
SentinelOne
알려지지 않은 악성코드 분석을 위한 Threat Hunting의 새로운 기준, XDR
2023년 03월
SentinelOne Korea

현재 랜섬웨어 차단 솔루션이 가진 문제점은?

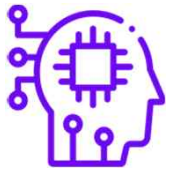
위협 가시성 부족

- 이미 유입된 위협 탐지 불가
- 랜섬웨어 유입 경로, 실행 이력 및 시스템 변경사항에 대한 가시성 확보 불가

알려지지 않은 랜섬웨어 탐지 불가

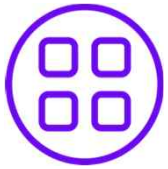
- 시그니처 기반의 한계로 알려 지지 않은 랜섬웨어 탐지 불가

자동 치료 및 복구 기능 부재



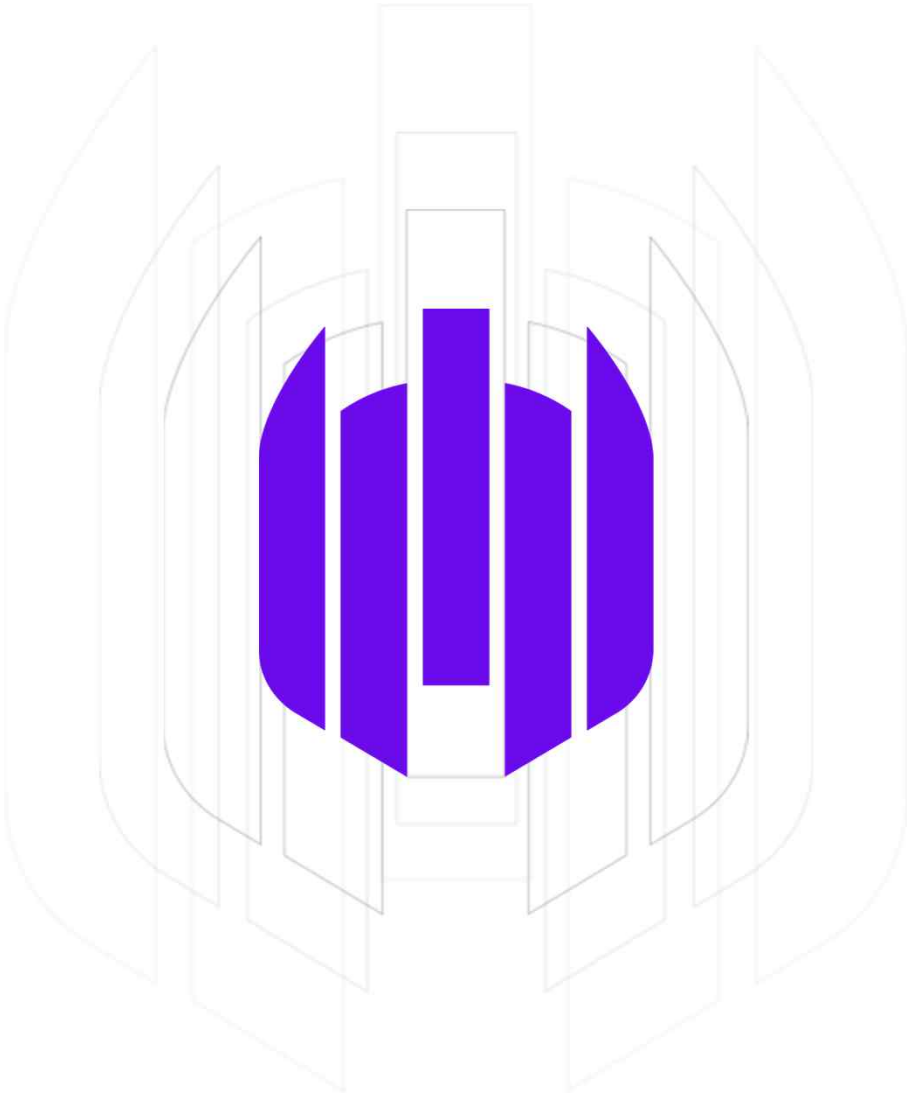
- 보안 전문가에 의한 수동 복구 또는 엔드포인트 포맷 및 OS 재설치 필요
- 랜섬웨어 감염 시 복구 불가

시그니처 DB 사이즈 증가로 관리 어려움



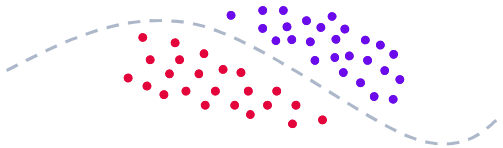
- 업데이트로 인한 네트웍 부하, 시스템 리소스 소모 증가

랜섬웨어를 효과적으로 차단하기 위해 필요한 기술은?



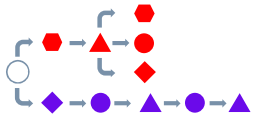
SentinelOne 기술 개요

실시간 파일 분석



머신러닝 for PEs & Docs

행위 기반 분석



Dynamic Behavioral Models

자동화된 대응 조치

- Kill & Quarantine
- App Control
- Disconnect / Isolate
- Attack Story Cleanup
- Full Rollback
- Works online & offline

EDR 및 대응

- Threat Hunting
- STAR Watchlists
- Fast queries. Highly scalable.
- Full attack storyline
- Mark entire story as threat
- MITRE ATT&CK™TTP hunt
- Full remote shell

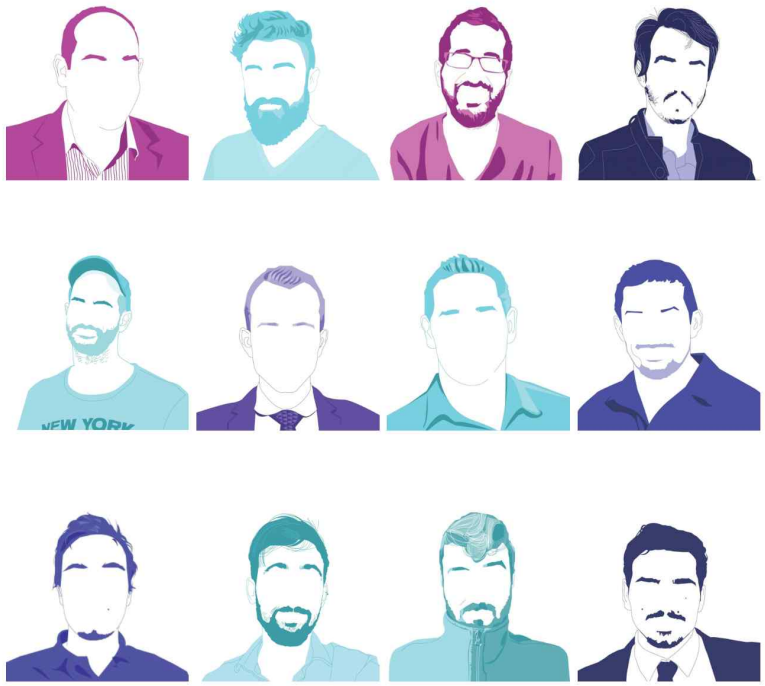
자율형 악성코드 차단 및 대응 + **교정 및 복구** | **위협 조사 및 대응**

- 처리시간: 대응까지 수초내 처리
- 단일 및 가벼운 에이전트
- 관리자 개입 없는 자율적 운영
- 지원범위: Windows, Mac, Linux, VDI, Cloud, Kubernetes/Docker

로그 저장 기간:
14일부터 최대 1년 지원
Full context and correlation
Integrated response workflow

SentinelOne 보안 기술 연구소

SelnelLabs 는 모든 플랫폼에서 사이버 범죄의 세계를 조명하는 위협헌터, 리버싱 엔지니어, 익스플로잇 개발자로 기여하며
더 안전한 디지털 라이프라는 공동의 사명을 강화하기 위해 툴, 컨텍스트, 인사이트를 공유합니다.



SentinelLABS

"사이버 보안 영역에서 취약점 발견하여 리포트"

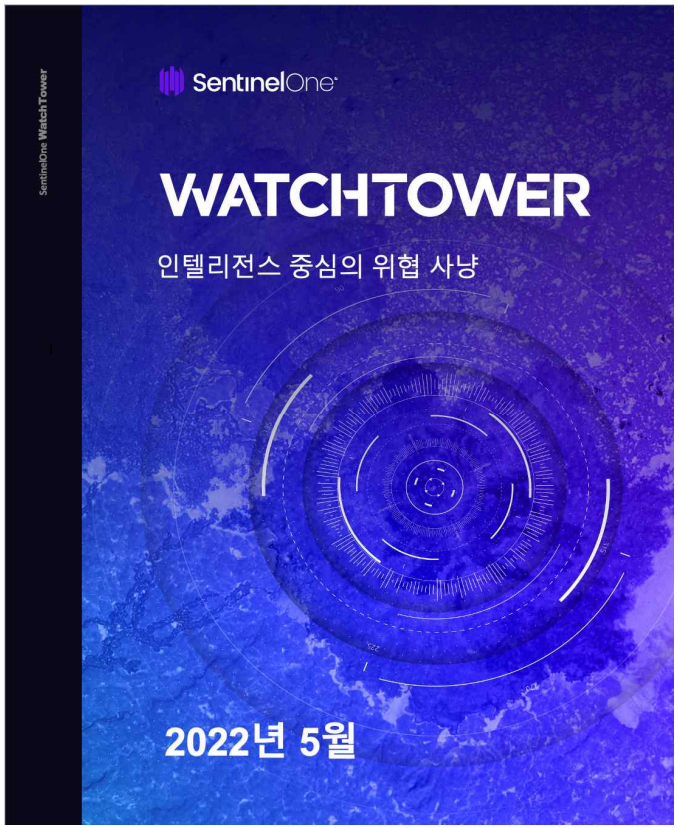
2021년 SentinelOne 보안 기술 연구소가 발견한 주요 취약점 (32개 Zero Day 취약점 보고)

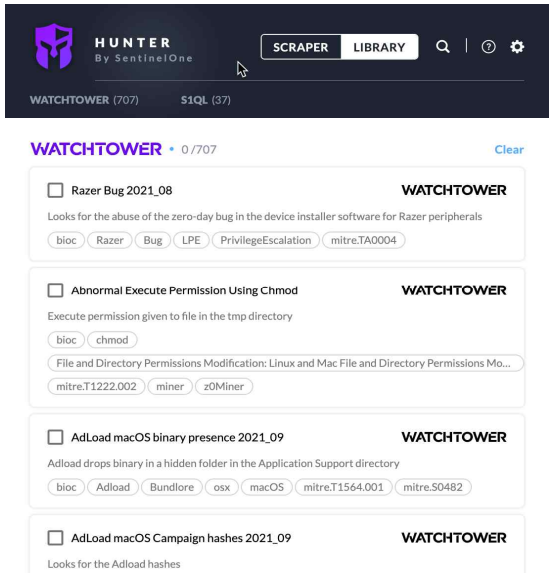
- CVE-2021-24092
  12 Years in Hiding – A Privilege Escalation Vulnerability in Windows Defender
- CVE-2021-21551
  Hundreds Of Millions Of Dell Computers At Risk Due to Multiple BIOS Driver Privilege Escalation Flaws
- CVE-2021-3438
  16 Years In Hiding – Millions of Printers Worldwide Vulnerable
- CVE-2021-36798
  New Cobalt Strike DoS Vulnerability That Lets You Halt Operations
- AWS Vulnerabilities
  USB Over Ethernet | Multiple Vulnerabilities in AWS and Other Major Cloud Services

SentinelOne

WATCH TOWER Service

WATCH TOWER는 센티넬원의 위협 헌팅 서비스입니다. 사이버 위협 인텔리전스 전문가, 위협 헌터, 분석가가 전 세계의 사이버 범죄에 대한 위협을 분석하여 TTP(전술, 기술, 절차)를 결정하고 헌팅 방법을 생성 및 실행합니다.





"랜섬웨어 최신 정보 매월 제공"

가장 활발하게 활동하고 있는 Lockbit 외 다수의 랜섬웨어 공격에 대한 분석 자료 및 전세계 사이버 보안 위협 정보 제공

- 3월 18일 LockBit 그룹은 48시간 내에 22개 조직을 해킹하는 데 성공했다고 보고
- 상용 도구에 의존하고 있음을 관찰
  - GMER 와 고급 포트 스캐너가 추가됨

LOCKBIT INCIDENT INVESTIGATION

INTRUSION	RECON	CREDENTIAL ACCESS	PERSISTENCE	LATERAL MOVEMENT	DISCOVERY	DEFENSE	EXFILTRATION
Email RDP	Net commands Ping WMI	Mimikatz	Schedule tasks GPO	PsExec Compromised domains and user accounts RDP CrackMapExec	ADFind	Process Hacker PC Hunter BATCH scripts to disable AV services. GPO to disable security settings	WinSCP SealthBit DataExfiltrator

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

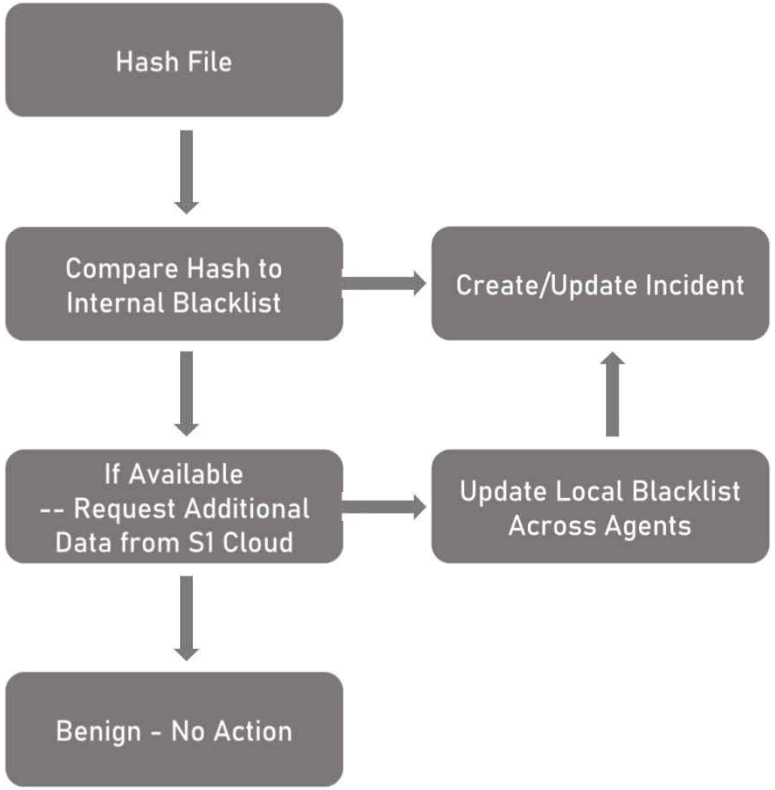
DEEP VISIBILITY
액티브 EDR

데이터 가시성
Storyline 기반 위협 헌팅

Reputation – 평판기반 엔진

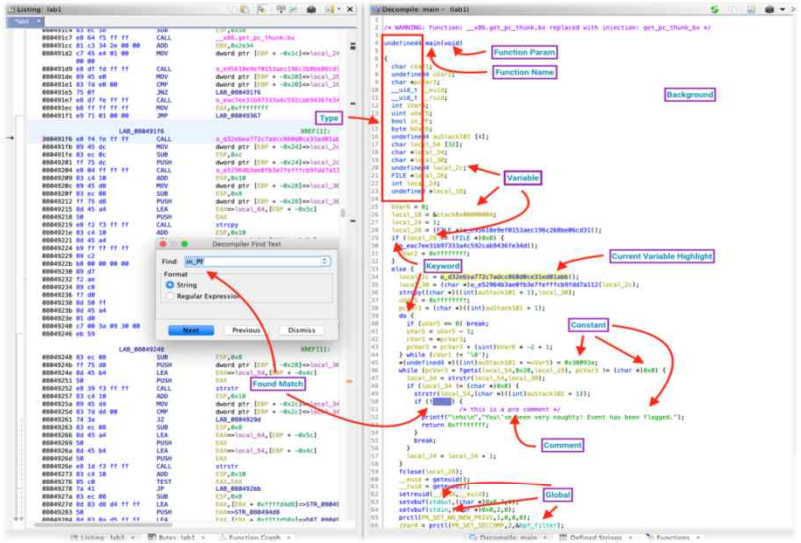
Reputation Engines

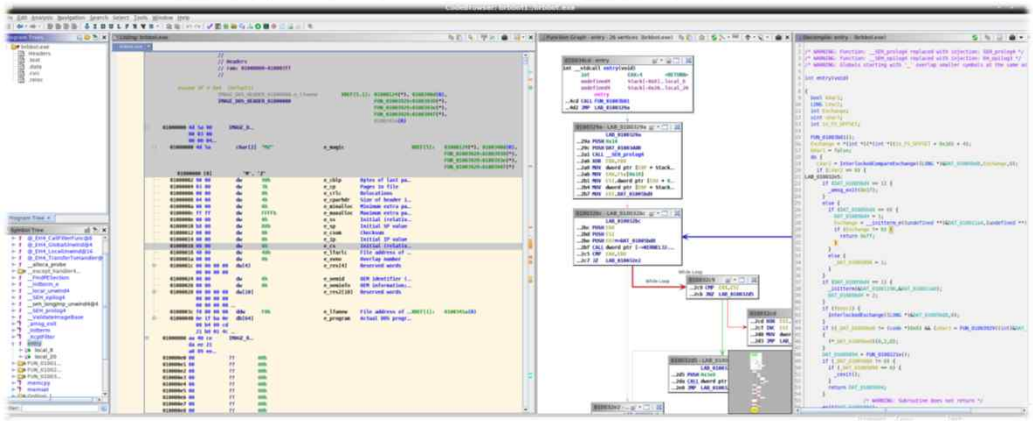
- 해쉬값 기반 분석
- 파일의 해쉬값을 확인 후 S1 cloud에 쿼리하여 동일 해쉬값을 차단 하는 기능
- 관리자에 의한 수동 등록 지원



Static AI 엔진 – 헤더 및 파일 구조 분석

AI Detection Engines



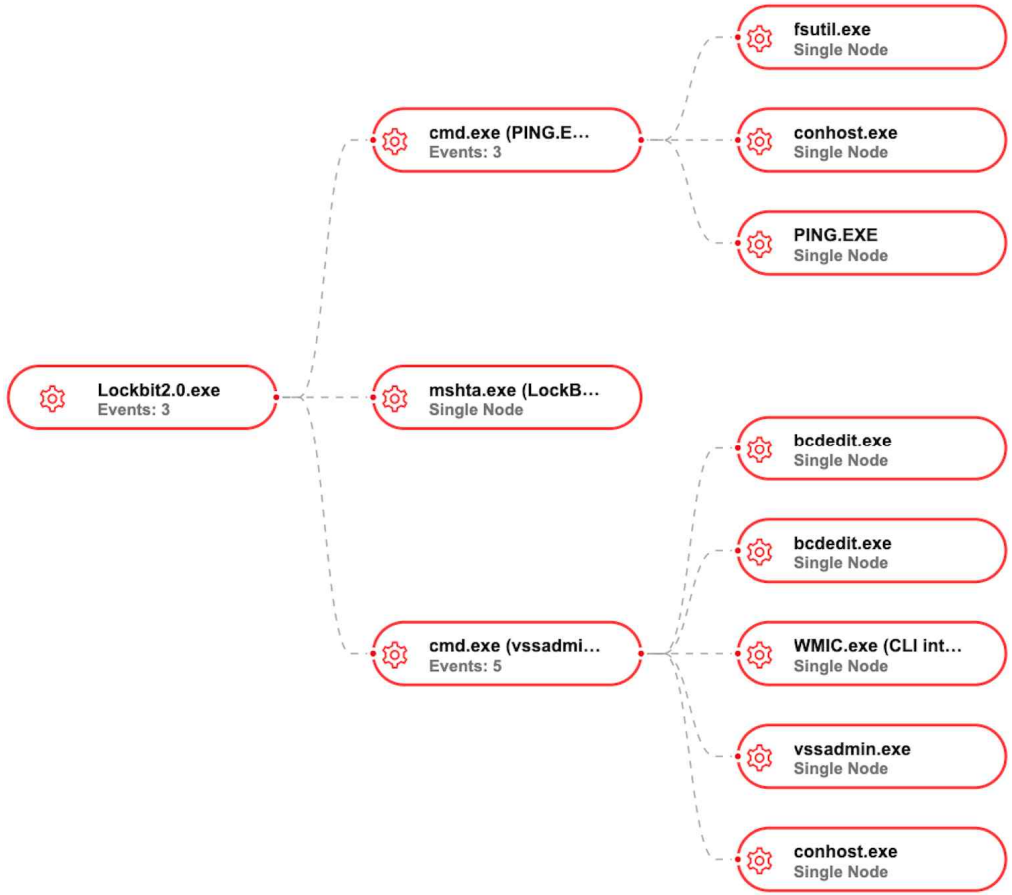


- 파일을 실행하지 않고 파일의 헤더 및 구조를 통한 악성 여부 파악
- 실행 없이 파일을 분석하므로 크기 및 APP 설치 유무에 상관없이 분석

Dynamic AI 엔진 – 행위 기반 탐지 (AI 머신 러닝)

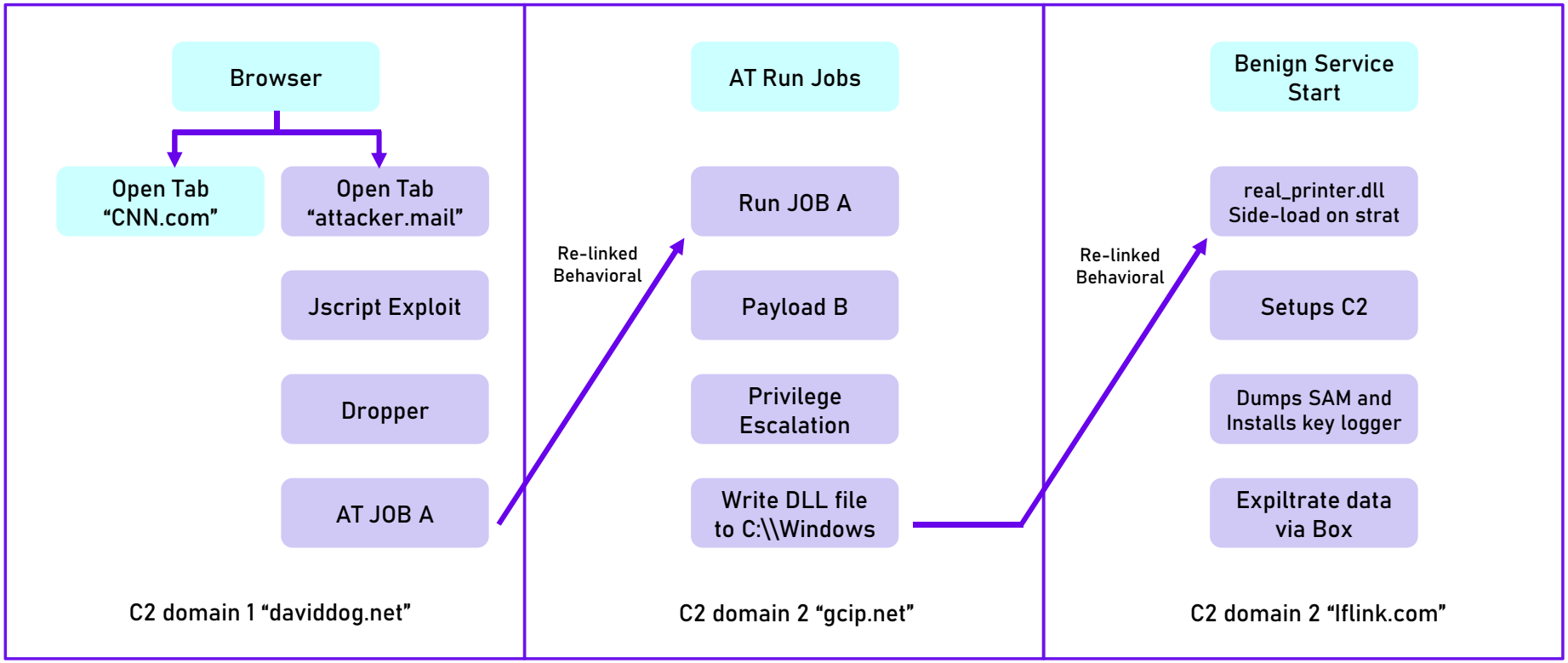
AI Behavioral Engines

- 파일이 실행될 때 AI 머신 러닝 기반 분석
- 파일 크기 및 종류와 무관
- 악성 행위 수행 시 실시간 탐지/차단

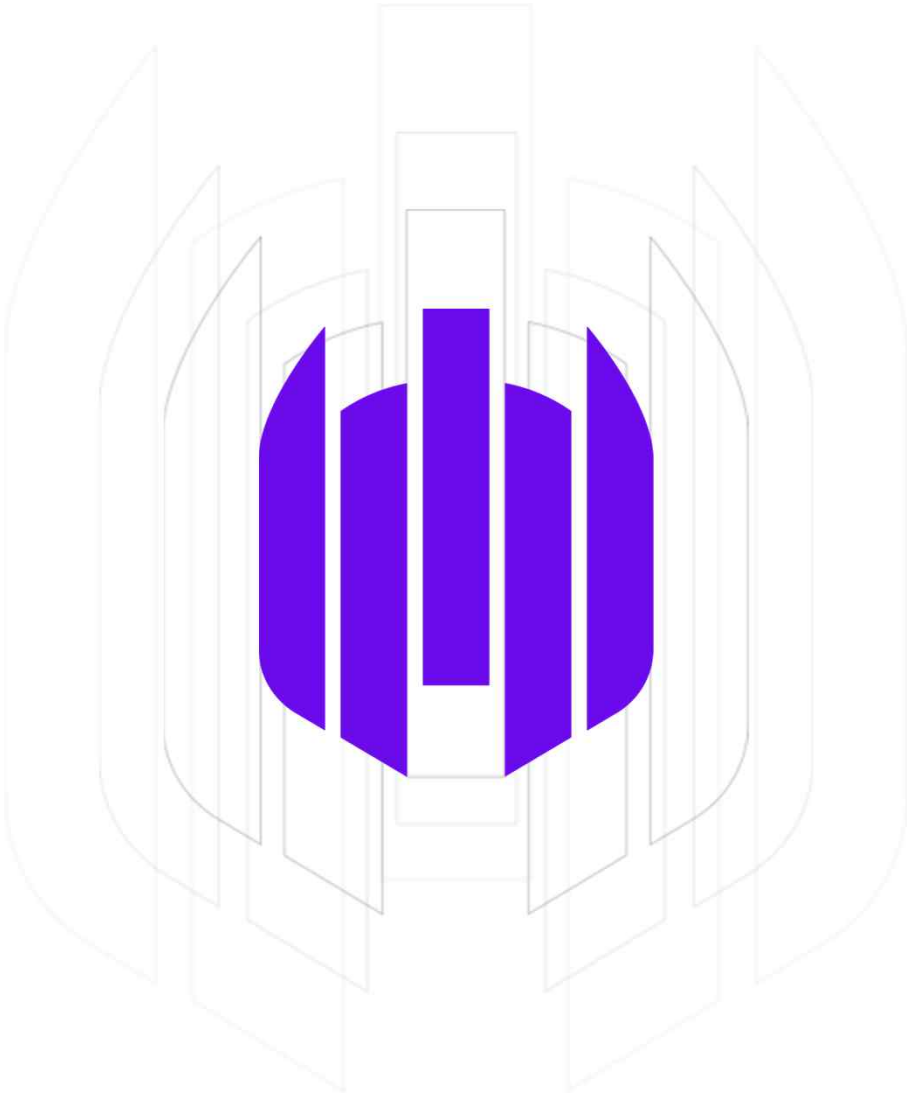


StoryLine – 행위의 상관관계 분석

모든 활동은 Machine Learning 기반 StoryLine을 통해 Context 기반 탐지 지원



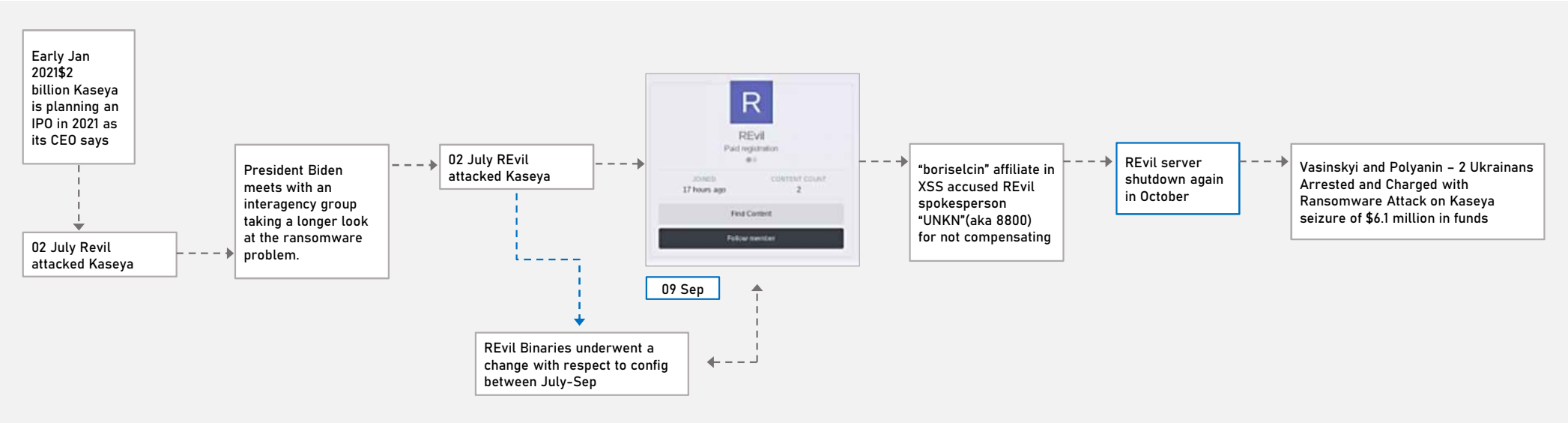
랜섬웨어 탐지 사례



랜섬웨어 탐지 사례 – Revil Ransomware

- **Revil 랜섬웨어 공격 과정**

1. 공격자가 원격접속
2. 피싱홈페이지를 이용하여 공격 파일 다운로드 유도
3. 사용자가 엑셀 매크로 파일 실행
4. UAC Bypass를 이용하여 권한 상승
5. 작업 스케쥴러에 원격접속 실행 등록
6. 사용자 추가 및 관리자 그룹에 추가
7. 서비스 중지 (spooler)
8. 문서 파일 다운로드, 삭제
9. REVIL 랜섬웨어 다운로드/실행



위협 헌팅 – EDR(Deep Visibility)

- 암호화된 파일 확장자 기준 암호화된 파일 검색

```
EventType = "File Modification"  and TgtFilePath Contains Anycase "i822q597"
```

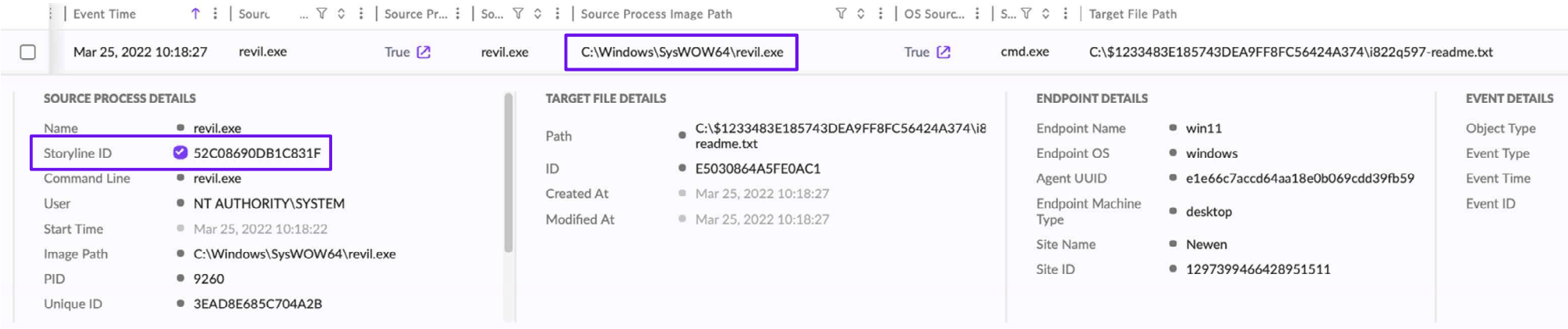
탐지된 이벤트 중
파일 변경 관련 이벤트 검색

확장자 중 랜섬웨어 암호화로 인해
“i822q597”로 변경된 파일 검색

Source Process Image Path	OS Source ...	S...	Target File Path
C:\Windows\SysWOW64\revil.exe	True	cmd.exe	C:\$1233483E185743DEA9FF8FC56424A374\i822q597-readme.txt
C:\Windows\SysWOW64\revil.exe	True	cmd.exe	C:\$B2016D368D854330A6C4247D2EFE2EE6\i822q597-readme.txt
C:\Windows\SysWOW64\revil.exe	True	cmd.exe	C:\$B3A8860855924478BE0134D353F0524F\i822q597-readme.txt
C:\Windows\SysWOW64\revil.exe	True	cmd.exe	C:\Documents\i822q597-readme.txt

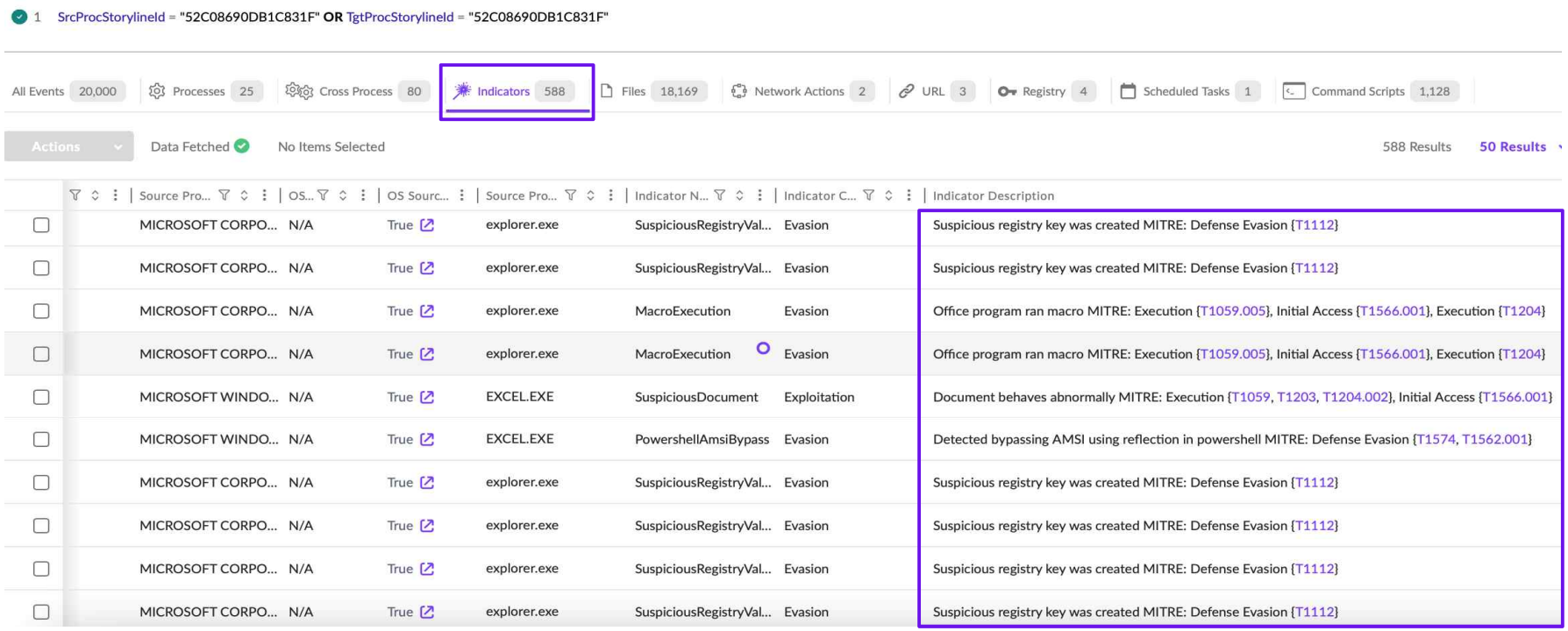
위협 헌팅 – EDR(Deep Visibility)

- 파일 암호화 수행 시 암호화 시킨 프로세스 확인
- REVIL.EXE와 관련 악성 행위 검색을 위한 StoryLine ID 확인



위협 헌팅 – EDR(Deep Visibility)

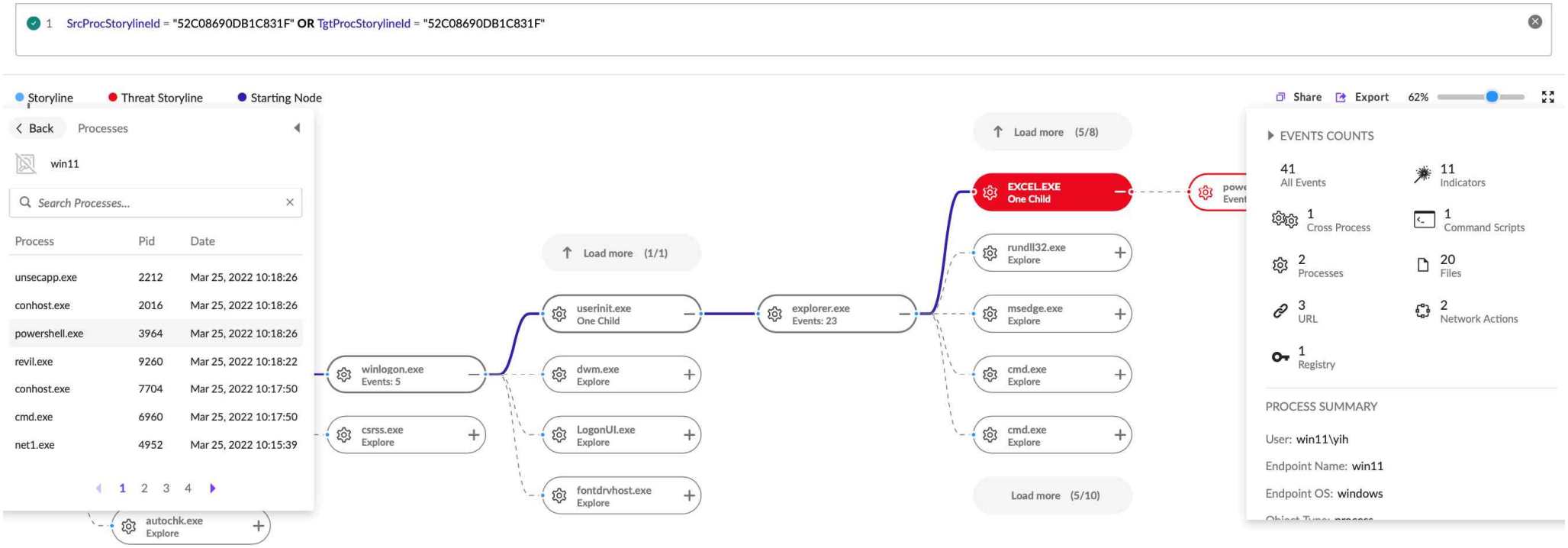
- StoryLine ID 기반의 검색 수행
- 공격자에 의해서 수행된 악성 행위(Indicators) 588건 탐지
- MITRE 기준 IoC 정보 제공



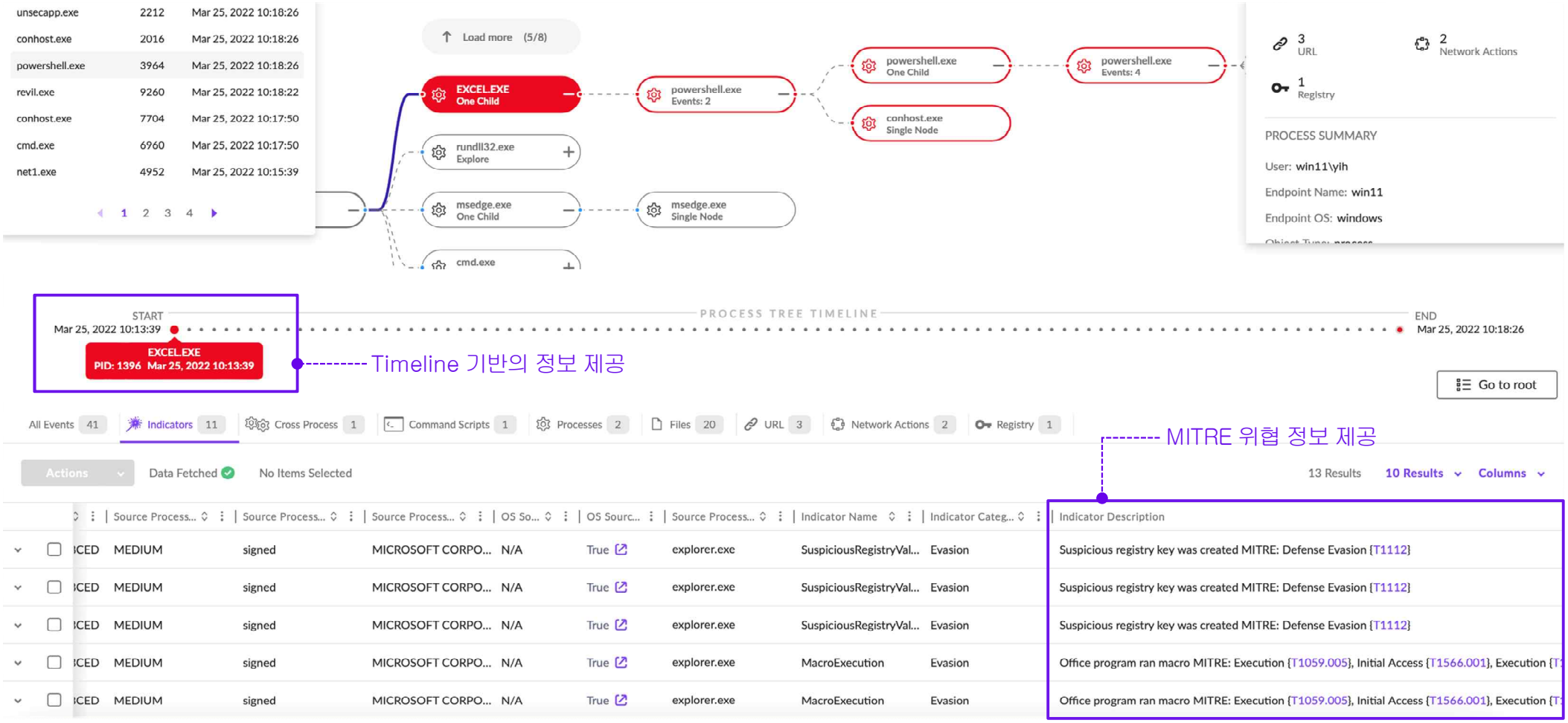
위협 헌팅 – StoryLine (스토리라인)

StoryLine

- StoryLine ID 및 관련 행위 검색

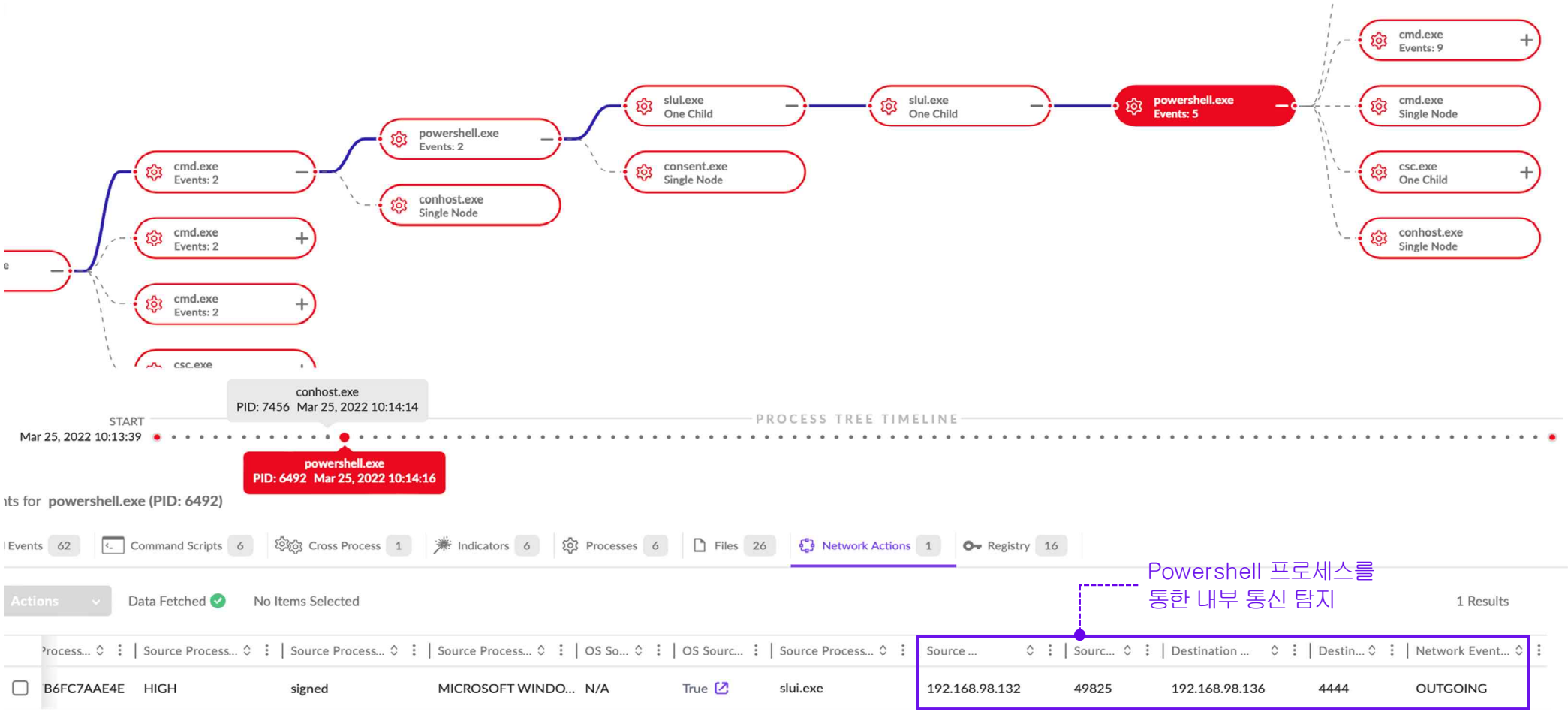


위협 헌팅 – StoryLine (스토리라인)



SentinelOne

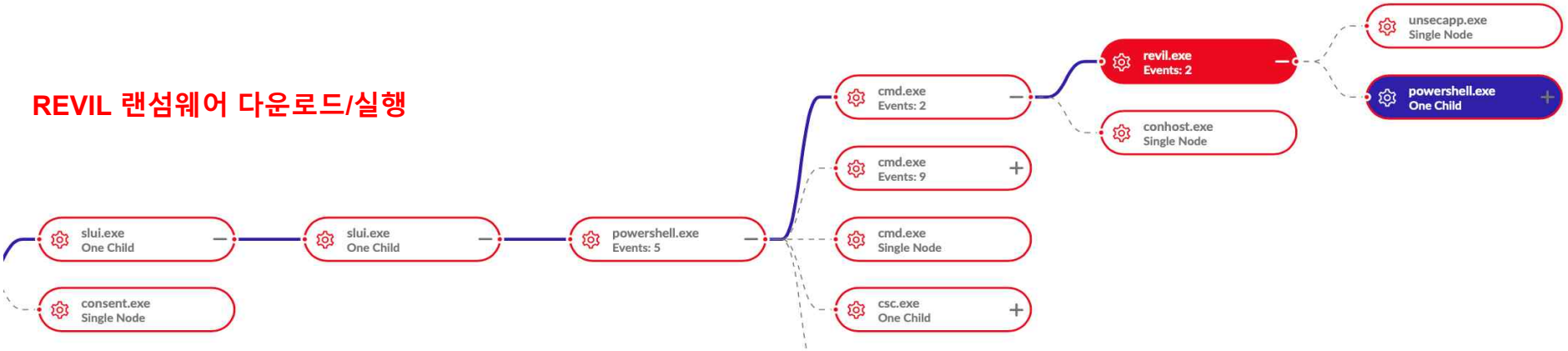
위협 헌팅 – StoryLine (스토리라인)

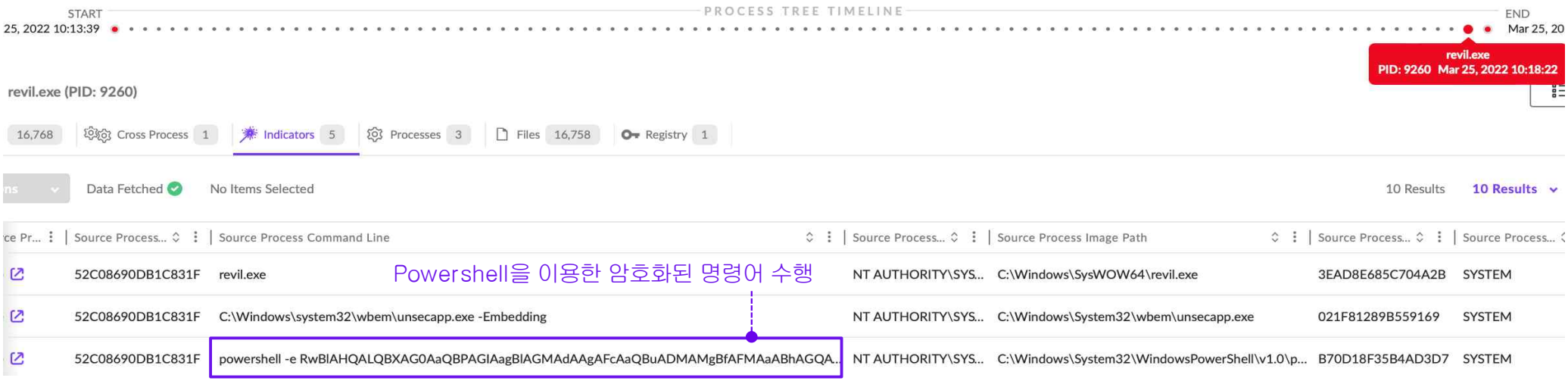


SentinelOne

위협 헌팅 – StoryLine (스토리라인)

REVIL 랜섬웨어 다운로드/실행

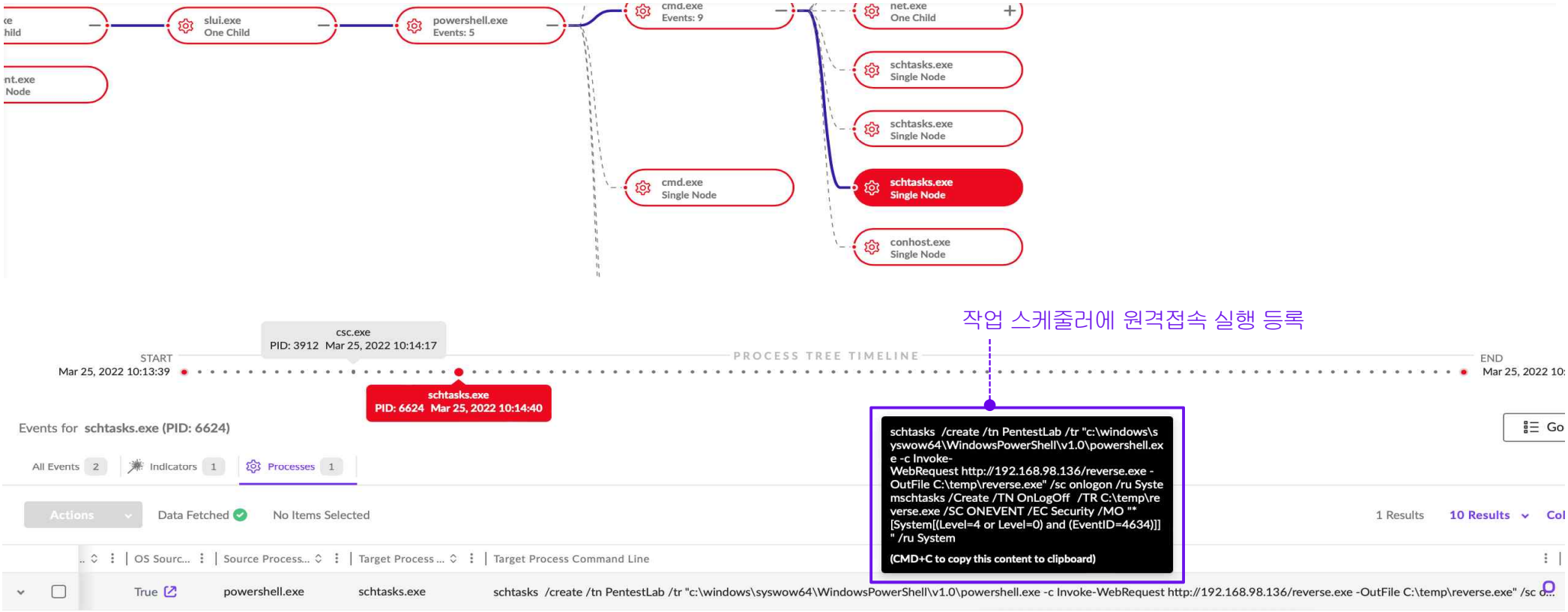




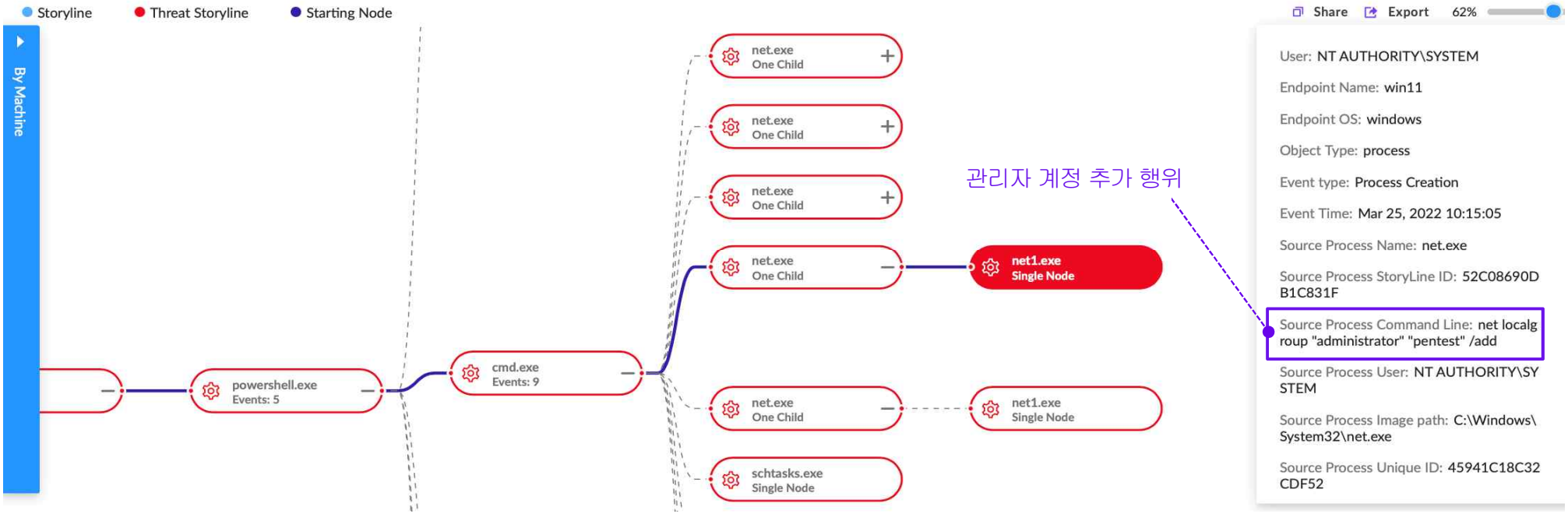
Powershell을 이용한 암호화된 명령어 수행

SentinelOne

위협 헌팅 – StoryLine (스토리라인)



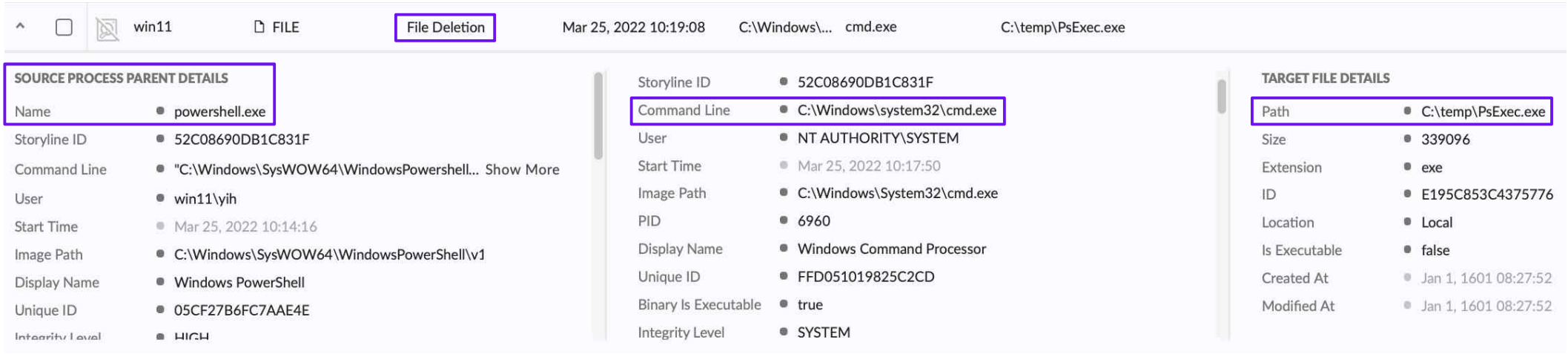
위협 헌팅 – StoryLine (스토리라인)



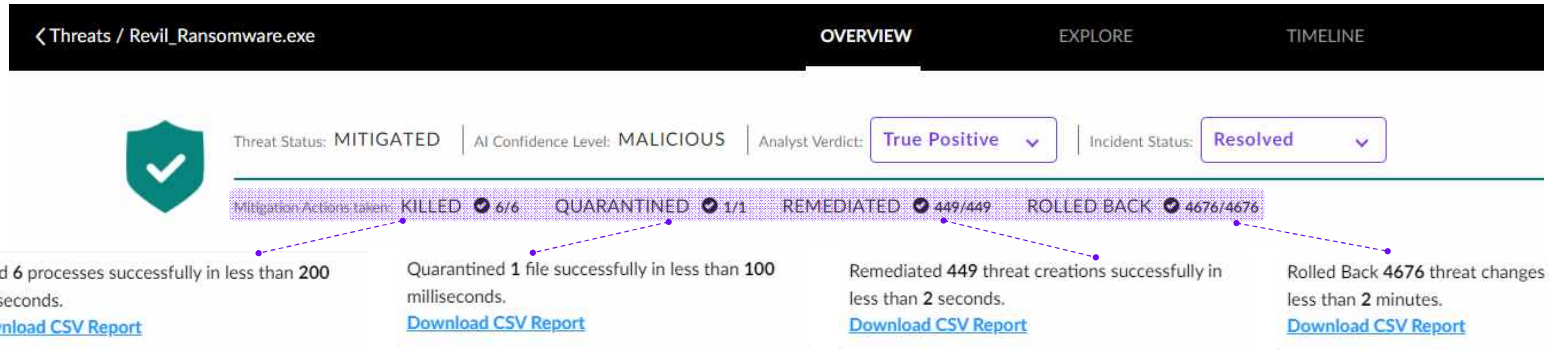
위협 헌팅 – StoryLine (스토리라인)

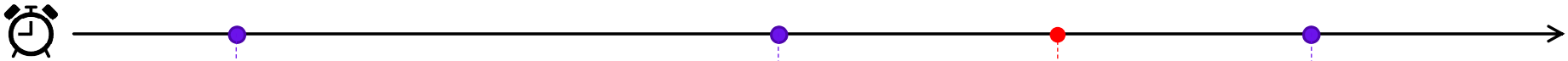
StoryLine

- 공격자에 의한 파일 삭제 행위



시스템 복구



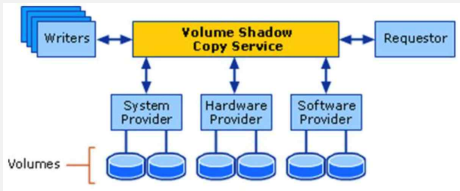


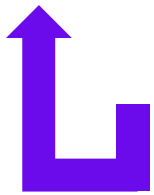
리부팅
(스냅샷 Ⅰ 생성)

4시간 경과
(스냅샷 Ⅱ 생성)

4시간 경과
(스냅샷 Ⅲ 생성)

<Windows Volume Shadow Service 활용>





악성코드로 인한 손상 시
(스냅샷 Ⅱ 데이터를 이용한 롤백 수행)

Thank you

SentinelOne®

sentinelone.com