SentinelOne™

자율형 악성코드 차단 솔루션

(Endpoint Protection Detection & Response)

SentinelOne Korea

악성코드 공격 사례 및 레거시 백신 대비 우수성

SentinelOne™

악성 코드 공격 사례

악성코드의 진화 – 타겟화, 고도화 및 다양한 우회 기술 탑재

<사진설명: 2021년 사이버 위협 시그널 포스터>

https://www.kisa.or.kr/notice/press_View.jsp?mode=view&p_No=8&b_No=8&d_No=1978

- 국내 유통사 일부 매장 영업 중단사례
- 영국 의료 서비스 장애
- 독일 병원 IT서비스 운영 중지
- 일본 자동차 기업 세계 11곳 공장 서비스 마비

악성 코드 공격 사례 – Supply Chain Attack

특정 기관의 컴퓨팅 체계 개발 작업에 끼어들어 악성 코드나 해킹 도구를 미리 숨겨 둔 뒤 해를 끼치는 행위. 정상적이고 일상적인 컴퓨팅 체계 개발 작업에 숨어들기 때문에 피해 규모와 범위를 가늠하기 어렵다.
1991년 걸프전 발생 전 미국 국가안보국이 이라크에 수출하는 컴퓨터 프린터에 미리 심어 둔 악성코드를 가동해 이라크 군 지휘 통신망을 공격한 사례가 대표적

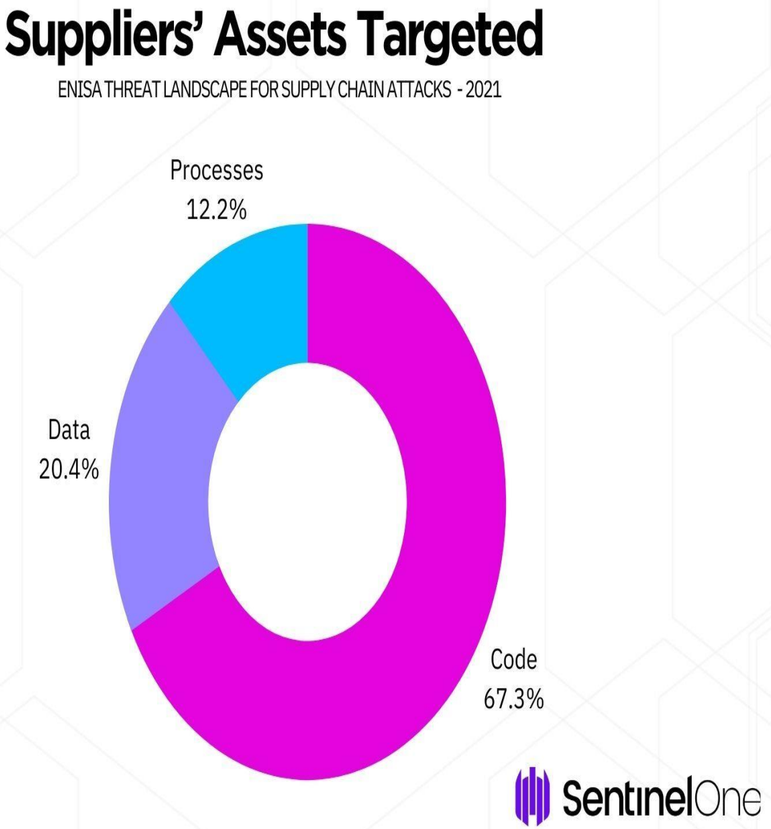
https://terms.naver.com/entry.nhn?docId=3586213&cid=59277&categoryId=59281

SentinelLabs, the research division of SentinelOne, has confirmed that devices with SentinelOne agents deployed were excluded from the SUNBURST attack from an early stage, even before any communication with a malicious C2. Technical analysis confirmed that SUNBURST was unable to disable or bypass SentinelOne in any environment.

"We're continuously monitoring and testing the latest SUNBURST variants to ensure our customers remain protected," said Raj Rajamani, Chief Product Officer, SentinelOne. "Unlike traditional antivirus and other next-gen products, SentinelOne's autonomous AI and robust anti-tampering protected our customers at the point of attack – without requiring any reactive product updates. Our customers have confidence knowing SentinelOne has them secured."

해외 Supply Chain 공격 사례

Attack	Suspected Goal	Potential Adversary	Supply Chain Attack Method
RSA - 2011	Military targets that leveraged RSA technology	APT based	Bypass authentication systems using RSA SecurID
CCleaner - 2017	Target a defined list of organisations by distributing ShadowPad malware.	APT based	Backdoored popular software app
NotPetya - 2017	Destruction of Ukrainian financial organisations endpoint infrastructure	APT based	Backdoored update mechanism to legitimate MeDoc financial software
ASUS - 2019	Consumers and businesses leveraging ASUS but targeted to a limited set of systems.	APT based (Widely discussed as related to CCleaner attackers)	Compromised digital certifications to sign updates to appear legitimate
SolarWinds - 2020	US Government related targets	APT based (reported as threat group APT29).	Updates to the Orion platform and digitally signed.
Kaseya - 2021	Indiscriminate targets for financial gain via ransomware	REvil ransomware group	External breach of Kayesa VSA service which was used to push out ransomware via their update mechanism



https://www.sentinelone.com/blog/how-todays-supply-chain-attacks-are-changing-enterprise-security/

국내 Supply Chain 및 ATP 공격 사례

이니텍社의 CrossWebEX3 Non-ActiveX 제품에서 발생하는 오버플로우 취약점 … 검증이 미흡한 함수를 사용하여 발생하는 버퍼 오버플로우 취약점 (CVE-2020-7859)https://www.boho.or.kr/data/secInfoView.do?bulletin_writing_sequence=36104

정보보호 제품 이용한 북한발 해킹 또 발견 이니텍 인터넷뱅킹용 보안 솔루션 `이니세이프` 시리즈와 닉스테크 `세이프 PC` 사용 고객은 피해를 입지 않도록 주의해야 한다.https://m.etnews.com/20161130000395

[긴급] 국내 시장점유율 1위 지니언스의 NAC 제품, 권리자 권한 탈취 가능 취약점 발견https://m.boannews.com/html/detail.html?idx=99832

김수키(Kimsuky) 조직, 청와대 보안 이메일로 사칭한 APT 공격 수행https://www.estsecurity.com/enterprise/security-center/notice/view/9805?category-id=

통일부 사칭, 北 연계 APT공격 등장… '사이버 공격 주의 업무로 둔갑'
https://www.estsecurity.com/enterprise/security-center/notice/view/136354?category-id=

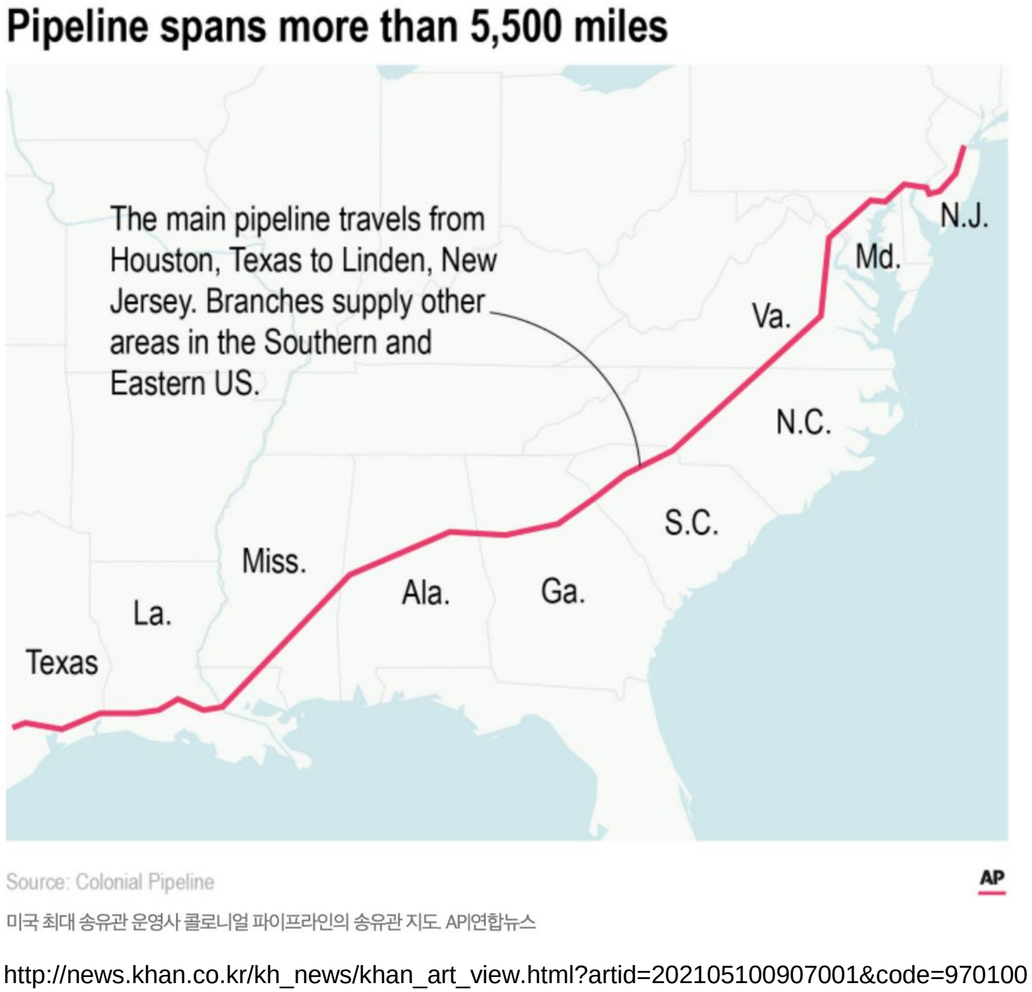
北 연계 사이버 위협 조직 탈륨, PDF 문서 취약점 이용한 공격 수행
https://www.estsecurity.com/enterprise/security-center/notice/view/123186?category-id=

이스트시큐리티, 北 해커 탈륨 추정 APT 공격 증가
http://it.chosun.com/site/data/html_dir/2021/08/03/2021080300854.html

Dark Side 공격 사례 – 미국 국가 비상사태 선포

미국 현지 시간 5월 9일, 미국 최대 유류 파이프라인 사업자인 Colonial Pipeline사 랜섬웨어 공격으로 가동 중단 사태 발생했으며, 국가 비상사태를 선포

BBC에 따르면, DarkSide 해킹 그룹으로 추정되는 집단으로부터 랜섬웨어 공격을 받아 송유관 기름 공급 차질 발생



미국 최대 송유관 운영사 콜로니얼 파이프라인의 송유관 지도. AP연합뉴스

http://news.khan.co.kr/kh_news/khan_art_view.html?artid=202105100907001&code=970100

SentinelOne 방어 기술

SentinelOne 기존 다른 보안 제품의 시그니처가 아닌 행위 기반 분석 AI 기술을 활용하여 사전 악성코드에 대한 사전 정보 없이 차단 가능

다양한 변종이 나올 것으로 예상되며, 새로운 변종에 대해서도 패턴 없이 차단 지원

미국 정보기관 및 대기업을 공격했던 Sunburst 역시 패턴 없이 사전 대응
https://www.sentinelone.com/press/all-sentinelone-customers-protected-from-solarwinds-sunburst-attack/

MITRE ATT&CK

T1112 Modify Registry

T1012 Query Registry

T1082 System Information Discovery

T1120 Peripheral Device Discovery

T1005 Data from Local System

T1486 Data Encrypted for Impact

T1543.003 Create or Modify System Process: Windows Service

T1490 Inhibit System Recovery

T1553.004 Subvert Trust Controls: Install Root Certificate

T1078 Valid Accounts

DarkSide 공격에 사용된 기법

기존 백신 프로그램의 한계

악성코드 실행 이력에 대한 가시성 부족

악성코드 탐지 전 수행한 실행 이력 및 변경사항에 대한 가시성 확보 불가

알려지지 않은 악성코드 탐지 불가

시그니처 기반의 한계로 알려 지지 않은 악성코드 탐지 불가,

시그니처 DB 증가로 인한 성능 이슈 발생

자동 치료 및 복구 기능 부재

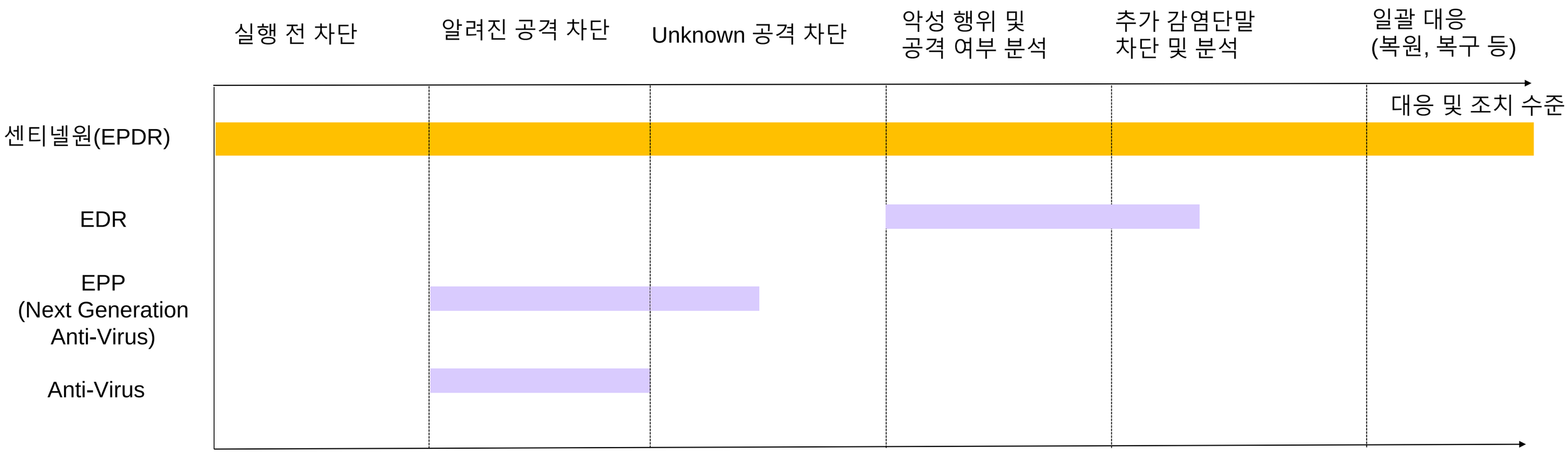
보안 전문가에 의한 수동 복구 또는 엔드 포인트 포맷 필요,

랜섬웨어 탐지 시 복구 불가

너무 많은 보안 기능 탑재로 인한 복잡성 증가

다양한 보안 기능을 탑재하여 복장성 증가 및 장애 시 분석 어려움

보안 솔루션 트렌드(EPP에서 EDR로)



Endpoint Protection Detection & Response
악성코드 탐지 + 차단 + 원격조치

SentinelOne 대응 기술

Storyline™

악성코드 시작부터 마지막까지 모든 과정을 분석할 수 있는 단일 식별자

ActiveEDR®

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

Rogue & Ranger®

사내 네트워크 상 에이전트 미설치 단말 및 IoT자산 식별/관리

Singularity™ XDR

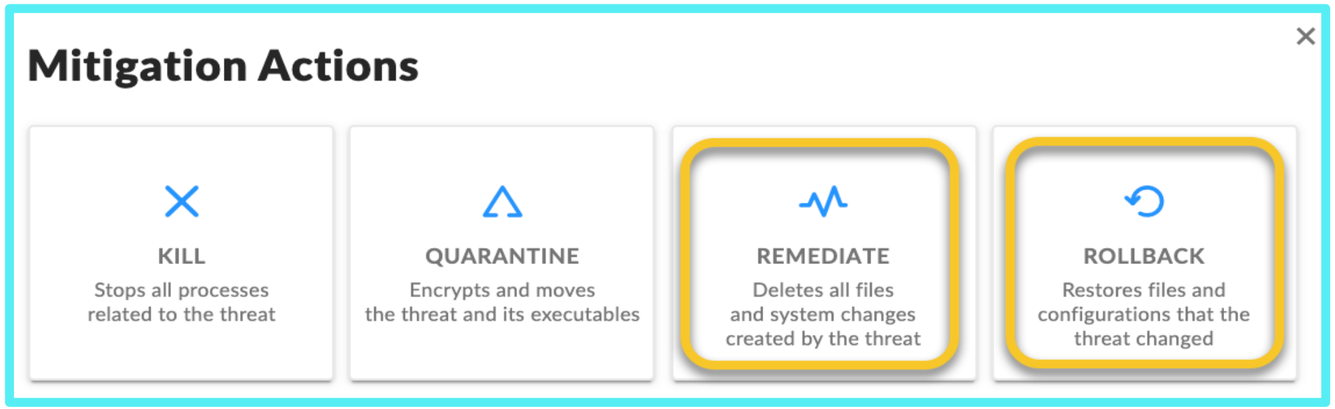
EPP + EDR 센티널원 제공하는 모든 기능을 단일 에이전트로 통합, XDR로 확장

1

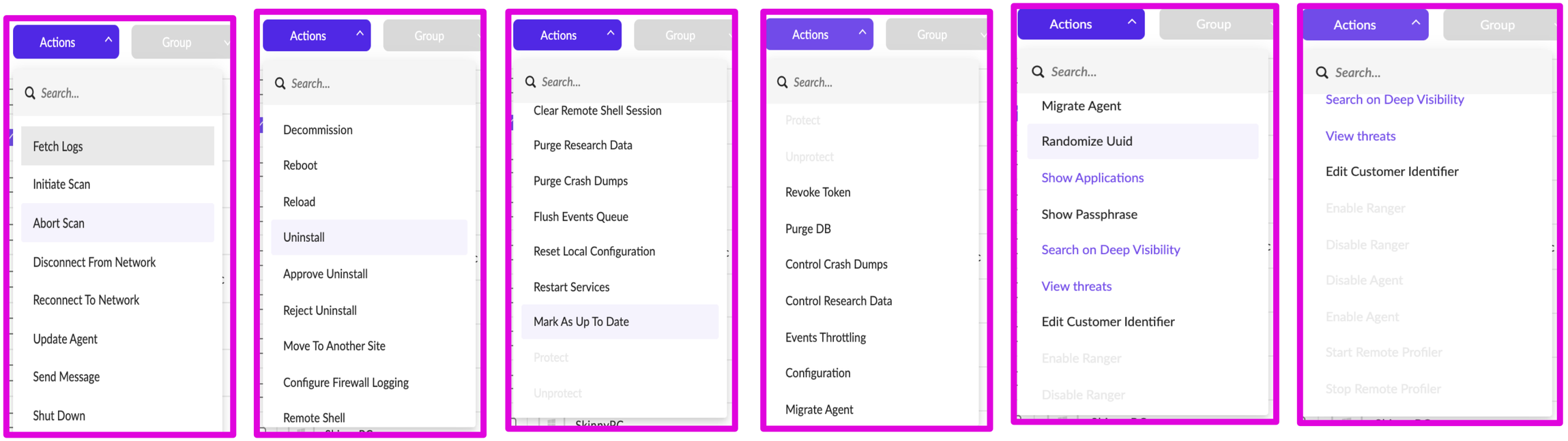
ONE Console

전세계 모든 지역에서 단일 콘솔로 통합 관리 제공

악성코드에 감염되어 PC 내 설정값, 레지스트리 및 파일 들이 암호화 되거나 변경/삭제된 경우 원래 상태로 복구하는 기술

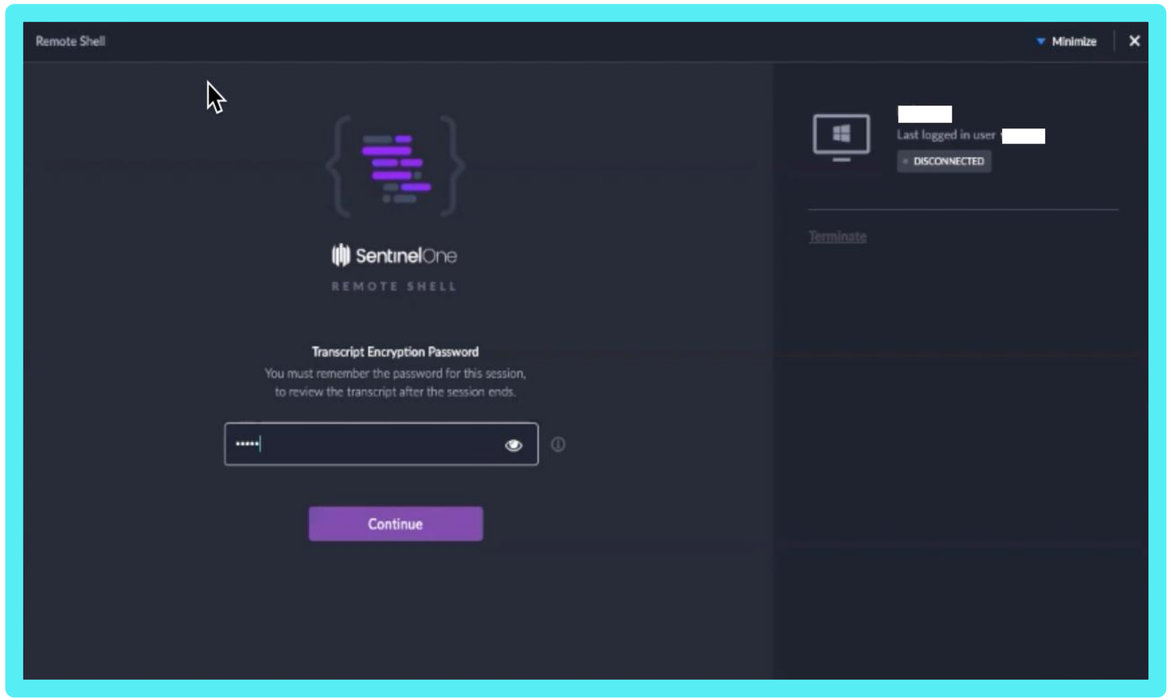


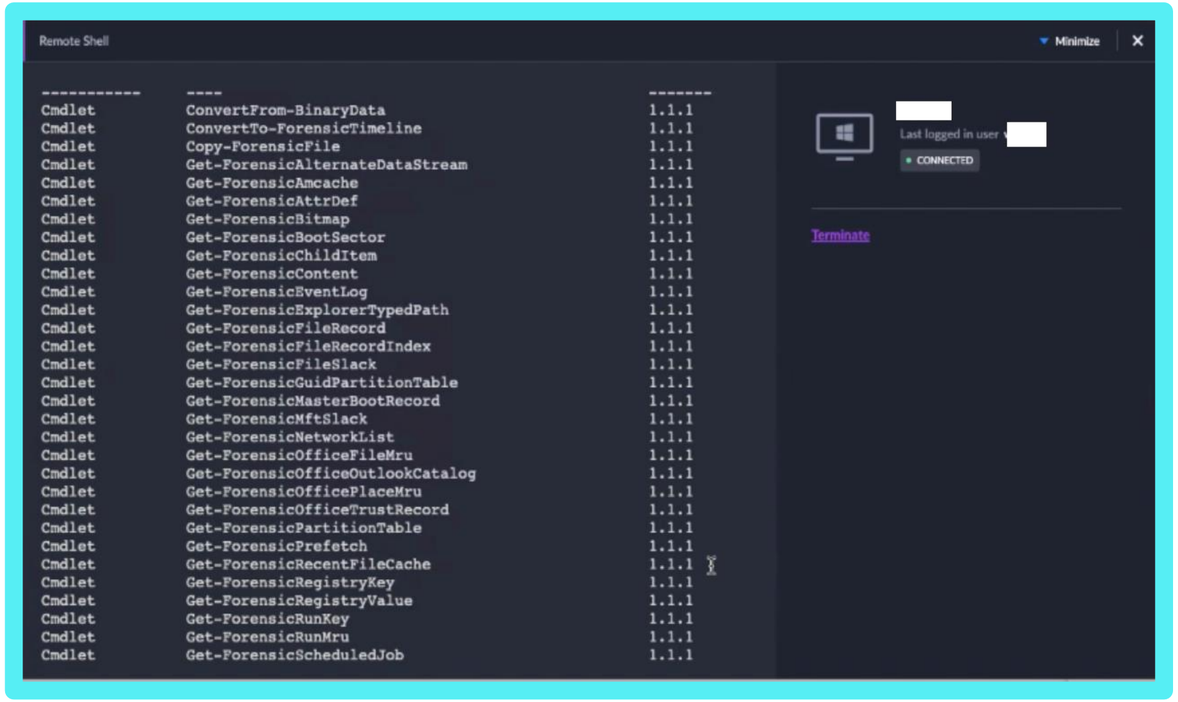
SentinelOne 에이전트 관리 기능



메세지 전송, 리부팅, 셧다운, 서비스 재시작, 로그 수집, 에이전트 업그레이드 등
다양한 기능 수행 – 엔드포인트 접속 없이 악성 행위 분석 지원

SentinelOne 에이전트 관리 기능





SentinelOne
탐지 기술

SentinelOne™

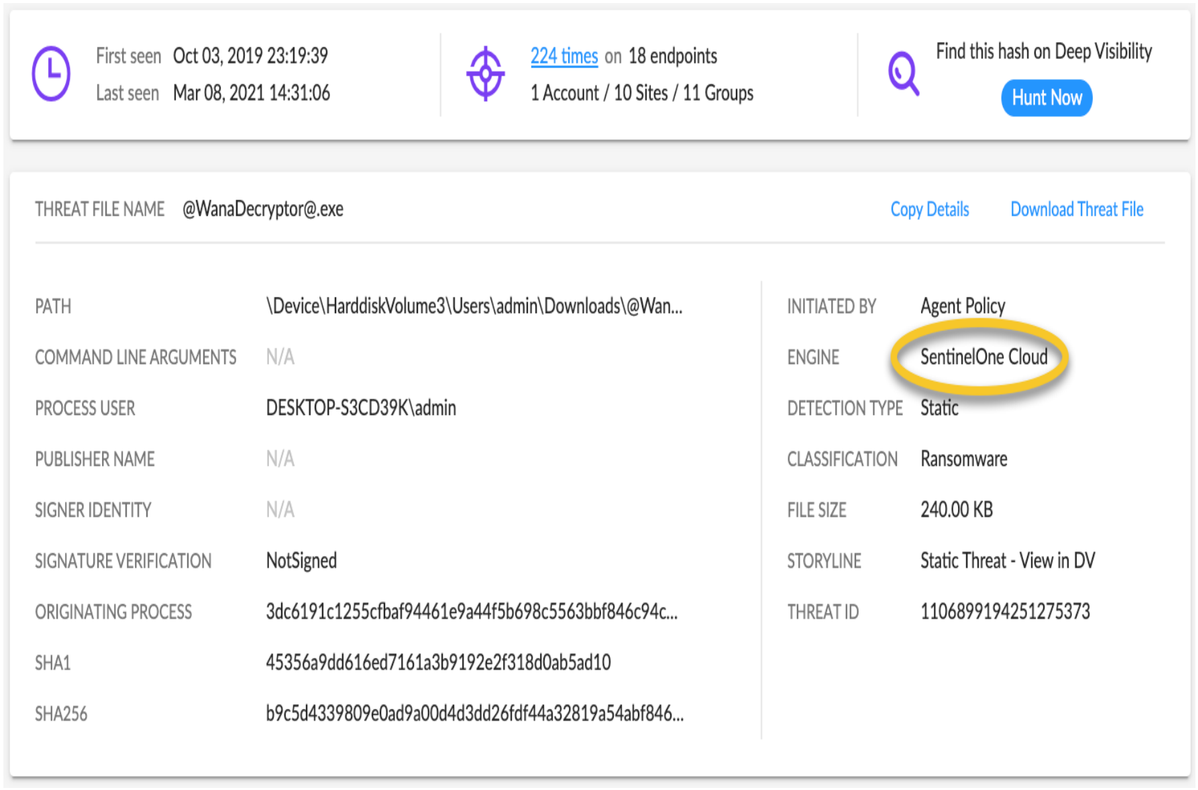
SentinelOne 탐지 엔진

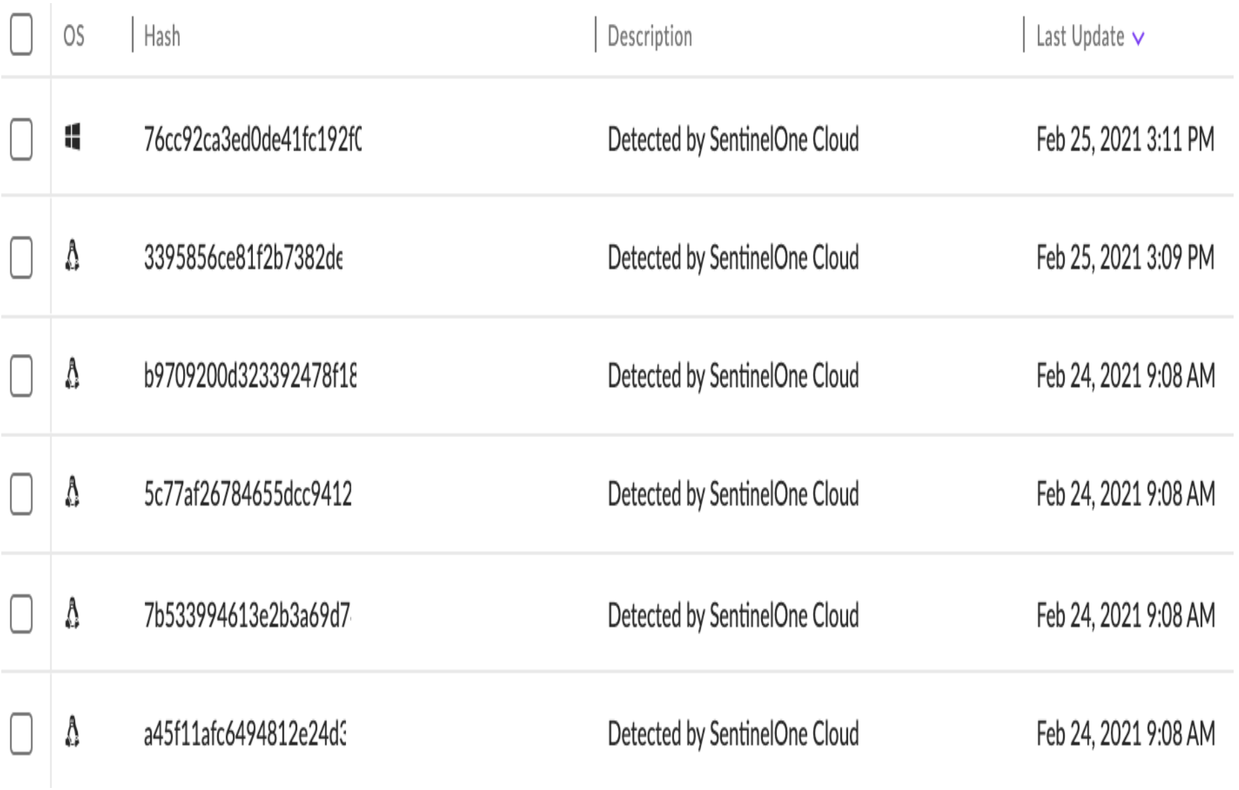
평판	Static AI	Behavioral AI	Deep Visibility
실행 전		실행 중	실행 후
해쉬값 기준 악성코드 차단 – OS별 최적화된 해쉬DB 제공 바이너리 볼트 – 고객사 엔드포인트 환경에서 확정자별, 폴드별 선별적 클라우드 업로드 및 분석	파일을 실행하지 않고 헤더기반 분석 헤더값 분석 후 AI기반 분석 수행 후 차단	파일 실행 후 행위기반 분석 – Mitre TTP기준 IoC 분석 정도 제공 시그니처 없이 악성 행위 기준 차단 패턴 업데이트 불필요	엔드포인트 내 모든 행위 로깅 – 프로세스, IP, 레지스트리, DNS, URL 등 14개 항목 정상 프로세스의 경우에도 IoC기준 행위 분석 및 Mitre TTP 제공

악성코드로 의해 변경된 설정값 및 암호화된 파일 복구

평판(Reputation Engine)

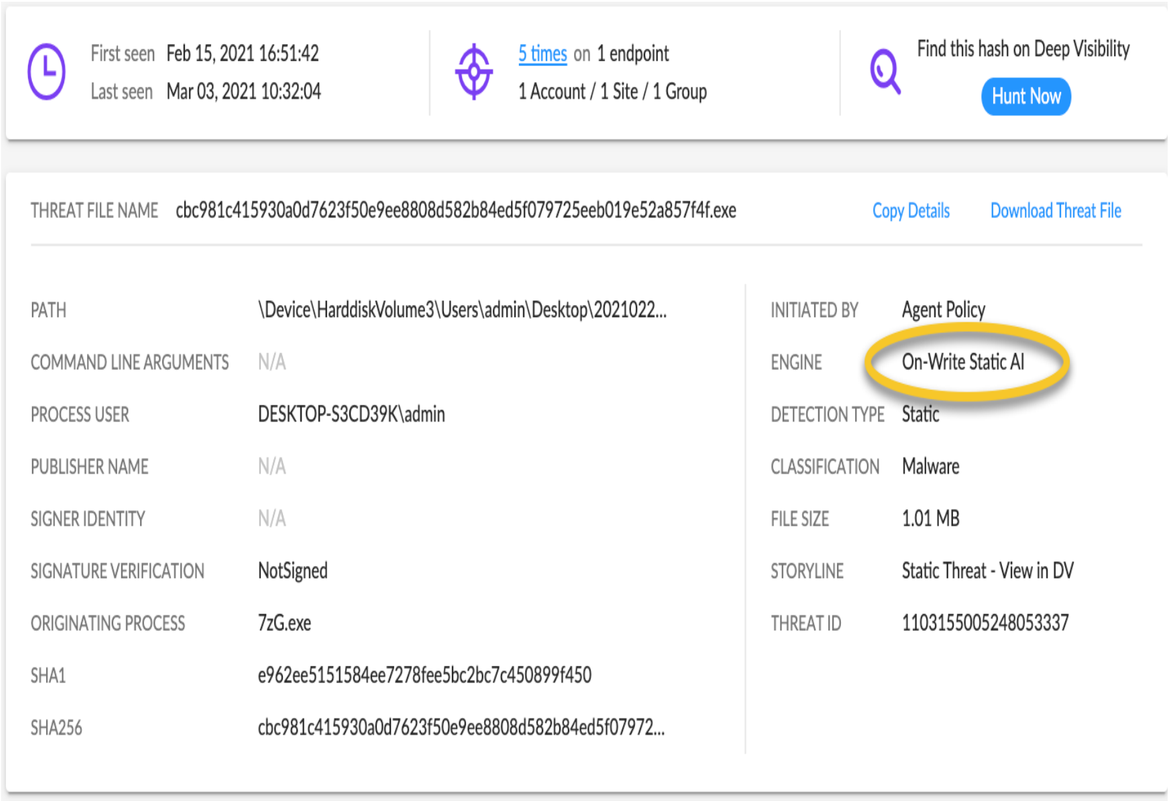
실행되는 파일의 해쉬값을 수집하여 SentinelOne 클라우드에서 비교하여 판단
OS별 각각의 해쉬 DB 운영
한번 실행된 악성코드의 해쉬 DB는 Blacklist에 유지

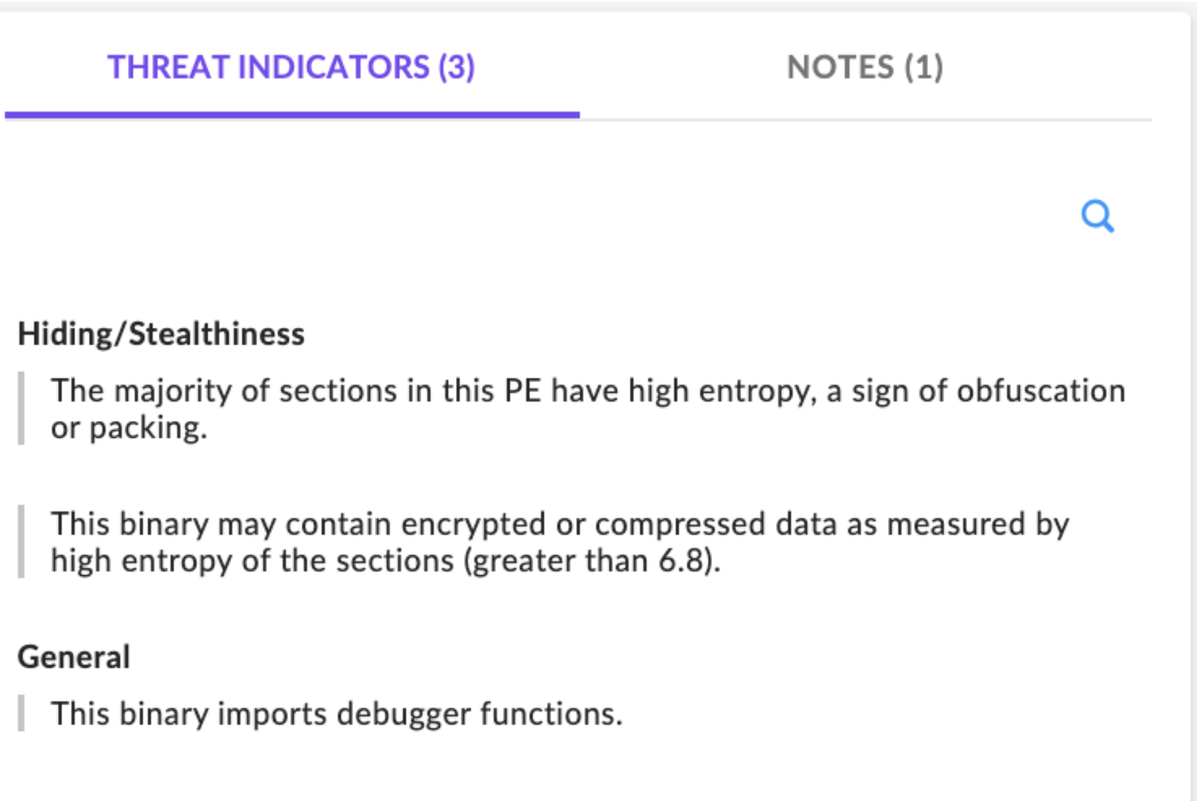




Static AI(Artificial Intelligence)

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





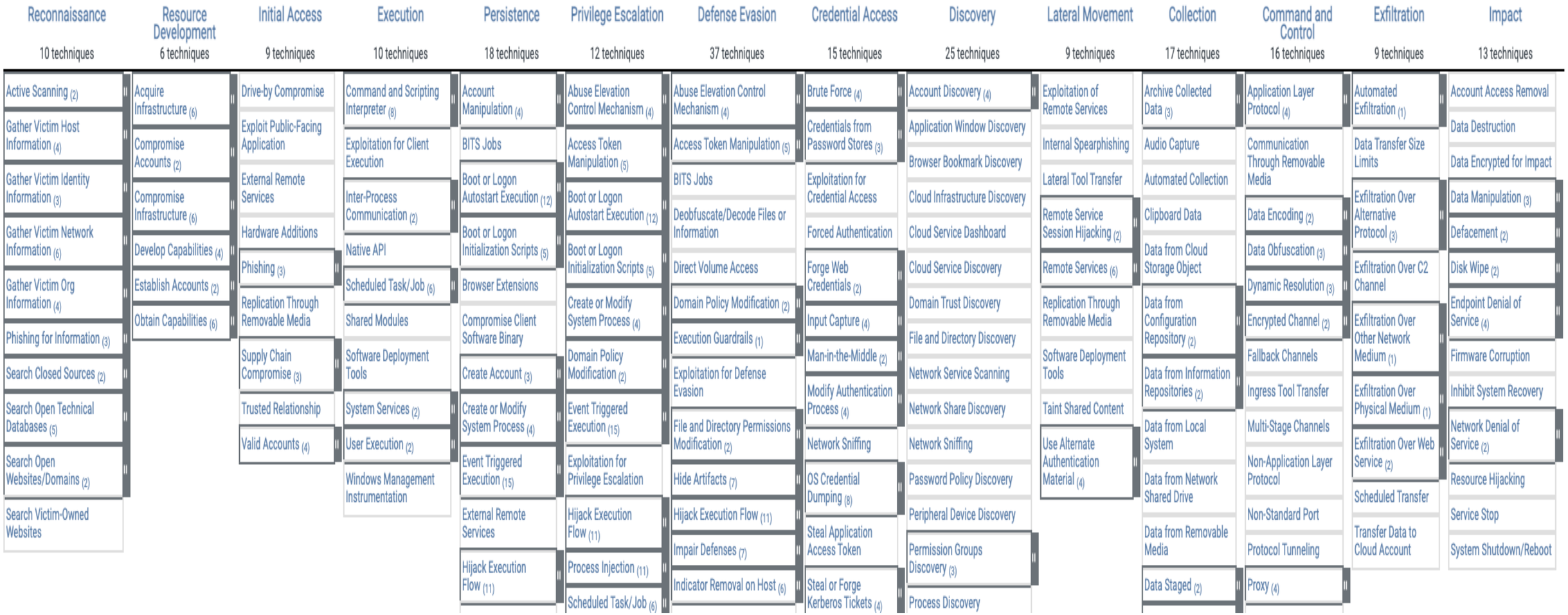
SentinelOne 행위 기반 탐지 엔진

❑ 모든 행위 기반 탐지 엔진의 경우 Mitre TTP기준 IoC정보 제공

구분	상세 내용
Reputation	해쉬값 기준 실행 파일 탐지 및 차단
Behavioral AI	파일이 실행하면서 수행하는 작업들을 분석하여 악성 여부 판단
Documents, Scripts	문서 파일에 특화된 행위 기반 탐지 엔진 문서 오픈 시 매크로 등 수행되는 행위 분석 및 탐지
Anti-Exploitation/Fileless	웹 또는 OS 취약점 기반 공격에 대한 행위 기반 분석 및 탐지
Application Control	컨테이너 기반 사전 정의된 응용 프로그램만 실행 가능
Manual	SentinelOne 분석팀 및 관제팀에서 수동으로 입력한 행위 또는 정보 기준 차단
Intrusion Detection	엔드포인트 내부 계정 권한을 획득하여 cmd, powershell 등을 통해 시도하는 공격 시도 탐지
Later Movement	네트워크 상의 다른 엔드포인트로 부터 시작된 공격 시도 탐지

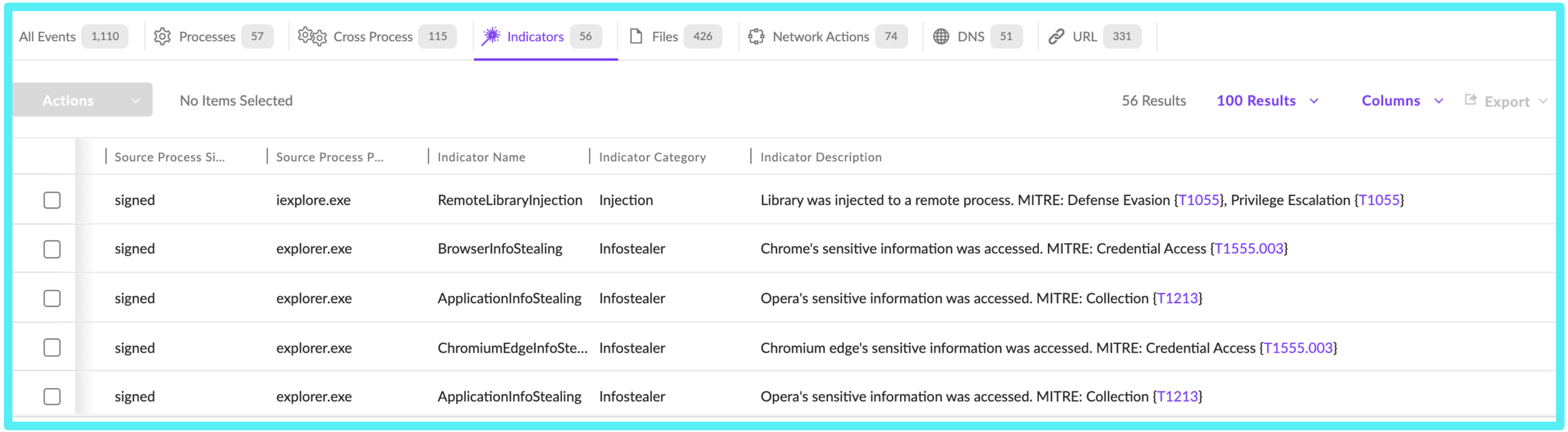
SentinelOne 행위 기반 탐지 엔진

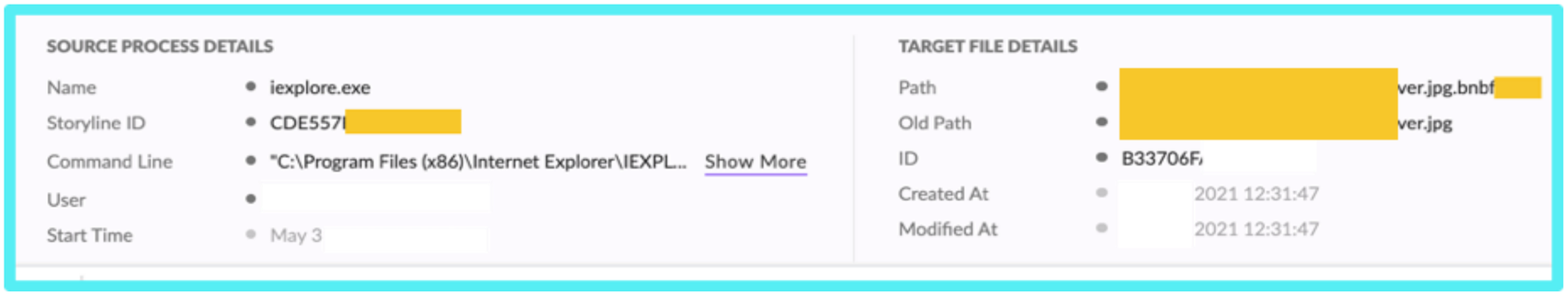
❑ 각 공격 기법별 상세 정보 제공 (Mitre TTP)



공격 사례 – Drive by download

브라우저 취약점을 악용한 공격 사례 – Exploit





파일 암호화 수행
추가 악성 코드 설치 없이
브라우저 기반 공격

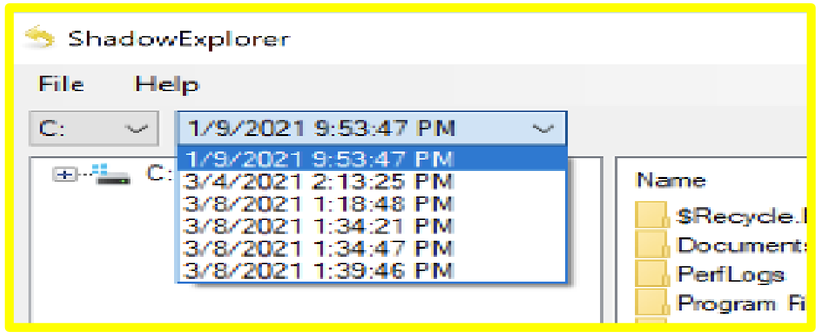
복구 기능

리부팅
(Shadow Copy 1 생성)

4시간 경과
(Shadow Copy2 생성)

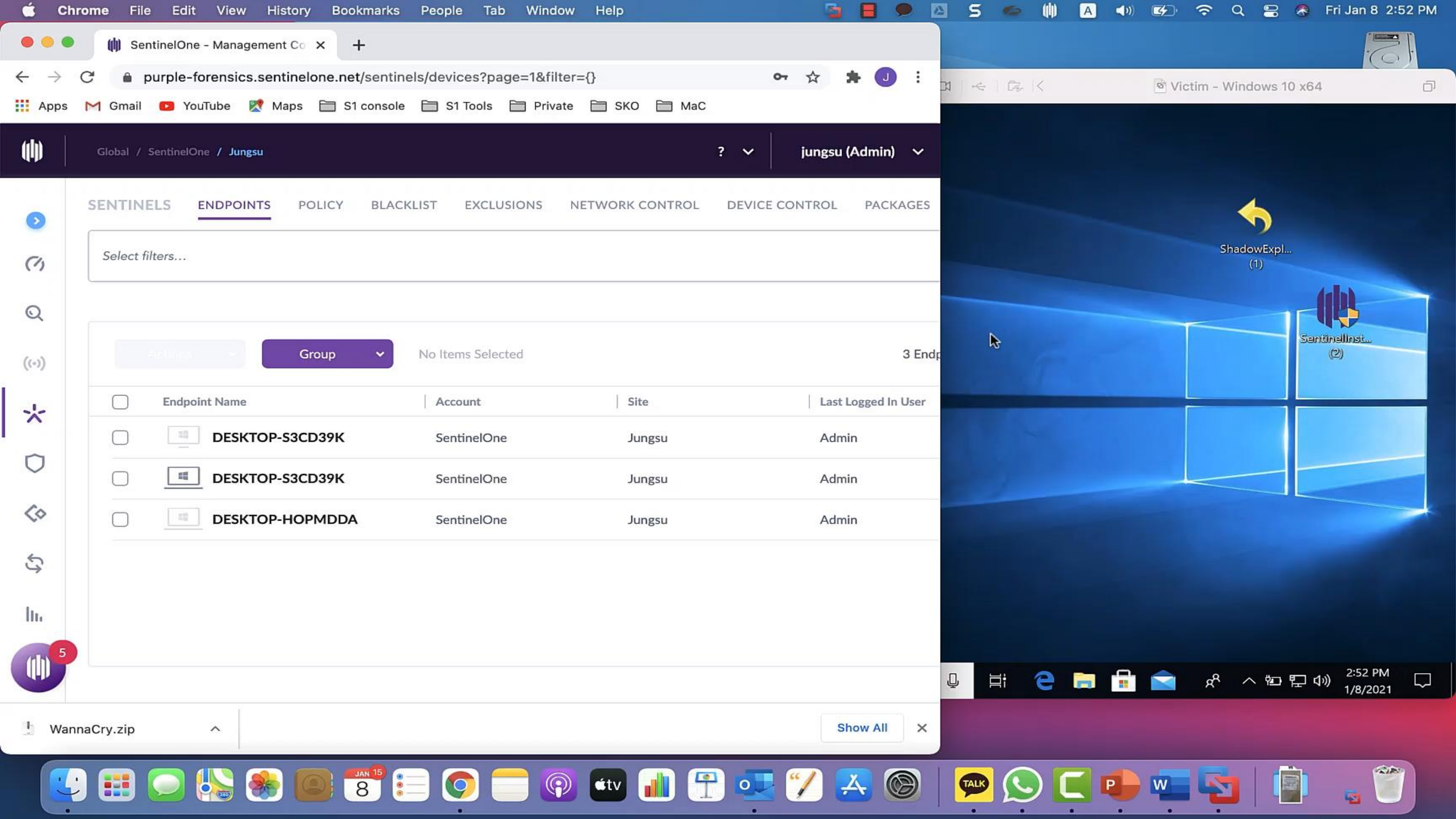
4시간 경과
(Shadow Copy3 생성)

악성코드 탐지
(롤백 수행, 악성코드가 변경한 값 복구)



Shadow Explorer를 이용한 시점 복구

VSS는 Microsoft 서비스로 변경된 파일에 대해 복구를 지원하는 기능

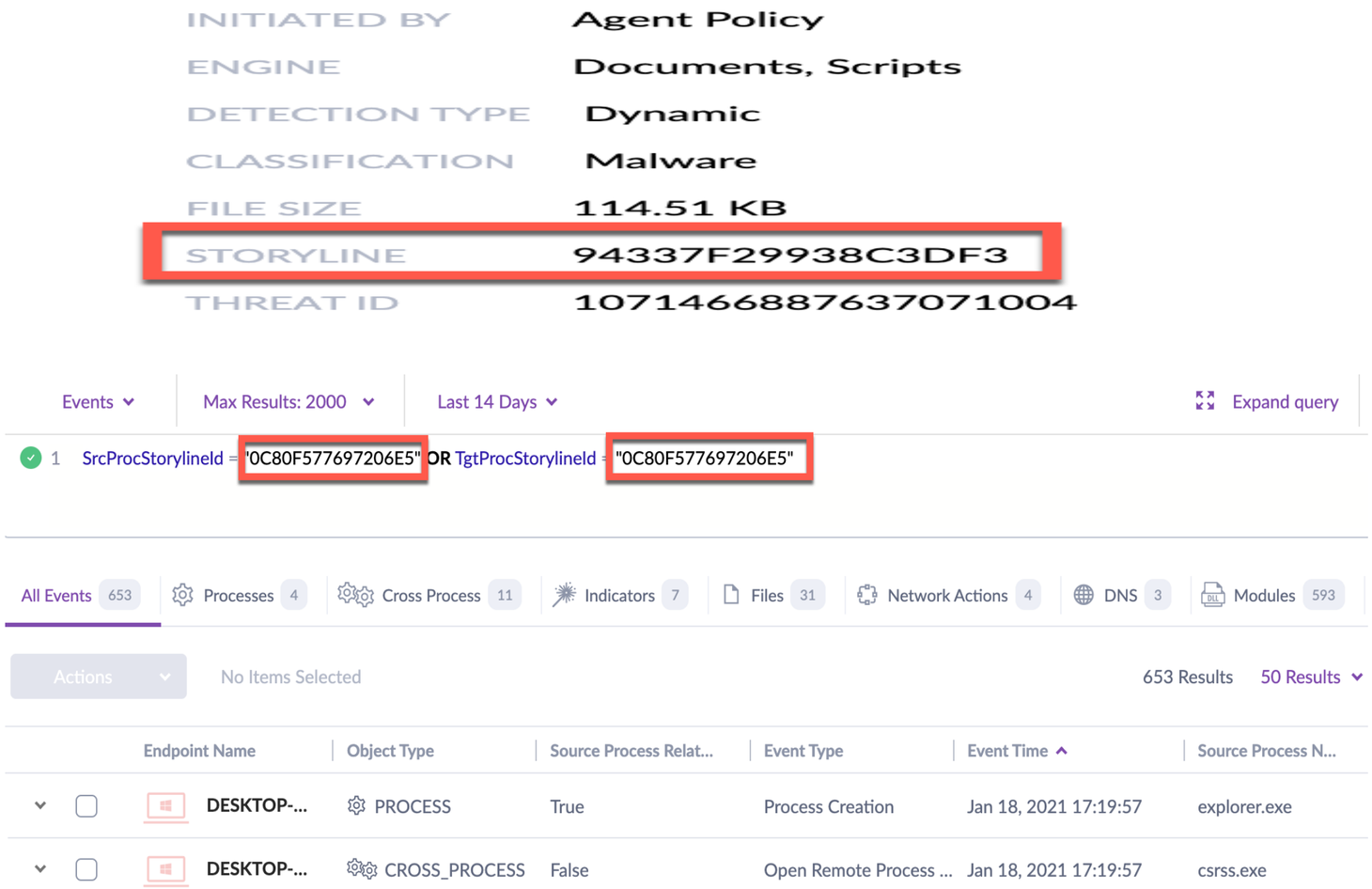

Chrome File Edit View History Bookmarks People Tab Window Help
Fri Jan 8 2:52 PM
SentinelOne - Management Co
purple-forensics.sentinelone.net/sentinels/devices?page=1&filter={}
Apps Gmail YouTube Maps S1 console S1 Tools Private SKO MaC
Global / SentinelOne / Jungsu
jungsu (Admin)
SENTINELS ENDPOINTS POLICY BLACKLIST EXCLUSIONS NETWORK CONTROL DEVICE CONTROL PACKAGES
Select filters...
Group
No Items Selected
3 Endp
Endpoint Name Account Site Last Logged In User
DESKTOP-S3CD39K SentinelOne Jungsu Admin
DESKTOP-S3CD39K SentinelOne Jungsu Admin
DESKTOP-HOPMDDA SentinelOne Jungsu Admin
WannaCry.zip
Show All
Victim - Windows 10 x64
ShadowExpl...
(1)
SentinelInst...
(2)
2:52 PM
1/8/2021

스토리라인이란?

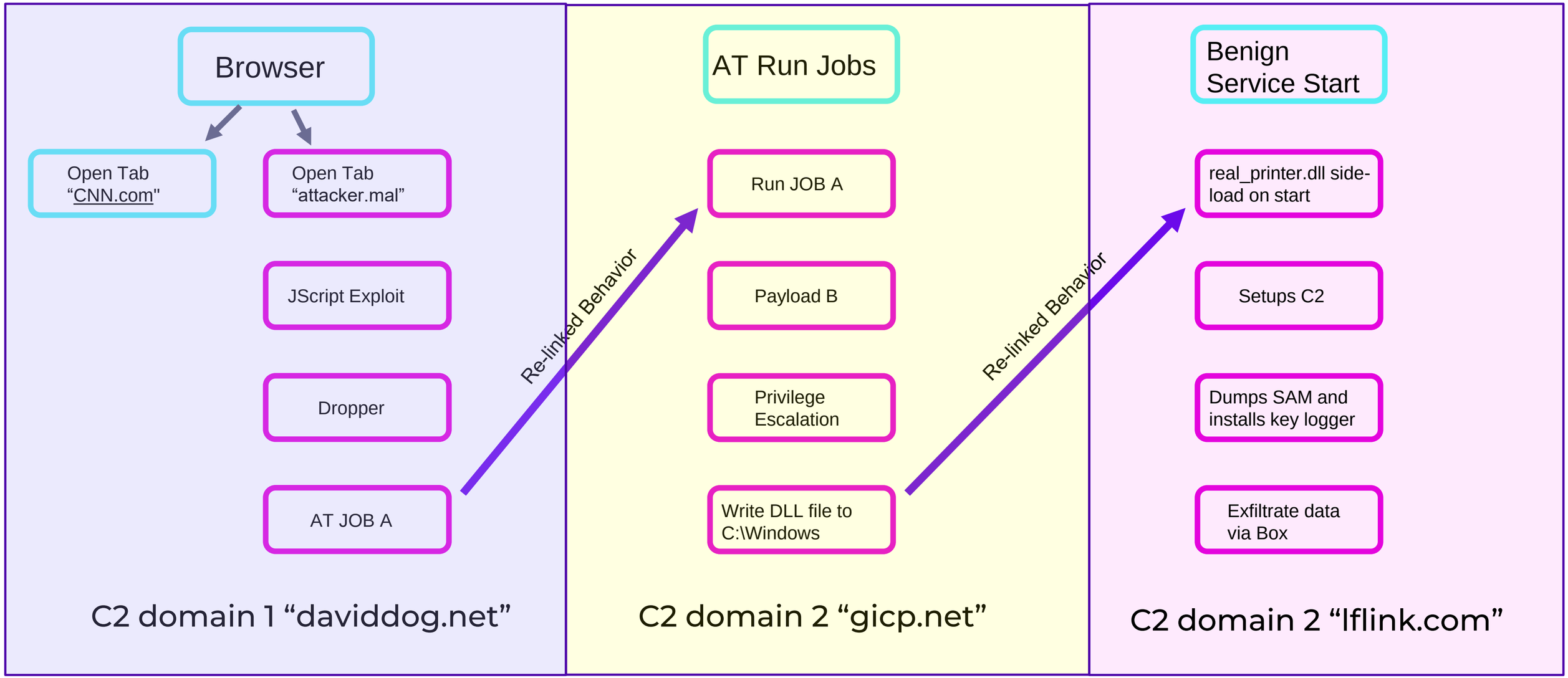
악성코드 공격 시작부터 끝까지
관련 모든 행위를 연관하여 분석할
수 있는 SentinelOne의 고유 기술

- 브라우저 악성코드 다운로드
- C&C 통신
- 추가 악성코드 다운로드
- 레지스트리 변경
- 백업본 삭제
- 파일 삭제 및 암호화

단일 악성 행위가 아닌 연관된 악성
행위를 통합 관리할 수 있는 기능



SentinelOne Agent Data - Context Relinking

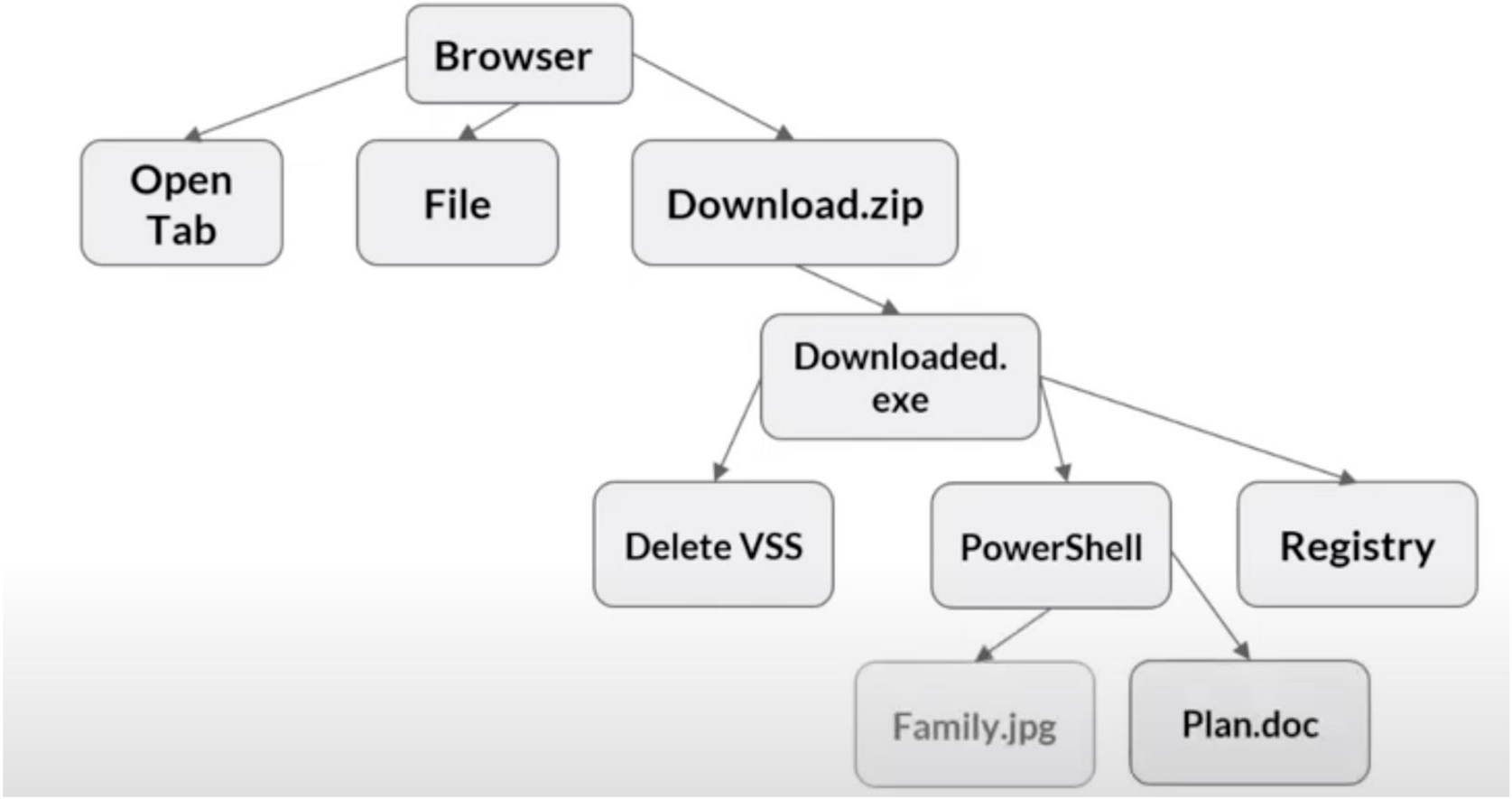


모든 활동은 Machine Learning 기반 StoryLine을 통해 Context 기반 탐지 지원

프로세스 동작 순서 및 연관관계 분석

PC 상에서 사용자가
실행하는 프로세스 기반
변경 사항 추적관리

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



Kali-Linux | Victim

root@kali: ~ 11:02:17 0%

root@kali: ~

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo su -
[sudo] password for kali:
┌──(Message from Kali developers)
│
│  We have kept /usr/bin/python pointing to Python 2 for backwards
│  compatibility. Learn how to change this and avoid this message:
│  ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└──(Run "touch ~/.hushlogin" to hide this message)
┌──(root💀kali)-[~]
└─# msfconsole
```

```
       =[ metasploit v6.0.30-dev                          ]
+ -- --=[ 2099 exploits - 1129 auxiliary - 357 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 >
```

침투 테스트 - StoryLine

Exploitation

Identified write action to LSASS process.
MITRE : Credential Access [T1098]

Remote shell was opened.
MITRE : Command and Control [T1071]

Shellcode execution was detected.
MITRE : Execution [T1106]

Execution of a metasploit stager.

Injection

Unusual code injection to a remote process.
MITRE : Defense Evasion [T1055]
MITRE : Privilege Escalation [T1055]

Code injection to a remote process.
MITRE : Defense Evasion [T1055]
MITRE : Privilege Escalation [T1055]

Code injection to other process memory space via Reflection.
MITRE : Defense Evasion [T1055]

Evasion

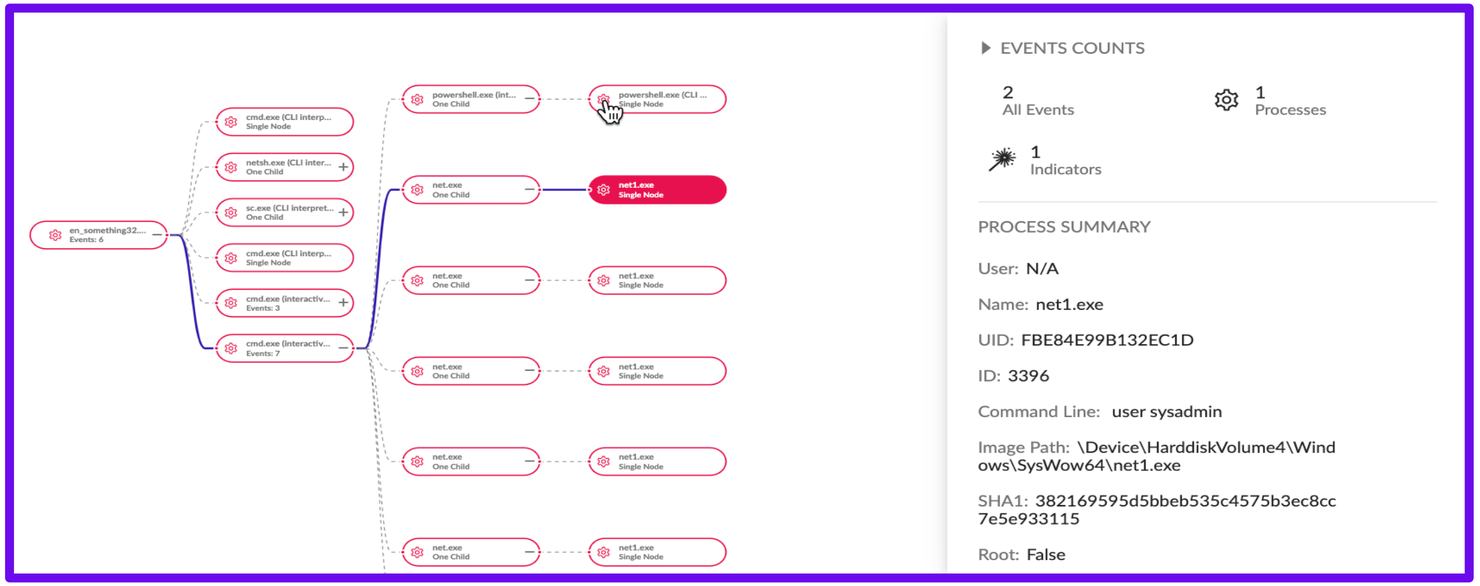
Application added firewall rules to allow network traffic.
MITRE : Exfiltration [T1041]
MITRE : Defense Evasion [T1562.004]

Indirect command was executed.
MITRE : Defense Evasion [T1202]

A file was created with an internal system name.
MITRE : Persistence

Persistence

Application registered itself to become persistent via service.
MITRE : Privilege Escalation [T1543.003]
MITRE : Persistence [T1543.003]



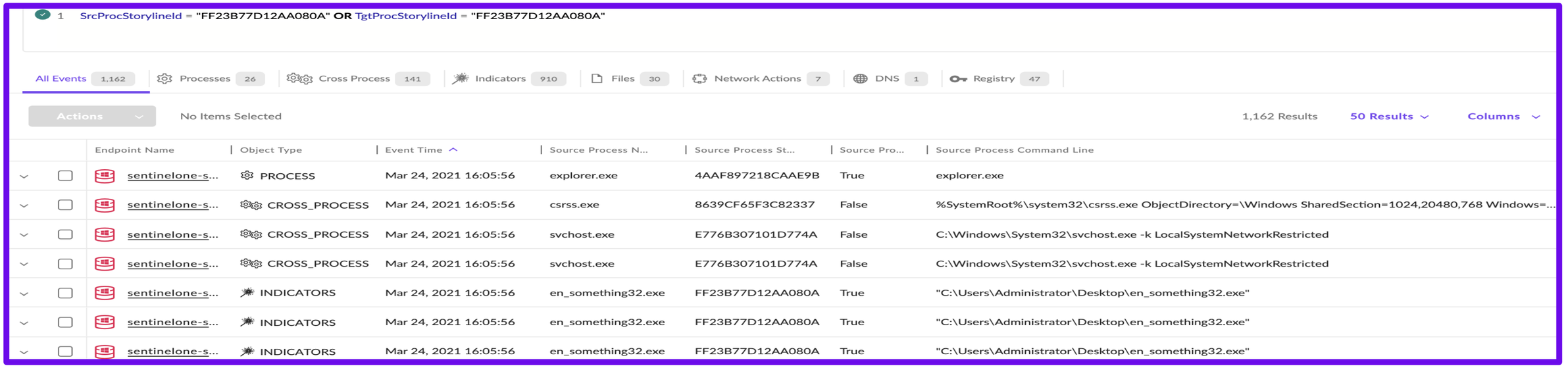
Events for en_something32.exe (5652) Clear Filter

All Events 12 | Files 2 | Network Actions 3 | Processes 7

12 Items 50 Result

Object Type	Event Type	Time	Attribute					
ip	IP Connect	Mar 24, 2021 16:05:56	Source IP 172.20.6.72	Source Port 49746	Destination IP 172.20.6.75	Destination Port 4444	Protocol tcp	Source Process Name en_something32.exe
process	Process Creation	Mar 24, 2021 16:06:12	Target Process Root False	Target Process Name en_something32.exe	Source Process Name N/A	Has Active Content N/A		
process	Process Creation	Mar 24, 2021 16:06:12	Target Process Root True	Target Process Name cmd.exe (interactive sessi...	Source Process Name en_something32.exe	Has Active Content N/A		
ip	IP Connect	Mar 24, 2021 17:12:32	Source IP 172.20.6.72	Source Port 49840	Destination IP 172.20.6.75	Destination Port 4444	Protocol tcp	Source Process Name en_something32.exe
process	Process Creation	Mar 24, 2021 17:12:47	Target Process Root True	Target Process Name cmd.exe (interactive sessi...	Source Process Name en_something32.exe	Has Active Content N/A		
ip	IP Connect	Mar 24, 2021 17:58:01	Source IP 172.20.6.72	Source Port 49857	Destination IP 172.20.6.75	Destination Port 4444	Protocol tcp	Source Process Name en_something32.exe

2. 침투 테스트



SOURCE PROCESS DETAILS

Name	en_something32.exe
Storyline ID	FF23B77D12AA080A
Command Line	"C:\Users\Administrator\Desktop\en_something32.exe"
User	SENTINELONE-SER\Administrator
Start Time	Mar 24, 2021 16:05:54
Image Path	C:\Users\Administrator\Desktop\en_something32.exe
PID	5652
Integrity Level	HIGH

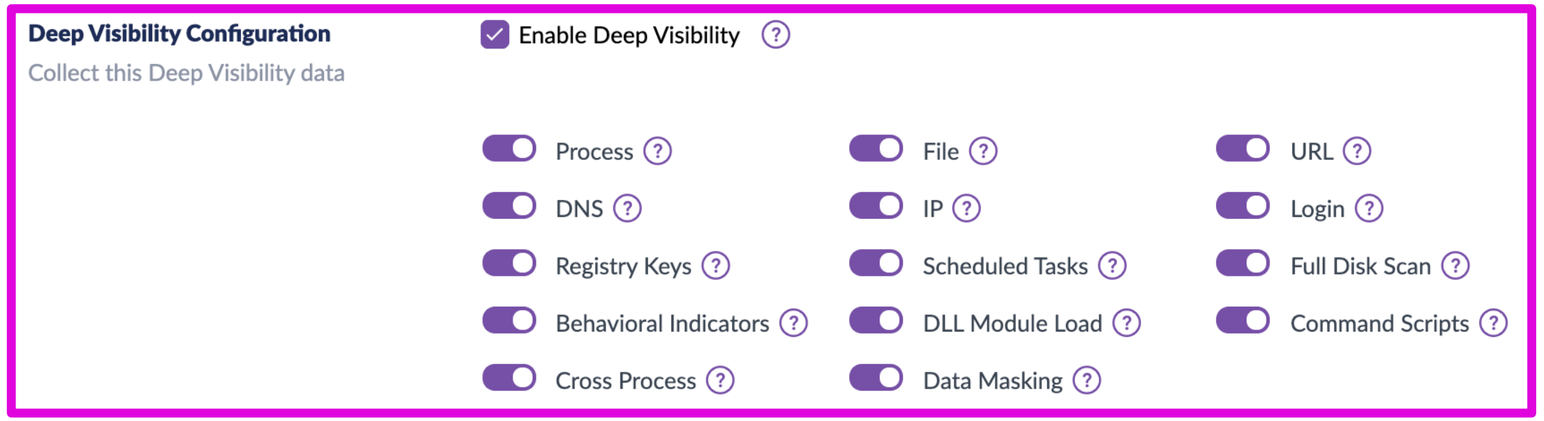
INDICATOR DETAILS

Name	SuspiciousShellcode
Category	Exploitation
Description	Shellcode execution was detected. MITRE: Execution {T1059, T1203} Show More

ENDPOINT DETAILS

Endpoint Name	sentinelone-server-client
Endpoint OS	windows
Agent UUID	9506e728b34e458cbe060ede625a5fcc
Endpoint Machine Type	server
Site Name	Default site
Site ID	1051279783026642145

S1 Complete EDR



엔드 포인트 내 발생하는 다양한 이벤트 로깅

```
1  -- Suspicious data compression
2  EventType = "Process Creation" and TgtProcCmdLine contains anycase "-hp" and TgtProcCmdLine regexp "\sa\s.*\s-hp[^\s]+\s" and TgtProcCmdLine regexp "\sa\s.*\s-m[0-5]+\s"
```

```
1  -- Allow SMB and RDP on Defender Firewall
2  (TgtProcName = "netsh.exe" AND TgtProcCmdLine ContainsCIS "remote desktop" AND TgtProcCmdLine ContainsCIS "enable=Yes") OR (TgtProcName = "netsh.exe" AND TgtProcCmdLine ContainsCIS "file and printer sharing" AND TgtProcCmdLine ContainsCIS "enable=Yes")
```

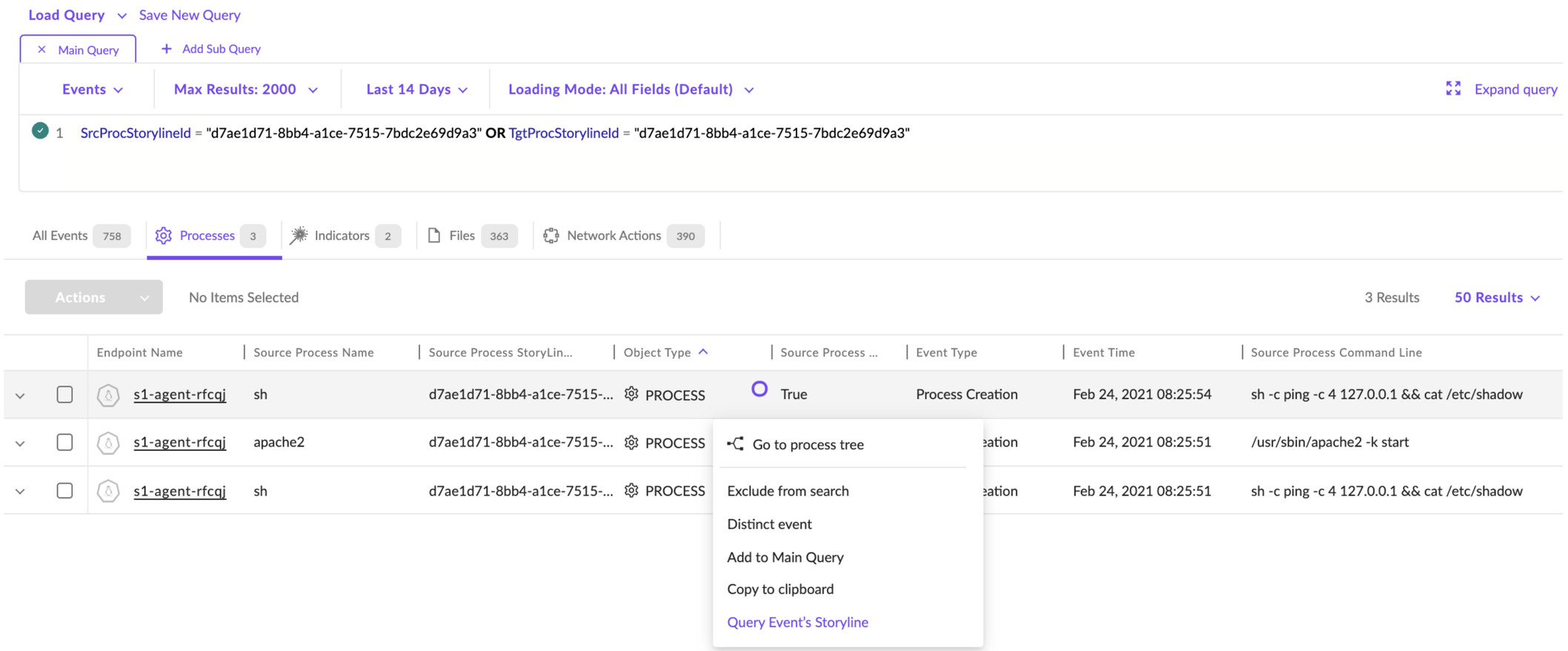
다양한 검색 조건을 통한 검색 지원

악성 행위 탐지 시

차단, 격리 등 대응 방안 지원

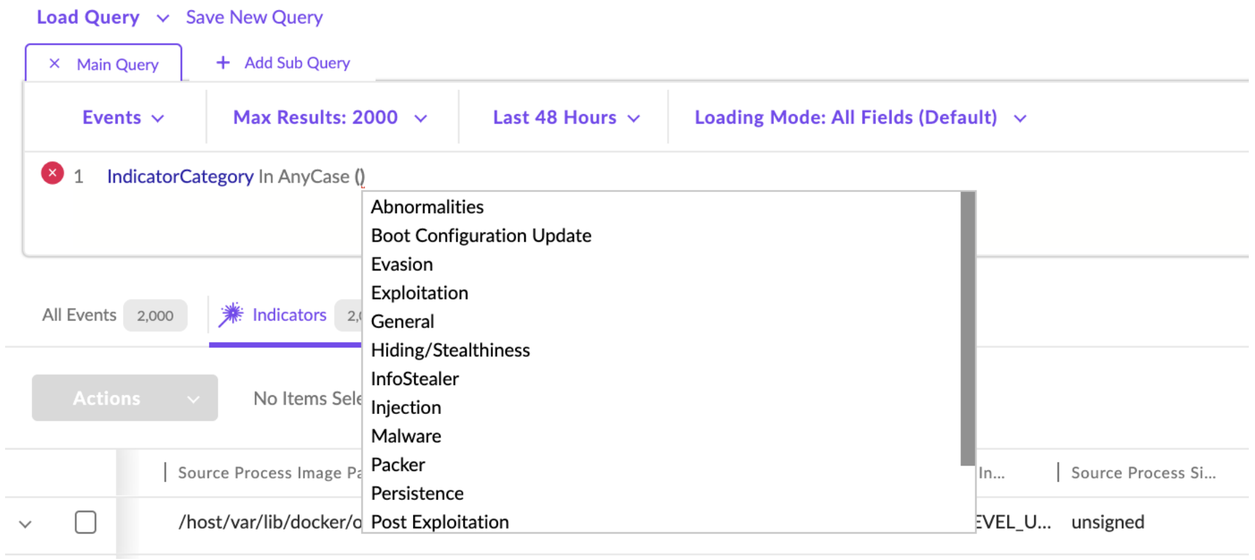
```
1  -- Rundll or Regsvr executes a script
2  (SrcProcDisplayName = "Windows host process (Rundll32)" or SrcProcDisplayName = "Microsoft(C) Register Server") AND SrcProcCmdLine RegExp ".*(javascript|mshtml|runhtmlapplication).*"
```

The Real Storyline & ActiveEDR



PC 내 Process, File, Registry, IP, URL, DLL loading 등 14개 항목 기준 로깅

The Real Storyline & ActiveEDR



악성 행위 기반 검색 지원
- PC 수행된 행위에 대해 분석 후 악성 행위일 경우 고유 식별자 부여 및 검색 지원

The Real Storyline & ActiveEDR

All Events 998 | Processes 402 | Indicators 5 | Files 72 | Network Actions 519

Actions | No Items Selected

ocess In...	Source Process Si...	Source Process P...	Source Process P...	Indicator Category	Indicator Description
TY_LEVEL_U...	unsigned	N/A	kube-proxy	Reconnaissance	Enumerated file system objects. MITRE: Discovery {T1083}
TY_LEVEL_U...	unsigned	N/A	bash	Reconnaissance	Enumerated file system objects. MITRE: Discovery {T1083}
TY_LEVEL_U...	unsigned	N/A	kubelet	Reconnaissance	Enumerated file system objects. MITRE: Discovery {T1083}
TY_LEVEL_U...	unsigned	N/A	bash	Reconnaissance	Enumerated file system objects. MITRE: Discovery {T1083}
TY_LEVEL_U...	unsigned	N/A	bash	Reconnaissance	Enumerated file system objects. MITRE: Discovery {T1083}

PC 내에서 수행된
행위에 대한 Mitre기준
Indicator정보 생성

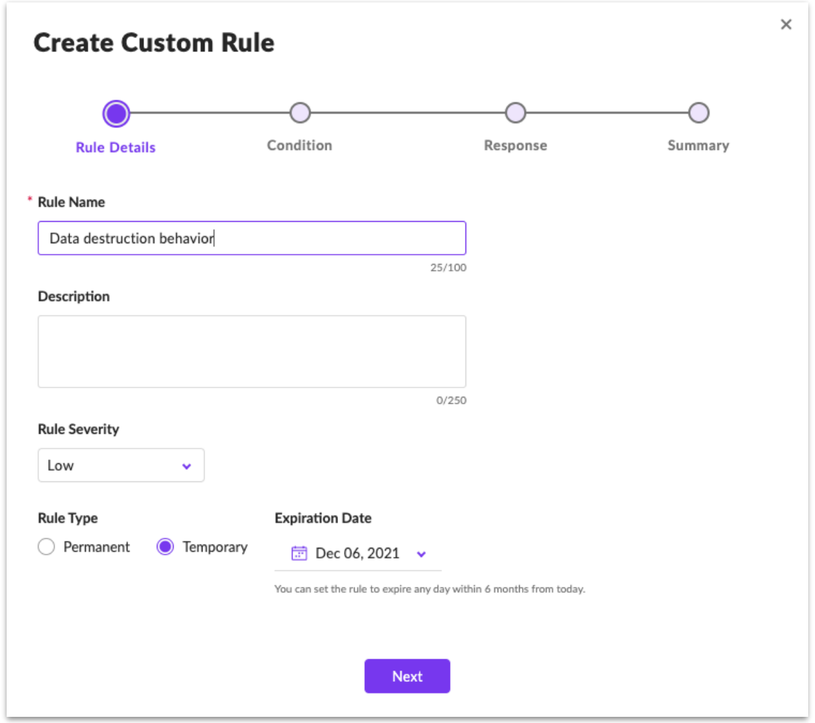
향후 해당 IoC 기준
검색 지원

rocess U...	Source Process In...	Source Process Si...	Source Process P...	Source Process P...	Indicator Name	Indicator Category	Indicator Description
:f-4a6c-486e-...	INTEGRITY_LEVEL_U...	unsigned	N/A	kube-proxy	FileAndDirectoryDiscovery	Reconnaissance	Enumerated file system objects. MITRE: Discovery {T1083}
.4-7d02-8835...	INTEGRITY_LEVEL_U...	unsigned	N/A	kube-proxy	FileAndDirectoryDiscovery	Reconnaissance	Enumerated file system objects. MITRE: Discovery {T1083}
'1-243d-f8b4-...	INTEGRITY_LEVEL_U...	unsigned	N/A	kube-proxy	FileAndDirectoryDiscovery	Reconnaissance	Enumerated file system objects. MITRE: Discovery {T1083}
0-630c-3946-...	INTEGRITY_LEVEL_U...	unsigned	N/A	kubelet	FileAndDirectoryDiscovery	Reconnaissance	Enumerated file system objects. MITRE: Discovery {T1083}
45-2f27-9c2b-...	INTEGRITY_LEVEL_U...	unsigned	N/A	kube-proxy	FileAndDirectoryDiscovery	Reconnaissance	Enumerated file system objects. MITRE: Discovery {T1083}
ea-cade-34b9-...	INTEGRITY_LEVEL_U...	unsigned	N/A	kubelet	FileAndDirectoryDiscovery	Reconnaissance	Enumerated file system objects. MITRE: Discovery {T1083}

STAR (StoryLine Active Response)

What is STAR?

STAR는 고객이 원하는 탐지룰을 생성하여 차단 뿐 아니라 자동화된 EDR 기능을 사용할 수 있는 기능



STAR 동작 방식

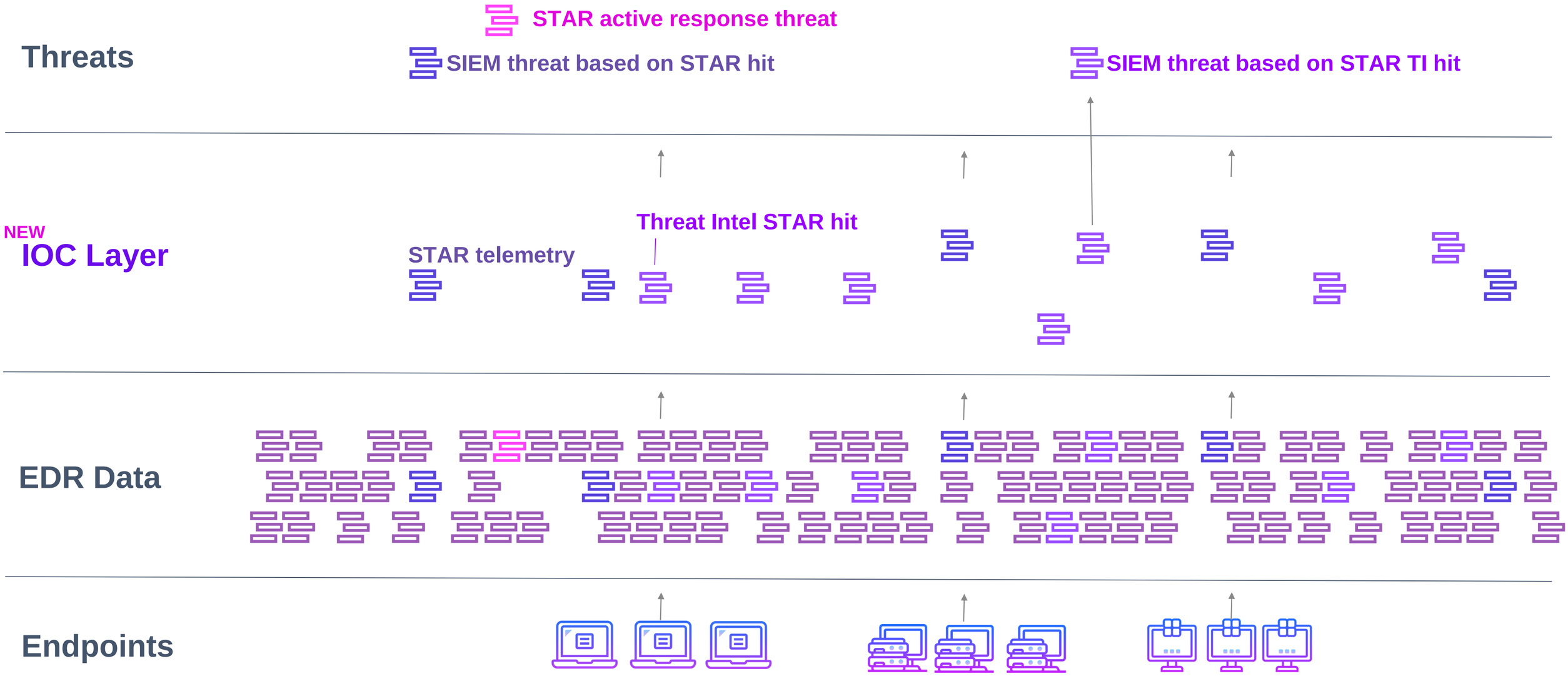
- 엔드포인트 상에서 지정된 행위에 대한 탐지 및 차단 룰셋 생성
- 에이전트 상에서 발생 이벤트 수신 시 바로 탐지
- 탐지, 위협 인지, 실시간 탐지/차단까지 모두 지원
- STAR 탐지 위협 및 이벤트는 GUI 및 syslog를 통해 전송 지원

STAR 경쟁 우위

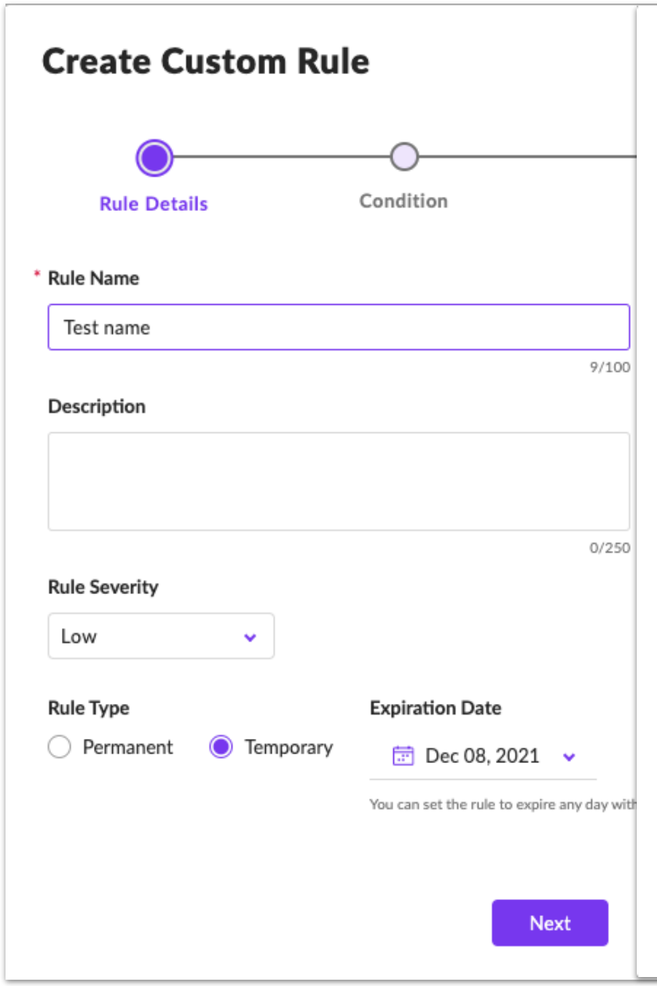
SentinelOne	Carbon Black	Crowdstrike
Near real-time hits	Runs every ten minutes	Runs periodically
Active response	Alert only	Alert only

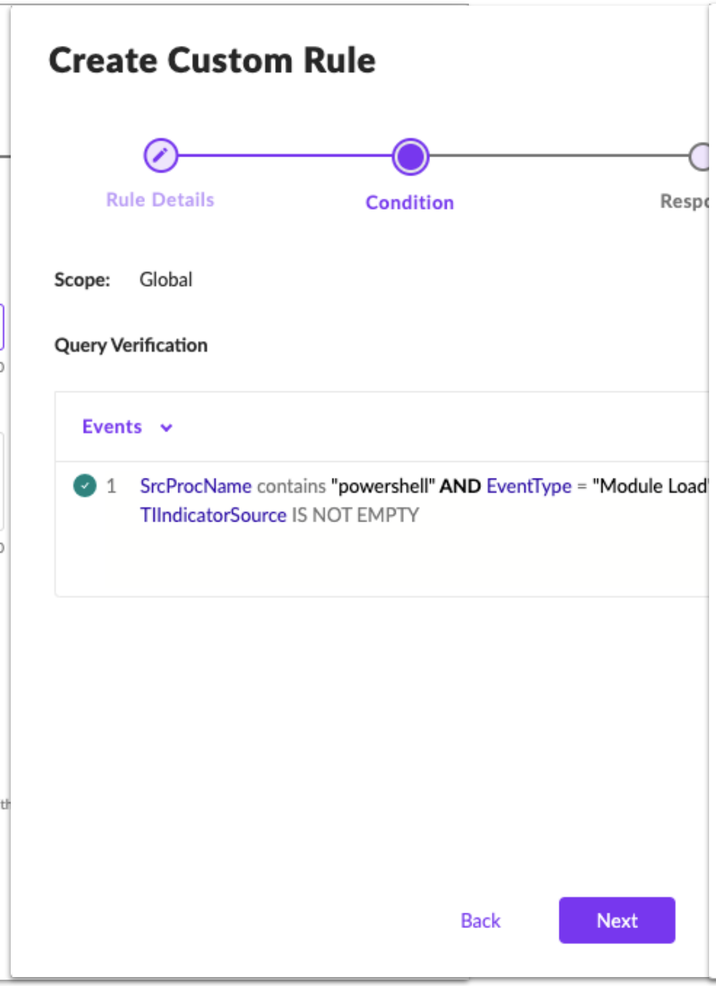
SentinelOne

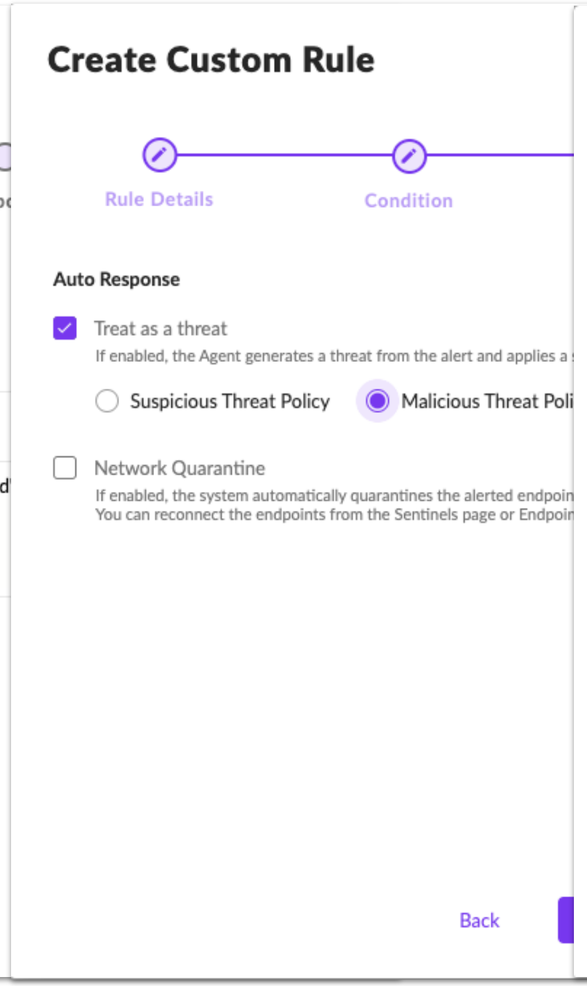
STAR 동작 레이버

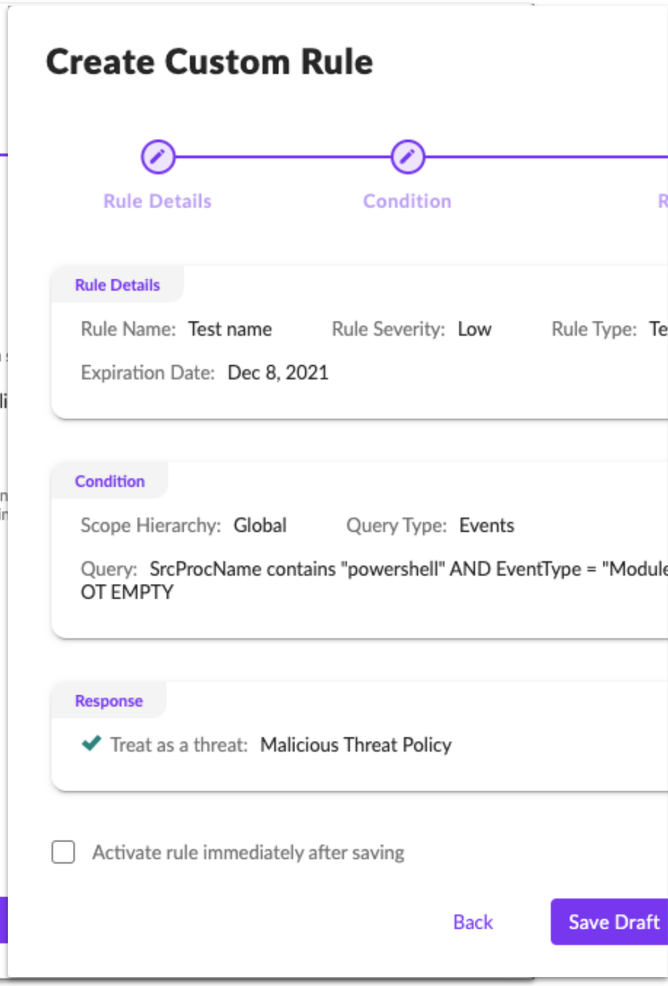


STAR Workflow: 룰 생성 방식









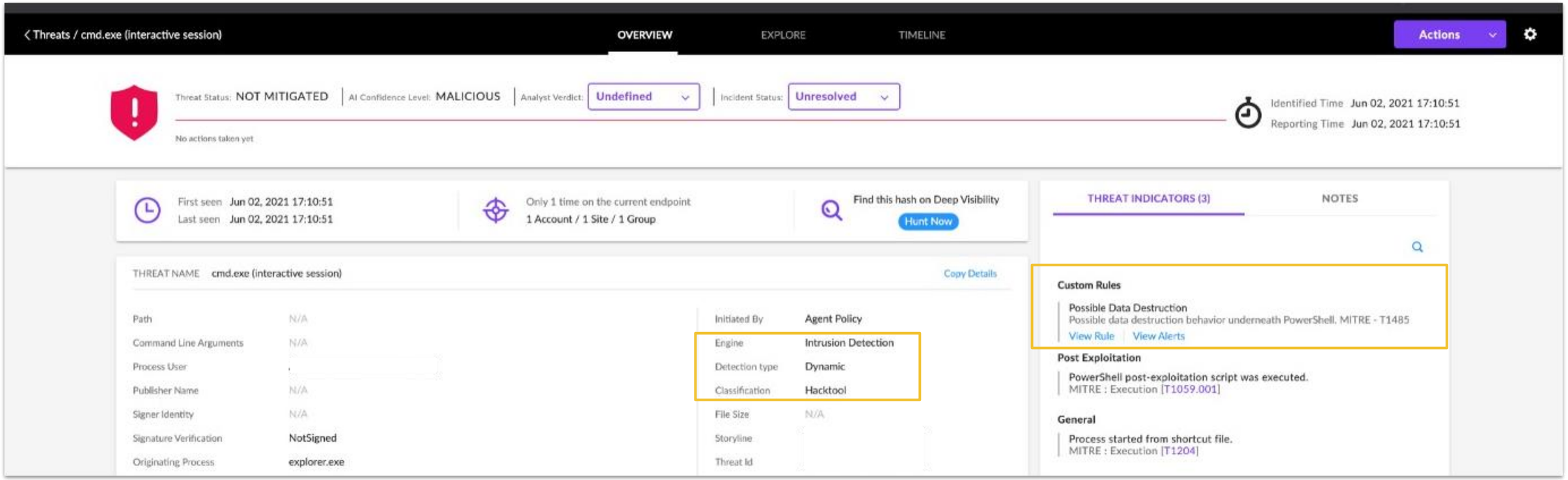
Active Response: 자동 대응

STAR를 통한 탐지 능력 강화

AI엔진에서는 powershell 실행 후 엔드 포인트에 악성 행위를 수행하여
엔드 포인트에 피해가 가는 경우 탐지, STAR를 행위 자체에 대한 탐지 확장

STAR Rule

EventType = "File Deletion"
AND SrcProcParentName = "powershell.exe"
AND TgtFileDeletionCount > "5"



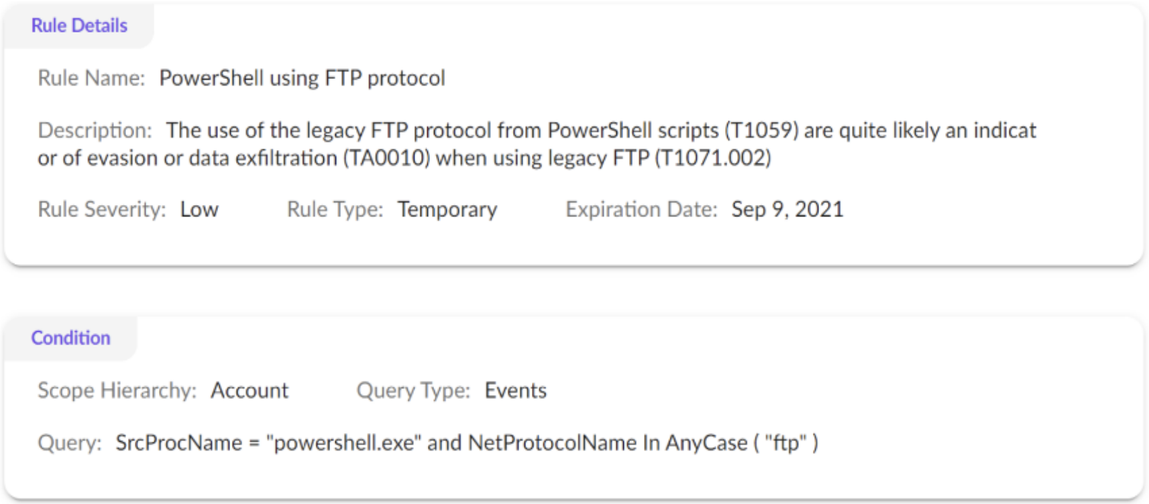
Threat Intelligence 기반 Active Response

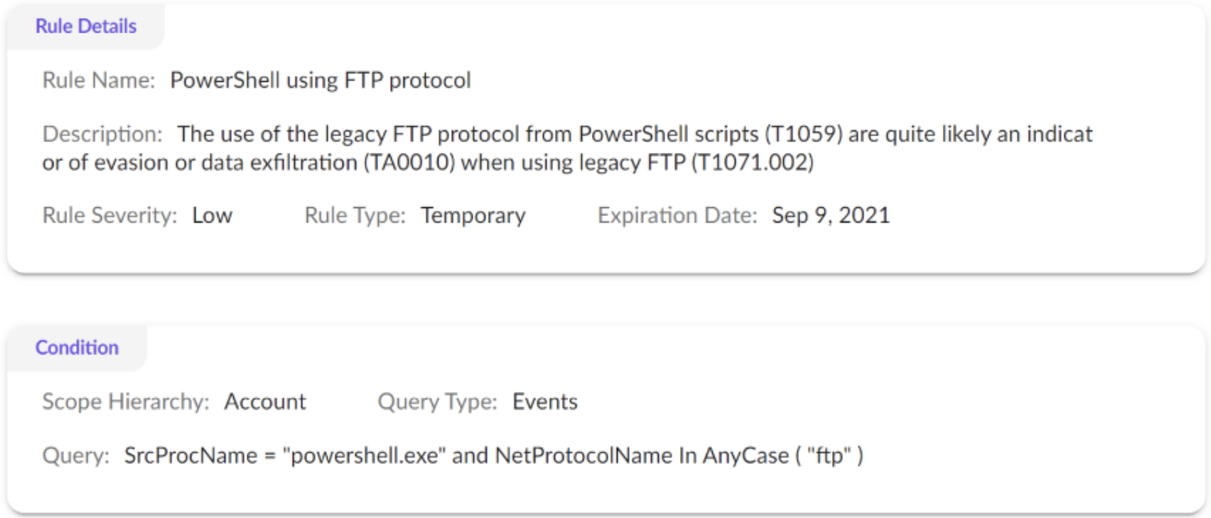
Threat Intelligence 서비스 제공 업체의 정보를 활용한 검색 지원

SrcProcName contains "powershell"

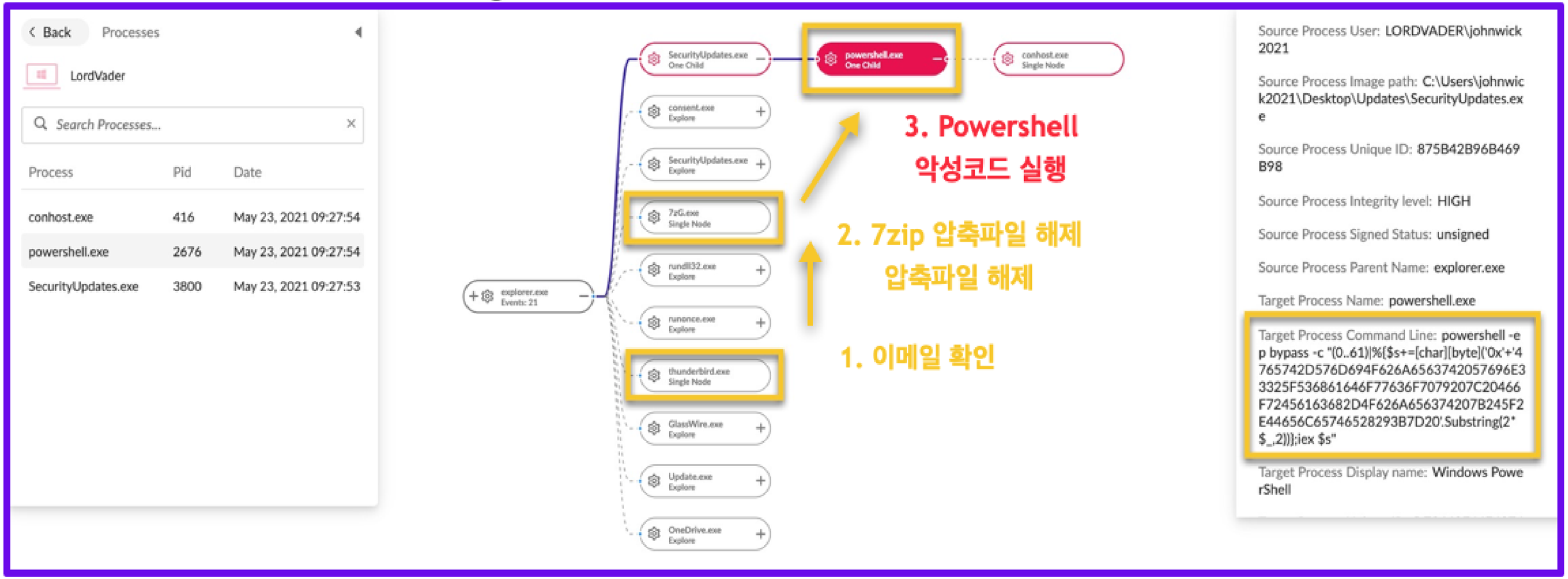
AND EventType = "Module Load"

AND TIIndicatorSource = "Recorded Future"





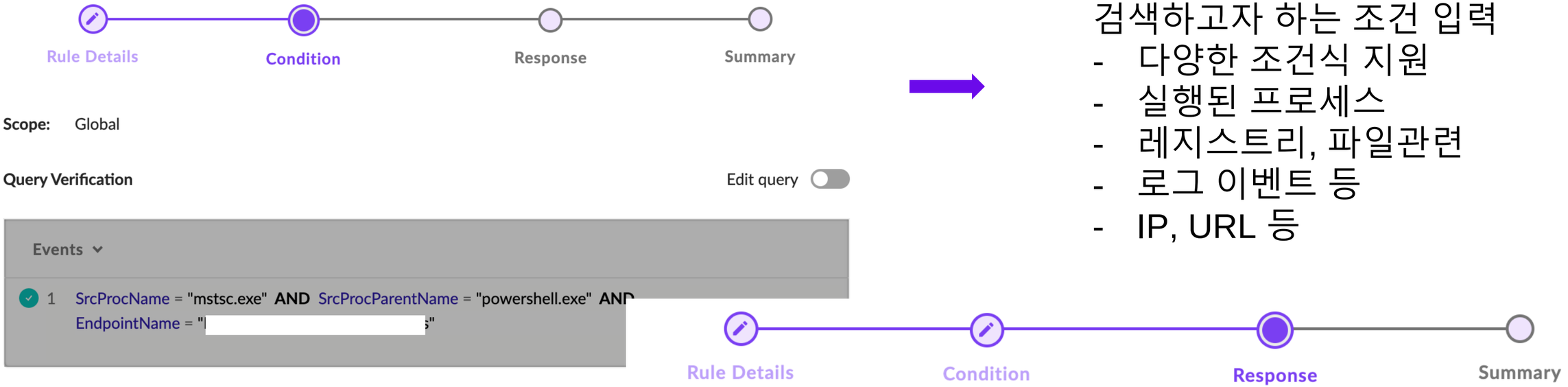
Threat Hunting 사례



악성 행위 : Powershell을 통한 악성코드 실행, 붉은 색 표시

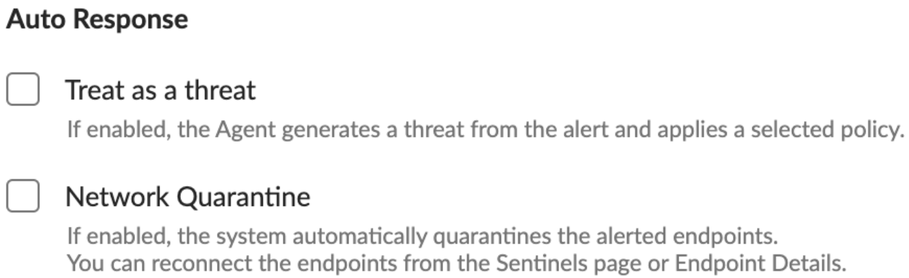
정상 행위 : Thunderbolt를 통해 이메일 확인/다운로드, 7zip을 통한 압축 파일 압축 해제, 검은색 표시

Star Alert



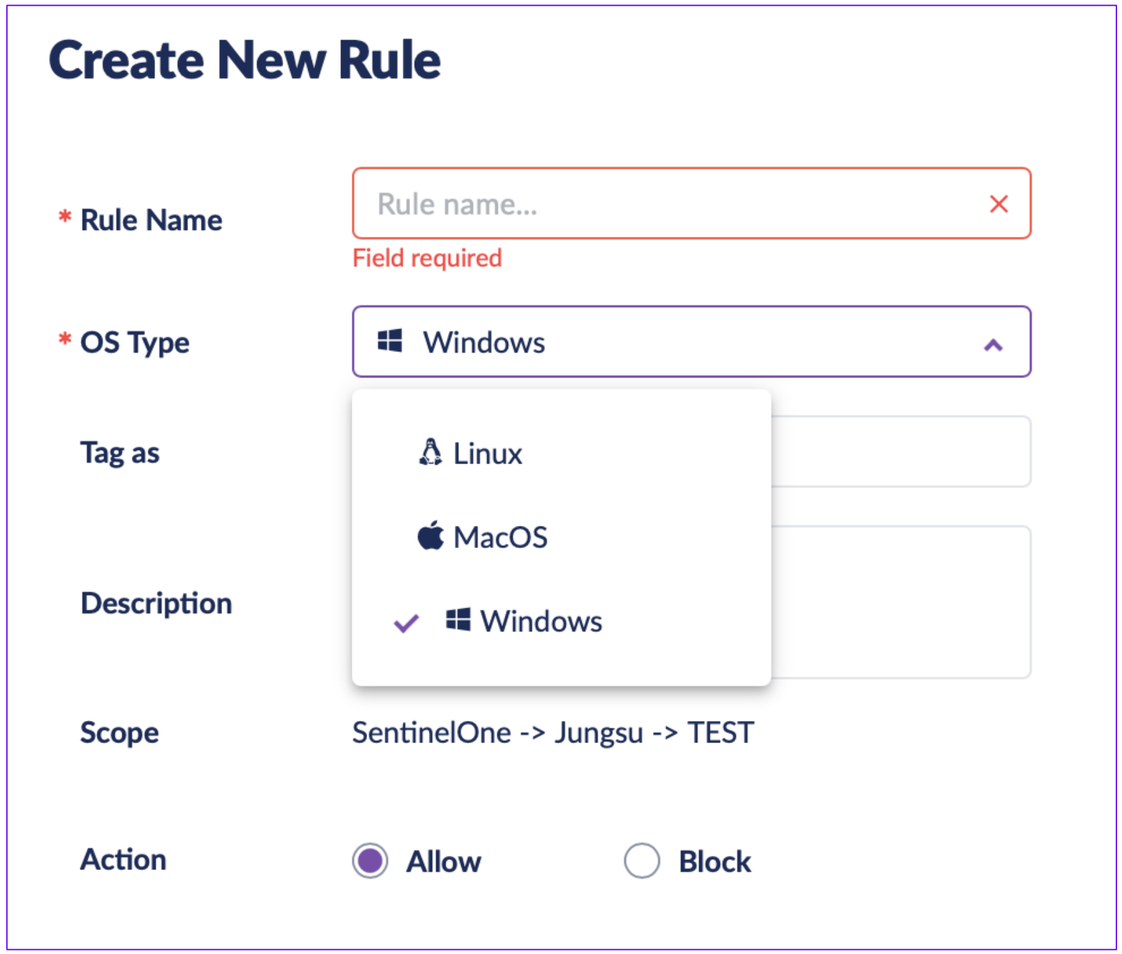
검색하고자 하는 조건 입력
- 다양한 조건식 지원
- 실행된 프로세스
- 레지스트리, 파일관련
- 로그 이벤트 등
- IP, URL 등

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

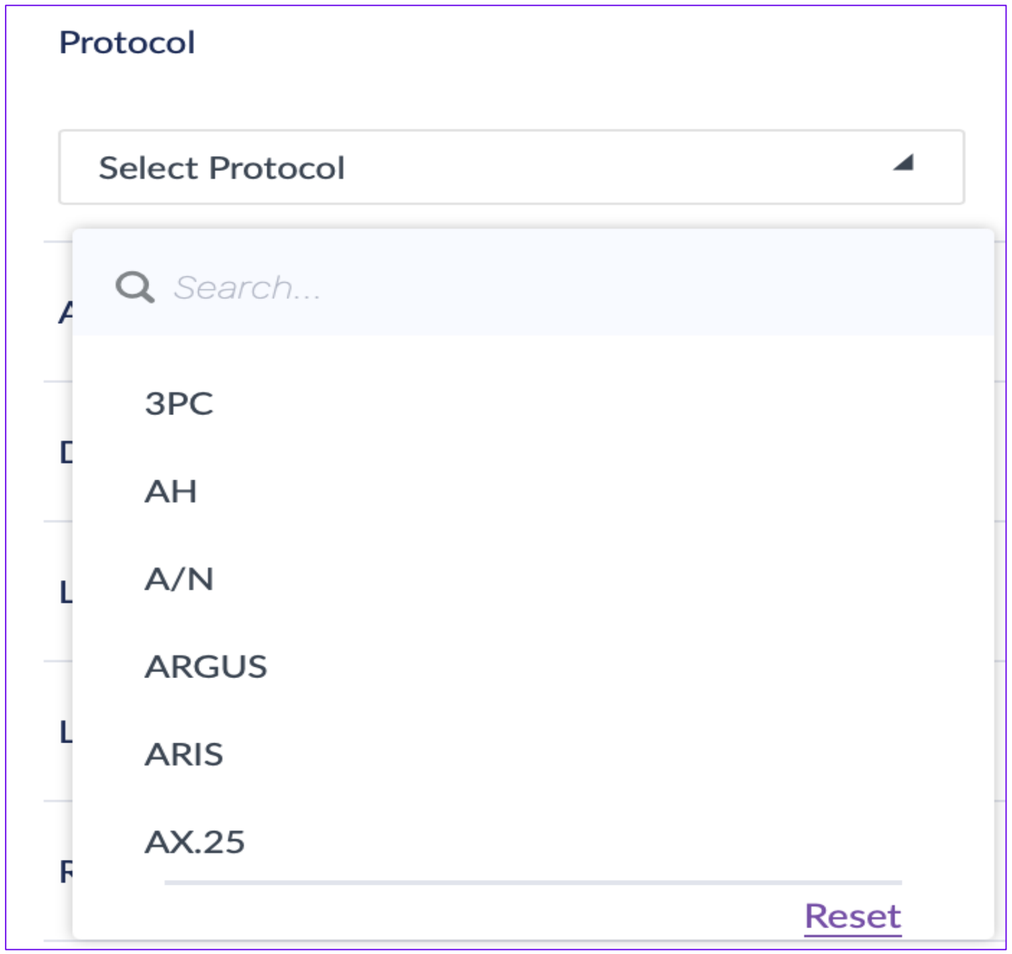


S1 Control

Core
Control
Complete



윈도우, 맥 및 리눅스 통합관리



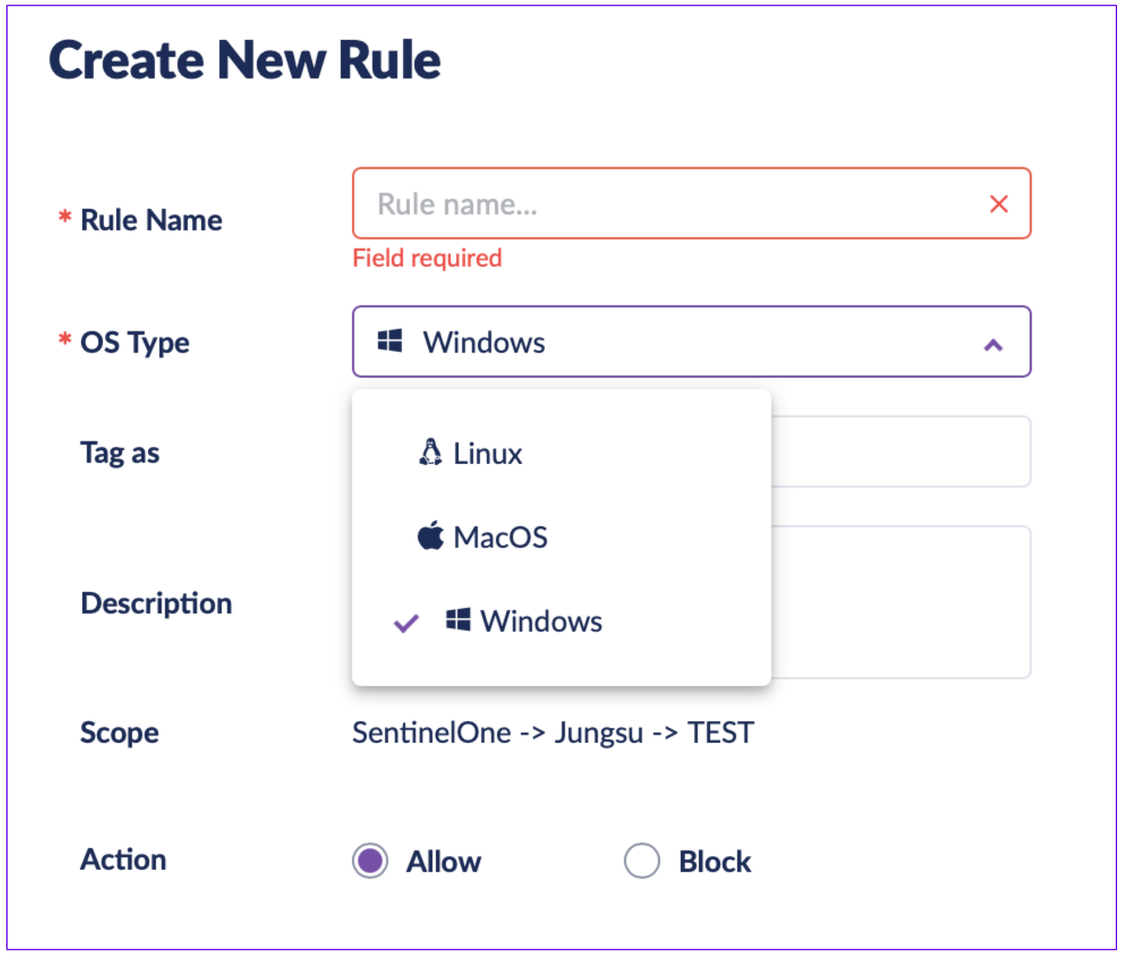
TCP/UDP 등 다양한 프로토콜 지원

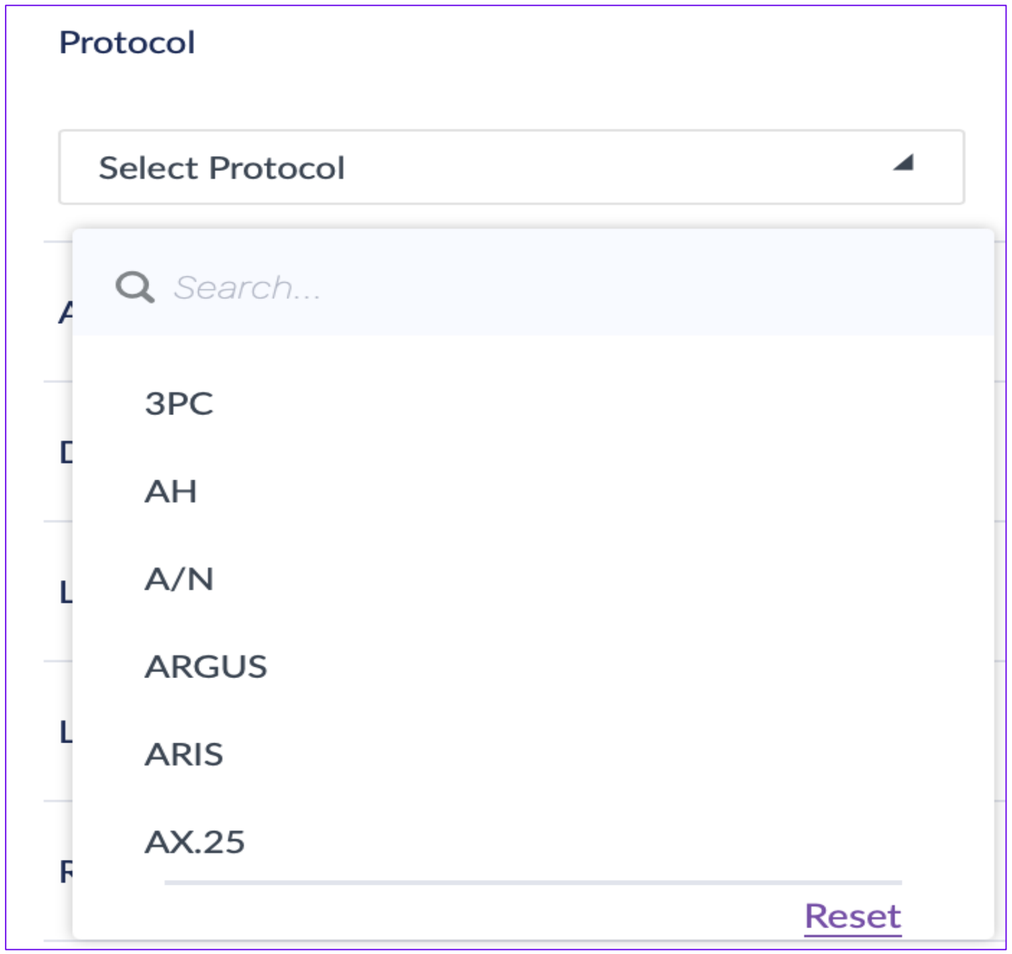
S1 Control

Core

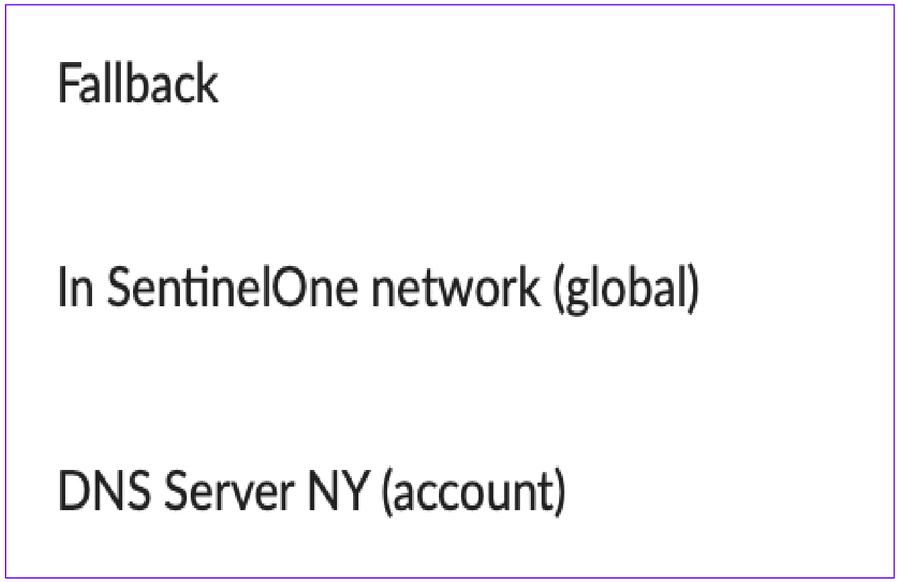
Control

Complete





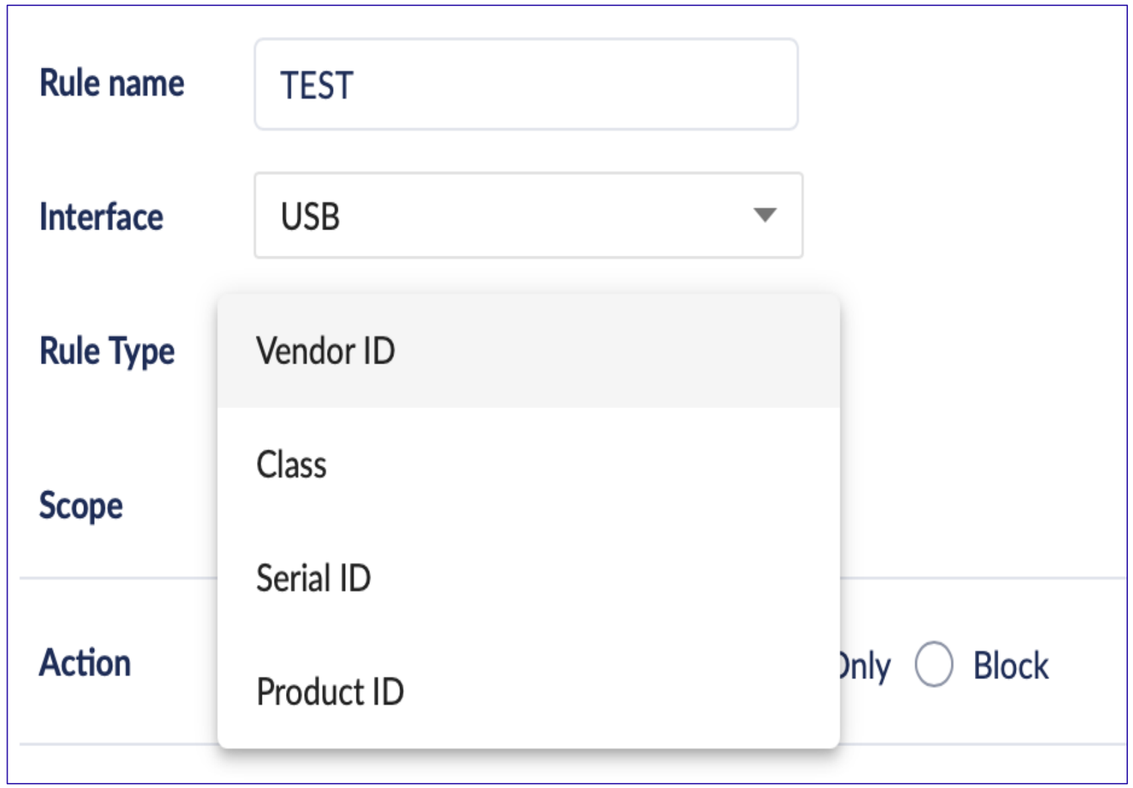
S1 Control



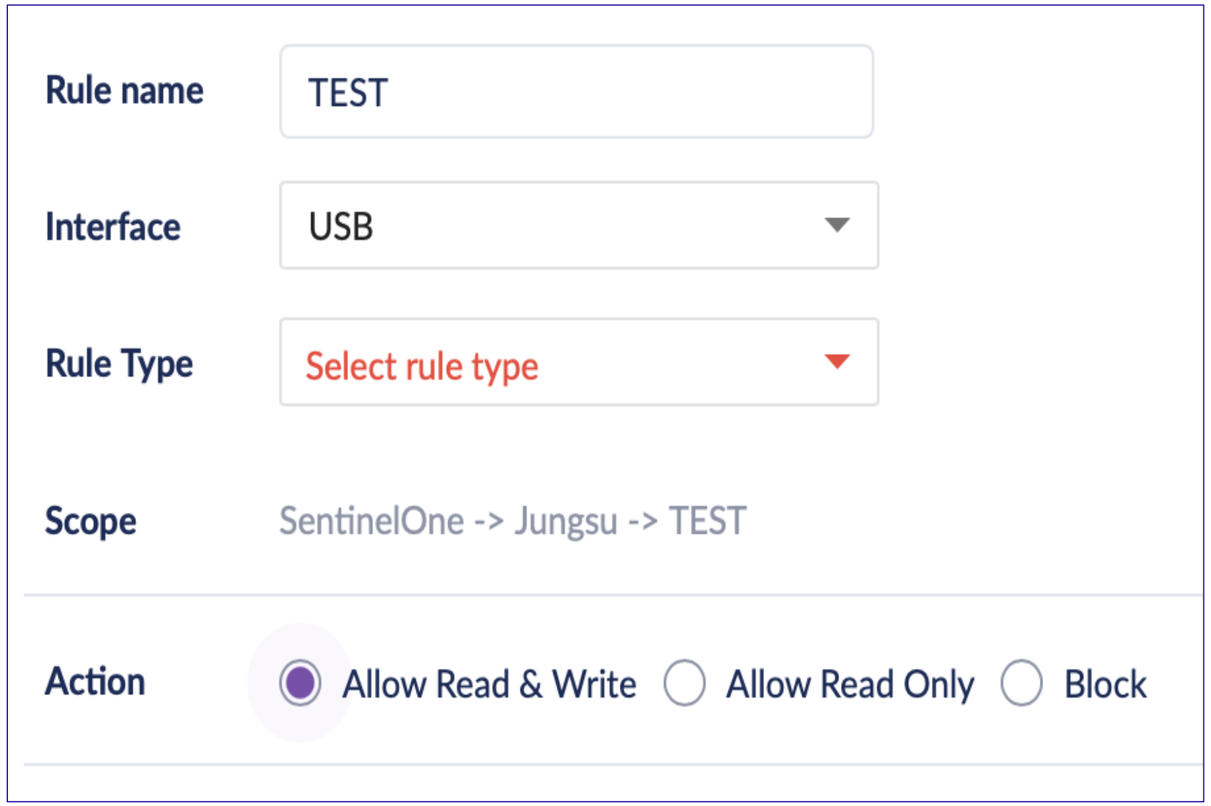
Location기반 정책 관리

애플케이션별 방화벽 정책 설정

S1 Control

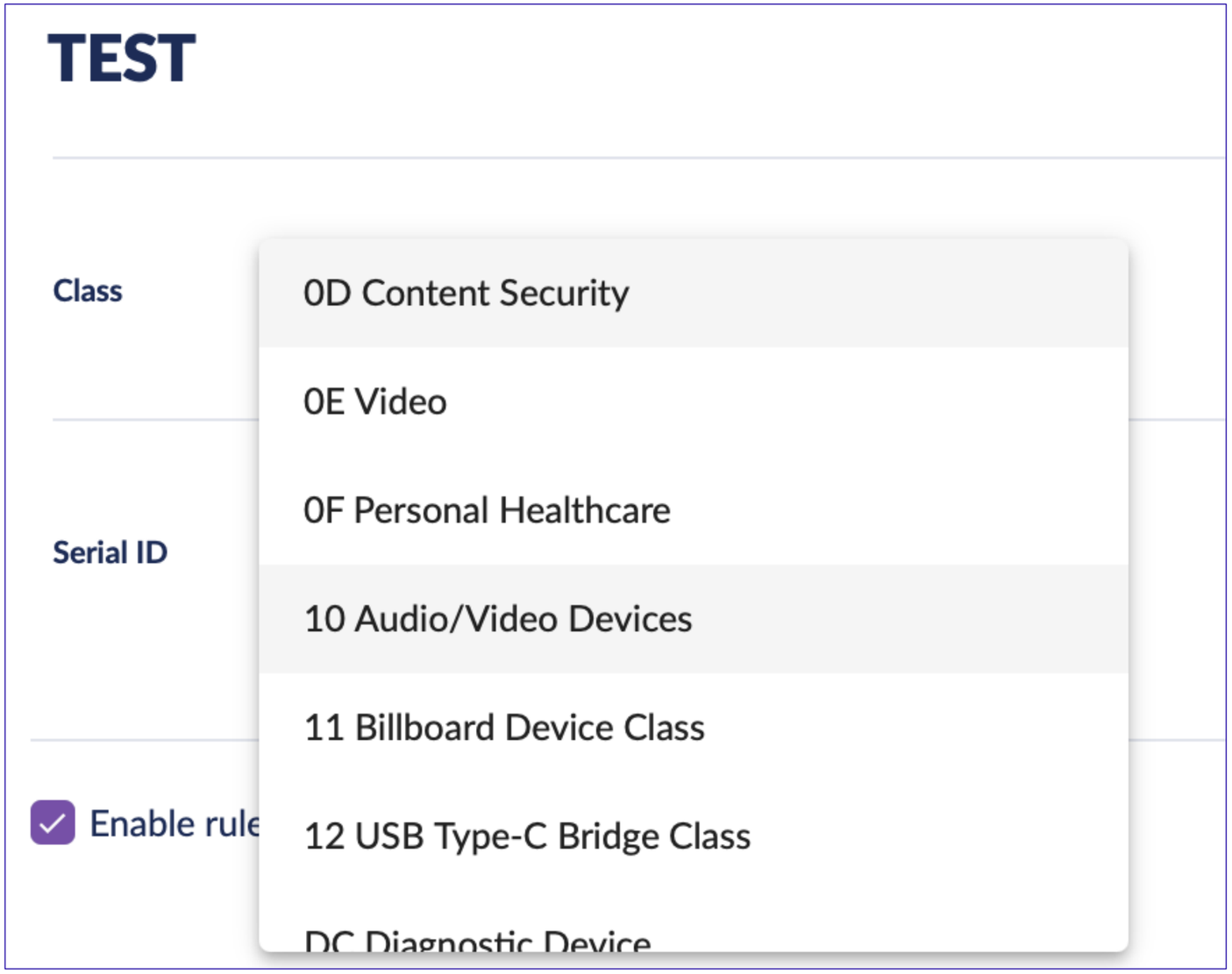


다양한 Rule Type 지원



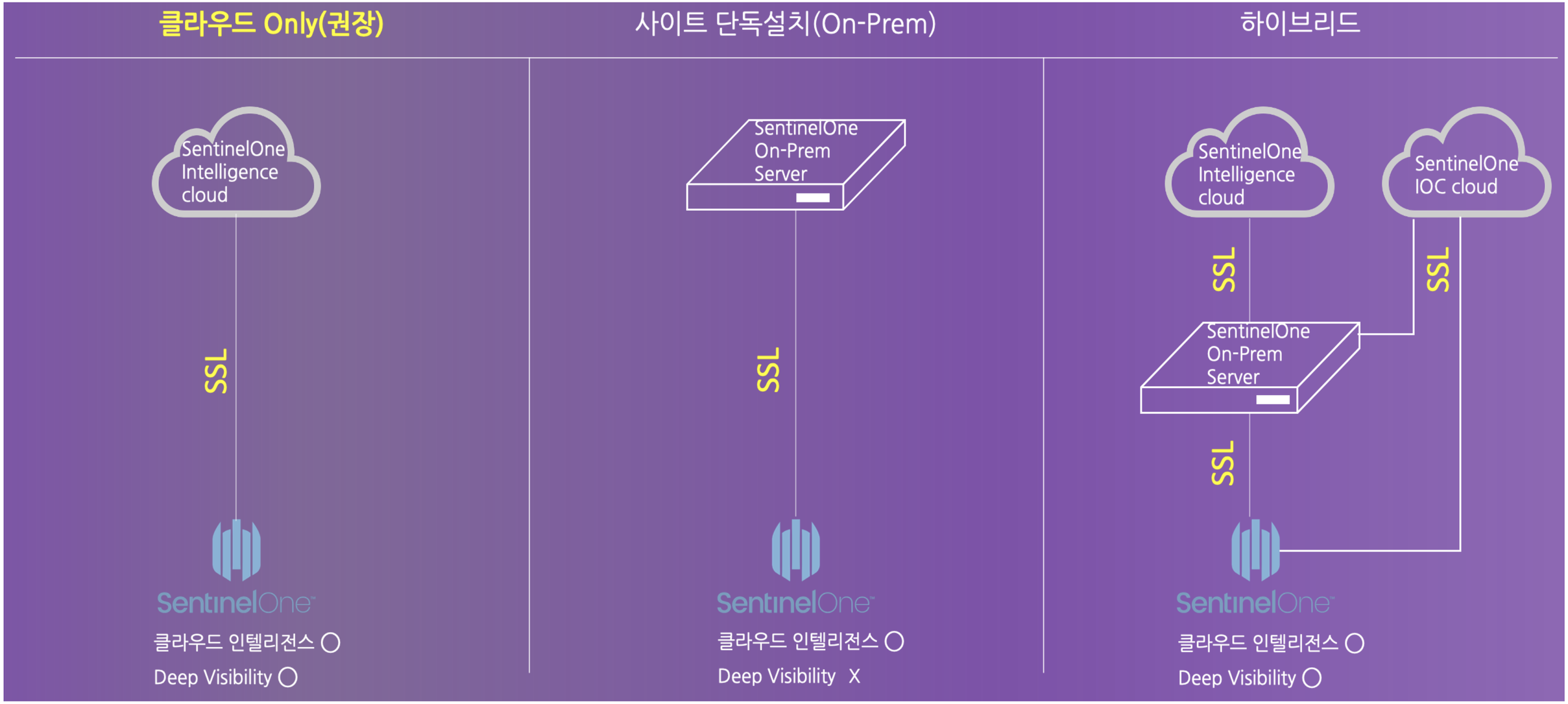
차단/읽기 전용/허용

S1 Control



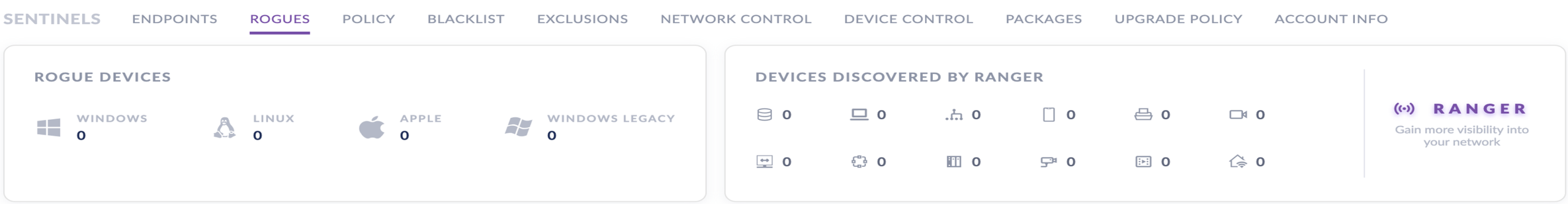
고객 요구사항에 따라
다양하게 설정할 수 있는
Class 지원

구성 방법

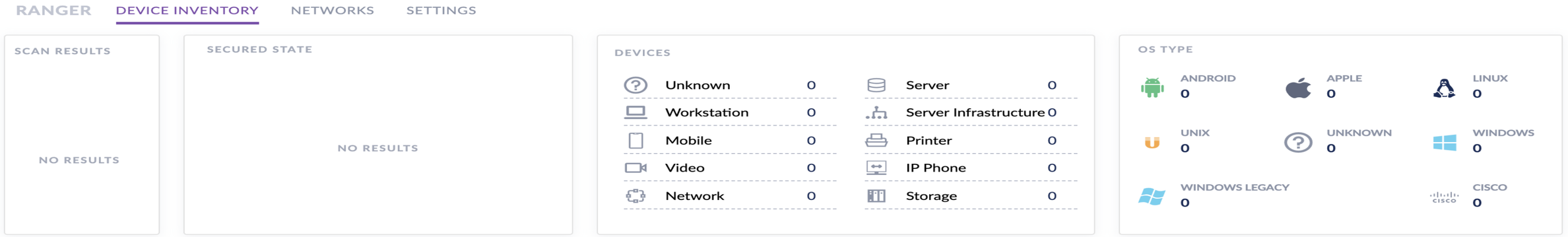


에이전트 미설치 단말 및 IoT 단말 검색

Rogue - S1 에이전트 미설치 단말 검색 및 격리



Ranger – IoT자산 검색 및 격리 (추가 라이센스 필요)



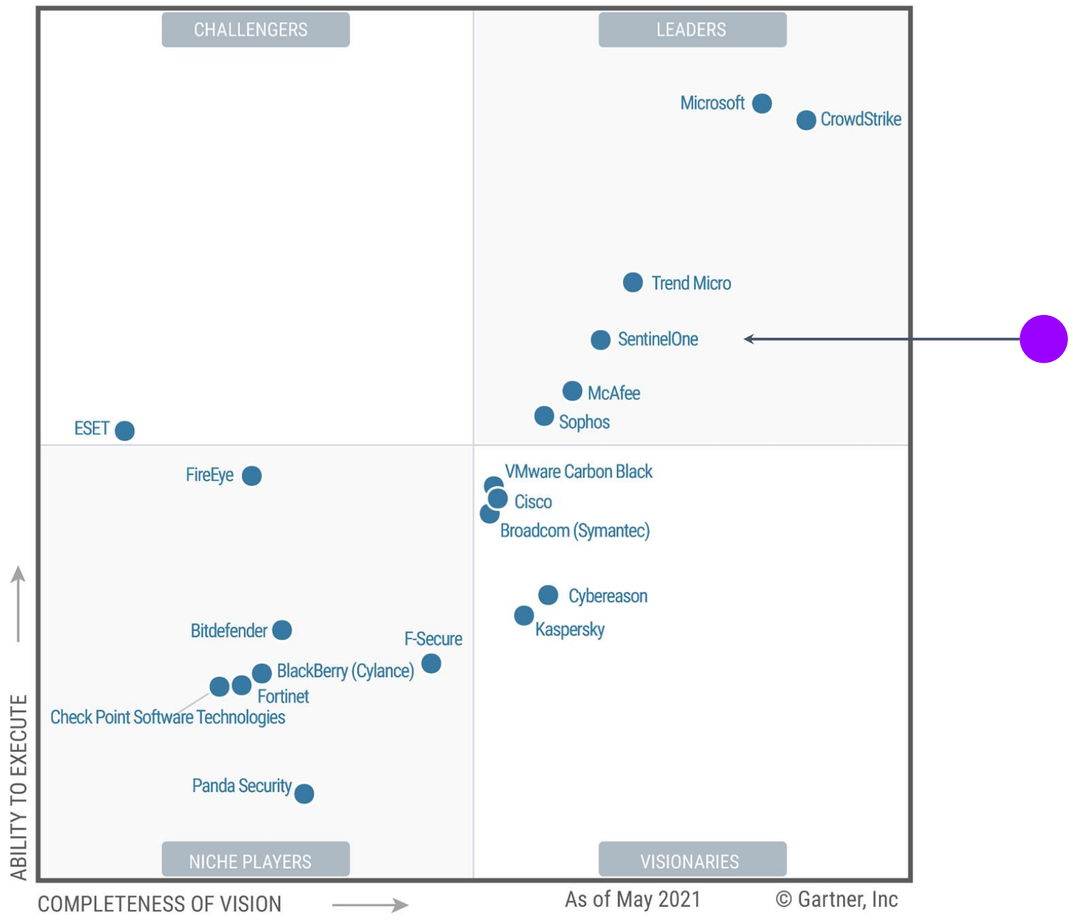
외부기관 평가

SentinelOne™

SentinelOne 리더로 확정

2021 Gartner Magic Quadrant for Endpoint Protection Platforms

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)

SentinelOne Characteristics

- Easy deployment
- Effective protection
- Options to suit all organizations
- Cloud workload ready
- Strong MITRE ATT&CK results
- Timely, quality customer support

SentinelOne 리더 그룹 확정

상세 리포트는 s1.ai/gartnermq

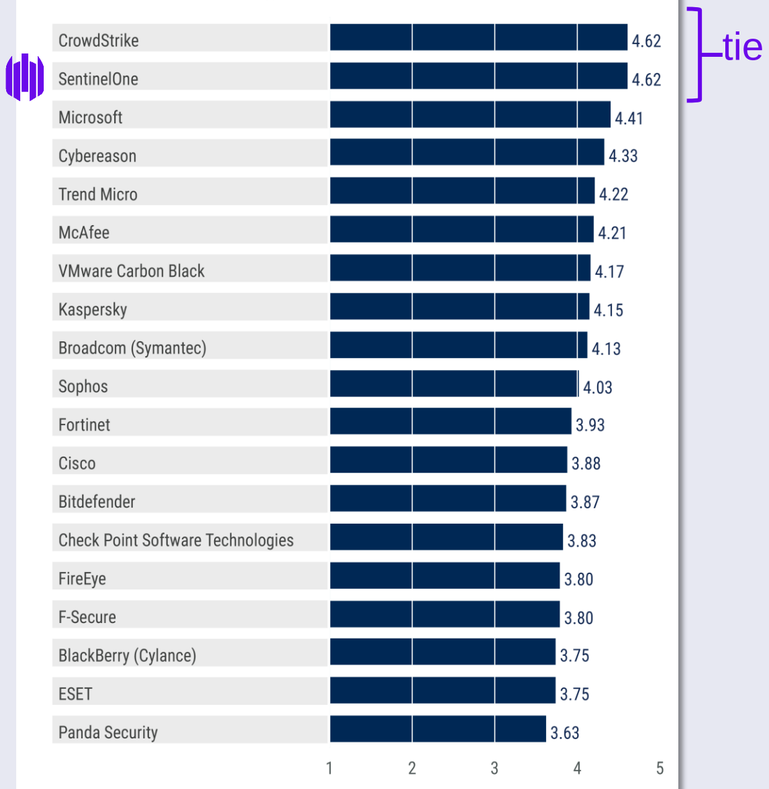
Gartner Critical Capabilities Scoring Elements

2021 Gartner Magic Quadrant for Endpoint Protection Platforms

- Ease of use
- Cloud management
- Prevention
- EDR functionality
- EPP suite
- Managed services
- Geographic support
- OS support

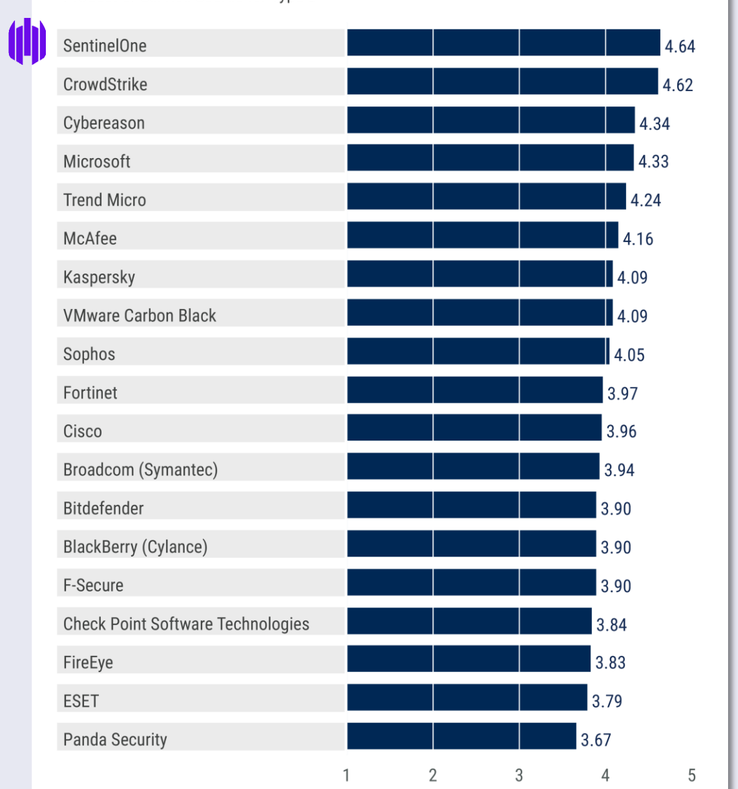
Critical Capabilities places “emphasis on hardening, detection of advanced and fileless attacks, and response capabilities, favoring cloud-delivered solutions offering a fusion of products and services.”

Figure 1. Vendors’ Product Scores for the Type A Use Case



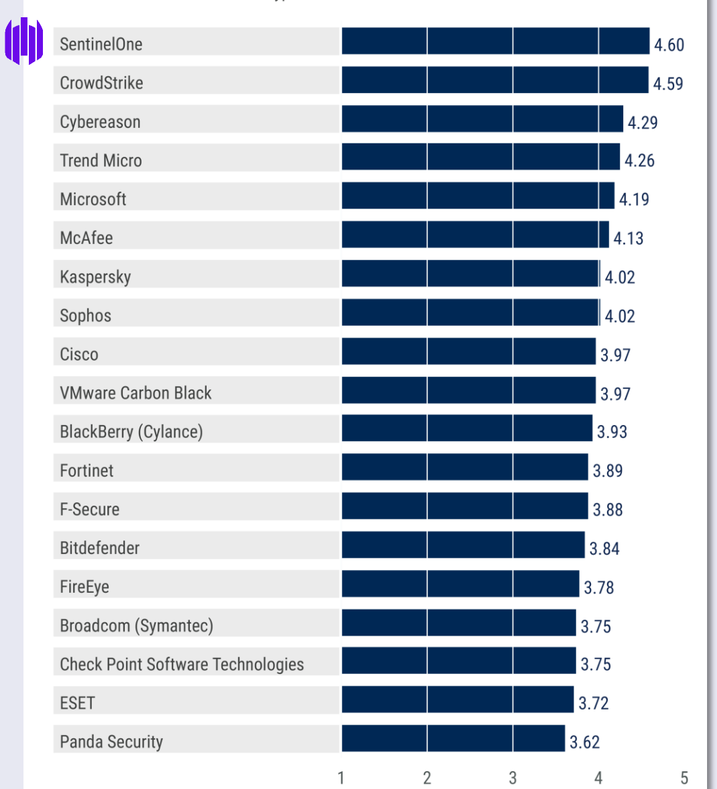
Source: Gartner (May 2021)

Figure 2. Vendors’ Product Scores for the Type B Use Case



Source: Gartner (May 2021)

Figure 3. Vendors’ Product Scores for the Type C Use Case



Source: Gartner (May 2021)

외부기관의 평가

Overall Ratings

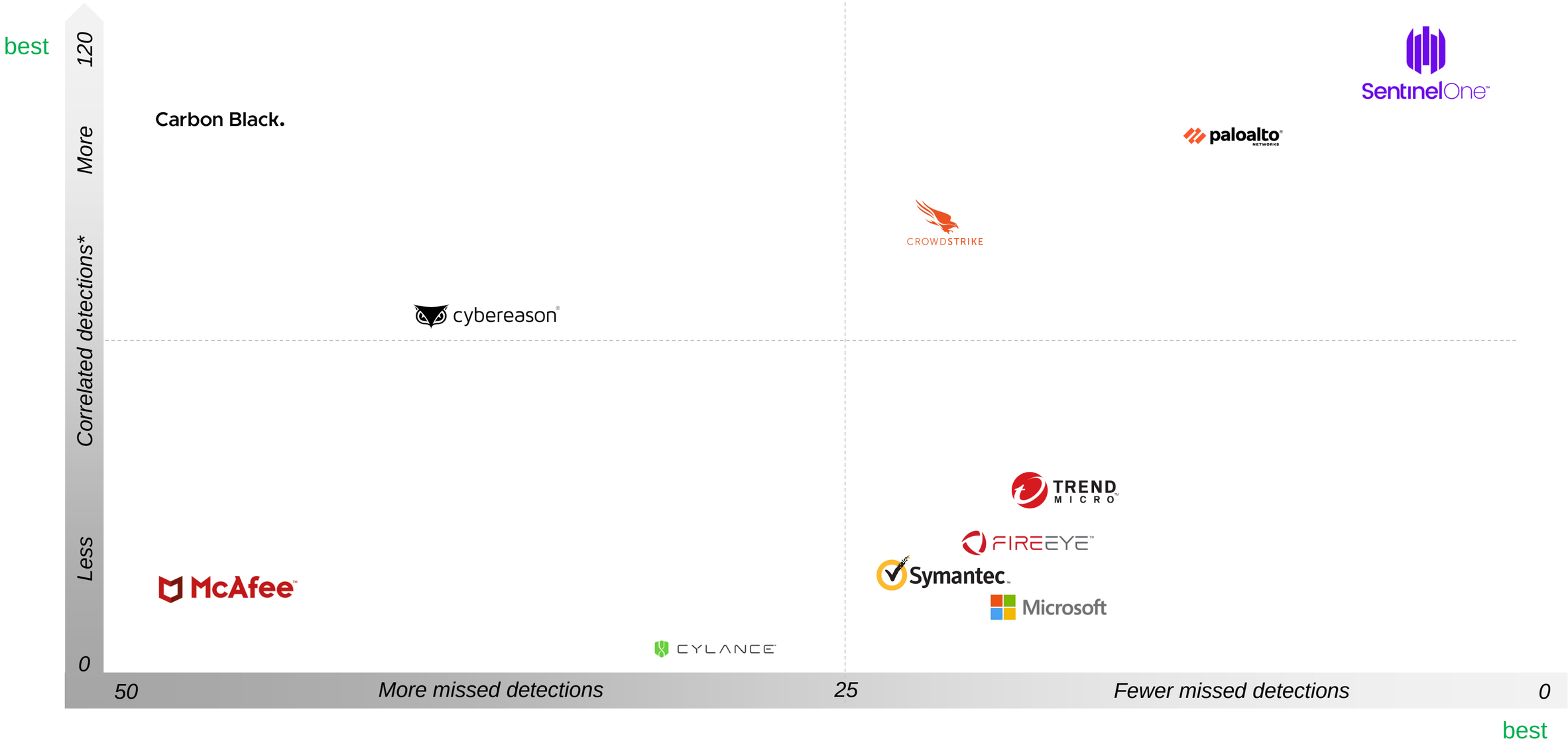
As of 31 October 2019 — Sorted by overall reviews

Eligible Vendors	Overall Rating	95% Confidence Range (lower – upper)	Overall Reviews
Kaspersky	4.5	4.5 – 4.6	815
Microsoft	4.3	4.3 – 4.4	663
Symantec	4.5	4.4 – 4.5	657
McAfee	4.4	4.4 – 4.5	624
Trend Micro	4.4	4.4 – 4.5	224
CrowdStrike	4.9	4.8 – 4.9	188
ESET	4.6	4.5 – 4.7	178
Sophos	4.3	4.2 – 4.4	164
SentinelOne	4.9	4.8 – 4.9	143
Carbon Black	4.7	4.6 – 4.8	115
Malwarebytes	4.8	4.6 – 4.8	105
Check Point Software Technologies	4.3	4.2 – 4.5	84
Panda Security	4.6	4.4 – 4.7	78
Bitdefender	4.6	4.4 – 4.7	65
BlackBerry Cylance	4.4	4.2 – 4.6	51
Cisco	4.5	4.2 – 4.7	31
Fortinet	4.5	4.3 – 4.7	30
F-Secure	4.3	4.1 – 4.7	24
Palo Alto Networks	4.3	4.1 – 4.7	21
Comodo	4.5	4.1 – 4.8	17
Morphisec	4.6	4.2 – 4.9	14
Cybereason	4.7	4.2 – 4.8	13
enSilo	4.8	4.2 – 4.9	10

4.0 4.5 5.0

MITRE ATT&CK Phase 2 Testing

SentinelOne Leads with Fewest Misses & Most Correlations



MITRE ATT&CK Phase 2 Results Data: https://attackevals.mitre.org/evaluations.html?round=APT29

*Y-Axis = All Tool Correlated (Telemetry + General + Tactics + Techniques)

SentinelOne

외부기관의 평가

June 2020

SentinelOne Endpoint Security Platform

Windows 7 version	3.7.2.45
Windows 10 version	3.7.2.45
WildList detection	99.9%
False positive rate	0.001%
Diversity Test rate	100.00%

April 2020

SentinelOne Endpoint Security Platform

Windows 7 version	3.7.2.45
Windows 10 version	3.7.2.45
WildList detection	99.9%
False positive rate	0.001%
Diversity Test rate	100.00%

SE Labs Awards

Thank You