



자율형 악성코드 차단 솔루션

(Endpoint Protection Detection & Response)

SentinelOne Korea



악성코드 공격 사례 및 레거시 백신 대비 우수성

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>

[Sentinel Labs](#), 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.

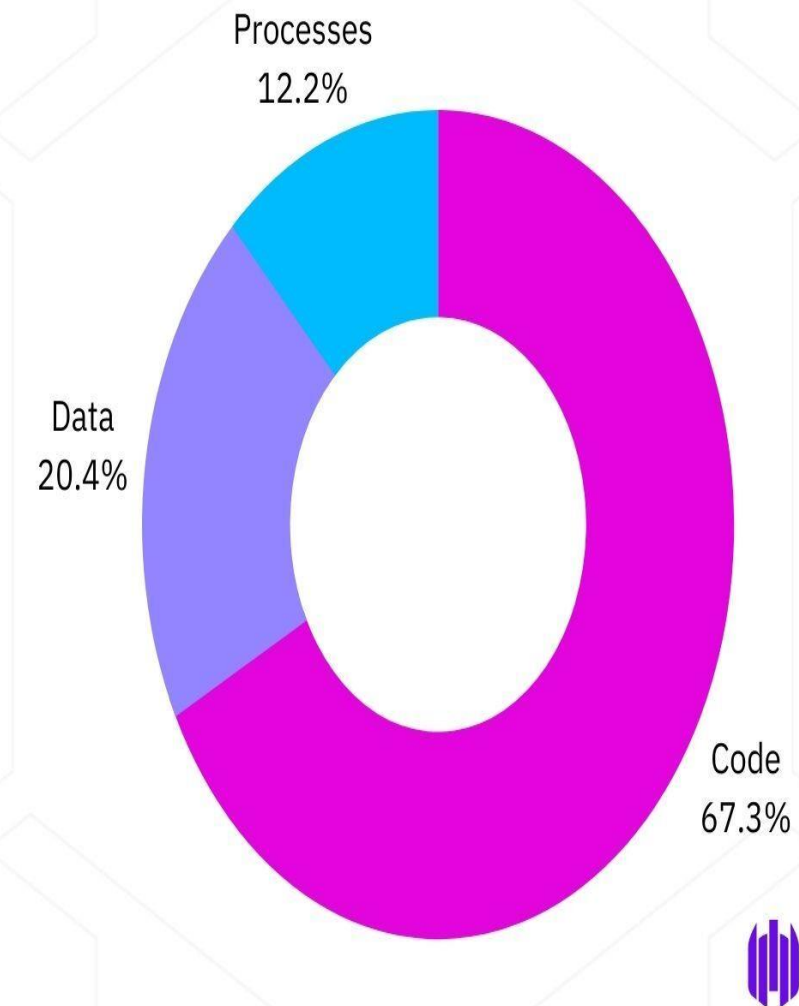
“We’re continuously monitoring and testing the latest SUNBURST variants to ensure our customers remain protected,” said Raj Rajamani, Chief Product Officer, SentinelOne. “Unlike traditional antivirus and other next-gen products, SentinelOne’s autonomous AI and robust anti-tampering protected our customers 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

Suppliers' Assets Targeted

ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS - 2021



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

국내 Supply Chain 및 APT 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 '이니
세이프' 시리즈와 닉스텍 '세이프 PC' 사용 고객은 피해를 입지 않도록 주의해야
한다.<https://m.etnews.com/20161130000395>

[긴급] 국내 시장점유율 1위 지니언스의 NAC 제품, 관리자 권한 탈취 가능 취약점
발견<https://m.boannews.com/html/detail.html?idx=99832>

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

통일부 사칭, 北 연계 APT공격 등장... '사이버 공격 주의 업
무로 둔갑'

<https://www.estsecurity.com/enterprise/security-center/notice/view/136354?category-id=>

北 연계 사이버 위협 조직 탈륨, PDF 문서 취약점 이용한 공
격 수행

<https://www.estsecurity.com/enterprise/security-center/notice/view/123186?category-id=>

이스트시큐리티, 北 해커 탈륨 추정 APT 공격 증가

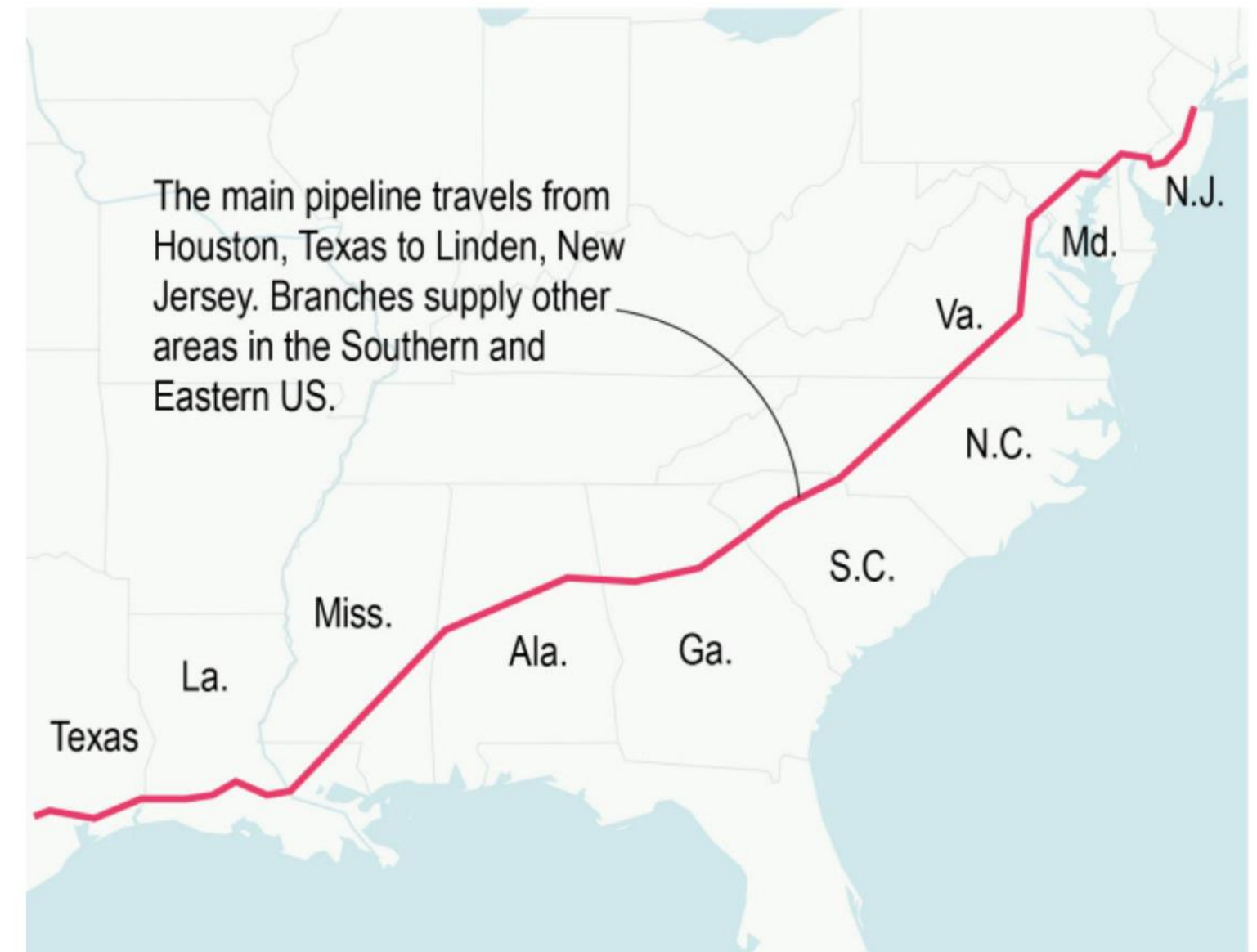
http://it.chosun.com/site/data/html_dir/2021/08/03/2021080300854.html

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

Pipeline spans more than 5,500 miles



Source: Colonial Pipeline

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

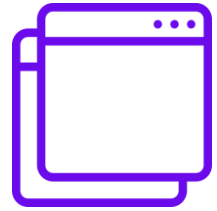
[T1490](#) Inhibit System Recovery

[T1553.004](#) Subvert Trust Controls: Install Root Certificate

[T1078](#) Valid Accounts

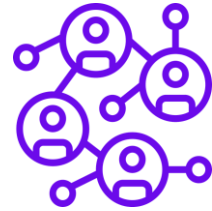
DarkSide 공격에 사용된 기법

기존 백신 프로그램의 한계



**악성코드 실행
이력에 대한
가시성 부족**

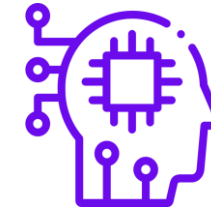
악성코드 탐지 전
수행한 실행 이력
및 변경사항에
대한 가시성 확보
불가



**알려지지 않은
악성코드 탐지 불가**

시그니처 기반의
한계로 알려지지
않은 악성코드 탐지
불가,

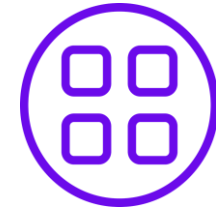
시그니처 DB 증가로
인한 성능 이슈 발생



**자동 치료 및
복구 기능 부재**

보안 전문가에
의한 수동 복구
또는 엔드 포인트
포맷 필요,

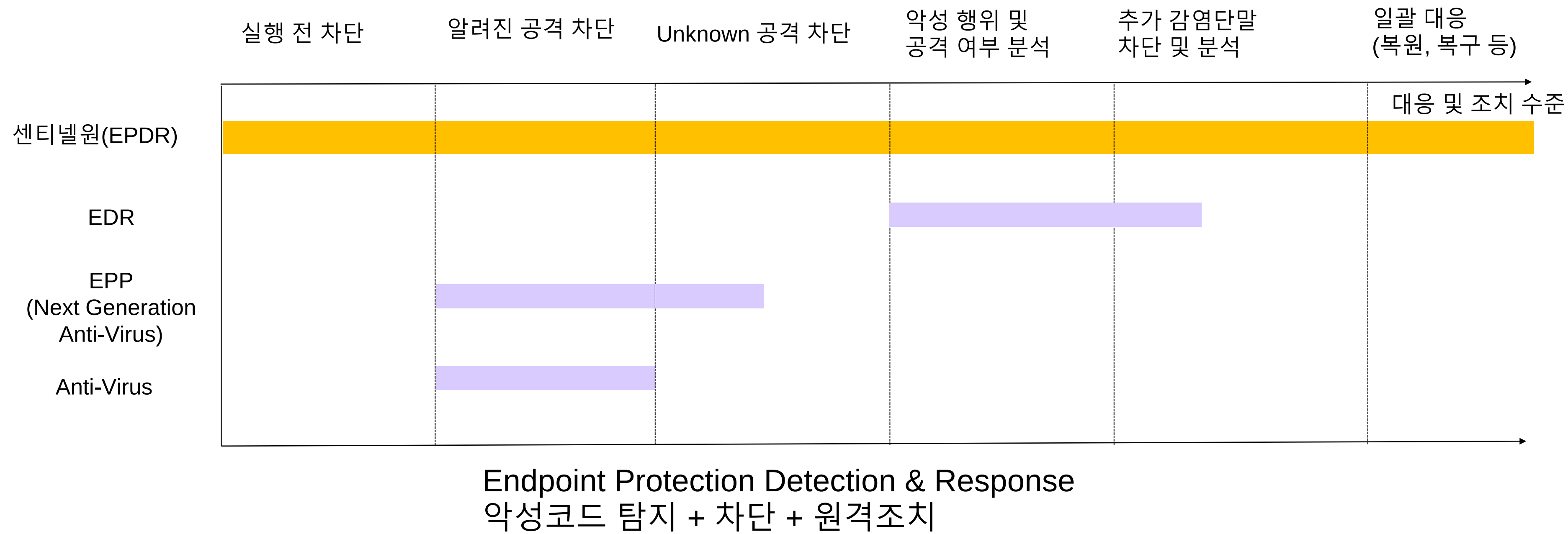
**랜섬웨어 탐지 시
복구 불가**



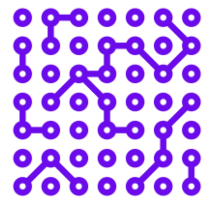
**너무 많은 보안 기능
탑재로 인한 복잡성
증가**

다양한 보안
기능을 탑재하여
복잡성 증가 및
장애 시 분석
어려움

보안 솔루션 트렌드(EPP에서 EDR로)

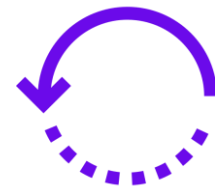


SentinelOne 대응 기술



Storyline™

악성코드
시작부터
마지막까지 모든
과정을 분석할 수
있는 단일 식별자



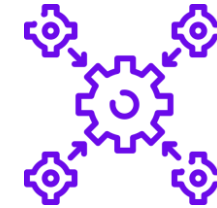
ActiveEDR®

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



ONE Console

전세계 모든
지역에서 단일
콘솔로 통합 관리
제공

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

Mitigation Actions



KILL

Stops all processes
related to the threat



QUARANTINE

Encrypts and moves
the threat and its executables



REMEDiate

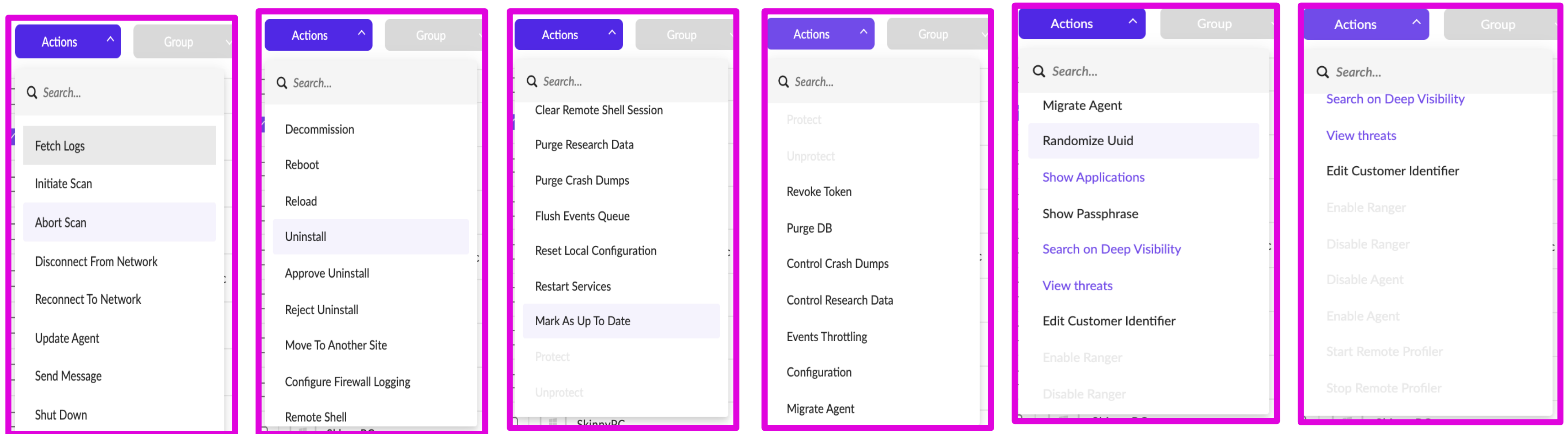
Deletes all files
and system changes
created by the threat



ROLLBACK

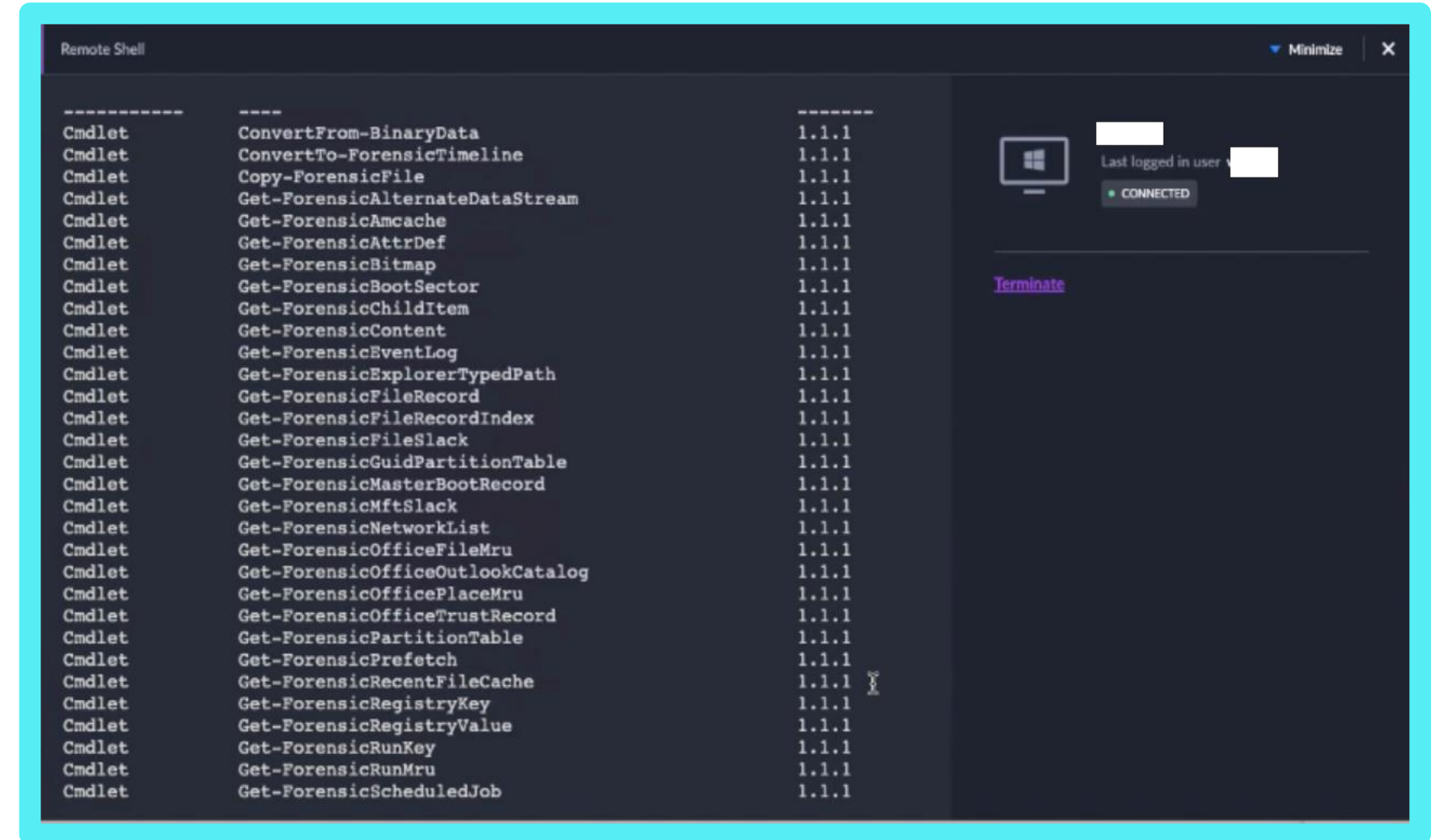
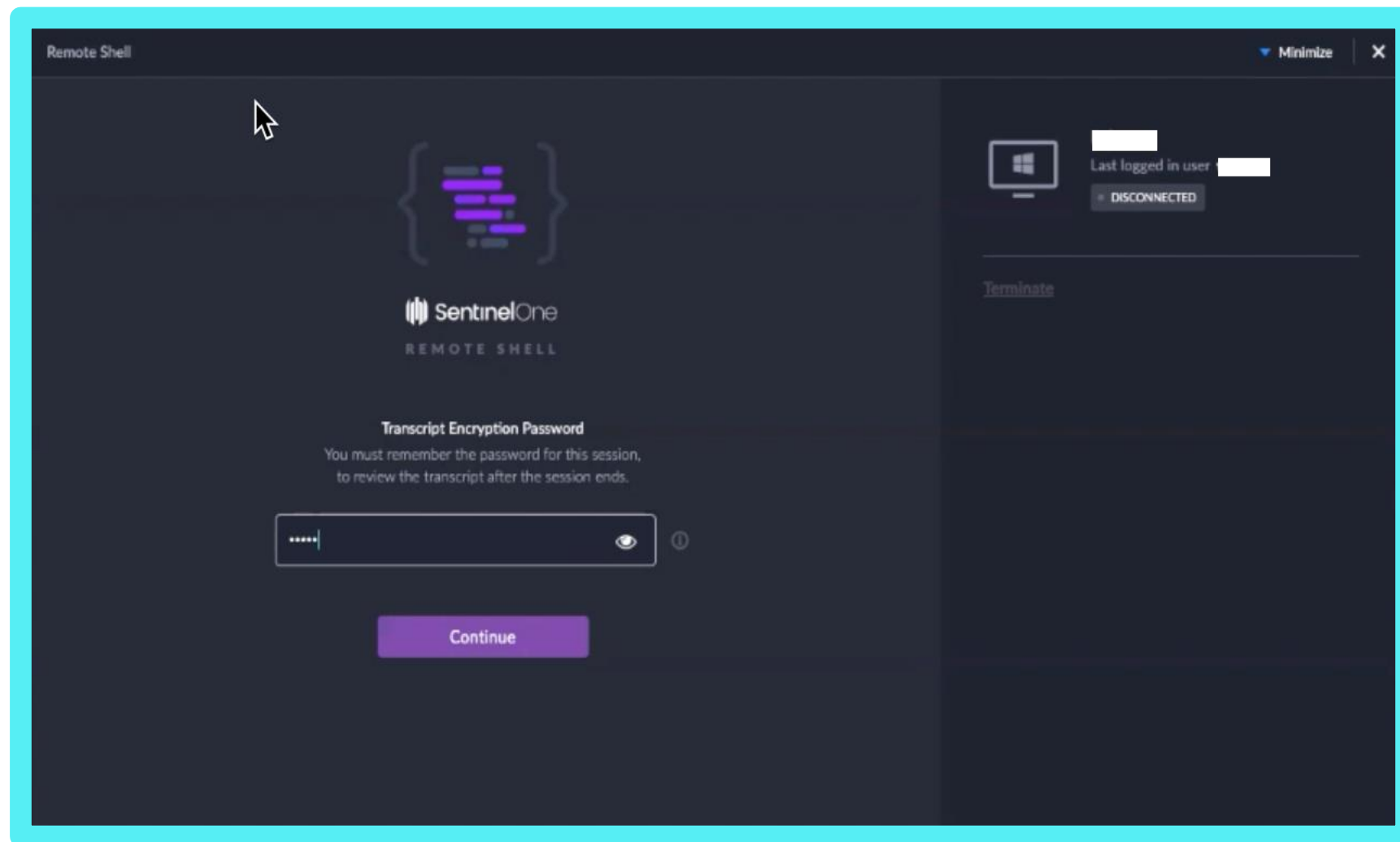
Restores files and
configurations that the
threat changed

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 탐지 엔진

평판

Static AI

Behavioral AI

Deep Visibility

실행 전

실행중

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 시기반 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



First seen Oct 03, 2019 23:19:39
Last seen Mar 08, 2021 14:31:06



224 times on 18 endpoints
1 Account / 10 Sites / 11 Groups



Find this hash on Deep Visibility
[Hunt Now](#)

THREAT FILE NAME @WanaDecryptor@.exe

[Copy Details](#)[Download Threat File](#)

PATH

\Device\HarddiskVolume3\Users\admin\Downloads\@Wan...

COMMAND LINE ARGUMENTS

N/A

PROCESS USER

DESKTOP-S3CD39K\admin

PUBLISHER NAME

N/A

SIGNER IDENTITY

N/A

SIGNATURE VERIFICATION

NotSigned

ORIGINATING PROCESS

3dc6191c1255cfbaf94461e9a44f5b698c5563bbf846c94c...

SHA1

45356a9dd616ed7161a3b9192e2f318d0ab5ad10

SHA256

b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846...

INITIATED BY

Agent Policy

ENGINE

SentinelOne Cloud

DETECTION TYPE

Static

CLASSIFICATION

Ransomware

FILE SIZE

240.00 KB

STORYLINE

Static Threat - View in DV

THREAT ID

1106899194251275373

☐	OS	Hash	Description	Last Update ▼
☐	Windows	76cc92ca3ed0de41fc192fc	Detected by SentinelOne Cloud	Feb 25, 2021 3:11 PM
☐	Android	3395856ce81f2b7382de	Detected by SentinelOne Cloud	Feb 25, 2021 3:09 PM
☐	Android	b9709200d323392478f1e	Detected by SentinelOne Cloud	Feb 24, 2021 9:08 AM
☐	Android	5c77af26784655dcc9412	Detected by SentinelOne Cloud	Feb 24, 2021 9:08 AM
☐	Android	7b533994613e2b3a69d7	Detected by SentinelOne Cloud	Feb 24, 2021 9:08 AM
☐	Android	a45f11afc6494812e24d5	Detected by SentinelOne Cloud	Feb 24, 2021 9:08 AM

 SentinelOne™

©2020 SentinelOne, All Rights Reserved.

16

Static AI(Artificial Intelligence)

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

 First seen Feb 15, 2021 16:51:42
Last seen Mar 03, 2021 10:32:04

 [5 times](#) on 1 endpoint
1 Account / 1 Site / 1 Group

 Find this hash on Deep Visibility
[Hunt Now](#)

THREAT FILE NAME `cbc981c415930a0d7623f50e9ee8808d582b84ed5f079725eeb019e52a857f4f.exe`

[Copy Details](#)[Download Threat File](#)

PATH	\Device\HarddiskVolume3\Users\admin\Desktop\2021022...	INITIATED BY	Agent Policy
COMMAND LINE ARGUMENTS	N/A	ENGINE	On-Write Static AI
PROCESS USER	DESKTOP-S3CD39K\admin	DETECTION TYPE	Static
PUBLISHER NAME	N/A	CLASSIFICATION	Malware
SIGNER IDENTITY	N/A	FILE SIZE	1.01 MB
SIGNATURE VERIFICATION	NotSigned	STORYLINE	Static Threat - View in DV
ORIGINATING PROCESS	7zG.exe	THREAT ID	1103155005248053337
SHA1	e962ee5151584ee7278fee5bc2bc7c450899f450		
SHA256	cbc981c415930a0d7623f50e9ee8808d582b84ed5f07972...		

THREAT INDICATORS (3)

NOTES (1)

Hiding/Stealthiness

The majority of sections in this PE have high entropy, a sign of obfuscation or packing.

This binary may contain encrypted or compressed data as measured by high entropy of the sections (greater than 6.8).

General

This binary imports debugger functions.

 SentinelOne™

©2020 SentinelOne, All Rights Reserved.

17

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)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	15 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Execution Guardrails (1)	Execution Guardrails (1)	Man-in-the-Middle (2)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Exploitation for Defense Evasion	Exploitation for Defense Evasion	Modify Authentication Process (4)	File and Directory Permissions Modification (2)	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hide Artifacts (7)	Hide Artifacts (7)	OS Credential Dumping (8)	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (2)
				Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
				Scheduled Task/Job (6)	Process Injection (11)	Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery			Protocol Tunneling		Service Stop
					Scheduled Task/Job (6)	Indicator Removal on Host (6)		Peripheral Device Discovery					System Shutdown/Reboot
								Permission Groups Discovery (3)					
								Process Discovery					

공격 사례 – Drive by download

브라우저 취약점을 악용한 공격 사례 – Exploit

All Events1,110

Processes57

Cross Process115

Indicators56

Files426

Network Actions74

DNS51

URL331

Actions

No Items Selected

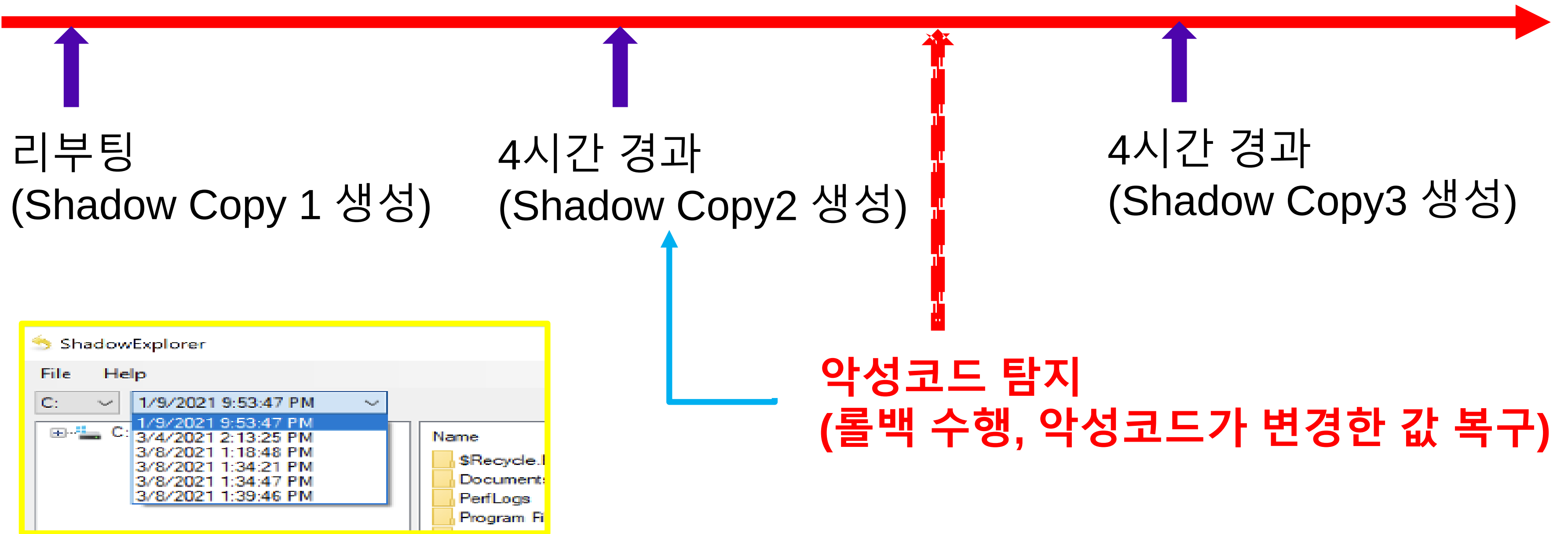
56 Results100 ResultsColumnsExport

	Source Process Si...	Source Process P...	Indicator Name	Indicator Category	Indicator Description
☐	signed	iexplore.exe	RemoteLibraryInjection	Injection	Library was injected to a remote process. MITRE: Defense Evasion {T1055}, Privilege Escalation {T1055}
☐	signed	explorer.exe	BrowserInfoStealing	Infostealer	Chrome's sensitive information was accessed. MITRE: Credential Access {T1555.003}
☐	signed	explorer.exe	ApplicationInfoStealing	Infostealer	Opera's sensitive information was accessed. MITRE: Collection {T1213}
☐	signed	explorer.exe	ChromiumEdgeInfoSte...	Infostealer	Chromium edge's sensitive information was accessed. MITRE: Credential Access {T1555.003}
☐	signed	explorer.exe	ApplicationInfoStealing	Infostealer	Opera's sensitive information was accessed. MITRE: Collection {T1213}

SOURCE PROCESS DETAILS		TARGET FILE DETAILS	
Name	• iexplore.exe	Path	• [REDACTED]ver.jpg.bnb[REDACTED]
Storyline ID	• CDE557[REDACTED]	Old Path	• [REDACTED]ver.jpg
Command Line	• "C:\Program Files (x86)\Internet Explorer\IEXPL... Show More	ID	• B33706F[REDACTED]
User	• [REDACTED]	Created At	• 2021 12:31:47
Start Time	• May 3	Modified At	• 2021 12:31:47

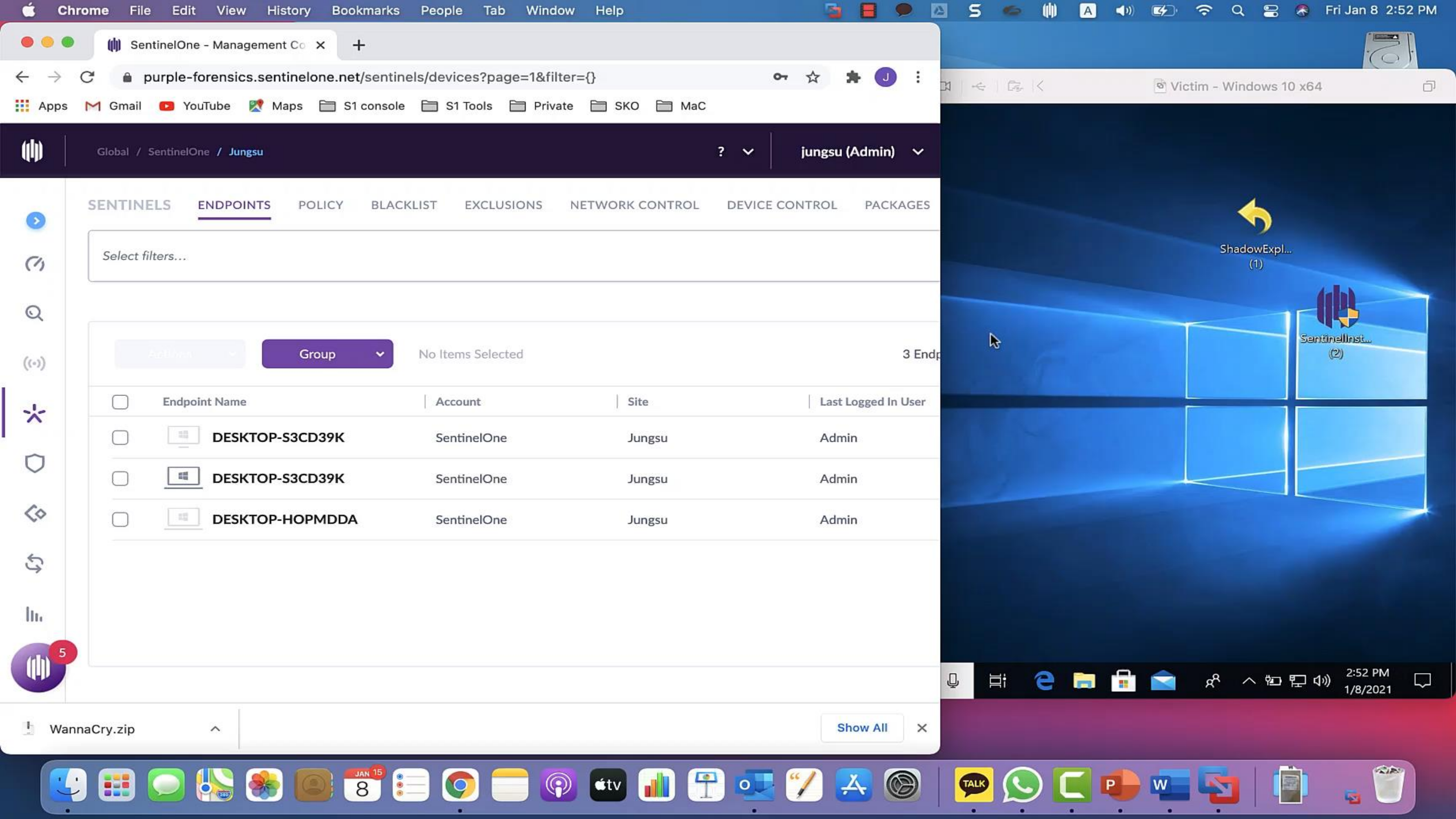
파일 암호화 수행
추가 악성 코드 설치 없이
브라우저 기반 공격

복구 기능



Shadow Explorer를 이용한 시점 복구

VSS는 Microsoft 서비스로 변경된 파일에 대해 복구를 지원하는 기능



SentinelOne - Management Co x +

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...

Applied 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 x

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

INITIATED BY	Agent Policy
ENGINE	Documents, Scripts
DETECTION TYPE	Dynamic
CLASSIFICATION	Malware
FILE SIZE	114.51 KB
STORYLINE	94337F29938C3DF3
THREAT ID	1071466887637071004

Events ▾ Max Results: 2000 ▾ Last 14 Days ▾ Expand query

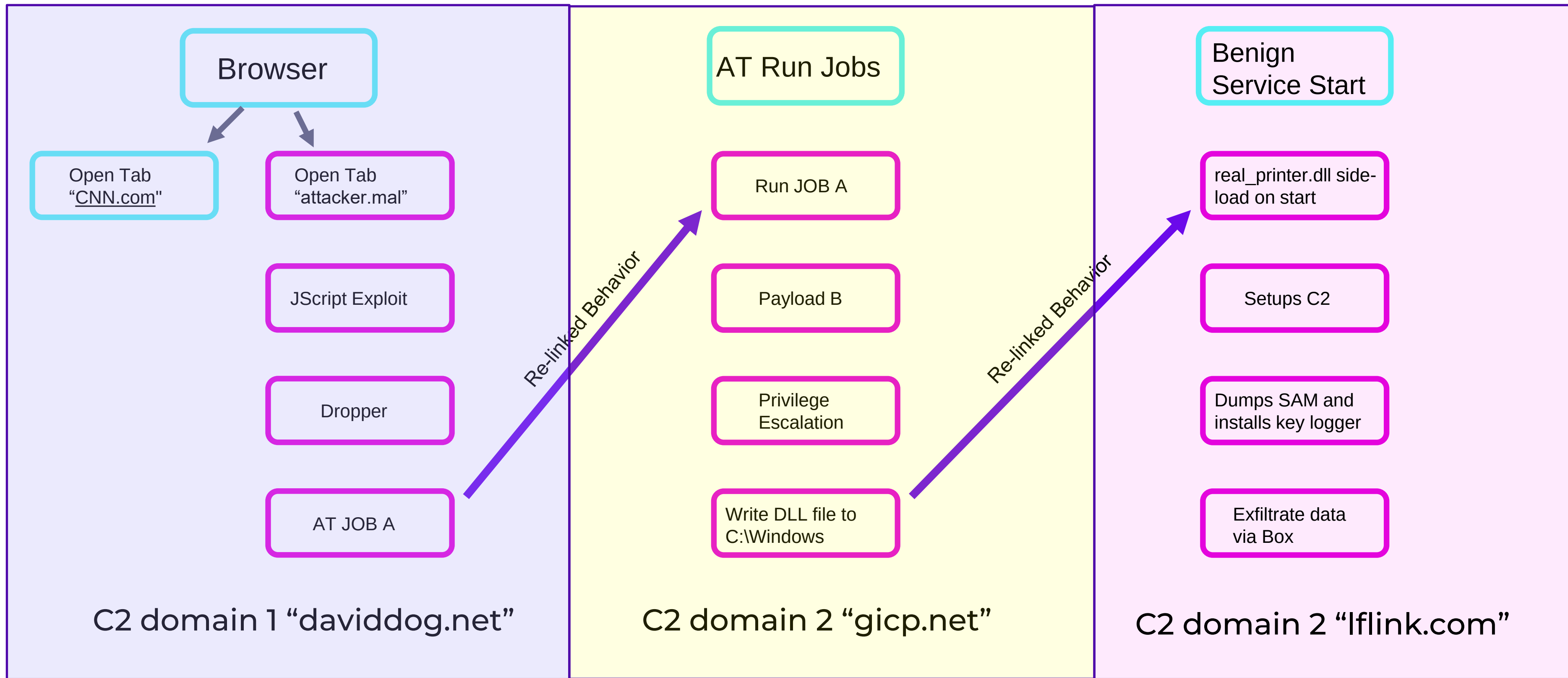
✓ 1 SrcProcStorylineId = "OC80F577697206E5" OR TgtProcStorylineId = "OC80F577697206E5"

All Events 653 Processes 4 Cross Process 11 Indicators 7 Files 31 Network Actions 4 DNS 3 Modules 593

Actions ▾ No Items Selected 653 Results 50 Results ▾

	Endpoint Name	Object Type	Source Process Relat...	Event Type	Event Time ▲	Source Process N...
▾ ☐	 DESKTOP-...	PROCESS	True	Process Creation	Jan 18, 2021 17:19:57	explorer.exe
▾ ☐	 DESKTOP-...	CROSS_PROCESS	False	Open Remote Process ...	Jan 18, 2021 17:19:57	csrss.exe

SentinelOne Agent Data - Context Relinking

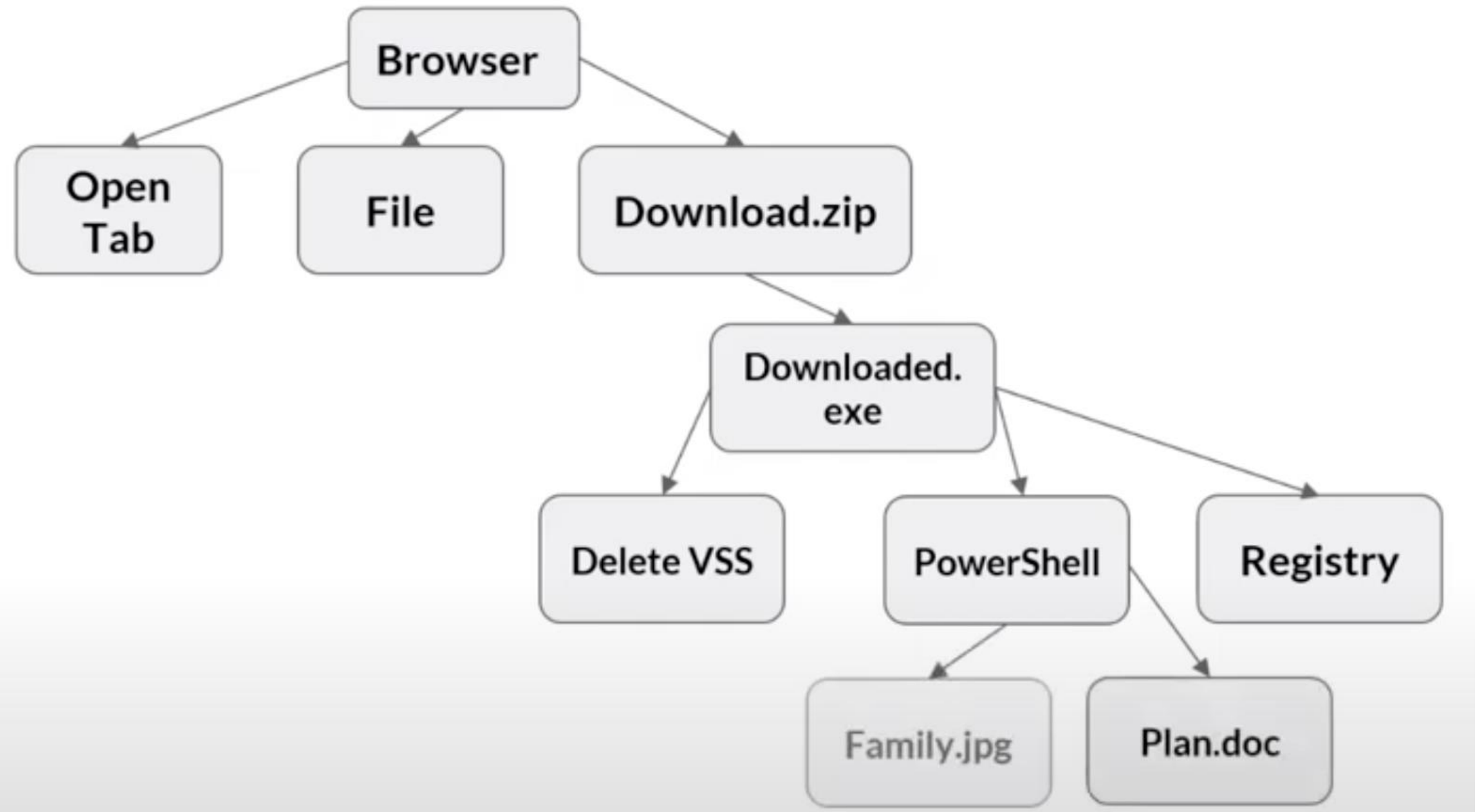


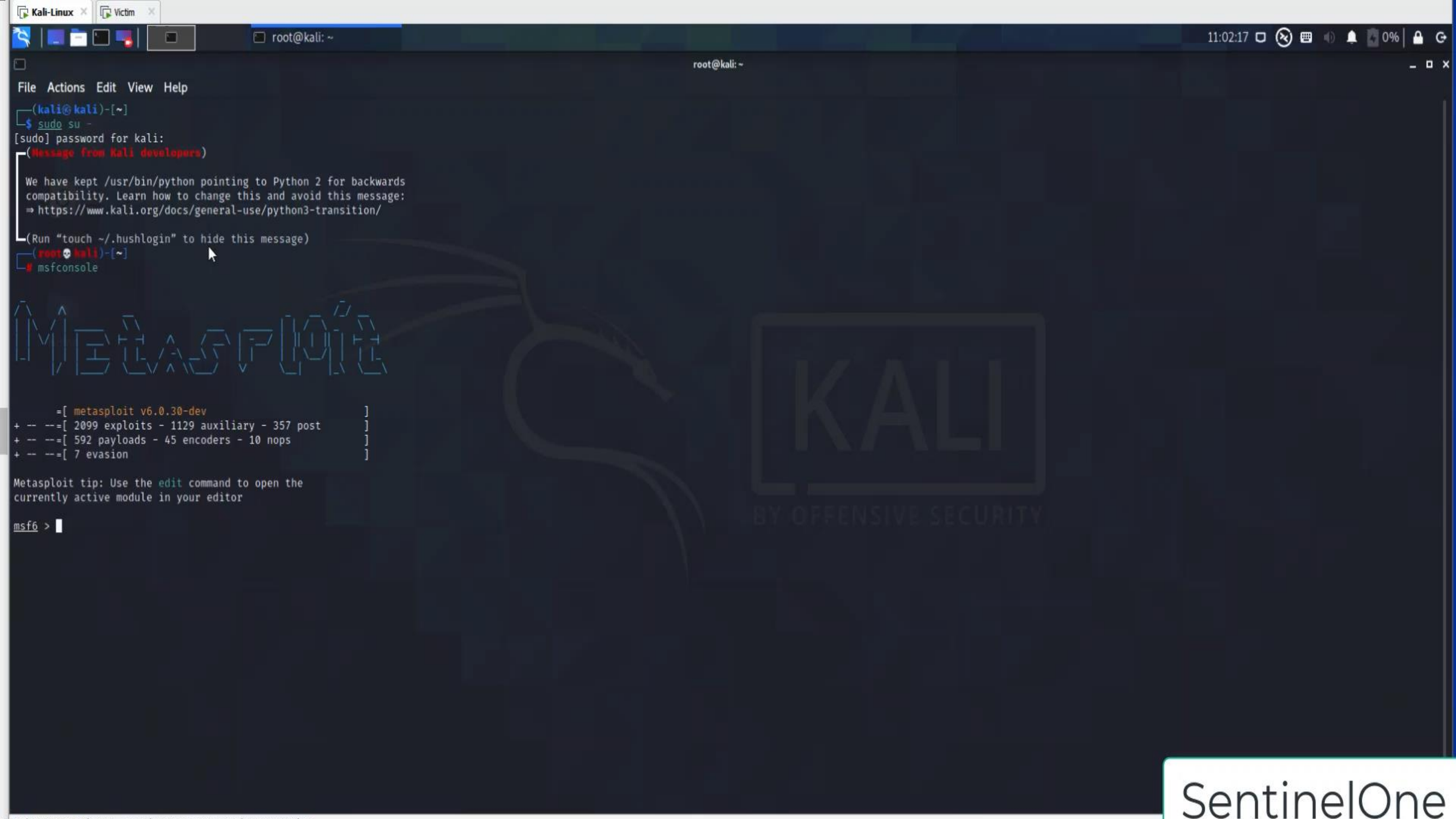
모든 활동은 Machine Learning 기반 StoryLine을 통해 Context 기반 탐지 지원

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
- 파워셸 이용 공격 시도
- 레지스트리 변경 시도





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

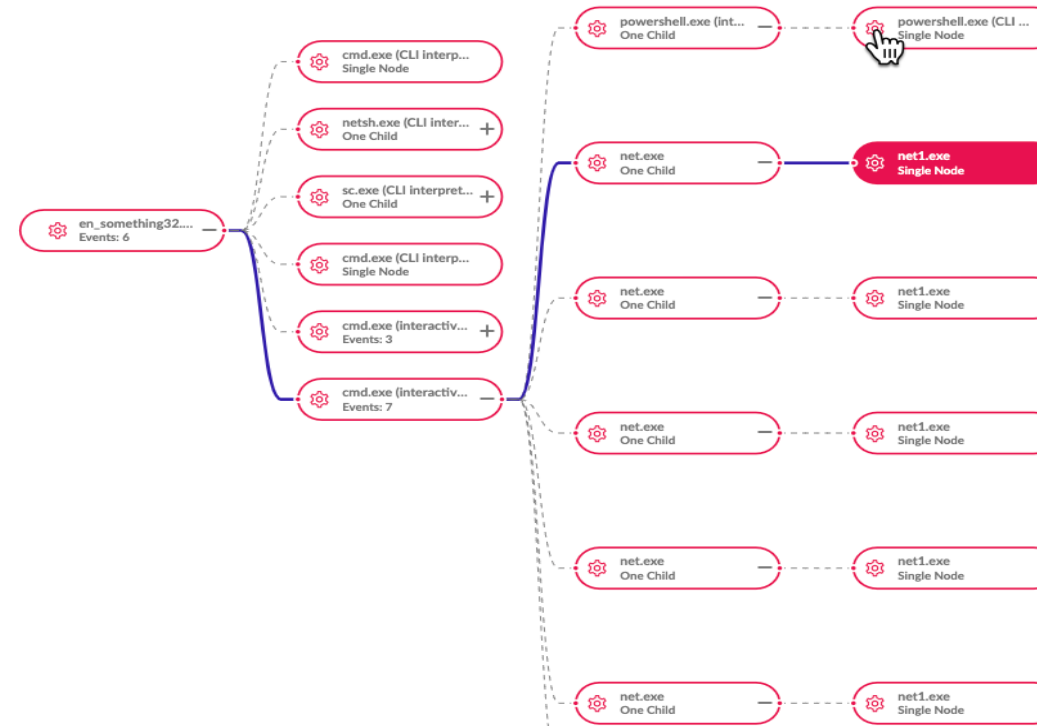
Application added firewall rules to allow network traffic.
MITRE : Exfiltration [T1041]
MITRE : Defense Evasion [T1562.004]

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 COUNTS

2
All Events

1 Processes

 1 Indicators

PROCESS SUMMARY

User: N/A

Name: net1.exe

UID: FBE84E99B132EC1D

ID: 3396

Command Line: user sysadmin

Image Path: \Device\HarddiskVolume4\Windows\SysWow64\net1.exe

SHA1: 382169595d5bb535c4575b3ec8cc
7e5e933115

Root: False

Events for en_something32.exe (5652) Clear Filter

All Events 12

Files 2

Network Actions 3

Processes 7

12 Items50 Results

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

1

SrcProcStorylineId = "FF23B77D12AA080A" OR TgtProcStorylineId = "FF23B77D12AA080A"

All Events1,162

Processes26

Cross Process141

Indicators910

Files30

Network Actions7

DNS1

Registry47

Actions

No Items Selected

1,162 Results

50 Results

Columns

	Endpoint Name	Object Type	Event Time	Source Process N...	Source Process St...	Source Pro...	Source Process Command Line
✓	sentinelone-s...	PROCESS	Mar 24, 2021 16:05:56	explorer.exe	4AAF897218CAAE9B	True	explorer.exe
✓	sentinelone-s...	CROSS_PROCESS	Mar 24, 2021 16:05:56	csrss.exe	8639CF65F3C82337	False	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=...
✓	sentinelone-s...	CROSS_PROCESS	Mar 24, 2021 16:05:56	svchost.exe	E776B307101D774A	False	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
✓	sentinelone-s...	CROSS_PROCESS	Mar 24, 2021 16:05:56	svchost.exe	E776B307101D774A	False	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
✓	sentinelone-s...	INDICATORS	Mar 24, 2021 16:05:56	en_something32.exe	FF23B77D12AA080A	True	"C:\Users\Administrator\Desktop\en_something32.exe"
✓	sentinelone-s...	INDICATORS	Mar 24, 2021 16:05:56	en_something32.exe	FF23B77D12AA080A	True	"C:\Users\Administrator\Desktop\en_something32.exe"
✓	sentinelone-s...	INDICATORS	Mar 24, 2021 16:05:56	en_something32.exe	FF23B77D12AA080A	True	"C:\Users\Administrator\Desktop\en_something32.exe"

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

Deep Visibility Configuration

Collect this Deep Visibility data

☒ Enable Deep Visibility ?

Process ?

DNS ?

Registry Keys ?

Behavioral Indicators ?

Cross Process ?

File ?

IP ?

Scheduled Tasks ?

DLL Module Load ?

Data Masking ?

URL ?

Login ?

Full Disk Scan ?

Command Scripts ?

✓

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")

✓

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).*"

엔드 포인트 내 발생하는 다양한 이벤트 로깅

다양한 검색 조건을 통한 검색 지원
악성 행위 탐지 시
차단, 격리 등 대응 방안 지원

 SentinelOne™

©2020 SentinelOne, All Rights Reserved.

29

The Real Storyline & ActiveEDR

Load Query ▾ Save New Query

×

 Main Query

+

 Add Sub Query

Events ▾

Max Results: 2000 ▾

Last 14 Days ▾

Loading Mode: All Fields (Default) ▾

Expand query

1

SrcProcStorylineId = "d7ae1d71-8bb4-a1ce-7515-7bdc2e69d9a3" OR TgtProcStorylineId = "d7ae1d71-8bb4-a1ce-7515-7bdc2e69d9a3"

All Events 758

Processes 3

Indicators 2

Files 363

Network Actions 390

Actions ▾

No Items Selected

3 Results

50 Results ▾

	Endpoint Name	Source Process Name	Source Process StoryLin...	Object Type ^	Source Process ...	Event Type	Event Time	Source Process Command Line
▾ ☐	s1-agent-rfcqj	sh	d7ae1d71-8bb4-a1ce-7515-...	PROCESS	☒ True	Process Creation	Feb 24, 2021 08:25:54	sh -c ping -c 4 127.0.0.1 && cat /etc/shadow
▾ ☐	s1-agent-rfcqj	apache2	d7ae1d71-8bb4-a1ce-7515-...	PROCESS		Process Creation	Feb 24, 2021 08:25:51	/usr/sbin/apache2 -k start
▾ ☐	s1-agent-rfcqj	sh	d7ae1d71-8bb4-a1ce-7515-...	PROCESS		Process Creation	Feb 24, 2021 08:25:51	sh -c ping -c 4 127.0.0.1 && cat /etc/shadow

Go to process tree

Exclude from search

Distinct event

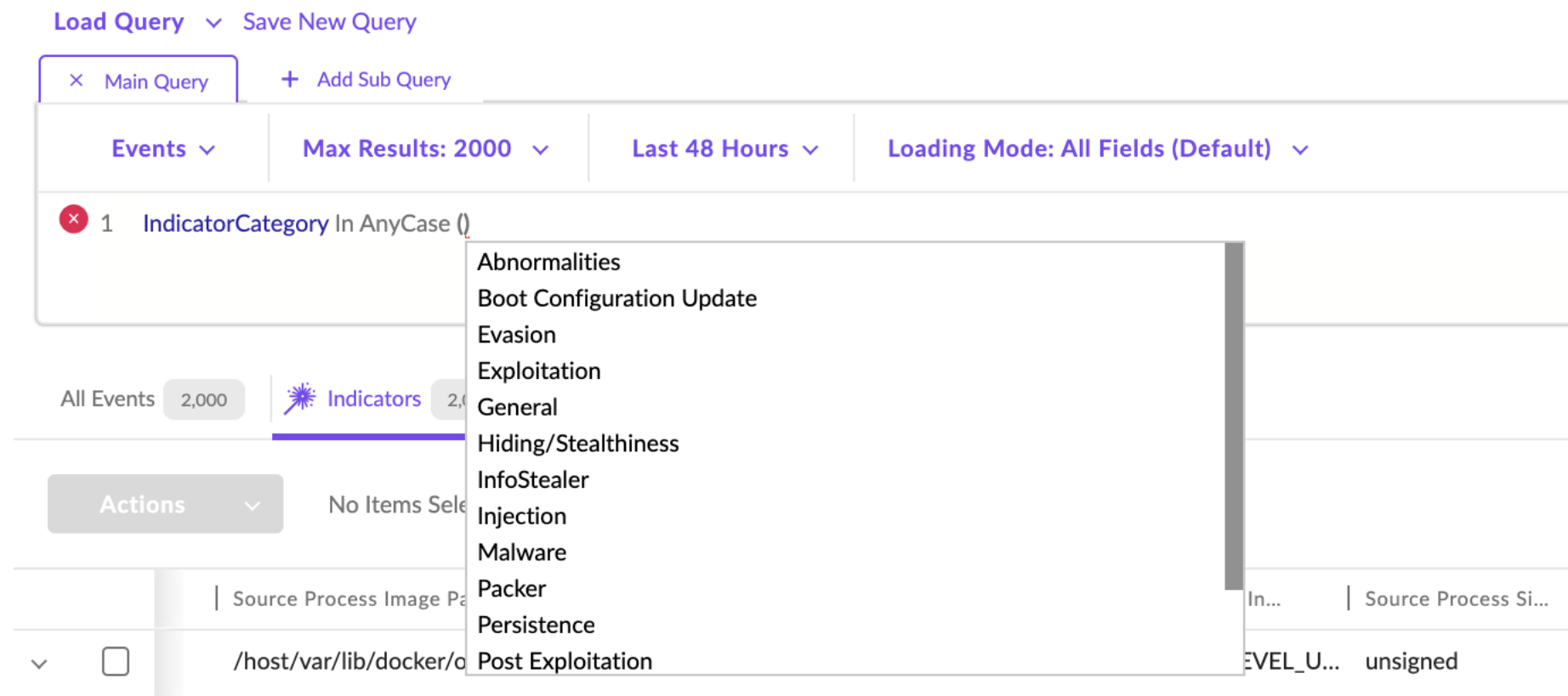
Add to Main Query

Copy to clipboard

Query Event's Storyline

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 Events998

Processes402

Indicators5

Files72

Network Actions519

Actions

No Items Selected

		Process 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}

		Process U...	Source Process In...	Source Process Si...	Source Process P...	Source Process P...	Indicator Name	Ind
✓	☐	f-4a6c-486e-...	INTEGRITY_LEVEL_U...	unsigned	N/A	kube-proxy	FileAndDirectoryDiscovery	Re
✓	☐	4-7d02-8835...	INTEGRITY_LEVEL_U...	unsigned	N/A	kube-proxy	FileAndDirectoryDiscovery	Re
✓	☐	1-243d-f8b4-...	INTEGRITY_LEVEL_U...	unsigned	N/A	kube-proxy	FileAndDirectoryDiscovery	Re
✓	☐	0-630c-3946-...	INTEGRITY_LEVEL_U...	unsigned	N/A	kubelet	FileAndDirectoryDiscovery	Re
✓	☐	45-2f27-9c2b-...	INTEGRITY_LEVEL_U...	unsigned	N/A	kube-proxy	FileAndDirectoryDiscovery	Re
✓	☐	a-cade-34b9-...	INTEGRITY_LEVEL_U...	unsigned	N/A	kubelet	FileAndDirectoryDiscovery	Re

PC 내에서 수행된
행위에 대한 Mitre기
Indicator정보 생성

향후 해당 IoC 기준
검색 지원

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

Near real-time hits

Active response

Carbon Black

Runs every ten minutes

Alert only

Crowdstrike

Runs periodically

Alert only

Create Custom Rule

Progress: Rule Details (active), Condition, Response, Summary

Rule Name
Data destruction behavior (25/100)

Description
(0/250)

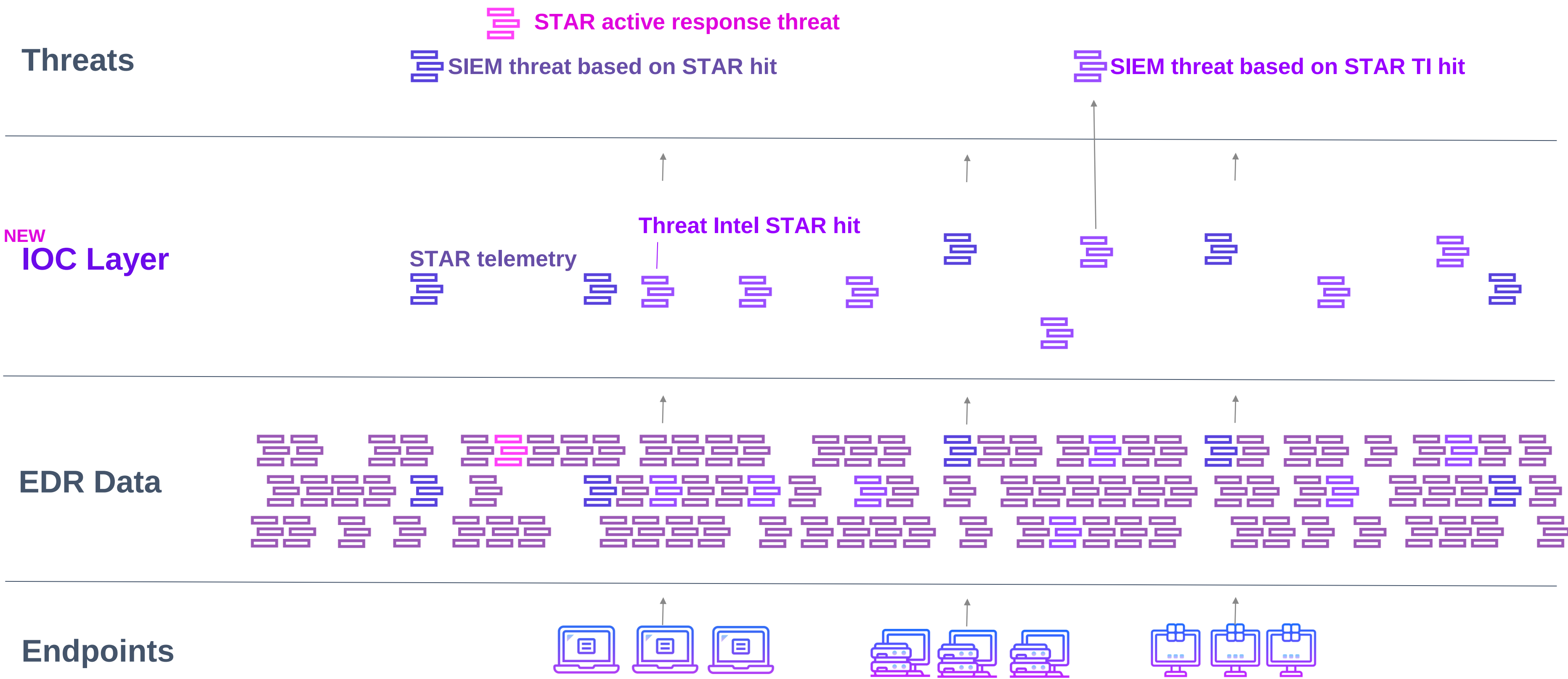
Rule Severity
Low

Rule Type
☐ Permanent ☒ Temporary

Expiration Date
Dec 06, 2021
You can set the rule to expire any day within 6 months from today.

Next

STAR 동작 레이어



STAR Workflow: 룰 생성 방식



Create Custom Rule

Rule Details Condition

* Rule Name

Test name 9/100

Description

0/250

Rule Severity

Low

Rule Type

☐ Permanent ☒ Temporary

Expiration Date

Dec 08, 2021

You can set the rule to expire any day with

Next

Create Custom Rule

Rule Details Condition Response

Scope: Global

Query Verification

Events

1 SrcProcName contains "powershell" AND EventType = "Module Load" AND TIndicatorSource IS NOT EMPTY

Back Next

Create Custom Rule

Rule Details Condition

Auto Response

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

☐ Suspicious Threat Policy ☒ Malicious Threat Policy

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

Back

Create Custom Rule

Rule Details Condition Response

Rule Name: Test name Rule Severity: Low Rule Type: Temporary

Expiration Date: Dec 8, 2021

Condition

Scope Hierarchy: Global Query Type: Events

Query: SrcProcName contains "powershell" AND EventType = "Module Load" AND TIndicatorSource IS NOT EMPTY

Response

☒ Treat as a threat: Malicious Threat Policy

☐ Activate rule immediately after saving

Back Save Draft

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"

< Threats / cmd.exe (interactive session)

OVERVIEW EXPLORE TIMELINE

Actions

Threat Status: NOT MITIGATED | AI Confidence Level: MALICIOUS | Analyst Verdict: Undefined | Incident Status: Unresolved

Identified Time: Jun 02, 2021 17:10:51
Reporting Time: Jun 02, 2021 17:10:51

No actions taken yet

First seen: Jun 02, 2021 17:10:51
Last seen: Jun 02, 2021 17:10:51

Only 1 time on the current endpoint
1 Account / 1 Site / 1 Group

Find this hash on Deep Visibility
Hunt Now

THREAT NAME: cmd.exe (interactive session) [Copy Details](#)

Path	N/A	Initiated By	Agent Policy
Command Line Arguments	N/A	Engine	Intrusion Detection
Process User	.	Detection type	Dynamic
Publisher Name	N/A	Classification	Hacktool
Signer Identity	N/A	File Size	N/A
Signature Verification	NotSigned	Storyline	
Originating Process	explorer.exe	Threat Id	

THREAT INDICATORS (3) NOTES

Custom Rules

- Possible Data Destruction
Possible data destruction behavior underneath PowerShell, MITRE - T1485
[View Rule](#) [View Alerts](#)

Post Exploitation

- PowerShell post-exploitation script was executed.
MITRE : Execution [T1059.001]

General

- Process started from shortcut file.
MITRE : Execution [T1204]

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"

Rule Details

Rule Name: PowerShell using FTP protocol

Description: The use of the legacy FTP protocol from PowerShell scripts (T1059) are quite likely an indicator of evasion or data exfiltration (TA0010) when using legacy FTP (T1071.002)

Rule Severity: Low Rule Type: Temporary Expiration Date: Sep 9, 2021

Condition

Scope Hierarchy: Account Query Type: Events

Query: SrcProcName = "powershell.exe" and NetProtocolName In AnyCase ("ftp")

Rule Details

Rule Name: PowerShell using FTP protocol

Description: The use of the legacy FTP protocol from PowerShell scripts (T1059) are quite likely an indicator of evasion or data exfiltration (TA0010) when using legacy FTP (T1071.002)

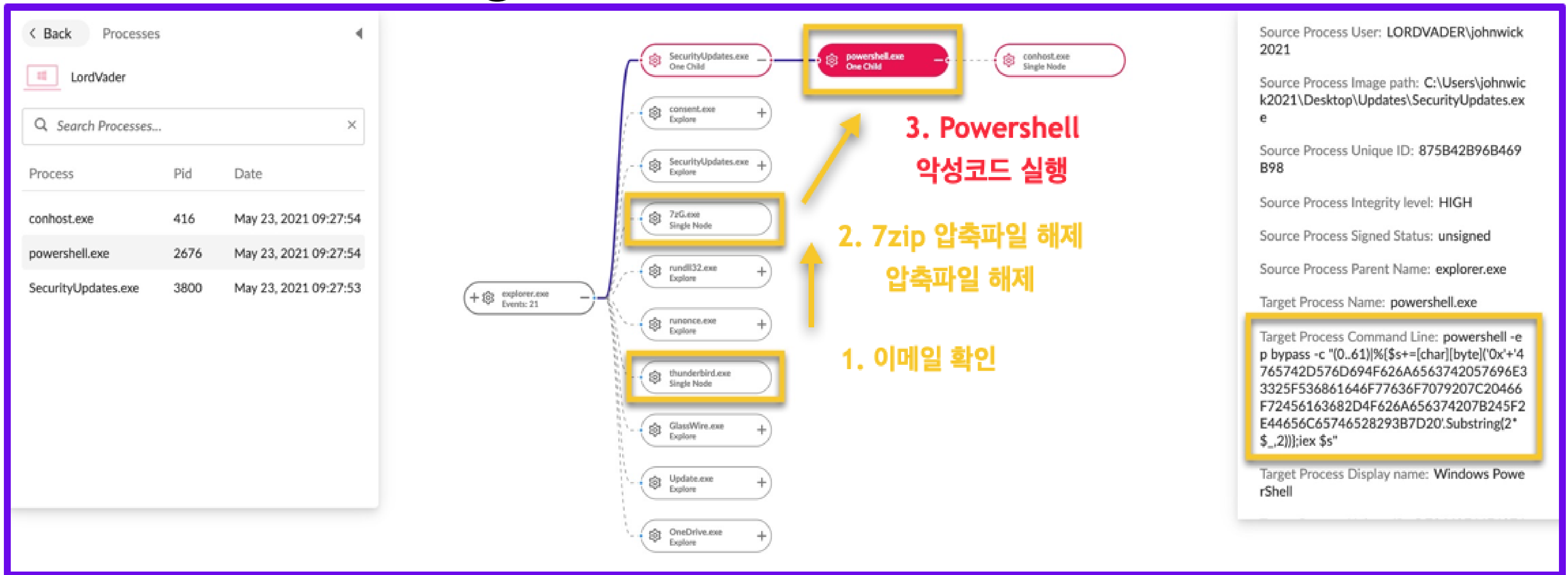
Rule Severity: Low Rule Type: Temporary Expiration Date: Sep 9, 2021

Condition

Scope Hierarchy: Account Query Type: Events

Query: SrcProcName = "powershell.exe" and NetProtocolName In AnyCase ("ftp")

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

Rule Details Condition Response Summary

Scope: Global

Query Verification Edit query ☐

Events ▾

1 ✓ SrcProcName = "mstsc.exe" AND SrcProcParentName = "powershell.exe" AND EndpointName = "..."

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

Auto Response

- ☐ Treat as a threat
If enabled, the Agent generates a threat from the alert and applies a selected policy.
- ☐ Network Quarantine
If enabled, the system automatically quarantines the alerted endpoints.
You can reconnect the endpoints from the Sentinels page or Endpoint Details.

S1 Control

Core

Control

Complete

Create New Rule

* Rule Name Field required

* OS Type

Windows

Linux

MacOS

✓ Windows

Tag as

Description

Scope SentinelOne -> Jungsu -> TEST

Action ☒ Allow ☐ Block

Protocol

Select Protocol

Search...

3PC

AH

A/N

ARGUS

ARIS

AX.25

[Reset](#)

윈도우, 맥 및 리눅스 통합관리

TCP/UDP 등 다양한 프로토콜 지원

S1 Control

Create New Rule

* Rule Name

Rule name...

✕

Field required

* OS Type

Windows

^

Linux

MacOS

✓ Windows

Tag as

Description

Scope

SentinelOne -> Jungsu -> TEST

Action

☒ Allow

☐ Block

Protocol

Select Protocol

▼

Search...

3PC

AH

A/N

ARGUS

ARIS

AX.25

Reset

S1 Control

Fallback

In SentinelOne network (global)

DNS Server NY (account)

Location기반 정책 관리

Application Path

Done

☐ All

☒ Path

C:\Program files\abc.exe

애플리케이션별 방화벽 정책 설정

S1 Control

Core

Control

Complete

Rule name	TEST
Interface	USB
Rule Type	Vendor ID Class Serial ID Product ID
Scope	
Action	☐ Allow Read Only ☐ Block

다양한 Rule Type 지원

Rule name	TEST
Interface	USB
Rule Type	Select rule type
Scope	SentinelOne -> Jungsu -> TEST
Action	☒ Allow Read & Write ☐ Allow Read Only ☐ Block

차단/읽기 전용/허용

S1 Control

Core
Control
Complete

TEST

Class

Serial ID

☒ Enable rule

0D Content Security

0E Video

0F Personal Healthcare

10 Audio/Video Devices

11 Billboard Device Class

12 USB Type-C Bridge Class

DC Diagnostic Device

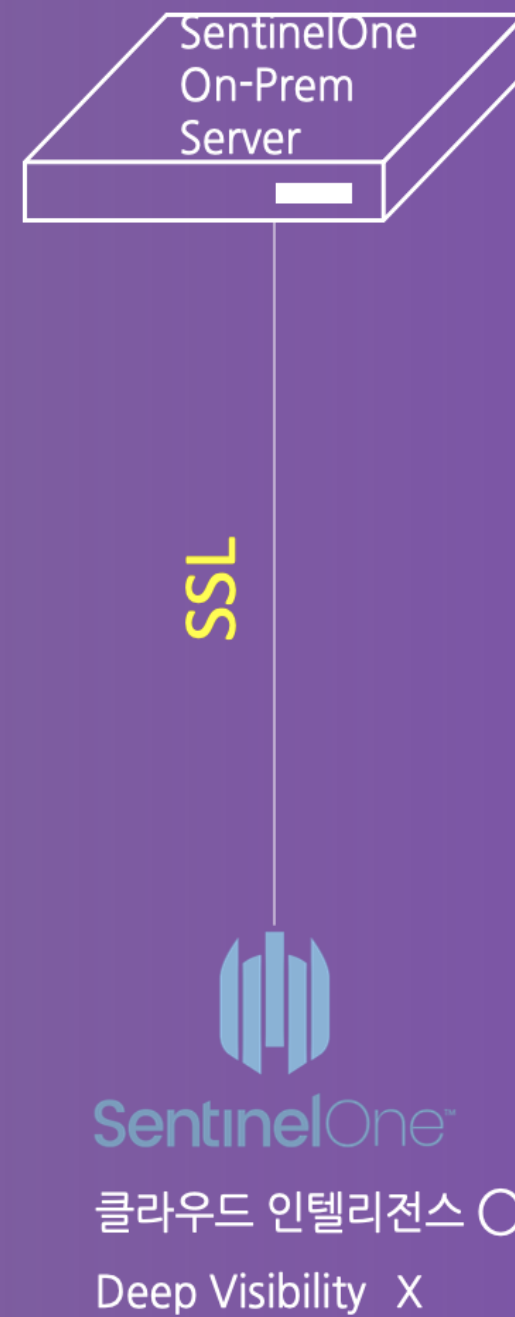
고객 요구사항에 따라
다양하게 설정할 수 있는
Class 지원

구성 방법

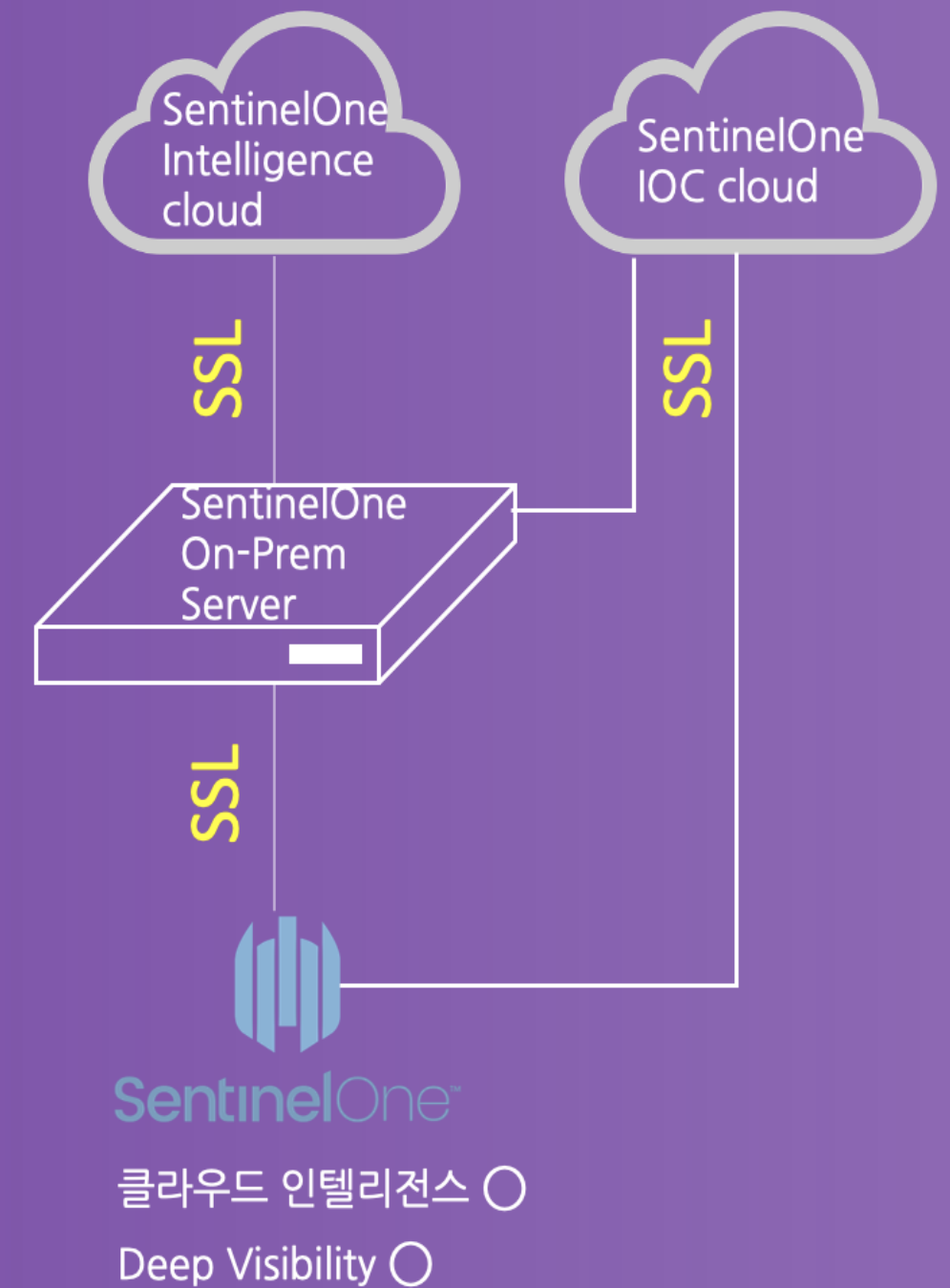
클라우드 Only(권장)



사이트 단독설치(On-Prem)

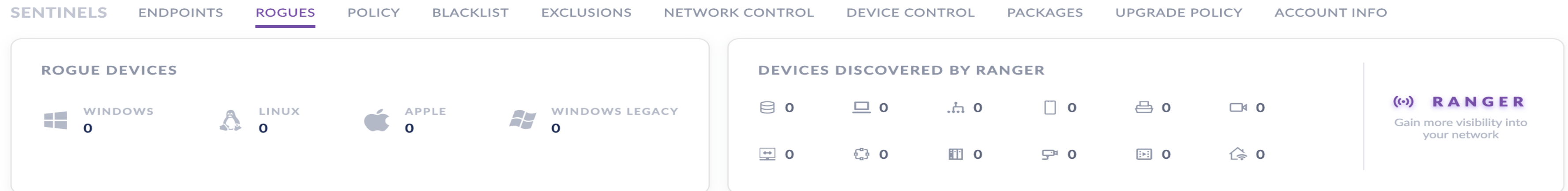


하이브리드

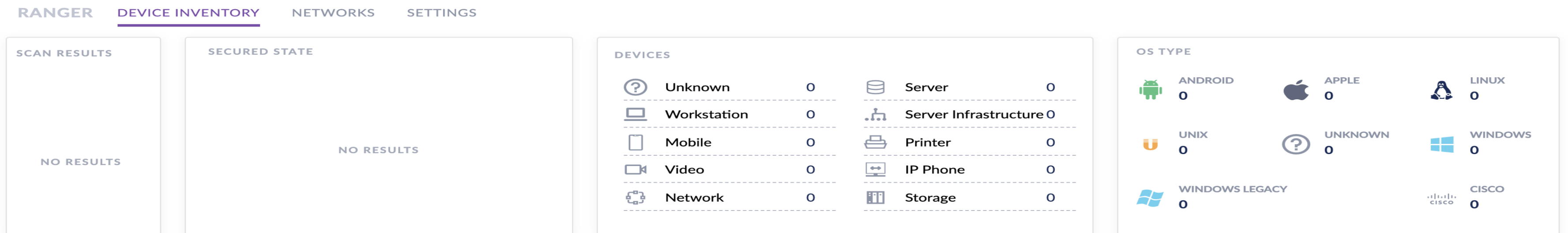


에이전트 미설치 단말 및 IoT 단말 검색

Rogue - S1 에이전트 미설치 단말 검색 및 격리



Ranger – IoT자산 검색 및 격리 (추가 라이선스 필요)



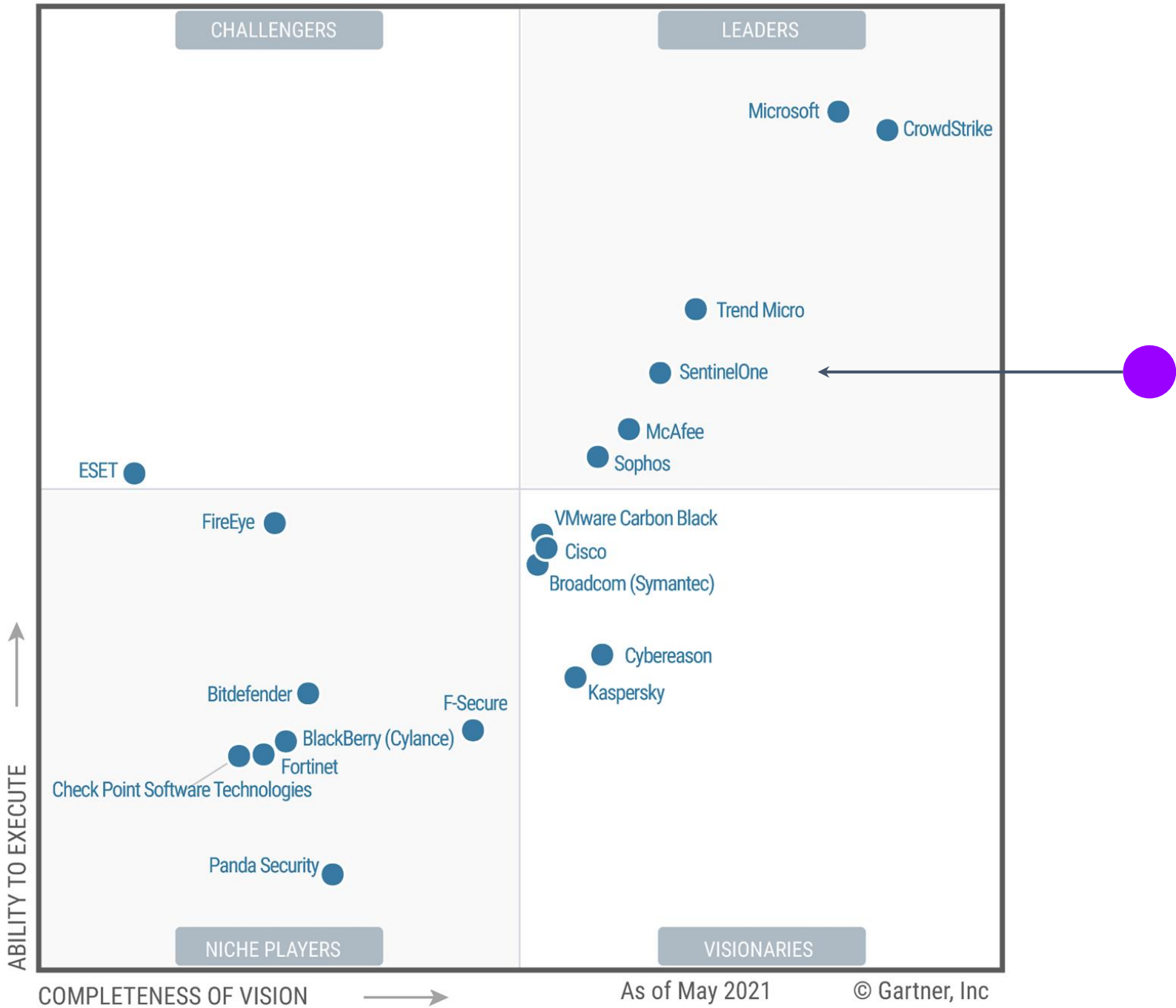


외부기관 평가

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

Disclaimer: Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner Critical Capabilities Scoring Elements

2021 Gartner Magic Quadrant for Endpoint Protection Platforms

- ✓

Ease of use
- ✓

Cloud management
- ✓

Prevention
- ✓

EDR functionality
- ✓

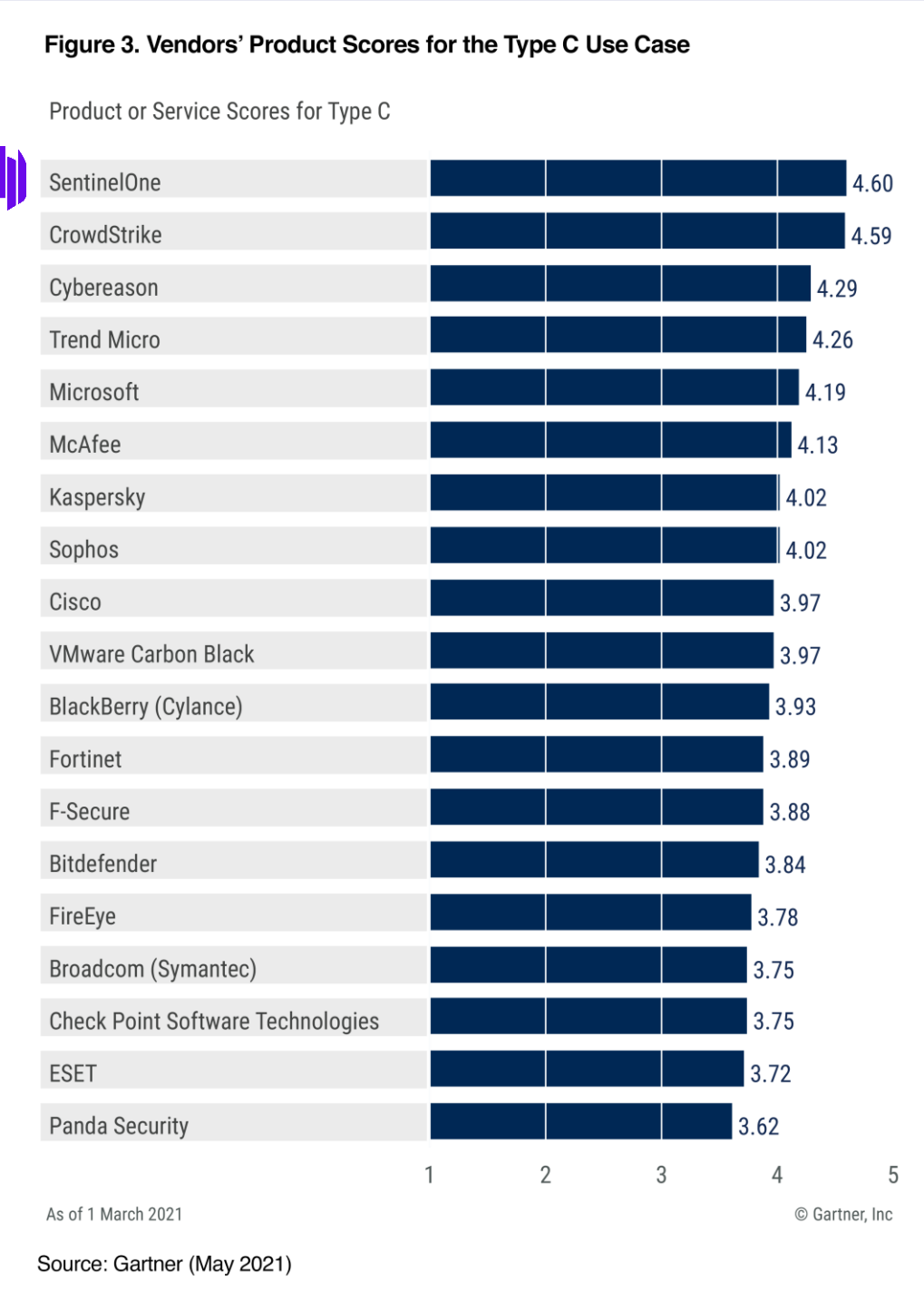
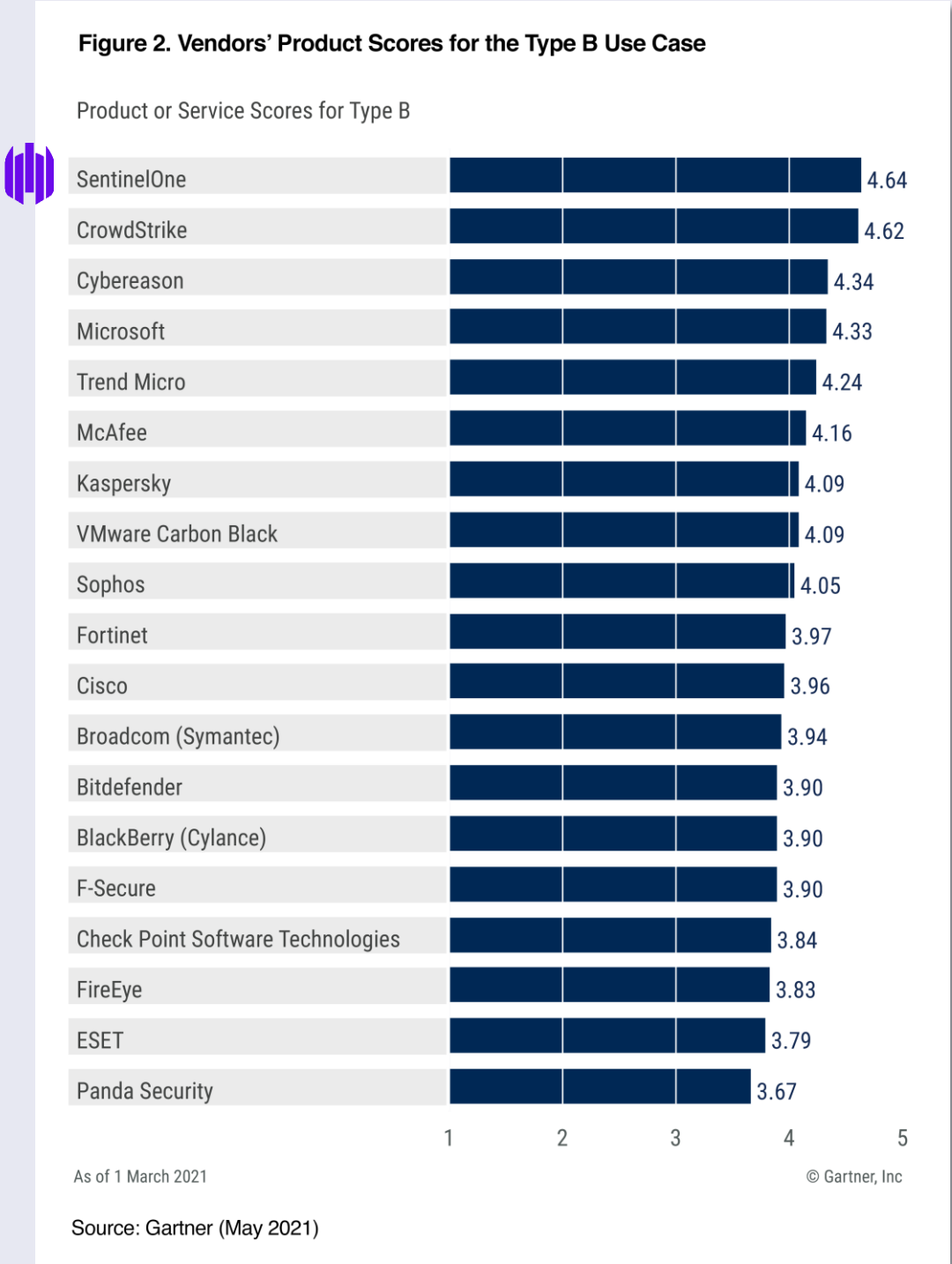
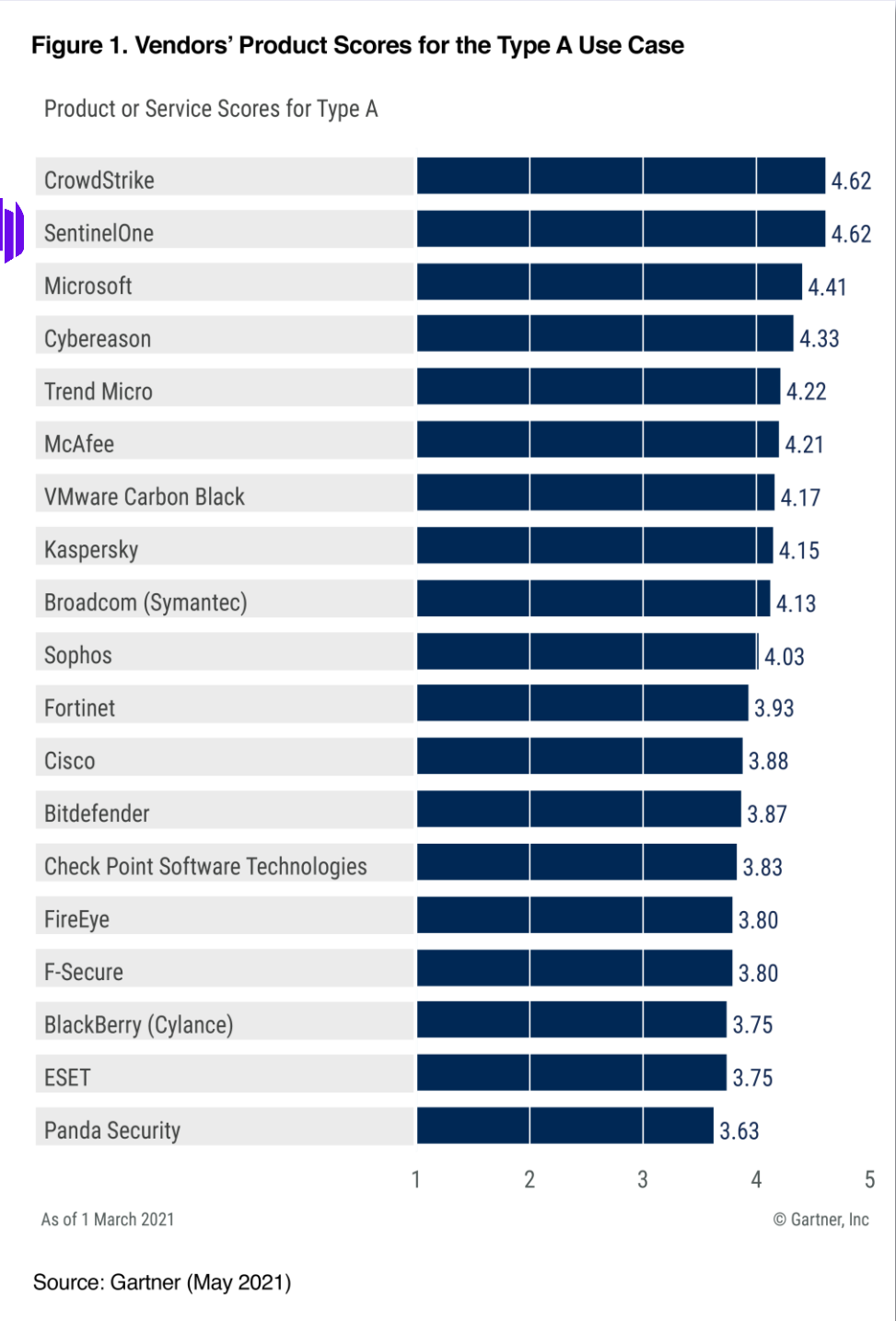
EPP suite
- ✓

Managed services
- ✓

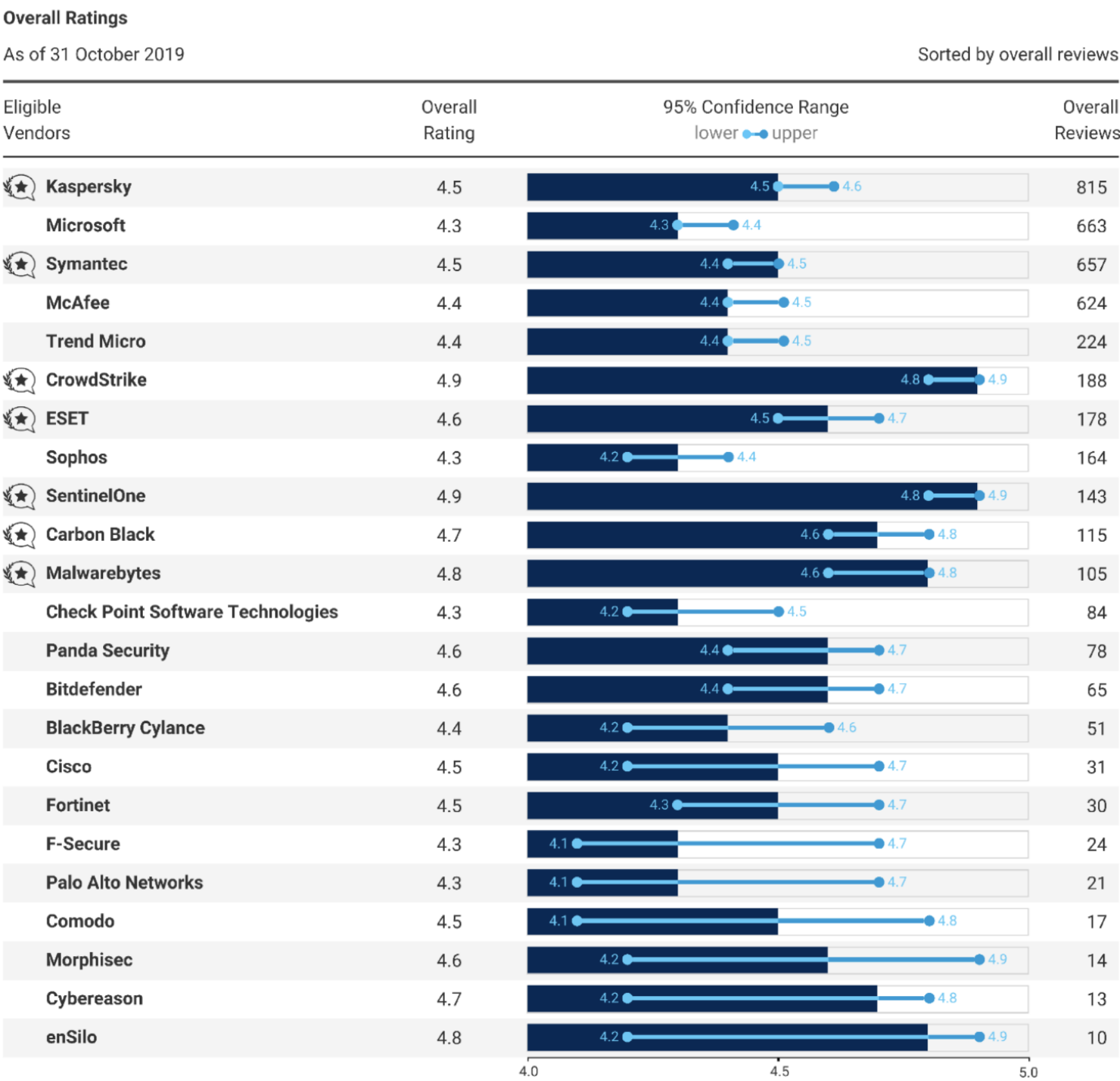
Geographic support
- ✓

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.”

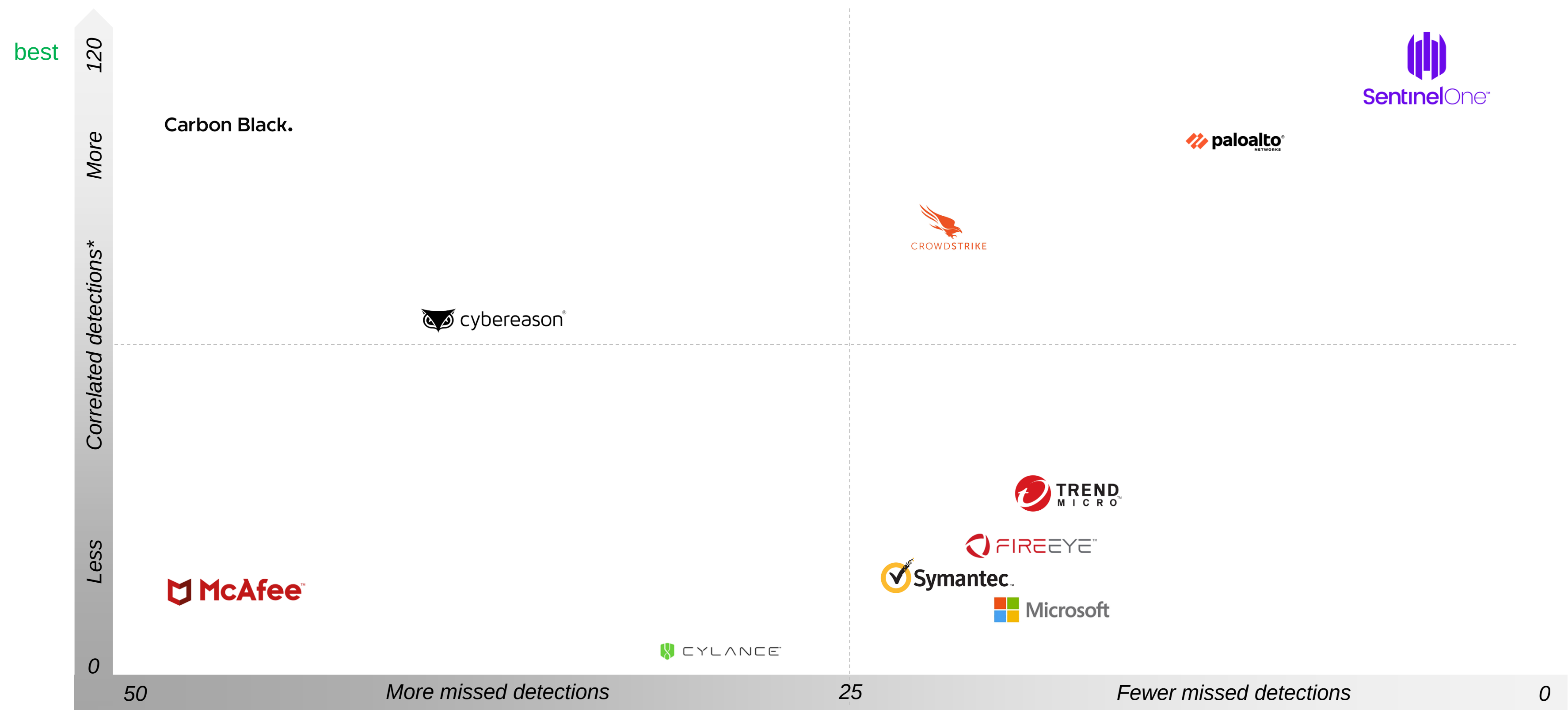


외부기관의 평가



MITRE ATT&CK Phase 2 Testing

SentinelOne Leads with Fewest Misses & Most Correlations



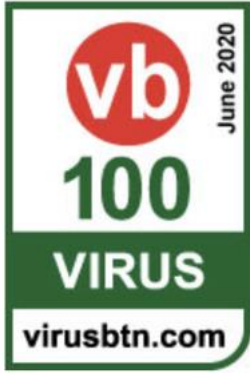
MITRE ATT&CK Phase 2 Results Data: <https://attackevals.mitre.org/evaluations.html?round=APT29>

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

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





SentinelOne™

Thank You