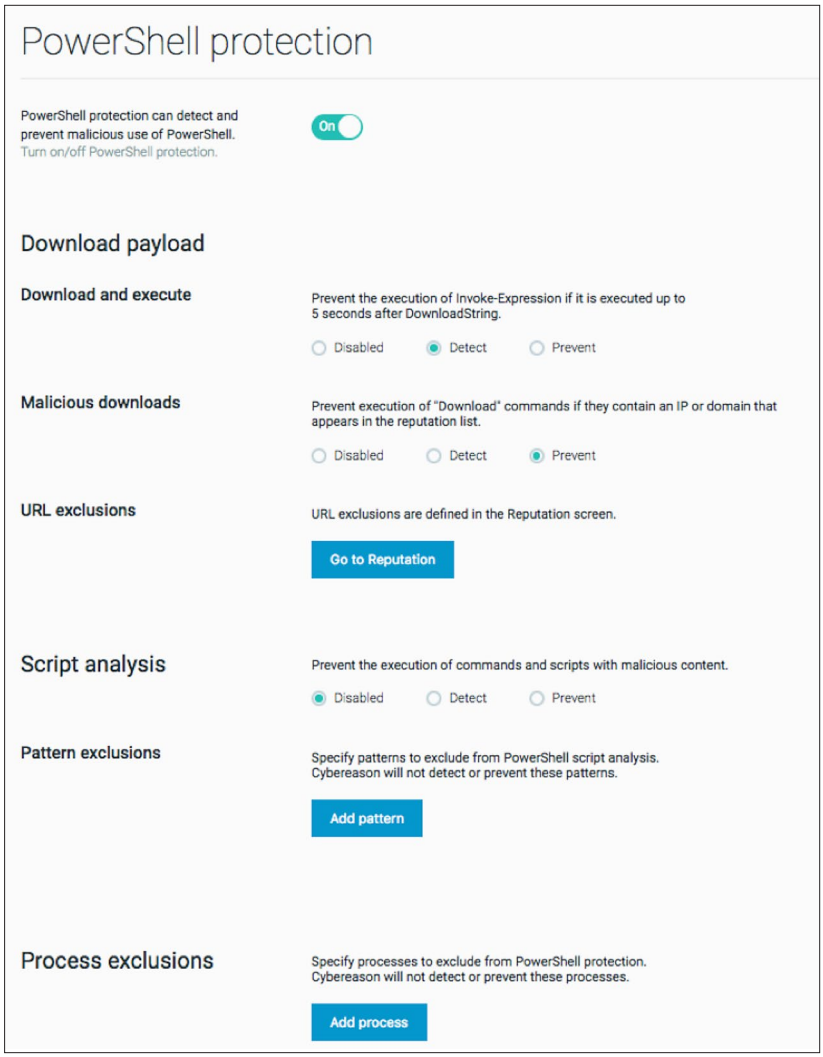

Figure 15. PowerShell Protection

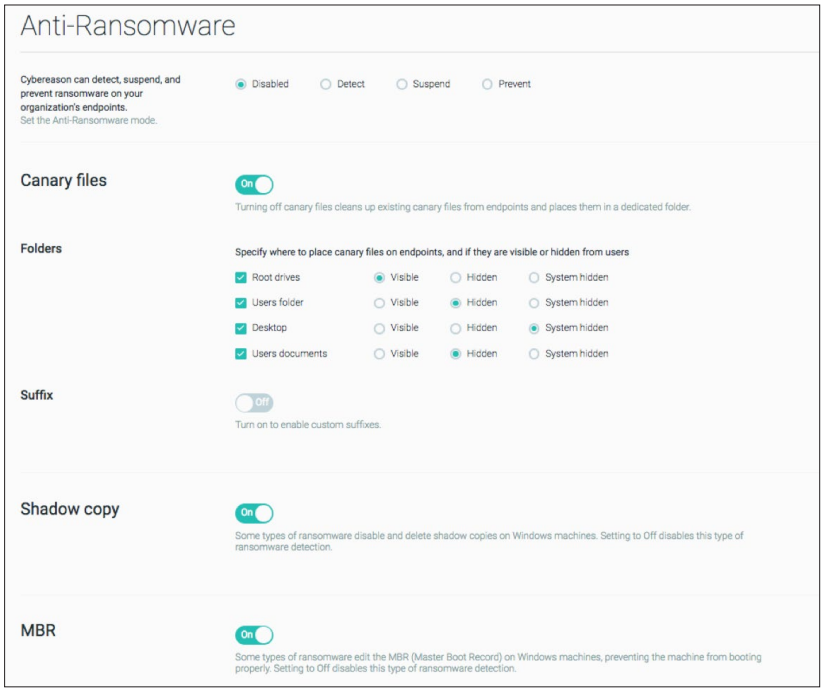

Figure 16. Ransomware Controls

Last, the platform supports settings to configure alerting through email, strong authentication and others, most of which we didn't test during this review.

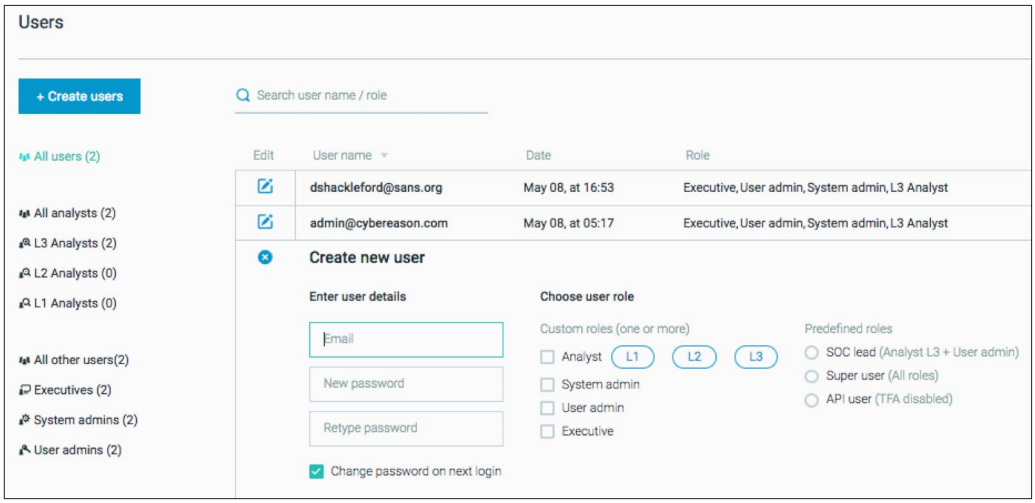

Figure 17. User and Role Creation and Assignment

Conclusion

Overall, Cybereason impressed us with its capabilities and thorough coverage of prevention, detection and response. The product was easy to get started with and use, and the various dashboards were intuitive to navigate. Creating endpoint policies was straightforward, and communicating with sensors was fast and painless.

Cybereason has some of the best visualization tools we've seen for endpoint security analysis. Junior analysts can easily dig deep, query systems and leverage queries built by more senior analysts. A tool that combines both next-generation AV and endpoint detection and response can simplify security operations and reduce overhead on systems. In addition, Cybereason is bringing a lot of advanced techniques together for a unique approach to layered defenses. Signature and AI-based signatureless prevention and detection, deception and behavioral monitoring for ransomware prevention, and emphasis on native tools like PowerShell make this a powerful group of combined tactics that analysts can benefit from. We found that the platform also provides all the necessary tools to hunt for files, processes and behaviors across all endpoints very rapidly, and then take remediation actions immediately.

About the Author

Dave Shackleford, a SANS analyst, instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsor

SANS would like to thank this paper's sponsor:

Last Updated: July 26th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Amsterdam October 2018	Amsterdam, NL	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Riyadh July 2018	OnlineSA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced