SentinelOne

AI 기반의 위협 차단 및 대응
(Endpoint Prevention Detection & Response)

위협 동향 및 레거시 백신 대비 차별점



최신 위협 현황

원격에서 수행된 명령어	명령어 요약
"c:₩windows₩system32₩cmd.exe" /c "whoami"	모든 사용자 정보와 그룹 정보를 표시하여 시스템의 사용자와 그룹 관계를 확인 사용된 명령어 - cmd - whoami - wmic - tasklist
"C:₩Program Files₩OpenSSH-Win64₩sshd.exe" -z	
"c:₩windows₩system32₩cmd.exe" /c "chcp"	
"C:₩Program Files₩OpenSSH-Win64₩sshd.exe" -z	
"c:₩windows₩system32₩cmd.exe" /c "wmic useraccount get name, sid && echo LINE_DELIMITER && wmic /namespace:₩₩root₩cimv2 path win32_groupuser"	
cmd.exe /Q /c cd 1> ₩₩127.0.0.1₩ADMIN$₩__1729701705.8193433 2>&1	
cmd.exe /Q /c query user 1> ₩₩127.0.0.1₩ADMIN$₩__1729701705.8193433 2>&1	
cmd.exe /Q /c wmic user account get name 1> ₩₩127.0.0.1₩ADMIN$₩__1729701705.8193433 2>&1	
cmd.exe /Q /c wmic useraccount get name 1> ₩₩127.0.0.1₩ADMIN$₩__1729701705.8193433 2>&1	
cmd.exe /Q /c wmic account get name 1> ₩₩127.0.0.1₩ADMIN$₩__1729701705.8193433 2>&1	
cmd.exe /Q /c tasklist 1> ₩₩127.0.0.1₩ADMIN$₩__1729701705.8193433 2>&1	
'cmd.exe /Q /c net user D**** password******/add /y & net user D**** /active:yes & net user D**** /expires:never & net localgroup "Administrators" D**** /add & net localgroup "Remote Desktop Users" D**** /add & reg add "HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩SpecialAccounts₩Userlist" /v D**** /t REG_DWORD /d 0 /f 1> ₩₩127.0.0.1₩ADMIN$₩__1729701705.8193433 2>&1	숨겨진 관리자 계정을 생성하고 원격 접근 권한을 부여, 로그 파일을 로컬 시스템의 ADMIN$ 공유 폴더에 저장 사용된 명령어 - net (user, localgroup)
'net user D**** password******/add /y	
'cmd.exe /Q /c net user D**** password******/add /y & net user D**** /active:yes & net user D**** /expires:never & net localgroup "Administrators" D**** /add & net localgroup "Remote Desktop Users" D**** /add & reg add "HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩SpecialAccounts₩Userlist" /v D**** /t REG_DWORD /d 0 /f 1> ₩₩127.0.0.1₩ADMIN$₩__1729701705.8193433 2>&1	
net user D**** /active:yes	
'cmd.exe /Q /c net user D**** password******/add /y & net user D**** /active:yes & net user D**** /expires:never & net localgroup "Administrators" D**** /add & net localgroup "Remote Desktop Users" D**** /add & reg add "HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩SpecialAccounts₩Userlist" /v D**** /t REG_DWORD /d 0 /f 1> ₩₩127.0.0.1₩ADMIN$₩__1729701705.8193433 2>&1	
net user D**** /expires:never	
'cmd.exe /Q /c net user D**** password******/add /y & net user D**** /active:yes & net user D**** /expires:never & net localgroup "Administrators" D**** /add & net localgroup "Remote Desktop Users" D**** /add & reg add "HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩SpecialAccounts₩Userlist" /v D**** /t REG_DWORD /d 0 /f 1> ₩₩127.0.0.1₩ADMIN$₩__1729701705.8193433 2>&1	
net localgroup "Administrators" D**** /add	
wevtutil qe Microsoft-Windows-TerminalServices-LocalSessionManager/Operational /c:5 "/q:*[System [(EventID=25)]]" /rd:true /f:text	원격 데스크톱 세션 이벤트를 조회하여 최근 원격 데스크톱 연결 시도를 확인 사용된 명령어 - wevtutil

특징

1. 악성코드는 없었다.
2. 탈취된 계정 정보를 활용한 것으로 보인다.
3. 외부로 서비스 되고 있는 리눅스 시스템을 활용했다.
4. Windows OS 가 제공하는 기본 유틸리티만 사용했다.

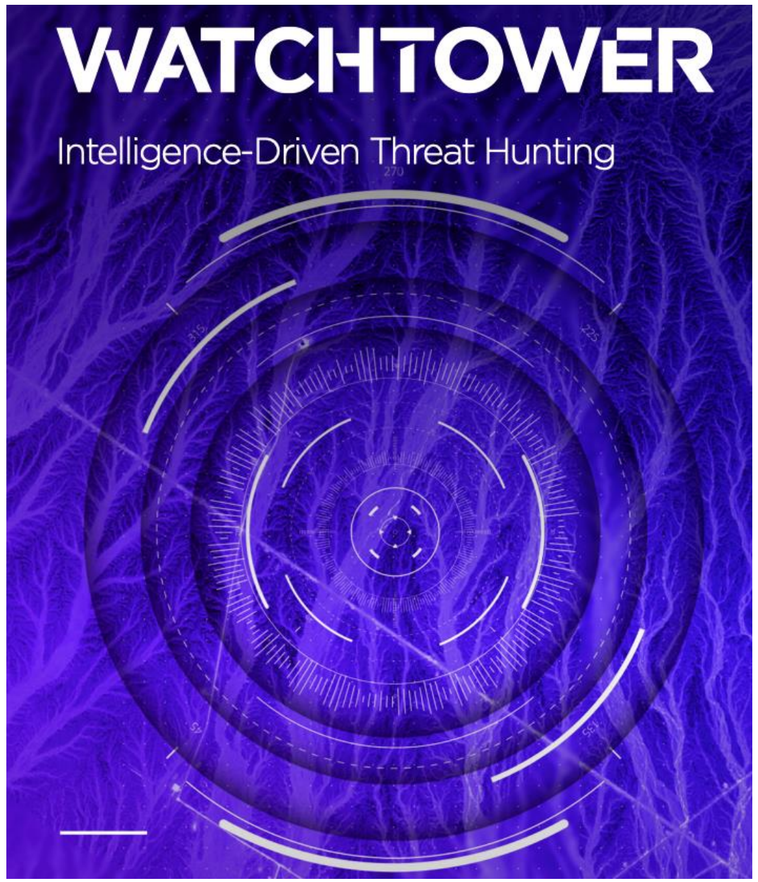
만약 EDR 이 없었다면?

ITEM	Antivirus(백신)	Antivirus + EDR
데이터 수집	악성코드 탐지와 관련된 데이터만 존재	악성 + 정상 데이터 프로세스, 파일, 네트웍(IP, DNS, URL), 레지스트리, 로그온, 스케줄 작업, 커맨드 스크립트, 드라이버 로드
위협 가시성	파일 중심, 시각화 불가	수집된 데이터 기반의 악성 프로세스 중심의 시각화
커스텀 탐지	제공하지 않음	IoC, 인디케이터(악성 행위) 기반의 탐지 수행으로 선제적 위협 탐지
출처(원인) 분석	불가	데이터 기반의 추적
대응	파일 격리	파일 격리, 호스트 격리, 시스템 침해 복구
XDR 연계	지원하지 않음	연계된 3’d party 솔루션과 연계(계정 재설정, 접근통제 등)

사이버 위협 동향

Reconnaissance	Credential Theft	Lateral Movement	Remote Access	Defense Evasion	Staging	Data Exfiltration
Ipconfig	Lsass Dump	Psexec	RDP (mstsc)	Defender Disable	SCCM	RClone
Whoami	Mimikatz	PDQ Install	TeamViewer	Gmer	Group	FileZilla
Net.exe	Meterpreter	Winrm	AnyDesk	Icesword	Policy	Winscp
ADFind	Cobalt Strike	impacket	Splashtop	Regedit (reg.exe)	Psexec	Telegram
ADRecon.py	BloodHound	SSH	ZohoAssist	Process Hacker	PowerShell	Cloud services (MegaSync, megacloud, etc.)
Advanced Port Scanner	SharpHound	SMB	ConnectWise	PowerShell	Remote	Ngrok
IP Scanner	ProcDump	Chisel	BeyondTrust	Service Kill (bat file)	Connectwise	
PingCastle	Process Hacker	WMI	GoToAssist	Process Kill (bat file)		
Powerview	ninjacopy	RDP	RemotePC	Hrsword		
Winrm	NirSoft		TightVNC	Terminator		
Impacket	Lazagne		Registry terminal server enable	Vulnerable drivers		
Cobalt Strike	PassView		NetSupport			
Powershell Empire	PowerDump		NetCat			
arp.exe			Ngrok			
Netstat			FRP			
Nslookup			PowerShell remoting			
WMI						
Ping Castle						
PowerView						
BloodHound						

2023년에 악용된 주요 상용 툴



SentinelOne 차별화된 기술

AI 탐지 엔진

정적 / 동적 AI 엔진으로 알려지지 않은 위협 탐지

ActiveEDR®

악성코드가 수행한 프로세스, 레지스트리, 파일 등 14항목을 기록/관리 및 분석

Storyline™

악성코드 시작부터 마지막까지 모든 과정을 분석 지원

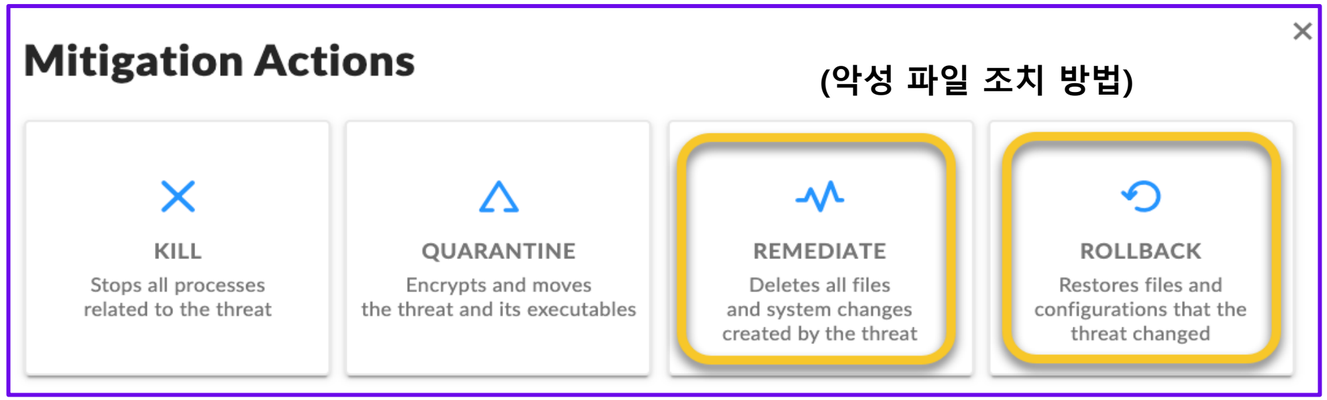
강력한 대응 - 복구

EPP + EDR 센티널원 제공하는 모든 기능을 단일 에이전트로 통합, XDR로 확장

1

ONE Console

전세계 모든 지역에서 단일 콘솔로 통합 관리 제공



SentinelOne
- 탐지 기술



SentinelOne 탐지 엔진



REPUTATION
클라우드 평판엔진

해쉬값 기준 악성코드 차단 –
OS별 최적화된 해쉬DB 제공



STATIC AI
정적 AI 엔진

AI 데이터 모델 기반
파일 속성을 추출하여 비교



BEHAVIORAL AI
동적 AI 엔진

MITRE framework 기반
실시간 악성 활동 탐지

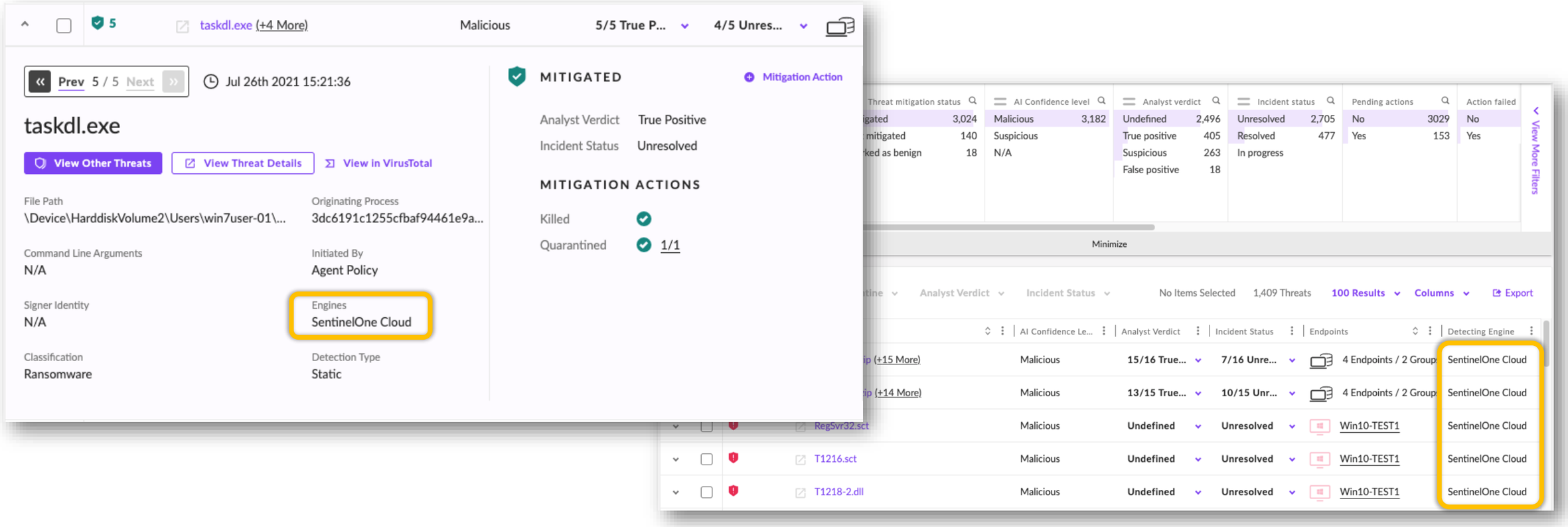


DEEP VISIBILITY
액티브 EDR

데이터 가시성
Storyline 기반 위협 헌팅

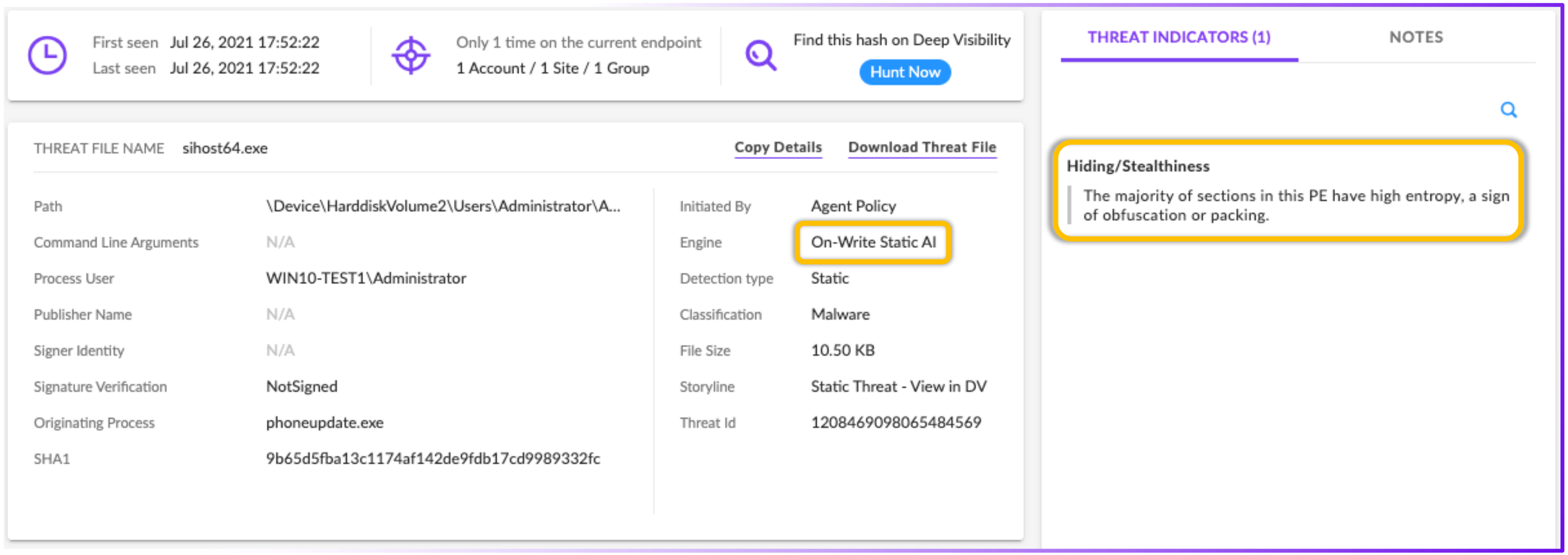
평판(Reputation Engine)

- 실행되는 파일의 해쉬값을 수집하여 SentinelOne 클라우드에서 비교하여 판단
- OS별 각각의 해쉬 DB 운영
- 한번 실행된 악성코드의 해쉬 DB는 Blacklist에 유지



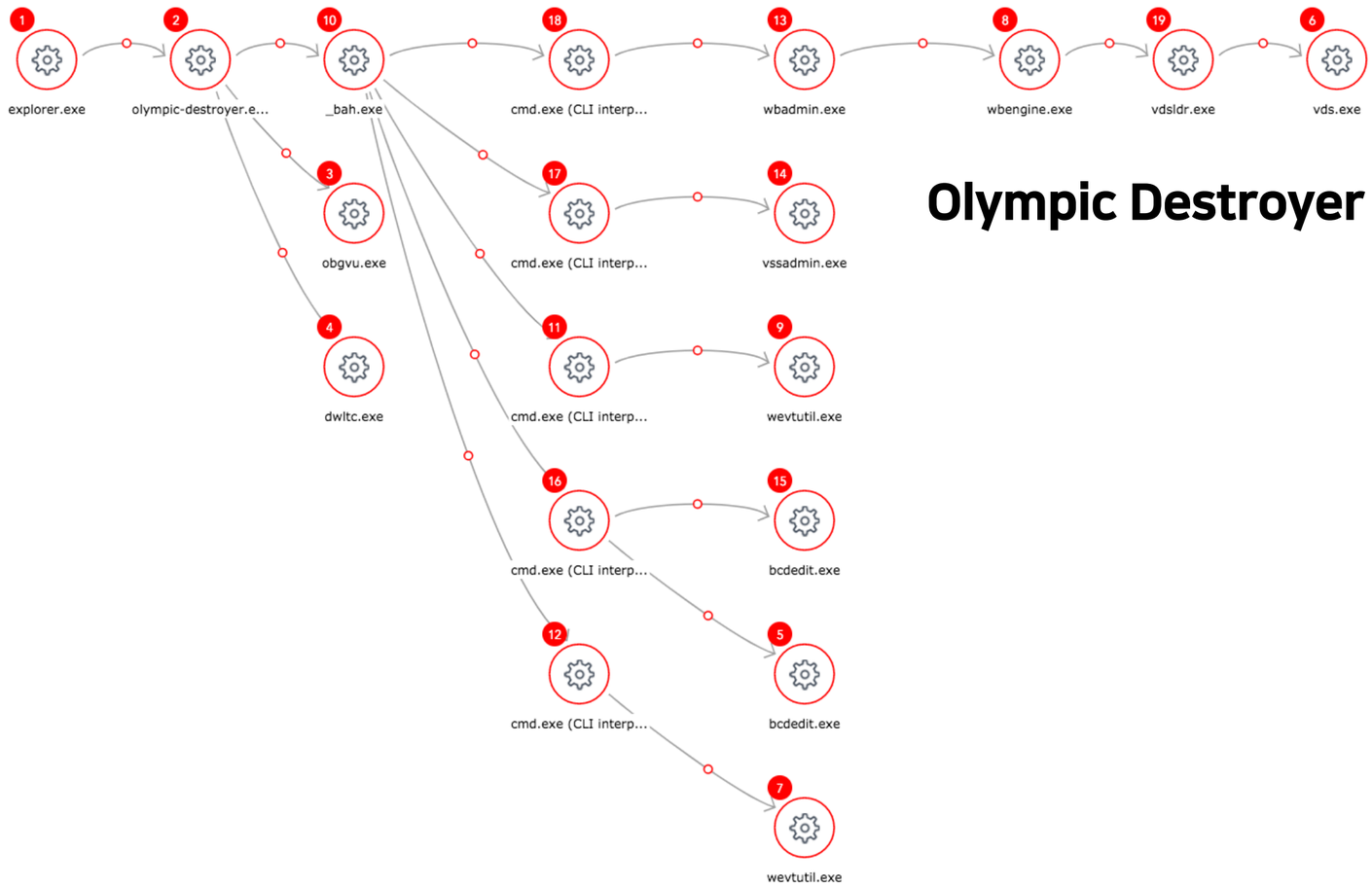
Static AI(Artificial Intelligence)

- 파일을 실행하지 않고 헤더 정보 수집하여 AI를 활용한 악성코드 여부 판단
- Entropy기반 분석 및 차단
- Training Set을 통한 AI엔진 분석



SentinelOne 행위 기반 탐지 엔진

- **MITRE ATT&CK 프레임워크를 따르는 악성 활동 탐지**
  - MITRE 공격 프레임워크정보를 활용
    - 침투 단계, 공격 전술에 대한 가시성 확



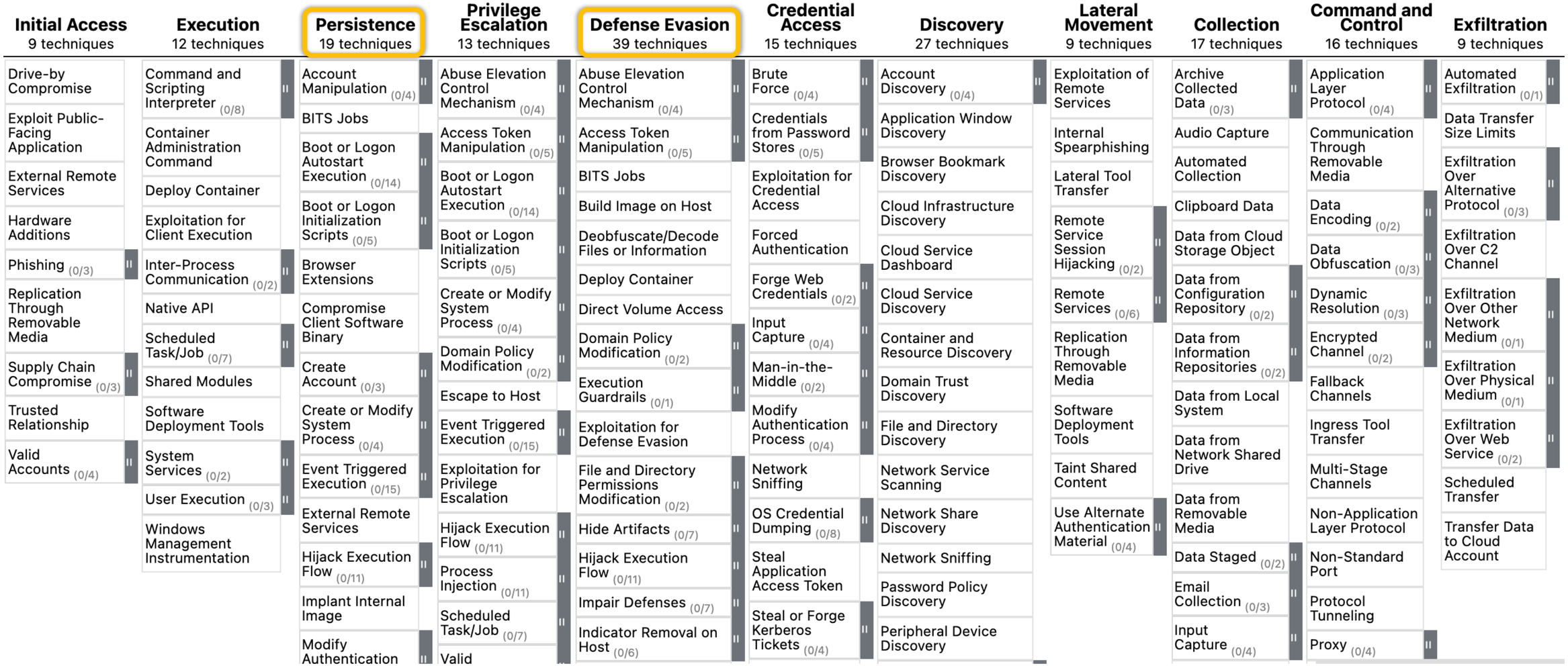
Olympic Destroyer

- Lateral movement(횡 이동 공격)
- 스크립트, local CLI
- 메모리 익스플로잇
- 권한 상승
- 시스템 조작, 레지스트리 & 커널 작업
- 스텔스, 스파잉, 탐지 회피
- 네트워 행위
- 지속 공격, anti-debugging
- 데이터 수집
- 파일 작업과 조작
- 프로세스 작업

SentinelOne 행위 기반 탐지 엔진

- 각 공격 기법 별 Tactics(공격 전술), Techniques(공격기술) 상세 정보 제공

MITRE ATT&CK Framework

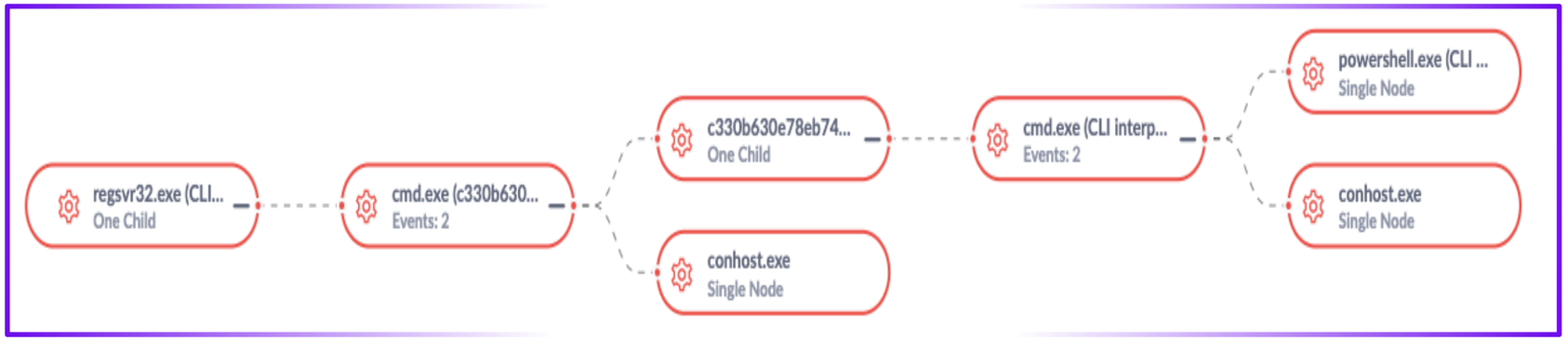


Anti-exploitation / Fileless

- 탐지 사례

PowerShell 의
암호화(Encryption) 옵션을
활용한 명령 실행으로 악성
행위를 숨기기 위한 행위 탐지





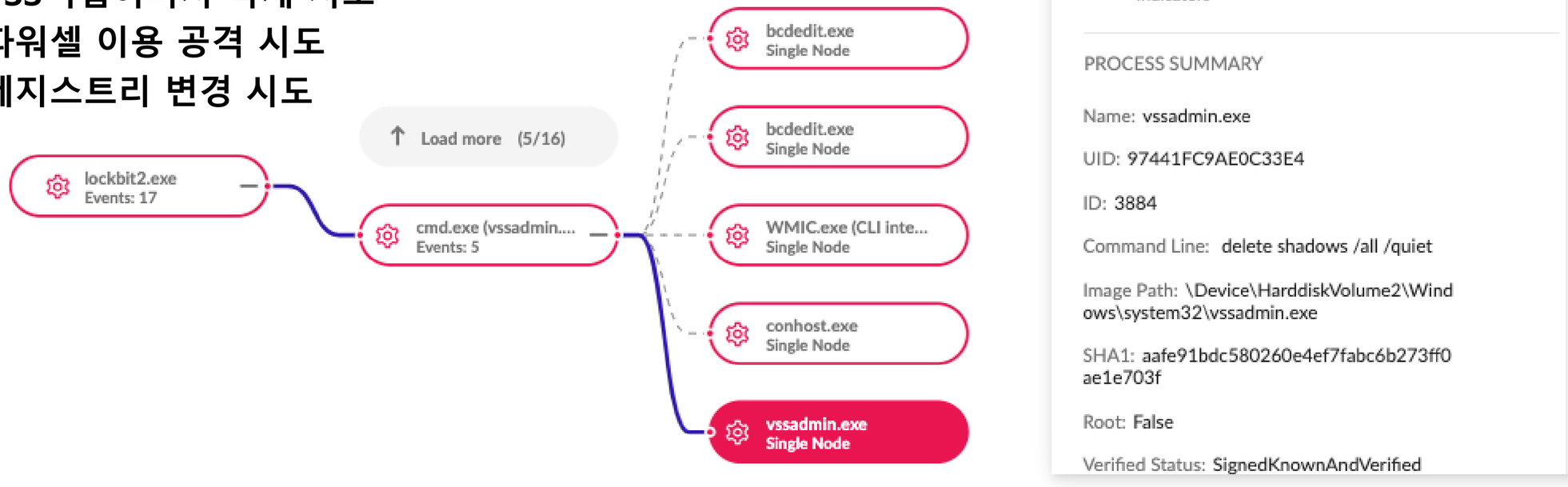


Storyline (스토리라인)

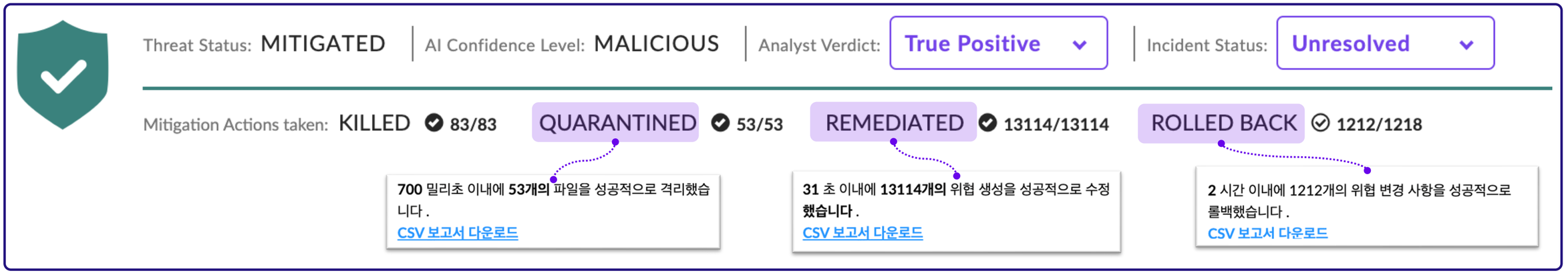
- 악성코드 공격 시작부터 끝까지 관련 모든 행위를 연관하여 분석할 수 있는 기술

PC 상에서 사용자가 실행하는 프로세스 기반 변경 사항 추적관리

- 브라우저 실행
- 새로운 탭 시작
- 파일 다운로드
- 다운로드된 파일 실행
- VSS백업이미지 삭제 시도
- 파워셸 이용 공격 시도
- 레지스트리 변경 시도



복구 기능

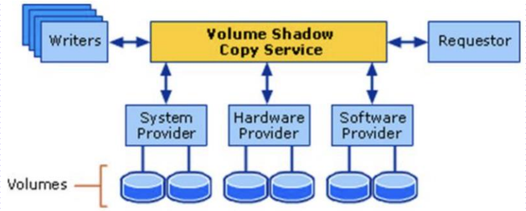


리부팅
(스냅샷 I 생성)

4시간 경과
(스냅샷 II 생성)

4시간 경과
(스냅샷 III 생성)

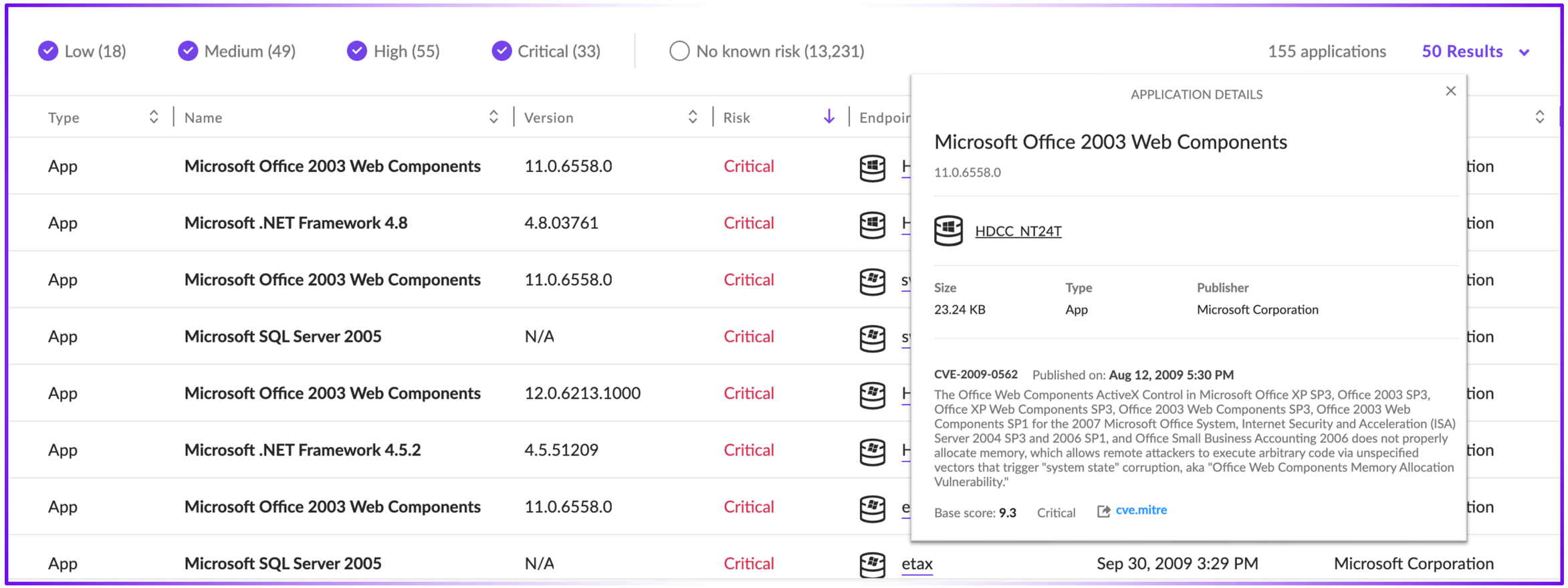
Windows Volume Shadow Service 활용



악성코드로 인한 손상 시
(스냅샷 II 데이터를 이용하여 롤백 수행)

어플리케이션 취약점 정보 제공

- 설치된 어플리케이션 정보와 CVE 취약점 데이터를 결합하여 시스템의 취약점 정보 제공

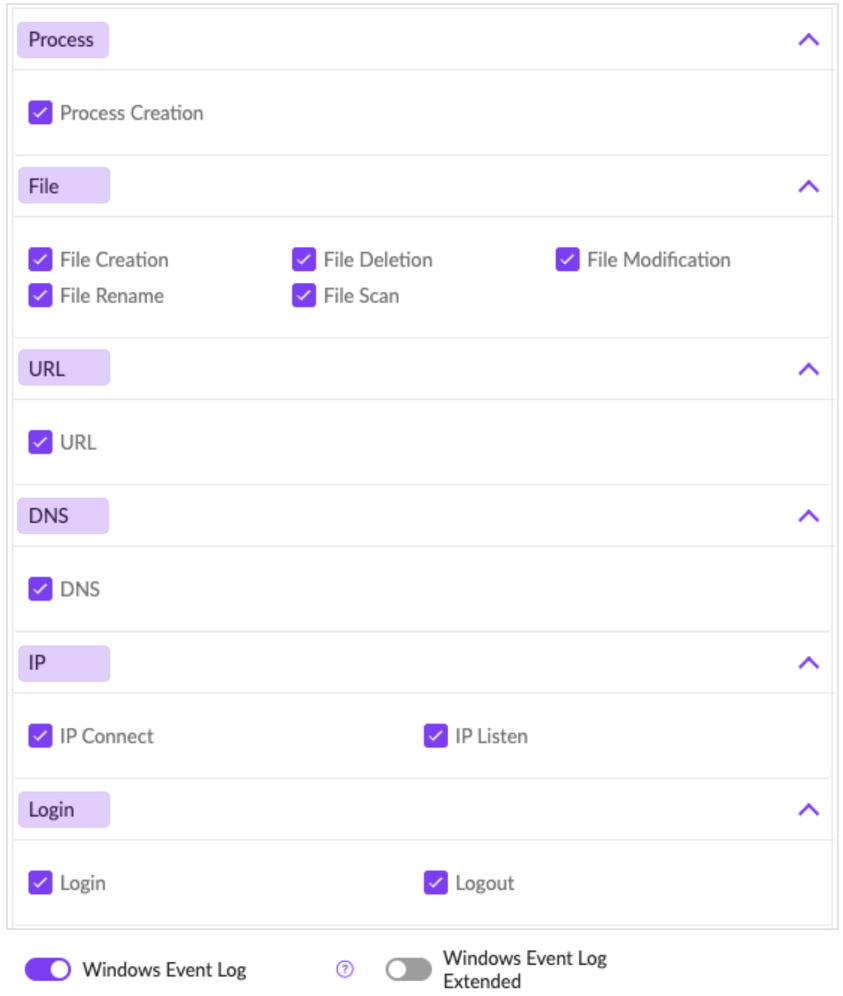


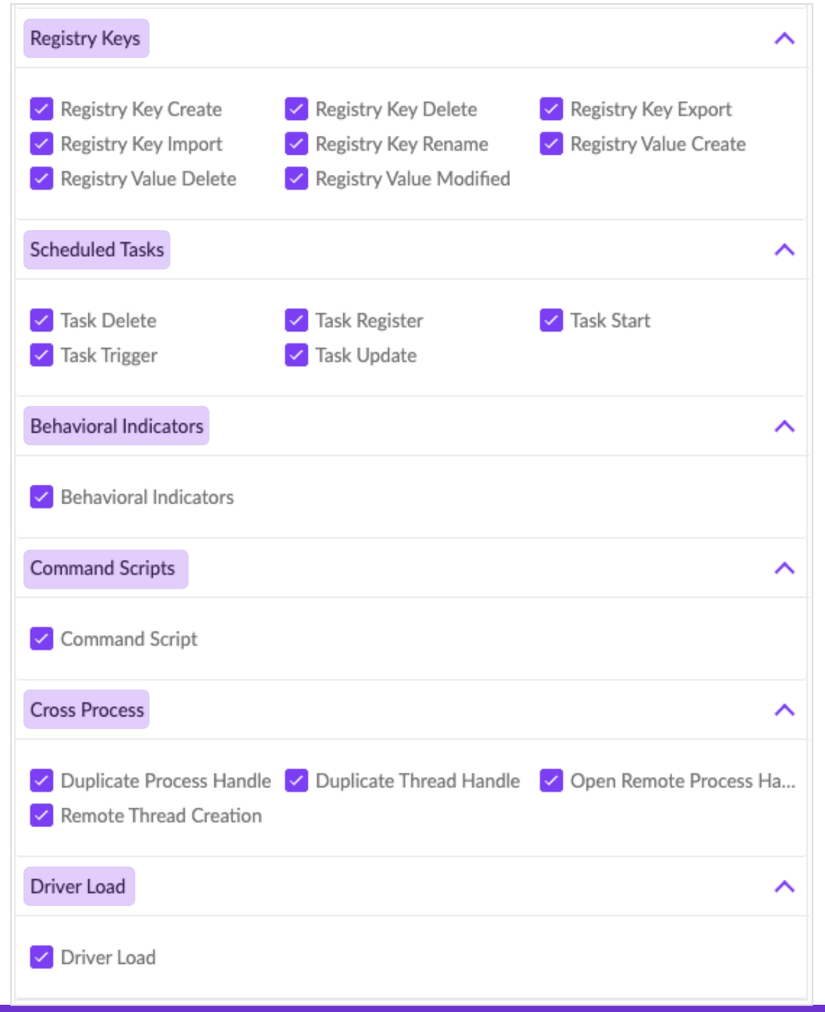
SentinelOne - EDR



EDR 수집 데이터

Process, Indicator, File, Network Action, DNS, Registry, Scheduled Task, Login





EDR 상세

Registry 상세

2021 17:35:33 | @WanaDecryptor@.exe | True | D453A462A7992FE5 | "C:\Users\hmm\Desktop\@WanaDecryptor@.exe" | DESKTOP-SGJ7JH9\h... | C:\Users\hmm\D

SOURCE PROCESS DETAILS

Name	@WanaDecryptor@.exe
Storyline ID	D453A462A7992FE5
Command Line	"C:\Users\hmm\Desktop\@WanaDecryptor@.exe"
User	DESKTOP-SGJ7JH9\hmm
Start Time	Oct 15, 2021 17:35:33
Image Path	C:\Users\hmm\Desktop\@WanaDecryptor@.exe
PID	4356

REGISTRY DETAILS

Key Path	USER\S-1-5-21-3001522091-808374922-7666... Show More
Value	C:\Users\hmm\Desktop\@Wan
Old Value Type	SZ
Old Value	C:\Windows\web\wallpaper\

ENDPOINT DETAILS

Endpoint Name	DESKTOP-SGJ7JH9
Endpoint OS	windows
Agent UUID	54ed31ee65a545f1910cc55b316e163e
Endpoint Machine Type	desktop
Site Name	ESCARE STD
Site ID	1159824934048771541

DNS 상세

IT-WKS-26 | DNS | DNS Resolved | Oct 18, 2021 09:24:06 | chrome.exe | False | 5DD08E7FF3B08013 | "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --ty

SOURCE PROCESS PARENT DETAILS

Name	chrome.exe
Start Time	Oct 8, 2021 08:19:48
Image Path	C:\Program Files (x86)\Google\Chrome\Applicati...
Unique ID	9104584C3395E33F

SOURCE PROCESS DETAILS

Name	chrome.exe
Storyline ID	5DD08E7FF3B08013
Command Line	"C:\Program Files (x86)\Google\Chrome\Applica... Show More
User	ITTELLIGENT\Gui.Salgado
Start Time	Oct 8, 2021 08:19:48

DNS DETAILS

Request	argus.shopifycloud.com
Response	type: 5 argus-server-production-web-ngin-k

EDR 상세

Process 상세

Agent UUID	Event type	Event Time	Source Process Unique ID	Source Process StoryLine ID
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4	Open Remote Process Handle	Nov 8 2024 14:31:18	conhost.exe 71C479713E605A46	DBBA79713E605A46

Open Remote Process Handle

Agent UUID	VMware- OH (Windows10 - 2)
Source Process Unique ID	conhost.exe 71C479713E605A46
Source Process Comma...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Source Process User	DESKTOP-N3DR6K9\ESCARE-OH Windows 2
Target Process Unique ID	fsutil.exe 89C479713E605A46
Target Process Relation	other
Target Process Comman...	fsutil file setZeroData offset=0 length=524288 "C:\Users\ESCARE-OH Windows 2\...
Target Process User	DESKTOP-N3DR6K9\ESCARE-OH Windows 2

Files 상세

Agent UUID	Event type	Event Time	Source Process Unique ID	Source Process StoryLine ID
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4	File Rename	Nov 8 2024 14:30:48	0545f842ca2eb77bcac0fd17d6d... DABA79713E605A46	DBBA79713E605A46

File Rename

Agent UUID	VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4
Source Process Unique ID	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe DABA79713E605A46
Target File Path	C:\Users\Public\Documents\afterSentDocuments\docs9\ghi3.pdf.lockbit
Target File Old File Path	C:\Users\Public\Documents\afterSentDocuments\docs9\ghi3.pdf
Target File size	6656

EDR 상세

Indicator 상세

oral Indicators | Oct 15, 2021 17:35:34 | @WanaDecryptor@.exe | True | D453A462A7992FE5 | C:\Users\hmm\Desktop\@WanaDecryptor@.exe | "C:\Users\hmm\Desktop\@WanaDecryptor@.exe"

3f4a711

SOURCE PROCESS DETAILS

Name	@WanaDecryptor@.exe
Storyline ID	D453A462A7992FE5
Command Line	"C:\Users\hmm\Desktop\@WanaDecryptor@.exe"
User	DESKTOP-SGJ7JH9\hmm
Start Time	Oct 15, 2021 17:35:33
Image Path	C:\Users\hmm\Desktop\@WanaDecryptor@.exe
PID	4356

INDICATOR DETAILS

Name	RansomwareBehavior
Category	Ransomware
Description	Behaves like ransomware. MITRE: Impact {T1486}

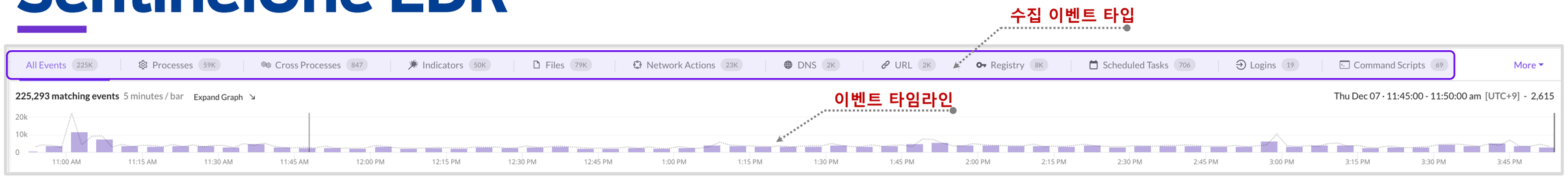
ENDPOINT DETAILS

Endpoint Name	DESKTOP-SGJ7JH9
Endpoint OS	windows
Agent UUID	54ed31ee65a545f1910cc55b316e163e
Endpoint Machine Type	desktop
Site Name	ESCARE STD
Site ID	1159824934048771541

Network 상세

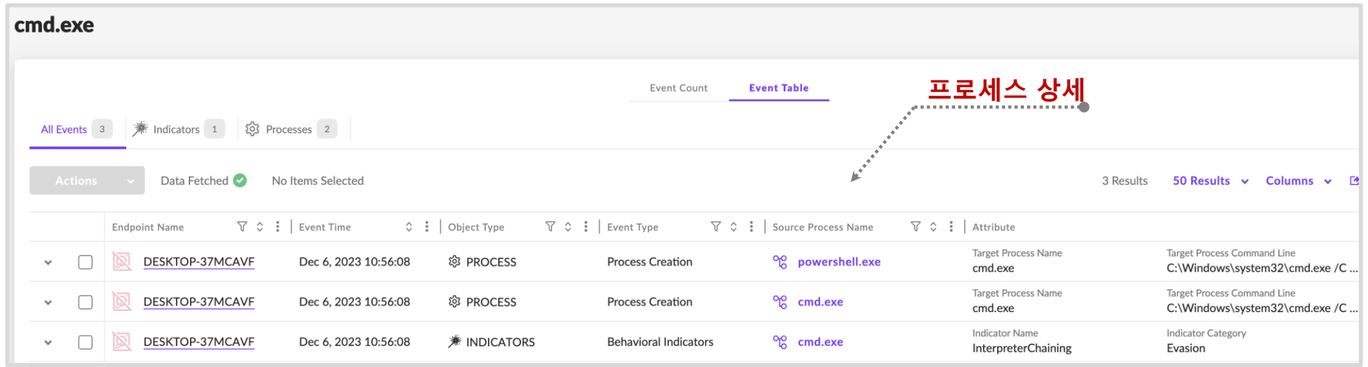
Agent UUID	Event type	Event Time	Source Process Unique ID	Source IP	Source Port	Destination IP	Destination Port	Network Event Direction	Network Connection Status
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4	IP Connect	Nov 8 2024 14:29:32	0545f842ca2eb77bcac0fd17d6d... DABA79713E605A46	192.168.2.144	50217	192.168.2.254	445	OUTGOING	BLOCKED
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4	IP Connect	Nov 8 2024 14:29:32	0545f842ca2eb77bcac0fd17d6d... DABA79713E605A46	192.168.2.144	50216	192.168.2.254	135	OUTGOING	BLOCKED
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4	IP Connect	Nov 8 2024 14:29:32	0545f842ca2eb77bcac0fd17d6d... DABA79713E605A46	192.168.2.144	50215	192.168.2.253	445	OUTGOING	BLOCKED
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4	IP Connect	Nov 8 2024 14:29:32	0545f842ca2eb77bcac0fd17d6d... DABA79713E605A46	192.168.2.144	50214	192.168.2.253	135	OUTGOING	BLOCKED
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4	IP Connect	Nov 8 2024 14:29:32	0545f842ca2eb77bcac0fd17d6d... DABA79713E605A46	192.168.2.144	50213	192.168.2.252	445	OUTGOING	BLOCKED
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4	IP Connect	Nov 8 2024 14:29:32	0545f842ca2eb77bcac0fd17d6d... DABA79713E605A46	192.168.2.144	50212	192.168.2.252	135	OUTGOING	BLOCKED
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4	IP Connect	Nov 8 2024 14:29:32	0545f842ca2eb77bcac0fd17d6d... DABA79713E605A46	192.168.2.144	50211	192.168.2.251	445	OUTGOING	BLOCKED
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4	IP Connect	Nov 8 2024 14:29:32	0545f842ca2eb77bcac0fd17d6d... DABA79713E605A46	192.168.2.144	50210	192.168.2.251	135	OUTGOING	BLOCKED

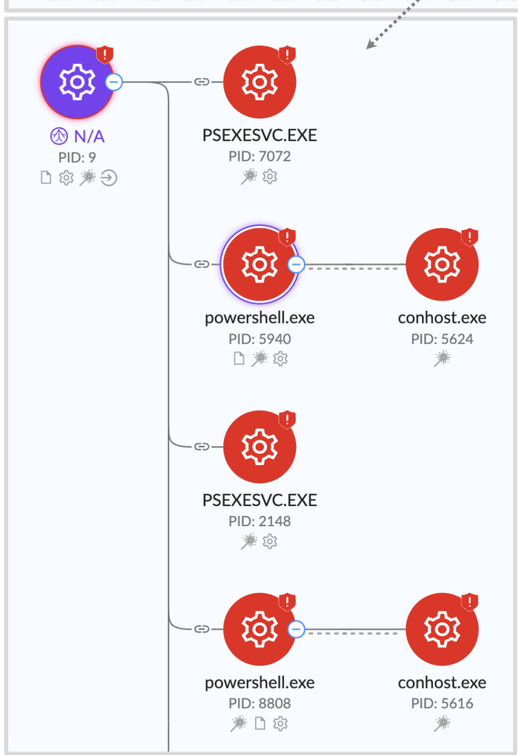
SentinelOne EDR

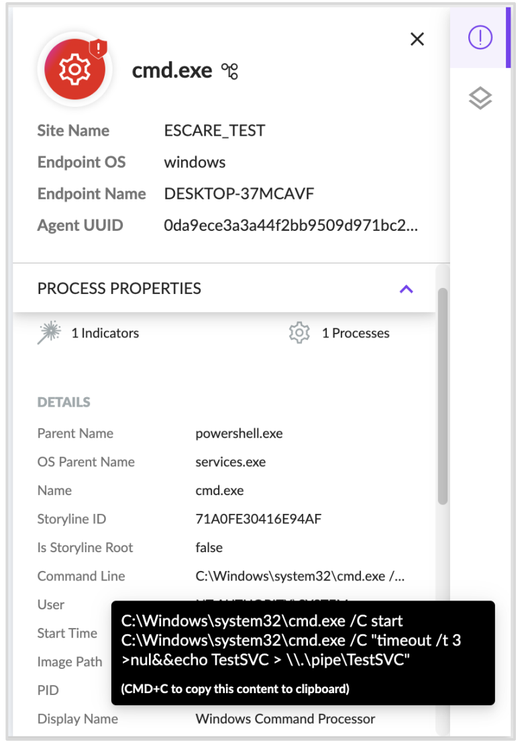


Event Time	Agent UUID	Event Category	Event type	Event Details		URL
Dec 7 2023 11:46:36	DESKTOP-2DGA439 b072099f1200413aa0b993856a29c93f	url	POST	URL Action POST		https://teams.events.data.microsoft.com/OneCollector/1.0/
Dec 7 2023 11:46:36	DESKTOP-2DGA439 b072099f1200413aa0b993856a29c93f	ip	IP Connect	Network Event Direction OUTGOING	Network Connection Status SUCCESS	
Dec 7 2023 11:46:33	DESKTOP-2DGA439 b072099f1200413aa0b993856a29c93f	ip	IP Connect	Network Event Direction OUTGOING	Network Connection Status SUCCESS	
Dec 7 2023 11:46:33	DESKTOP-2DGA439 b072099f1200413aa0b993856a29c93f	file	File Deletion	Target File size 23082		
Dec 7 2023 11:46:33	DESKTOP-2DGA439 b072099f1200413aa0b993856a29c93f	dns	DNS Resolved	DNS Response type: 5 enterprise-activity-ge...		
Dec 7 2023 11:46:33	DESKTOP-2DGA439 b072099f1200413aa0b993856a29c93f	registry	Registry Value ...	Registry Value Type BINARY	Registry Value Full Size 24	
Dec 7 2023 11:46:33	DESKTOP-2DGA439 b072099f1200413aa0b993856a29c93f	file	File Rename	Target File Old File Path C:\Users\ESCARE\AppData\...	Target File size 3122	
Dec 7 2023 11:46:33	DESKTOP-2DGA439 b072099f1200413aa0b993856a29c93f	file	File Rename	Target File Old File Path C:\Users\ESCARE\AppData\...	Target File size 3134	
Dec 7 2023 11:46:33	DESKTOP-2DGA439 b072099f1200413aa0b993856a29c93f	file	File Rename	Target File Old File Path C:\Users\ESCARE\AppData\...	Target File size 21922	

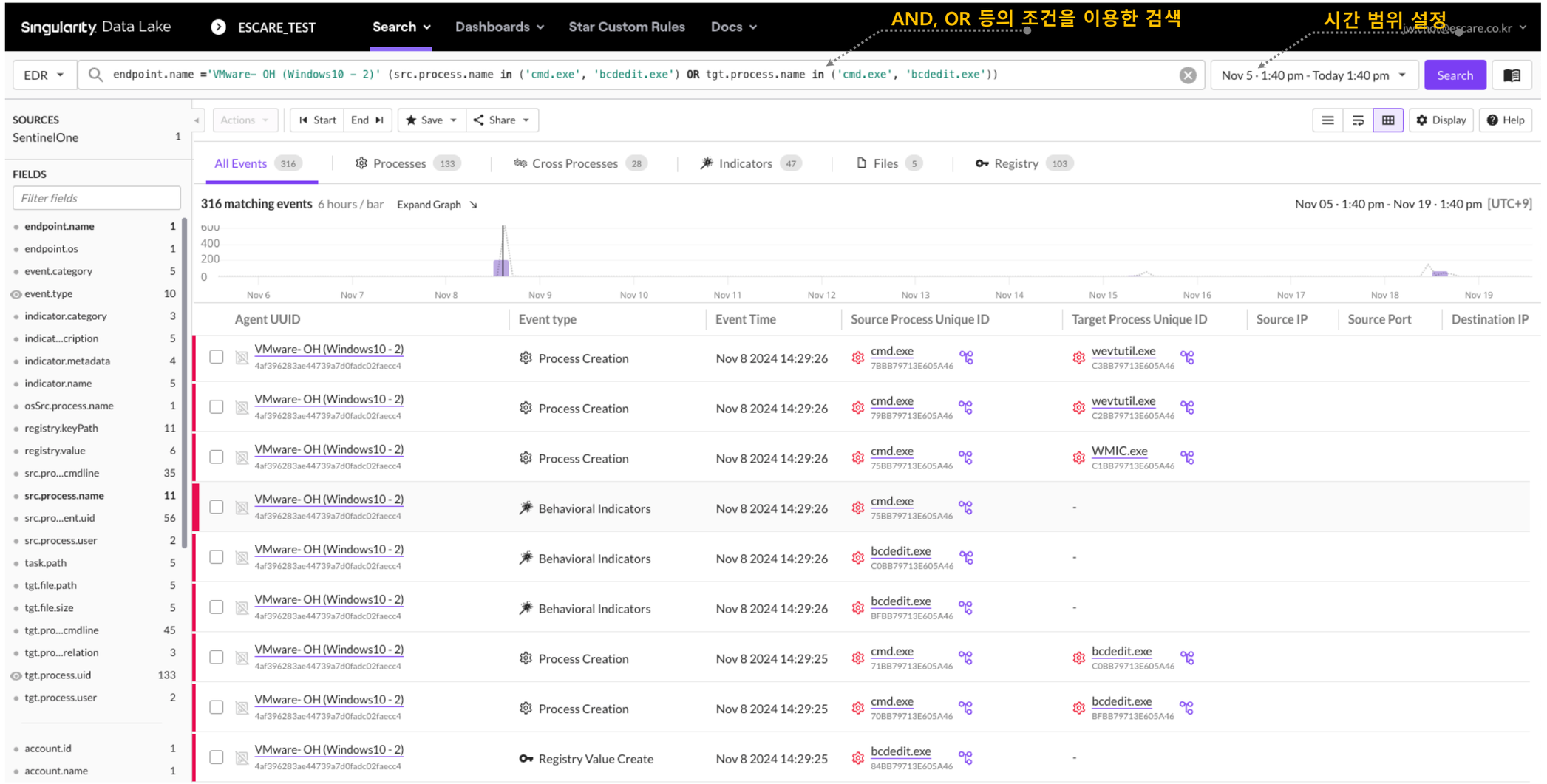








EDR 데이터 검색


AND, OR 등의 조건을 이용한 검색
시간 범위 설정
Singularity Data Lake
ESCARE_TEST
Search
Dashboards
Star Custom Rules
Docs
EDR
endpoint.name ='VMware- OH (Windows10 - 2)' (src.process.name in ('cmd.exe', 'bcdedit.exe') OR tgt.process.name in ('cmd.exe', 'bcdedit.exe'))
Nov 5 · 1:40 pm - Today 1:40 pm
Search
SOURCES
SentinelOne 1
FIELDS
Filter fields
endpoint.name 1
endpoint.os 1
event.category 5
event.type 10
indicator.category 3
indicat...cription 5
indicator.metadata 4
indicator.name 5
osSrc.process.name 1
registry.keyPath 11
registry.value 6
src.pro...cmdline 35
src.process.name 11
src.pro...ent.uid 56
src.process.user 2
task.path 5
tgt.file.path 5
tgt.file.size 5
tgt.pro...cmdline 45
tgt.pro...relation 3
tgt.process.uid 133
tgt.process.user 2
account.id 1
account.name 1
Actions
Start
End
Save
Share
Display
Help
All Events 316
Processes 133
Cross Processes 28
Indicators 47
Files 5
Registry 103
316 matching events 6 hours / bar
Expand Graph
Nov 05 · 1:40 pm - Nov 19 · 1:40 pm [UTC+9]
600
400
200
0
Nov 6
Nov 7
Nov 8
Nov 9
Nov 10
Nov 11
Nov 12
Nov 13
Nov 14
Nov 15
Nov 16
Nov 17
Nov 18
Nov 19
Agent UUID
Event type
Event Time
Source Process Unique ID
Target Process Unique ID
Source IP
Source Port
Destination IP
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4
Process Creation
Nov 8 2024 14:29:26
cmd.exe 7BBB79713E605A46
wevtutil.exe C3BB79713E605A46
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4
Process Creation
Nov 8 2024 14:29:26
cmd.exe 79BB79713E605A46
wevtutil.exe C2BB79713E605A46
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4
Process Creation
Nov 8 2024 14:29:26
cmd.exe 75BB79713E605A46
WMIC.exe C1BB79713E605A46
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4
Behavioral Indicators
Nov 8 2024 14:29:26
cmd.exe 75BB79713E605A46
-
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4
Behavioral Indicators
Nov 8 2024 14:29:26
bcdedit.exe C0BB79713E605A46
-
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4
Behavioral Indicators
Nov 8 2024 14:29:26
bcdedit.exe BFBB79713E605A46
-
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4
Process Creation
Nov 8 2024 14:29:25
cmd.exe 71BB79713E605A46
bcdedit.exe C0BB79713E605A46
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4
Process Creation
Nov 8 2024 14:29:25
cmd.exe 70BB79713E605A46
bcdedit.exe BFBB79713E605A46
VMware- OH (Windows10 - 2) 4af396283ae44739a7d0fadc02faecc4
Registry Value Create
Nov 8 2024 14:29:25
bcdedit.exe 84BB79713E605A46
-

EDR 활용 - Threat Hunting

- **Living off the Land Attack**



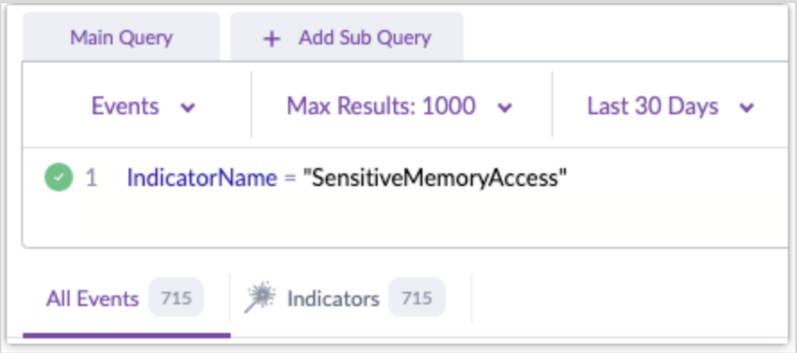
새로운 사용자가 생성된 후 해당 사용자가 생성한 프로세스 확인

- **비정상적 스케줄 작업 생성**



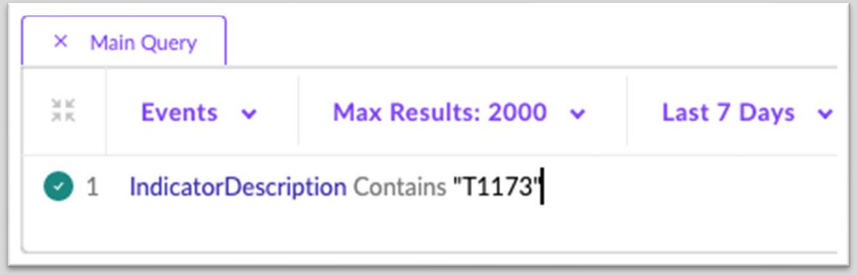
예약된 작업을 생성하는 악의적 프로세스를 탐지

- **악성 행위 헌팅**



민감한 메모리 접근

- **문서에서 발생되는 위협 헌팅**



src.process.parent.name in ("Microsoft Word" , "MicrosoftWnExcel" , "Microsoft Outlook" , "Microsoft Powerpoint") AND src.process.name in ("powershell.exe" , "cmd.exe" , "python.exe")

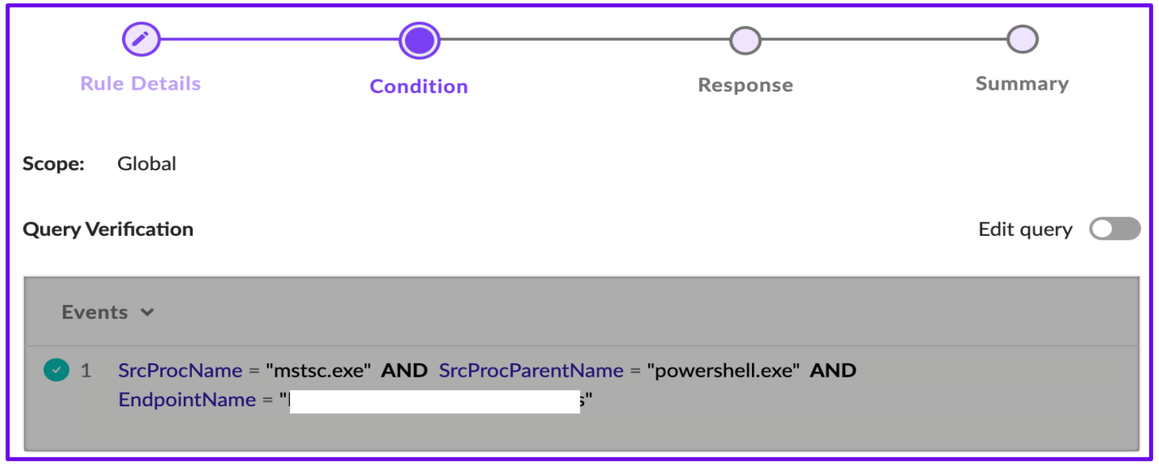
MS Office 문서에서 발생되는 로컬 데이터 수집, C&C 서버 통신 등에 사용되는 악성행위를 탐지

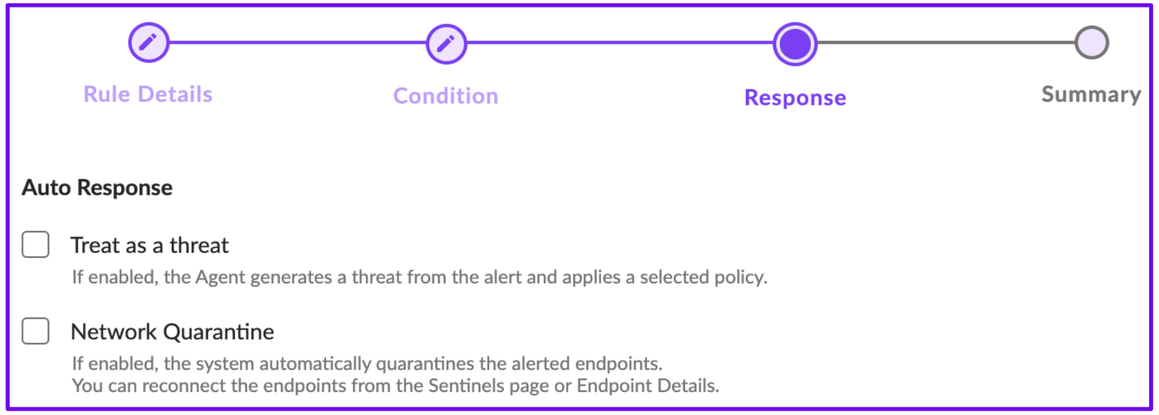
Star Alert (커스텀 탐지 룰)

- 원하는 조건에 해당되는 이벤트 알림 제공 및 조치까지 자동화 기능

검색하고자 하는 조건 입력
- 다양한 조건식 지원
- 실행된 프로세스
- 레지스트리, 파일
- 로그 이벤트 등
- IP, URL 등

대응 방법
- Treat as a Threat
  공격으로 인지, 롤백/차단 등
- Network Quarantine
  네트워크 격리 지원





커스텀 탐지 룰

	Status	Severity	Generated Alerts	Description
Powershell Download Cradles	Active	Low	2971	악의적인 파일을 다운로드하기 위한 PowerShell 사용을 감지
SparkRAT Detection	Active	Medium	1	SparkRAT with VPN Agent (국내 VPN 프로그램의 인스톨...
SQL Server threat detection	Active	Low	61	맬록스 랜섬웨어 SQL 서버 공격 탐지
LOLBin BITS Jobs	Active	Medium	0	BITS Jobs(Background Intelligent Transfer Service)을 악...
Windows Remote Management Execution	Active	Low	0	WMIC, MMC 등을 이용한 원격 프로세스 실행 탐지
Raspberry Robin Worm	Active	Low	0	MSIEXEC 를 이용하여 C2 서버와 통신 시도(설치프로그램 ...
Clear Windows Event Logs Powershell or W...	Active	Medium	0	윈도우 이벤트 로그 삭제 시도
Kerberoasting	Active	Low	0	액티브 디렉토리 포스트 익스플로잇 도메인 권한 상승 공격
Netcat Process	Active	Medium	0	Netcat(= 네트워크에서 데이터를 읽고 쓸 수 있도록하는 네트...
PsExec Process	Active	Medium	1	PsExec(= 원격 명령 실행 유틸리티) 탐지
Run Scripts through Office program	Active	Low	0	오피스 프로그램을 통한 스크립트 실행
External IPs connections attempts to RDP o...	Active	Low	50	외부 IP에서 RDP, SSH 접속 시도
Bat or cmd files are dropped directly to a te...	Active	Low	10	Bat 또는 cmd 파일에서 temp 폴더에 파일 생성
OS Credential Dumping(SAM)	Active	High	0	CmdLine으로 SAM 파일 관련 커맨드 실행 탐지 (*SAM: 로...

Edit Custom Rule

Rule Details — Condition — **Response** — Summary

Active Response

When this rule matches a SentinelOne endpoint event, Storyline Active Response should:

탐지 시 대응정책

☑ Treat as a threat
If enabled, the Agent generates a threat from the alert and applies a selected policy.

○ Suspicious Threat Policy ◉ Malicious Threat Policy

☑ Network Quarantine
If enabled, the system automatically quarantines the alerted endpoints.
You can reconnect the endpoints from the Sentinels page or Endpoint Details.

RULE DETAILS

Rule Name	[HMM] External IPs connections attempts to RDP or SSH
Description	외부 IP에서 RDP, SSH 접속 시도
Rule Severity	Low
Rule Type	Permanent
Expiration Date	N/A
Rule ID	1827447938224745773
Created by	jy.cheang@escare.co.kr
Created At	Nov 27, 2023 18:32:50

커스텀 탐지 룰

CONDITION — View In Deep Visibility

Scope Hierarchy	Account
Query Language	S1QL 1.0
Query Type	Events
Query	SrcIP RegExp "^((?!((^127\.)|(^10\.)|(^172\.1[6-9]\.)|(^172\.2[0-9]\.)|(^172\.3[0-1]\.)|(^150\.)|(^192\.168\.))).)*$" AN...show more

상세 탐지 내역

SOURCE PROCESS DETAILS — View Related Threat

Name	svchost.exe
Image Path	C:\Windows\System32\svchost.exe
User	NT AUTHORITY\NETWORK SERVICE
Start Time	Dec 6, 2023 12:33:39
Command Line	C:\Windows\System32\svchost.exe -k termsvcs
Integrity Level	system
Publisher	MICROSOFT WINDOWS PUBLISHER

NETWORK CONNECTION DETAILS

Source IP	45.119.210.146
Source Port	52859
Destination IP	172.17.102.226
Destination Port	3389
Direction	INCOMING

ENDPOINT DETAILS

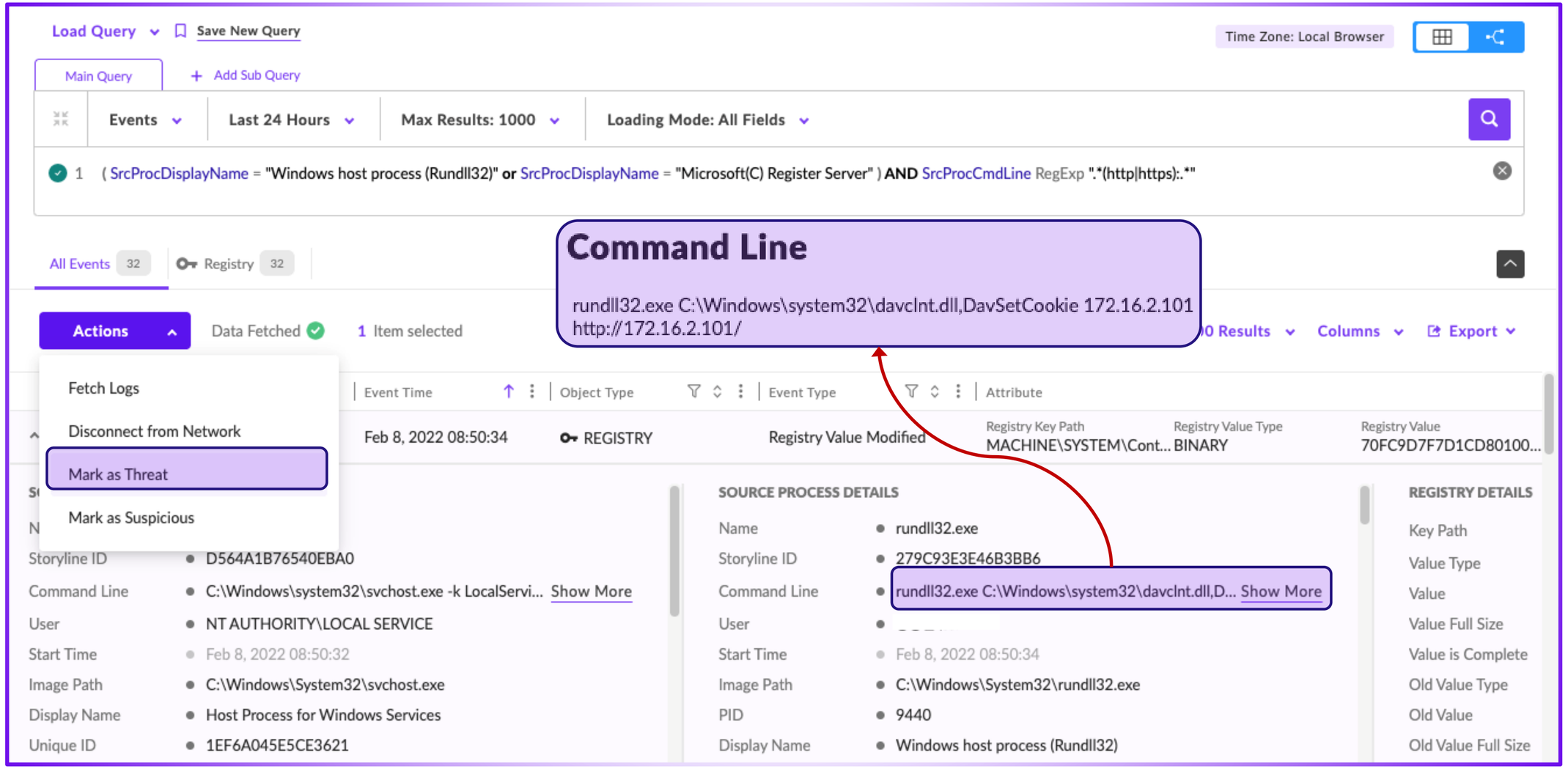
Endpoint Name	
Endpoint OS Type	windows
Endpoint OS Name	Windows Server 2016 Standard
Endpoint OS Revision	14393
Agent UUID	ef2e637df3144d94b1aa331ad0029085
Agent Version	23.2.3.358

CUSTOM RULE — View Custom Rule

Name	External IPs connections attempts to RDP or SSH
Description	외부 IP에서 RDP, SSH 접속 시도
Scope	account
Query Language	1.0
Query	SrcIP RegExp "^((?!((^127\.)|(^10\.)|(^172\.1[6-9]\.)|(^172\.2[0-9]\.)|(^172\.3[0-1]\.)|(^150\.)|(^192\.168\.))).)*$" AND DstPort In ("3389" , "22" ,

Mark as Threat

- EDR 헌팅을 통해 발견된 인시던트를 위협으로 정의, 기존에 탐지 하지 못한 위협으로 인한 시스템 피해 복원



EDR 통계 기반의 쿼리

Singularity Data Lake | ESCARE_TEST | Search | Dashboards | Star Custom Rules | Docs

```
src.process.storyline.id = "DBBA79713E605A46" src.process.cmdline = *
|filter src.process.parent.name != 'dllhost.exe' src.process.name != 'conhost.exe'
|columns timestamp, endpoint.name, src.process.parent.name,  src.process.name, src.process.cmdline
|sort timestamp
```

다양한 조건 기반의 쿼리

EDR | columns | dataset | filter | group | join | inner join | sql inner join | left join | sql left join | outer join | sql outer join | let | limit | lookup | parse | sort | transpose | union

204 rows returned

timestamp	Endpoint Name	Source Process Parent Name	Source Process Name	Source Process Command Line
Nov 8 · 2:29:18.847 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	"C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit …
Nov 8 · 2:29:18.856 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	"C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit …
Nov 8 · 2:29:20.049 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	/c vssadmin Delete Shadows /All /Quiet
Nov 8 · 2:29:20.063 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	/c vssadmin Delete Shadows /All /Quiet
Nov 8 · 2:29:20.166 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	"C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit …
Nov 8 · 2:29:20.223 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	/c bcdedit /set {default} recoveryenabled No
Nov 8 · 2:29:20.251 pm	VMware- OH (Windows10 - 2)	cmd.exe	vssadmin.exe	vssadmin delete shadows /all /quiet
Nov 8 · 2:29:20.302 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	/c bcdedit /set {default} recoveryenabled No
Nov 8 · 2:29:20.308 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	/c bcdedit /set {default} bootstatuspolicy ignoreallfailures
Nov 8 · 2:29:20.484 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	/c bcdedit /set {default} bootstatuspolicy ignoreallfailures
Nov 8 · 2:29:20.655 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	/c wmic SHADOWCOPY /nointeractive
Nov 8 · 2:29:20.882 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	/c wmic SHADOWCOPY /nointeractive
Nov 8 · 2:29:21.075 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	/c wevtutil cl security
Nov 8 · 2:29:21.210 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	/c wevtutil cl security
Nov 8 · 2:29:21.214 pm	VMware- OH (Windows10 - 2)	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049.exe	cmd.exe	/c wevtutil cl system

PowerQuery를 이용한 위협 탐지

- 통계 기반의 위협 탐지

PowerQuery | New | Load Query | Save New Query | Time Zone: Local Browser

Events | Last 48 Hours | Max Results: 1000

```
1  | join Outlook_Modified_File = (src.process.name contains "outlook.exe" and tgt.file.path contains "AppData\\Local\\Temp\\Olktmp" and tgt.file.extension = "png"
2  | columns src.process.name, src.process.storyline.id, endpoint.name, tgt.file.path, event.time), SMB_Traffic = (dst.port.number = "445" and src.process.image.path contains
   "C:\\Windows\\System32\\ntoskrnl.exe" and event.network.direction contains "OUTGOING" and !(dst.ip.address in ("0.0.0.0", "127.0.0.1")) and !(net_reserved(dst.ip.address))
3  | columns dst.port.number, src.ip.address , src.process.image.path, src.process.storyline.id, endpoint.name, tgt.file.path, dst.ip.address , event.time ) on endpoint.name
4  | let delta = Outlook_Modified_File.event.time - SMB_Traffic.event.time | filter (delta < 60000) and (delta >= 0)
```

Available Commands: columns | filter | group | inner join | join | left join | limit | sort | transpose | let

PowerQuery Fields

Endpoint.Name	Src.Process.Name	Outlook_Modified_File.Tgt.File.Path	Outlook_Modified_File.Src.Process.Storyline.Id	Src.Process.Image.Path	Src.Ip.Address	Dst.Ip.Address	Dst.Port.Number	SMB_Traffic.Src.Process.Storyline.Id
DESKTOP-E6JIPEM	OUTLOOK.EXE	C:\Users\hp\AppData\Local\Temp\Olktmp.png	289D32E5A6116D71	C:\Windows\System32\ntoskrnl.exe	19	19	445	91115D2BBAF68ED2
DESKTOP-E6JIPEM	OUTLOOK.EXE	C:\Users\hp\AppData\Local\Temp\Olktmp.png	289D32E5A6116D71	C:\Windows\System32\ntoskrnl.exe	19	19	445	91115D2BBAF68ED2
DESKTOP-BGP8VRL	OUTLOOK.EXE	C:\Users\E.K. Lee\AppData\Local\Temp\Olktmp56.png	402444D7749FCA60	C:\Windows\System32\ntoskrnl.exe	10.	19	445	F41830D7749FCA60
DESKTOP-BGP8VRL	OUTLOOK.EXE	C:\Users\E.K. Lee\AppData\Local\Temp\Olktmp56.png	402444D7749FCA60	C:\Windows\System32\ntoskrnl.exe	10.	19	445	F41830D7749FCA60

#CVE-2023-23397 (릴리스 날짜: 2023년 3월 14일)
Outlook 캘린더 내 약속을 알리는 '미리 알림'이라는 기능을 악용하여 NTLM 자격 증명을 탈취할 수 있는 취약점
사용자가 악의적으로 작성된 메일을 수신하는 경우, 공격자가 제어하는 SMB 서버(TCP 445)에 강제 인증하도록 하여 사용자의 정보(NTLM 해시)를 탈취

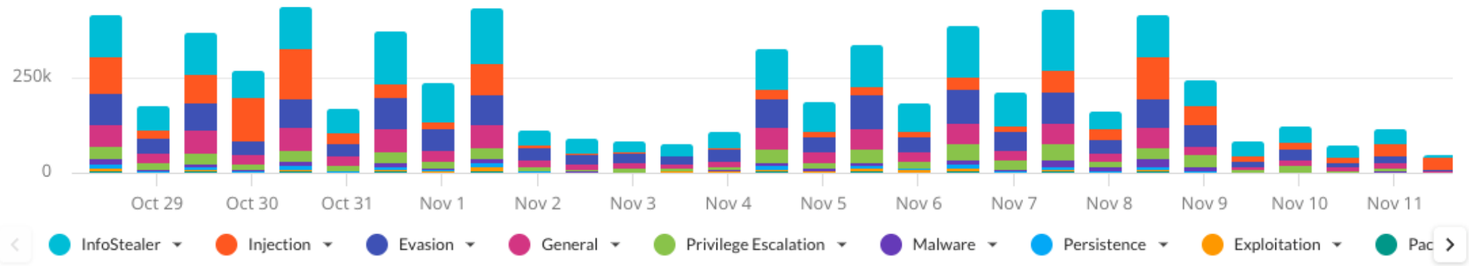
EDR 데이터 가시화

EDR Overview

Oct 28 · 8:33 am - Nov 11 · 8:33 am UTC+9

Endpoint Investigation | File & Registry Monitoring | User Investigation | Storyline Investigation | Behavioral Indicators By Category | Hunt

Indicator Breakdown



Privilege Escalation

Filter results

Technique	indicator.count
ProcessCreatedWithDifferentToken	516,49
Sudo	22,888
ManySPNRequests	12,163

Hiding/Stealthiness

Filter results

Technique	indicator.count
UnauthorizedLsaAccessRights	37,992

General

Filter results

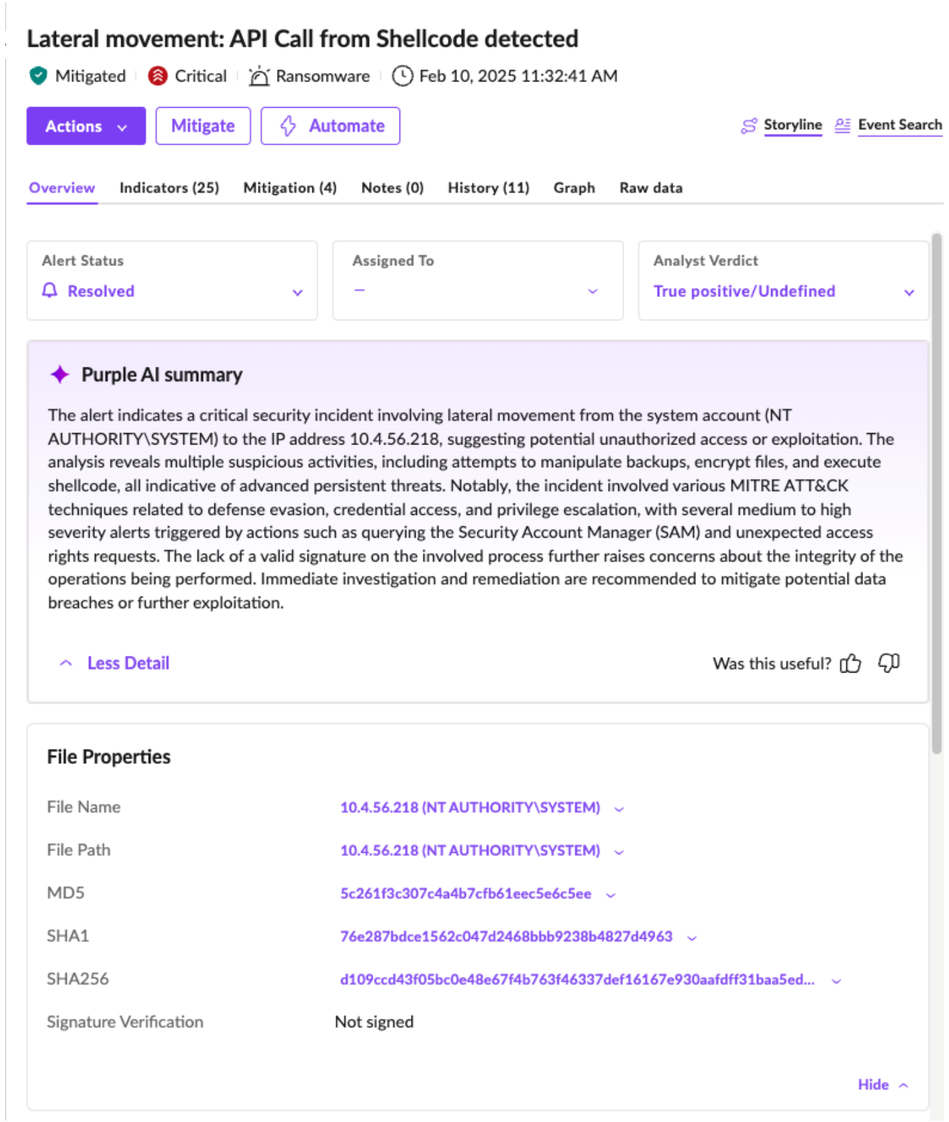
Technique	indicator.count
ServiceStopped	484,92
HookingViaSetHookAPI	407,22
ProcessStartedFromLnk	12,845
LogonProcessRegistered	9,434
DnsPoison	2,343

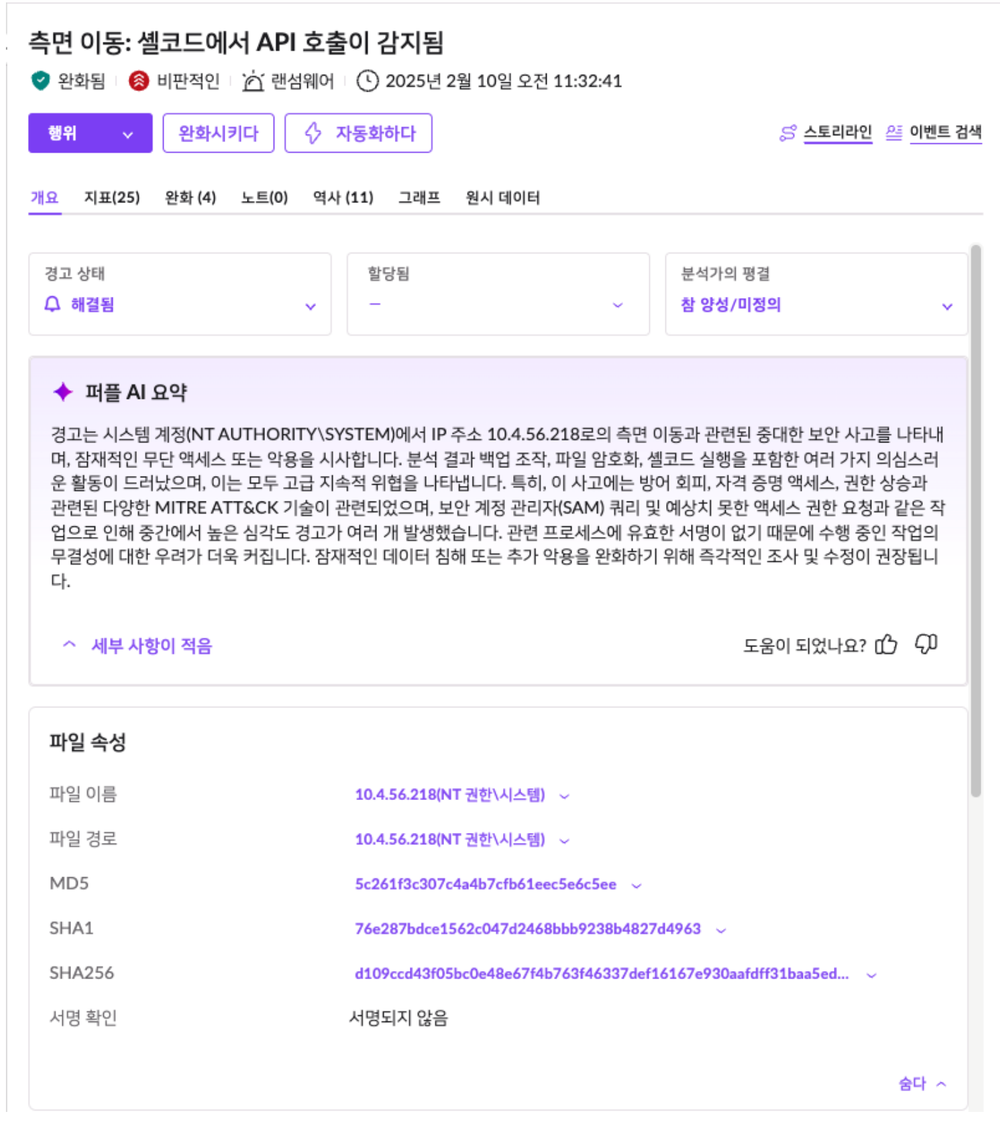
Malware

Filter results

Technique	indicator.count
CoreDllRead	145,71
SuspiciousRedirectionInterpreter	18,612
DirectSyscallAfterNtdllRead	5,604
SuspiciousRedirectionPipe	2,934
SuspiciousRedirectionHidden	1,247

Purple AI


Lateral movement: API Call from Shellcode detected
Mitigated
Critical
Ransomware
Feb 10, 2025 11:32:41 AM
Actions
Mitigate
Automate
Storyline
Event Search
Overview
Indicators (25)
Mitigation (4)
Notes (0)
History (11)
Graph
Raw data
Alert Status
Resolved
Assigned To
–
Analyst Verdict
True positive/Undefined
Purple AI summary
The alert indicates a critical security incident involving lateral movement from the system account (NT AUTHORITY\SYSTEM) to the IP address 10.4.56.218, suggesting potential unauthorized access or exploitation. The analysis reveals multiple suspicious activities, including attempts to manipulate backups, encrypt files, and execute shellcode, all indicative of advanced persistent threats. Notably, the incident involved various MITRE ATT&CK techniques related to defense evasion, credential access, and privilege escalation, with several medium to high severity alerts triggered by actions such as querying the Security Account Manager (SAM) and unexpected access rights requests. The lack of a valid signature on the involved process further raises concerns about the integrity of the operations being performed. Immediate investigation and remediation are recommended to mitigate potential data breaches or further exploitation.
Less Detail
Was this useful?
File Properties
File Name
10.4.56.218 (NT AUTHORITY\SYSTEM)
File Path
10.4.56.218 (NT AUTHORITY\SYSTEM)
MD5
5c261f3c307c4a4b7cfb61eec5e6c5ee
SHA1
76e287bdce1562c047d2468bbb9238b4827d4963
SHA256
d109ccd43f05bc0e48e67f4b763f46337def16167e930aafdff31baa5ed...
Signature Verification
Not signed
Hide


측면 이동: 셸코드에서 API 호출이 감지됨
완화됨
비판적인
랜섬웨어
2025년 2월 10일 오전 11:32:41
행위
완화시키다
자동화하다
스토리라인
이벤트 검색
개요
지표(25)
완화 (4)
노트(0)
역사 (11)
그래프
원시 데이터
경고 상태
해결됨
할당됨
–
분석가의 평결
참 양성/미정의
퍼플 AI 요약
경고는 시스템 계정(NT AUTHORITY\SYSTEM)에서 IP 주소 10.4.56.218로의 측면 이동과 관련된 중대한 보안 사고를 나타내며, 잠재적인 무단 액세스 또는 악용을 시사합니다. 분석 결과 백업 조작, 파일 암호화, 셸코드 실행을 포함한 여러 가지 의심스러운 활동이 드러났으며, 이는 모두 고급 지속적 위협을 나타냅니다. 특히, 이 사고에는 방어 회피, 자격 증명 액세스, 권한 상승과 관련된 다양한 MITRE ATT&CK 기술이 관련되었으며, 보안 계정 관리자(SAM) 쿼리 및 예상치 못한 액세스 권한 요청과 같은 작업으로 인해 중간에서 높은 심각도 경고가 여러 개 발생했습니다. 관련 프로세스에 유효한 서명이 없기 때문에 수행 중인 작업의 무결성에 대한 우려가 더욱 커집니다. 잠재적인 데이터 침해 또는 추가 악용을 완화하기 위해 즉각적인 조사 및 수정이 권장됩니다.
세부 사항이 적음
도움이 되었나요?
파일 속성
파일 이름
10.4.56.218(NT 권한\시스템)
파일 경로
10.4.56.218(NT 권한\시스템)
MD5
5c261f3c307c4a4b7cfb61eec5e6c5ee
SHA1
76e287bdce1562c047d2468bbb9238b4827d4963
SHA256
d109ccd43f05bc0e48e67f4b763f46337def16167e930aafdff31baa5ed...
서명 확인
서명되지 않음
숨다

SentinelOne

영업 및 기술 문의
㈜ 세니즈
www.seniz.co.kr

배상일 이사
bae@seniz.co.kr
010-71335486

Thank you

SentinelOne

sentinelone.com