WHITE PAPER

How Symantec® Endpoint Security Complete Helps Detect, Investigate, and Respond to Advanced Attacks

TABLE OF CONTENTS

Introduction

Today's environment is difficult for defenders. The threat landscape continues to evolve with expanded threats from the supply chain, more sophisticated phishing, and an ever-expanding set of vulnerabilities. Regardless of the latest methods used by the most advanced attackers, Symantec® Endpoint Security (SES) Complete provides cutting edge technologies so you can know when your organization is under attack, determine the scope of the attack, and contain and eradicate the threat.

In this paper we show a real world attack and how SES Complete blocks most attacks before any damage is done, alerts you to suspicious activities, and gives you the tools to confidently defend your organization.

The Attack

Browser Executes Malicious JavaScript

The attack starts with a web browser dropping and executing JavaScript. This malicious JavaScript is obfuscated to avoid detection and make analysis difficult. This first stage of the attack determines if the victim is worthy of continuing the attack. It performs discovery of the local user and system and communicates this information to a Command and Control server. After determining that this is a suitable victim, it downloads and executes malicious PowerShell.

PowerShell-Based Bypass User Access Control

At this phase of the attack, the attacker has only limited user access, which makes it difficult to do very much on the machine. Thus, the attacker's next step is to elevate privileges.

PowerShell-Based Discovery, Credential Theft, Exfiltration, and Lateral Movement

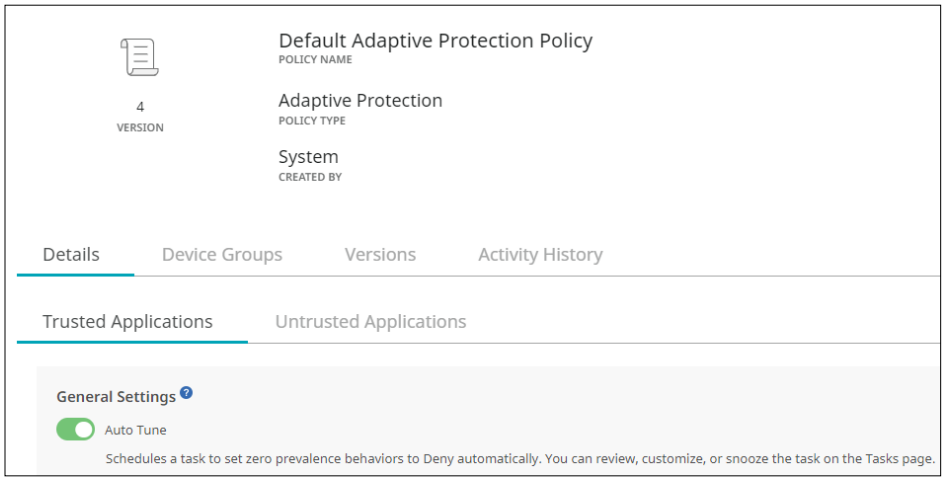
Now that the attacker has local administrator privileges, the attacker has greater capabilities. With this, the attacker learns more about the user, system, and other machines on the network, steals credentials, exfiltrates the stolen data, and moves laterally to other machines on the network.

ADAPTIVE PROTECTION IS ONE OF THE MOST POWERFUL TOOLS FOR BLOCKING ADVANCED ATTACKS BEFORE ATTACKERS CAN GAIN A TOEHOLD.

Blocking The Attack Before It Even Gets Started

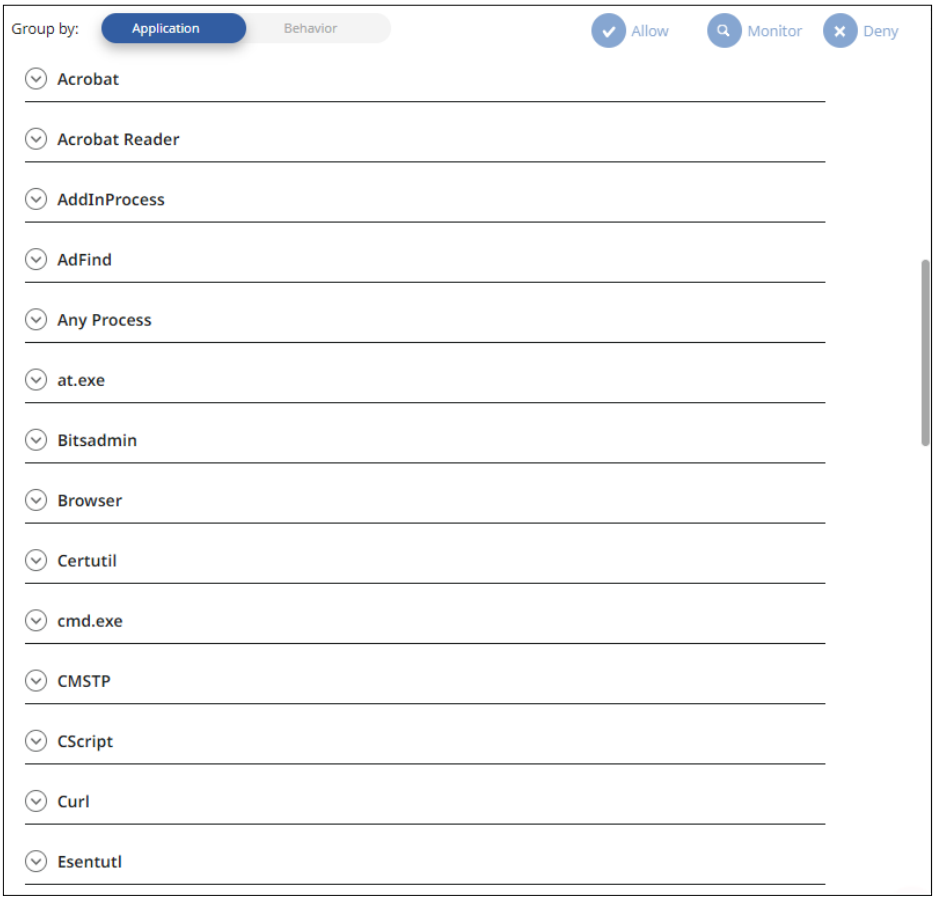
Adaptive Protection is one of the most powerful tools for blocking advanced attacks before attackers can gain a toehold. Attackers often attempt to hide their activities by leveraging legitimate operating system binaries or other common binaries such as web browsers or document viewers/editors. Adaptive Protection uses this knowledge to close off these avenues of attack. To accomplish this, Adaptive Protection first learns how these commonly exploited applications currently function in the environment. Then, once Adaptive is sure there is no legitimate use, it automatically blocks all future malicious behaviors.

First, enable automatic learning by going to the Adaptive Protection policy and turning on Auto Tune, and apply the policy to the appropriate Device Groups.



POWERSHELL IS A POTENT ADMINISTRATIVE TOOL THAT CAN DO NEARLY ANYTHING THE ADMINISTRATOR WANTS TO DO.

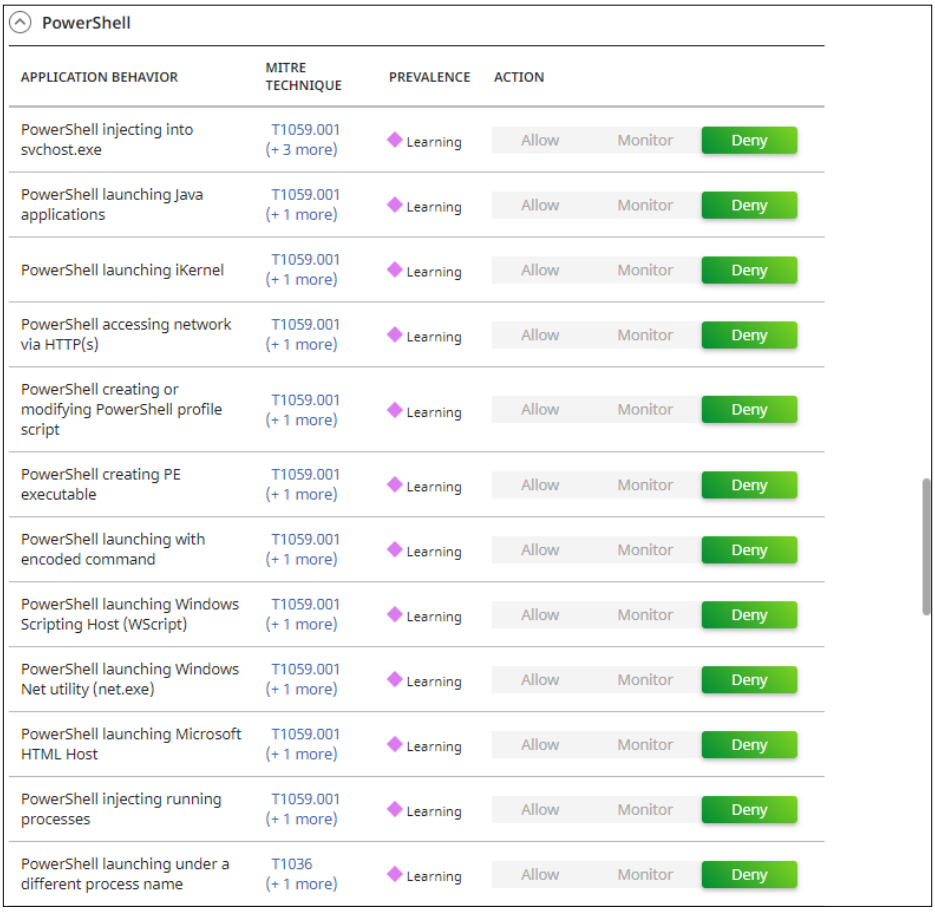
Adaptive Protection secures a wide variety of commonly misused programs. Click on any of the drop down arrows to see more details.



Take PowerShell as an example. PowerShell is a potent administrative tool that can do nearly anything the administrator wants to do. The attackers know this and also leverage PowerShell, hoping to look like normal administrator activity. Adaptive Protection learns how PowerShell is used in the organization, then prevents other malicious uses of PowerShell while allowing the normal administrative activities.

ADAPTIVE PROTECTION DETERMINES WHICH PROTECTIONS WON'T INTERFERE WITH YOUR NORMAL WORKFLOWS.

Here's a sampling of the PowerShell Adaptive Protection behaviors.



PowerShell

APPLICATION BEHAVIOR	MITRE TECHNIQUE	PREVALENCE	ACTION
PowerShell injecting into svchost.exe	T1059.001 (+ 3 more)	Learning	Allow Monitor Deny
PowerShell launching Java applications	T1059.001 (+ 1 more)	Learning	Allow Monitor Deny
PowerShell launching iKernel	T1059.001 (+ 1 more)	Learning	Allow Monitor Deny
PowerShell accessing network via HTTP(s)	T1059.001 (+ 1 more)	Learning	Allow Monitor Deny
PowerShell creating or modifying PowerShell profile script	T1059.001 (+ 1 more)	Learning	Allow Monitor Deny
PowerShell creating PE executable	T1059.001 (+ 1 more)	Learning	Allow Monitor Deny
PowerShell launching with encoded command	T1059.001 (+ 1 more)	Learning	Allow Monitor Deny
PowerShell launching Windows Scripting Host (WScript)	T1059.001 (+ 1 more)	Learning	Allow Monitor Deny
PowerShell launching Windows Net utility (net.exe)	T1059.001 (+ 1 more)	Learning	Allow Monitor Deny
PowerShell launching Microsoft HTML Host	T1059.001 (+ 1 more)	Learning	Allow Monitor Deny
PowerShell injecting running processes	T1059.001 (+ 1 more)	Learning	Allow Monitor Deny
PowerShell launching under a different process name	T1036 (+ 1 more)	Learning	Allow Monitor Deny

By default, Adaptive Protection determines which protections won't interfere with your normal workflows. You can also choose to Allow, Monitor or Deny any behavior manually.

In the case of the attack outlined above, the organization uses JavaScript in its normal activities, so this is allowed. However, normally JavaScript doesn't do Account Discovery nor does it launch PowerShell, so these are blocked automatically. The block is made not by signatures, which can be bypassed by attackers obfuscating or otherwise modifying their code. Rather, the behaviors themselves are blocked, closing off whole techniques from any chance of exploitation.

Here's an example of SESC blocking key elements of the attack based on Adaptive Protection.

TIME ↑	DESCRIPTION	DISPOSITION	PARENT CMD LINE	PROCESS COMMAND LINE
Nov 14, 2022, 2:09:11 PM	Windows Scripting Host (WScript) launching PowerShell (actor: ...	1-Process Detection - Blocked	"C:\Windows\System32\wscript.exe" jkhert...	PowerShell -windowstyle hidden -NoProfile -...
Nov 14, 2022, 2:09:10 PM	PowerShell accessing network via HTTP(s) (actor: PowerShell) (ta...	1-Process Detection - Blocked	"C:\Windows\System32\wscript.exe" jkhert...	PowerShell -windowstyle hidden -NoProfile -...
Nov 14, 2022, 2:09:06 PM	Windows Scripting Host (WScript) launching Windows Net utility ...	1-Process Detection - Blocked	"C:\Windows\System32\wscript.exe" jkhert...	net user

Adaptive Protection is just one of the many cutting edge technologies SES Complete brings to bear to prevent breach. The protection provided by SES Complete's Firewall, Network Intrusion Protection, Device Control, System Lockdown, Memory Exploit Detection, Reputation, Advanced Machine Learning, Emulation, Deception, and Behavioral Monitoring is deep. While some competitors defend offering inferior protection with sayings like "breach is inevitable", we believe that protection is a critical piece of security posture. At the end of the day, the best protection will block many attacks, offer insight into attacks in progress, and cause some attackers to go after softer targets.

You wouldn't leave your front door unlocked just because you have security cameras. Similarly, the best security posture is to leverage the best protection as well as the best detection for when protection fails.

Even if the attackers kept modifying their techniques, the next step is blocked anyway, and the step after that, and the step after that. Quite simply, SES Complete is a potent protection solution because it offers multiple complementary control layers. That's why SES Complete received SE Labs' Best Enterprise Endpoint award for 2023 (source https://selabs.uk/wp-content/uploads/2023/02/annual-report-2023.pdf page 18), and AV-TEST's Best Protection award in 2022 (the latest year it was awarded; source https://www.av-test.org/en/news/av-test-award-2022-tested-and-award-winning-security/) for "perfect protection against malware, far above the industry average".

Even if the attacker is persistent and changes their initial techniques (alerting you along the way), subsequent steps of the attack are blocked as shown here.

Nov 16, 2022, 3:35:31 PM	PowerShell created a suspicious PE executable	1-Process Detection - Blocked	"C:\Windows\system32\ChangePk.exe"	"PowerShell.exe" -windowstyle hidden -exec bypass -C "IEX (New...
Nov 16, 2022, 3:35:34 PM	Windows Scripting Host (WScript) launched sc.exe	1-Process Detection - Blocked	"PowerShell.exe" -windowstyle hidden -exec by...	"C:\Windows\system32\sc.exe" query
Nov 16, 2022, 3:35:34 PM	PowerShell executing Windows Service Control utility (sc.exe) (actor...	1-Process Detection - Blocked	"PowerShell.exe" -windowstyle hidden -exec by...	"C:\Windows\system32\sc.exe" query
Nov 16, 2022, 3:35:35 PM	Windows Scripting Host (WScript) launching Windows Net utility (n...	1-Process Detection - Blocked	"PowerShell.exe" -windowstyle hidden -exec by...	"C:\Windows\system32\net.exe" share
Nov 16, 2022, 3:35:36 PM	PowerShell launching Windows Net utility (net.exe) (actor: PowerSh...	1-Process Detection - Blocked	"PowerShell.exe" -windowstyle hidden -exec by...	"C:\Windows\system32\net.exe" share

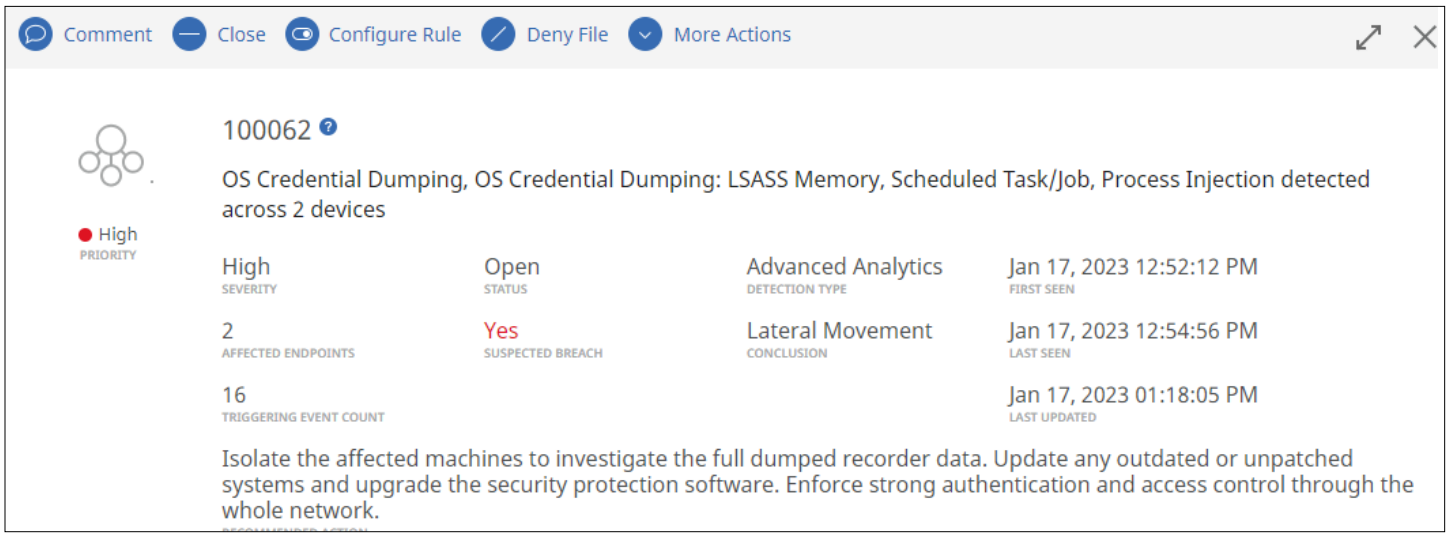
But What If, Even After All That, The Attack Succeeded?

Even though the attack was stopped again and again and again before it even got a toehold, Symantec's defense-in-depth approach still plays out. From here on, we simulate what would happen if each subsequent block didn't happen by putting SES Complete into a special Monitor Only mode. SES Complete will alert us of suspicious activities but will not block any of them. While it is not recommended to run in Monitor Only mode in a production environment, we do so in this case to see how SES Complete would react to the rest of the attack assuming each previous step was not blocked.

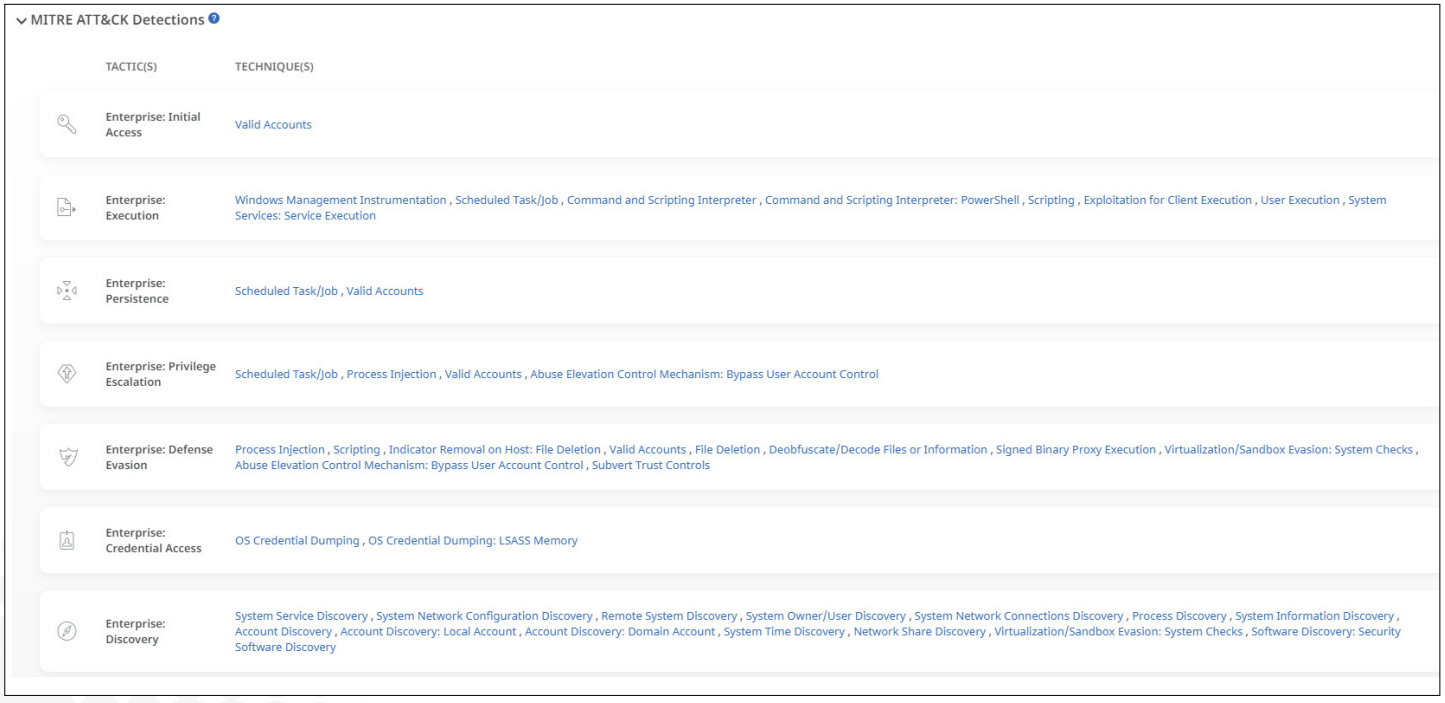
SES Complete alerts you with a high severity incident warning of credential theft and privilege escalation.

ID ↓	DESCRIPTION	SEVERITY	ENDPOINT COUNT
100062	OS Credential Dumping, OS Credential Dumping: LSASS Memory, Scheduled Task/Job, Process Injection detected across 2 devices	High	2

A number of views help summarize the attack. First, the incident description shows some of the most critical MITRE ATT&CK techniques leveraged by the attackers.

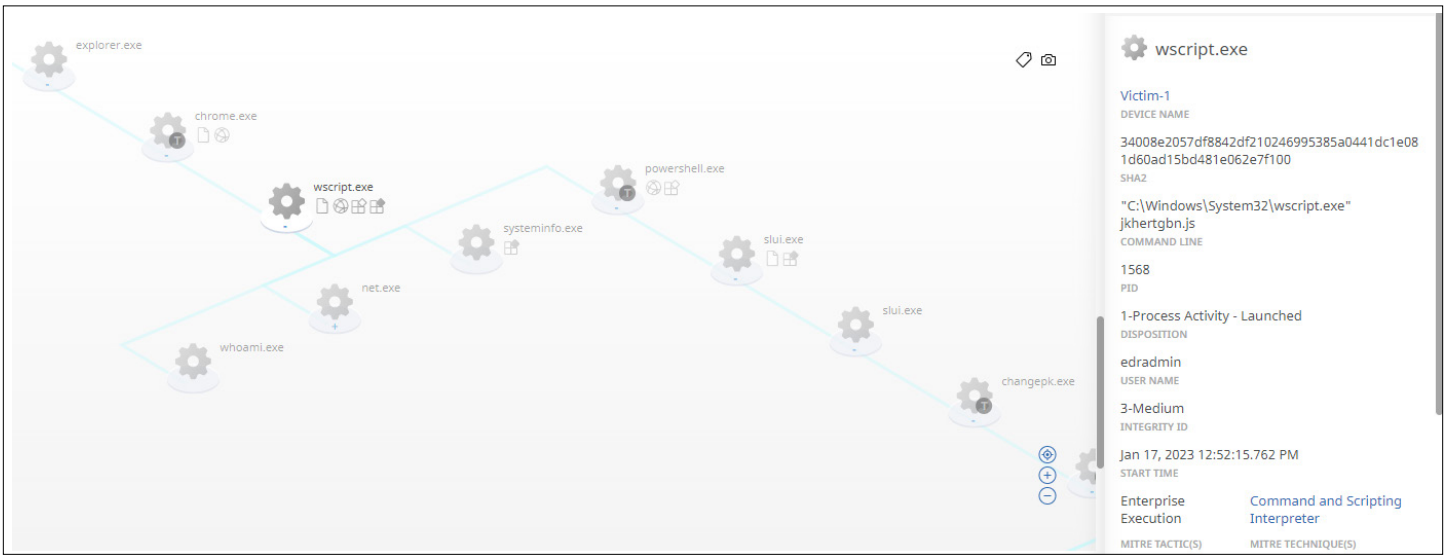


The MITRE ATT&CK Detections section shows a more detailed list of all the ATT&CK Tactics and Techniques utilized in the attack.

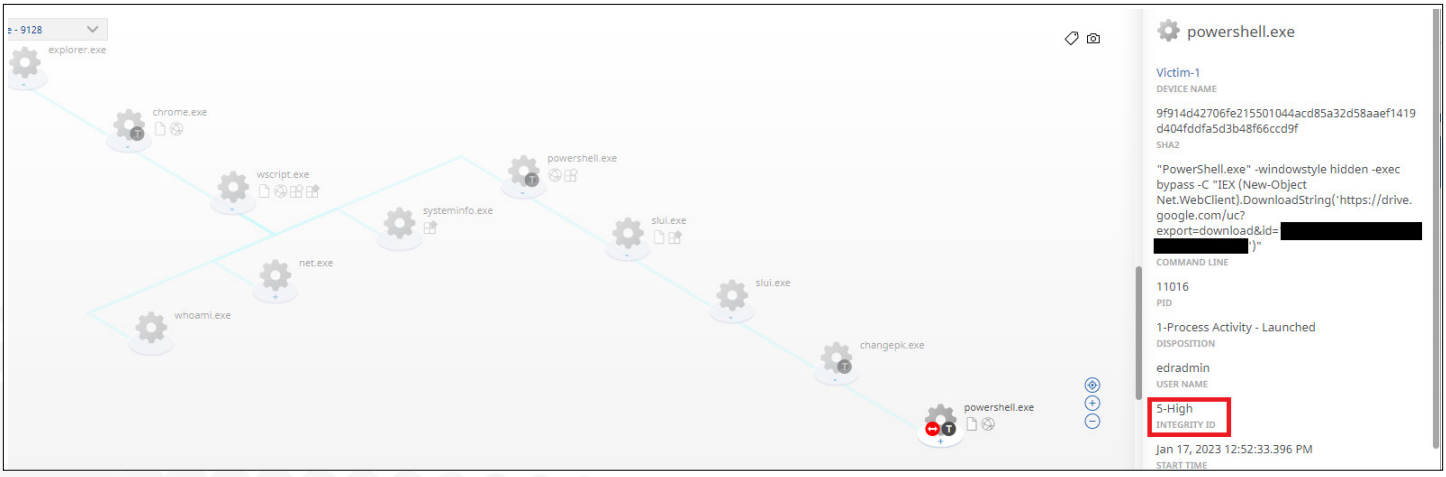


The Lineage Visualization is a super useful view to see how the attack progressed across processes. Here we see chrome.exe launched wscript.exe, which started the attack. WScript then calls whoami, net, and systeminfo to determine if this is a machine the attacker is interested in. Then powershell.exe is called to perform a UAC Bypass.

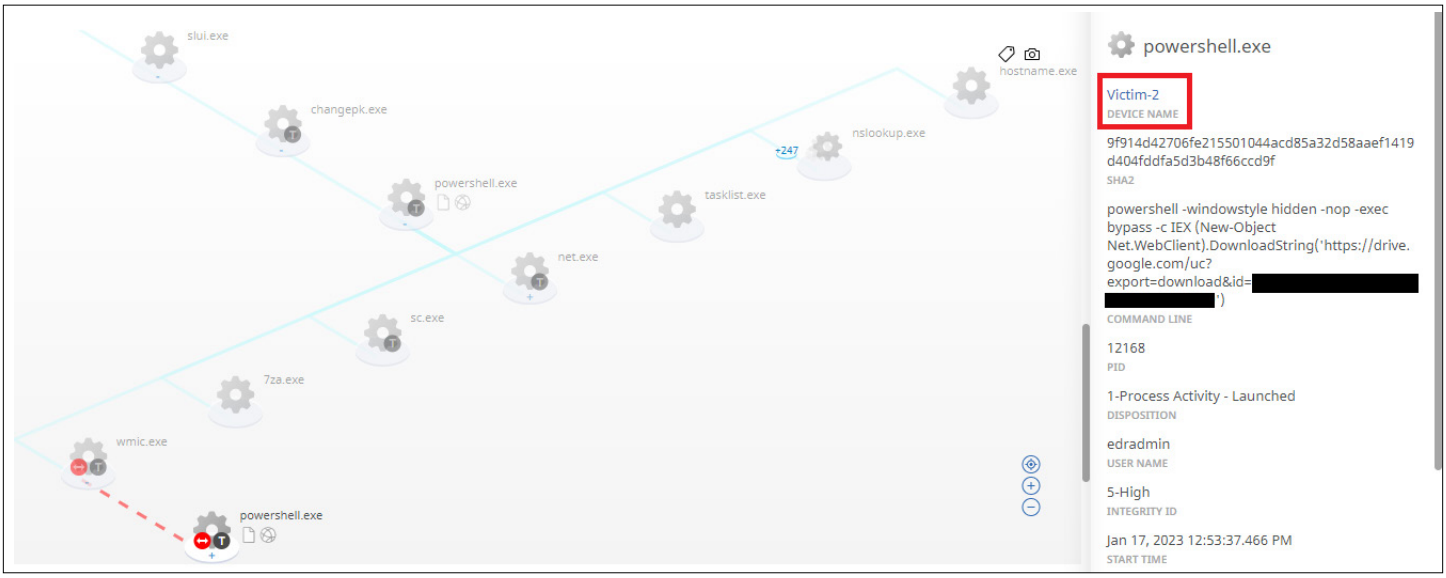
Clicking on any process, as we have done for wscript.exe, gives more details about the process such as the command line, user, and integrity level.



Looking further down the lineage graph, we see that PowerShell launches slui.exe, which launches another instance of slui.exe, which launches changepk.exe, which launches PowerShell. This is all part of a UAC Bypass leveraging the Windows licensing tools. More information is available at https://mattharr0ey.medium.com/privilege-escalation-uac-bypass-in-changepk-c40b92818d1b. This is indicated in SES Complete by the last version of PowerShell running at High Integrity Level.



Looking even further down the lineage graph, we see PowerShell calls wmic. Then there is a red dotted line and another PowerShell process. This indicates that lateral movement has occurred where wmic caused PowerShell to launch on another machine. Notice the Device Name of the latest PowerShell instance is now Victim-2, indicating that the threat has moved from Victim-1 to Victim-2.



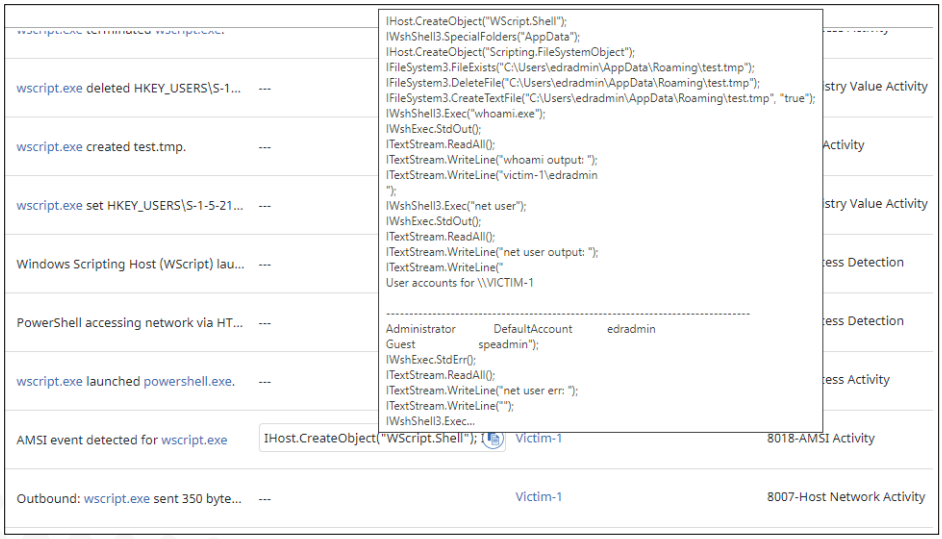
The Events area shows, in very granular detail, every step of the attack. Here's a screenshot of the very beginning of the attack where the user launches Chrome. Chrome performs some network activity, downloads the malicious JavaScript, then launches wscript.exe to run the malicious JavaScript.

TIME ↑	DESCRIPTION	ATT&CK TECHNIQUE NAME	PROCESS COMMAND LINE	EVENT TYPE ID	DEVICE NAME
Jan 17, 2023, 12:52:12 PM	explorer.exe launched chrome.exe.	User Execution	"C:\Users\edradmin\AppData\Roaming\Google C...	8001-Process Activity	Victim-1
Jan 17, 2023, 12:52:14 PM	Outbound: chrome.exe sent 618 byte...	Application Layer Protoc... + 1 other	---	8007-Host Network Activity	Victim-1
Jan 17, 2023, 12:52:15 PM	An untrusted process launched a sys...	Process Injection	"CSIDL_PROFILE\appdata\roaming\google chrome...	8027-Process Detection	Victim-1
Jan 17, 2023, 12:52:15 PM	Outbound: chrome.exe sent 806 byte...	Application Layer Protoc... + 1 other	---	8007-Host Network Activity	Victim-1
Jan 17, 2023, 12:52:15 PM	chrome.exe created javascript[1].	Ingress Tool Transfer	---	8003-File Activity	Victim-1
Jan 17, 2023, 12:52:15 PM	chrome.exe created jkhertgbn.js.	Ingress Tool Transfer	---	8003-File Activity	Victim-1
Jan 17, 2023, 12:52:15 PM	chrome.exe launched wscript.exe.	Command and Scripting... + 1 other	"C:\Windows\System32\wscript.exe" jkhertgbn.js	8001-Process Activity	Victim-1

ONE TREMENDOUSLY HELPFUL ASPECT OF THIS ANALYSIS IS THAT SES COMPLETE AUTOMATICALLY DECRYPTS OBFUSCATED, ENCODED, AND ENCRYPTED SCRIPTS.

One tremendously helpful aspect of this analysis is that SES Complete automatically decrypts obfuscated, encoded, and encrypted scripts. The JavaScript downloaded and run by Chrome in this attack is obfuscated to the point that normal humans can no longer decipher it.

Symantec Endpoint Detection and Response (SEDR), however, decodes the script for you and shows you exactly what the script is really doing. It tells you that the script ran, and also shows variable values, like the Account Discovery data that's being staged as the script runs, as shown below. This greatly simplifies analysis to confirm that the script is indeed malicious and the activities performed.



SES COMPLETE KEEPS TRACK OF DATA IN TRULY STAGGERING AMOUNTS.

Need Even More Data? SES Complete Has You Covered!

SES Complete keeps track of data in truly staggering amounts.. Each endpoint generates hundreds of thousands of events per day, taking up approximately 1 GB of data per endpoint per day. It's a truly staggering amount of data. With numbers like that, SES Complete needs world class engineering to store it all.

That's done with a distributed database. The data most likely to be needed is kept in the cloud database where it's most easily accessible. The remaining data is kept on endpoints to be leveraged whenever it's needed.

There are two cases when data is moved from the endpoint store to the cloud.

1. Whenever a suspicious activity occurs, SES Complete examines the attack lineage to find all actors involved. It then pulls up all of their recorded activity, thus saving you time by having all of the related activity available for your investigation.

2. You can choose to move data from endpoints to the cloud when you will be using the data frequently.

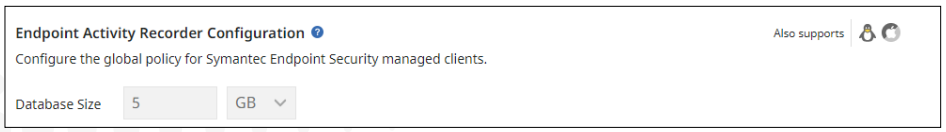
What type of data is normally kept in the cloud versus on endpoints?

Cloud	Endpoint
Process launches	DLL loads
All suspicious activity	File creation, modification and deletion
Activities related to any process group that has performed suspicious activities	Registry key/value creation, modification and deletion
Network activity summaries	Network activity details

Inside the Detection and Response policy, administrators control what is recorded and where it is stored. Policies can be tailored to the whole organization, to groups or even individual machines.

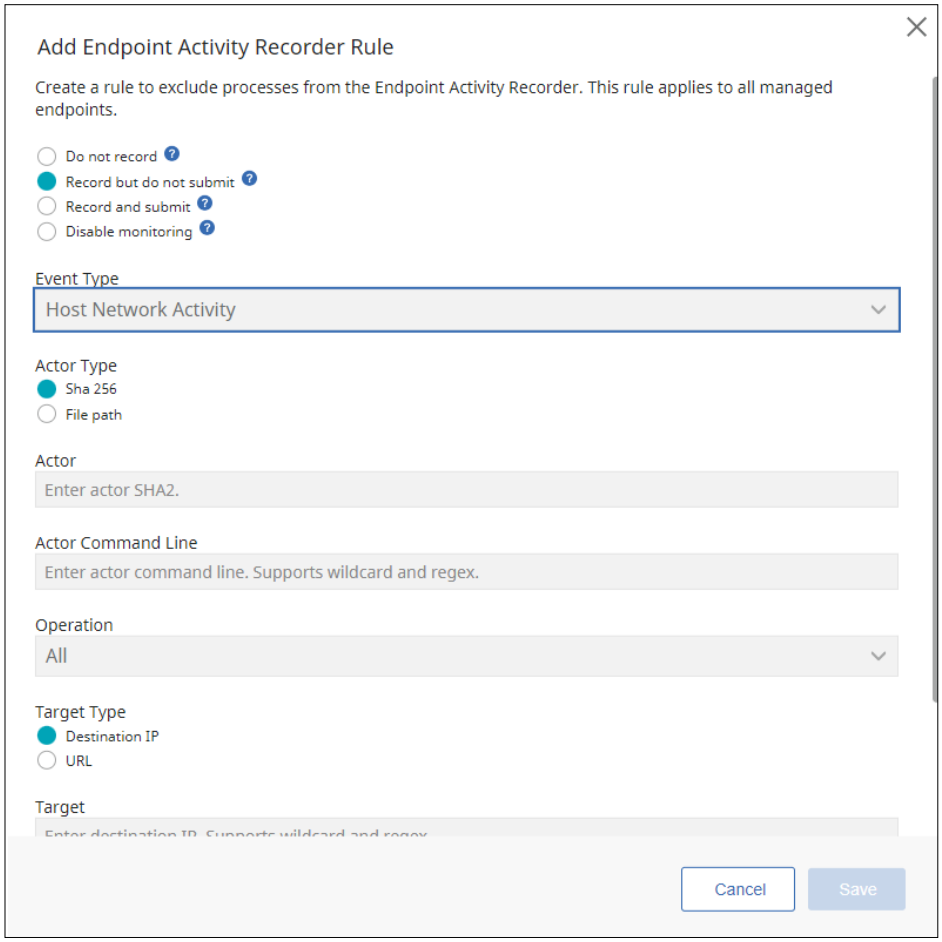
Configuring Endpoint Activity Collection

SES Complete gives you control over how much data will be stored on endpoints.



WHENEVER A SUSPICIOUS ACTIVITY OCCURS, SES COMPLETE EXAMINES THE ATTACK LINEAGE TO FIND ALL ACTORS INVOLVED. IT THEN PULLS UP ALL OF THEIR RECORDED ACTIVITY, THUS SAVING YOU TIME BY HAVING ALL OF THE RELATED ACTIVITY AVAILABLE FOR YOUR INVESTIGATION.

For fine-grained control over what data are stored and where they are stored, add Endpoint Activity Recorder rules.



This allows users to have fine-grained control over what event types such as Process, File, Registry, and Network are recorded, and where the data are stored.

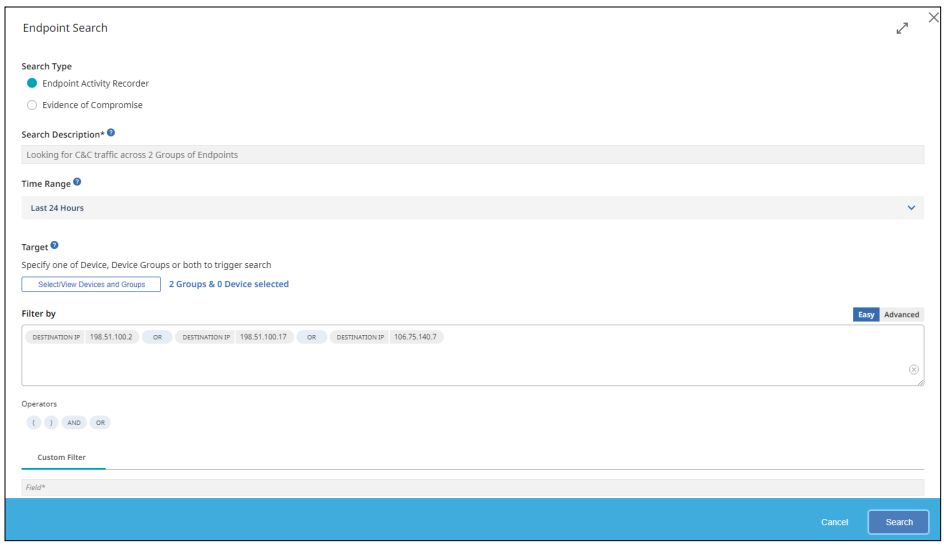
Performing Endpoint Indicator of Compromise Searches, Full Dumps and Process Dumps

To search endpoint data, go to the Investigate tab, select Endpoint, and press the Endpoint Search button. There are two different search types:

- Endpoint Activity Recorder - look through the endpoint's database of activities that have occurred.
- Evidence of Compromise - examine the current state of the endpoint looking for targets such as files, registry entries, or running processes.

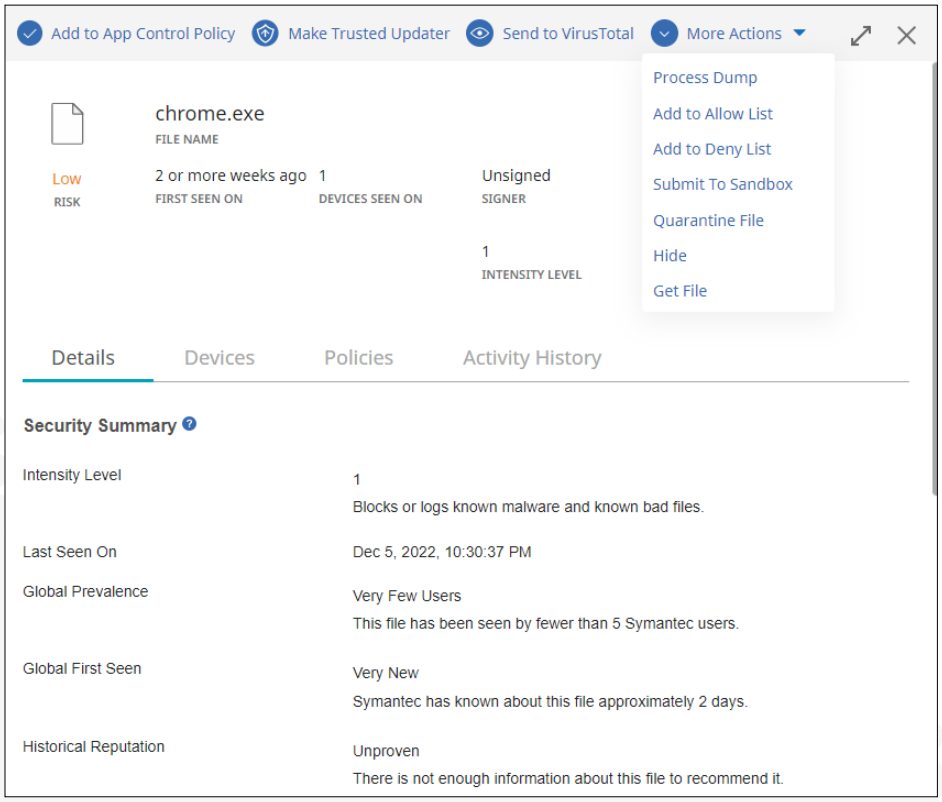
IF MULTIPLE ENDPOINT ACTIVITY RECORDER SEARCHES ARE PLANNED, ENDPOINT DATA CAN BE UPLOADED TO THE CLOUD FIRST TO MAKE SEARCHING FASTER.

Here's an example of an Endpoint Search for C&C traffic. Here we're looking for any network activity with three known C&C servers.



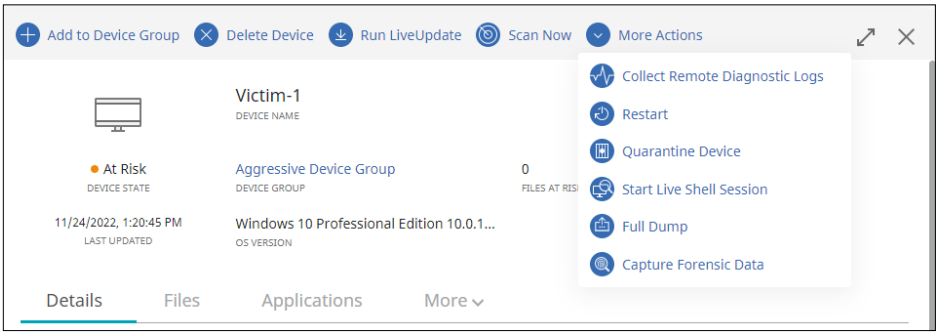
If multiple Endpoint Activity Recorder searches are planned, Endpoint data can be uploaded to the cloud first to make searching faster. You can choose to upload all the data, all the data for a specified time period, or just the data for a single process.

In the screenshot below, a suspicious file masquerading as Google Chrome has been found. We can tell it's not the real Chrome because it's not signed, has been seen on very few endpoints and is brand new. Select More Actions, then Process Dump to get a dump of all the endpoint activity recorder events related to the activities it performed.

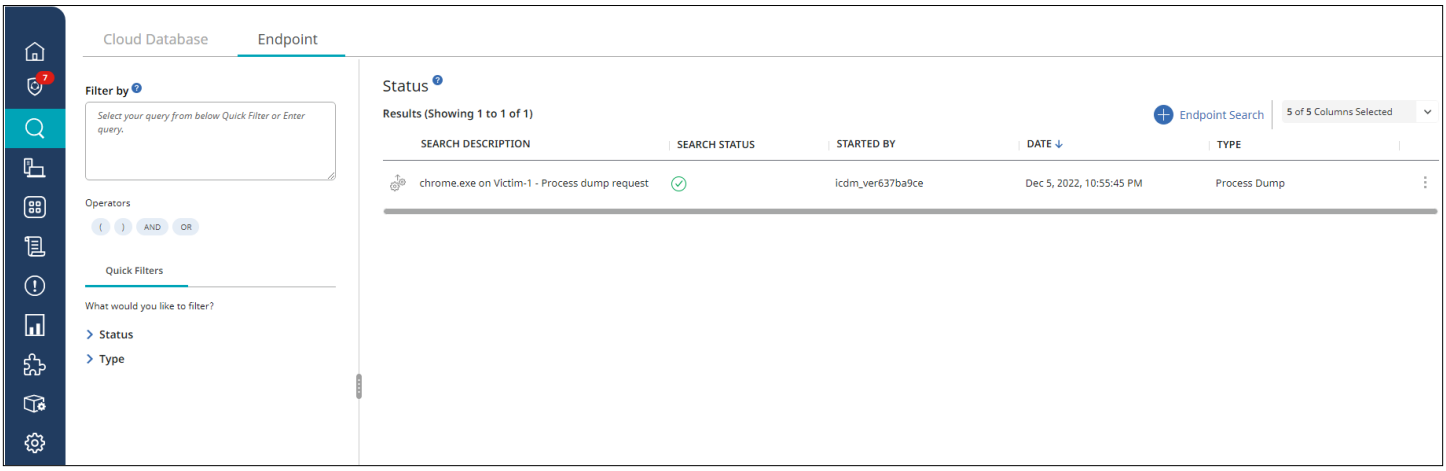


FORENSIC DATA GATHERS INFORMATION ABOUT THE CURRENT STATE OF THE ENDPOINT INCLUDING RUNNING PROCESSES, SERVICES, OPEN NETWORK CONNECTIONS/NETWORK LISTENS, PRIVILEGE ESCALATION, USER/ GROUP INFORMATION, AND MUCH MORE.

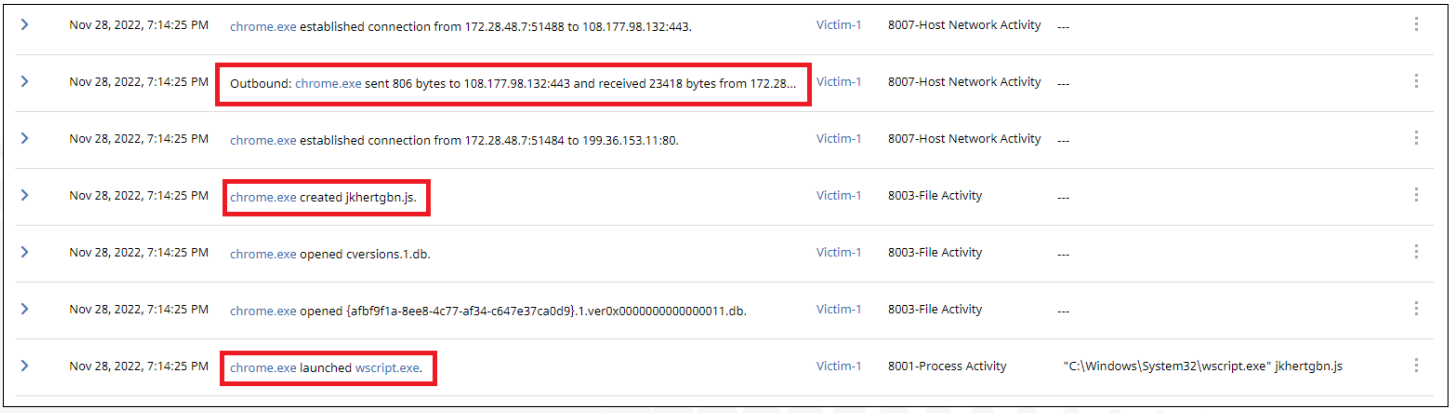
To upload all the endpoint activity recorder data from an endpoint, select the endpoint, press More Actions then Full Dump.



Whether a Full Dump or a Process Dump was performed, the results can be found by going to the Investigate tab and selecting Endpoint.



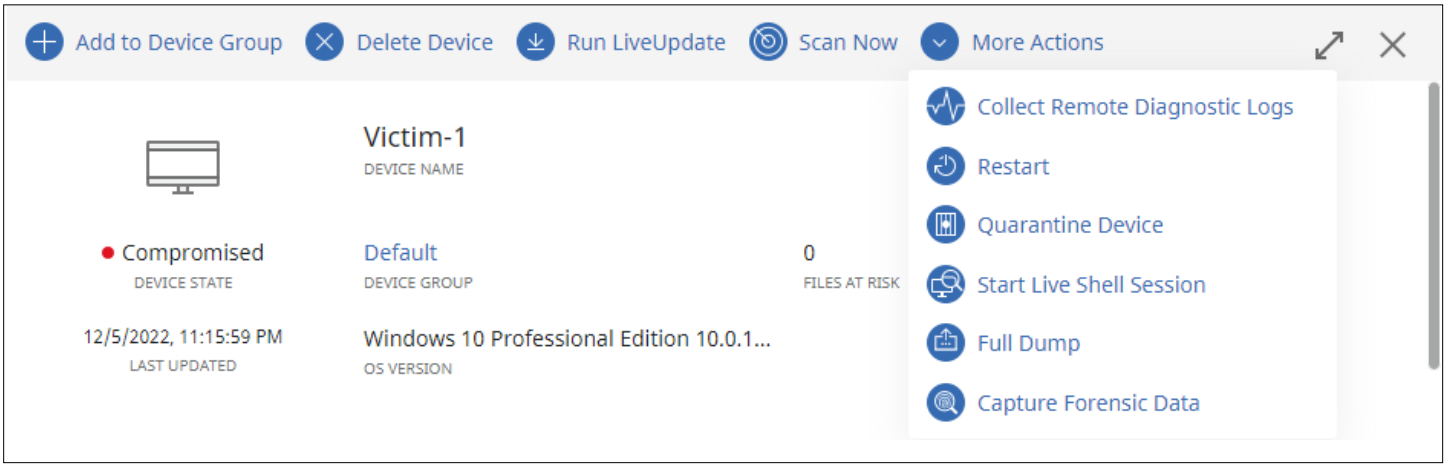
Selecting the dump gives a very detailed list of activities the endpoint or process performed. Here, the process dump shows the suspicious version of chrome.exe performing C&C traffic, creating malicious javascript, then running the malicious javascript.



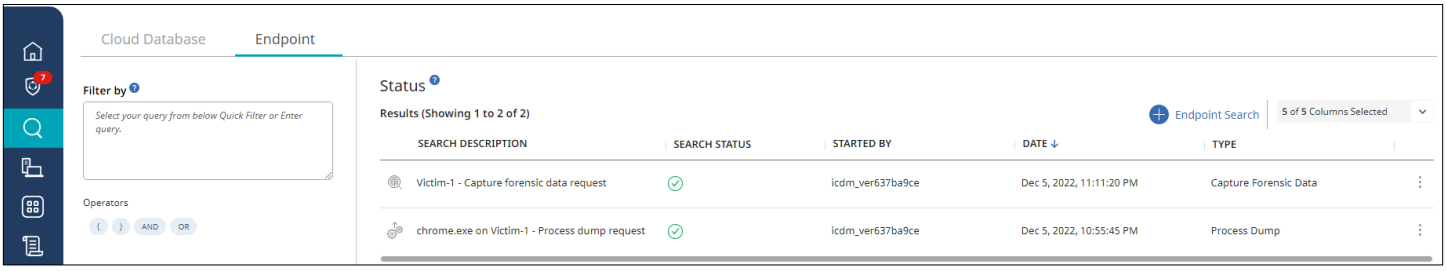
Forensic Data Requests

Forensic Data requests are a bit like Full Dumps and Process Dumps in that they reach out to the specified endpoints to gather data. Forensic data gathers information about the current state of the endpoint including running processes, services, open network connections/network listens, privilege escalation, user/group information, and much more. See https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Endpoint-Detection-and-Response/EDR-Actions/Collecting-forensic-data.html for more. And we're constantly adding new data such as browser history and downloaded files.

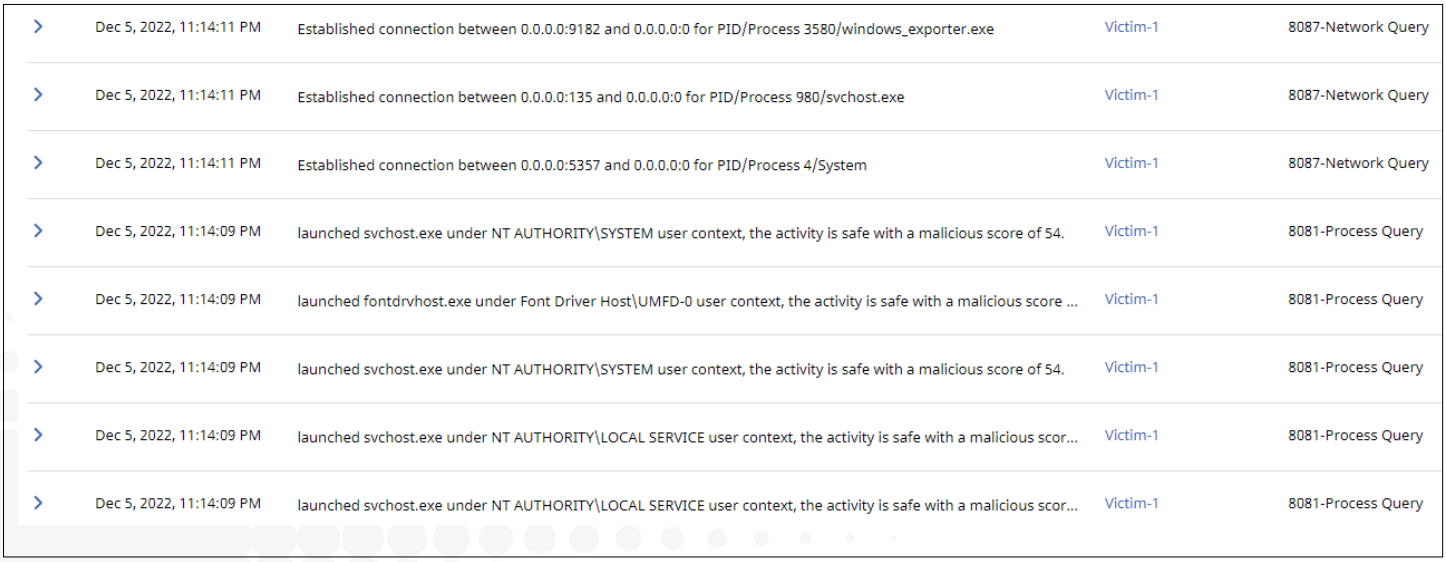
To initiate a Forensic Data request, select the endpoint, press More Actions, then Capture Forensic Data.



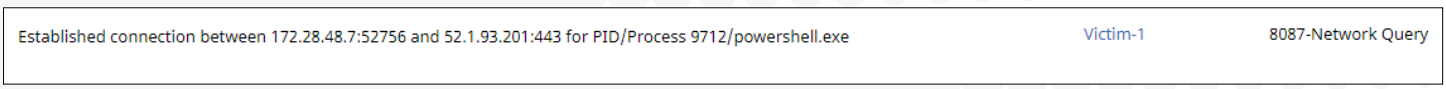
Just like viewing Full or Process Dumps, to view the Forensic Data, select Investigate, then Endpoint.



The forensic data show the current state of the endpoint.



This includes an open connection to the C&C server, indicating the threat is still present on the endpoint.

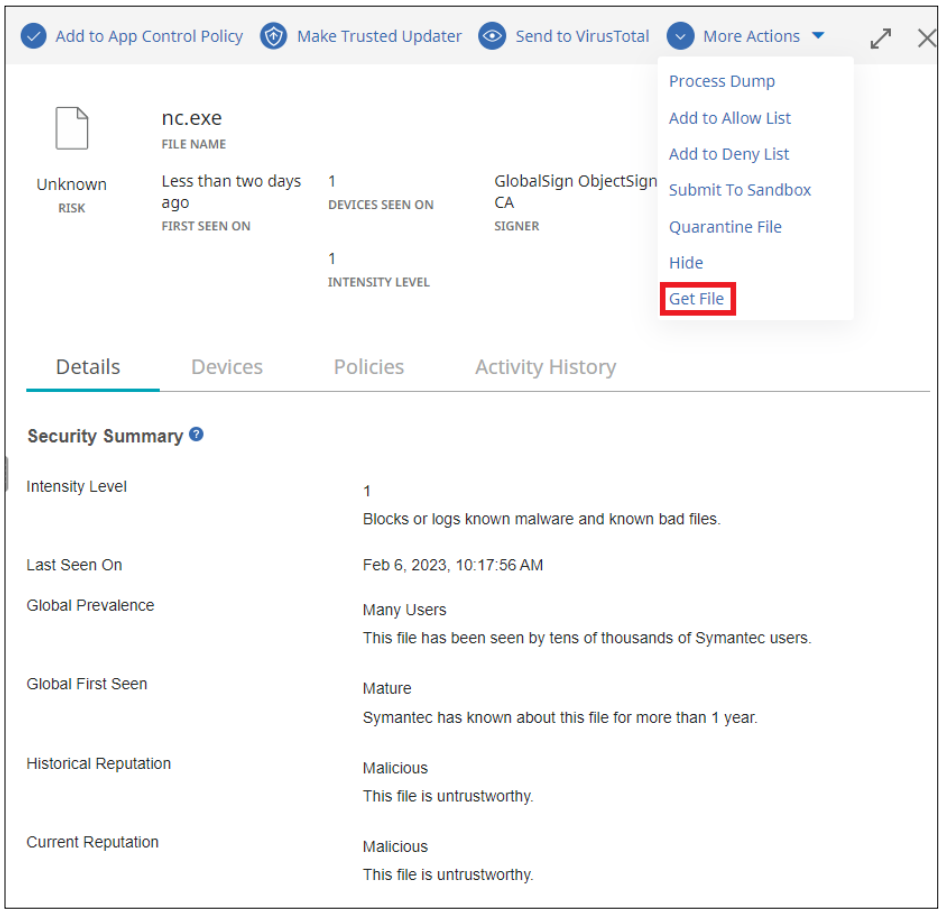


SES COMPLETE ALREADY PROVIDES METADATA ABOUT THE FILES ENCOUNTERED INCLUDING HASHES, FILE SIZE, LOCATION, ETC.

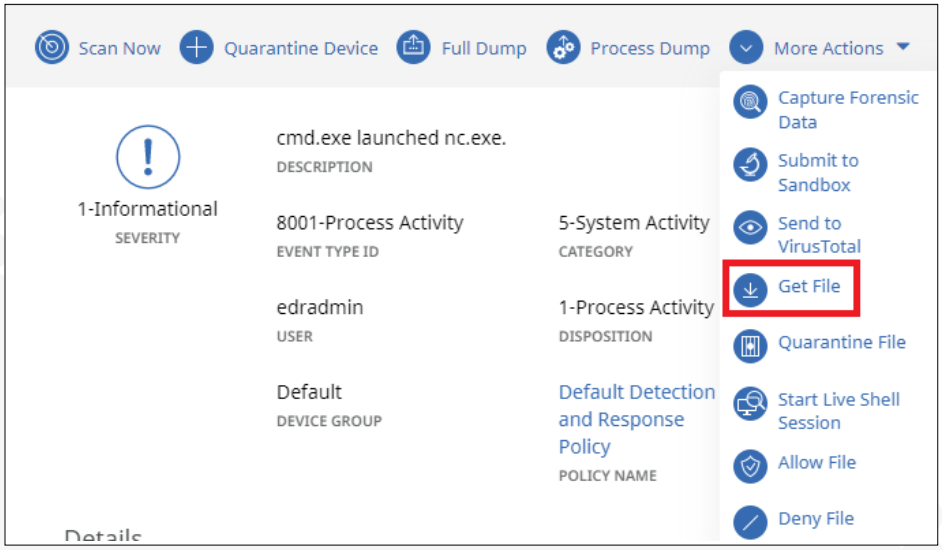
Gather Files From Endpoints

SES Complete already provides metadata about the files encountered including hashes, file size, location, etc. To help in an analysis, a copy of the file can also be retrieved by any of the following methods.

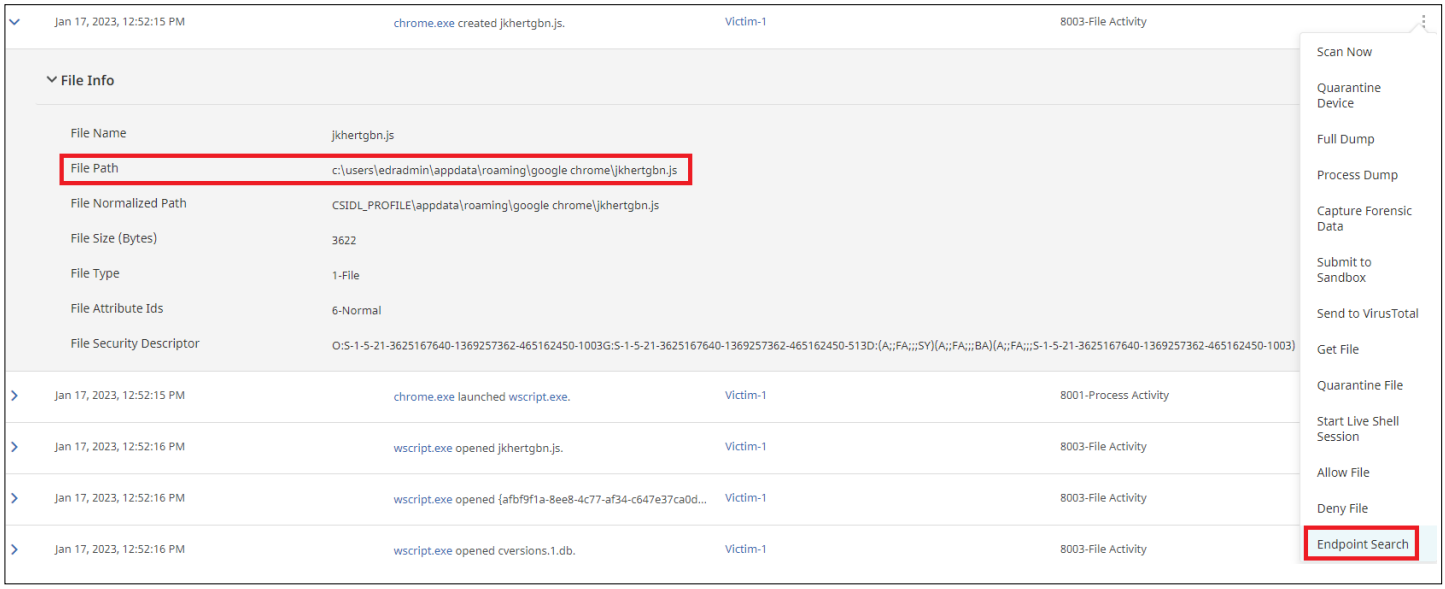
1. Go to Devices, select the endpoint where the file is located, select the Files tab, select the file, and press Get File.



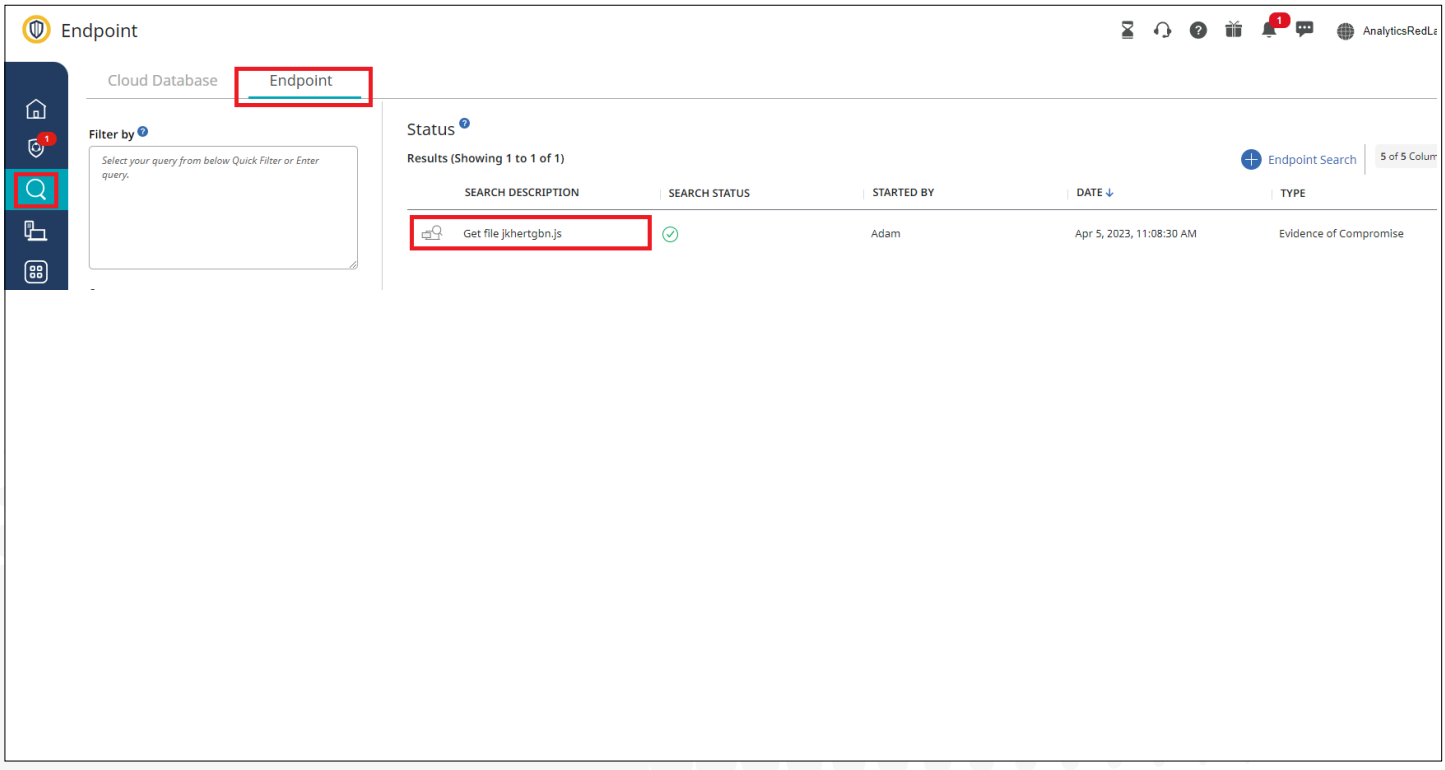
2. Go to an event the file is a part of and select Get File.



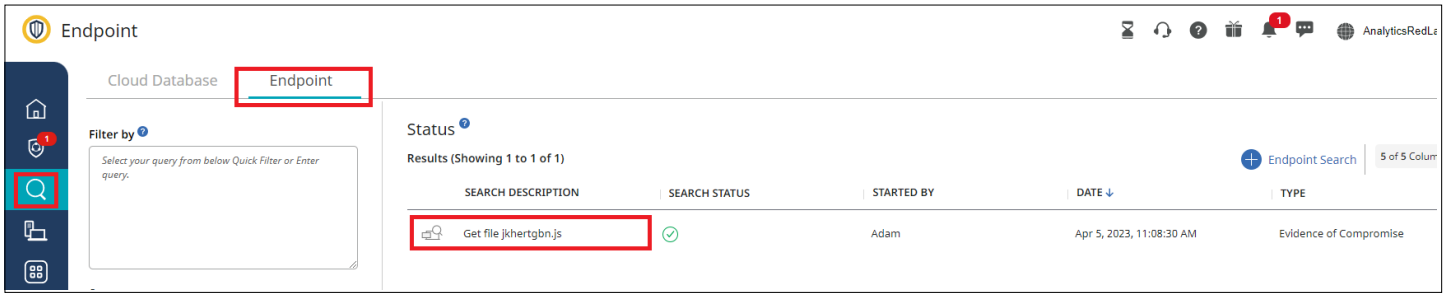
3. For non-executable files, navigate to an event involving the file, copy the File Path to the clipboard, then select the three vertical dots to the right and select Endpoint Search.



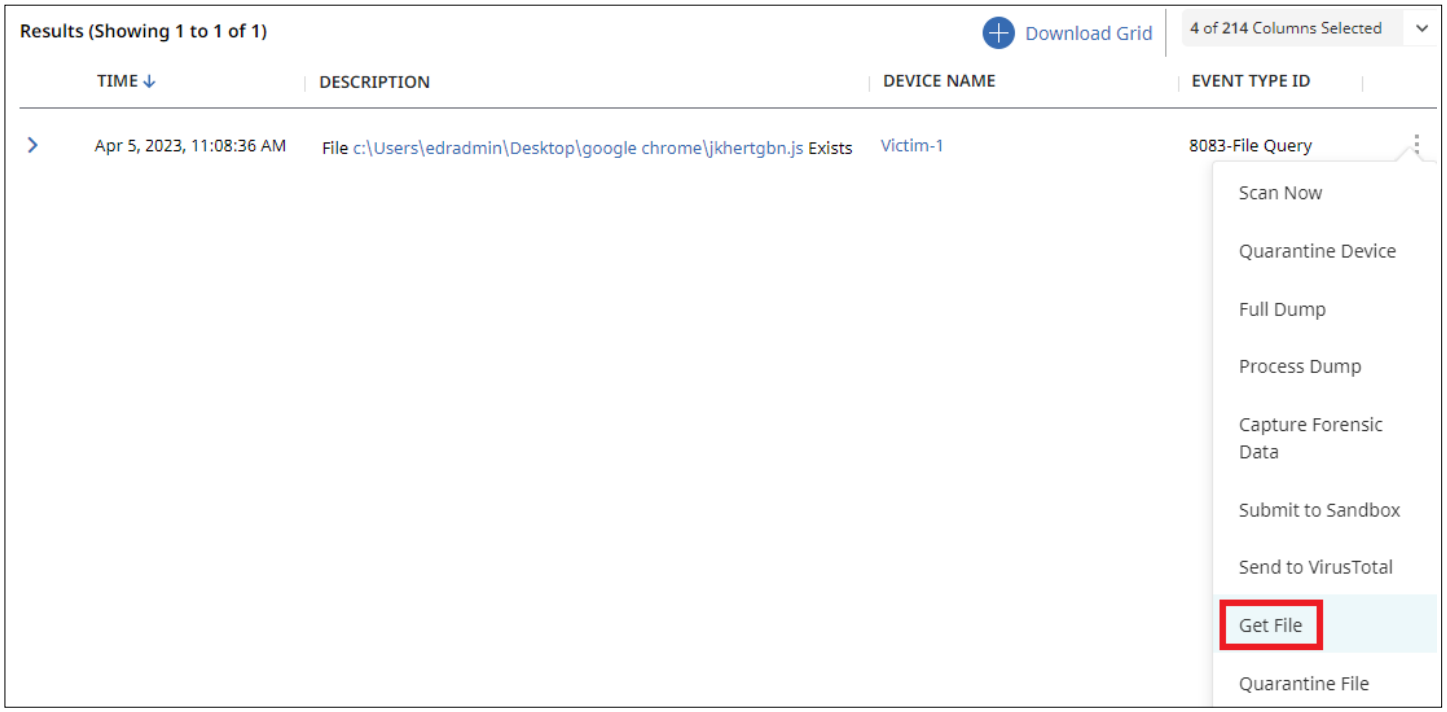
Select Evidence of Compromise, enter a Search Description, in "Filter by" enter "FilePath:" and paste the full path to the target file, then select the Search button at the bottom right.



The results of the Evidence of Compromise search is available by selecting Investigate and Endpoint, then selecting the search result.

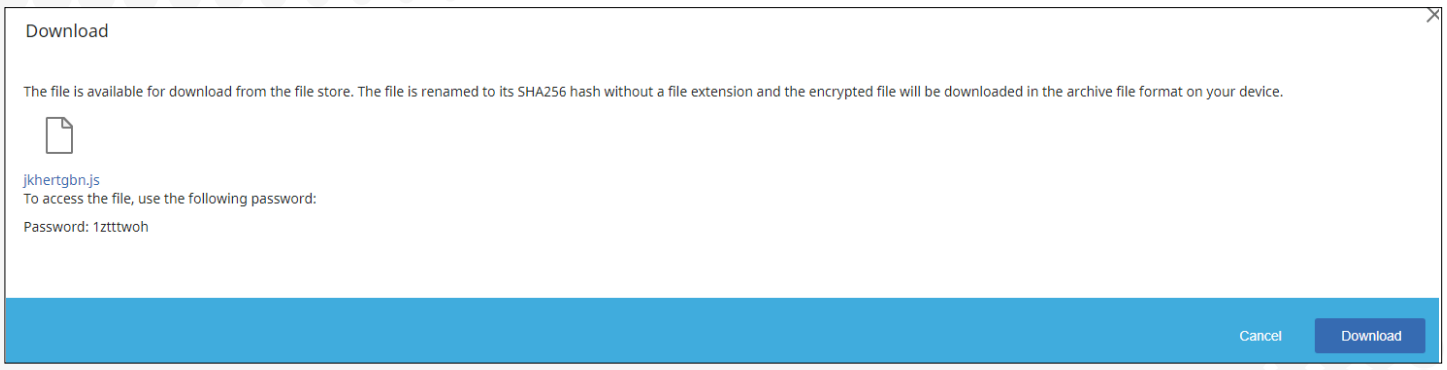


From the search result, select Get File.



Any file can be chosen, including documents with sensitive data. To keep such data secure, you may be prompted for credentials (local account or domain admin account) to the target machine.

Because the file is potentially malicious, the file is downloaded as a password protected archive so it won't trigger your security software. The file inside is renamed to the hash of the file without any extension to prevent accidentally running the file.



Investigate an Entire Process Tree

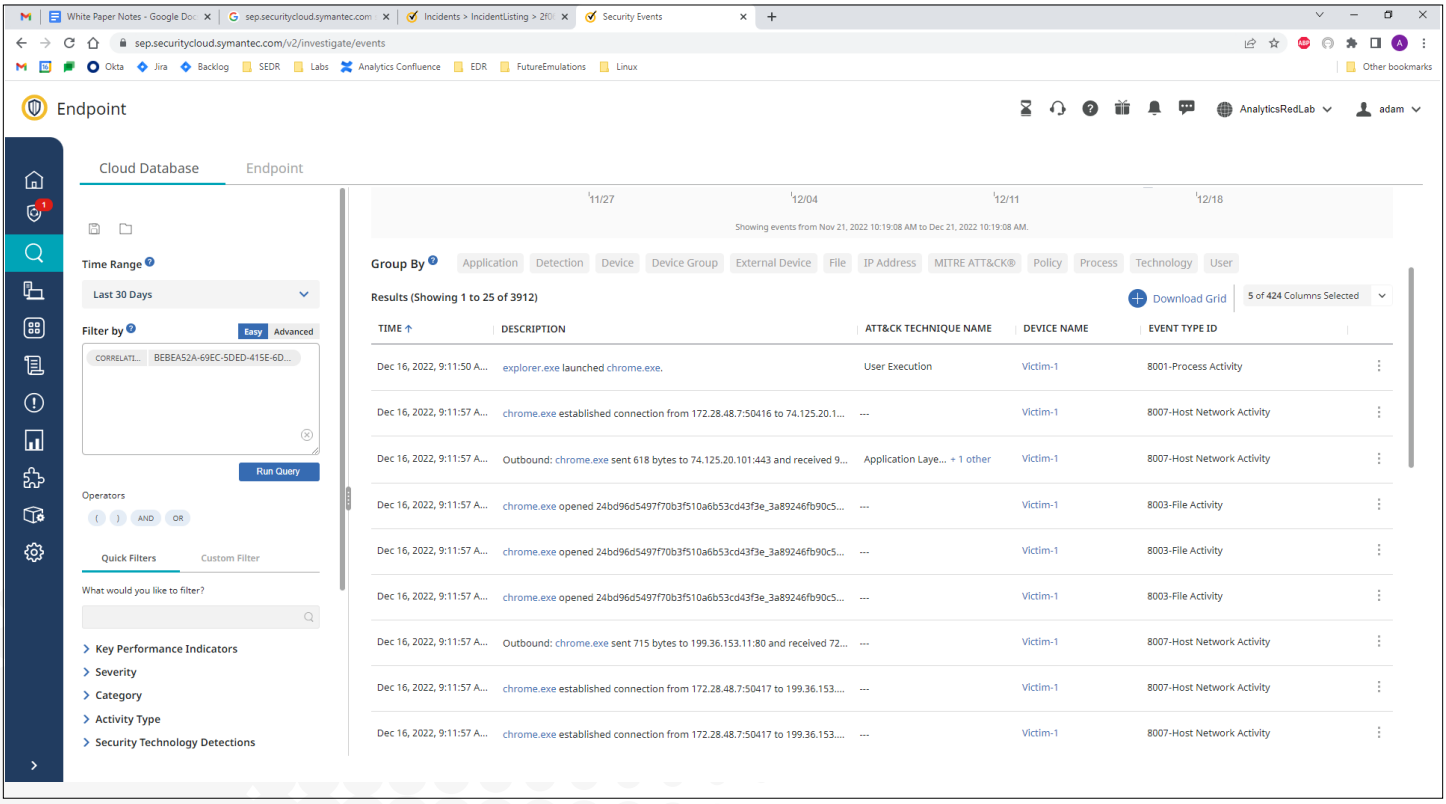
Imagine you find a suspicious or even just an interesting activity and you want to investigate further. SES Complete makes it very easy to show all activities performed by the process, its ancestors and its descendants. For example, you see PowerShell performing unusual network activity to a suspicious host.

	TIME ↓	DESCRIPTION	DEVICE NAME	EVENT TYPE ID
›	Dec 16, 2022, 9:14:29 AM	Outbound: powershell.exe sent 298392 bytes to 52.55.161.82:443 and received 1054677 bytes from 172.28.48.7:50798 via HTTPS,TLS.	Victim-1	8007-Host Network Activity

Open up the event details by clicking on the arrow to the left of the event and scroll down to the Correlation ID field. This is a unique identifier for the entire process tree.

	TIME ↓	DESCRIPTION	DEVICE NAME	EVENT TYPE ID
⌄	Dec 16, 2022, 9:14:29 AM	Outbound: powershell.exe sent 298392 bytes to 52.55.161.82:443 and received 1054677 bytes from 172.28.48.7:50798 via HTTPS,TLS.	Victim-1	8007-Host Network Activity
	Correlation ID	BEBEA52A-69EC-5DED-415E-6DE364E5FCF4		

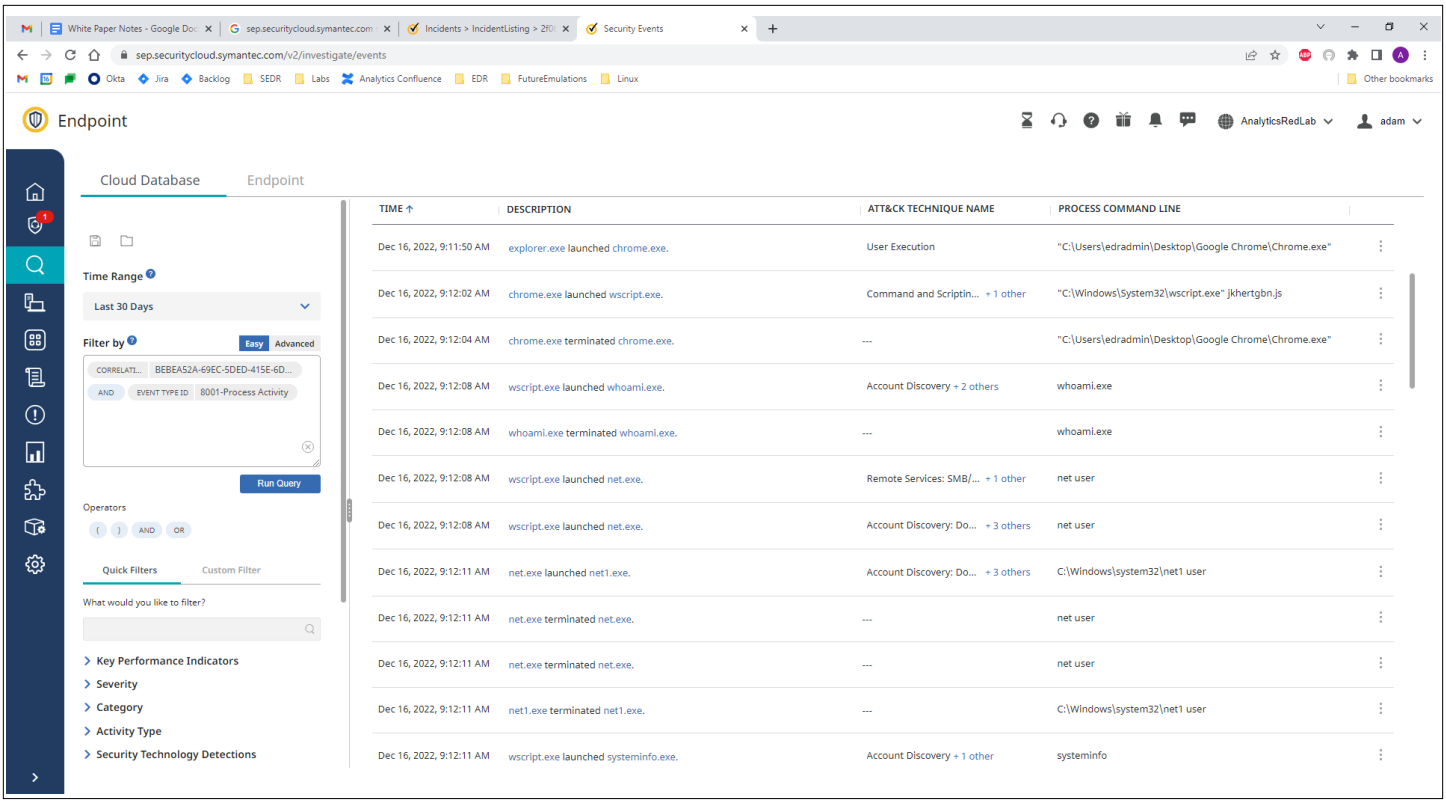
Copy the Correlation ID value by clicking on the Copy icon just to the right of the Correlation ID field. Then navigate to the Investigate tab. In the "Filter By" field enter "Correlation ID:" and paste the Correlation ID from the clipboard. You'll get a view of the entire process tree and every event performed by all processes in that process tree.



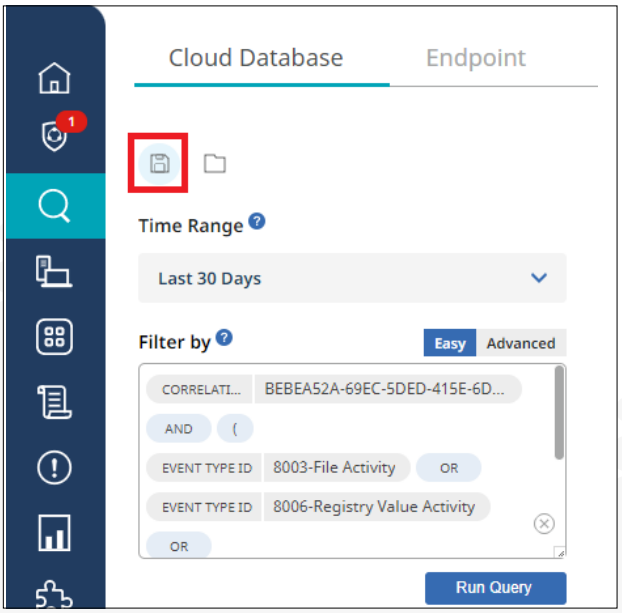
This provides a sequential list of activities starting from the earliest ancestor, explorer.exe launching the chrome browser in our case. One option is to browse through the data to look for interesting events, and we find some pretty quickly with chrome.exe creating and launching script on the local machine.

Dec 16, 2022, 9:12:00 AM	chrome.exe created jkhertgbn.js.	Ingress Tool Transfer	---
Dec 16, 2022, 9:12:02 AM	chrome.exe launched wscript.exe.	Command and Scriptin... + 1 other	"C:\Windows\System32\wscript.exe" jkhertgbn.js

One way to speed up the investigation is to further filter events, for example showing only the process events. Here we quickly see that the suspicious script is doing all sorts of Discovery ATT&CK techniques. Presumably the threat is getting the lay of the land to determine if this is a valuable victim machine.

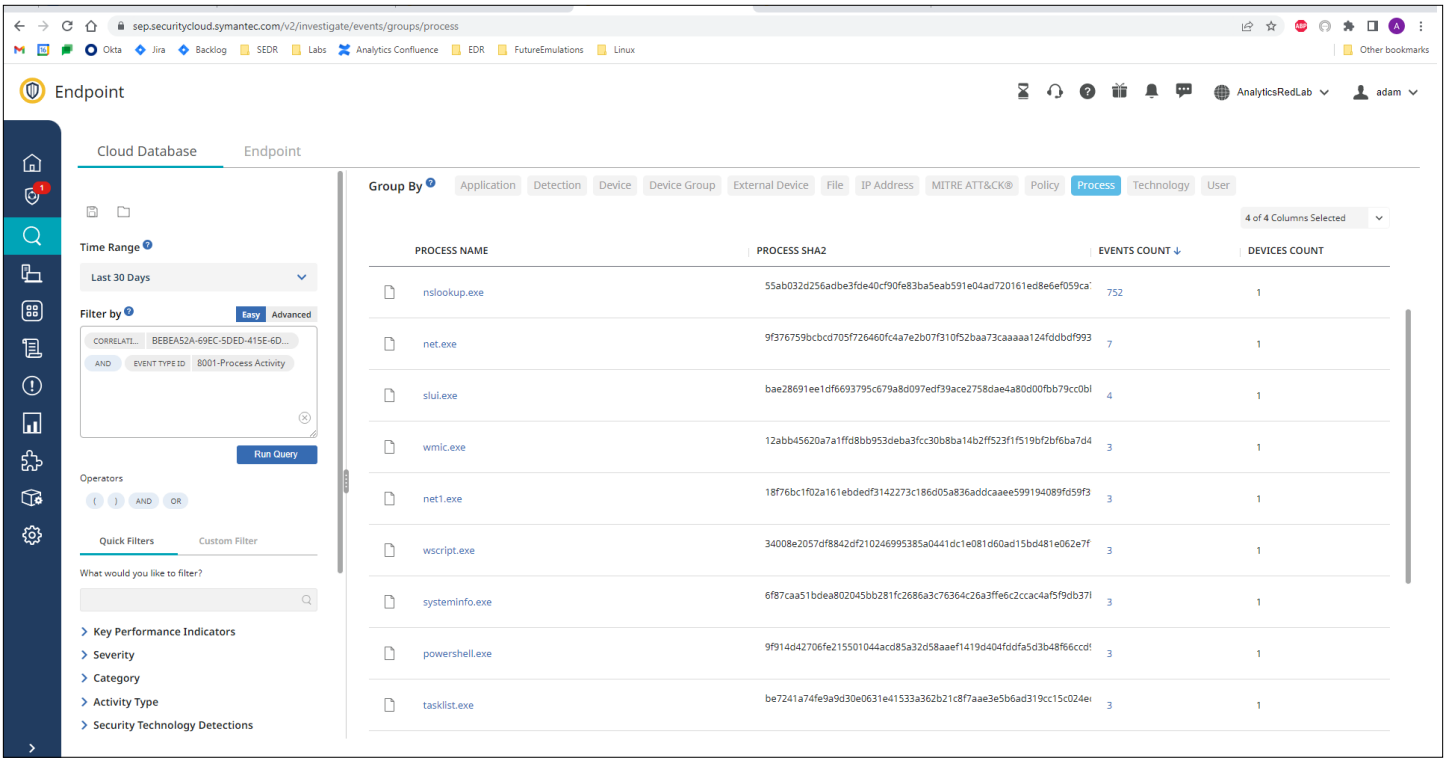


Once you've gotten some queries you might want to revisit or reuse in future investigations, you can save the query by clicking on the "Save search" icon. Here's a query showing all the file, Registry, and network activities performed by the process group.

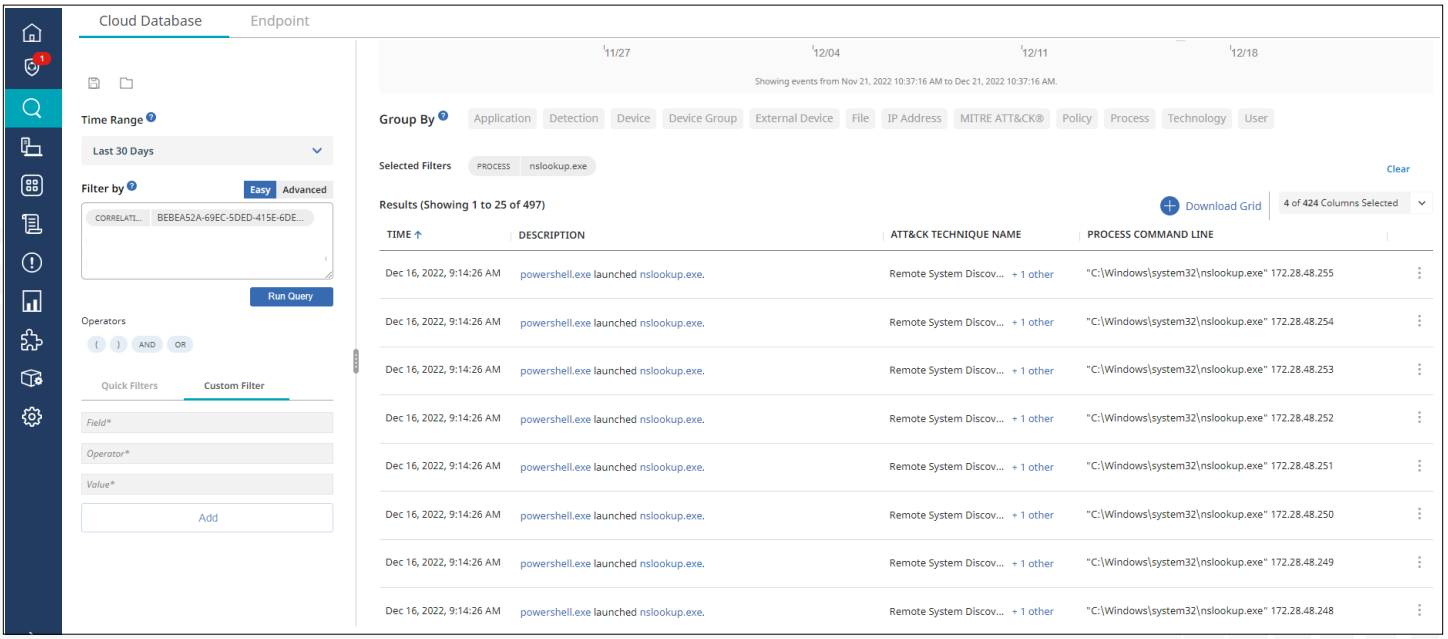


Click on the "Open search" icon right next to Save to find the query next time you want it.

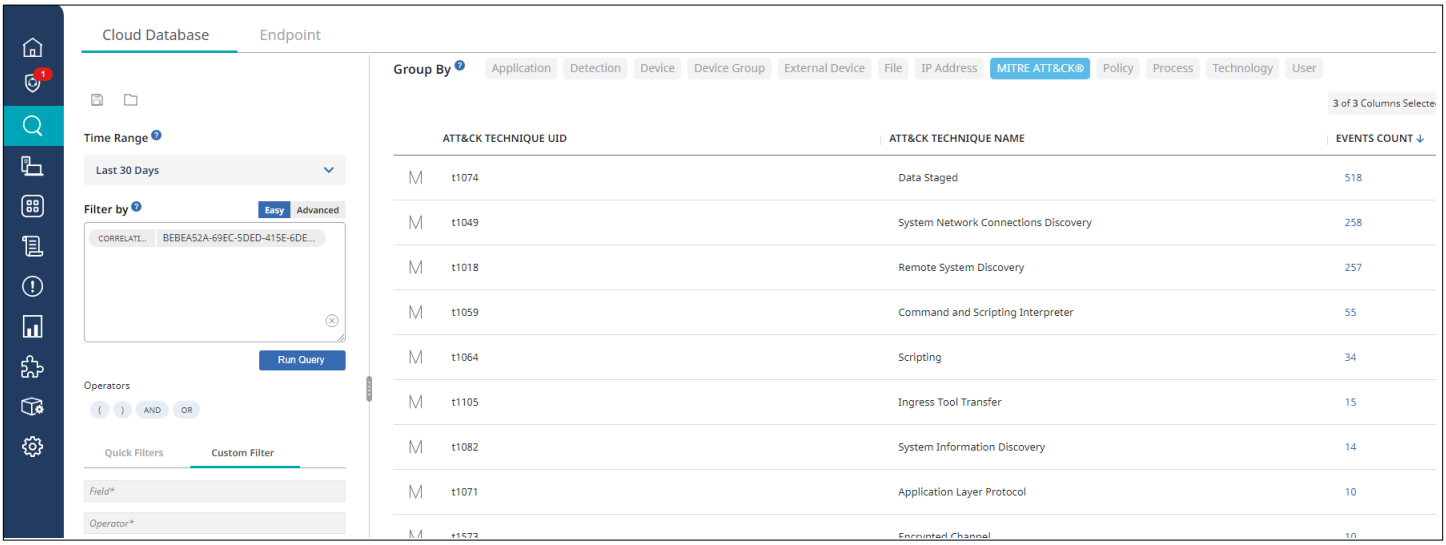
Another way to get an overview of what the entire process tree is doing is to use SES Complete's Group By logic. Grouping by Process is good to get an overview of what processes are involved.



Clicking on the Events Count shows all the activities by the process. This pretty quickly shows that the threat is using nslookup to perform Remote System Discovery of all machines on the local subnet. Notice the changing IP addresses in the nslookup command line in the far right column.



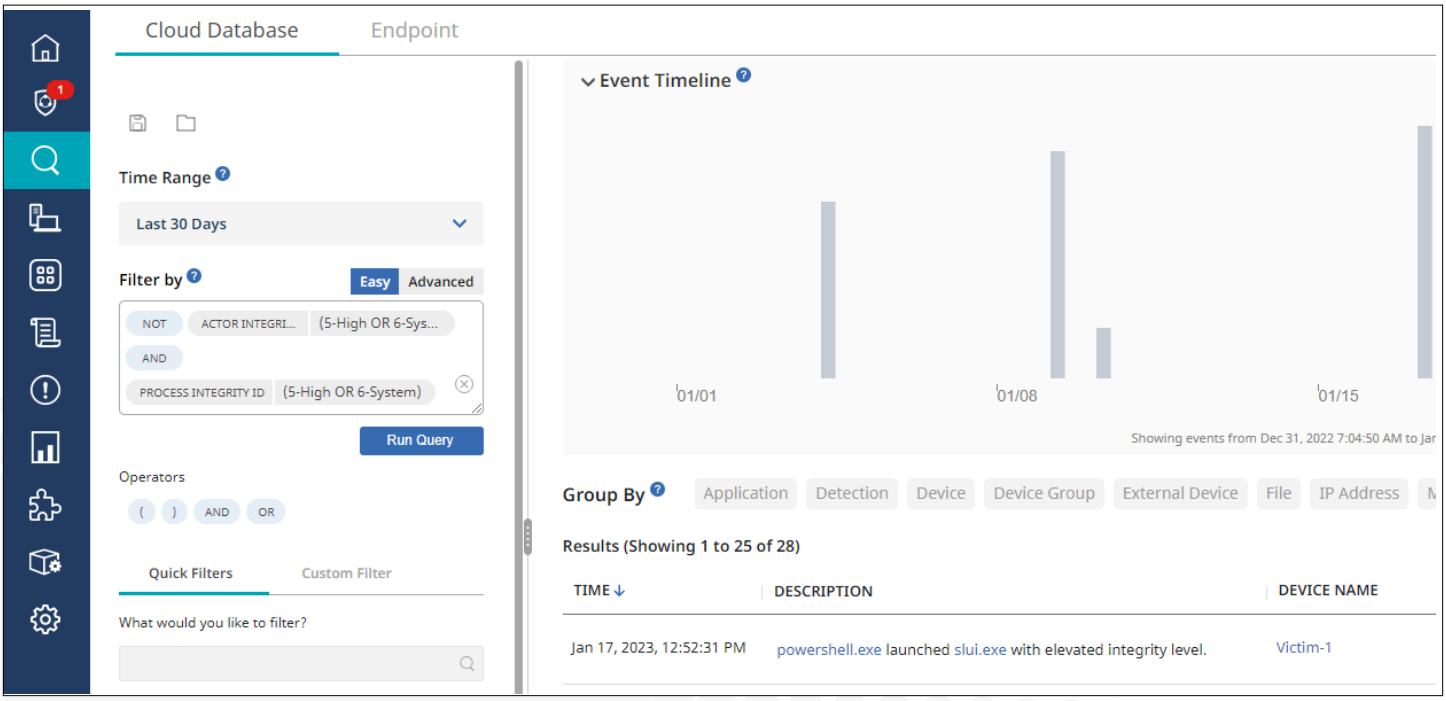
Perhaps even more useful is grouping by MITRE ATT&CK to get an overview of the techniques used by the entire process group. Clicking on any of the Events Count shows details of the activities.



Find Privilege Escalation

Often attackers will need to increase their privilege level to complete their objectives. SES Complete makes this very easy to find.

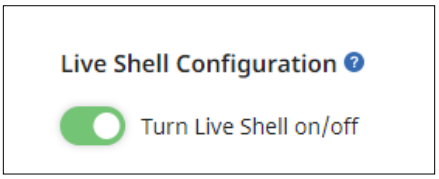
Go to the Investigate tab and Filter By "NOT Actor Integrity Id:(5-High OR 6-System) AND Process Integrity Id:(5-High OR 6-System)". You'll instantly get a list of all processes that were launched with a higher Integrity Level than their parent.



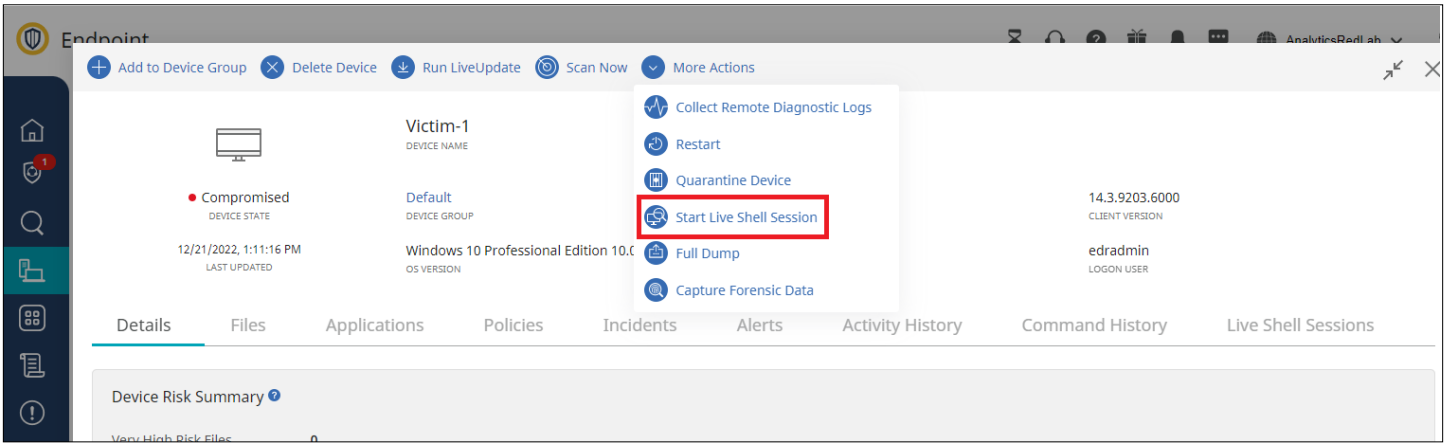
Custom Investigation Using Live Shell

Even with SES Complete's robust capabilities, you sometimes may want to use your own tools. SES Complete makes this incredibly easy.

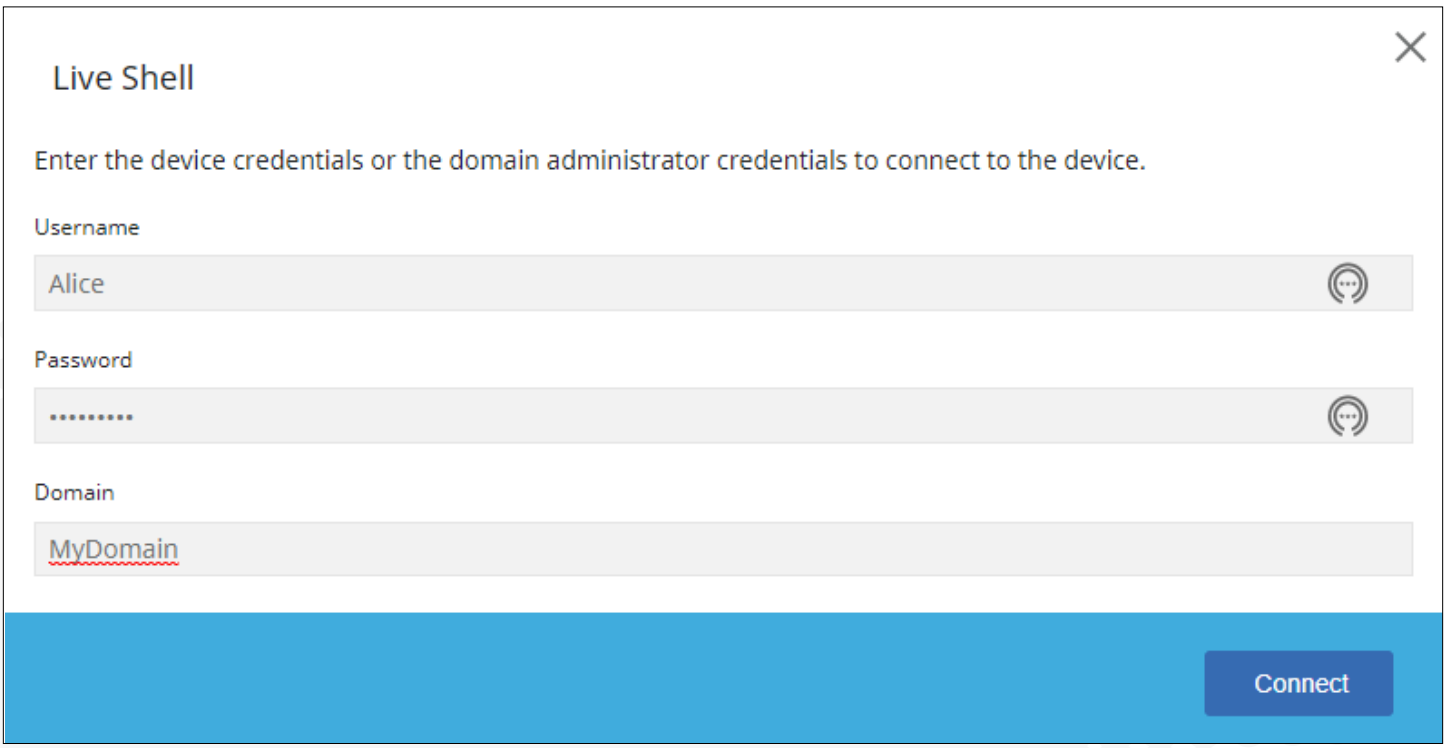
First, make sure you enable LiveShell in the Detection and Response policy.



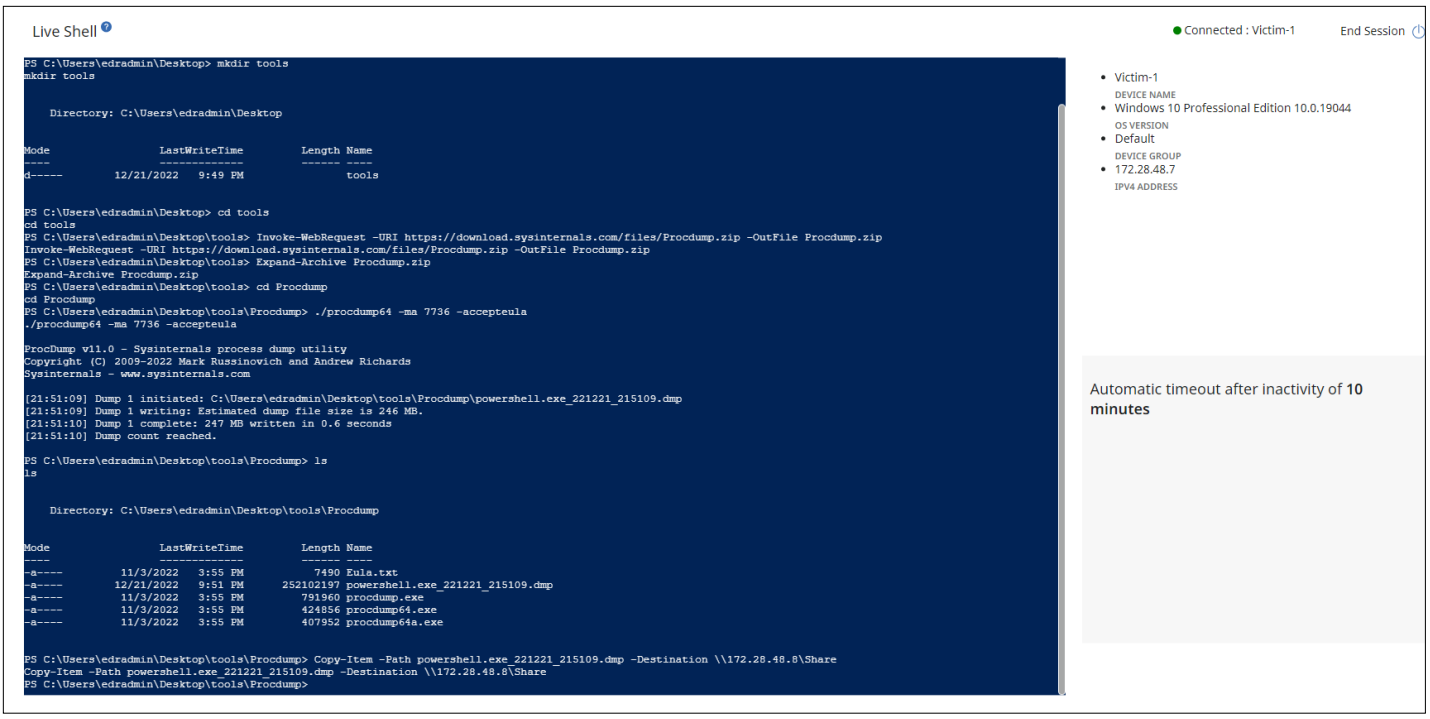
Then, it's as easy as navigating to the endpoint and selecting More Actions, then Start Live Shell Session.



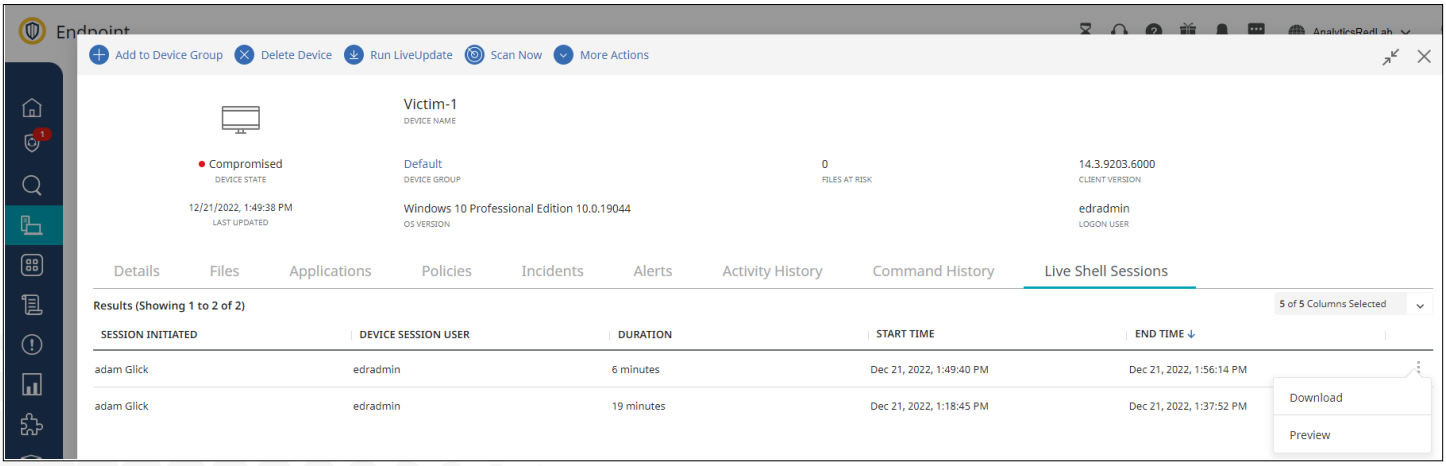
For security purposes, you'll be prompted for credentials to access the device.



You'll then get access to a PowerShell session on the endpoint. If the provided credentials have administrative privileges, so will your session. The session can then be used to download tools you prefer and run commands to help investigate or remediate the machine. Here, ProcDump is downloaded and run to get a dump of a running process. It then copies the dump to a file store for analysis.



Logs of previous sessions are kept at Devices, device name, Live Shell Sessions for future review or download.



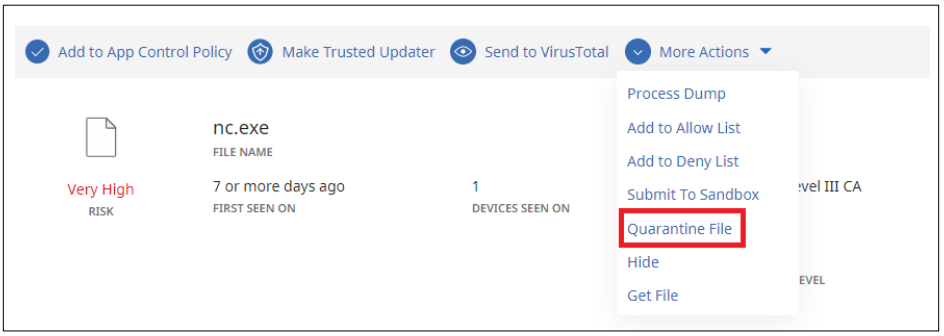
SES COMPLETE OFFERS FAST, EASY-TO-USE RESPONSE FEATURES TO HELP CONTAIN AND REMOVE THREATS.

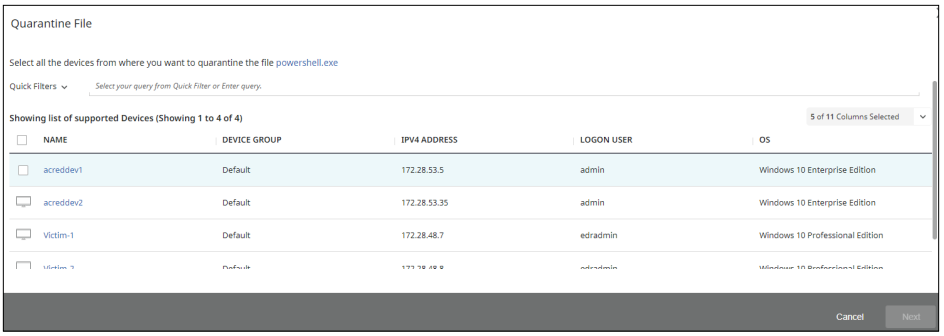
SES Complete Speeds Response Efforts

SES Complete offers fast, easy-to-use response features to help contain and remove threats.

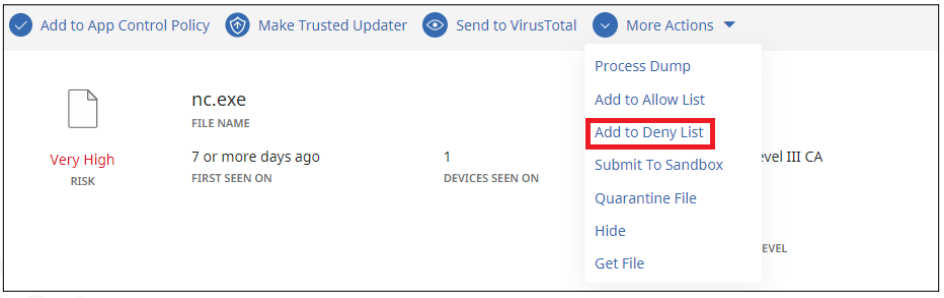
Quarantining and Blocking Files

Choose a file either from any event or from the Discovered Items list, select More Actions, then Quarantine File to move the file on a selected list of endpoints to quarantine.

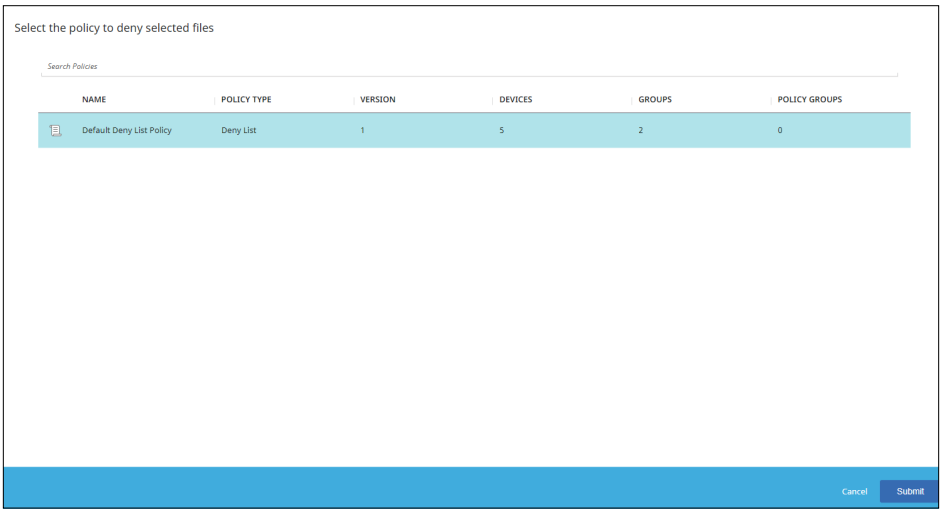




Alternately choose Deny File to remove existing instances of a file and prevent future creation of the file and processes based on the file across all endpoints. SES Complete prompts for a Deny List Policy so you can choose which endpoints this Deny File request applied to.

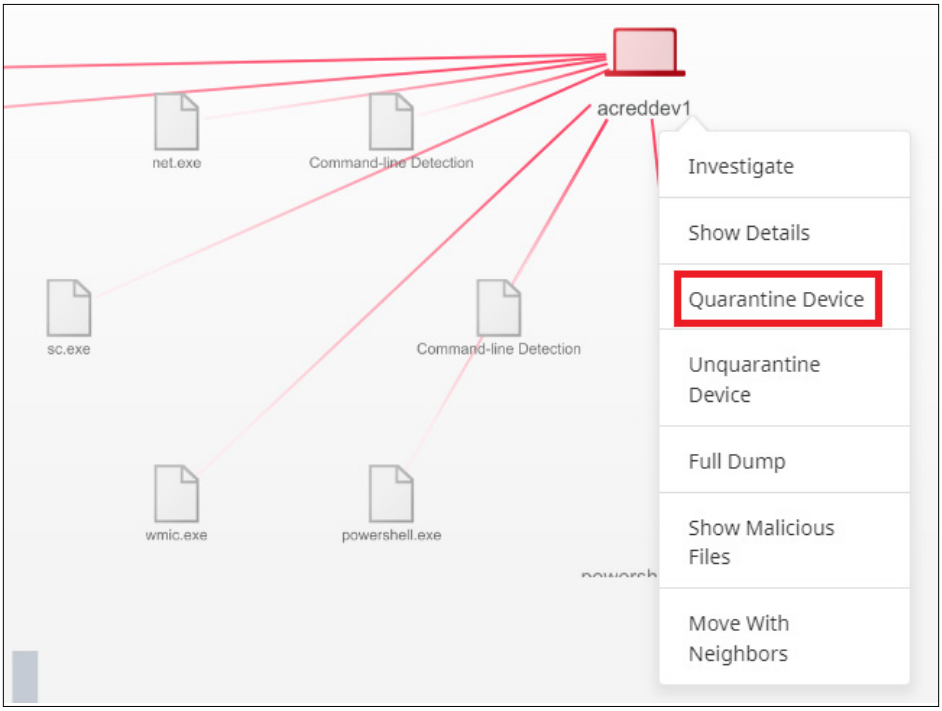


BEING ABLE TO COMMUNICATE WITH SES COMPLETE ALLOWS YOU TO CONTINUE TO PERFORM REMEDIATION ACTIONS FROM THE CONSOLE, PROVIDE SECURITY UPDATES, PERFORM ADDITIONAL REMEDIATION, AND MORE.



Quarantining Devices

If a device is compromised, you can isolate it from other devices to prevent the infection from spreading and to stop C&C traffic, including data exfiltration, from the compromised device. Choose the device from anywhere in SES Complete, such as an incident visualization, an event, or the device details page. Then select "Quarantine Device".



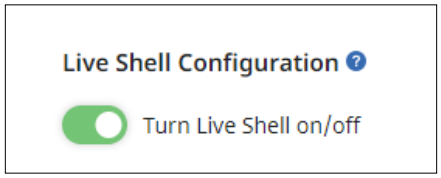
While quarantined, the device will not be able to communicate on the network except with SES Complete and, optionally, with any hosts you choose to provide access to (for example a file share with security tools). Being able to communicate with SES Complete allows you to continue to perform remediation actions from SES Complete, provide security updates, perform additional remediation, etc.

LIVE SHELL ALSO CAN BE USED TO PERFORM CUSTOM REMEDIATION STEPS.

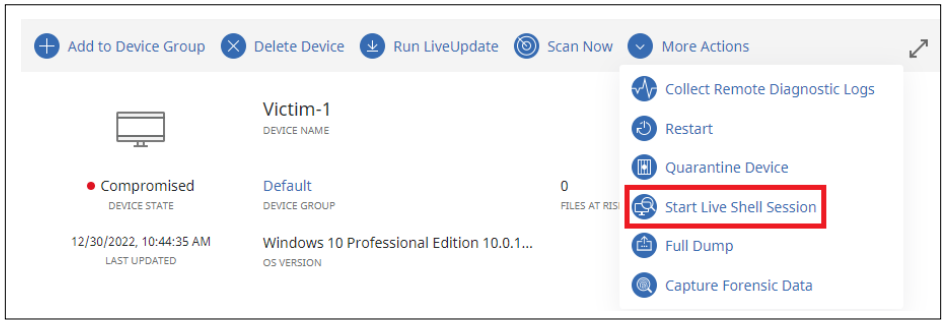
Custom Remediation with Live Shell

We saw earlier how SESC's Live Shell allows you to do custom investigation on endpoints. Live Shell also can be used to perform custom remediation steps. Here, we show how to determine what processes are currently running on an endpoint, and to forcibly terminate malicious processes.

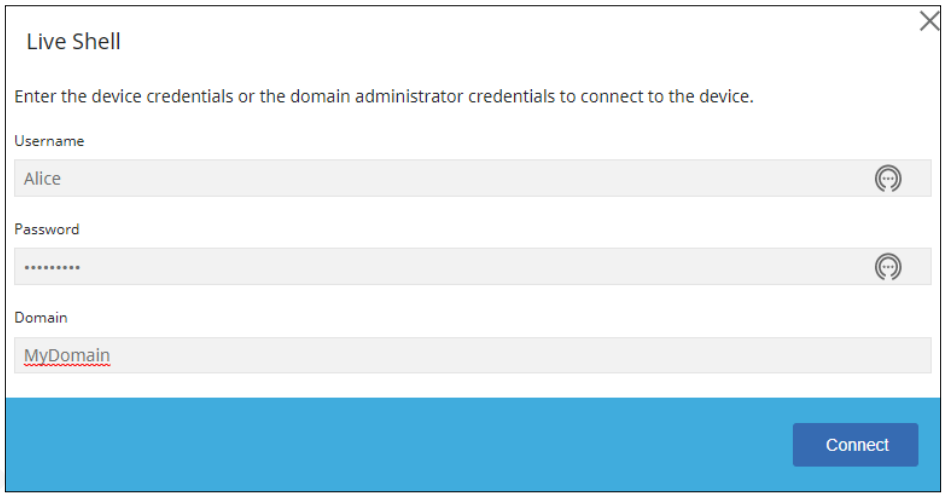
First, make sure you enable LiveShell in the Detection and Response policy.



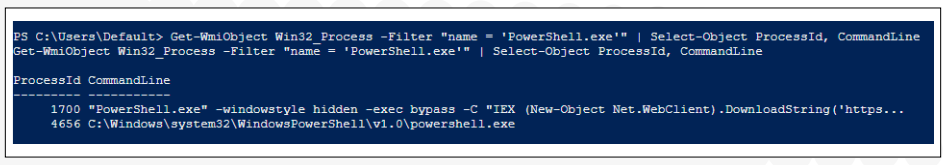
Connect to the endpoint by selecting the endpoint, More Actions, and Start Live Shell Session.



You'll be prompted for credentials to access the device.



To find all running PowerShell, we use the built-in command Get-WMIObject. Of course, you could instead use any other native PowerShell commands or download whatever tools you prefer.



BACKING SES COMPLETE IS A TOP NOTCH TEAM EVALUATING THE LATEST MALWARE. SYMANTEC EXPERT ENGINEERS ARE CONSTANTLY UPDATING SES COMPLETE PROTECTION AND DETECTION FOR THE LATEST THREATS AND ACTIVITIES.

The malicious PowerShell command stands out from benign PowerShell processes that happen to be running (including our own Live Shell session). It's the one that downloads and runs script from the network, ProcessId 1700.

We then terminate the malicious script with the PowerShell Stop-Process command, and verify it has been successfully terminated by again looking at all running PowerShell.

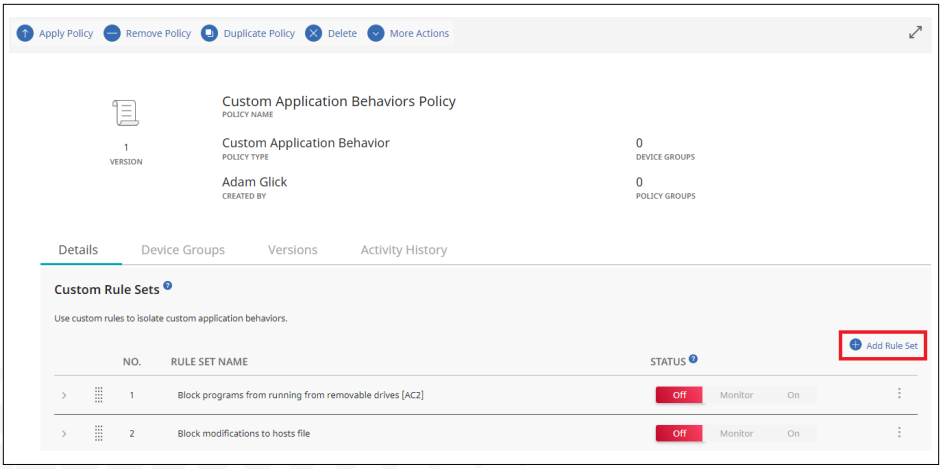
```
PS C:\Users\Default> Stop-Process -Id 1700
Stop-Process -Id 1700


PS C:\Users\Default> Get-WmiObject Win32_Process -Filter "name = 'PowerShell.exe'" | Select-Object ProcessId, CommandLine
Get-WmiObject Win32_Process -Filter "name = 'PowerShell.exe'" | Select-Object ProcessId, CommandLine

ProcessId CommandLine
--------- -----------
     4656 C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe


PS C:\Users\Default>
```

Write Your Own Custom Protection

Backing SES Complete is a top notch team evaluating the latest malware. Symantec expert engineers are constantly updating SES Complete protection and detection for the latest threats and activities. But no one knows your environment like you do, so SES Complete lets you write your own protection and detection and tailor it to your organization.

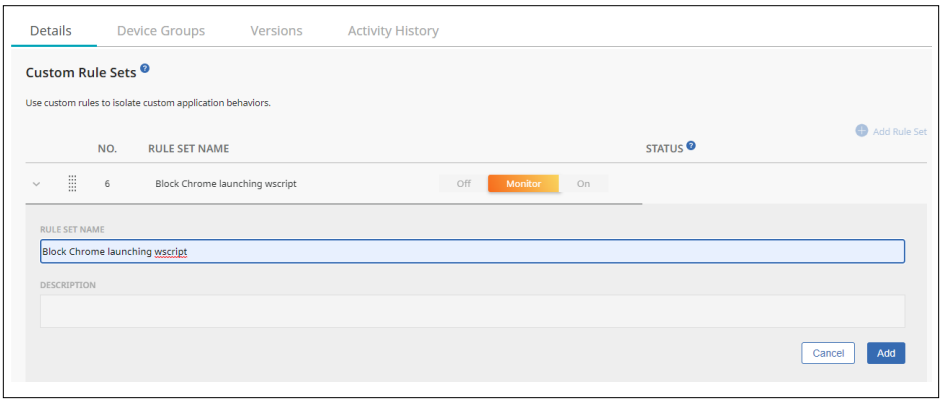
Let's say, for example, that we want to block the initial stage of the attack: Chrome launching wscript.exe to run malicious JavaScript. SES Complete allows us to do that with Custom Application Behaviors Policy. Custom Application Behaviors Policy is similar to Adaptive Protection described earlier, but allows us to write our own rules customized to our organization. It's a bit of work to set up, but is a tremendously powerful tool to lock down an environment.

Go to Policies, and select an existing (or create a new) Custom Application Behaviors Policy. Select Add Rule Set to add a new rule set.

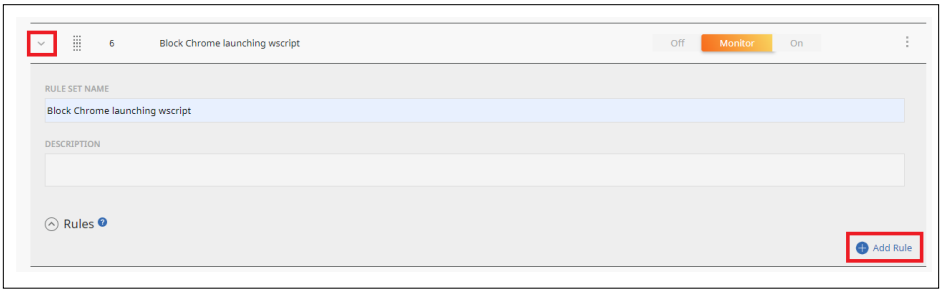


Type a name for the rule and press Add to add the new rule.

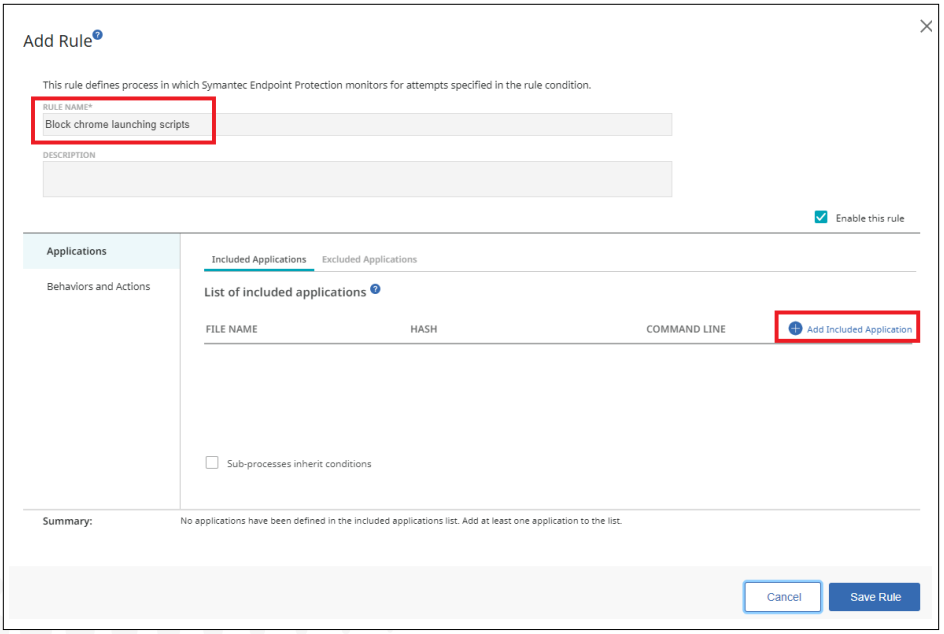
THIS IS WHERE THE PARENT APPLICATION, CHROME IN OUR CASE, IS SPECIFIED.



Click the down arrow next to the new rule and press the Add Rule button.

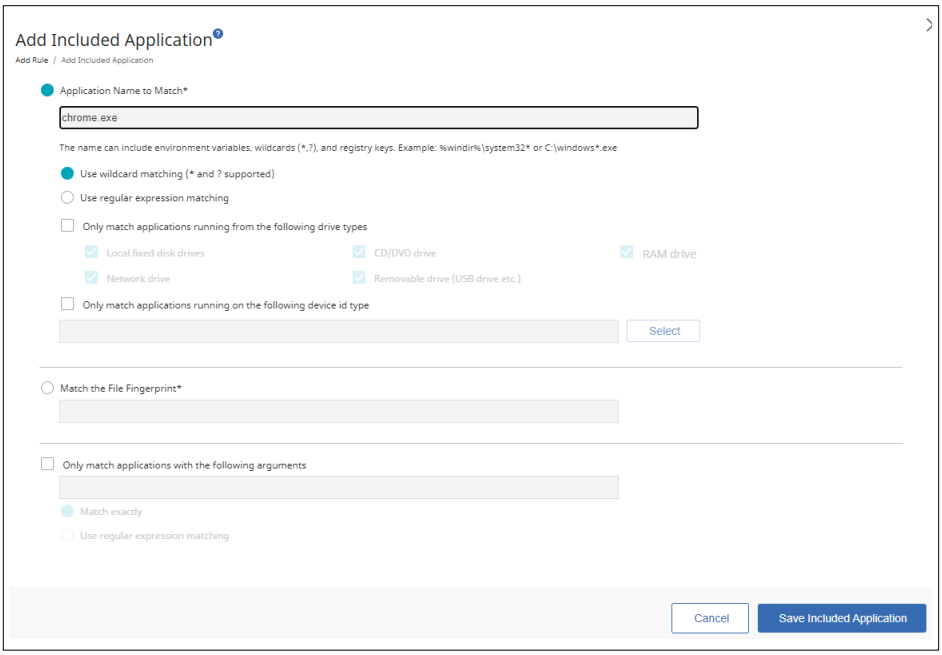


Type a name for the rule and press Add Included Application

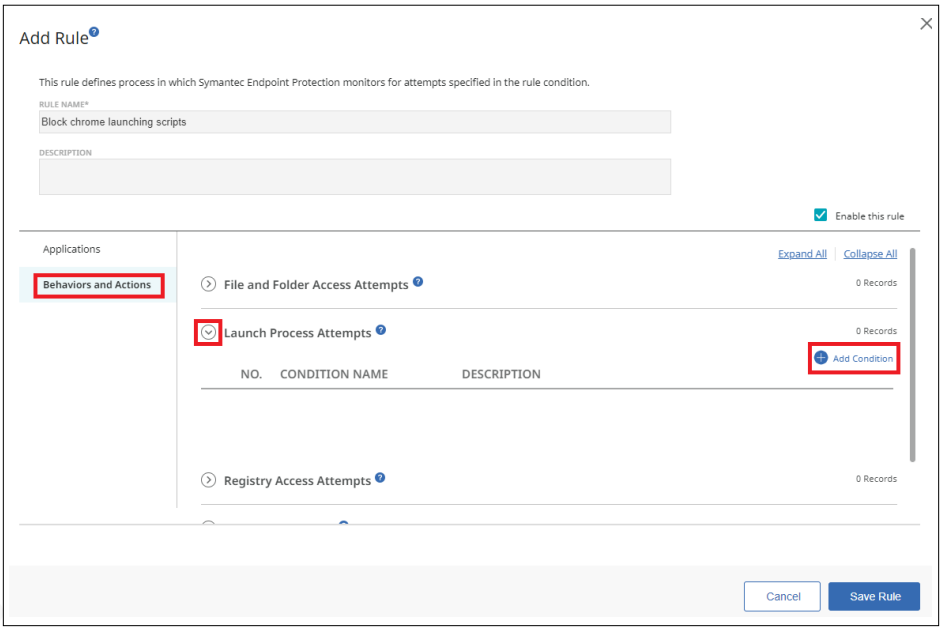


This is where the parent application, Chrome in our case, is specified. SES Complete provides all sorts of options for choosing which processes this rule applies to. For example, you could choose a full path, just an application name, filtering by drive types (such as network drives or removable media such as USB thumb drives), hash matches, or command line argument regular expressions. In our case, we choose any application named chrome.exe running from anywhere.

THE NEXT STEP IS TO SPECIFY WHAT WE WANT TO BLOCK CHROME FROM DOING.

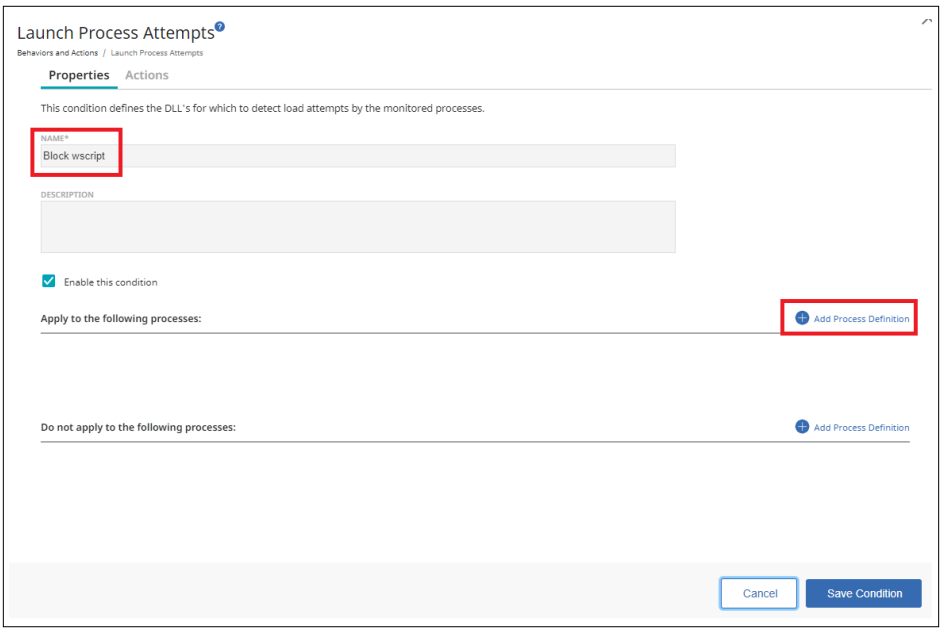


The next step is to specify what we want to block Chrome from doing. In our case, we want to block Chrome from launching a specific process. Select "Behaviors and Actions", the down arrow next to "Launch Process Attempts" and "Add Condition".

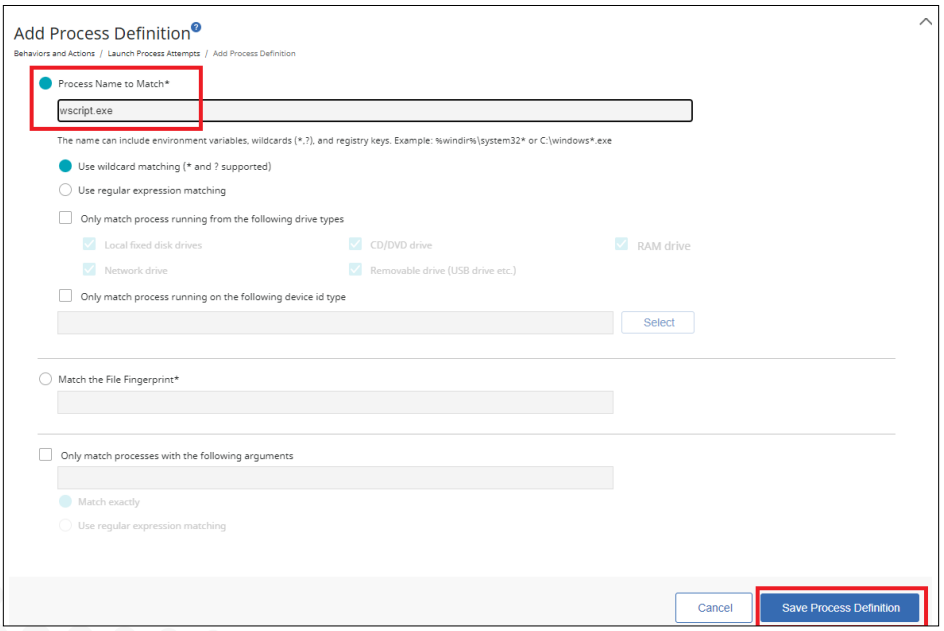


ONCE AGAIN, WE GET ALL SORTS OF OPTIONS TO GRANULARLY SPECIFY THE TARGET PROCESS.

Give the condition a name and press Add Process Definition.

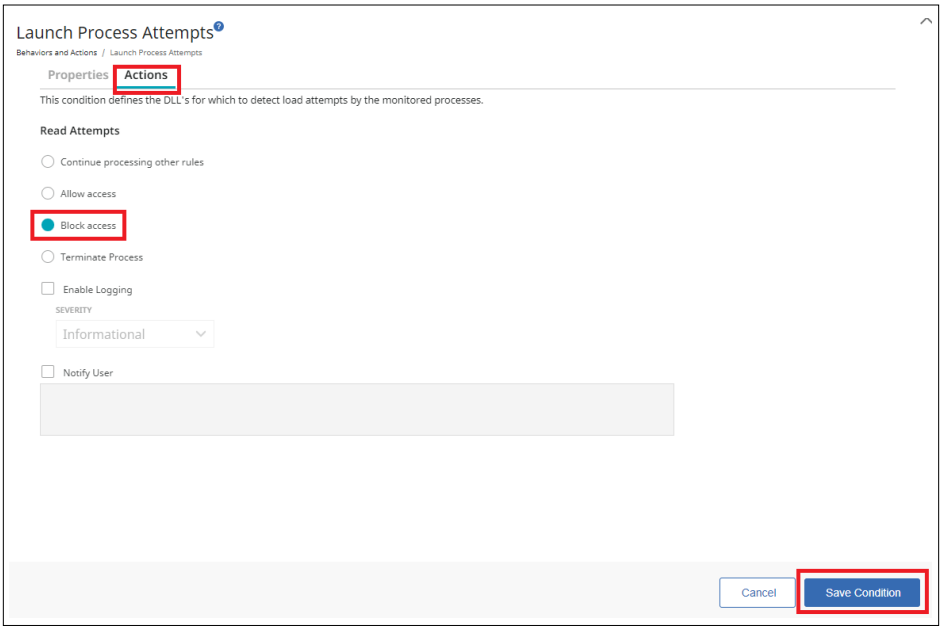


Once again, we get all sorts of options to granularly specify the target process. In our case, we'll block any process named wscript.exe. Enter a "Process Name to Match" and press "Save Process Definition".

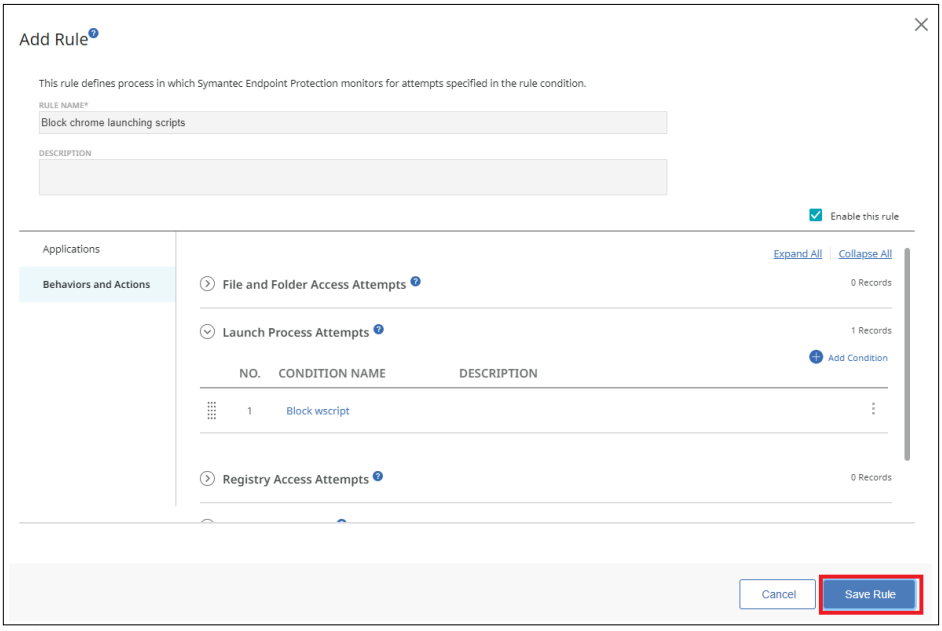


IT'S A GOOD IDEA TO RUN NEW RULES IN MONITOR MODE FOR A WHILE TO MAKE SURE THERE AREN'T LEGITIMATE USES HAPPENING IN YOUR ORGANIZATION.

Now we specify what we want to do when wscript.exe is launched by chrome.exe. Select the Actions tab, press "Block access" and "Save Condition".



Press "Save Rule".

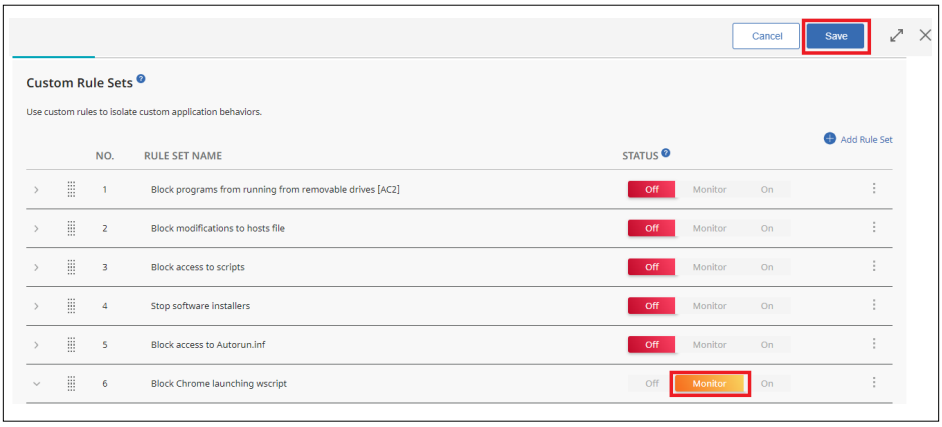


Choose what you want to do with the Rule Set. If you just want notifications when Chrome launches wscript, select Monitor. It's a good idea to run new rules in Monitor mode for a while to make sure there aren't legitimate uses happening in your organization.

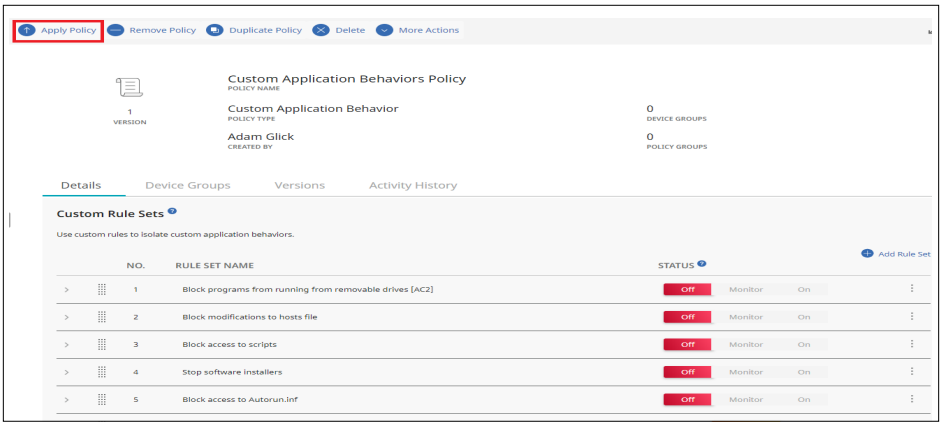
When you're ready to set the rule to blocking, select On.

SES COMPLETE WOULD HAVE BLOCKED THE ATTACK MANY TIMES OVER BEFORE IT EVEN GOT STARTED.

Select Save near the top of the screen to save the policy.



And finally, make sure to apply the policy to one or more groups of endpoints. Select Apply Policy near the top of the page and select which Device Groups to apply the policy to.



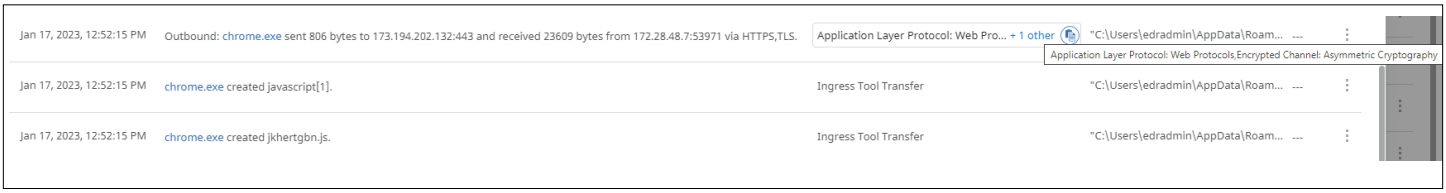
Attack Investigation Summary

Way back in the section The Attack, we described a real world attack involving Execution using heavily obfuscated JavaScript, various Discovery techniques to determine if the victim is a suitable target, encrypted Command and Control traffic, Ingress Tool Transfer to move tools to the victim machine, PowerShell based UAC Bypass privilege escalation, Credential Theft, Staged Data, Lateral Movement and Exfiltration of stolen data.

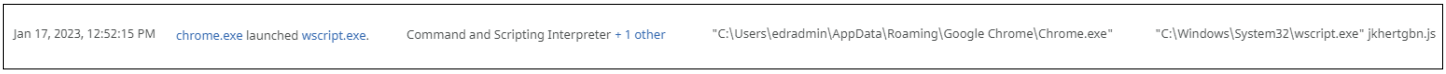
So how well did SES Complete do in showing these steps in a clear, easy to understand way?

As stated earlier, SES Complete would have blocked the attack many times over before it even got started. To test SES Complete's capabilities beyond these blocks, we put SES Complete in a special Monitor Only mode (which is not recommended for production environments) where the user is alerted to all activities but nothing is blocked. Given that blocking was turned off, let's see step-by-step what SESC shows.

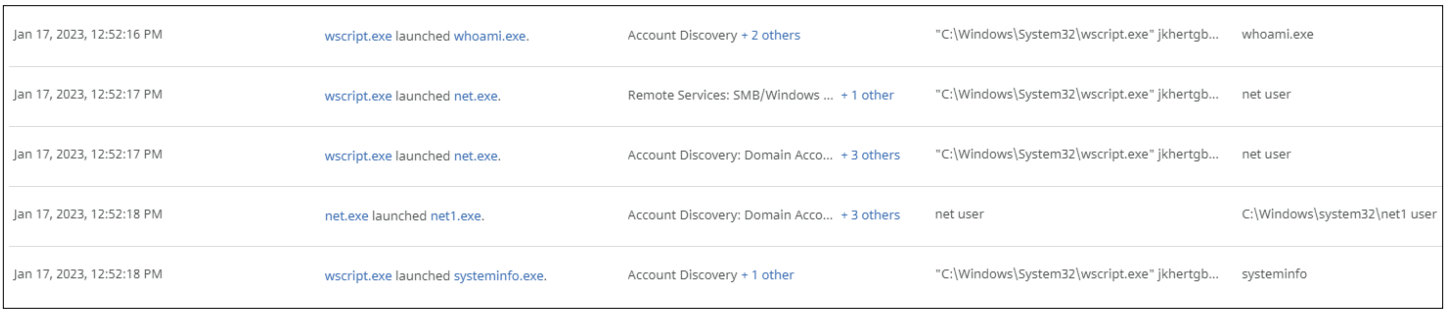
The attack started with Chrome downloading malicious JavaScript. Chrome initially downloads this to a temporary file named “javascript[1]”, then copies it to the final destination at jkhertgbn.js.



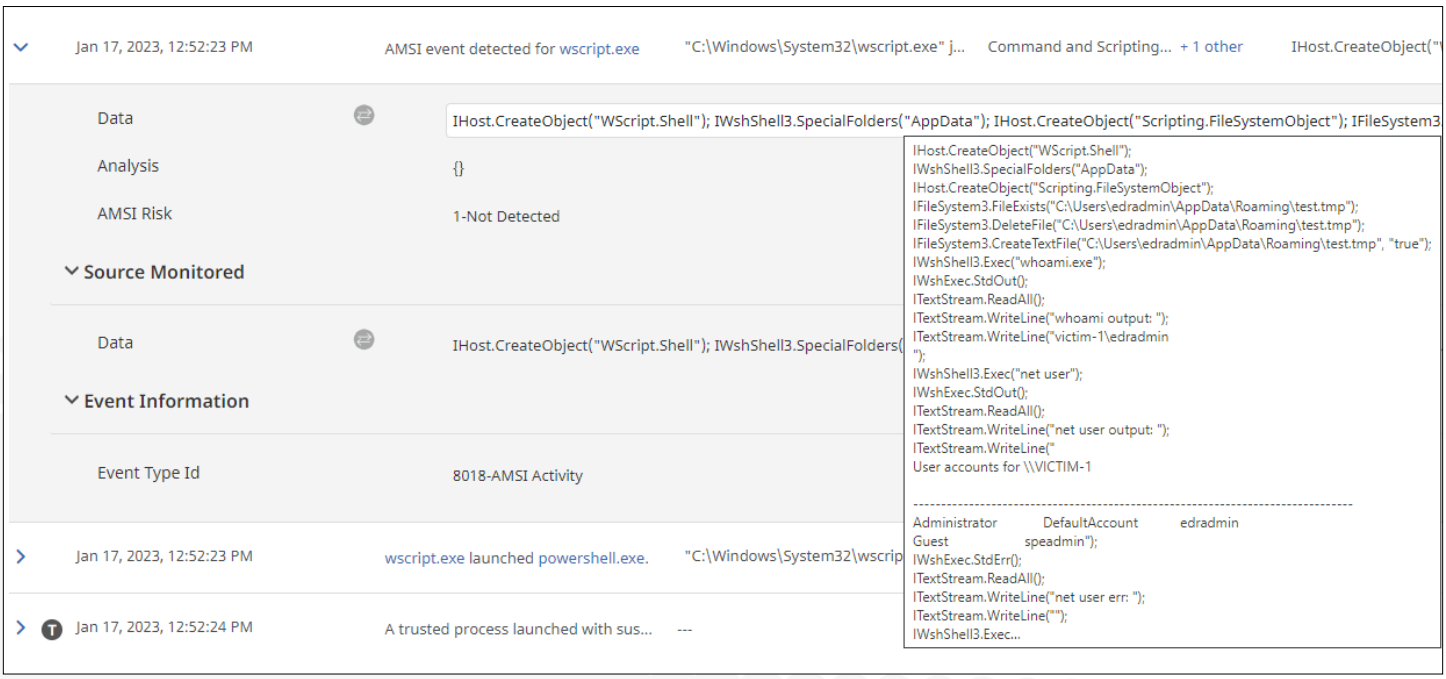
Chrome then runs the malicious JavaScript it just downloaded.



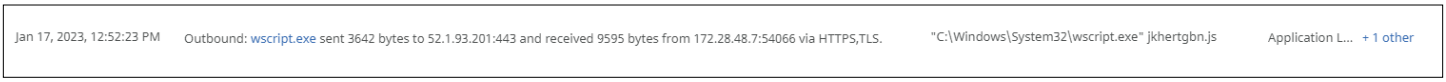
The malicious JavaScript then calls various Windows programs to gather information about the local machine.



SES Complete decodes the JavaScript as it runs and even substitutes variables to see the results of the living off the land Windows programs run in the previous step.



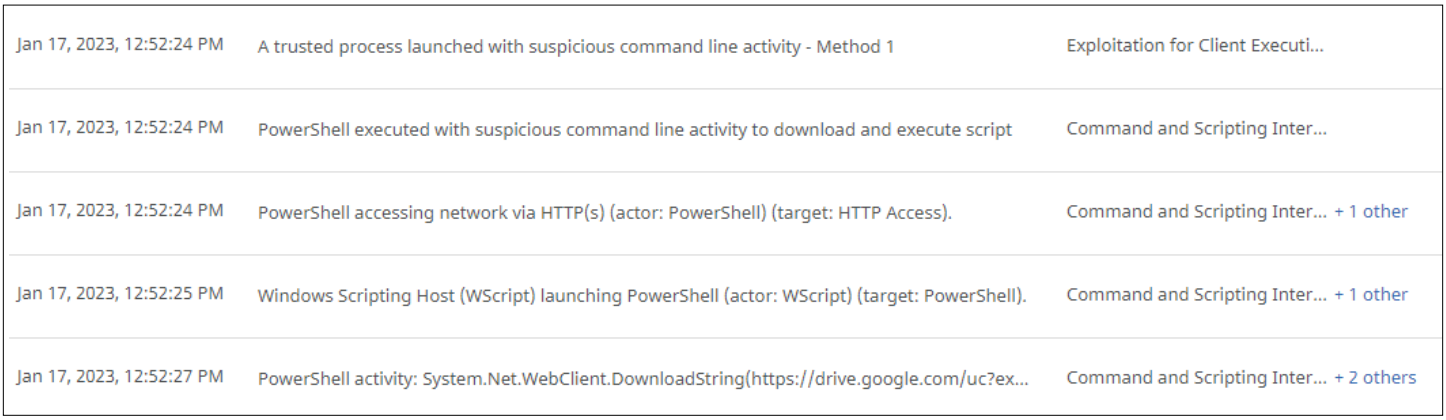
We then see JavaScript sending the data up to the C&C server and receiving further instructions to continue the attack on this target.



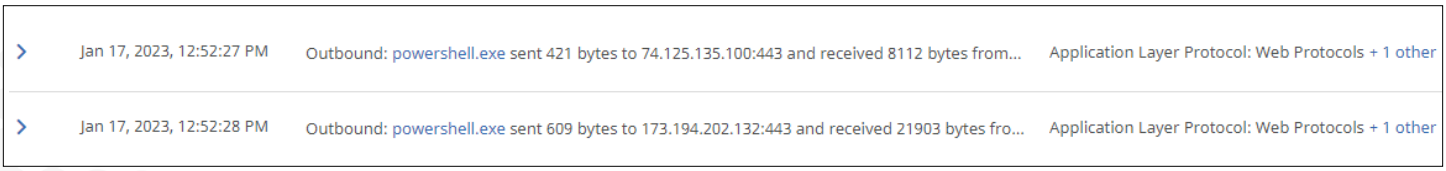
In the previous step, the attacker sent a command to have the JavaScript run a PowerShell command to download and execute the next phase of the attack.

This command is pretty suspicious. SES Complete sends various warnings that

1. The command line is suspicious
2. The command will download and execute script
3. The PowerShell is accessing the network
4. JavaScript is running PowerShell



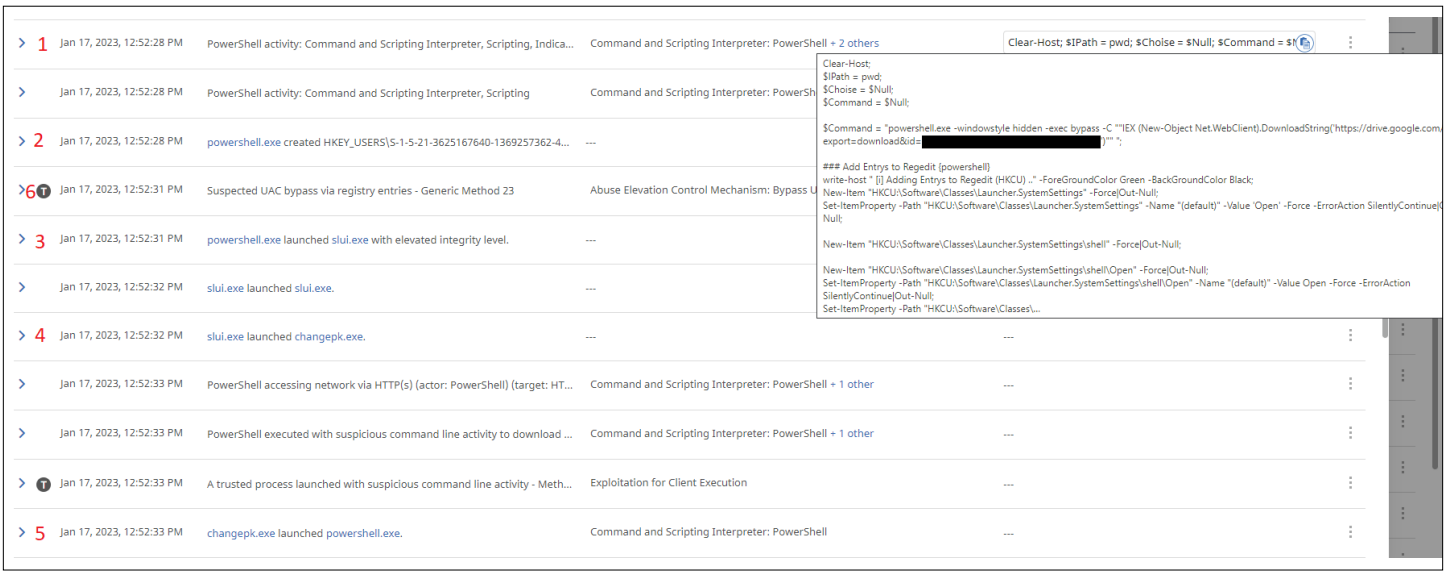
The command then downloads the malicious script from Google Drive. This is entirely in memory; the file is never written to disk.



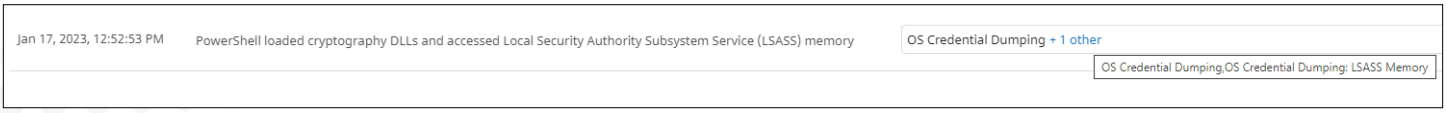
We then see a bunch of interesting activity from the downloaded PowerShell.

1. As with the earlier JavaScript, SES Complete shows the details of the PowerShell being run.
2. A registry key is created at HKCU:\Software\Classes\Launcher.SystemSettings\shellex\ContextMenuHandlers.
3. PowerShell launches the Windows licensing tool slui.exe, a legitimate Windows program with high integrity level.
4. Slui.exe then launches changepk.exe, another legitimate Windows program. This is a normal part of how this Windows licensing tool functions.
5. Changepk.exe then launches malicious PowerShell at high integrity level. This is not how Windows licensing normally functions.
6. This is an abuse of the Windows licensing functionality as a result of the change to the registry made at step 2 above. SES Complete calls this out as a suspected UAC Bypass.

These are important findings. SES Complete clearly calls out the Privilege Escalation that just occurred in addition to all the steps along the way that led to the Privilege Escalation.



Now that the attacker has elevated privileges, they steal credentials stored in LSASS' memory.



In addition, the attacker does a lot of Discovery about the user, machine, and other machines on the network.

Jan 17, 2023, 12:52:56 PM	powershell.exe launched sc.exe.	System Service Discovery	"C:\Windows\system32\sc.exe" query
Jan 17, 2023, 12:52:57 PM	powershell.exe launched net.exe.	Network Share Discovery + 1 other	"C:\Windows\system32\net.exe" share
Jan 17, 2023, 12:52:58 PM	net.exe launched net1.exe.	Network Share Discovery + 1 other	C:\Windows\system32\net1 share
Jan 17, 2023, 12:52:59 PM	powershell.exe launched tasklist.exe.	Process Discovery + 2 others	"C:\Windows\system32\tasklist.exe"
Jan 17, 2023, 12:53:03 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.1
Jan 17, 2023, 12:53:03 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.2
Jan 17, 2023, 12:53:03 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.3
Jan 17, 2023, 12:53:03 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.4
Jan 17, 2023, 12:53:04 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.5
Jan 17, 2023, 12:53:04 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.6
Jan 17, 2023, 12:53:04 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.7
Jan 17, 2023, 12:53:04 PM	powershell.exe launched nslookup.exe.	Remote System Discovery + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.8

All of the stolen credentials and discovery information is staged to a file on disk.

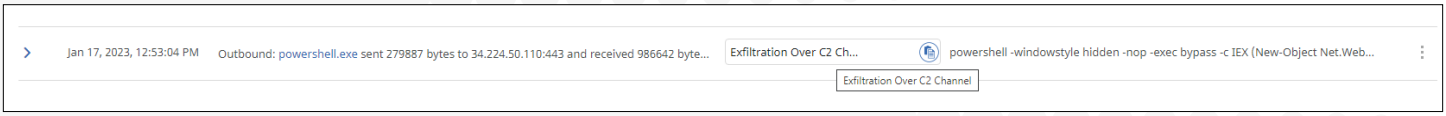
Jan 17, 2023, 12:53:04 PM	powershell.exe modified stageddata.txt.	"PowerShell.exe" -windowstyle hidden -exec bypass -C "IEX ...	Data Staged

Lateral Movement is performed to systems found using Remote System Discovery above. On Victim-1, the initial machine the attacker first accessed, we see PowerShell launching WMIC.exe to create a remote process on Victim-2.

Jan 17, 2023, 12:53:04 PM	powershell.exe launched wmic.e...	Victim-1	"PowerShell.exe" -windowstyle hidden -ex...	"C:\Windows\System32\Wbem\WMIC.exe" /failfast:on /node:"Victim-2" process call create "powershell -windowst...

Then we see the attacker gaining access to Victim-2.

The staged data containing stolen credentials and other staged data is then exfiltrated to the Command and Control server.



SES Complete alerts with an incident showing that something bad happened. But, even better, it clearly details every part of the attack.

Conclusion

With a single, easy-to-deploy agent, SES Complete provides unrivaled protection, blocking most attackers from even entering the door of your environment. If a threat does manage to bypass protection, SES Complete's advanced detection technologies elevate the attack to the incident response team in easy-to-understand MITRE ATT&CK terminology and provide granular detail on what events occurred. SES Complete's superior investigative and response tools are a ready aid in the swift and efficient remediation of threats.

About the Author

Adam Glick is Cyber Analytics Lead for Symantec at Broadcom. He has been developing defensive technologies for nearly twenty years. He's contributed to advanced anti-rootkit tools, behavioral analytics, and file reputation systems. He holds over twenty security related patents. Adam's current focus is on developing analytics to find advanced attacks in progress, detailing the major phases of the attack, such as privilege escalation, credential theft and lateral movement, as well as the individual attack activity, such as registry key modifications for a UAC bypass. Adam's goal is to help defenders separate noise from truly important alerts and act quickly to contain threats.

BROADCOM connecting everything®

For more information, visit our website at: www.broadcom.com

SESC-HRAA-WP100 August 15, 2023