2022 KARA 랜섬웨어 대응 보고서

SK쉴더스, 트렌드마이크로, 지니언스, 맨디언트, S2W, 베리타스, 캐롯손해보험, 법무법인

KARA 소개 및 랜섬웨어 통계

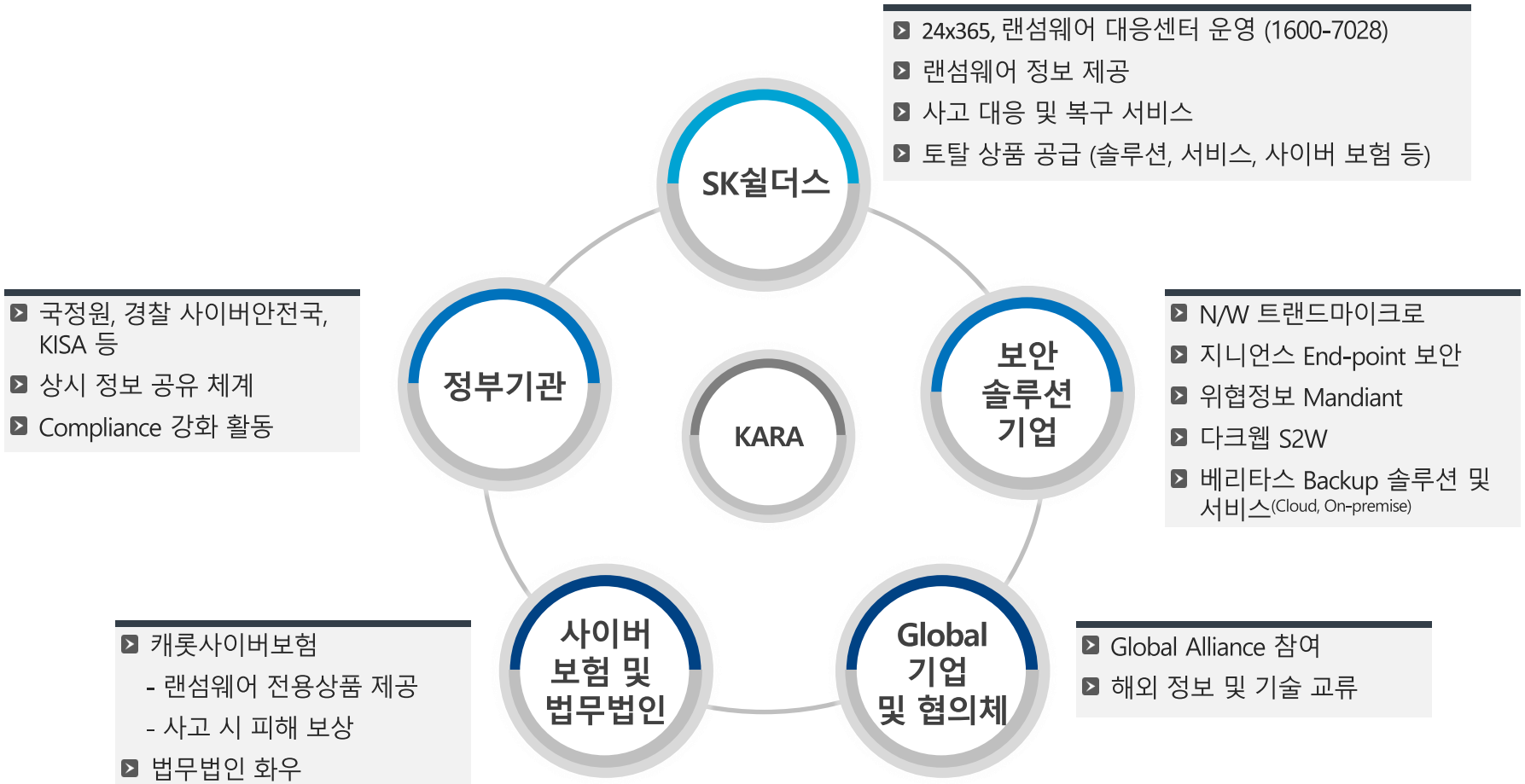
SK쉴더스 이호석 팀장

Ⅰ

KARA 소개

SK 쉴더스

랜섬웨어에 대한 정보 공유 및 공동 대응을 위해 유관 기관과 국내외 기업 및 협의체가 참여하여 Korea Anti Ransomware Alliance를 구성하였습니다.



KARA 랜섬웨어 협의체는 랜섬웨어 관련 정보 공유, 대외 활동, 사고합동대응, 사업협력 등에 대해 유기적으로 협업하여 랜섬웨어로부터 고객의 자산을 안전하게 보호할 예정입니다.

정보 공유

"참여사 보유 랜섬웨어 정보 공유"

랜섬웨어 정보 공유	랜섬웨어 정기 보고서
• 신규 랜섬웨어 분석 정보 • 공격자 동향 정보 • 사고 이슈 정보 공유	• Issue 랜섬웨어 분석 • 정기 Trend 보고서 발간 • 사고 분석에 대한 공유

대외 활동

"랜섬웨어 대응 관련 대외 활동 협력"

정부 기관 ⇔ 대응 협의체 ⇔ Global

공동 세미나 개최	정부기관 합동 조사
Global 업체 협력(인터폴)	언론 홍보 활동

Alliance 주요 활동

사고 대응

"랜섬웨어 전문기업 참여를 통한 통합 대응"

【사고대응절차】

사고접수	대응	복구	대책
• 사고 발생 정보 공유	• 사고 분석 - 원인파악 • 외부위협분석 • 언론대응	• 피해복구 - Data • 배상책임보상 • 복구비용보상	• 재발방지대책 • 결합상품제안 • Quick-Win과제

사업협력

"참여사 솔루션/서비스 결합하여 제공"

보안솔루션	보안서비스 및 보험
• N/W 랜섬웨어 대응 • Endpoint 보안 솔루션 • 랜섬웨어 대응 Back-up • 랜섬웨어 점검 Tool	• 보안 관제(24x365) • 보안 위협정보 서비스 • 랜섬웨어 전용 보험

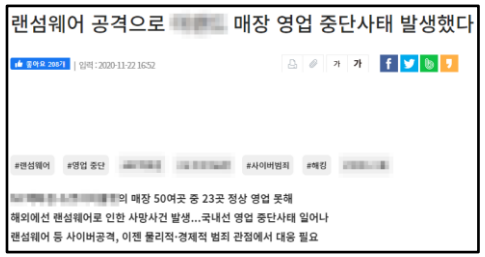
Ⅱ

랜섬웨어 트렌드 및 분석

SK 쉴더스

EQST
Experts, Qualified Security Team

2020년 말부터 서비스형 랜섬웨어가 폭발적으로 증가하기 시작하였고, 이와 더불어 수사를 회피하기 위한 랜섬웨어 Re-Branding까지 공격자들은 진화된 형태의 공격을 시도하고 있습니다.



- **Clop 랜섬웨어, A 社 매장 운영 차질**

- **LockBit 랜섬웨어, Accenture 社 6TB 데이터 탈취**

- **BlackCat 랜섬웨어, MONCLER 社 고객사, 내부 문건 등 데이터 유출**

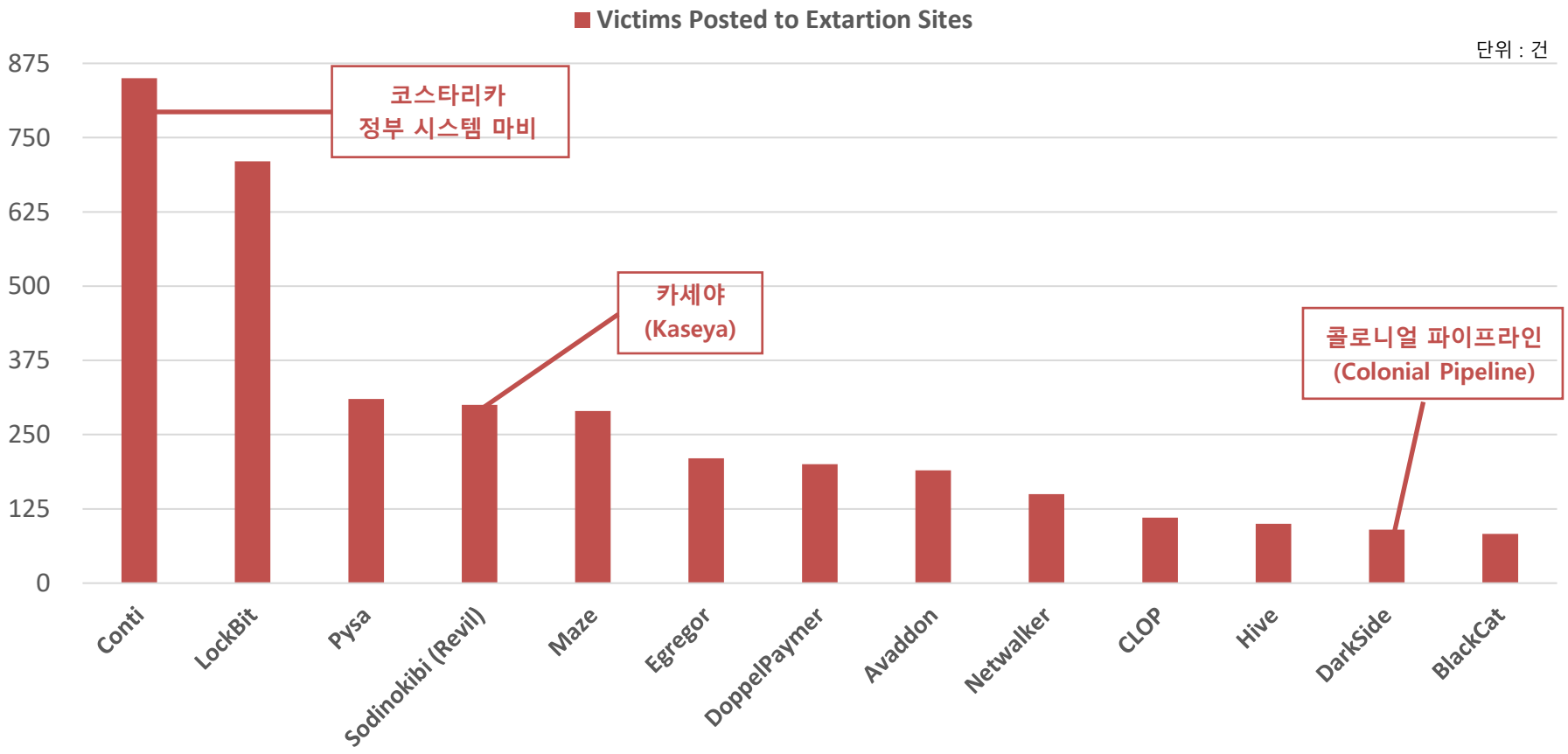
2020.11 — 2021.05 — 2021.08 — 2021.09 — 2022.01

- **Conti 랜섬웨어, B 社 내부 자료 유출**
- **DarkSide 랜섬웨어, Colonial Pipeline 社 연료 파이프라인 폐쇄**

- **BlackMatter 랜섬웨어, 일본 기술 기업 Olympus 社 네트워크 마비**
- **BlackMatter 랜섬웨어, C 社 공격 당해 150GB에 달하는 데이터 유출**

EQST
Experts, Qualified Security Team

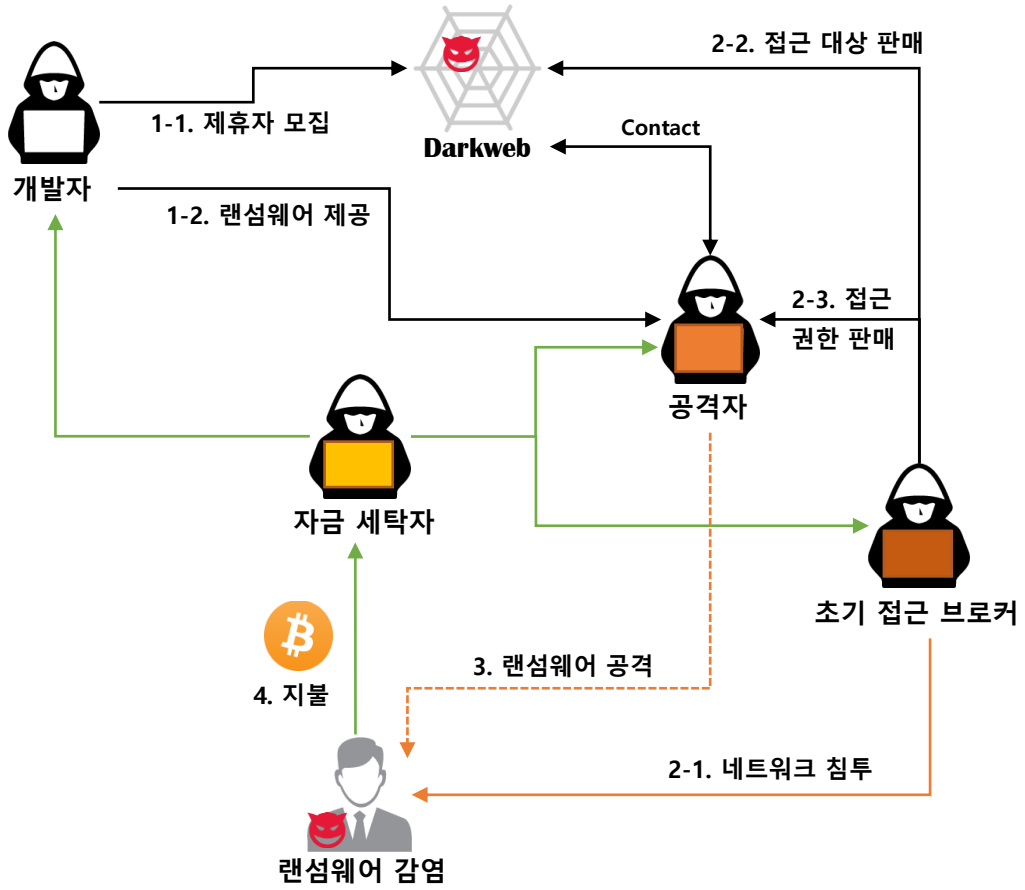
Conti와 Lockbit 같은 대규모 조직이 오랜 기간 ICS [1], OT [2] 와 같은 제조/서비스 환경을 타겟으로 랜섬웨어 전파 활동을 지속해왔습니다.



※ 1) ICS(Industrial Control System) : 산업 제어 시스템
※ 2) OT(Operational Technology) : 산업용 장비 제어 방식

※ 출처 : RECORD FUTURE

서비스형 랜섬웨어인 RaaS는 Ransomware-as-a-Service의 약자로, 랜섬웨어 제작자와 이를 사용하는 파트너들과의 제휴를 통해 공격이 성공할 경우 수익을 배분하는 형태로 운영되고 있습니다.



LockBit

VenusLocker 그룹에서 사용(2022.01~02)
2022.01 프랑스 법무부 감염
2022.02 Bridgestone Americas 社 감염

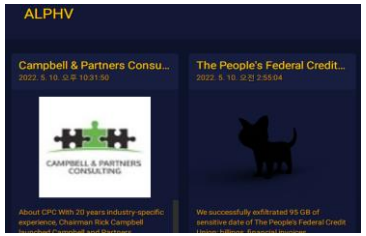
Conti

소스코드 유출(2022.03)
NB65 그룹에서 개조 후 러시아 공격
2022.03 러시아 연방 우주국 감염
2022.03 러시아 국영 방송국 감염

EQST
Experts, Qualified Security Team

수사기관의 감시가 집중되거나 운영의 어려움이 판단되는 경우 공격자 그룹은 Re-Branding을 통해 악성코드를 고도화하여 활동을 이어가고 있습니다.

- 파일 부분 암호화로 속도 증가
- 2021.05 Colonial Pipeline 社 공격
- **FBI, 정부의 집중적인 감시로 운영 중단**

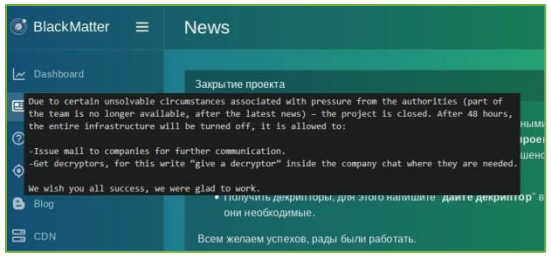


- 최초의 Rust based 랜섬웨어
- 2022.02 Swissport International 社 공격
- **BlackMatter Fendr 공격 도구 사용**

DarkSide
~2020.08
47건, $10M

BlackMatter
~2021.07
50건↑, $15M

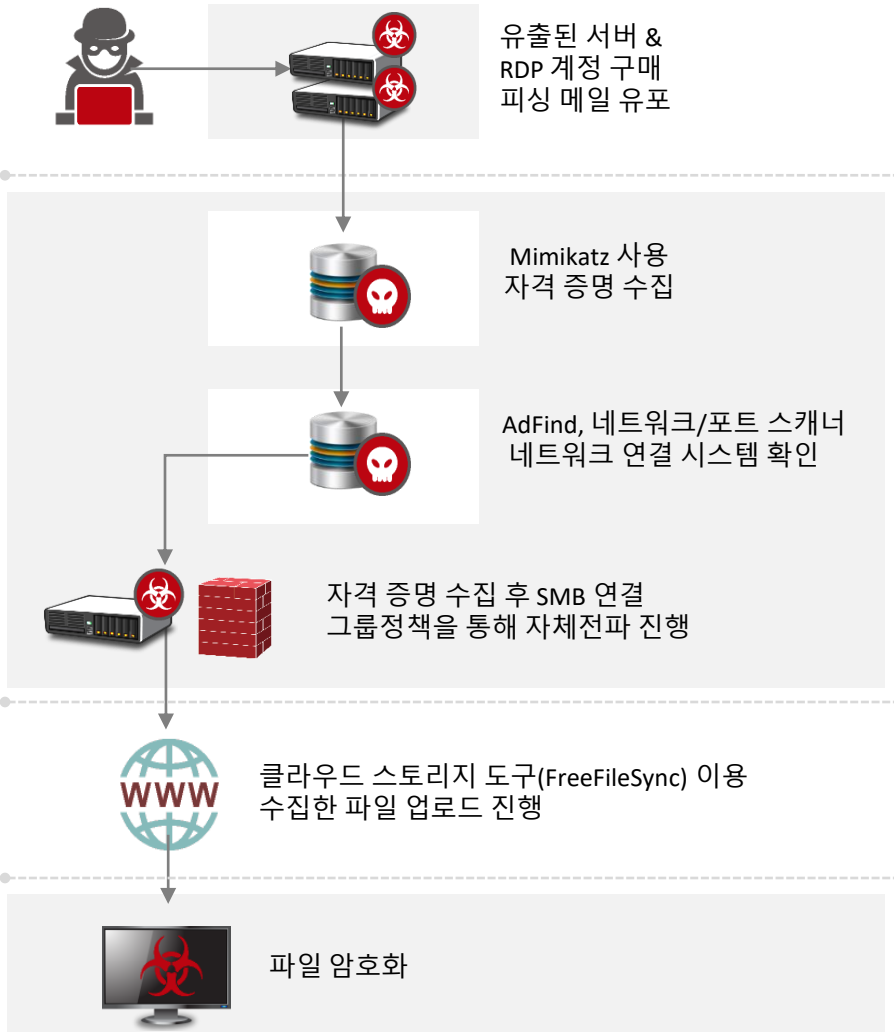
BlackCat
2021.11~
83건↑, $3M



- DarkSide Custom Salsa20과 동일
- 유출 사이트 문구 유사
- 2021.09 Olympus 社 공격
- **정부&수사기관 압력으로 운영 중단**

EQST
Experts, Qualified Security Team

LockBit

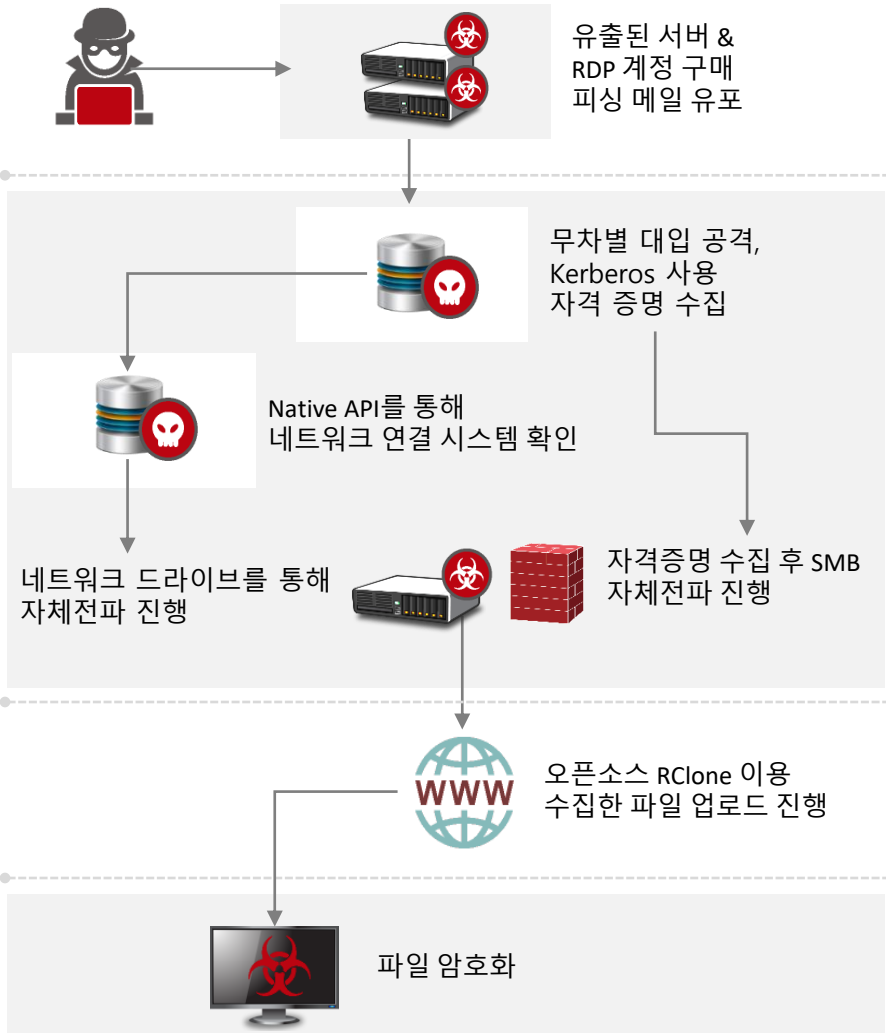


ATT&CK Matrix

초기 침투	Initial Access	Phishing Valid accounts
자격 증명 수집 & 내부 전파	Credential Access	Windows Credential Manager
	Discovery	File and directory discovery Network Share Discovery Remote system discovery
	Lateral Movement	Lateral tool transfer
유출	Exfiltration	Exfiltration over web service
영향	Impact	Data encrypted for impact

EQST
Experts, Qualified Security Team

Conti

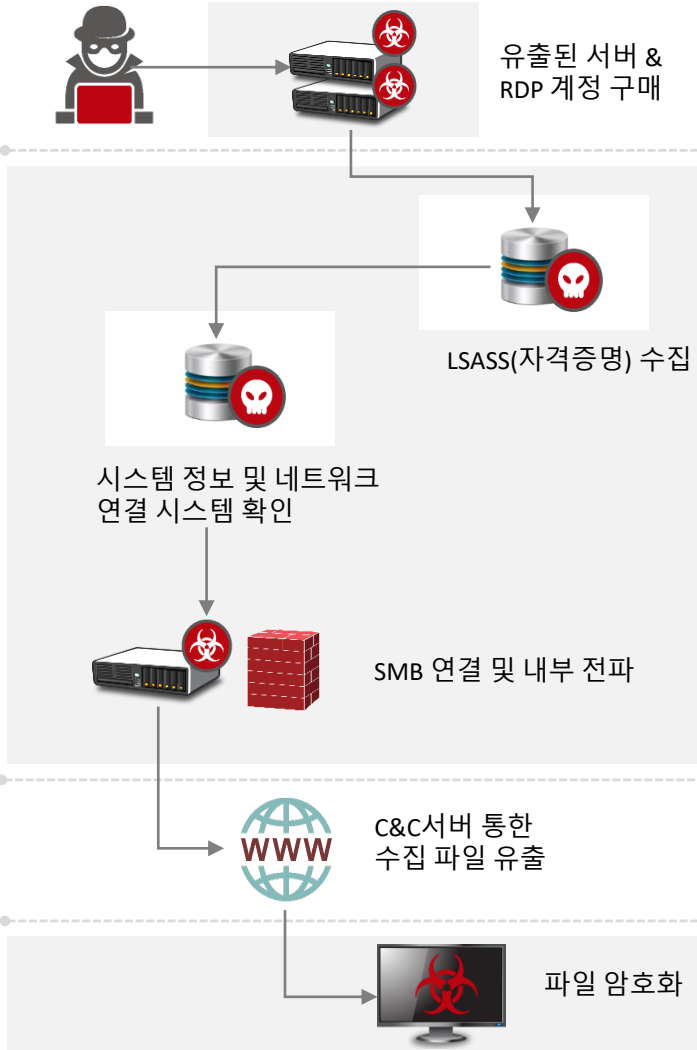


ATT&CK Matrix

초기 침투	Initial Access	Phishing Valid accounts
자격 증명 수집 & 내부 전파	Credential Access	Brute Force Kerberoasting
	Discovery	System Network Configuration System Network Connections Network Share Discovery
	Lateral Movement	Remote Services: SMB/Windows Admin Shares Taint Shared Content
유출	Exfiltration	Exfiltration over web service
영향	Impact	Data encrypted for impact

EQST
Experts, Qualified Security Team

BlackMatter

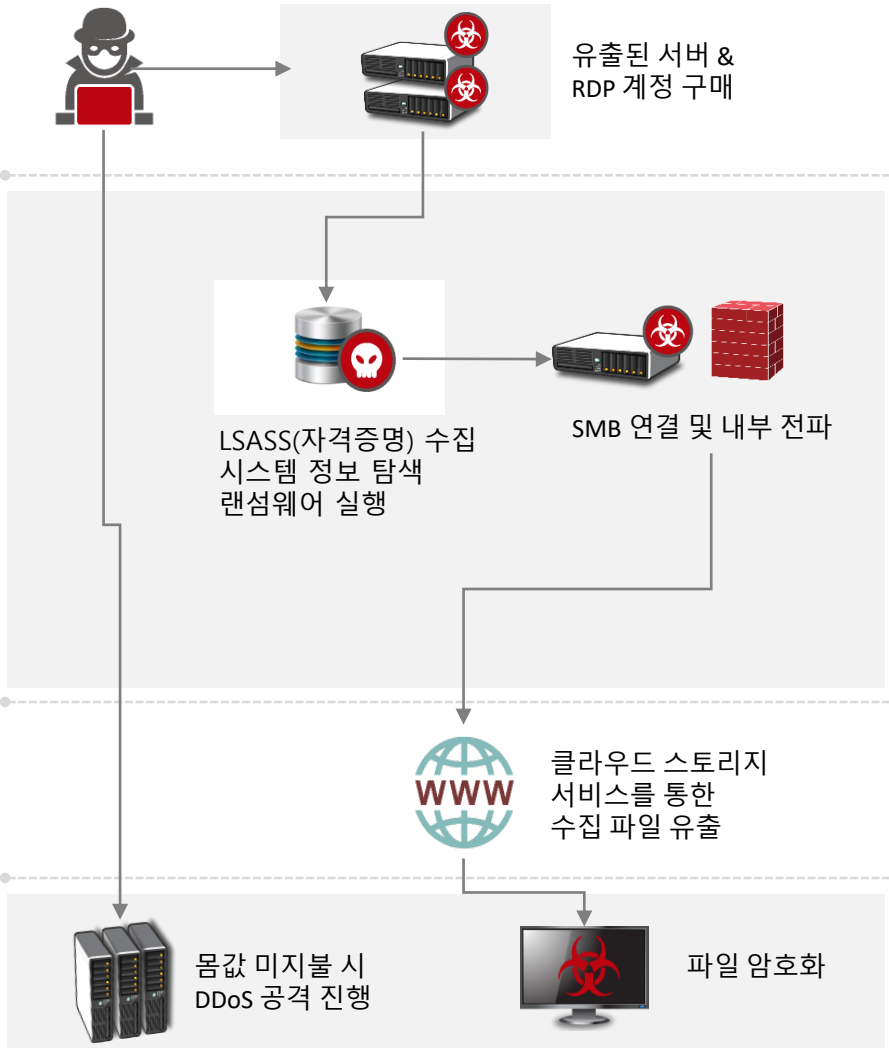


ATT&CK Matrix

초기 침투	Initial Access	Valid accounts
자격 증명 수집 & 내부 전파	Credential Access	OS Credential Dumping: LSASS Memory
	Discovery	Query Registry Process Discovery System Service Discovery File and Directory Discovery Remote System Discovery System Information Discovery
	Lateral Movement	Remote Services: SMB/Windows Admin Shares
유출	Exfiltration	Exfiltration Over C2 Channel
영향	Impact	Data encrypted for impact

EQST
Experts, Qualified Security Team

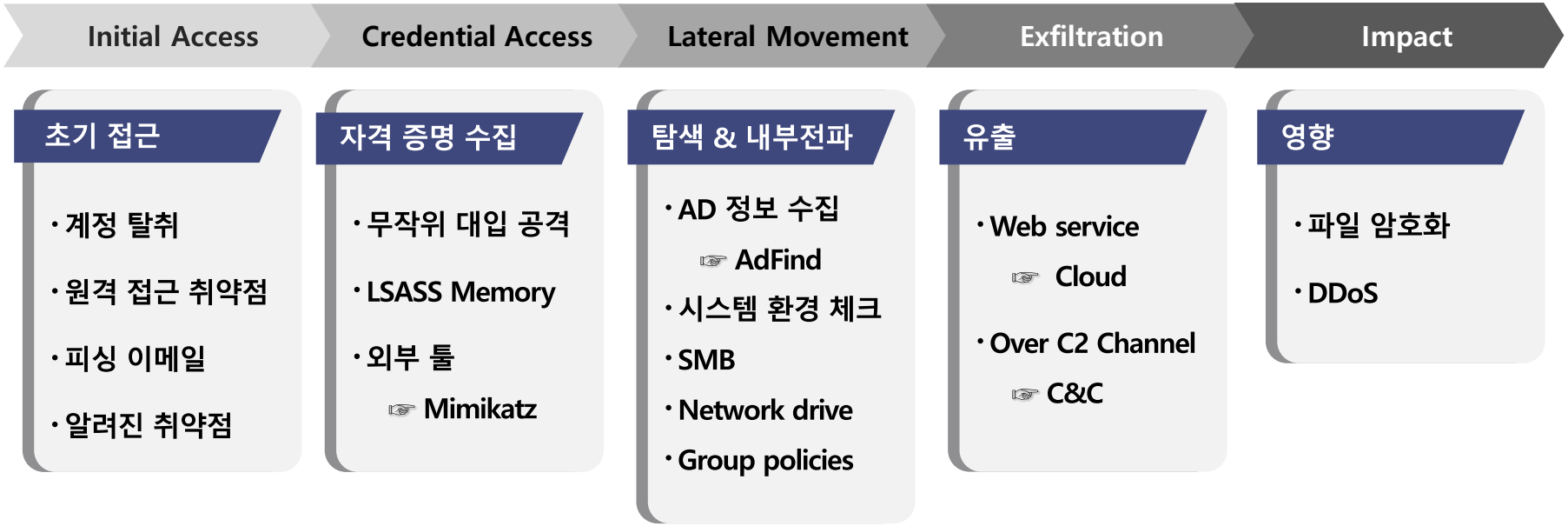
BlackCat



ATT&CK Matrix

초기 침투	Initial Access	Valid accounts
자격 증명 수집 & 내부 전파	Credential Access	Brute Force Kerberoasting
	Discovery	System Network Configuration System Network Connections Network Share Discovery
	Lateral Movement	Remote Services: SMB/Windows Admin Shares Taint Shared Content
유출	Exfiltration	Exfiltration over web service
영향	Impact	Data encrypted for impact

앞서 살펴본 바와 같이 랜섬웨어는 초기 접근부터 악성코드 내부 전파, 데이터 외부 유출까지 다양한 취약점들을 사용하고 있습니다. 이를 대응하기 위해 예방/탐지/복구/대응 각 영역에 특화된 대응방안 수립이 필요합니다.



예방 (Prevent)

- 위협의 조기 식별 및 실시간 탐지/차단을 통한 가용성 확보

탐지 (Detect)

- 랜섬웨어 특화 솔루션을 통한 신규 위협 대응

복구 (Restore)

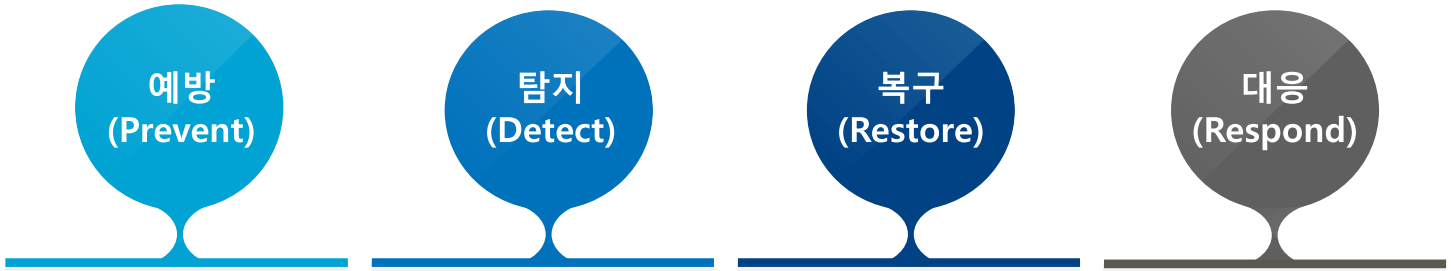
- 데이터 백업 솔루션을 통한 서비스 안정성 확보

대응 (Respond)

- 주기적인 점검을 통해 보안 위협 선제적 대응

EQST
Experts, Qualified Security Team

SK쉴더스에서는 랜섬웨어 방지를 위해 24x365보안관제부터 랜섬웨어 특화 솔루션까지 다양하고 체계적인 대응방안을 제공 하겠습니다.



보안 관제

- **사이버 위협 예방**
  - ✓ 최신 보안정보 트렌드 공유
  - ✓ 침해탐지패턴 사전 공유
- **상시 모니터링**
  - ✓ 24시간 365일 상시 대응체계
  - ✓ 위협 및 이상징후 초동 대응

모의 해킹

- **맞춤형 모의 해킹**
  - ✓ 기업 맞춤형 시나리오 진행
  - ✓ 회사만의 취약점 분석 가능
  - ✓ 보안 전문가 그룹 EQST가 진행하는 모의 해킹

랜섬웨어 전용상품 (사이버가드)

- **PC, 서버 보호**
  - ✓ 보안 점검, 백업, 백신
  - ✓ 랜섬웨어 탐지/차단
- **네트워크 보호**
  - ✓ 네트워크 접근 통제
  - ✓ 침해 관제 서비스

사고 분석

- **침해사고 분석 및 대응**
  - ✓ 신속한 사고 분석/상황 전파
  - ✓ 유형별 대응 방안 수립
  - ✓ 재발방지 대책 수립

EQST
Experts, Qualified Security Team

KARA 회원사에서는 사고 발생 시, 사고 접수부터 분석, 재발방지까지 종합적인 지원 체계를 구축하여 통합된 랜섬웨어 서비스를 제공할 예정입니다.

솔루션

트렌드 마이크로

- **랜섬웨어 N/W 솔루션 제공**
- **4단계 보안레이어를 통한 대응**
  - 이메일 / 웹
  - 엔드포인트
  - 네트워크
  - 워크로드 보안

지니언스

- **랜섬웨어 EDR솔루션 제공**
- **Genian Insight E**
  - 랜섬웨어 탐지 및 격리
  - EDR 기반 엔드포인트 대응

베리타스

- **랜섬웨어 전용 백업 솔루션 제공**
  - 변조/삭제 불가 스토리지 제공
  - 복구시스템
  - 크로스 시스템 이상요소탐지
  - 악성코드 검사

사고대응 / 분석

SK쉴더스

- **랜섬웨어 대응센터 운영 (24x365)**
- **랜섬웨어 정기 보고서 제공**
- **사고 조사, 대응 및 복구 서비스**
- **랜섬웨어 정보보안 패키지 서비스**
  - 클라우드 백업, 탐지/차단, 안심보험
- **랜섬웨어 모의 훈련 서비스**
- **자가 점검 도구 제공**

맨디언트

- **위협정보 분석 및 제공**
- **랜섬웨어 디펜스 밸리데이션**
  - 맨디언트 어드밴티지 플랫폼
  - 위협인텔리전스
  - 랜섬웨어 재구성 기능

S2W

- **다크웹 위협정보 분석 및 제공**
  - 랜섬웨어 인프라 분석
  - 비트코인 자금흐름 분석

보험

캐롯손해보험

- **랜섬웨어 전용 상품 제공 및 사고 시 피해보상**

법무

법무법인 화우

- **법률 자문 제공**

샌드박스 및 XDR 활용한 랜섬웨어 탐지와 대응방안

트렌드마이크로 최영삼 이사

샌드박스와 XDR을 활용한 랜섬웨어 탐지, 대응 방안

Trend Micro
최영삼 이사

랜섬웨어 위협 현황 - 2021

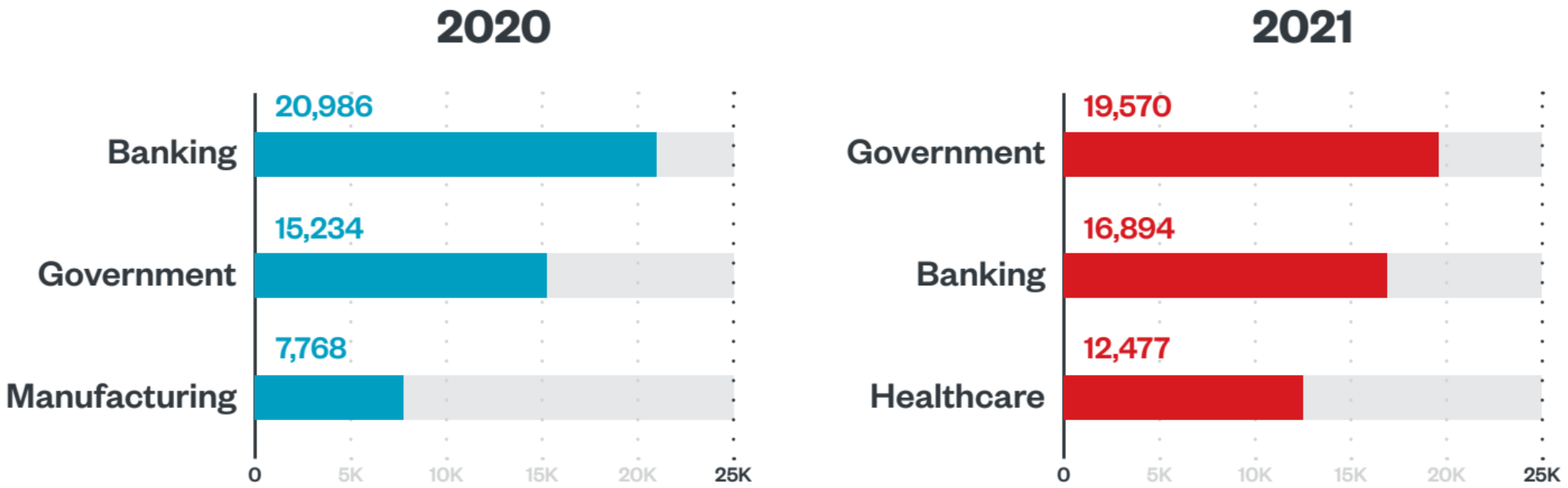


Figure 1. The top three industries in terms of ransomware file detections in 2021 and 2020

Source: Trend Micro Smart Protection Network

랜섬웨어 위협 현황 - 2021

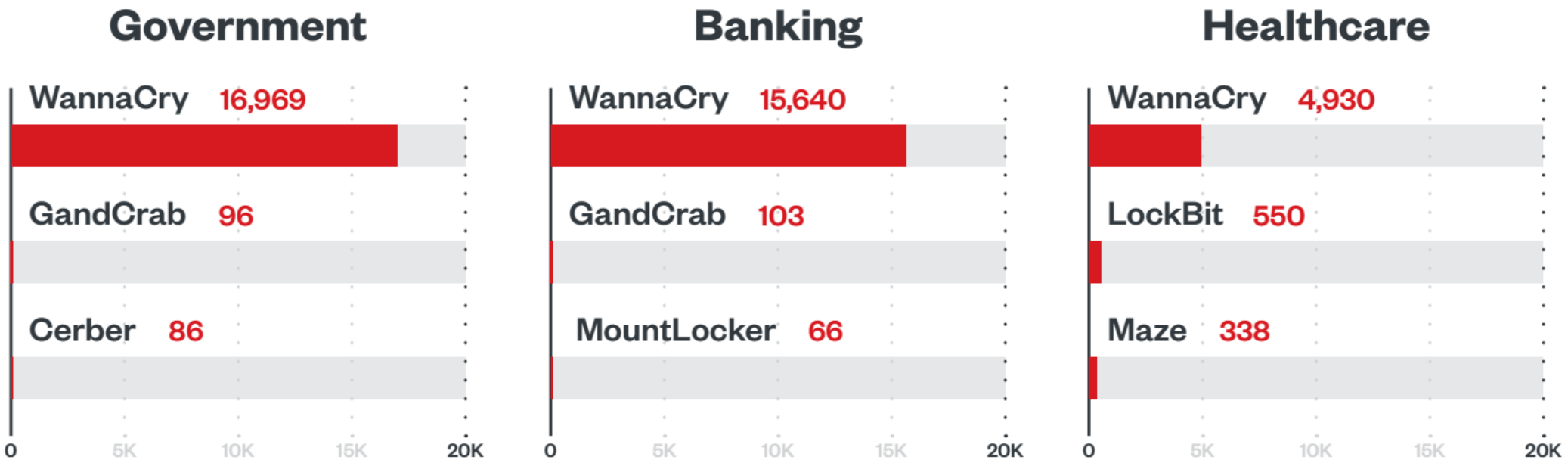


Figure 2. The top three ransomware families that affected the top three affected industries in 2021

Source: Trend Micro Smart Protection Network

랜섬웨어 위협 현황 - 2021

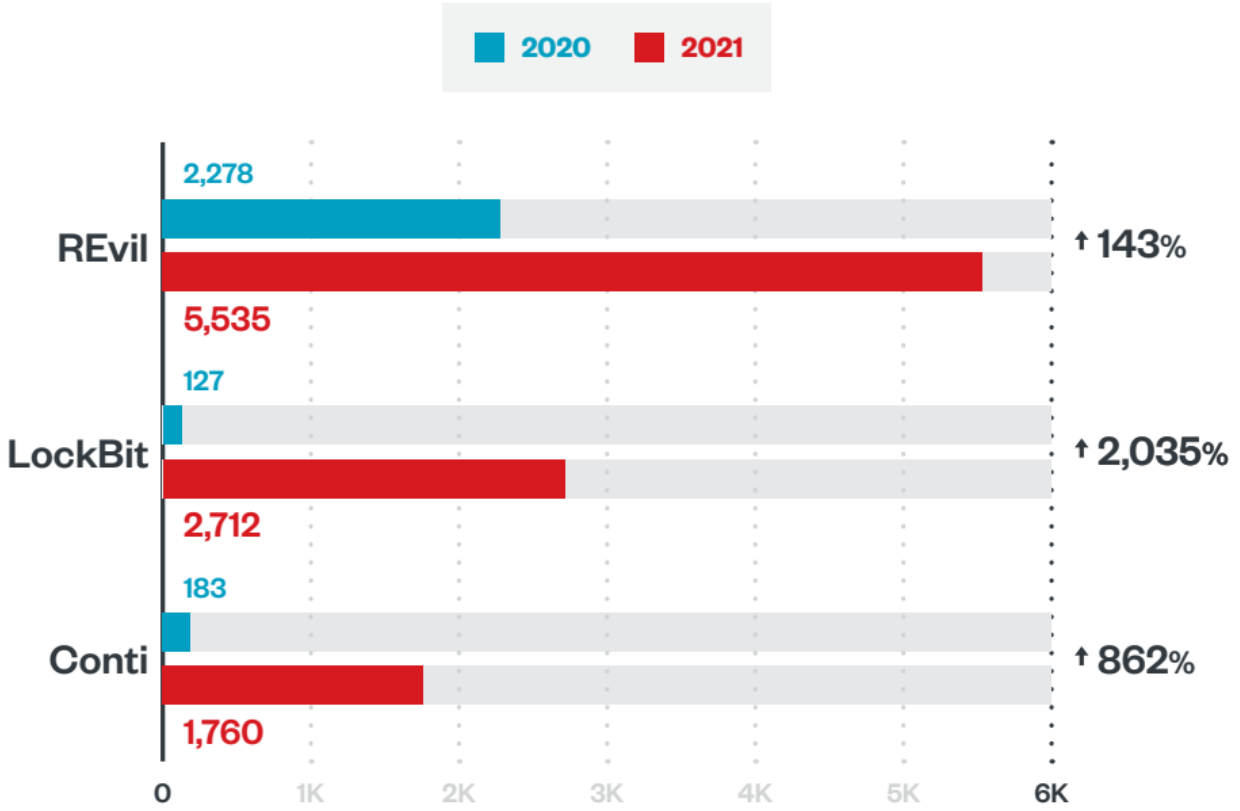


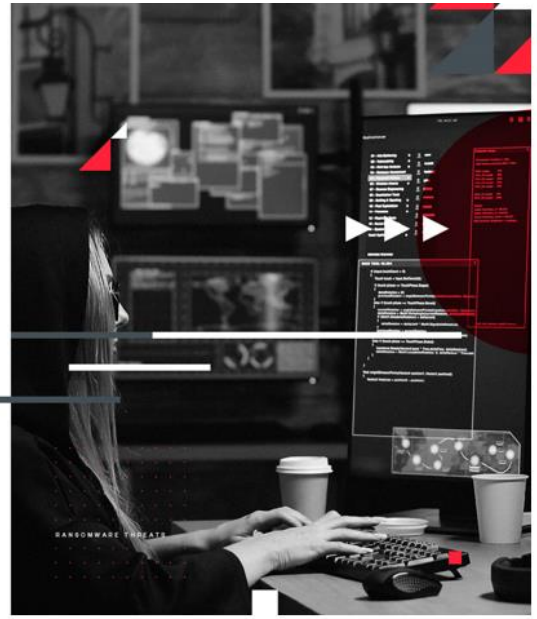
Figure 3. A year-on-year comparison of the top three modern ransomware families in terms of file detections in 2020 and 2021

Source: Trend Micro Smart Protection Network

랜섬웨어 위협 전망 - 2022

진화하는 랜섬웨어 위협으로부터 보호를 유지하기 위해 기업은 엄격한 server-hardening 및 애플리케이션 제어 정책으로 서버를 보호하는 데 주력할 것입니다.

서버는 랜섬웨어의 주요 타켓이 될 것입니다.



- 하이브리드 업무 모델은 공격 대상을 증가시키고 악의적인 행위자가 어떻게 침입하여 공격을 수행할지 정확히 파악하기 어렵게 만듭니다.
- 랜섬웨어 공격은 더욱 표적화되고 눈에 띄게 될 것입니다..
- 랜섬웨어 공격은 무기화를 위해 도난당한 데이터를 유출하고 마이닝하기 위해 중요한 데이터에 대한 액세스 거부를 회피할 것입니다.
- 랜섬웨어 공격자는 더 자주 클라우드를 표적으로 삼을 것입니다.

< 보안 권고 >

SECURITY RECOMMENDATION

기업은 다음을 통해 2022년에 랜섬웨어 위협을 막을 수 있습니다

보안에 대한 강력하고 다층적인 접근 방식을 갖고 모든 관련 운영체제 및 애플리케이션에 대한 Server-hardening 가이드라인을 준수합니다.

랜섬웨어 모범 사례

감사 및 인벤토리

- 자산 및 데이터 인벤토리 가져오기
- 승인 및 승인되지 않은 장치 및 소프트웨어 식별
- 감사 이벤트 및 로그

구성 및 모니터링

- 하드웨어 및 소프트웨어 구성 관리
- 관리자 권한 및 액세스 권한 부여
- 네트워크 포트, 프로토콜 및 서비스 사용 모니터링
- 방화벽 및 라우터와 같은 네트워크 인프라 장치에 보안 구성을 구현합니다.
- 악성 애플리케이션이 실행되는 것을 방지하기 위해 소프트웨어 허용 목록이 있어야 합니다.

패치 및 업데이트

- 정기적인 취약점 평가 수행
- 운영 체제 및 애플리케이션에 대한 패치 또는 가상 패치 수행
- 소프트웨어 및 애플리케이션을 최신 버전으로 업데이트

보호 및 복구

- 데이터 보호, 백업 및 복구 조치 시행
- 다단계 인증 구현

보안 및 방어

- 샌드박스 분석을 수행하여 악성 이메일 검사 및 차단
- 이메일, 엔드포인트, 웹 및 네트워크를 포함한 시스템의 모든 계층에 최신 버전의 보안 솔루션 적용
- 시스템에 의심스러운 도구가 있는 것과 같은 공격의 초기 징후를 탐지합니다.
- AI 및 머신 러닝 기반 기술과 같은 고급 탐지 기술 지원

트레이닝 및 테스트

- 정기적인 보안 기술 평가 및 교육
- 레드팀 연습 및 침투 테스트 수행

신변종 랜섬웨어 탐지는 어떻게?

Analysis Overview

Overall risk level	High risk	The object exhibited highly suspicious characteristics that are commonly associated with malware.	
Detections	VAN_RANSOMWARE.UMXX		
Exploited vulnerabilities	-		
Analyzed objects	ALZip ALZ File	1 - 이력서9.alz	E065F928308D7DB24607C73F590F82E57F40D47B
	Windows 32-bit EXE file	1.1 - 이력서_220501(경력사항도 같이 기재하였습니다 잘부탁드립니다).exe	72F846381E7B9F70AF61035BFEB221ECC2A55E10
	Windows 32-bit DLL file	1.2 - 지원서.jpg	47748C5B31B35671EF30663D9EEF51BA5FEEE0E6
	Hide child objects		

Analysis Environments

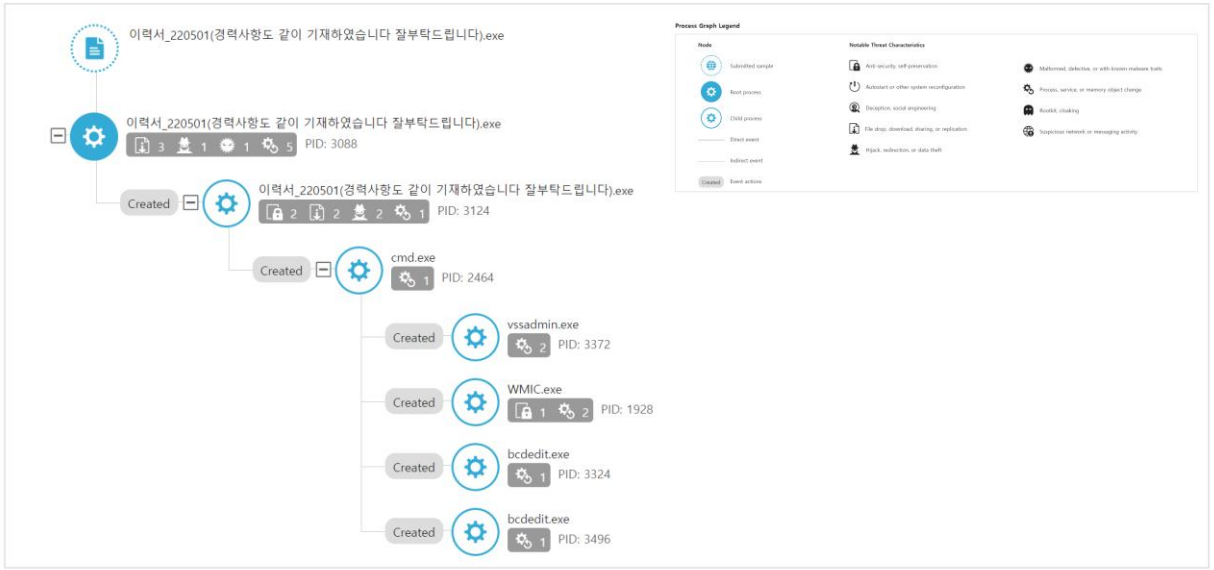
	Win7_32bit	Win10
Anti-security, self-preservation	✓	✓
Autostart or other system reconfiguration	✓	✓
Deception, social engineering		
File drop, download, sharing, or replication	✓	✓
Hijack, redirection, or data theft	✓	✓
Malformed, defective, or with known malware traits	✓	✓
Process, service, or memory object change	✓	✓
Rootkit, cloaking		
Suspicious network or messaging activity	✓	✓

악성 행위에 대한 카테고리

TREND MICRO

신변종 랜섬웨어 탐지는 어떻게?

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Command-Line Interface	Characteristics: 1
	Execution through API	Characteristics: 1, 2
	Execution through Module Load	Characteristics: 1
Persistence	Registry Run Keys / Startup Folder	Characteristics: 1
Privilege Escalation	Access Token Manipulation	Characteristics: 1, 2, 3
Defense Evasion	Software Packing	Characteristics: 1
	File Deletion	Characteristics: 1, 2, 3, 4
	Modify Registry	Characteristics: 1
	Access Token Manipulation	Characteristics: 1, 2, 3
Discovery	Process Discovery	Characteristics: 1
	System Information Discovery	Characteristics: 1, 2
Collection	Data from Local System	Characteristics: 1
Command and Control	Uncommonly Used Port	Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127
Impact	Data Encrypted for Impact	Characteristics: 1

멀웨어에 대한
프로세스 그래프

악성 행위에 대한
MITRE ATT&CK Framework의
Tactics 과 Technique 매칭

TREND MICRO

신변종 랜섬웨어 탐지는 어떻게?

Hijack, redirection, or data theft (31)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	■	Process ID: 3124 Info: Searches files by API
Executes commands or uses API to obtain system information	■	Process ID: 3124 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■	Process ID: 3088 Info: Obtains system version from API result
Accesses decoy file	■	C:₩documents₩contact.pst
Accesses decoy file	■	C:₩documents₩contact.pab
Accesses decoy file	■	C:₩documents₩contact.ost
Accesses decoy file	■	C:₩documents₩contact.oab
Accesses decoy file	■	C:₩documents₩agreement.docx
Accesses decoy file	■	C:₩documents₩agreement.doc
Accesses decoy file	■	C:₩documents₩account.xlsx
Accesses decoy file	■	C:₩documents₩account.xls
Accesses decoy file	■	F:₩project.ppt
Accesses decoy file	■	F:₩contact.pst
Accesses decoy file	■	F:₩contact.pab
Accesses decoy file	■	F:₩contact.ost
Accesses decoy file	■	F:₩contact.oab
Accesses decoy file	■	F:₩agreement.docx
Accesses decoy file	■	F:₩agreement.doc
Accesses decoy file	■	F:₩project.pptx
Accesses decoy file	■	F:₩account.xlsx
Accesses decoy file	■	F:₩account.xls
Accesses decoy file	■	E:₩contact.oab
Accesses decoy file	■	E:₩contact.pst
Accesses decoy file	■	E:₩contact.pab
Accesses decoy file	■	E:₩account.xlsx
Accesses decoy file	■	E:₩account.xls
Accesses decoy file	■	E:₩project.pptx
Accesses decoy file	■	E:₩project.ppt
Accesses decoy file	■	E:₩contact.ost
Accesses decoy file	■	E:₩agreement.docx
Accesses decoy file	■	E:₩agreement.doc

Malformed, defective, or with known malware traits (3)

Characteristic	Significance	Details
Exhibits behavior associated with ransomware	■■■	Encrypts Files
Causes process to crash	■	Process ID: 3088 Image Path: 이력서_220501(경력사항도 같이 기재하였습니다 잘부탁드립니다).exe
Rare executable file	■	Global Detections: 7

Search API를 통한 파일 리스트 정보 확인

샌드박스 내 미끼 파일에 접근하는 행위

랜섬웨어와 연관된 프로세스 행위
- 암호화 행위

신변종 랜섬웨어 탐지는 어떻게?

Process, service, or memory object change (13)

Characteristic	Significance	Details
Creates process in system directory	■ ■ ■	Process ID: 3496 Image Path: %windir%₩system32₩bcdedit.exe bcdedit /set {default} recoveryenabled no
Creates process in system directory	■ ■ ■	Process ID: 3324 Image Path: %windir%₩system32₩bcdedit.exe bcdedit /set {default} bootstatuspolicy ignoreallfailures
Creates process in system directory	■ ■ ■	Process ID: 1928 Image Path: %windir%₩System32₩Wbem₩WMIC.exe wmic shadowcopy delete
Creates process in system directory	■ ■ ■	Process ID: 3372 Image Path: %windir%₩system32₩vssadmin.exe vssadmin delete shadows /all /quiet
Escalates process privileges to gain a higher level of access	■ ■ ■	Process ID: 1928 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	■ ■ ■	Process ID: 3372 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	■ ■ ■	Process ID: 3088 Info: Obtains system level privileges
Creates command line process	■ ■ ■	Process ID: 2464 Image Path: %windir%₩System32₩cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 3088 Injected API: SetThreadContext Target Process ID: 3124 Target Image Path: %WorkingDir%₩이력서_220501(경력사항도 같이 기재하였습니다 잘부탁드립니다).exe
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 3088 Injected API: ZwMapViewOfSection Target Process ID: 3124 Target Image Path: %WorkingDir%₩이력서_220501(경력사항도 같이 기재하였습니다 잘부탁드립니다).exe
Creates process	■ ■ ■	Process ID: 3124 Image Path: %WorkingDir%₩이력서_220501(경력사항도 같이 기재하였습니다 잘부탁드립니다).exe
Creates process	■ ■ ■	Process ID: 3088 Image Path: %WorkingDir%₩이력서_220501(경력사항도 같이 기재하였습니다 잘부탁드립니다).exe Shell Command:
Uses Windows module loader to load dropped DLLs and execute code	■ ■ ■	Process ID: 3088 File: %TEMP%₩nsaE955.tmp₩System.dll

Suspicious network or messaging activity (254)

Characteristic	Significance	Details
Establishes uncommon connection	■ ■ ■	1.1.2.64:135
Establishes uncommon connection	■ ■ ■	1.1.2.63:445
Establishes uncommon connection	■ ■ ■	1.1.2.63:135
Establishes uncommon connection	■ ■ ■	1.1.2.62:445

시스템 디렉토리에 프로세스 생성

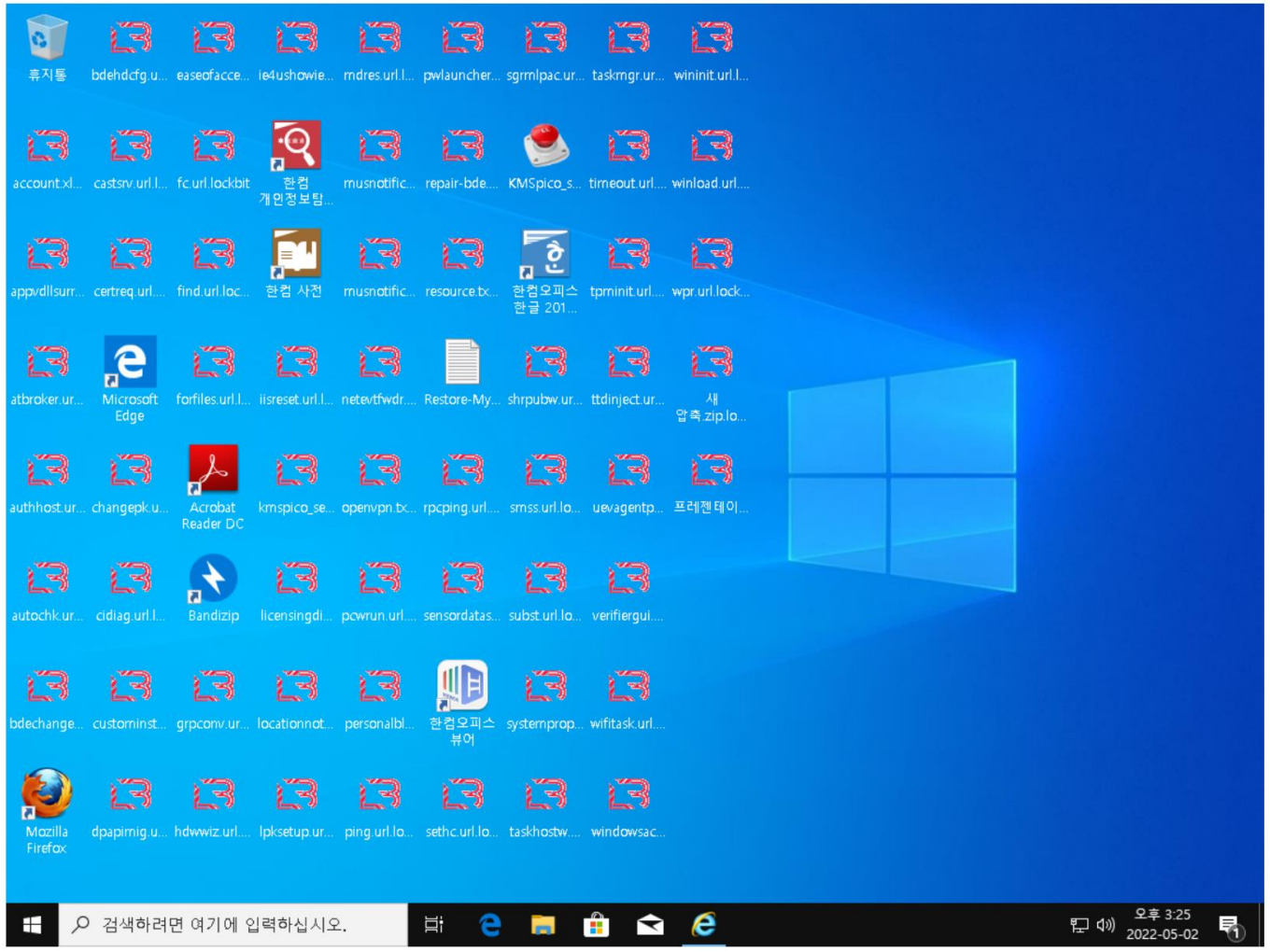
Shadowcopy 삭제

메모리 상주를 위한 Process에 Injection

네트워크 공유폴더 접속 시도

신변종 랜섬웨어 탐지는 어떻게?

▼ Screenshot



샌드박스 내 파일들에 대한 암호화 결과

Deep Discovery – APT 대응 솔루션

Deep Discovery Inspector - DDI

APT 탐지

네트워크 미러링 방식의 악성 사이트 접속, 악성코드 다운로드, C&C 통신 및 악성 행위 탐지

(모델 : DDI520/1200/4200/9200

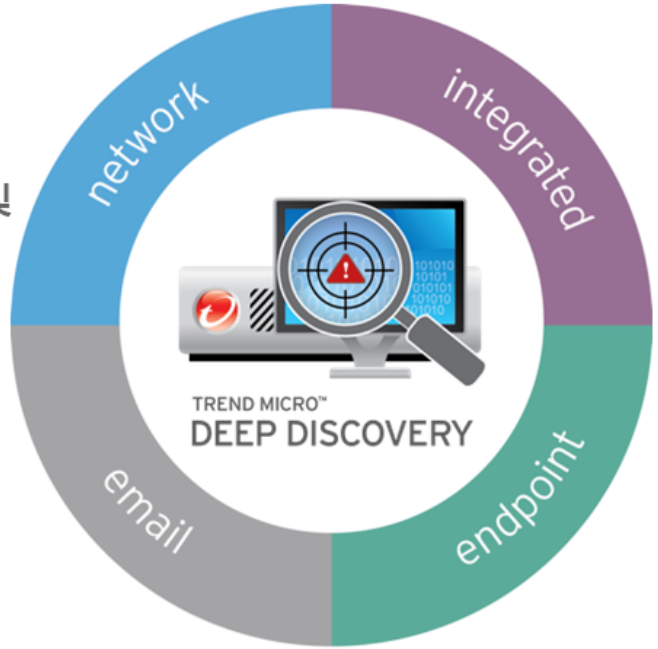
- 500Mbps/1Gbps/4Gbps/10Gbps)

Deep Discovery Email Inspector - DDEI

Email APT 차단

이메일에 첨부된 악성 첨부파일과 URL을 탐지, 분석, 차단하는 Email APT 전용 솔루션

(모델 : DDEI7200/9200)



Deep Discovery Analyzer - DDAN

APT 분석

알려지지 않은 신종/변종 악성코드에 대한 행위 분석 - Sandbox 분석 전용

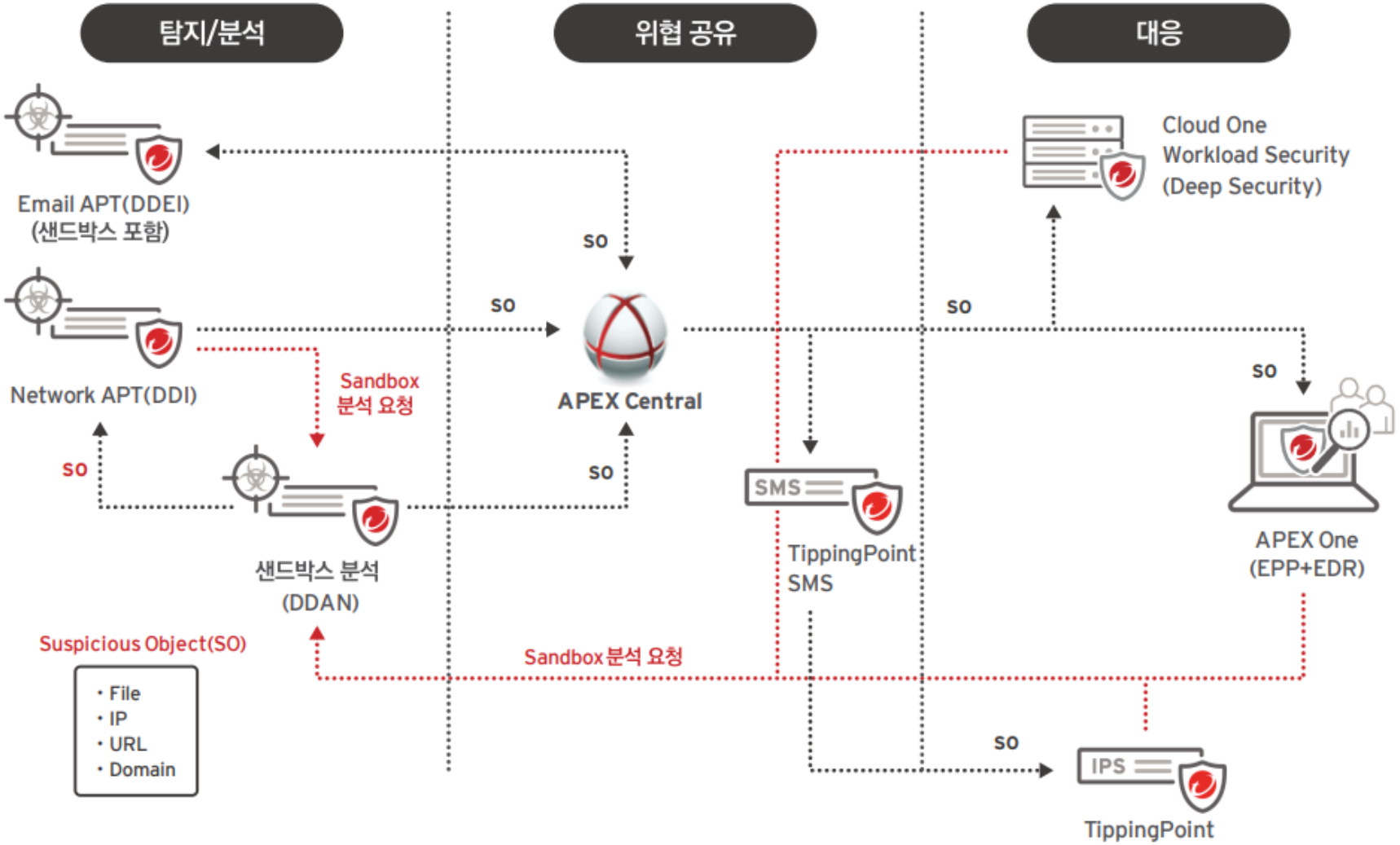
(모델 : DDAN1200)

Apex One Agent (Endpoint Anti-Malware, EDR)

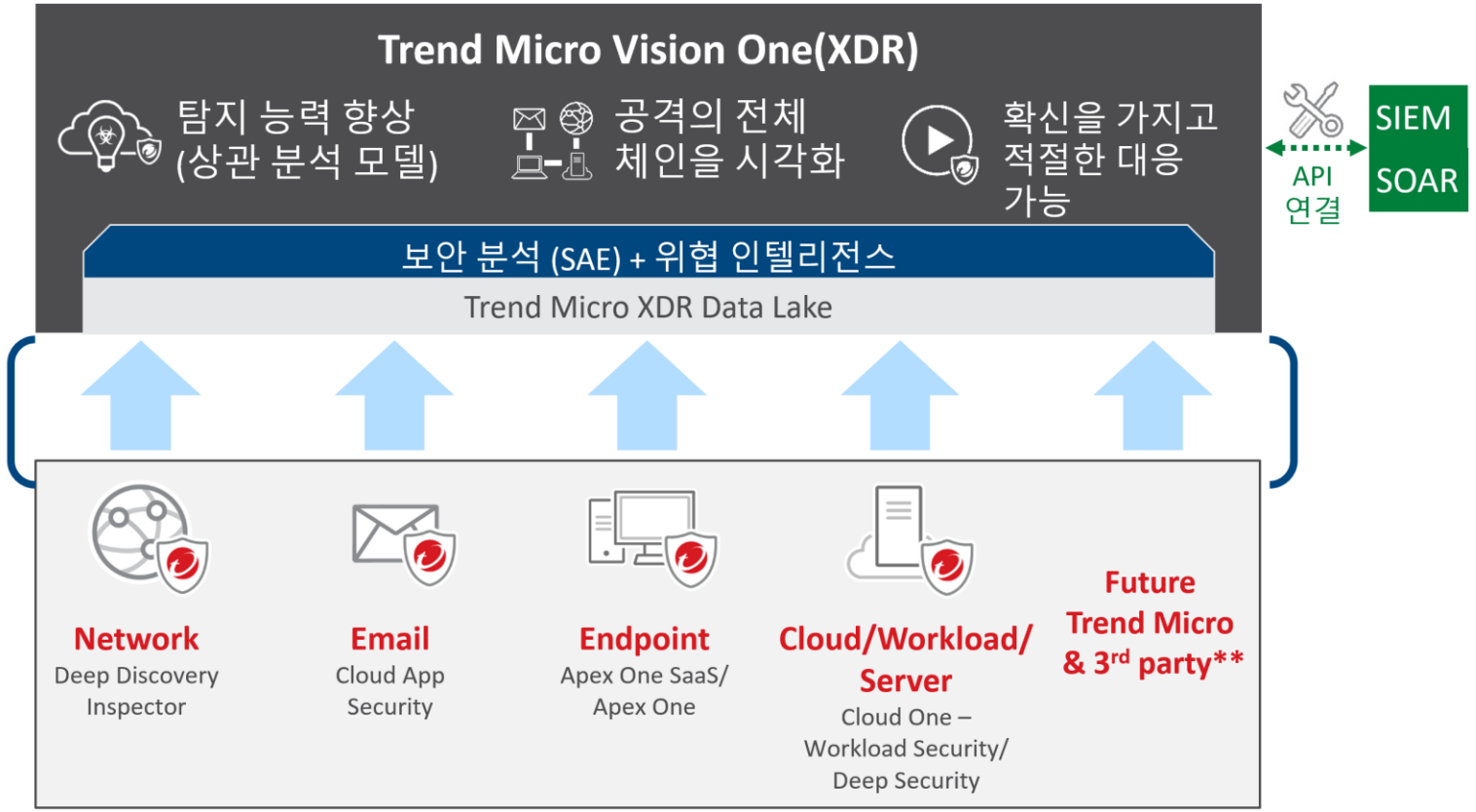
Endpoint 대응

알려진 악성코드 치료, Unknown Malware 격리 및 Endpoint Network 격리

Connected Threat Defense



XDR – 트렌드마이크로 Vision One

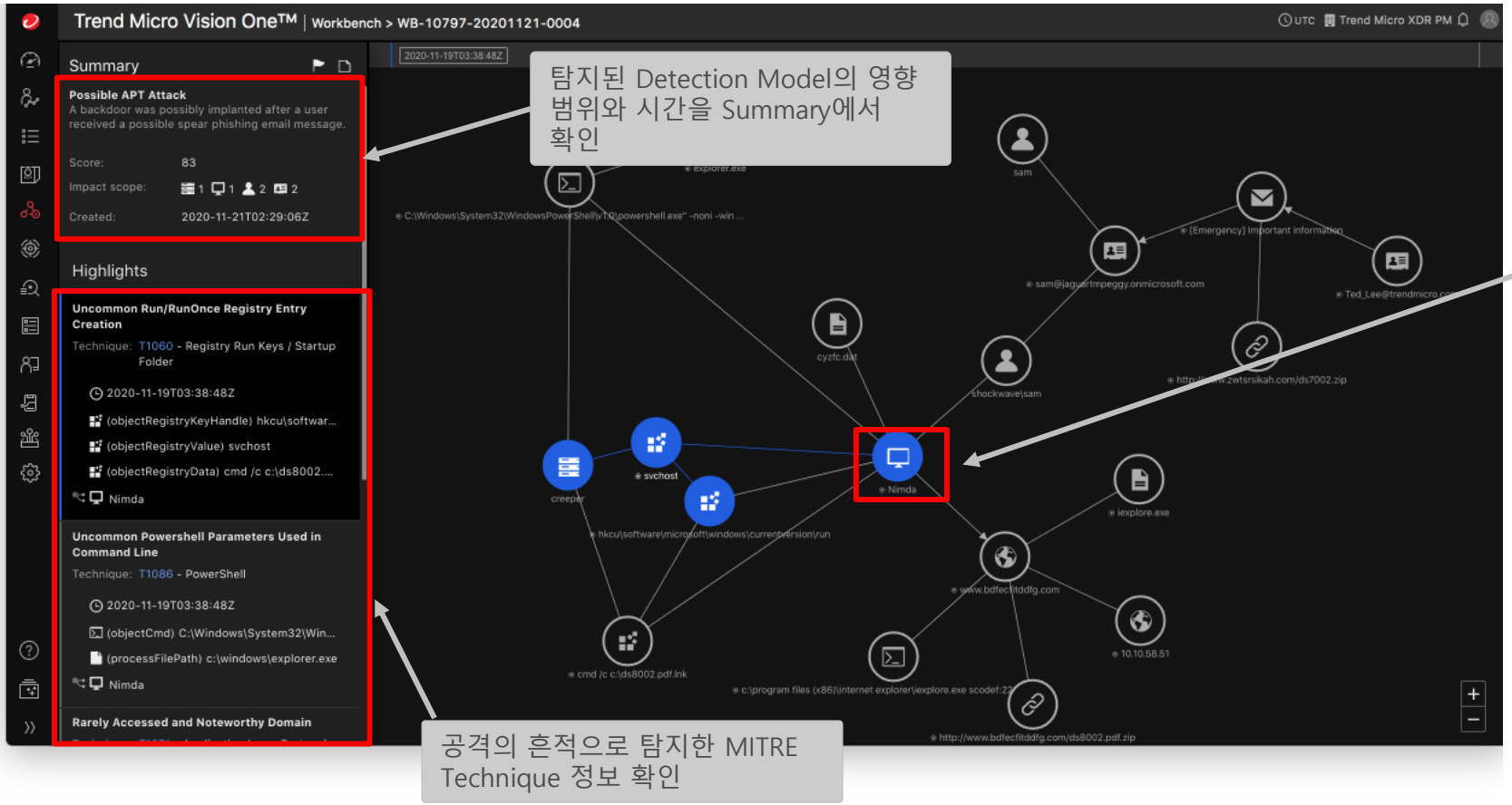


XDR 대응 제품 :
각 레이어의 보안
제품이 센서 역할

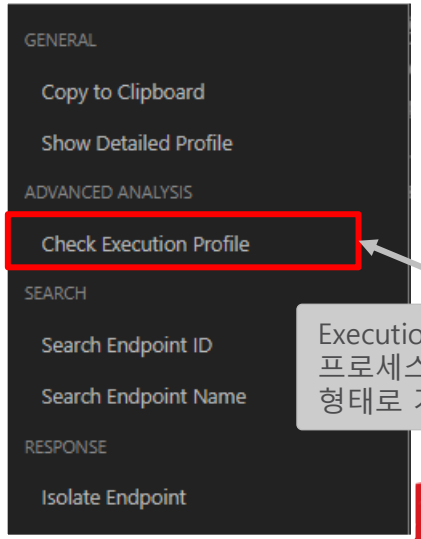
- 엔드포인트, 네트워크, 이메일, 서버 워크로드 전반에 걸친 활동데이터 수집
- 보안 분석과 위협 인텔리전스(TI)를 기반으로 위협 탐지 및 경보
- 개별 위협 경보의 연관성을 파악하여 Incident로 통합
- 자체 TI 및 외부 TI를 활용한 IOC Sweeping
- 위험 레벨 구분
- 상관관계 분석 및 위협 상세분석
- 의심스러운 객체(SO) 정보 배포
- 엔드포인트 취약점 감사
- 고위험 경고에 대한 자동 대응(Response)
- SIEM, SOAR 및 Third Party 연동

위협의 전체 스토리와 상관관계를 킬체인 형태로 제공(Insight)

- Workbench로 감지된 위협의 전체 체인을 시각화. MITER ATT & CK Technique에 따라 어떤 활동을 위협으로 감지했는지 확인.
- 각 객체를 선택하고 Execution Profile(상세 조사) 및 Response(대응) 기능을 수행.



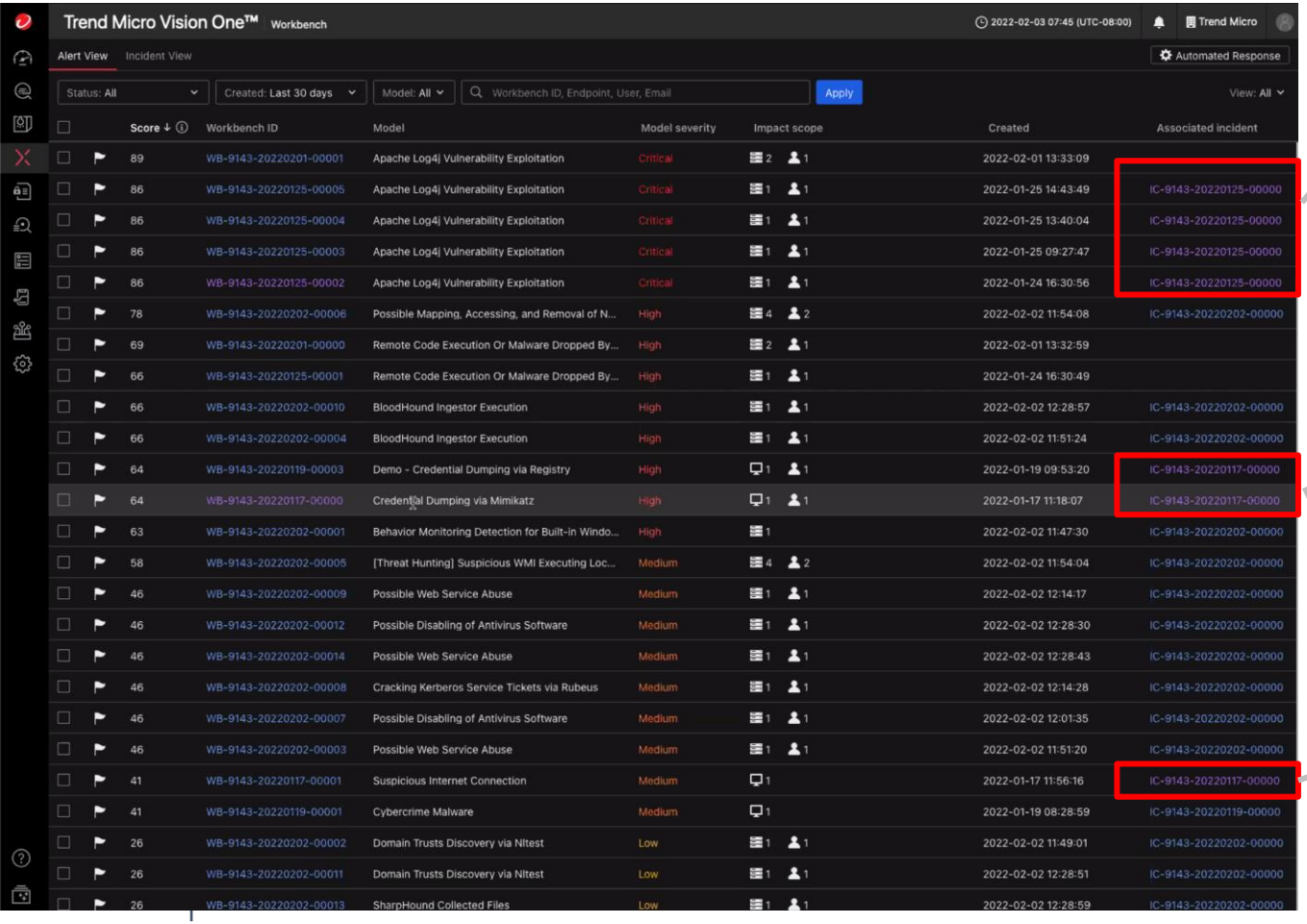
개체를 마우스 오른쪽 클릭하여 상세 조사 및 대응(Response) 기능을 수행

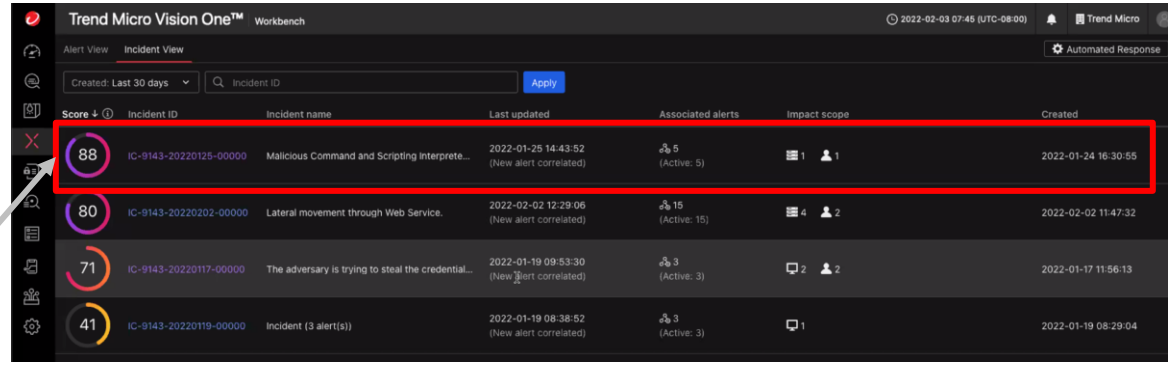


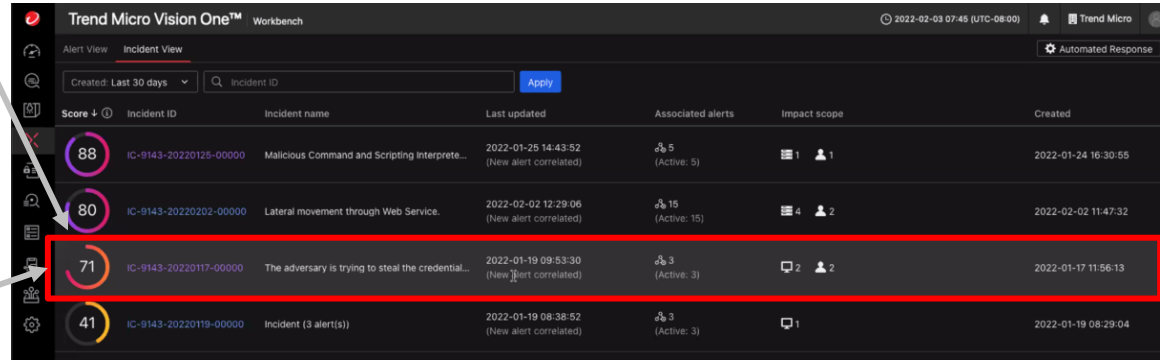
Execution Profile 의해 실행 된 프로세스의 흐름을 체인 형태로 가시화

개별 위협 경고의 상관관계를 하나의 Incident로 통합

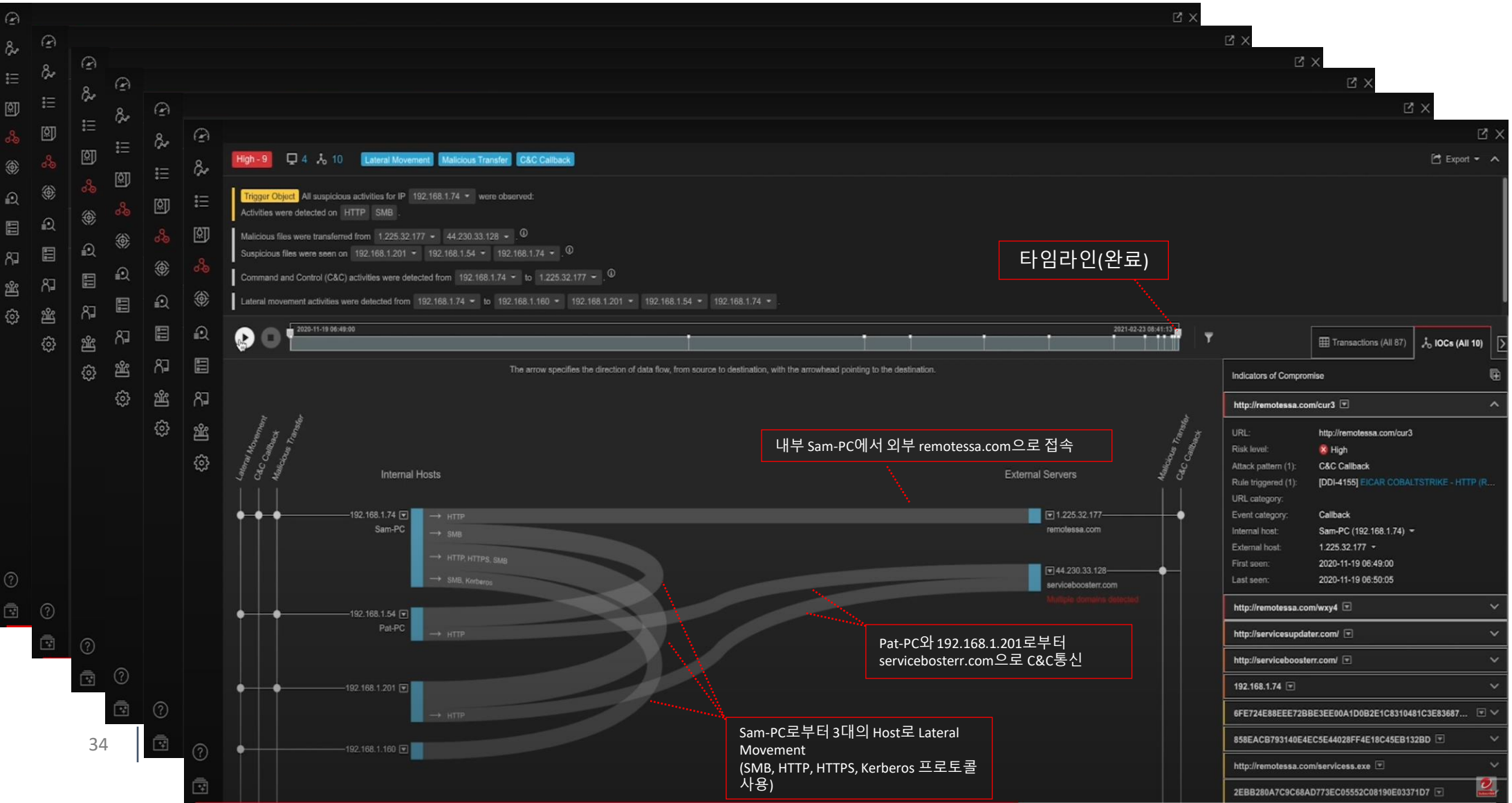
개별 Workbench 경고들의 연관성을 파악하여 하나의 Incident로 자동 통합







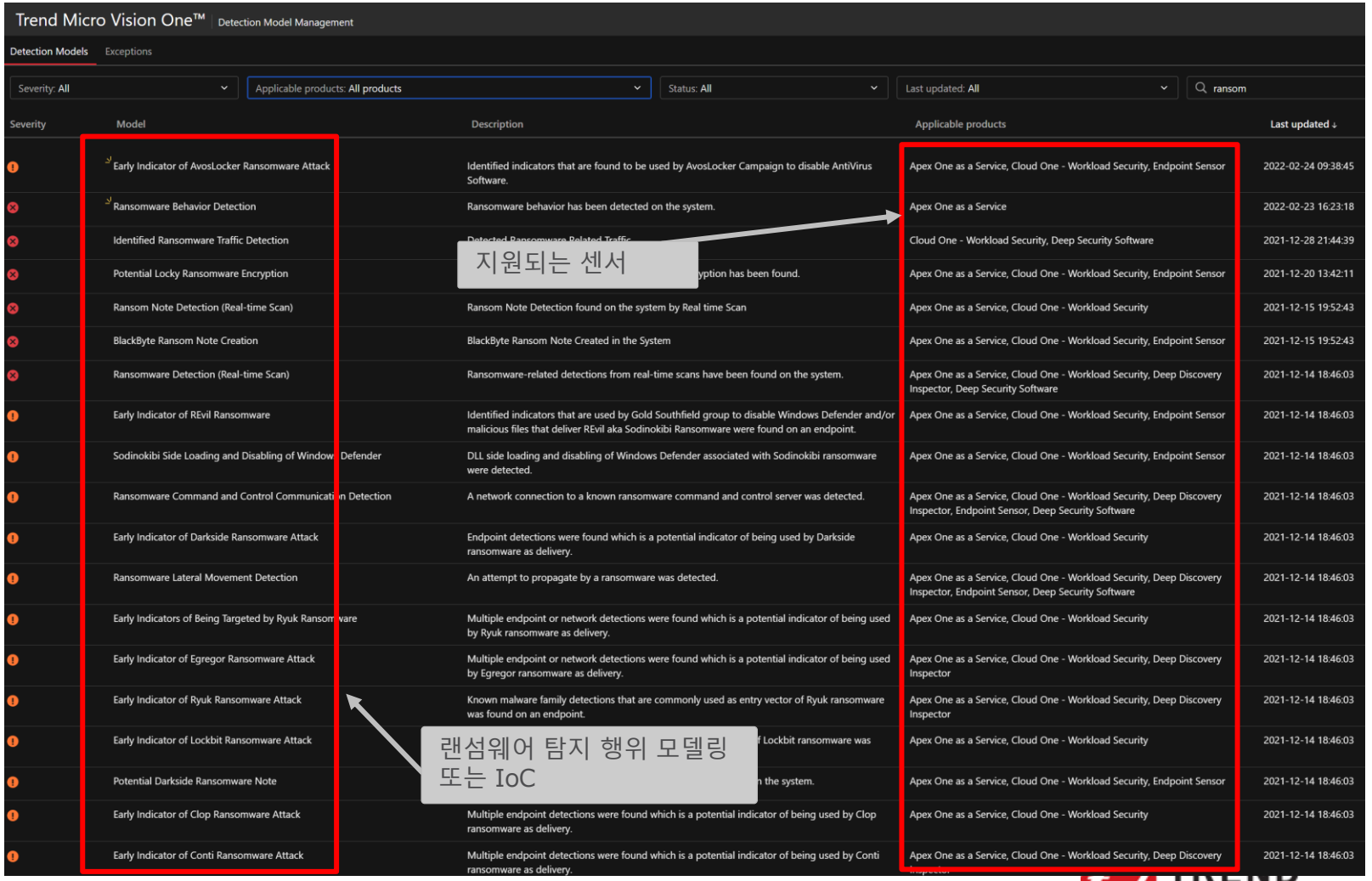
네트워크 위협 플로우 제공

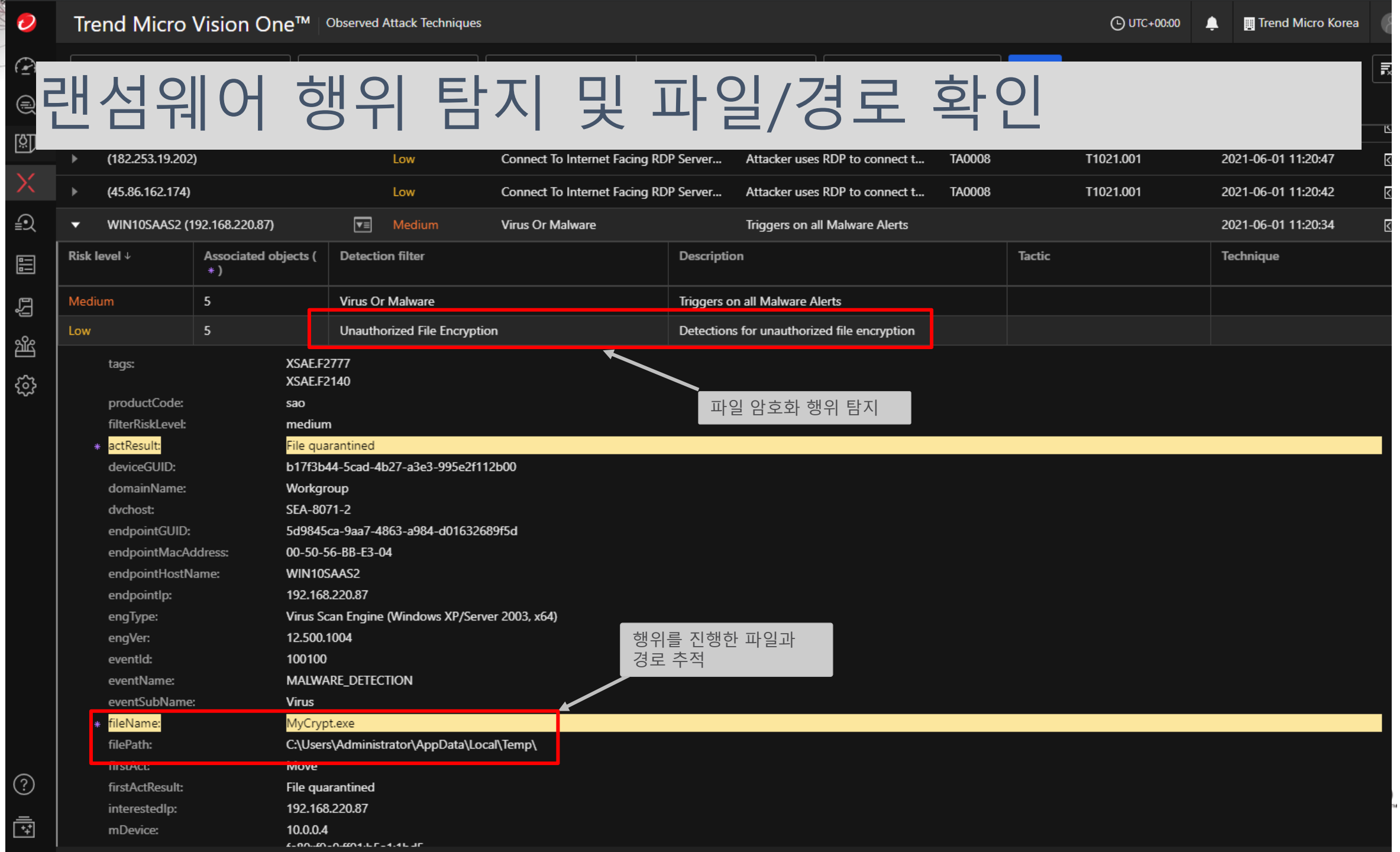


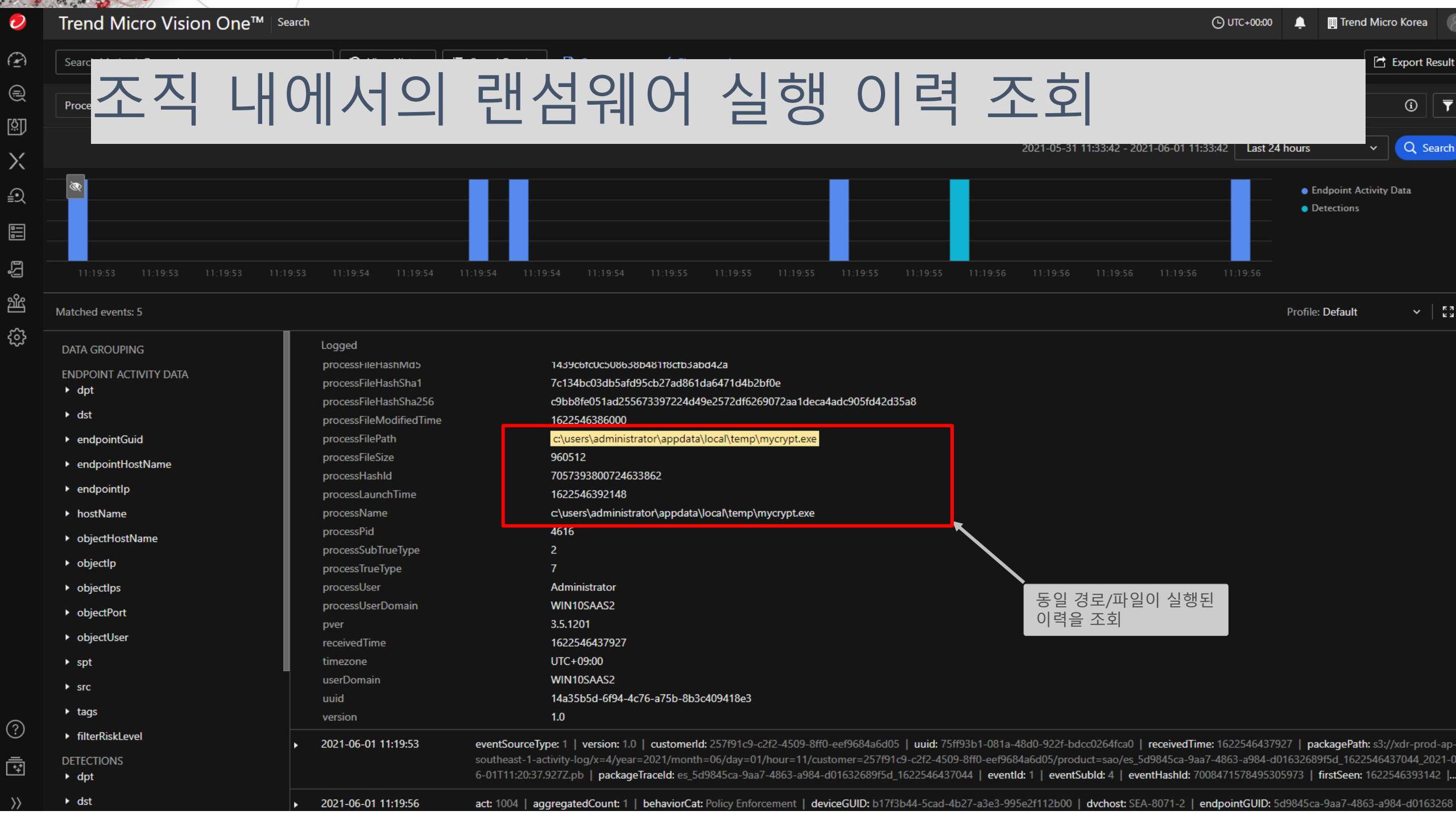
시간의 흐름에 따른 내외부 호스트간의 통신과 Lateral Movement, C&C 통신 상세 정보, 주목해야 하는 IOC정보를 파악

랜섬웨어 행위 탐지 모델 및 IOC

- XDR 전용센서, Apex One, Cloud One Workload Security 등의 트렌드마이크로 XDR센서가 설치된 엔드포인트에서 랜섬웨어의 행위 탐지 모델과 일치되는 행위를 탐지
- 랜섬웨어 IoC와 일치하는 객체 탐지
- 탐지된 이벤트는 상관관계를 킬체인으로 표현하여 XDR Workbench에서 알람 및 인시던트를 생성




Trend Micro Vision One™
Observed Attack Techniques
UTC+00:00
Trend Micro Korea
랜섬웨어 행위 탐지 및 파일/경로 확인
(182.253.19.202) Low Connect To Internet Facing RDP Server... Attacker uses RDP to connect t... TA0008 T1021.001 2021-06-01 11:20:47
(45.86.162.174) Low Connect To Internet Facing RDP Server... Attacker uses RDP to connect t... TA0008 T1021.001 2021-06-01 11:20:42
WIN10SAAS2 (192.168.220.87) Medium Virus Or Malware Triggers on all Malware Alerts 2021-06-01 11:20:34
Risk level
Associated objects (*)
Detection filter
Description
Tactic
Technique
Medium 5 Virus Or Malware Triggers on all Malware Alerts
Low 5 Unauthorized File Encryption Detections for unauthorized file encryption
파일 암호화 행위 탐지
tags: XSAE.F2777 XSAE.F2140
productCode: sao
filterRiskLevel: medium
actResult: File quarantined
deviceGUID: b17f3b44-5cad-4b27-a3e3-995e2f112b00
domainName: Workgroup
dvchost: SEA-8071-2
endpointGUID: 5d9845ca-9aa7-4863-a984-d01632689f5d
endpointMacAddress: 00-50-56-BB-E3-04
endpointHostName: WIN10SAAS2
endpointIp: 192.168.220.87
engType: Virus Scan Engine (Windows XP/Server 2003, x64)
engVer: 12.500.1004
eventId: 100100
eventName: MALWARE_DETECTION
eventSubName: Virus
행위를 진행한 파일과 경로 추적
fileName: MyCrypt.exe
filePath: C:\Users\Administrator\AppData\Local\Temp\
firstAct: Move
firstActResult: File quarantined
interestedIp: 192.168.220.87
mDevice: 10.0.0.4


Trend Micro Vision One™
Search
UTC+00:00
Trend Micro Korea
Export Result
조직 내에서의 랜섬웨어 실행 이력 조회
2021-05-31 11:33:42 - 2021-06-01 11:33:42
Last 24 hours
Search
Endpoint Activity Data
Detections
11:19:53
11:19:54
11:19:55
11:19:56
Matched events: 5
Profile: Default
DATA GROUPING
ENDPOINT ACTIVITY DATA
dpt
dst
endpointGuid
endpointHostName
endpointIp
hostName
objectHostName
objectIp
objectIps
objectPort
objectUser
spt
src
tags
filterRiskLevel
DETECTIONS
dpt
dst
Logged
processFileHashSha1 7c134bc03db5afd95cb27ad861da6471d4b2bf0e
processFileHashSha256 c9bb8fe051ad255673397224d49e2572df6269072aa1deca4adc905fd42d35a8
processFileModifiedTime 1622546386000
processFilePath c:\users\administrator\appdata\local\temp\mycrypt.exe
processFileSize 960512
processHashId 7057393800724633862
processLaunchTime 1622546392148
processName c:\users\administrator\appdata\local\temp\mycrypt.exe
processPid 4616
processSubTrueType 2
processTrueType 7
processUser Administrator
processUserDomain WIN10SAAS2
pver 3.5.1201
receivedTime 1622546437927
timezone UTC+09:00
userDomain WIN10SAAS2
uuid 14a35b5d-6f94-4c76-a75b-8b3c409418e3
version 1.0
동일 경로/파일이 실행된 이력을 조회
2021-06-01 11:19:53
2021-06-01 11:19:56

랜섬웨어 위협 체인 분석

Analysis Chain | Object Details

Target endpoint
Host name:
win10saas2
IP address:
192.168.220.87
Matched criteria:
(Matched any of the following)
undefined c:\users\administrator\appdata\local\temp

First observed object
ransomware_v026.exe
Chain 1
2021-06-01 11:19:23

Matched object (1)
Process: mycrypt.exe

Noteworthy objects
4

랜섬웨어 위협 체인 생성

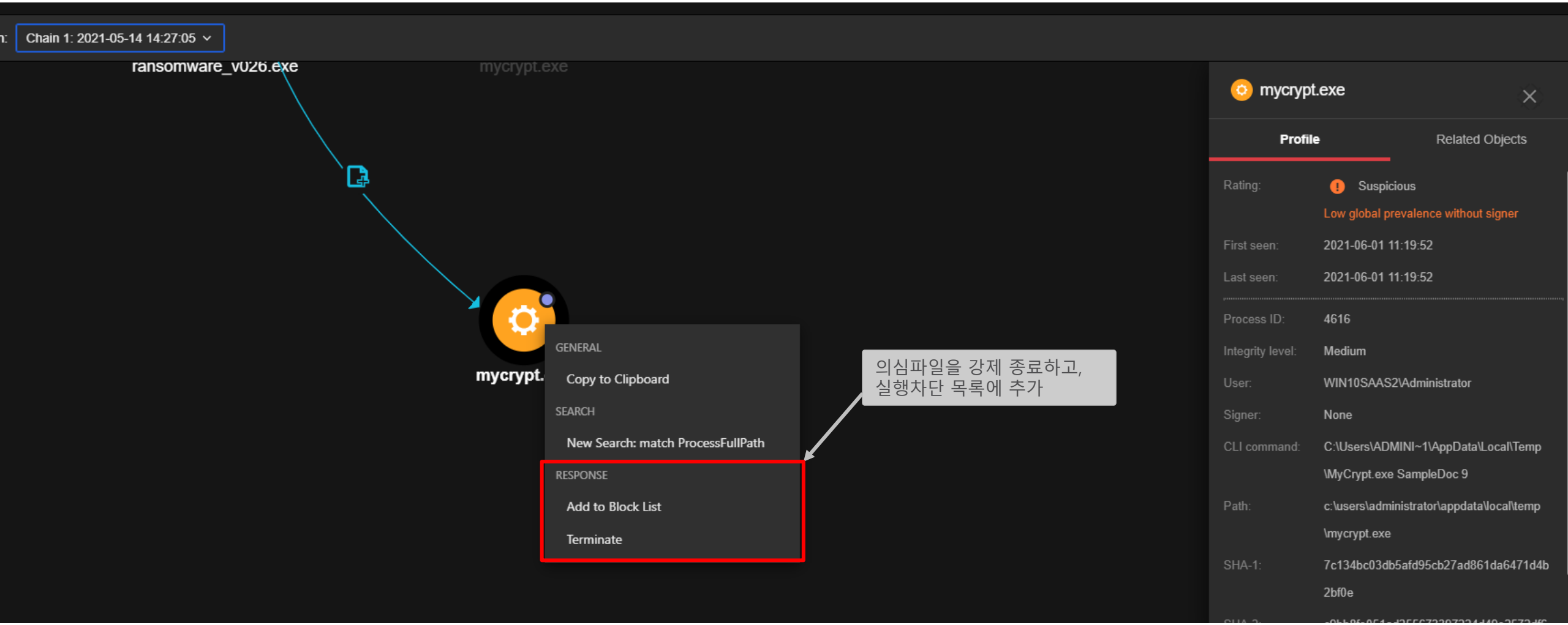
1 matched chain: Chain 1: 2021-05-14 14:27:05

mycrypt.exe

Profile | Related Objects

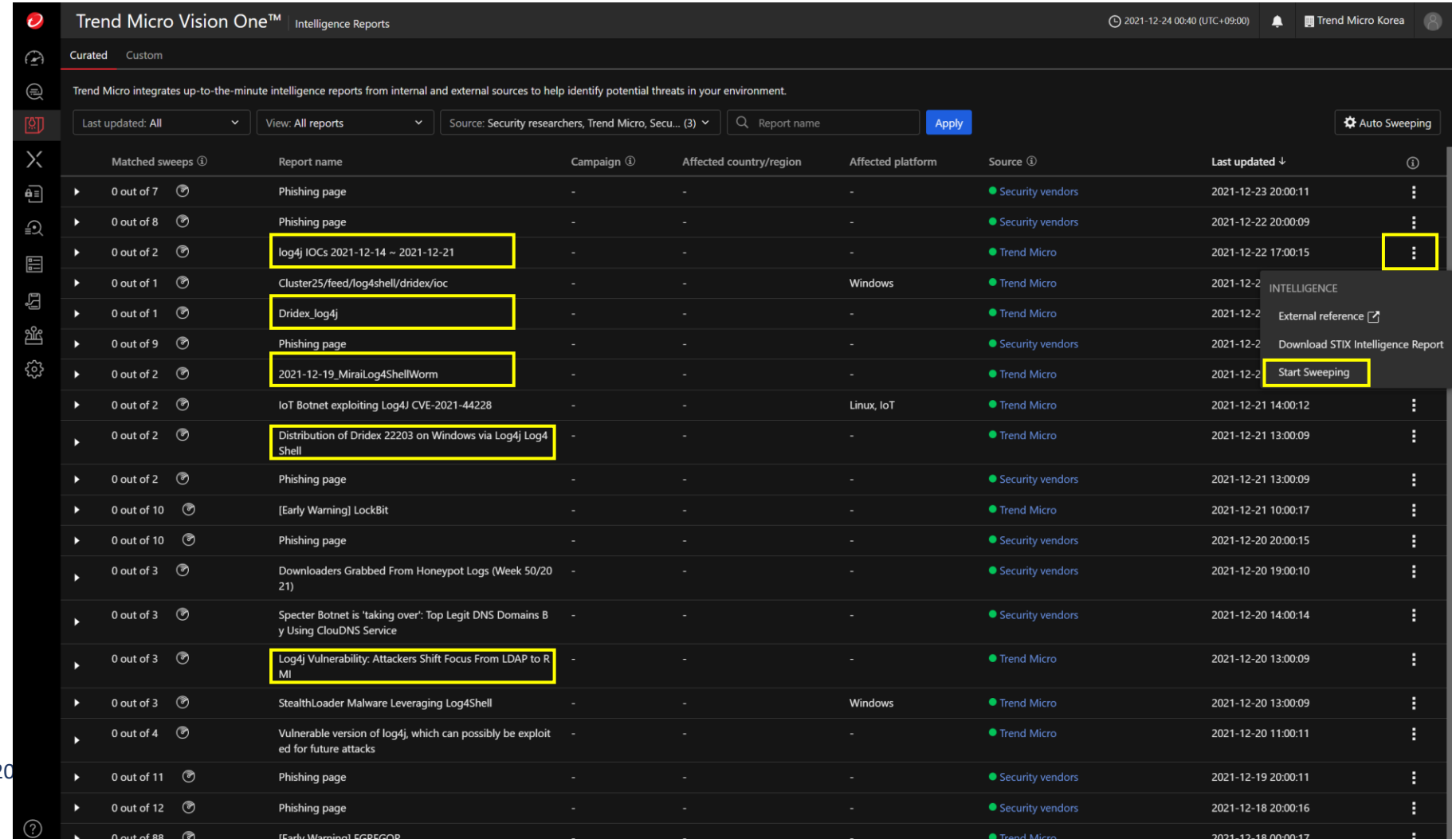
Rating:	Suspicious
	Low global prevalence without signer
First seen:	2021-06-01 11:19:52
Last seen:	2021-06-01 11:19:52
Process ID:	4616
Integrity level:	Medium
User:	WIN10SAAS2\Administrator
Signer:	None
CLI command:	C:\Users\ADMINI~1\AppData\Local\Temp\MyCrypt.exe SampleDoc 9
Path:	c:\users\administrator\appdata\local\temp\mycrypt.exe
SHA-1:	7c134bc03db5afd95cb27ad861da6471d4b

Unknown 랜섬웨어 조치



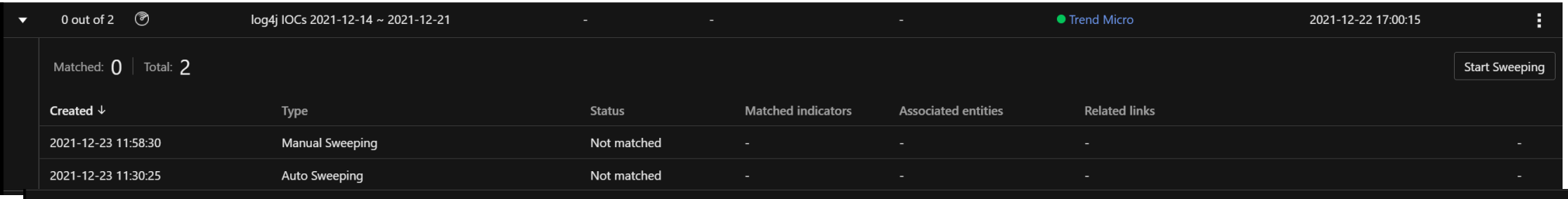
위협인텔리전스 활용 - IOC를 이용한 Sweeping

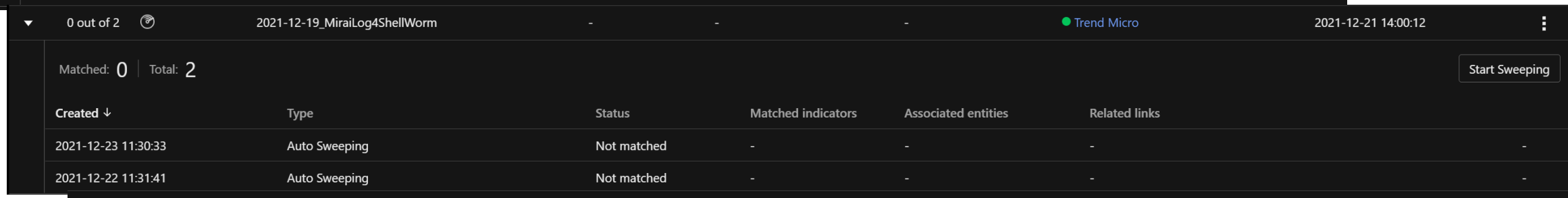
자동으로 다운로드된 Log4j IOC 들을 확인한 후 우측의 Start Sweeping 시작

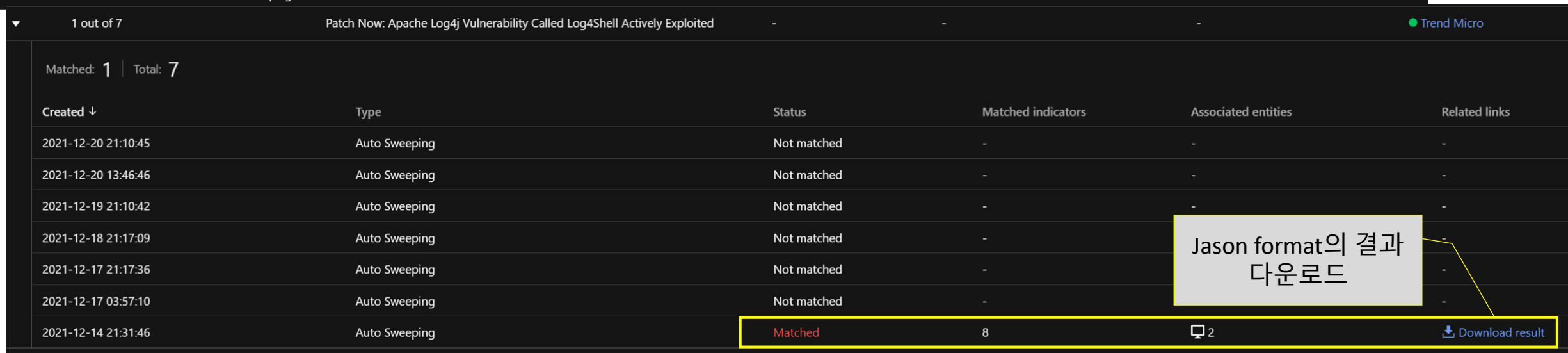


위협인텔리전스 활용 - IOC를 이용한 Sweeping

IOC Sweeping 결과 확인

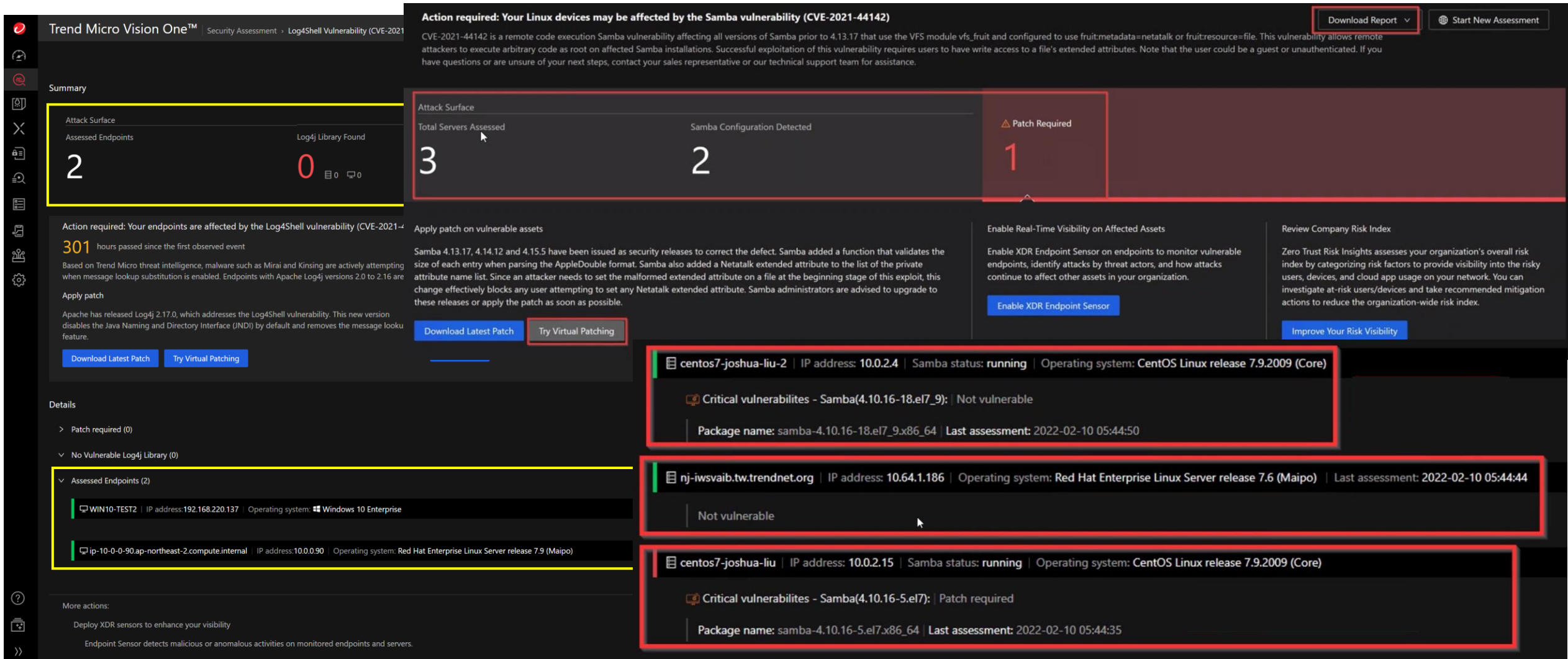






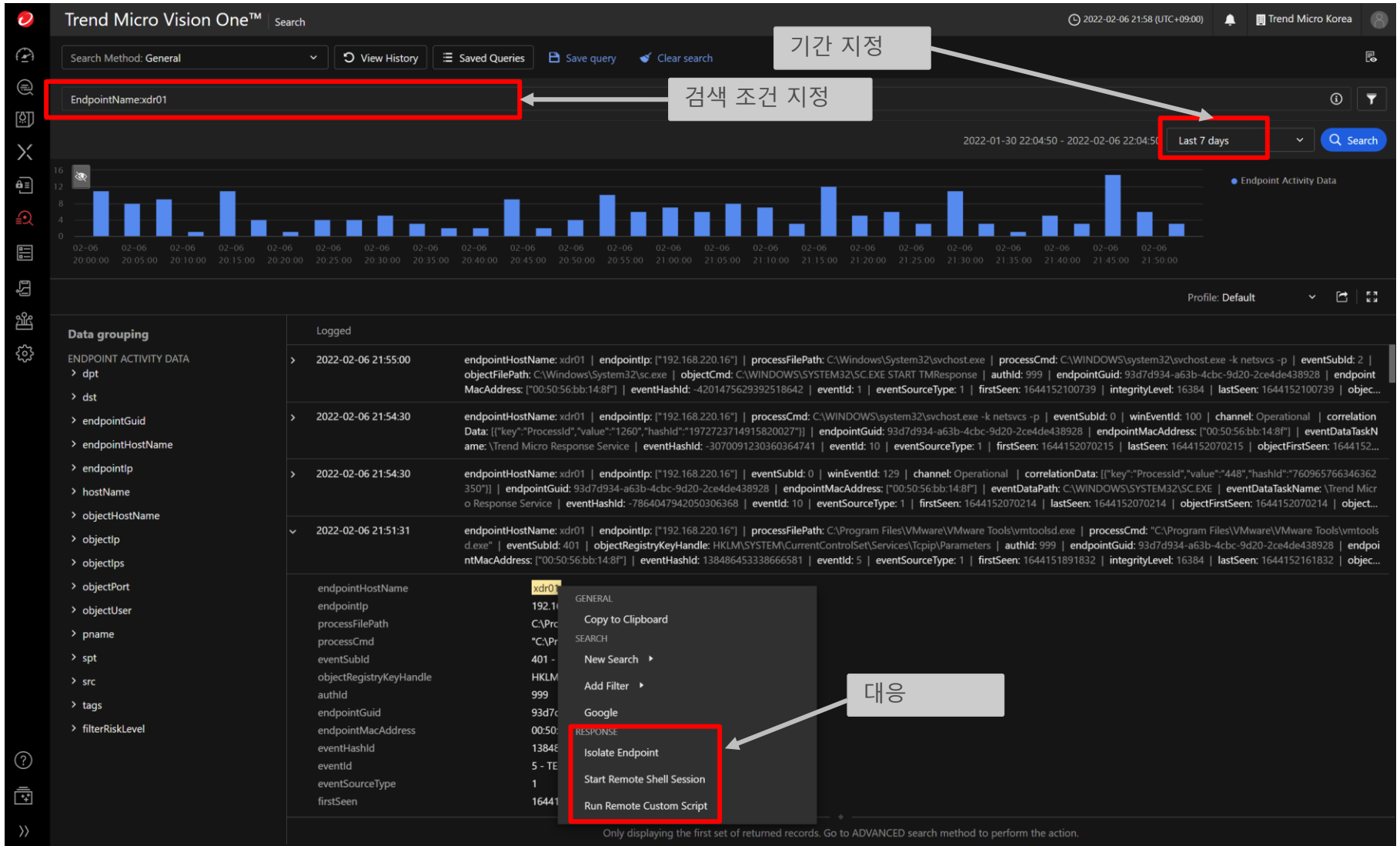
Security Assessment를 활용한 취약점 감사

Assessment 결과 확인



활동데이터 조회를 통한 위협 헌팅

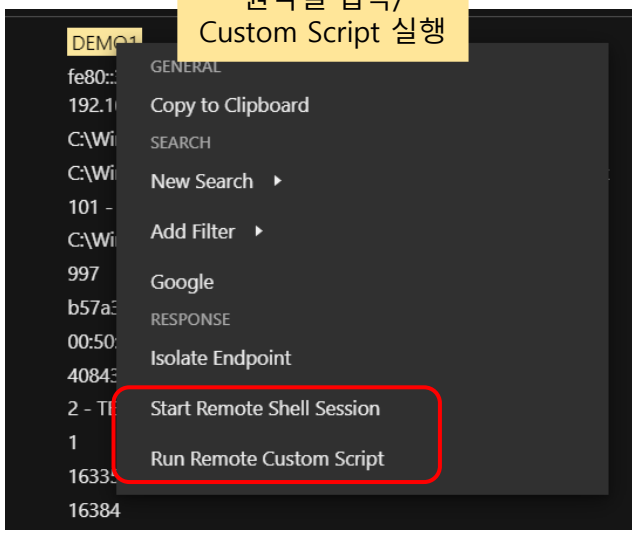
- 검색하고자 하는 값을 Activity 데이터로부터 쿼리. 위협 헌팅에 활용
- 유연한 검색 조건에서 활동 데이터를 검색 할 수 있는 기능. Workbench와 Observed Attack Techniques에서 발견되지 않은 데이터를 포함하여 검색 가능



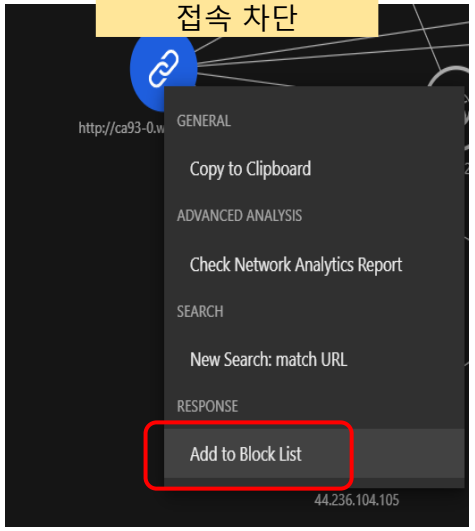
랜섬웨어 발견 시 조치할 수 있는 다양한 Response 기능

파일 실행 차단
파일 수집

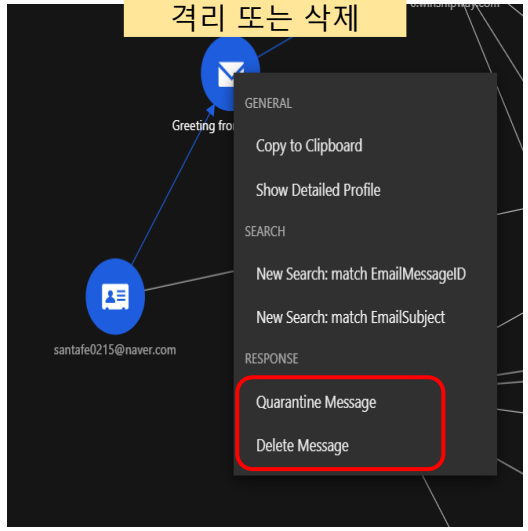
원격셸 접속/
Custom Script 실행



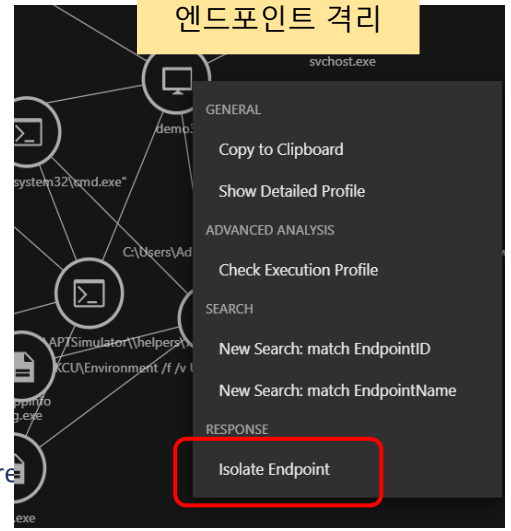
URL 또는 IP주소
접속 차단



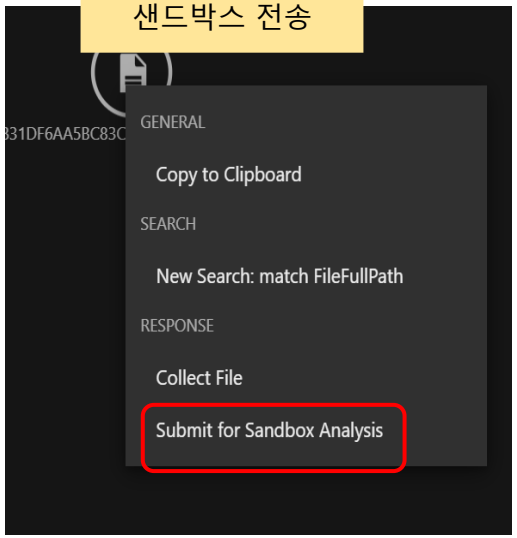
메일 메시지
격리 또는 삭제



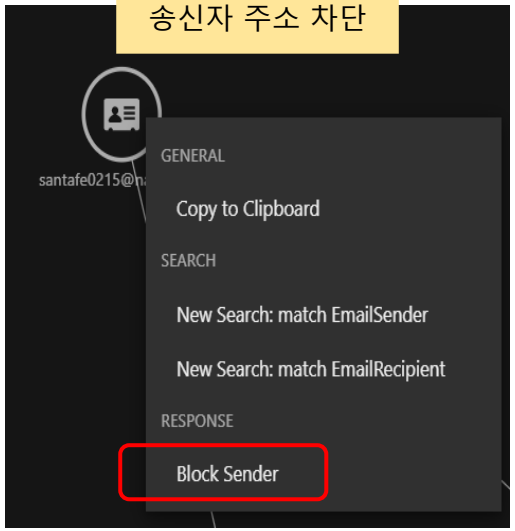
엔드포인트 격리



샌드박스 전송

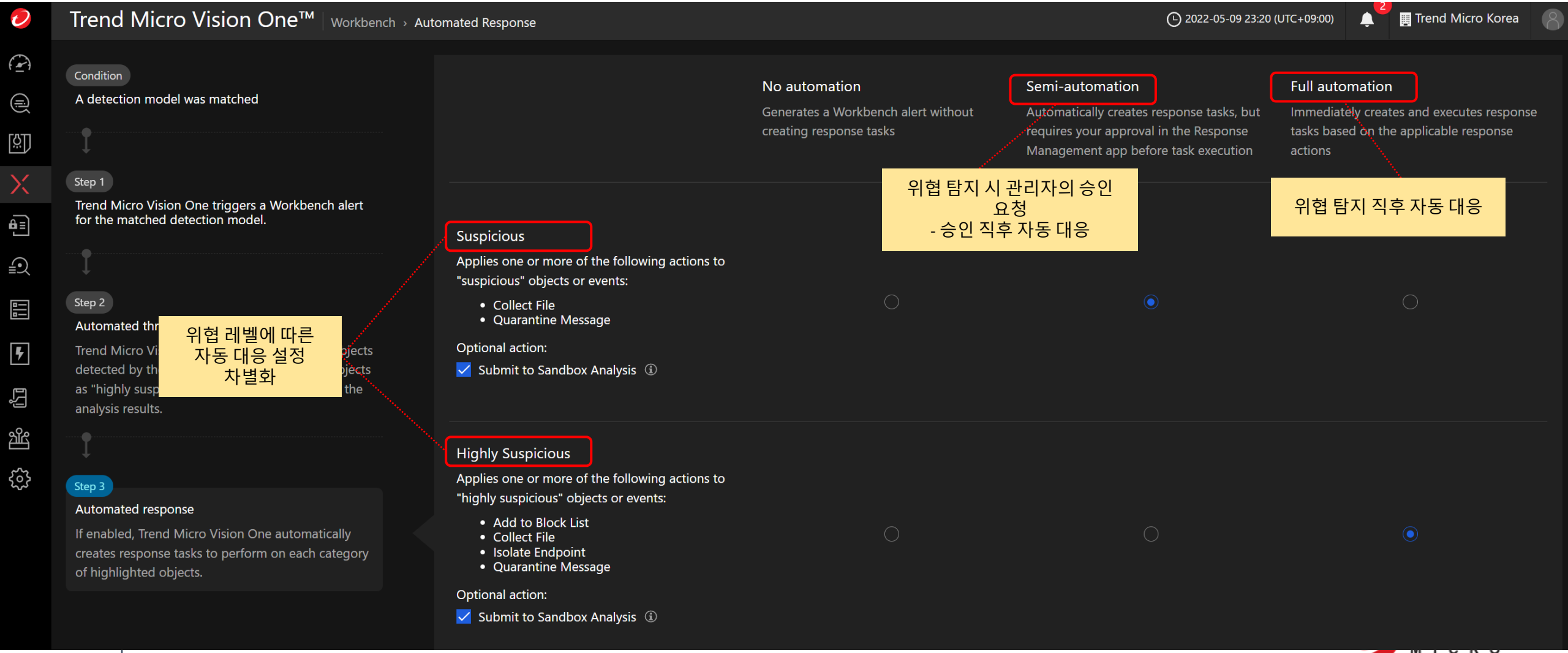


송신자 주소 차단



대응의 자동화 구현

탐지된 위협 레벨에 따라 자동화된 대응 적용



THE FORRESTER NEW WAVE™

Extended Detection & Response(XDR) Q4 2021

트렌드마이크로는 평가 대상 벤더사 14곳 중 원격 텔레메트리 감지, 조사 및 대응 기능 부문에서 가장 뛰어나다는 평가를 받았다. 이외에도, 이번 보고서의 열 개 평가 부문 중 ▲가시성 ▲탐지 ▲조사 ▲제품 아키텍처 ▲위협 헌팅 ▲제품 보안 ▲제품 비전 부문 등 총 일곱 개 부문에서 우수한 평가를 받음으로써 가장 높은 점수를 기록했다.

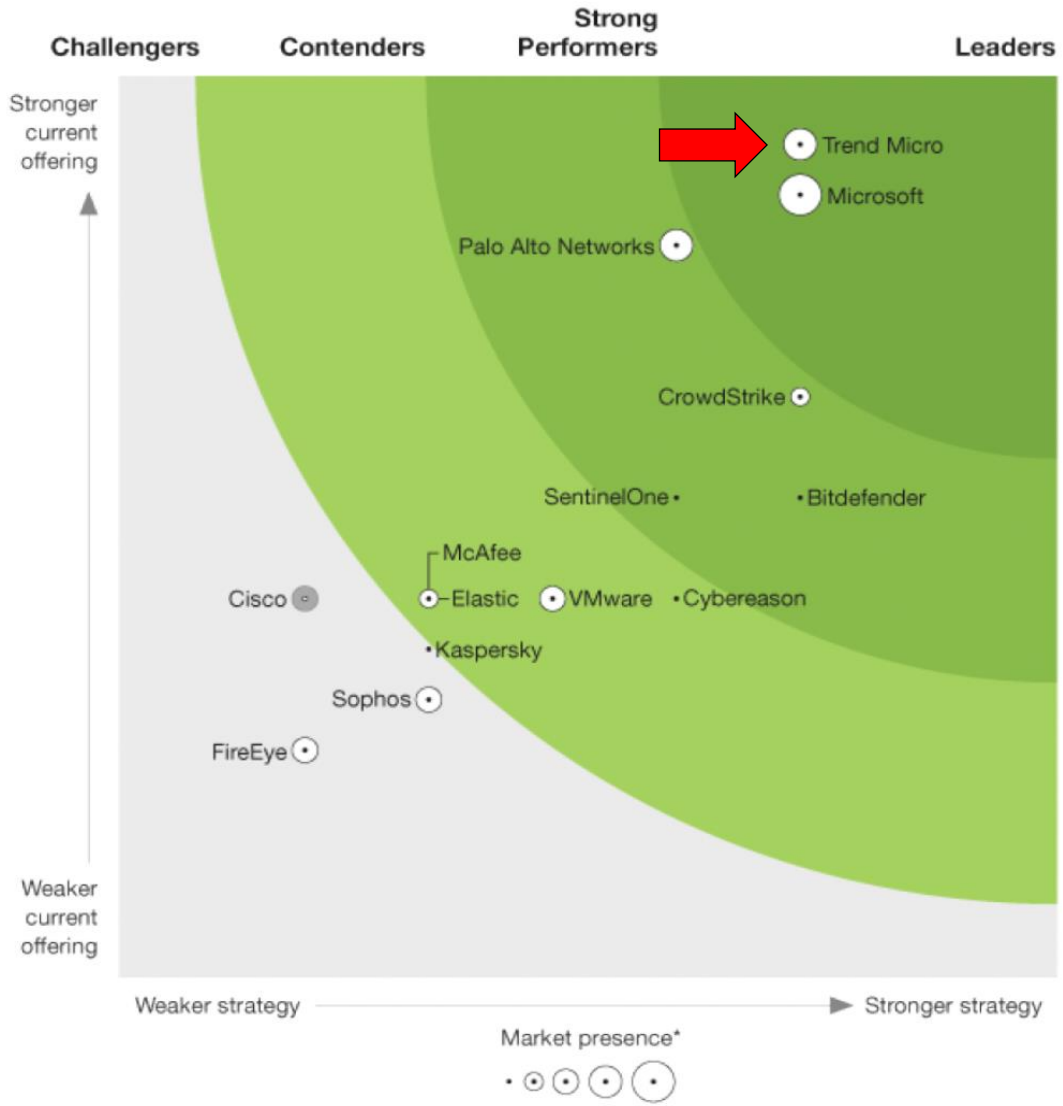
포레스터 뉴 웨이브 측은 이번 보고서를 통해 "트렌드마이크로만의 차별화된 기능은 보안 스택에서 환경을 완벽하게 파악할 수 있으며 아주 효과적이다"라며, "트렌드마이크로의 플랫폼은 각 계층의 보안 솔루션에 대한 텔레메트리(Telemetry)로의 연동과, 최고의 고객 서비스를 제공한다. 따라서 강력하고 운영하기 쉬운 보안 솔루션을 찾고 있는 기업은 트렌드마이크로를 고려할 것을 추천한다"고 평가했다.

또한 보고서는 트렌드마이크로가 제품의 보안 효율성을 신뢰하는 충성 고객을 확보하고 있다고 언급하며 이러한 고객들은 트렌드마이크로의 로드맵 투명성과 고객 지원의 우수성을 높이 평가한다고 덧붙였다.

THE FORRESTER NEW WAVE™

Extended Detection And Response (XDR) Providers

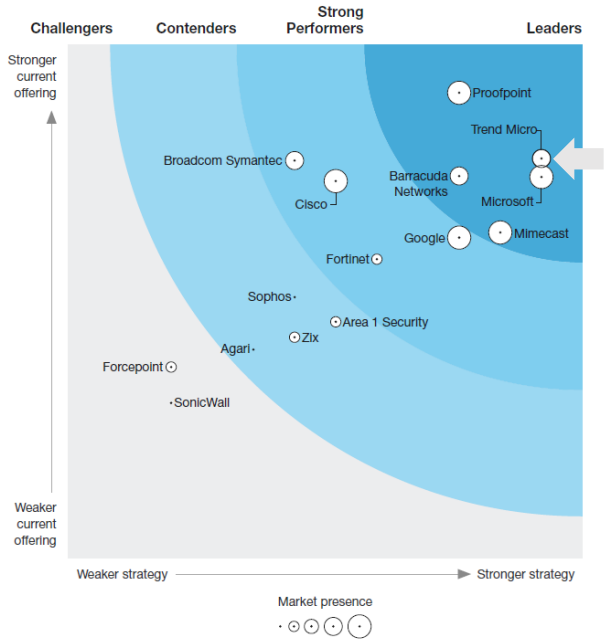
Q4 2021



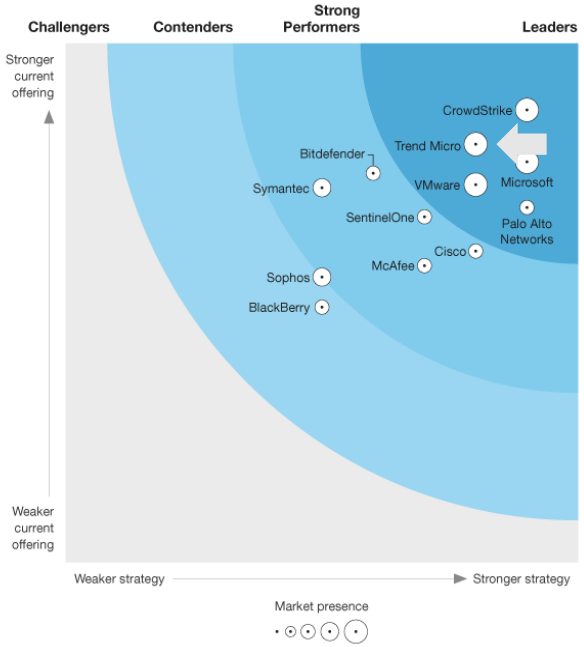
*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Leading Security Across the Enterprise

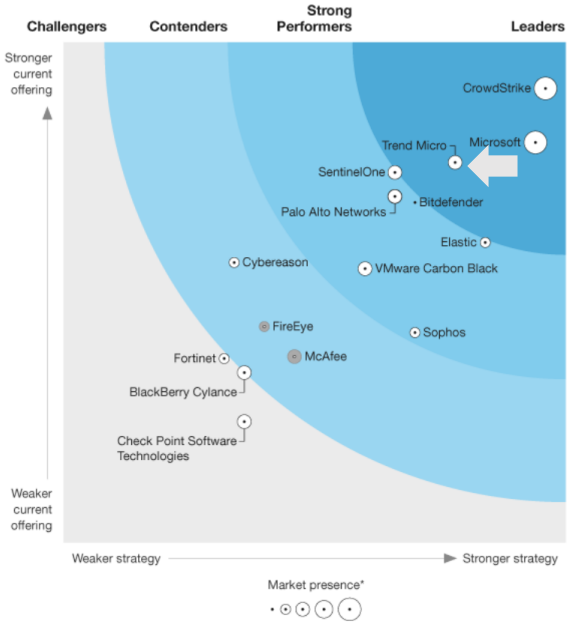


The Forrester Wave™: **Enterprise Email Security**, Q2 2021



The Forrester Wave™: **Endpoint Security Software as a Service**, Q2 2021

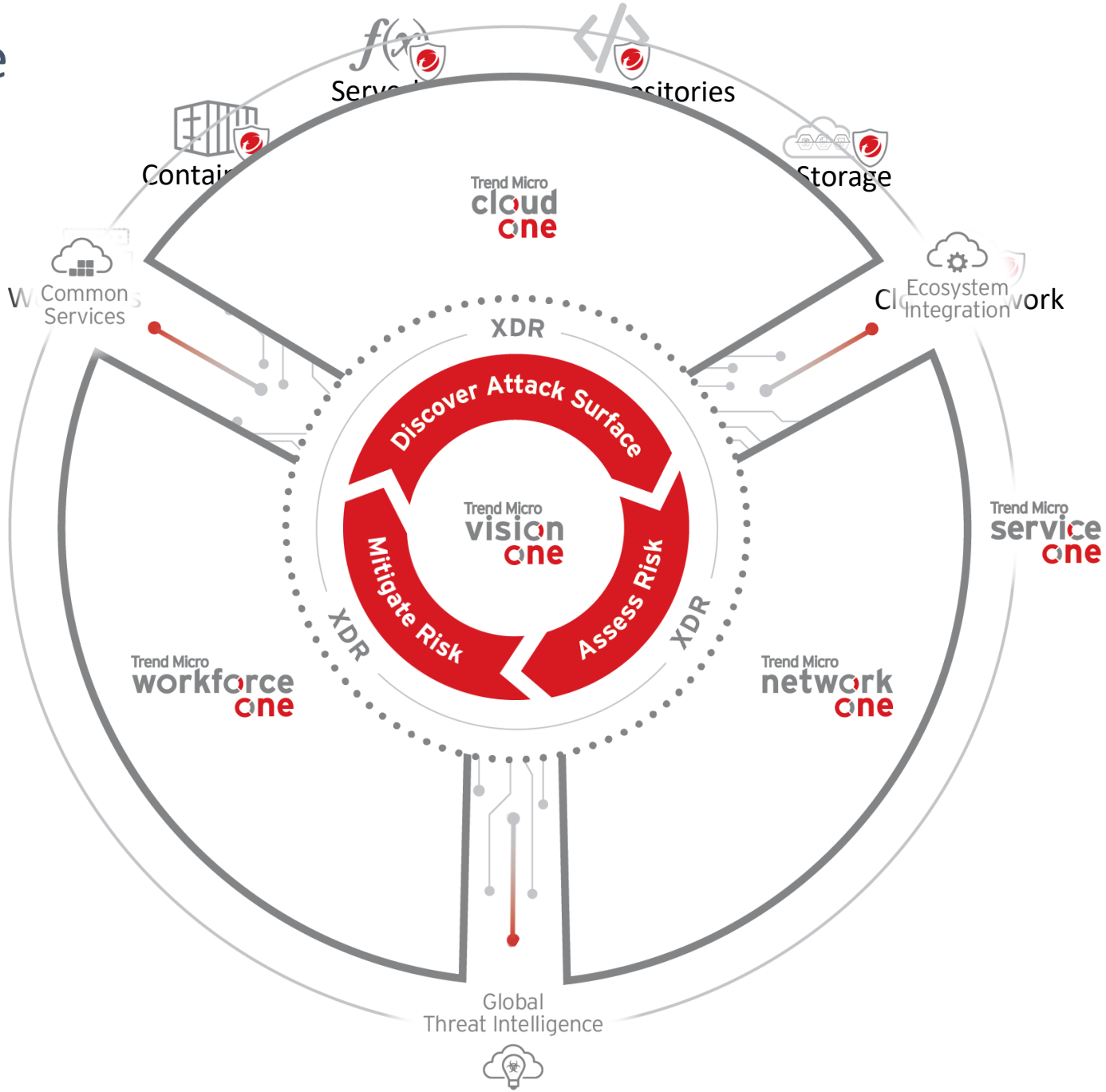
The Forrester New Wave™: **Extended Detection and Response (XDR)** Providers, Q4 2021



The Forrester Wave™: **Endpoint Detection and Response**, Q2 2022

"The Forrester Wave ™is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change."

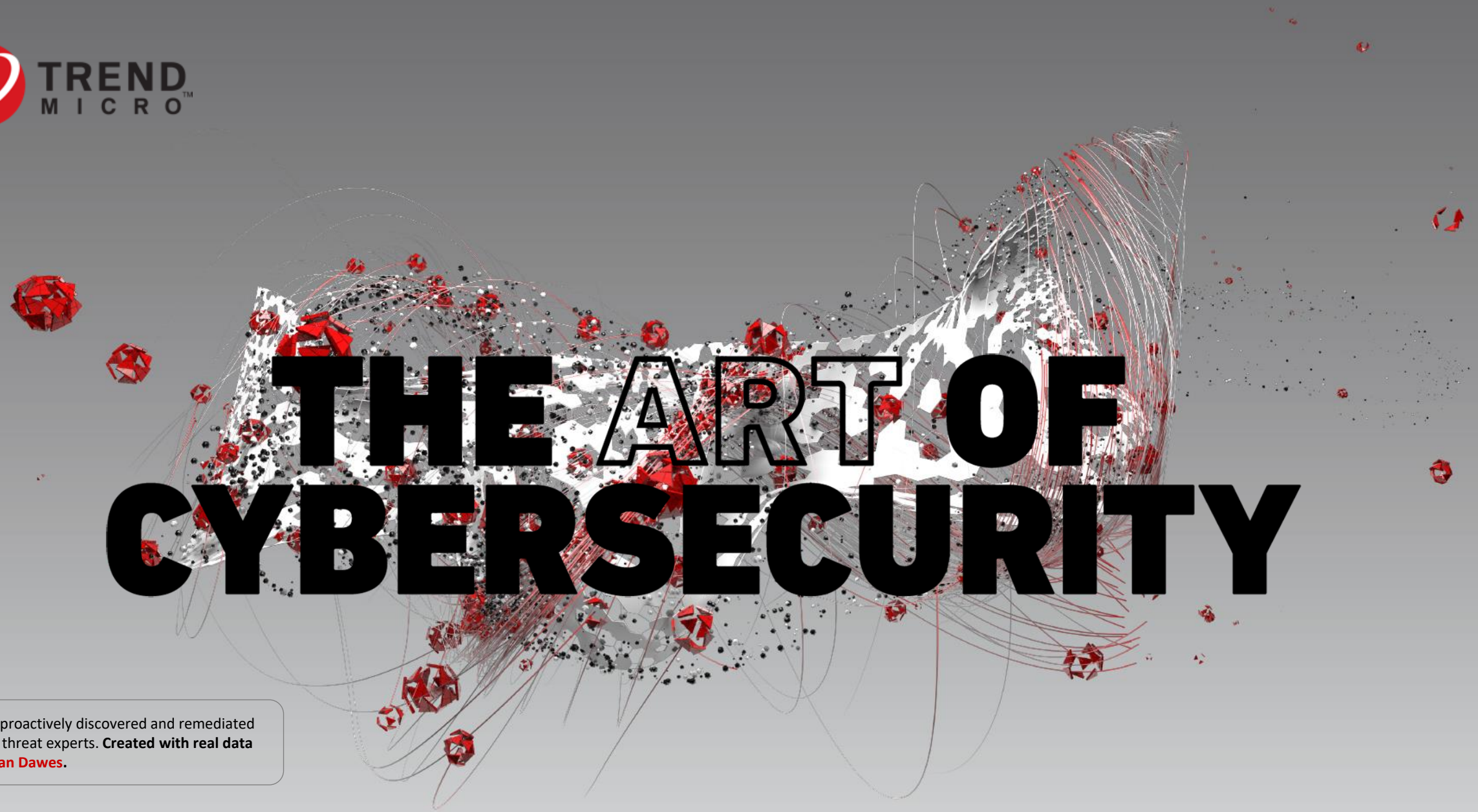
The Attack Surface Risk Management Lifecycle



Trend Micro one

A unified cybersecurity platform

TREND MICRO™



Hidden threats proactively discovered and remediated by Trend Micro threat experts. **Created with real data by artist Brendan Dawes.**

진화하는 랜섬웨어와 EDR의 역할

지니언스 홍재의 수석

통합 보안 플랫폼 기업, 지니언스

진화하는 랜섬웨어와 EDR의 역할

Genians

Table of Contents

01. 랜섬웨어의 진화

01 시스템 화면 잠금

- 시스템에 접근하지 못하도록 차단하는 시스템 화면 잠금

➢ 안전모드 부팅 후 시스템 복원

02 파일 암호화

- 악성파일을 활용해 시스템 내부의 문서 파일을 암호화 하는 형태

➢ 복원이 어려운 형태로 진화

03 공격 방법의 진화

- 공격 방법의 지능화/고도화

➢ Fileless 형태
➢ 제로데이 취약점

01. 랜섬웨어의 진화

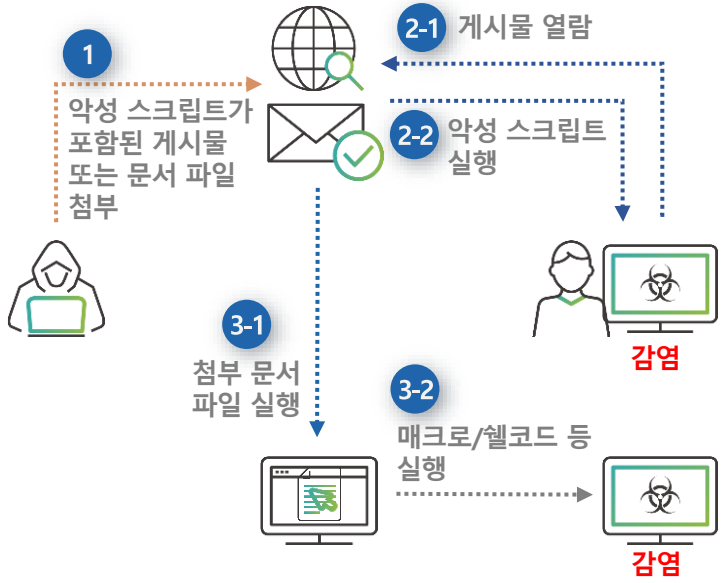
➢ 공격 방법의 지능화/고도화

01 무차별 배포

- 이메일/웹 등을 통한 랜섬웨어 파일의 무차별 배포

➢ **백신 등 기 보안솔루션의 빠른 업데이트 등을 통한 대응**

02 취약점 악용



- Fileless 형태로 진화
- Office/브라우저 등의 취약점을 악용하여 사용자 모르게 메모리 상 동작이나 스크립트 형태의 백그라운드 동작
- 정상적인 시스템 프로세스를 통한 암호화

➢ **행위 분석 기반 보안솔루션 등을 통한 대응**

03 침투 후 배포

침투	목표 대상 침투를 위한 정보 수집 후 취약점을 통해 침투 시도
정찰	내부 시스템/인프라 구조, 관리자 권한 획득 등을 위한 정찰 및 정보 수집
유출	기밀 정보 획득 및 외부 유출
감염	파일 암호화 및 흔적 삭제

- 사회공학/취약점 등 해킹을 통한 내부 침투
- 관리자 권한 획득
- 백신/보안 솔루션 등 우회 또는 무력화
- 정보 유출 후 암호화
- 내부 확산

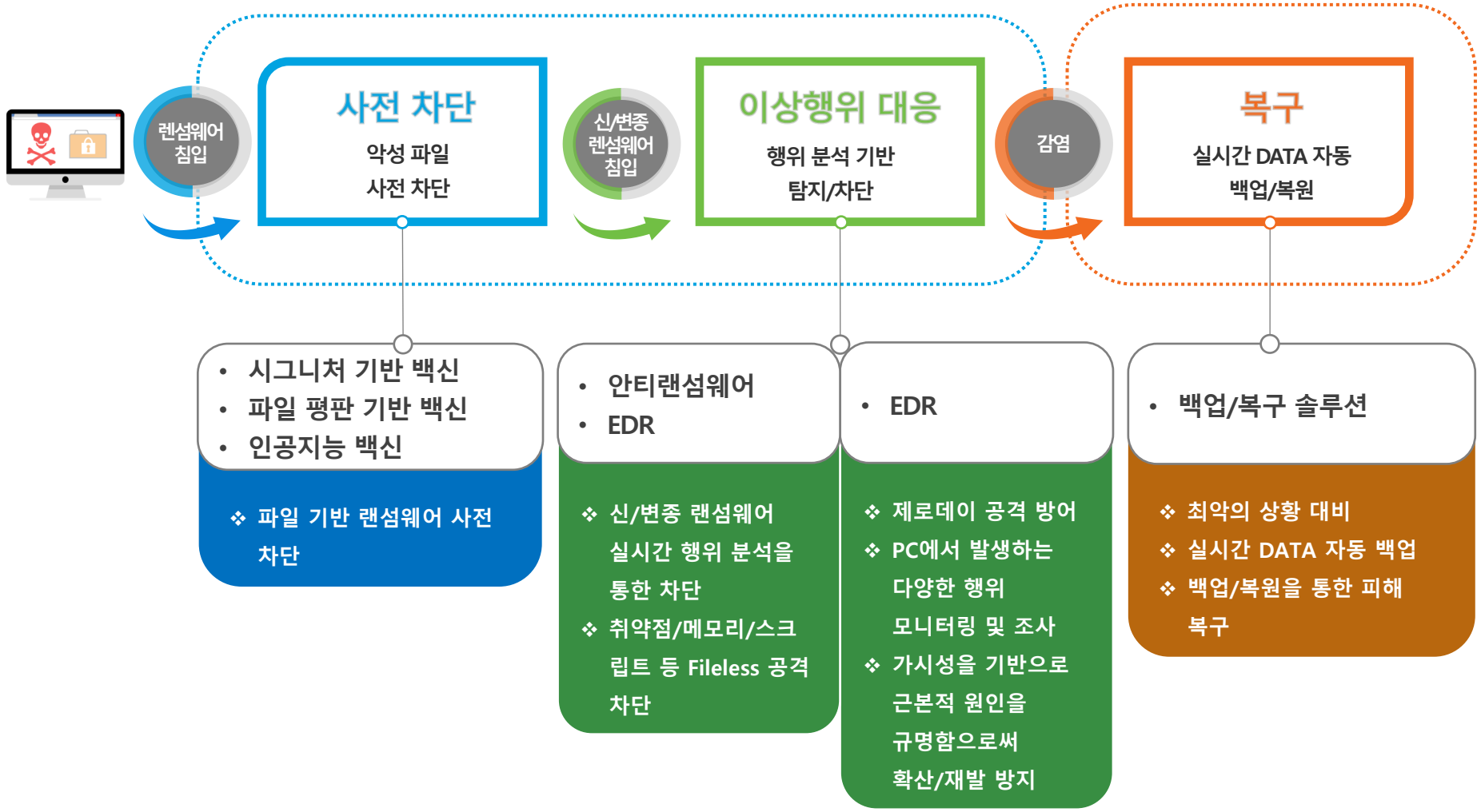
➢ **각 단계별 이상행위 사전 감지 및 행위 분석**

➢ **근본적인 원인 분석을 통한 확산/재발 방지**

✓최근의 랜섬웨어 공격은 APT 공격과 같이 지능형 공격 기법과 기술을 사용

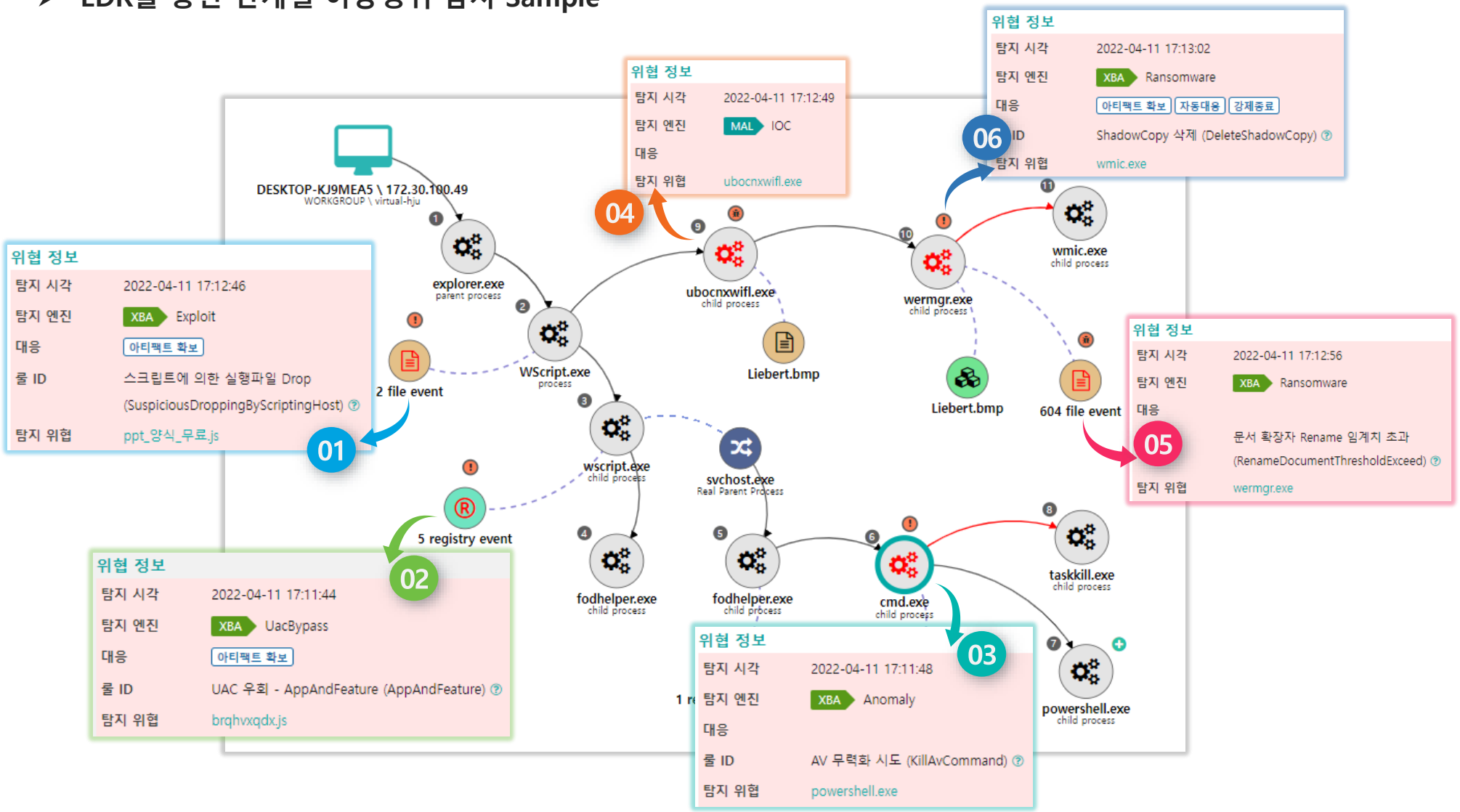
02. 랜섬웨어 대응

- 단일 솔루션으로는 대응에 한계
- 다양한 보안 솔루션을 구현하여 수준 높은 보안 위협 방지책 실행 필요



02. 랜섬웨어 대응

➢ EDR을 통한 단계별 이상행위 탐지 Sample



03. EDR의 역할

➢ 기존 보안 체계의 한계 보완

보안 담당자 관점의 현황 파악 어려움

- 악성파일 존재 여부 및 피해현황 파악의 한계
- 관리 감독 기관의 피해 상황 보고 요청 대응에 한계

지능화·고도화 공격 패턴

- Fileless, 잠복/은닉형 공격
- 소프트웨어/웹 취약점 공격

- 암호화된 공격 대응, 한계
- 가상화 환경 내 파일 조합 불가 및 다수의 샌드박스 회피 기법 존재

- 신종 랜섬웨어 및 지능형 공격 대응 한계
- 다수의 Anti-Virus 회피 기법 존재

네트워크 APT 대응 솔루션(샌드박스)

시그니처 기반 Anti-Virus

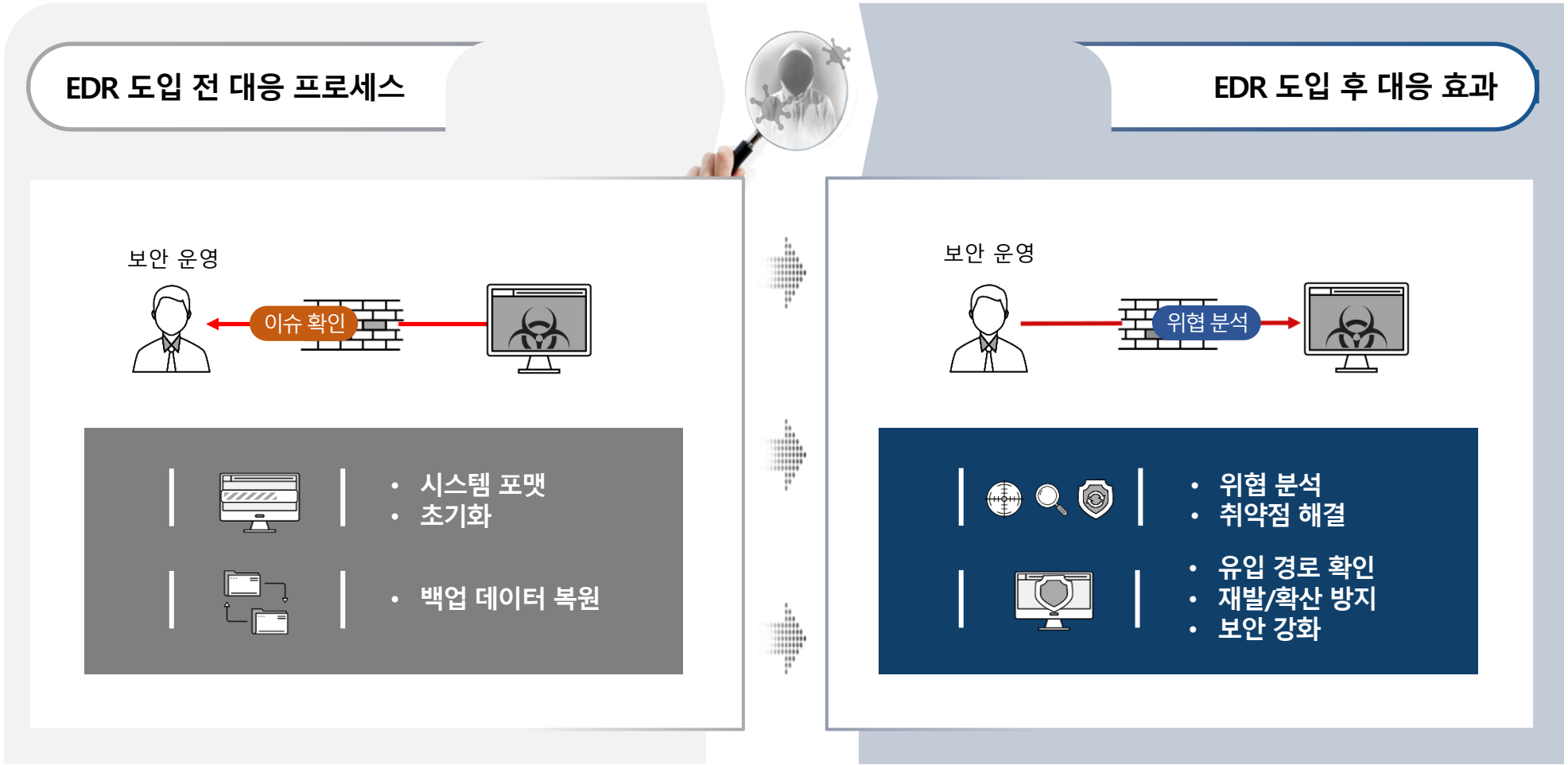
2021년 랜섬웨어 스페셜 리포트
(KISA. 2021년 9월)

보호대책 (보안솔루션)	. URL Filter, Firewall, IPS/IDS, 복호화 . SPAM Mail Filter . Malware Sand Box . Network Forensic Tool . SIEM (Security Info. Event Mgt.) . EDR (Endpoint Detection & Response)	. C&C(악성코드 유포지) 접속차단 . 피싱메일 차단(발송자,첨부,컨텐츠) . 악성코드 분석/탐지 . 감염확산 경로추적 . 보안 이벤트 통합 로그분석/관제 . 단말의 상세 로그분석/대응

표 15. 예방 대책과 사고 대응 체계

03. EDR의 역할

➢ 위협에 대한 가시성 확보를 통한 선제적 대응 및 위협 분석을 통한 엔드포인트 강화



03. EDR의 역할 – Genian EDR 개요

- Genian EDR은
- 단말에 대한 지속적인 모니터링 및 상시 정보 수집을 통해 위협의 탐지 및 분석, 대응을 제공하는 **단말 이상 행위 탐지 및 대응(Endpoint Detection & Response)** 솔루션입니다.

1 수집

단말 행위 상시 모니터링/수집

- File, Module, Process, Connection, Registry 정보
- 사용자 및 단말에서 발생하는 이상 행위
- 외부 저장매체 사용 현황
- 윈도우 이벤트 로그 수집
- 다양한 대시보드 제공

2 탐지

위협의 탐지

- IOC(침해지표) 기반의 알려진 위협 탐지
- ML(머신러닝) 기반의 알려지지 않은 위협 탐지
- 행위 기반의 Fileless 위협 탐지
- YARA를 이용한 사용자 설정 기반의 심층조사

4 조사 분석

탐지 위협의 조사/분석

- 탐지된 위협의 상세 정보 제공, 의심 파일 수집
- 통합 검색 및 연관 검색
- 이벤트 타임라인 및 연관 분석(Chain of Event)
- Ecosystem(평판서비스) 제공

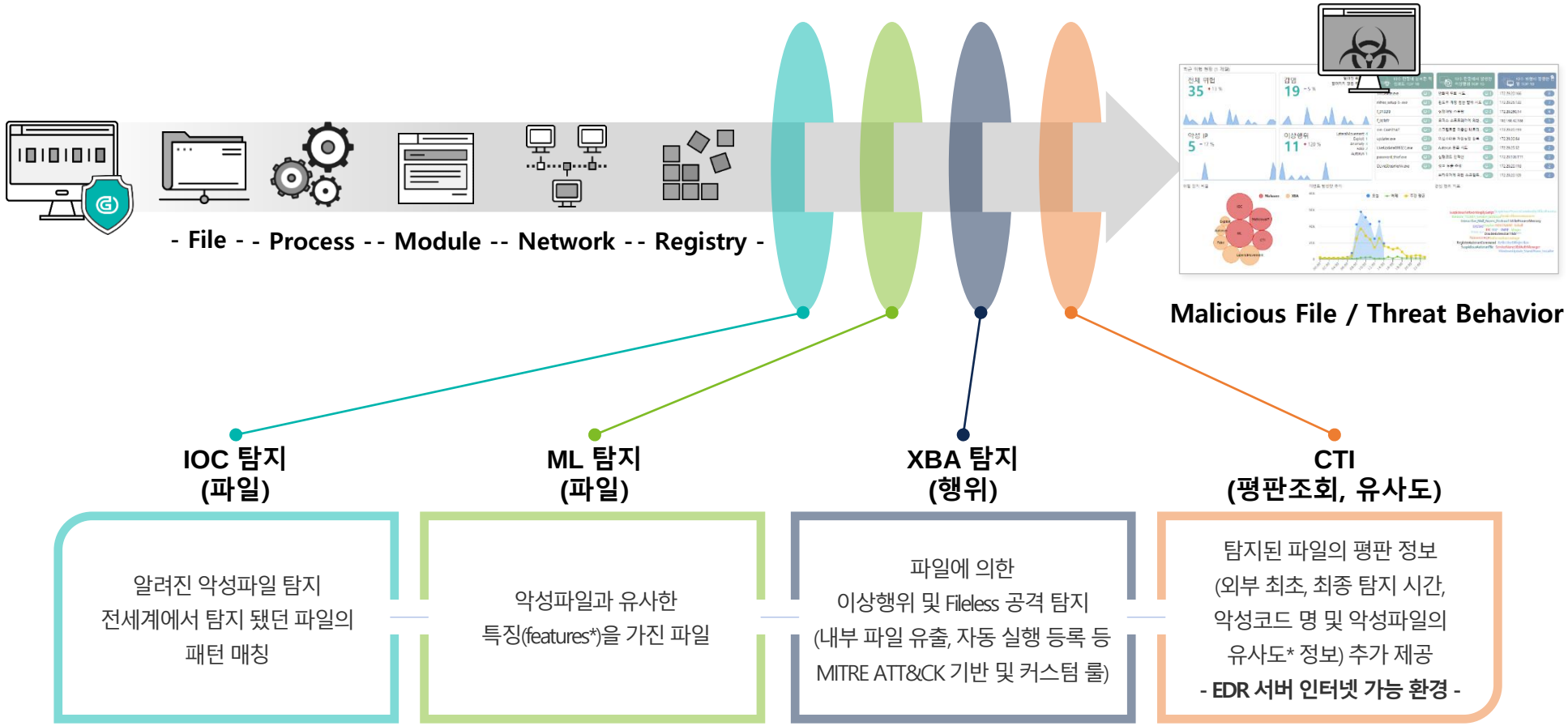
3 대응

위협의 대응

- 탐지된 위협 대상의 고지, 종료, 삭제, 네트워크 격리
- 알려진 위협 사전 대응
- 분석 후 대응 (대응 시 동일 이벤트 자동 대응)
- 샌드박스, SIEM 등 기존 보안 솔루션 연동

03. EDR의 역할 – Detection

➢ **Multi-layer 탐지 엔진으로 구성되어 악성파일 및 이상행위(file-less) 탐지와 함께 분석에 필요한 상세 정보를 제공합니다.**

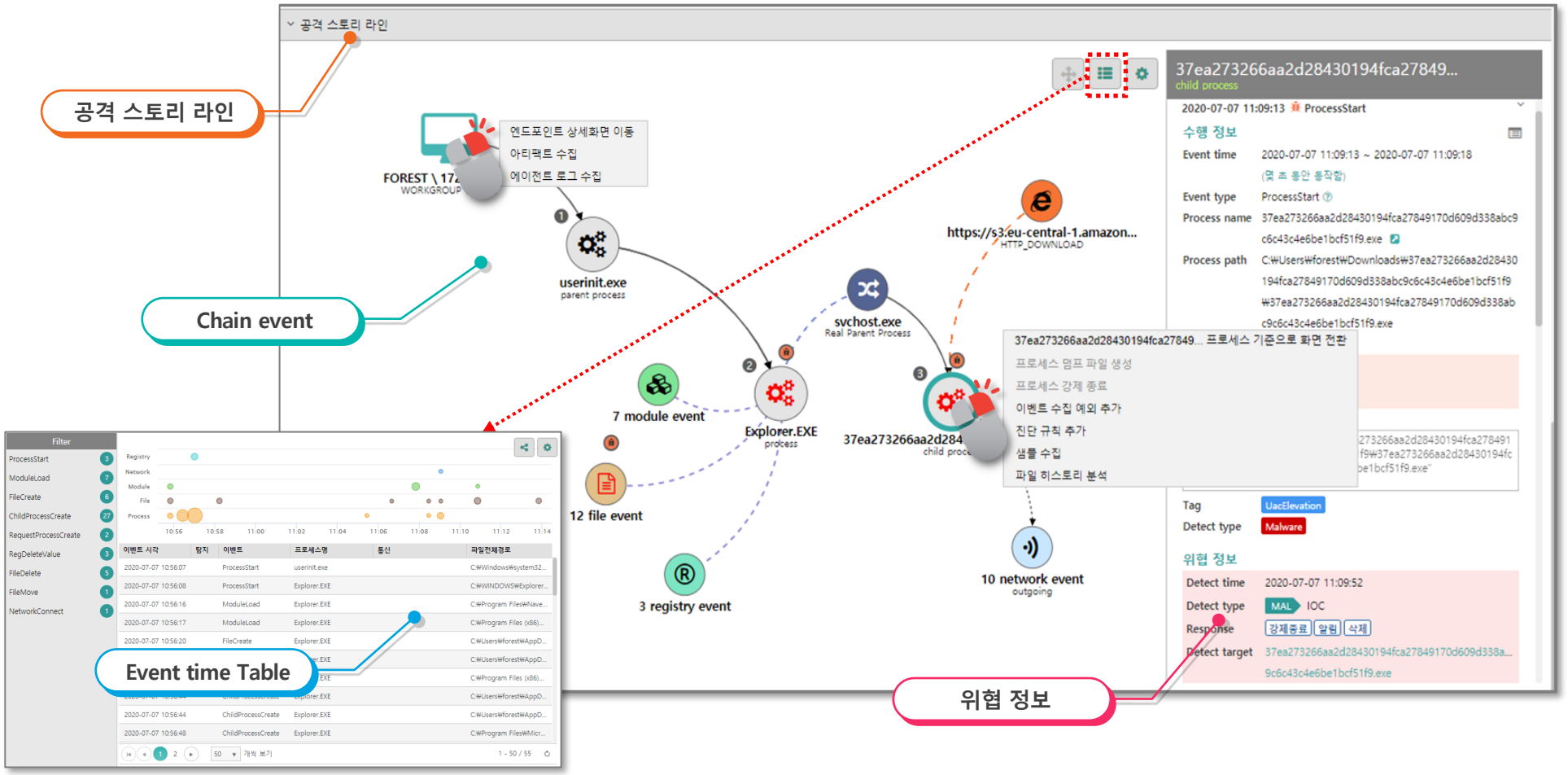


※ PE features : PE 파일은 수십개의 섹션이 있으면 해당 섹션의 특징을 features 라고 함

※ 유사도 : 탐지된 파일이 어떤 악성코드와 유사한 지에 대한 % 제공 (ssdeep hash)

03. EDR의 역할 – Analysis

➢ 공격 스토리 라인에서는 파일/프로세스의 실행 관계를 표시하며, 프로세스 제어, 파일 수집 등의 제어기능을 제공합니다.

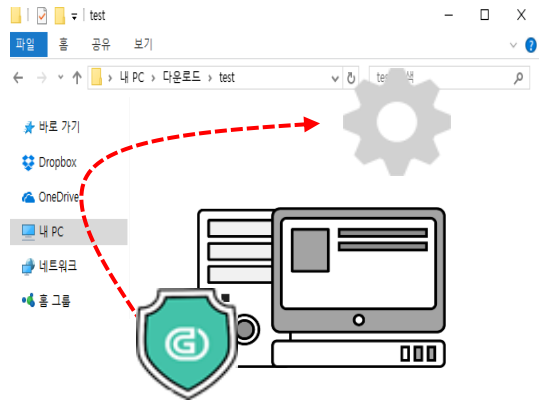


※ 위협 탐지와 관계없이 수집한 모든 로그에 대해서 위와 같은 chain event를 제공합니다.

03. EDR의 역할 – Response

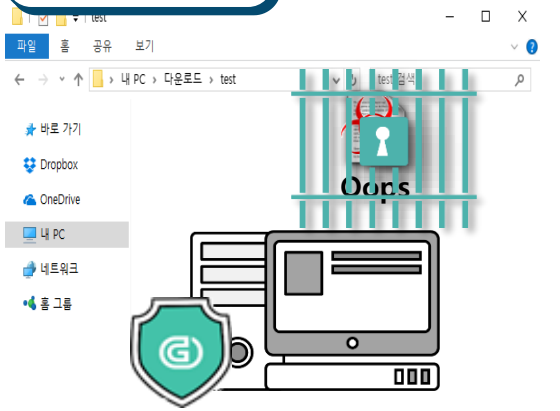
➢ 프로세스 강제종료, 파일 격리, 사용자/관리자 알람, 네트워크 격리 등의 대응 기능을 제공합니다.

프로세스 강제종료

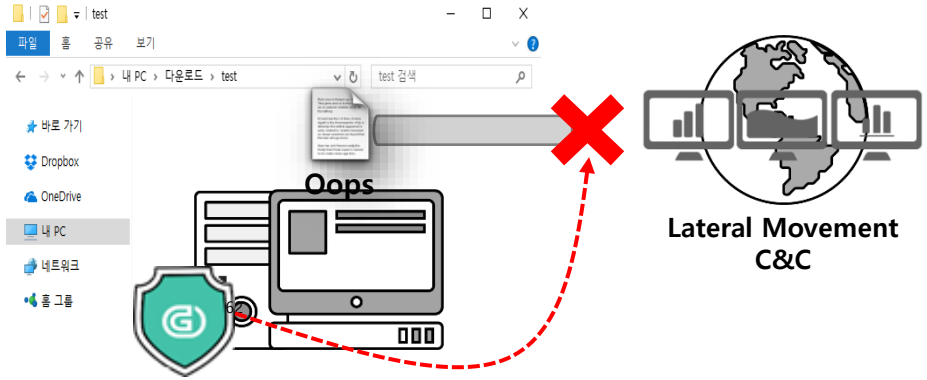


사용자/관리자 알람

파일 격리



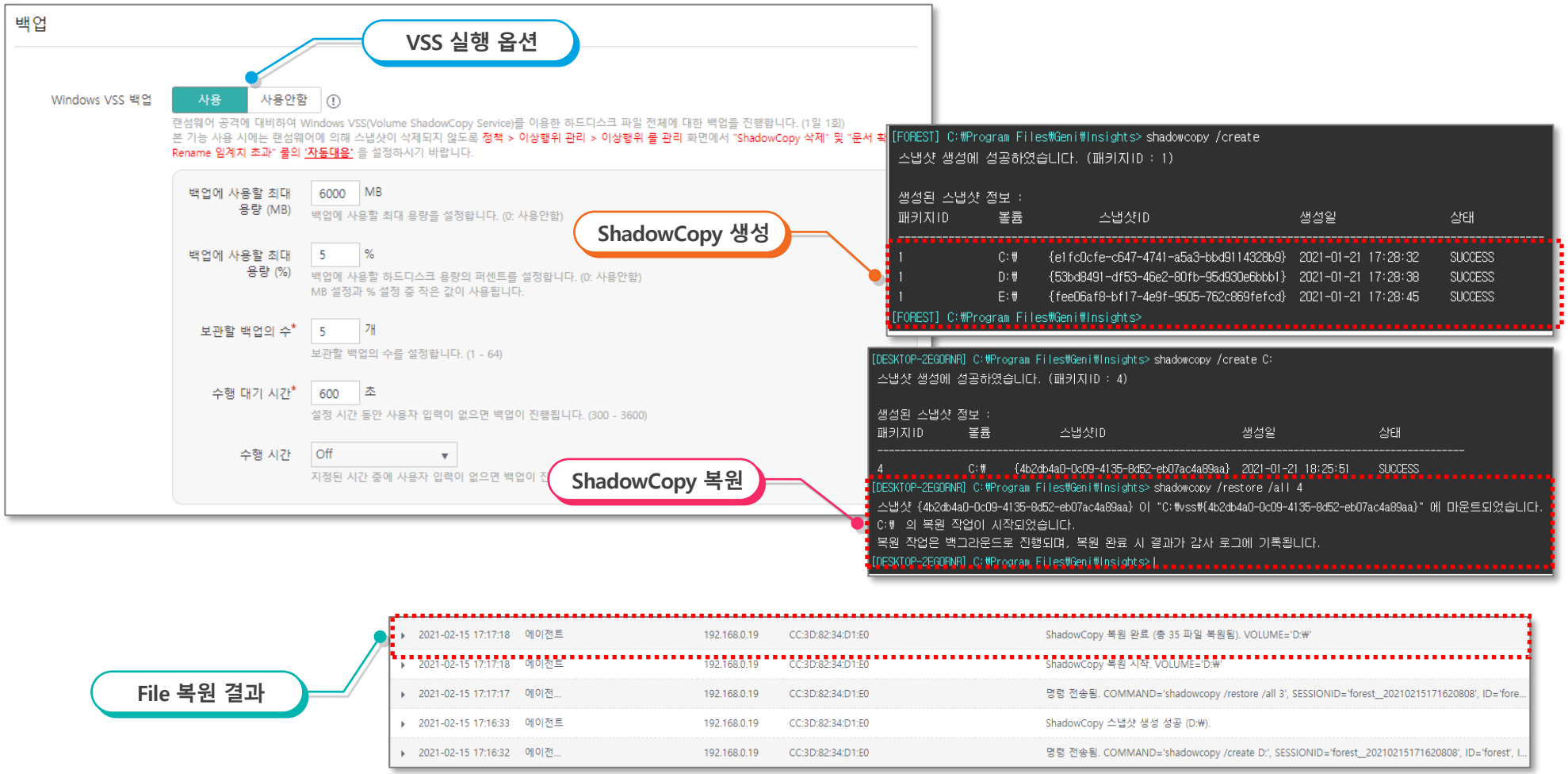
네트워크 격리



03. EDR의 역할 – Volume Shadow Copy Services

➢ **Window shadow copy 백업/복원 (Volume Shadow Copy Services) 서비스를 관리합니다.**

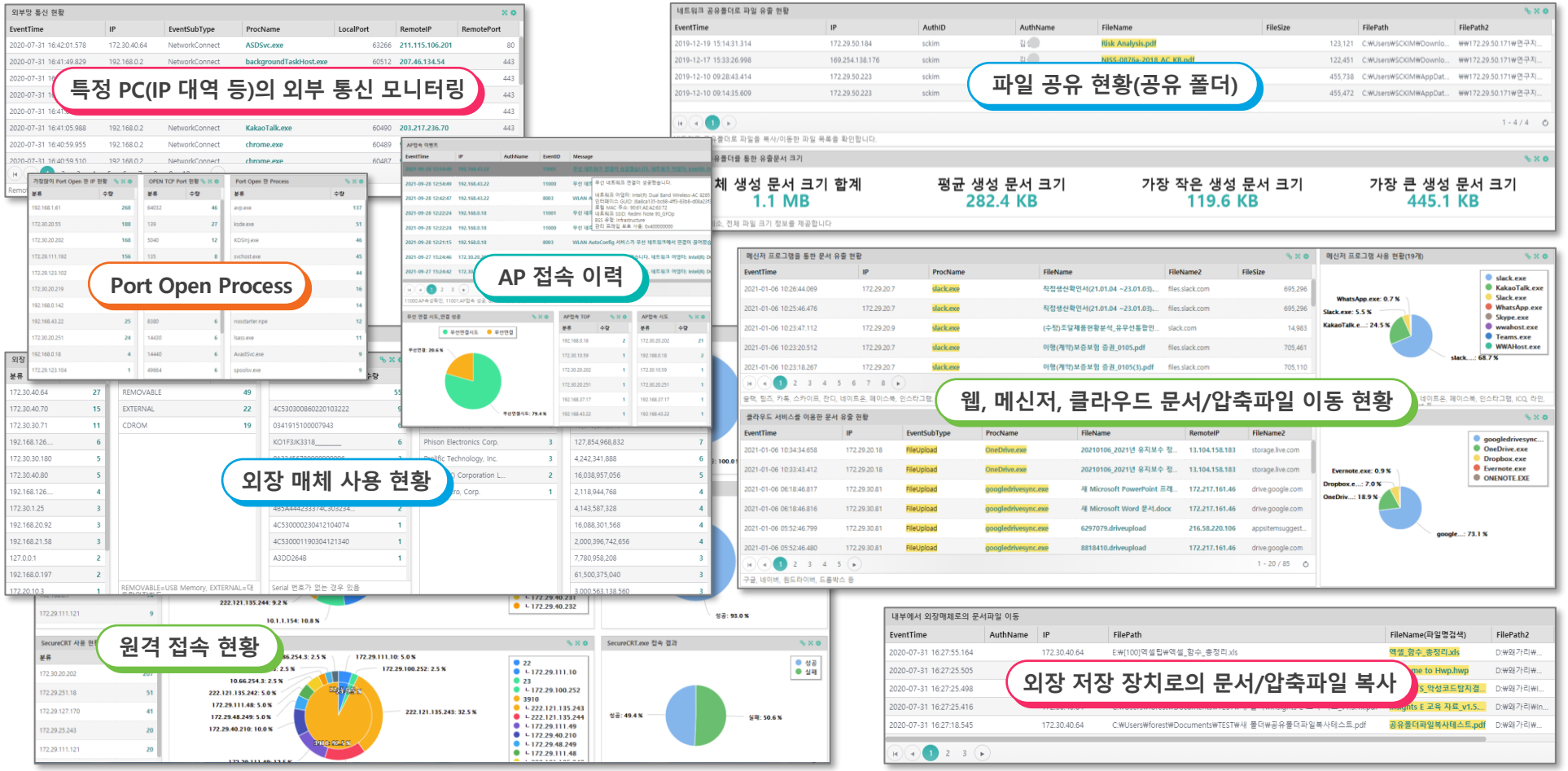
사용자 PC 의 데이터를 디스크 내의 특정 용량 이내, 보관 백업 수, 백업 수행 시간 설정으로 snapshot 저장



03. EDR의 역할 – Endpoint Discovery

➢ **기존에 확인이 어려웠던 엔드포인트 보안 정책의 정합성을 확인할 수 있습니다.**

폐쇄망 PC의 외부 통신, 내부 중요 시스템 접속 차단 PC의 통신 이력, USB 사용 금지 PC의 USB 사용 이력, 공유폴더 사용 여부, 테더링 사용, 개인 클라우드 사용 등 사용자 PC에서 적용되는 정책이 정상적으로 적용되고 있는지 확인 가능



04. Appendix

EDR을 통해 얻는 효과

- 사이버 공격 수법의 지능화/고도화로 → 사이버 공격을 100% 막는 것은 불가능
- 침입 방지 대책 뿐만 아니라 침입이 일어난 경우에 대한 대비 필요
- 엔드포인트에 대한 포괄적 가시성을 제공
- 악의적인 활동을 나타내는 비정상적인 행동을 탐지 및 검출
- EDR의 가시화 기능 활용 → 감염의 근본 원인이나 영향 범위를 용이하게 파악
- 사후 대응을 효율적이고 신속하게 실시

EDR 도입에 대한 조언

- EDR은 지능화/고도화 되고 있는 사이버 공격 대응에 효과적인 솔루션이라고 평가
- 백신과 달리 엔드포인트에서 수집하는 이벤트 로그의 양이 방대
- 이벤트가 가진 의미를 알 수 있는 통찰력과 전문성이 필요
- 침해대응이나 보안관제 업무를 어느정도 해 본 경력이면 어렵지 않게 EDR 운영
- 고도화된 침해 대응 체계가 필요한 기업/기관이라면 EDR 도입 추진
- EDR이 운영되는 환경과 도입 목적을 정확히 파악하고 체계적으로 진행

MA-SV 소개

: Mandiant Advantage Security Validation

맨디언트 오진석 상무

MANDIANT

Mandiant Advantage Security Validation

보안솔루션의 최신 위협 대응 능력 검증 및 향상을 통한 랜섬웨어 대응

Mandiant Korea

MANDIANT ADVANTAGE SECURITY VALIDATION

1. 공격자 그룹의 고도화

Security incidents with Supplicated Threat Actors in Cyber security

MANDIANT KOREA

80%

랜섬웨어 공격을 받았던 기업의 80%는, 다시
랜섬웨어의 공격을 받았습니다.
그중 45%는 동일한 램섬웨어의 공격을 받았습니다.

산업화/기업화된 Adversary GROUP (Threat Actor)

Hacker Selling Ransomware, DDoS botnet, RDP logins

And Credit Card Details in Underground

"Cybercrime as a Service"

"Ransom as a Service"

유효한 공격
빈도가 높아짐

What is a hacking Threat actor?

A Cyber Threat Actor (CTA) is a participant (person or group) in an action or process that is characterized by malice or hostile action (intending harm) using computers, devices, systems, or networks.

MANDIANT ADVANTAGE SECURITY VALIDATION

2. 기업 보안의 현주소 및 보안 검증 필요성

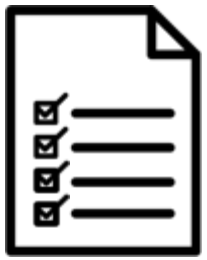
Current status of Security and needs for Security validation

MANDIANT KOREA

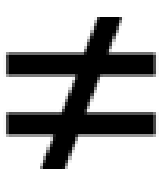
보안 공식의 변화

추가적인 보안 솔루션 도입 및 인력 투입을 통한 노력으로는 기업 보안의 효율성 개선에 한계를 보이고 있습니다.

보안 비용 투자



보안 노력



보안 효과

여러가지 가정/전제에 의한 보안 투자와 운영이 이를 방해하고 있음

- 운영팀은 효과적으로 이벤트를 처리할 것이다
- 우리는 환경 변화에 잘 대응하고 있을 것이다

현재 기업보안 침해대응 대응 현주소 파악

"많은 조직들은 내부의 자산이 여전히 잘 보호되고 있다고 생각합니다."

그러나,

테스트된 공격의 절반 이상(53%)이 **미탐**

침투 후 보안 툴에 의해 **탐지된 공격**은 26%,
완전히 **차단된 공격**은 33%.

경보를 발생시킨 공격은 단 9%

"탐지조차 되지 않고 있습니다"

그럼, 랜섬웨어를 위해서는 무엇을 알아야 할까?

TOYOTA 공급망 사이버보안 사고

AUTOMOBILES

Toyota stoppage highlights supply chain vulnerabilities

Cyberattacks on key links can shut down any mar

2022-02-28

공급자의 시스템 장애로 인한 도요타 자동차의 국내 전 공장 정지에 대해 정리

시스템 장애

2022년 2월 28일, 도요타 자동차는 부품 공급업체인 코지마 프레스 공업의 시스템 장애를 받아 국내의 모든 라인 정지를 공표했습니다. 여기에서는 관련 정보를 정리합니다.

처음으로 보이는 국내 전 공

- 도요타가 정지 대상으로 한
  전 공장의 정지는 처음으로
  (1직·2직 모두 대상). 도요타
  다이하츠 공업도 정지 대상
  공장에도 영향이 파급되는
- 도요타 자동차가 공장 가동
  업의 시스템 장애로 부품 공
  의 인테리어·익스텔리아와
- 3월 1일 국내 14공장 1일간
  1월 월간 생산량 5%에 해당
- 히노 자동차에서는 도요타
  시하고 있는 후루카와 공장
- 도요타 자동차는 3월 2일 이
  다. *5

영향을 받은 도요타 관련 기업	대상 공장
도요타 자동차	모토마치 공장, 타카오카 공장, 제방 공장, 타하라 공장
도요타 자동차 동일본	미야기 대형 공장, 이와테 공장
도요타 차체	후지마츠 공장, 요시하라 공장, 이나베 공장
기후차체공업	본사 공장
도요타 자동 직기	장초 공장
히노 자동차	하무라 공장
다이하츠 공업	교토 공장

'22/2/26

랜섬노트와 함께 여러 대의 서버가 바이러스에 감염되었음을 확인

'21/2/28

Kojima는 추가 손상을 방지하기 위해 네트워크를 종료. 당시 고지마는 도요타로부터 28일까지 필요한 모든 생산 데이터를 갖고 있었음

EMOTET 멀웨어를 통한 감염으로 확인됨

14개 공장 1일간 가동중단

https://piyolog.hatenadiary.jp/entry/2022/02/28/224420

보안 사고관련 INTELLIGENCE 수집 – Actionable

Toyota stoppage highlights supply chain vulnerabilities

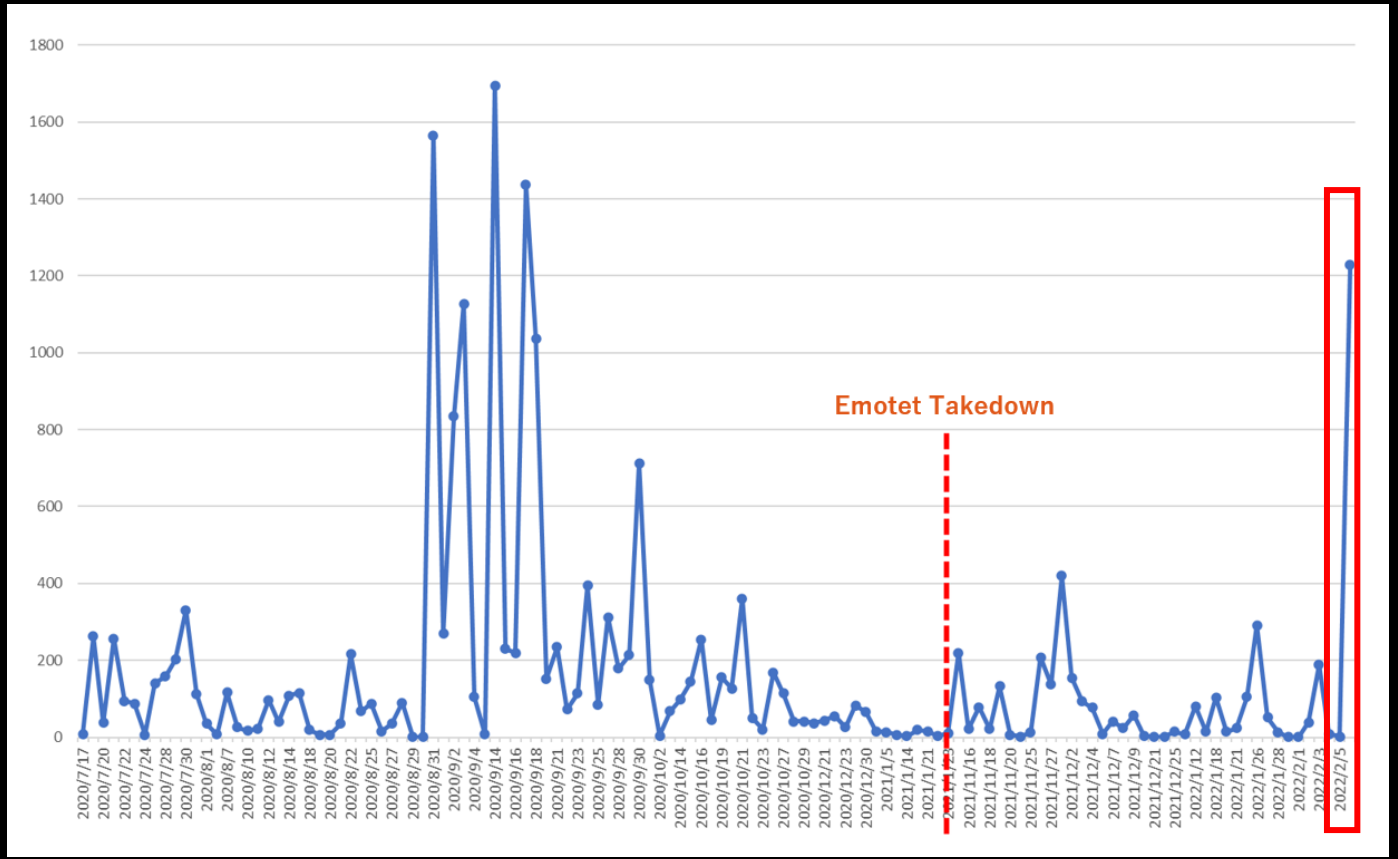
Cyberattacks on key links can shut down any manufacturer

Toyota's Takaoka plant, which halted production on March 1. (Photo by Yuki Nakao)

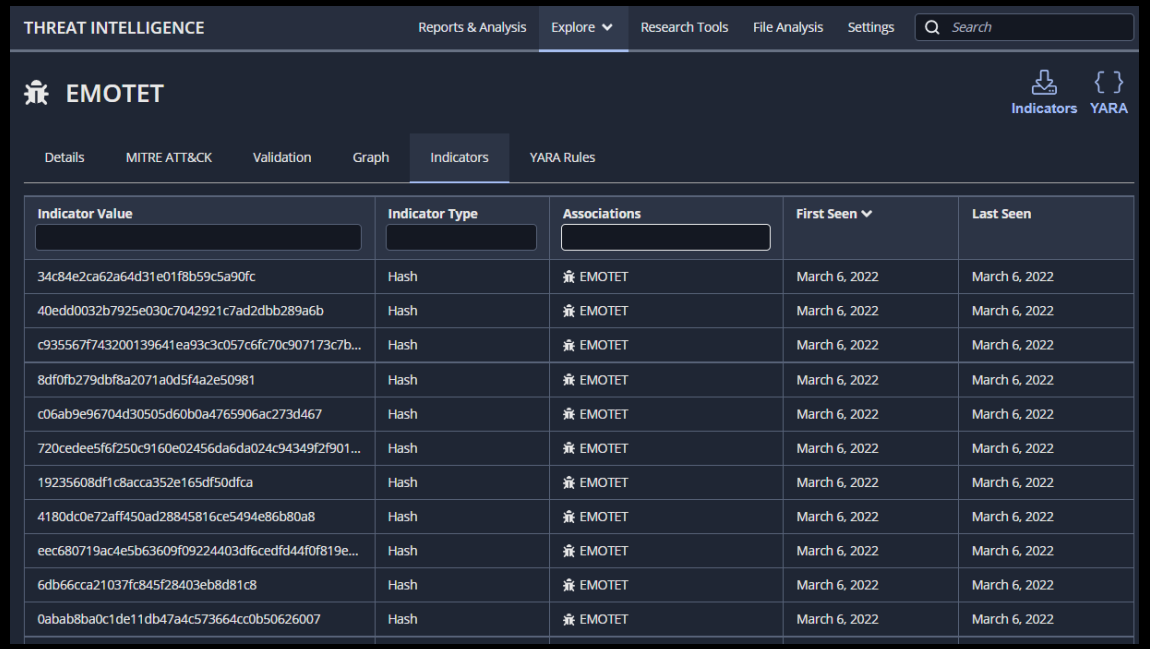
It is still unclear who targeted the company and why.

Prior to the cyberattack, security experts had noted suspicious activity. According to one, attempts had been made to breach Kojima's mail servers since February using the powerful Emotet malware and user name "toyota." It is believed that Emotet is directly responsible for the breach.

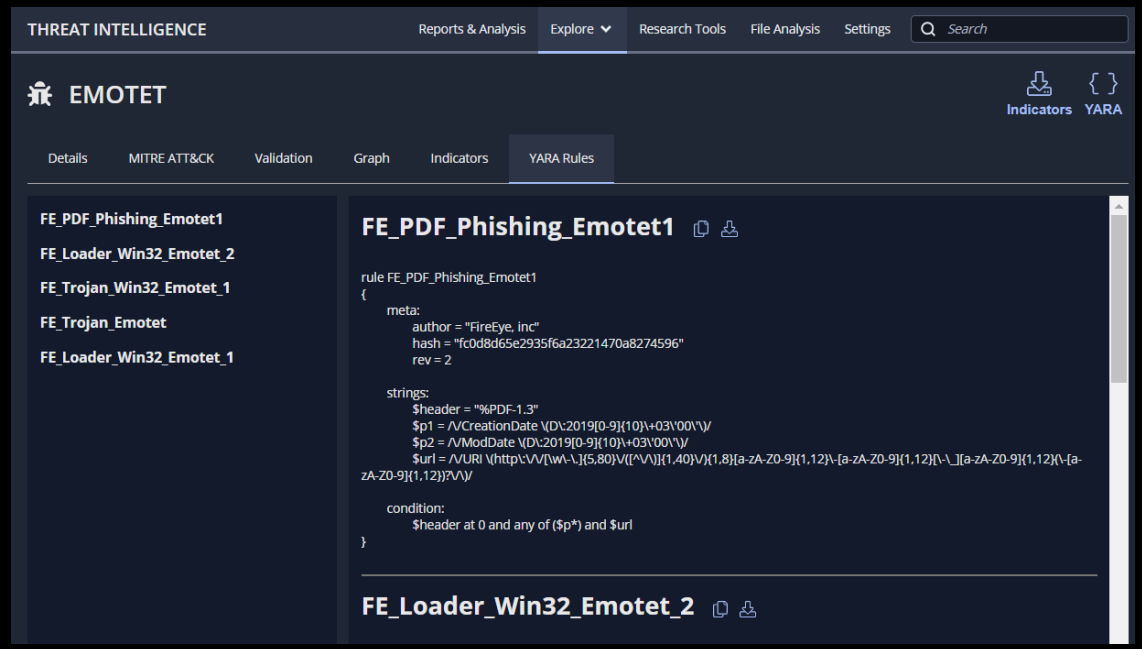
Alert Regarding Re-emergence of EMOTET Malware Infection Activities



INTELLIGENCE(Indicators)를 이용한 보안팀의 1차 대응



IP, URL, Hash Code, Malware



보안솔루션 RULE 업데이트
(앤드포인트 Signature, IPS and WAF 룰)

INTELLIGENCE(TTPs)를 이용한 보안팀의 2차 대응

EMOTET

Indicators YARA

Details | MITRE ATT&CK | Validation | Graph | Indicators | YARA Rules

MITRE ATT&CK

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control
Develop Capabilities T1587	Phishing T1566	Command and Scripting Interpreter T1059	Boot or Logon Autostart Execution T1547	Access Token Manipulation T1134	Access Token Manipulation T1134	Credentials from Password Stores T1555	Account Discovery T1087	Archive Collected Data T1560	Application Layer Protocol T1071
Obtain Capabilities T1588		System Services T1569	Create or Modify System Process T1543	Boot or Logon Autostart Execution T1547	Deobfuscate/Decode Files or Information T1140	Input Capture T1056	Application Window Discovery T1010	Clipboard Data T1115	Ingress Tool Transfer T1105
				Create or Modify System Process T1543	Hide Artifacts T1564	OS Credential Dumping T1003	File and Directory Discovery T1083	Email Collection T1114	Non-Application Layer Protocol T1095
				Process Injection T1055	Indicator Removal on Host T1070		Network Share Discovery T1135	Input Capture T1056	Proxy T1090
					Modify Registry T1112		Process Discovery T1057	Screen Capture T1113	
					Obfuscated Files or Information T1027		Query Registry T1012		
					Process Injection T1055		Software Discovery T1518		

Execution

Command and Scripting Interpreter
T1059

System Services
T1569

명령 및 스크립팅 인터프리터 (T1059)

공격자는 명령 및 스크립트 인터프리터를 남용하여 명령, 스크립트 또는 바이너리를 실행할 수 있습니다. 이러한 인터페이스와 언어는 컴퓨터 시스템과 상호 작용하는 방법을 제공하며 다양한 플랫폼에서 공통적인 기능입니다. 대부분의 시스템에는 명령줄 인터페이스와 스크립팅 기능이 내장되어 있습니다. 예를 들어 macOS 및 Linux 배포판에는 Unix Shell 의 일부가 포함되어 있는 반면 Windows 설치에는 Windows Command Shell 및 PowerShell 이 포함 됩니다.

Python 과 같은 플랫폼 간 인터프리터 는 물론 JavaScript/JScript 및 Visual Basic 과 같은 클라이언트 애플리케이션과 일반적으로 연결된 인터프리터도 있습니다.

공격자는 임의의 명령을 실행하는 수단으로 이러한 기술을 다양한 방식으로 남용할 수 있습니다. 명령과 스크립트는 피해자에게 유인 문서로 전달되거나 기존 C2에서 다운로드한 보조 페이로드로 전달되는 초기 액세스 페이로드 에 포함될 수 있습니다 . 공격자는 대화형 터미널/쉘을 통해 명령을 실행할 수도 있습니다.

추가적인 INTELLIGENCE(연관성)활용한 보안팀의 선제적 대응

EMOTET

Indicators YARA

Details | MITRE ATT&CK | Validation | Graph | Indicators | YARA Rules

Malware Details

Description

EMOTET is a downloader written in C/C++ that communicates via HTTP. EMOTET retrieves two types of payloads: plugins that extend its own functionality and additional malware. Downloaded plugins are mapped directly into memory and executed but additional malware payloads are written to disk prior to execution. Plugins include a credential stealer that targets web browsers and email clients, data miners that target Microsoft Outlook contacts and email messages, a spambot, a tunneler, and a lateral movement tool. Additional malware families downloaded by EMOTET include TRICKBOT, DRIDEX, QAKBOT, SILENTNIGHT, URSNIF, ANDROMEDA, ICEDID, PANDABOT, COREBOT, SMOKELOADER, and GOOTKIT.

Operating Systems: Windows

Associated Malware: DAVESHELL | MALTSHAKE | WARPGATE | WHITEDAGGER

Capabilities

memory	Anti-VM capabilities	Anti-VM: VMware
Anti-VM: VirtualBox	Anti-VM: WINE	Anti-VM: Xen
g capabilities	Calculates Adler-32 hashes	Calculates FNV hashes
Luhn checksums	Calculates MD5 hashes	Calculates MurmurHash3 hashes
SHA-1 hashes	Calculates hashes using CRC32	Capture CPU information
etwork Share information	Capture POP3 credentials	Capture clipboard contents
ure credentials stored by Chrome	Capture credentials stored by Firefox	Capture credentials stored by Internet Explorer
edentials stored by Microsoft Outlook	Capture credentials stored by Opera	Capture disk information
Capture email credentials	Capture email messages or contents	Capture hostname
Capture keyboard layout	Capture keyboard layout	Capture memory status

Indicators

News Analysis

MEDIA ON-TARGET
Group Behind Emotet Botnet Malware Testing New M... Microsoft Security
CYBERSCOOP

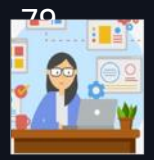
MEDIA ON-TARGET
MAR 23, 2022
Exotic Lily Initial Access Broker Works with Conti ...
SECURITY AFFAIRS

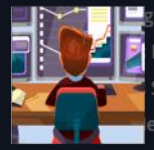
PLAUSIBLE
MAR 15, 2022
Multiple Automotive Manufacturers Infected with Emotet

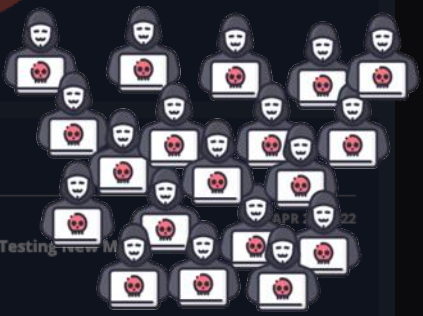
보안팀은 어디부터 시작해야 할까요?


Vulnerability Researcher


Software Engineer


Infrastructure Administrator


Analyst



" 전문해커 팀에 의한 작품~~!!!"

" 다음 공격 준비 중"

관련위협의 기술적 정보를 바탕으로 보안솔루션 대응 여부 검증

EMOTET

Indicators YARA

Details | MITRE ATT&CK | Validation | Graph | Indicators | YARA Rules

Validation

59 Actions Available

Validate

Name	VID
Copy of Phishing Email - Malicious Attachment, EMOTET Downloader, Variant #4	
Phishing Email - Malicious Attachment, EMOTET Downloader, Variant #2	
Malicious File Transfer - EMOTET, Second Stage, Download	
Command and Control - EMOTET, DNS Query, Variant #10	
Malicious File Transfer - EMOTET, Download, Variant #6	
Command and Control - EMOTET, DNS Query, Variant #16	
Command and Control - EMOTET, DNS Query, Variant #17	
Malicious File Transfer - EMOTET Malware, Download, Variant #11	
Phishing Email - Malicious Attachment, EMOTET, Download, Variant #5	
Command and Control - EMOTET, DNS Query, Variant #15	
Host CLI - EMOTET, Fake Word Message Error	
Malicious File Transfer - EMOTET Related Malicious Macro Enabled Doc, Download	
Phishing Email - Malicious Attachment, EMOTET Downloader, Variant #1	
Malicious File Transfer - TRICKBOT, Download, Variant #8	
Malicious File Transfer - EMOTET, Download, Variant #16	
Protected Theater - EMOTET Retrieval, Encoded Powershell Command	
Phishing Email - Malicious Link, EMOTET, Incorrect Invoice Lure	
Protected Theater - EMOTET Downloader, Encoded PowerShell Download Command	
Malicious File Transfer - EMOTET, Download, Variant #15	
Malicious File Transfer - EMOTET, Download, Variant #13	
Malicious File Transfer - EMOTET, Download, Variant #7	
Malicious File Transfer - EMOTET Malware, Download, Variant #2	
Malicious File Transfer - EMOTET, Download, Variant #3	
Malicious File Transfer - EMOTET, Download, Variant #2	
Command and Control - EMOTET, DNS Query, Variant #3	
Command and Control - EMOTET, Beacon, Variant #1	
Malicious File Transfer - EMOTET, Download, Variant #14	
Malicious File Transfer - EMOTET, Downloader, Variant #12	
Command and Control - EMOTET, DNS Query	
Command and Control - EMOTET, DNS Query, Variant #14	
Command and Control - EMOTET, DNS Query, Variant #8	
Command and Control - EMOTET, DNS Query, Variant #5	
Phishing Email - Malicious Attachment, EMOTET, Downloader, Variant #6	
Malicious File Transfer - EMOTET Malware, Download, Variant #7	
Malicious File Transfer - EMOTET, Download, Variant #5	
Command and Control - EMOTET Malware, C2 Check-in, Variant #2	
Command and Control - EMOTET, Data Exfil	A101-450
Malicious Activity - EMOTET, Initial Infection	A100-510
Malicious File Transfer - EMOTET Malware, Download, Variant #8	A100-059
Command and Control - EMOTET, GET DLL Payload	A101-473
Command and Control - EMOTET, Encrypted Check-in	A100-303
Command and Control - EMOTET Malware, C2 Check-in	A100-609
Command and Control - EMOTET, DNS Query, Variant #2	A100-045
Phishing Email - Malicious Attachment, EMOTET	A150-179
Phishing Email - Malicious Attachment, EMOTET Downloader, Variant #4	A100-079
Malicious File Transfer - EMOTET, Download, Variant #1	A100-591
Malicious File Transfer - EMOTET, Download, Variant #4	A150-441
Malicious File Transfer - EMOTET Malware, Download, Variant #9	A100-070
Phishing Email - Malicious Attachment, EMOTET Downloader, Variant #3	A100-078
Phishing Email - Malicious Attachment, EMOTET Dropper Delivery	A100-560
Malicious File Transfer - EMOTET Malware, Download, Variant #10	A100-052
Command and Control - EMOTET, Beacon, Variant #2	A102-363
Command and Control - EMOTET, DNS Query, Variant #13	A102-316
Command and Control - EMOTET, DNS Query, Variant #9	A101-454
Command and Control - EMOTET, DNS Query, Variant #4	A100-047
Command and Control - EMOTET, DNS Query, Variant #12	A101-451
Command and Control - EMOTET, Check-in and Response	A150-015
Command and Control - EMOTET, DNS Query, Variant #11	A101-452
Command and Control - EMOTET, TRICKBOT, Download	A150-125

MANDIANT ADVANTAGE SECURITY VALIDATION

3. MASV 보안 솔루션 검증 플랫폼

MASV(Mandiant Advantage Security Validation) 구성 아키텍처 / 지원환경 / 검증시나리오 / 레포트

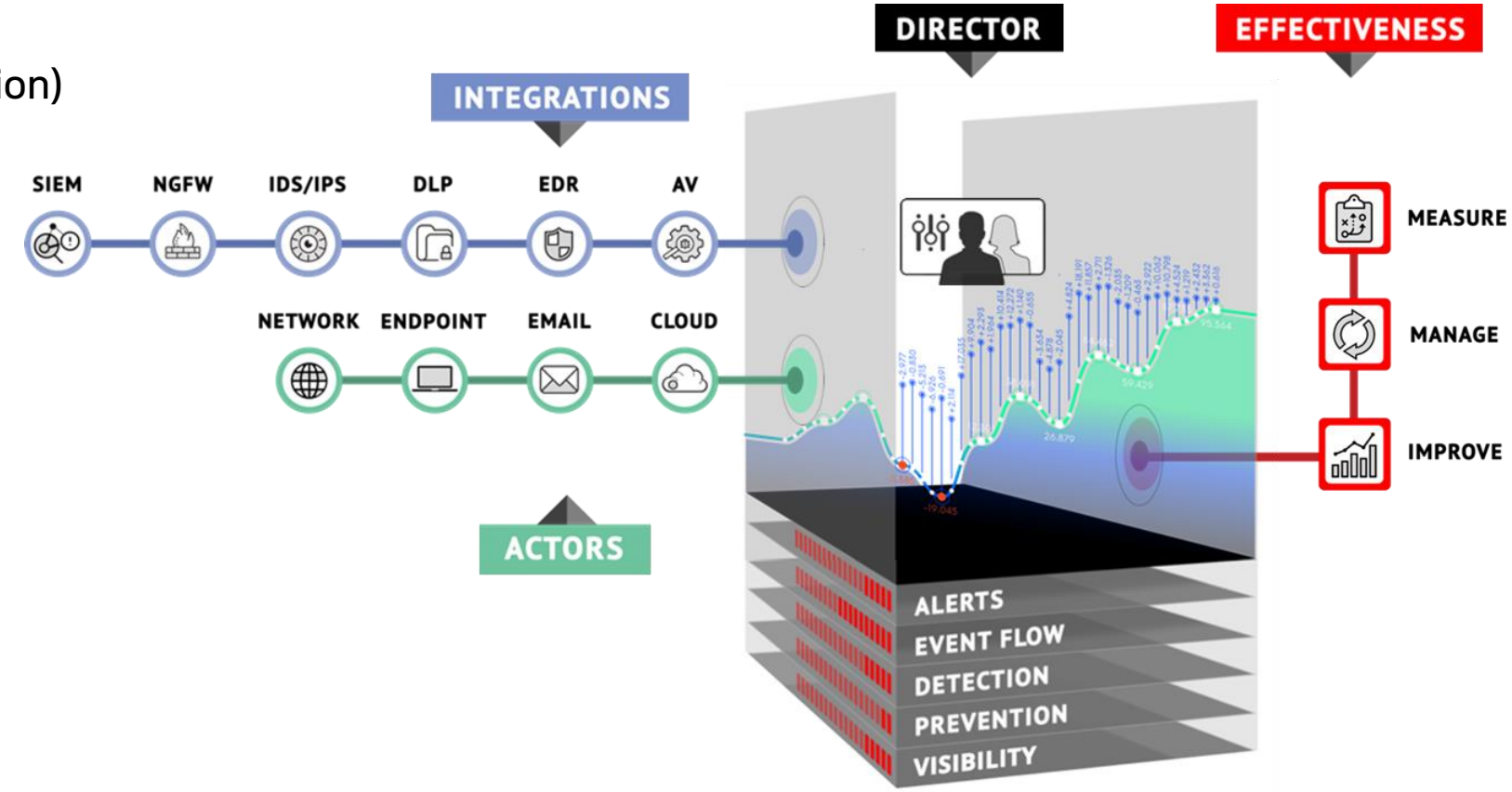
MANDIANT KOREA

MA-SV (Mandiant Security Validation) 아키텍쳐

보안 솔루션의 공격 대응 수준에 대한 평가를 위해서 실제 공격자가 사용자는 공격 시나리오 기반의 공격 데이터를 사용하여 보안 솔루션의 효율성 검증을 위한 BAS(Breach and Attack Simulation) 플랫폼입니다.

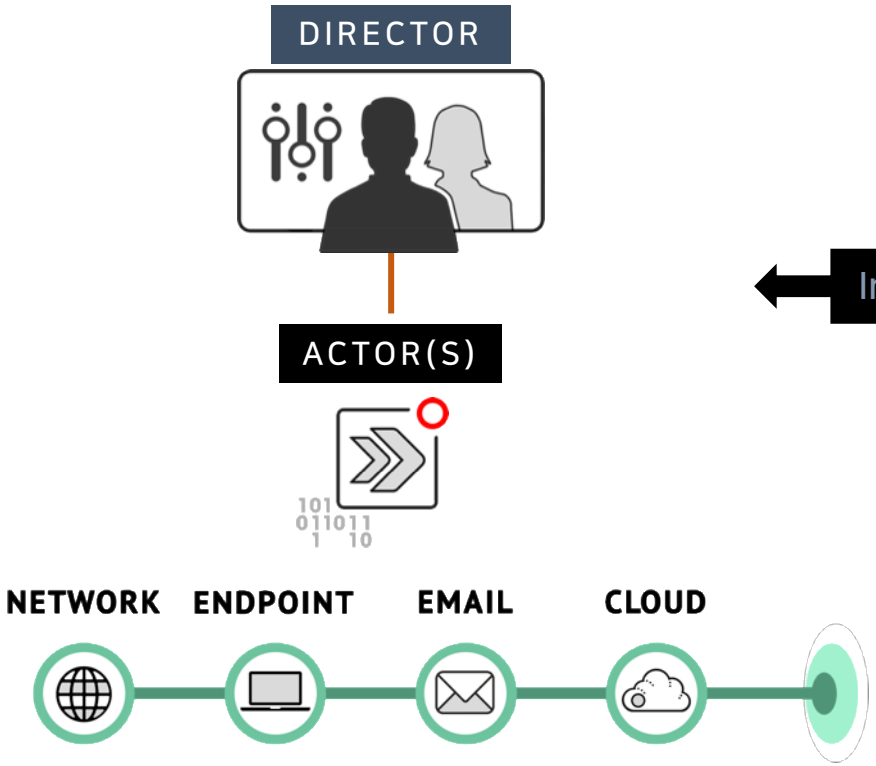
MASV 보안 효과 검증 플랫폼
(BAS, Breach and Attack Simulation)

- 보안 효율성 측정 (수치화)
- 보안 효율성 관리
- 보안 효율성 개선



MA-SV 환경구성

MASV는 검증에 대한 시나리오, 실행, 결과 관리를 하는 Director, 실제 공격에 대한 검증을 처리하는 Actor로 구성되며, 기존 운영중인 SIEM 및 개별 보안솔루션과의 연동을 통해 구성됩니다.



Integration

SIEM

ArcSight, AlienVault, Carbon Black, Check Point, Cisco, CrowdStrike, Cylance, cybereason, FireEye, Forcepoint, elastic, LogRhythm, McAfee, Microsoft, mimecast, paloalto, proofpoint, Radar, RSA, SentinelOne, SOURCEfire, splunk>, sumologic, Symantec, TippingPoint

MALWARE
IDS / IPS
WAF

FIREEYE
SOURCEfire
IMPERVA

DLP

FORCEPOINT
Symantec
VARONIS

PROXY

BLUE COAT
zscaler
f5

INTERNET
FIREWALL

paloalto NETWORKS
Check Point
CISCO

MA-SV 액터

다양한 유형과 형태로 운영할 수 있는 환경을 통해 실제 공격 테스트에서 안전을 보장하고 세부적이고 심층적인 분석을 진행할 수 있도록 네트워크, 엔드포인트, 이메일 등 다양한 환경의 보안 솔루션 검증을 지원합니다.

NETWORK ACTOR

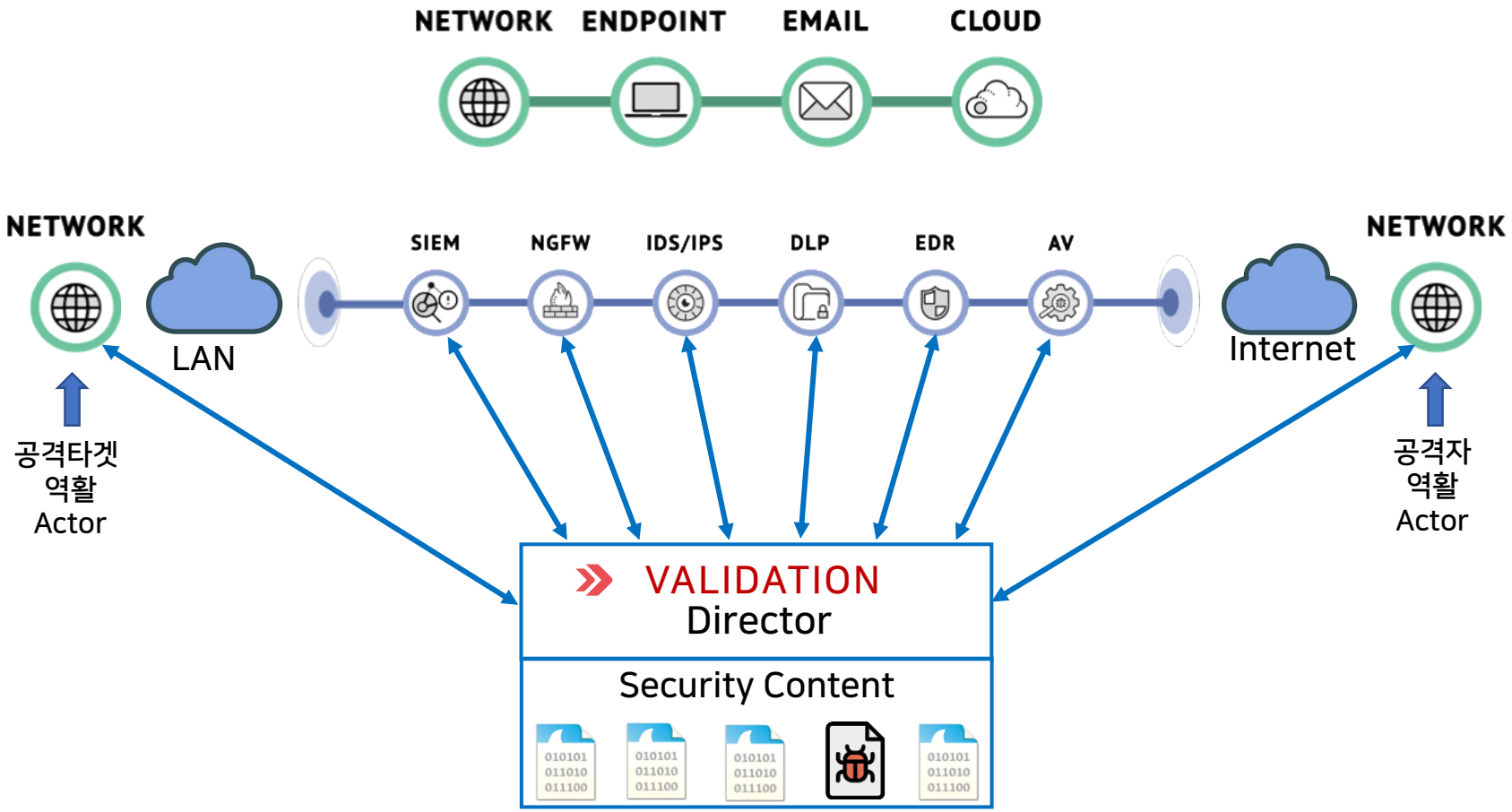
네트워크 기반 공격

- Segmentation & Policy Validation
- 의심스러운 파일 전송
- C2 통신
- 데이터 유출

ENDPOINT ACTOR

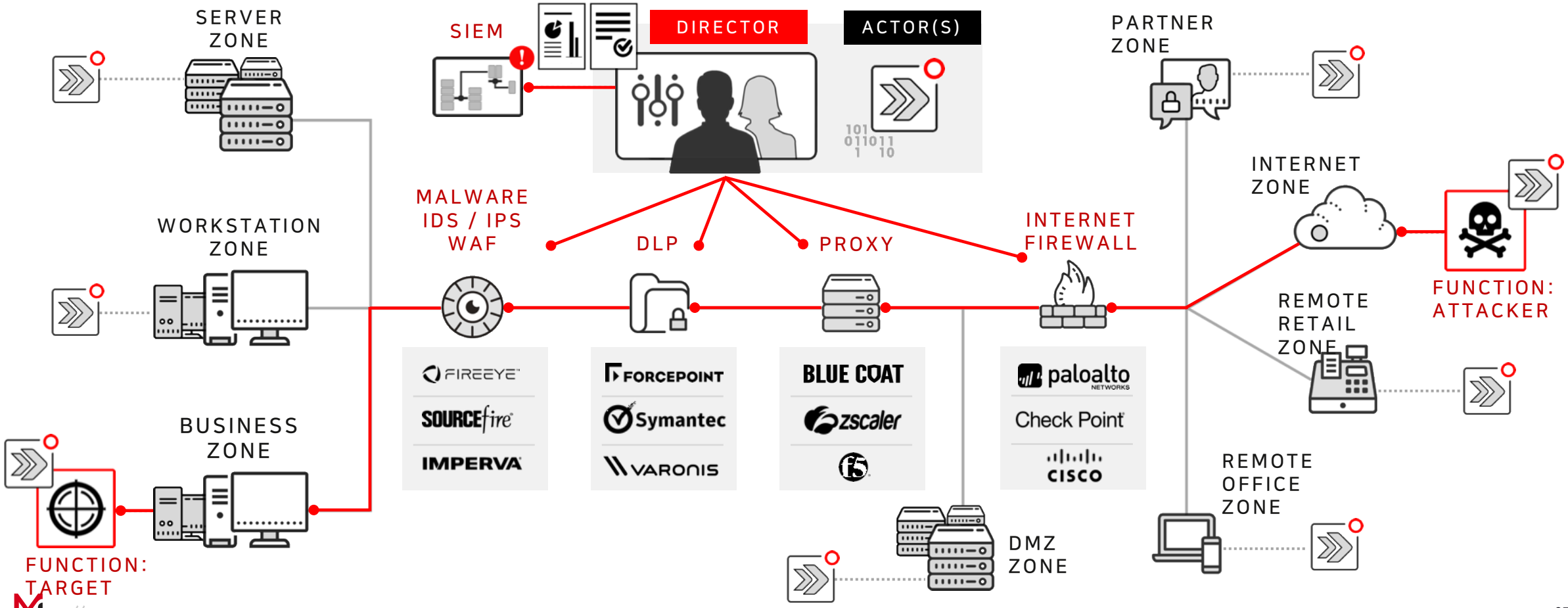
호스트 기반의 행위 공격

- Mimikatz
- Key logger
- 권한상승
- 데이터 유출
- Power shell, CMD, bash



MA-SV 아키텍처 구성

실제 공격자들이 사용하는 공격에 대해서 보안 솔루션의 대응 검증 테스트를 위해서 네트워크, 앤드포인트, 이메일을 통한 우회 공격을 자동화하고 시뮬레이션의 결과를 기준으로 보안대응 수준의 지속적인 개선이 가능하도록 구성합니다.



Validated Threat Contents update

Validation Content Update – May 11, 2022

The Mandiant Advantage Security Validation (MA-SV) Behavior Research Team (BRT) has published **VHR20220511 – Content Expansion**, a Security Content Pack focusing on **CVE-2022-1388** and **FIN7**. This content pack requires Director version **4.7.0.0-0 or newer**.

If you've enabled the Content Service, this content pack will automatically download and be applied to your Director (see the MA-SV Validation User Guide for full details). Otherwise, you can download the security content pack and release notes from the Content page of the Validation Customer Portal.

Summary of Changes

- 20 Actions added
- 15 Files added
- 69 Actions updated
- 23 Actions have been updated to reflect Common Detection Alert changes

Release Highlights

- New Actions for CVE-2022-1388, an authentication vulnerability within the iControl REST in F5 BIG-IP 16.1.2 and earlier that, when exploited, allows an attacker to remotely execute arbitrary system commands.
- New Actions focusing on malware used by FIN7, a financially motivated group. Mandiant Threat Intelligence has observed this group attempt to compromise diverse organizations for malicious operations involving the deployment of point-of-sale (POS) malware.
  - POWERPLANT
  - POWERTRASH

MA-SV USE CASES

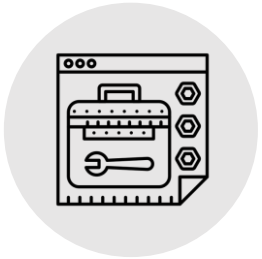
- ☐  핵심 네트워크 보안 제어 검증
- ☐  핵심 앤드포인트 제어 검증
- ☐  DLP 검증
- ☐  랜섬웨어 악성파일 전송 검증
- ☐  클라우드 제어 검증
- ☐  이메일 보안 검증
- ☐  네트워크 세그먼트 검증
- ☐  도입보안 제어 검증
- ☐  위협액터(Threat Actor) 대응 검증
- ☐  SOC/SIEM 보안 검증

MSV의 주요한 보안전략 및 가치

환경 변화에 대한 인지

보안솔루션 효율성/
구성&설정의 보증

- 우리의 보안 솔루션들이 우리가 기대하는 방식으로 작동하고 있습니까?
- 보안 설정이 제대로 잘 되어 있습니까?



솔루션 최적화

- 투자한 비용 만큼 보안 효율성을 높일 수 있습니까?
- 기 보안 솔루션의 가치를 최대한 활용하고 있습니까?
- ROI를 극대화하고 있습니까?

합리적인 운영

- 어디에 중복되어 투자되었고 기대치에 부합하게 잘 운영하고 있습니까?
- 보안환경에서 특정 보안 솔루션을 제거해도 됩니까?
- 보안 운영 환경을 단순화할 수 있습니까?

최적의 보안수준

지속적인 보안 환경 개선을 통한 보안 효율성 향상

지속적인 검증


MANDIANT
YOUR CYBERSECURITY ADVANTAGE

퀘이사(Quaxar)를 통한 랜섬웨어 대응 전략

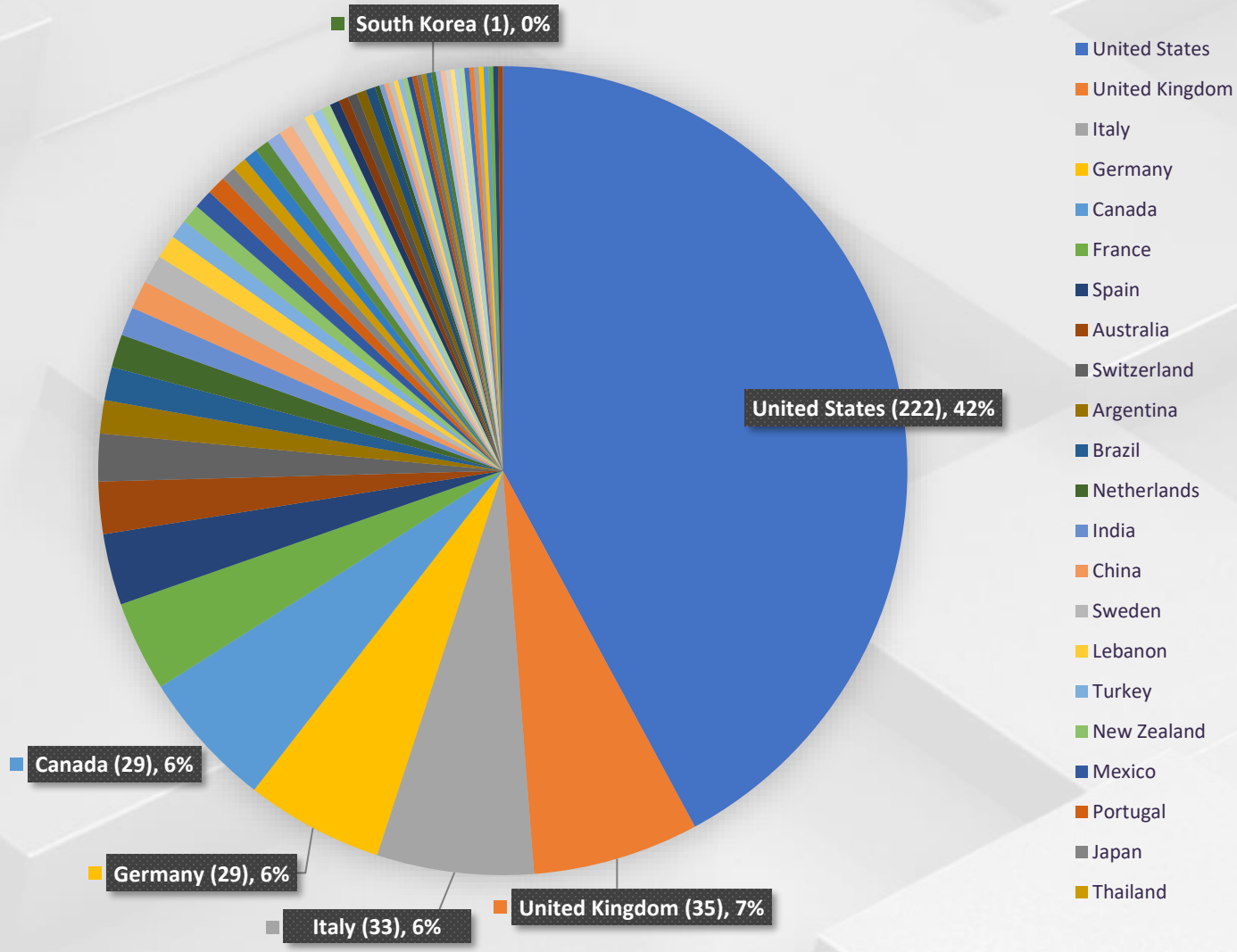
S2W 류소준 팀장

quaxar

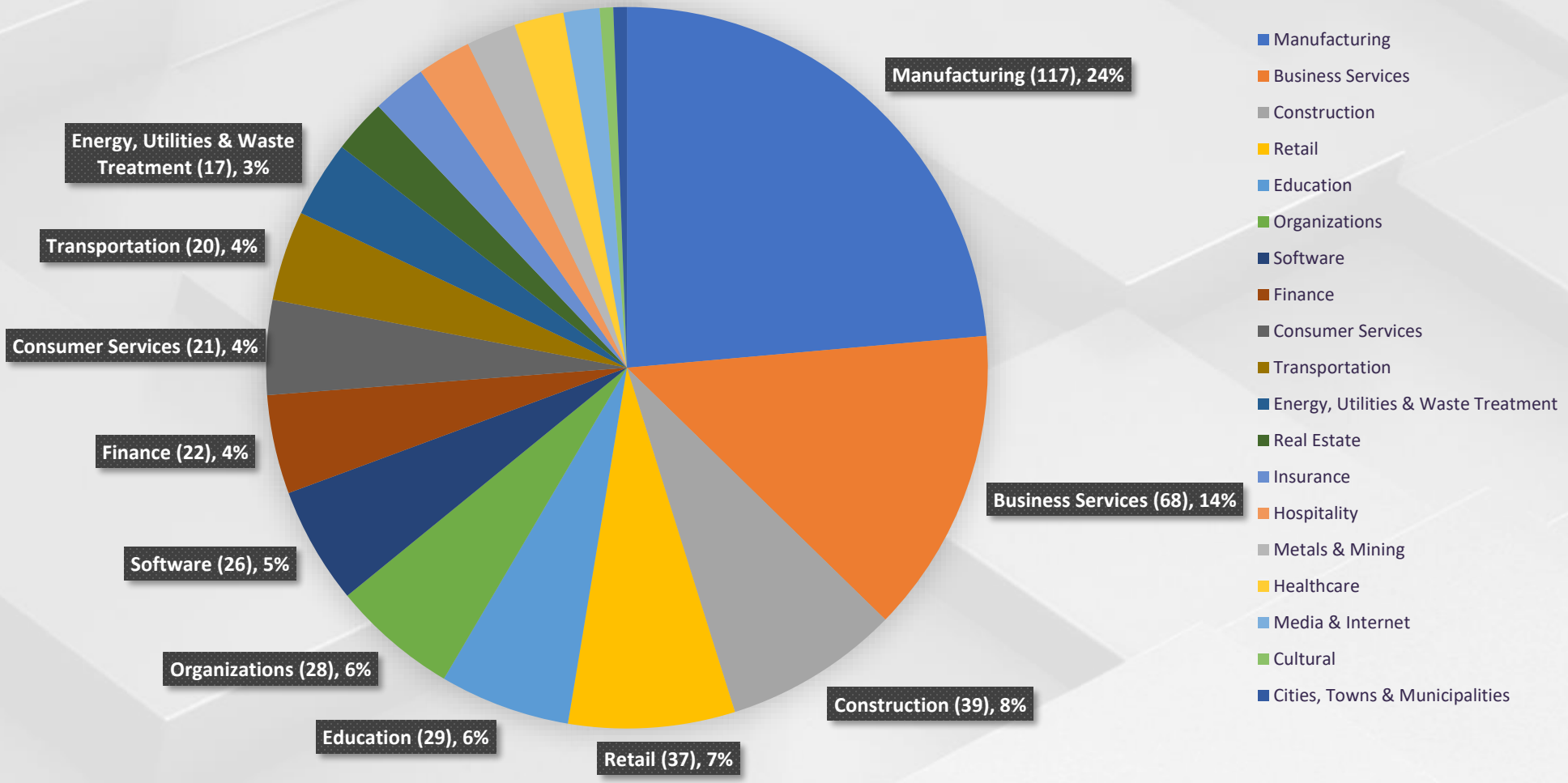
Leveling up your Cyber Threat Intelligence

S2W

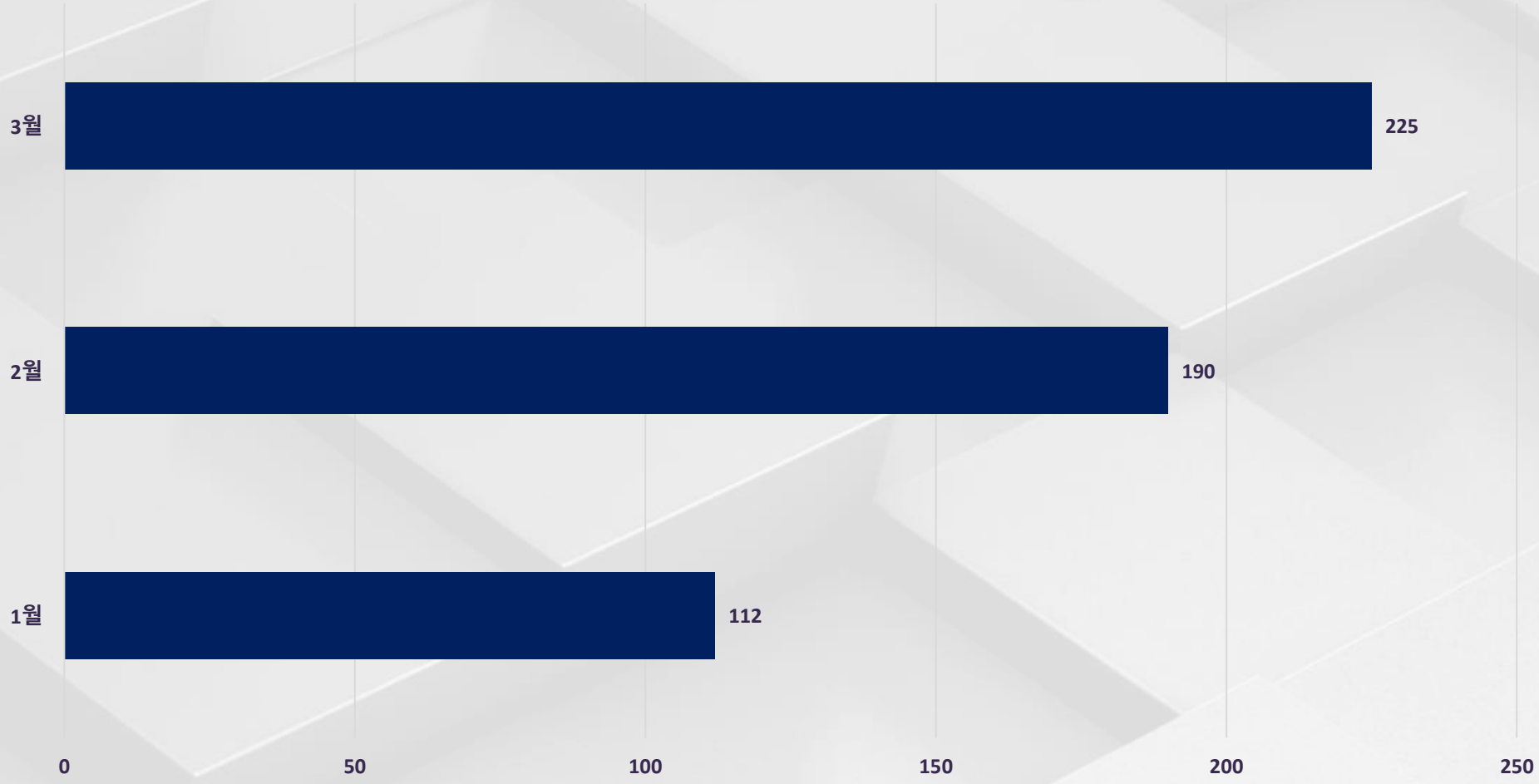
피해 국가 통계 (2022년 1분기)



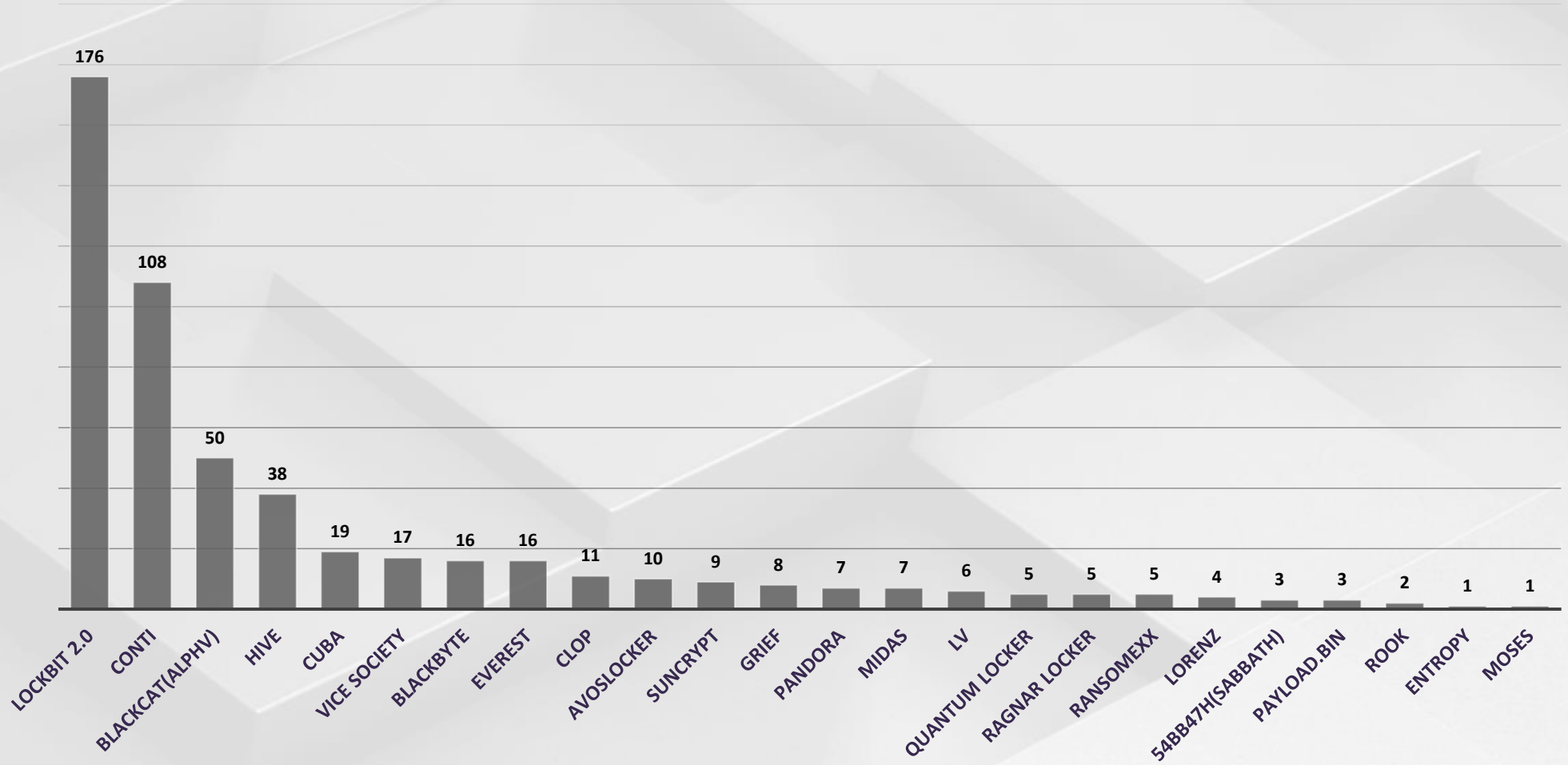
피해 산업별 통계 (2022년 1분기)



월별 피해 기업 개수 (2022년 1분기)



랜섬웨어 조직별 피해 기업 통계 (2022년 1분기)




The light shines in the darkness
quaxar

2억+

월평균 악성 도메인 탐지를 위해 수집하는 데이터 양

7,300%

작년 상반기 대비 수집 데이터양 증가 비율

S2W
Safe and Secure World

50억+

다크웹 내 유출된 개인정보 계정

2.5억+

다크웹 내 유출된 한국인 계정 정보

S2W
Safe and Secure World

1,200%

다크웹 / 표면웹 / 은닉 메신저 등 데이터 채널 대폭 확대를
통한 수집 데이터양 증가

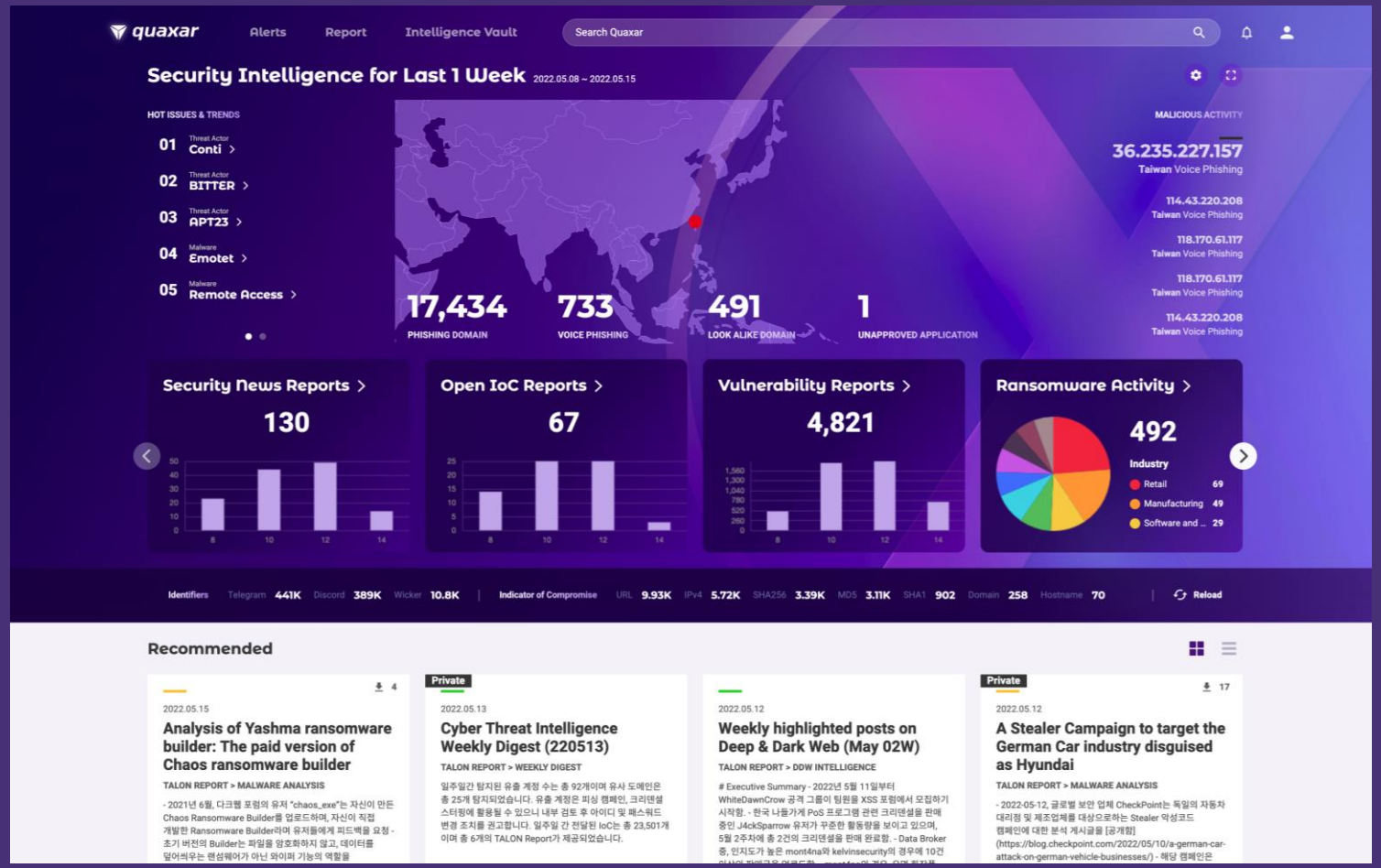
S2W
Safe and Secure World

180+

추적 중인 랜섬웨어 그룹

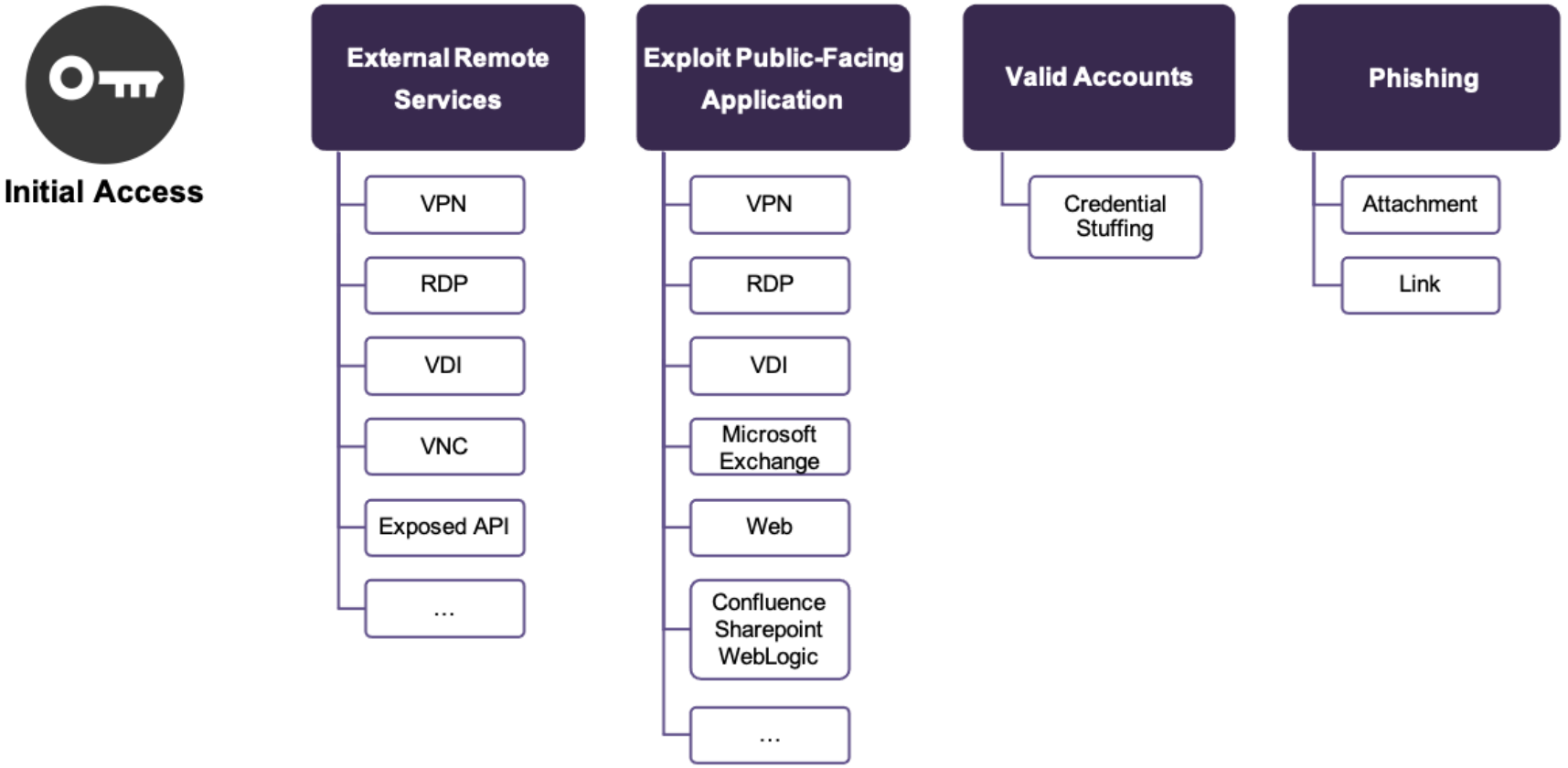
S2W
Safe and Secure World

quaxar



- ✓ 데이터 수집 채널, 데이터 수집량, 데이터 처리 속도, 자연어 처리 엔진, 데이터 저장 방식 효율화 등 전반적인 솔루션 핵심 성능 향상
- ✓ 데이터 가시성, 컨텐츠 모니터링 룰, 대시보드 사용자화 등 인텔리전스 제공 시의성 및 사용자 편의성을 향상시키기 위한 솔루션 기능 대폭 개선

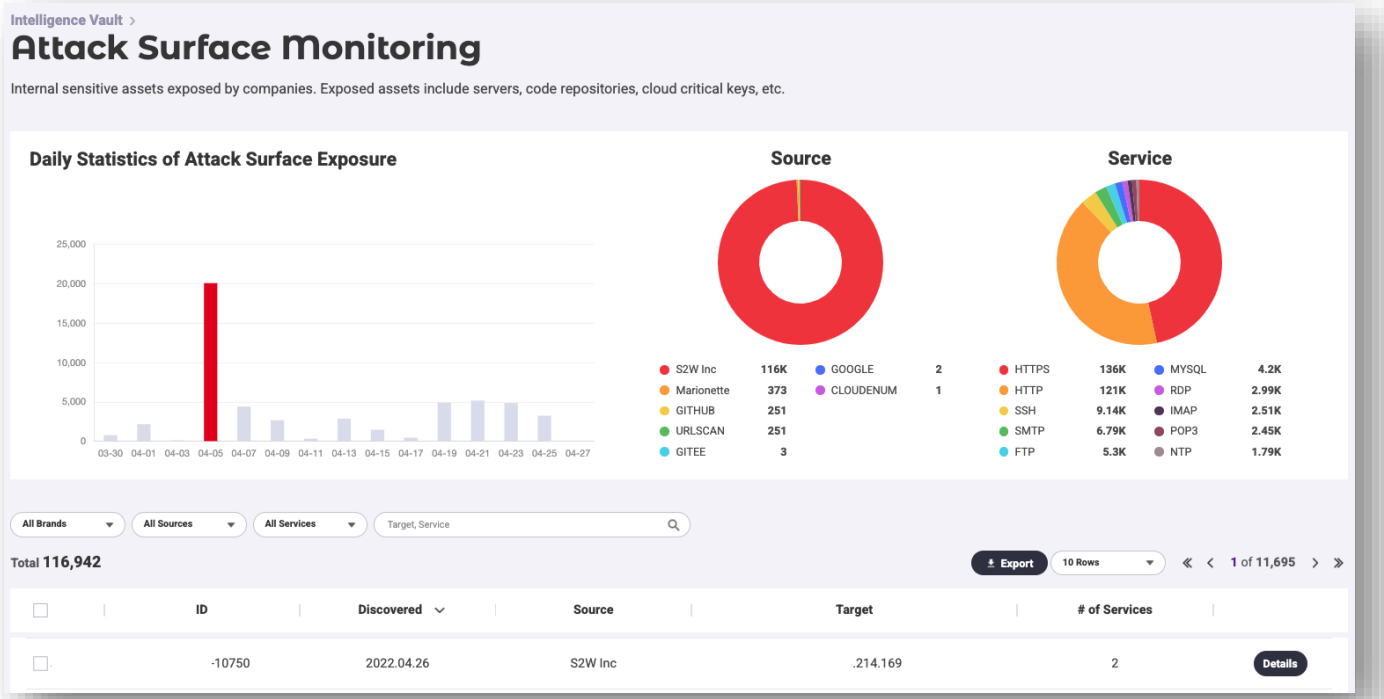
주요 침투 경로

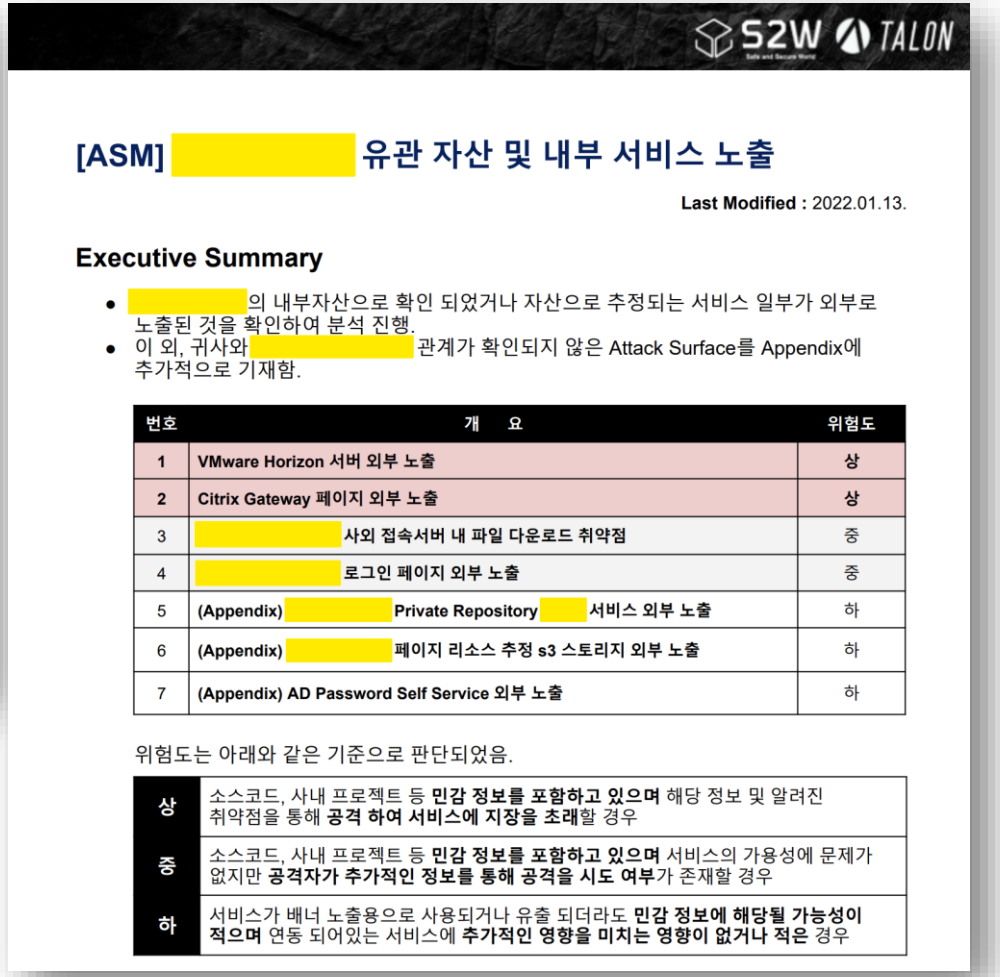


Active Threat and Vulnerability Management – *Attack Surface Monitoring*

Quaxar를 통해 기업의 공격 표면을 주기적으로 모니터링 합니다. 내부 통제를 벗어난 민감한 인프라와 정보의 노출을 관리합니다.

- 기업에서 사용 중인 클라우드 자산의 취약점 및 노출된 공격 표면에 대한 상태 진단도 진행합니다.





Active Threat and Vulnerability Management – *Attack Surface Monitoring*

다크웹 포럼 내 Auctions에서 Access가 거래 비중은 약 72%를 차지합니다.

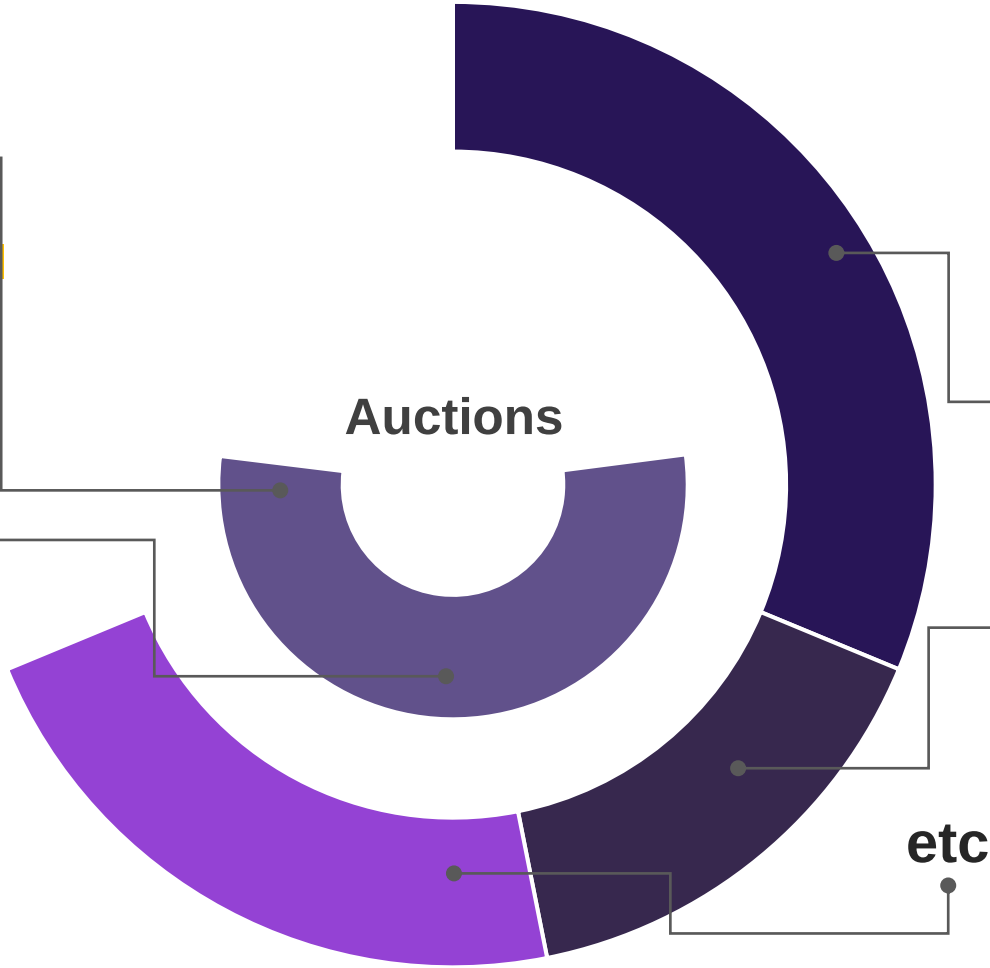
46%

Auctions에서 판매되는 **Access 거래 비율**

(옥션 내 전체 거래량 : 2,876)

110.75

월간 평균 Access 거래량



72%

기업 네트워크 Access 거래

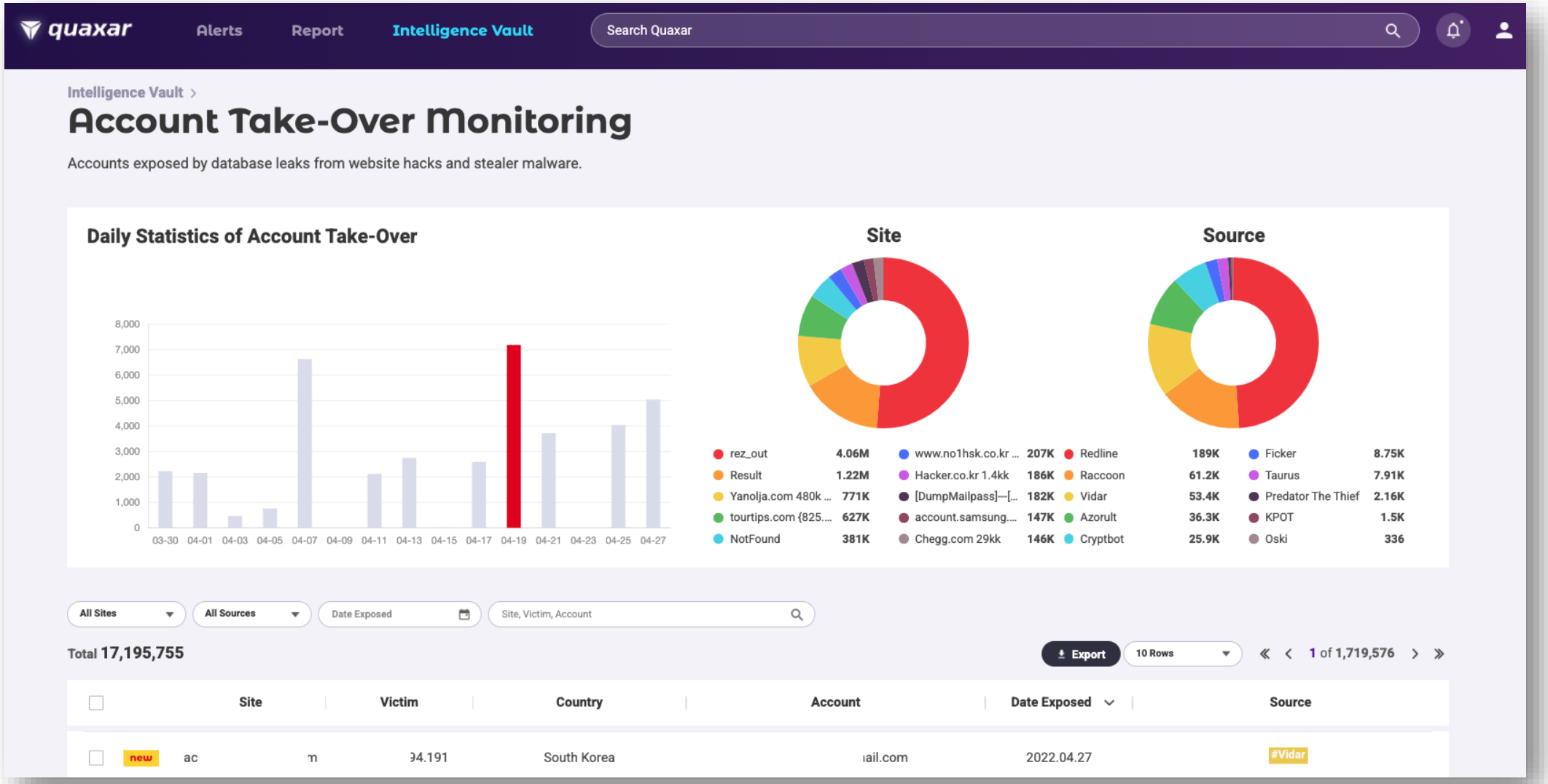
RDP 36%

VPN 27.82%

etc

Digital Risk Protection: *Account Take-over Monitoring*

Quaxar를 통해 외부에 유출된 직원 및 사용자 계정에 대한 가시성을 확보합니다.



Digital Risk Protection: *Account Take-over Monitoring*

랜섬웨어 공격자들은 Stealer 악성코드에 의해 탈취된 크리덴셜을 통해 기업 내부에 접근할 수 있습니다.

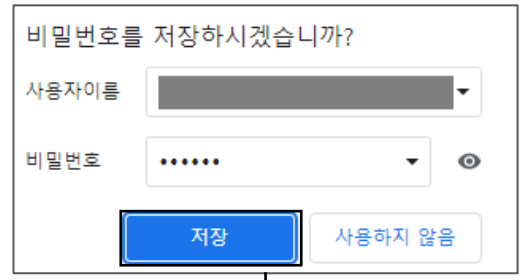
다크웹에서 판매되는 MaaS

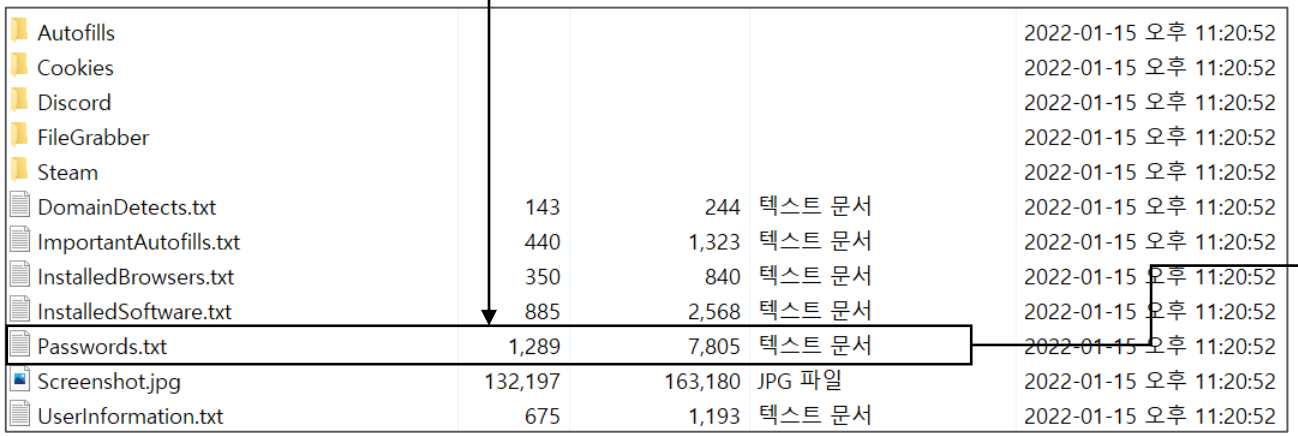
Raccoon stealer

Redline stealer

Ficker stealer

.
.
.





Autofills				2022-01-15 오후 11:20:52
Cookies				2022-01-15 오후 11:20:52
Discord				2022-01-15 오후 11:20:52
FileGrabber				2022-01-15 오후 11:20:52
Steam				2022-01-15 오후 11:20:52
DomainDetects.txt	143	244	텍스트 문서	2022-01-15 오후 11:20:52
ImportantAutofills.txt	440	1,323	텍스트 문서	2022-01-15 오후 11:20:52
InstalledBrowsers.txt	350	840	텍스트 문서	2022-01-15 오후 11:20:52
InstalledSoftware.txt	885	2,568	텍스트 문서	2022-01-15 오후 11:20:52
Passwords.txt	1,289	7,805	텍스트 문서	2022-01-15 오후 11:20:52
Screenshot.jpg	132,197	163,180	JPG 파일	2022-01-15 오후 11:20:52
UserInformation.txt	675	1,193	텍스트 문서	2022-01-15 오후 11:20:52

웹 브라우저에 저장되어 있는 ID / PW

URL: https://cc.[redacted]kr[redacted]admin/login.html
Username: [redacted]
Password: [redacted]
Application: Google_[Chrome]_Default

관리자 계정
아이디 패스워드

Digital Risk Protection: *Account Take-over Monitoring*

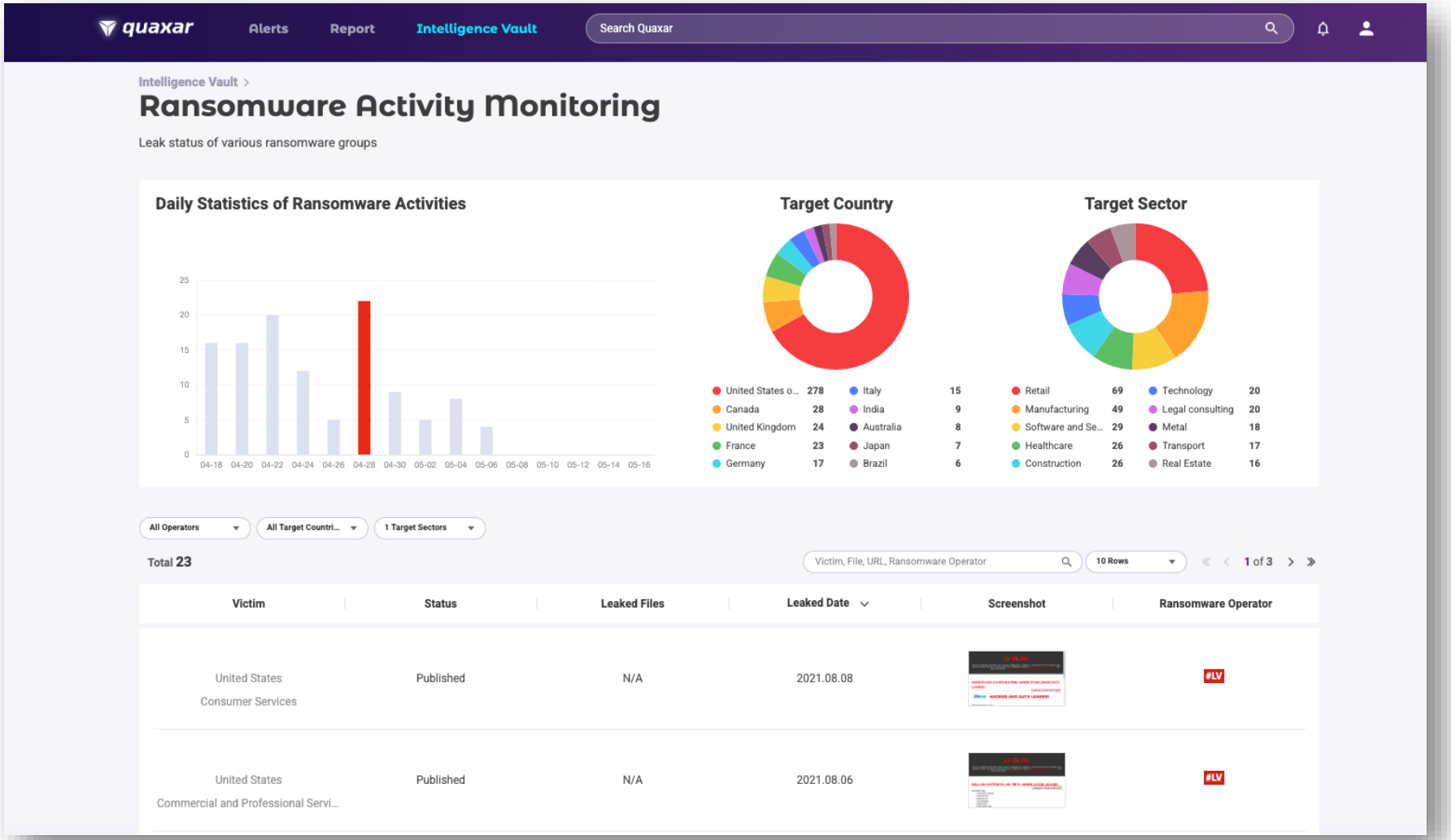
Stealer에 감염될 경우, 감염기기에 저장된 모든 민감 데이터 및 크리덴셜이 탈취됩니다.

Stored Path	Target Items		
User data in the Browser	Password AutoFill	History Downloads	CC
Crypto Wallet	wallet.dat		
Wallet Extension on Browser	Chrome	Edge	Edge Beta
FTP software	FileZilla	WinSCP	Total Commander
VPN software	ProtonVPN	OpenVPN	NordVPN
Messenger	TOX	Element	Signal	Proxifier
Others	Steam	Discord	Telegram	Pidgin
Outlook	Files	Outlook		

분류	수집 정보		
감염 기기 정보	- Username - Monitor Size - OS version	- Language - Malware File Location - Process	- HW Serial - Time zone - IPv4
하드웨어 정보	- Processor - Graphic - Memory		
설치 정보	[Browser] - Name - Version - Path	[SW] - Name - Version	[Anti-Virus] - Name
지갑 정보	- *wallet* file - wallet.dat file		
계정 정보	[FTP] - Port - Username - Password	[Browser] - Name - Autofill - Profile - CC - Login - Cookie	[VPN] - URL - Username - Password
User Data 정보	[Telegram] - All files in tdata folder	[Discord] - Token.txt file	[Steam] - *ssfn* files - *.vdf files
로컬 파일 정보	- Files in Desktop / Documents (keyword extension: *.txt, *.doc*, *key*, *wallet*, *seed*)		

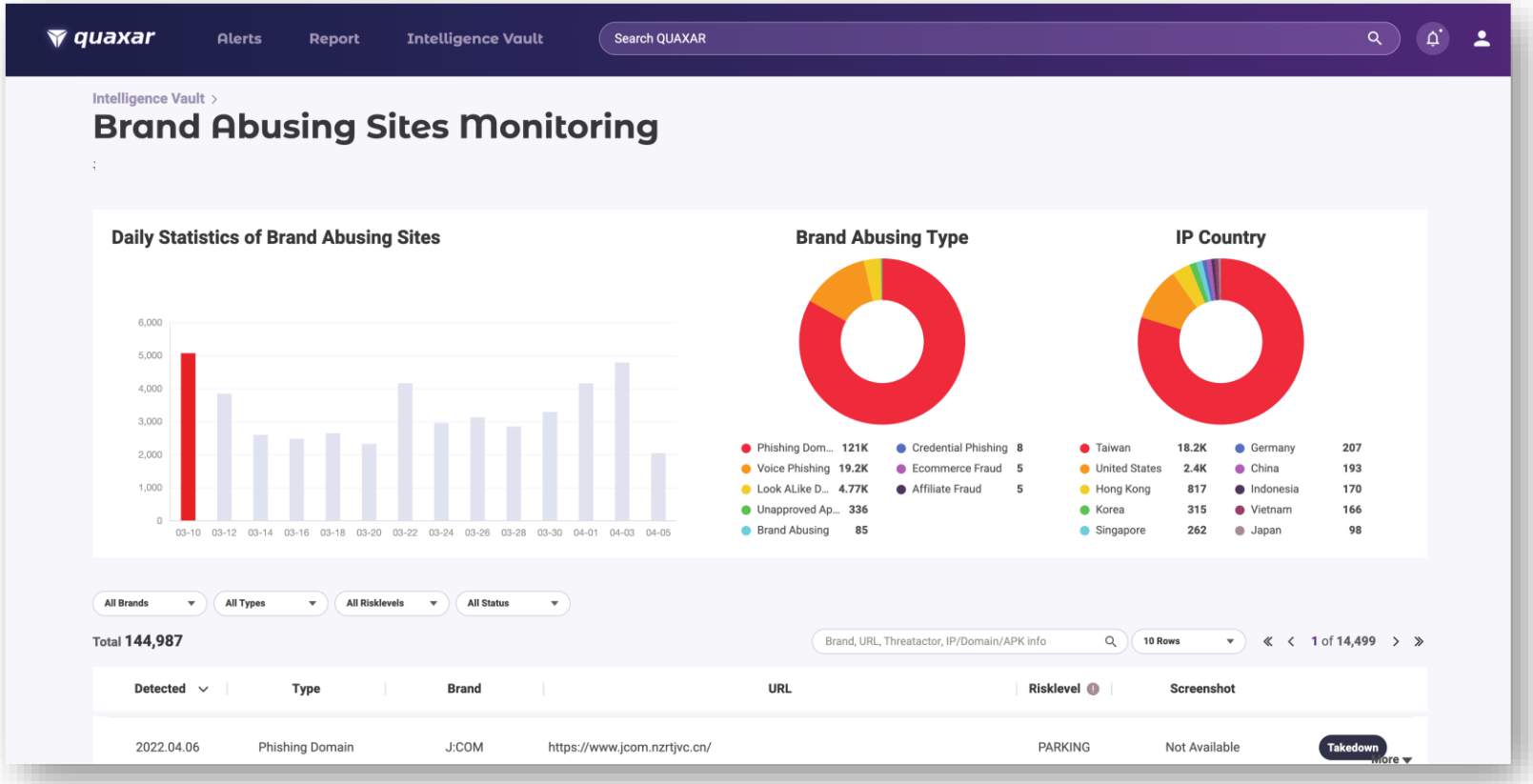
Digital Risk Protection: *Ransomware Activity Monitoring*

Quaxar를 통해 랜섬웨어에 타겟하는 대상의 국가 별, 산업 별 트렌드에 대한 가시성을 확보합니다.



Digital Risk Protection: *Brand Abusing Sites*

Quaxar를 통해 브랜드 사칭 및 악용 사이트 등 잠재적 위협으로부터 브랜드 가치를 보호합니다.



✓ QUAXAR는 월 평균 2억개 이상의 도메인 관련 정보를 분석하여 아래와 같은 위협을 탐지합니다.

✓ 브랜드 어뷰징 & 피싱 사이트 탐지

✓ 비정상 모바일 앱 탐지

› 어뷰징 사이트 종합적으로 탐지

› 실시간 수집, 일별로 통계 집계

› 어뷰징 사이트 활성화 상태 제공

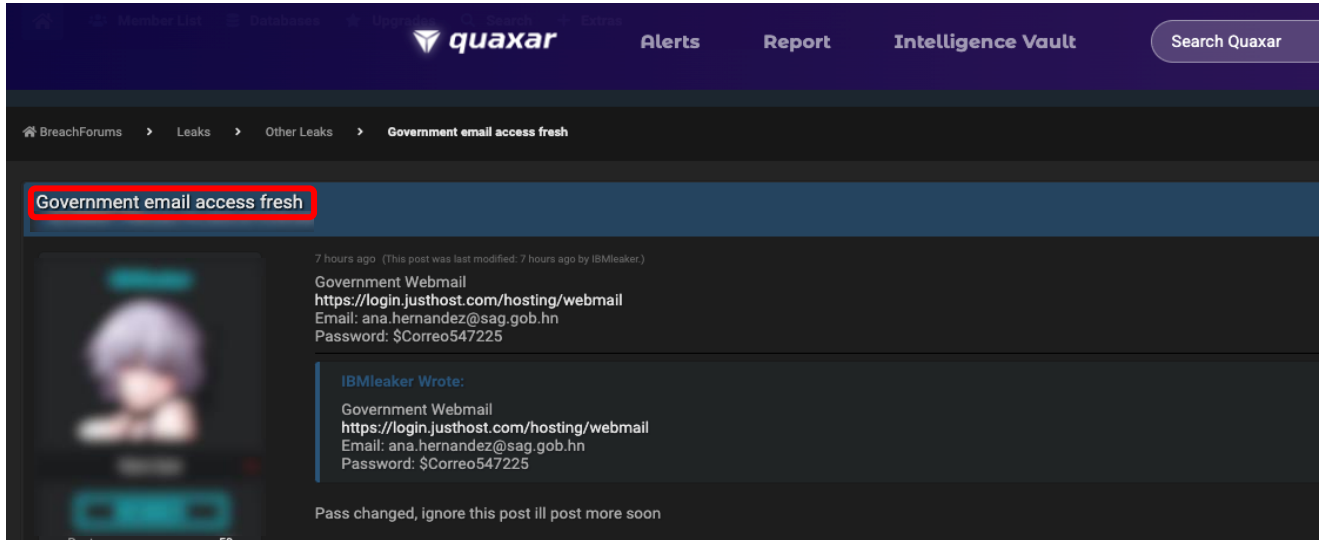
› 필터링으로 브랜드 어뷰징 유형별 위협 사이트 확인 가능

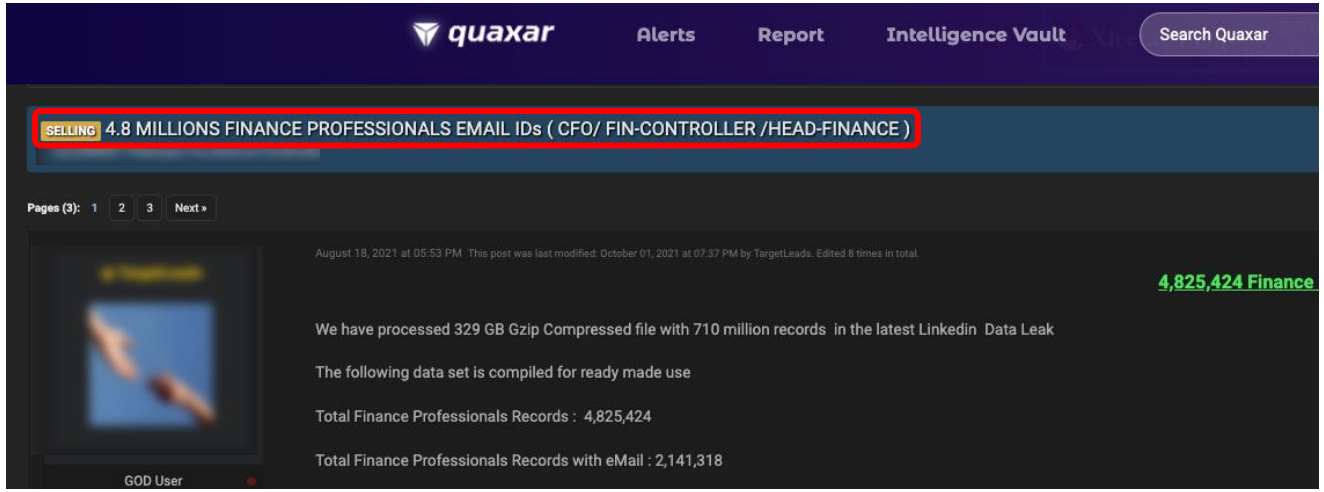
✓ 브랜드 악용 사이트/앱 테이크다운 (Take down)

› 어뷰징 사이트 및 앱 처리/제거 서비스

Digital Risk Protection: *Brand Abusing Sites*

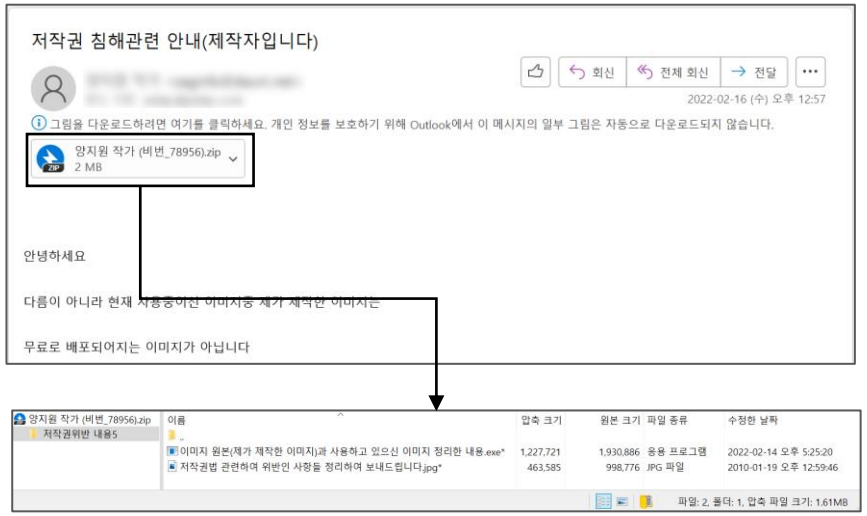
공격자들은 다크웹에서 확보한 기업 정보를 활용하여 해당 기업을 사칭하는 스팸 메일 캠페인을 수행할 수 있습니다.





유출된 계정 정보

특정 직업군, 기업 메일 등 정리되서 유출되는 계정



Talon Report: *(Quick) Overview of Ransomware Group*

랜섬웨어 전문 분석가가 제공하는 REPORT를 통해 랜섬웨어 그룹별 공격 도구 및 전략 등을 확인할 수 있습니다.

quaxar Alerts Report Intelligence Vault revil

RFI

2022.02.07

Who Is Behind the BlackCat Ransomware?

TALON REPORT > DDW INTELLIGENCE

PDF Report

11월 중순부터 활동을 시작한 BlackCat 랜섬웨어는 미국, 호주, 인도를 포함한 여러 국가를 대상으로 공격을 시도하였으며, 이들이 운영하고 있는 데이터 유출 사이트(Leak site)에 공개된 피해 기업만 현재까지 (2022. 02. 07) 28개가 확인되었다. 이들은 피해 기업 별로 협상 사이트를 제공하며 채팅 및 협상 금액 지불을 요구하는데, Bitcoin 또는 Monero를 통해 $400,000~$3,000,000의 몸값을 요구하는 것으로 알려져 있다.

BlackCat 랜섬웨어는 현재까지 기존 RaaS 랜섬웨어 그룹에서 사용한 이력이 없는 Rust 언어로 작성되었으며, Windows 및 Linux 운영 체제를 모두 지원하고 있다. 또한, ChaCha20 및 AES 암호화 알고리즘을 모두 지원하며, 암호화 모드와 같은 주요 설정 값은 협렵사들이 옵션을 통해 자유자재로 설정할 수 있다. BlackCat은 알려진 사이버 범죄 포럼에서 계열사를 모집하여 계열사가 피해기업과의 협상 금액의 80-90%를 가져갈 수 있도록 제안 중이다.

최근에는 TheRecord라는 매체를 통해 인터뷰를 수행했으며, 인터뷰 내용과 몇몇 분석가 등에 의해 BlackCat 랜섬웨어 공격자들이 Darkside와 BlackMatter의 리브랜드라고 알려졌지만, 현재까지 이를 뒷받침할 수 있는 증거는 공개되지 않은 상황이다. 인터뷰 상에서 공격자들은 자신들이 GandCrab/REvil 그룹, BlackMatter/DarkSide 그룹, Maze/Egregor 그룹, Lockbit 그룹과 연결되어 있다고 언급하였다.

Conclusion

랜섬웨어 그룹의 경우, RaaS 운영 및 랜섬웨어 개발과 같은 주요 핵심 멤버들과 실제 기업에 대한 공격을 수행하는 협력사들로 구성되어있는데, 협력사들의 경우 단일 그룹에 속해있지 않은 경우도 있고, 일시적으로 고용된 형태이기 때문에 같은 그룹의 일원이라고 보기는 어렵다. 그렇기 때문에 리브랜딩(Rebranding)이라 함은, RaaS를 실질적으로 운영하던 핵심 멤버들이 자신들의 랜섬웨어를 새롭게 개발하고, 새로운 관리자 패널을 개발하는 등의 인프라 변화가 일어난다고 할 수 있으며, 이후 포럼에서 광고 등을 통해 새로운 협력사를 구하는 과정이 추가로 필요하다.

BlackCat 랜섬웨어 공격자가 인터뷰에서 언급한 다른 그룹과의 연결은 현재까지는 핵심 멤버가 아닌, 해당 그룹과 함께 일했던 협력사들을 고용함으로써 언급한 것으로 추정된다.

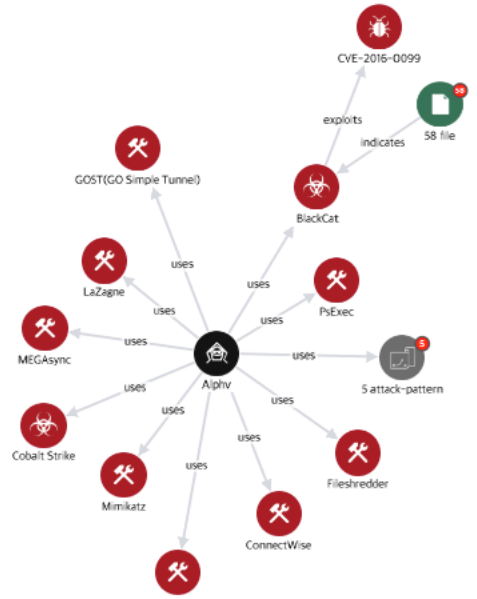
과거 BlackCat 랜섬웨어 관련 정리 보고서 참고: [DDW][MAL] BlackCat : New Rust based ransomware borrowing BlackMatter's configuration

Related

TAGS

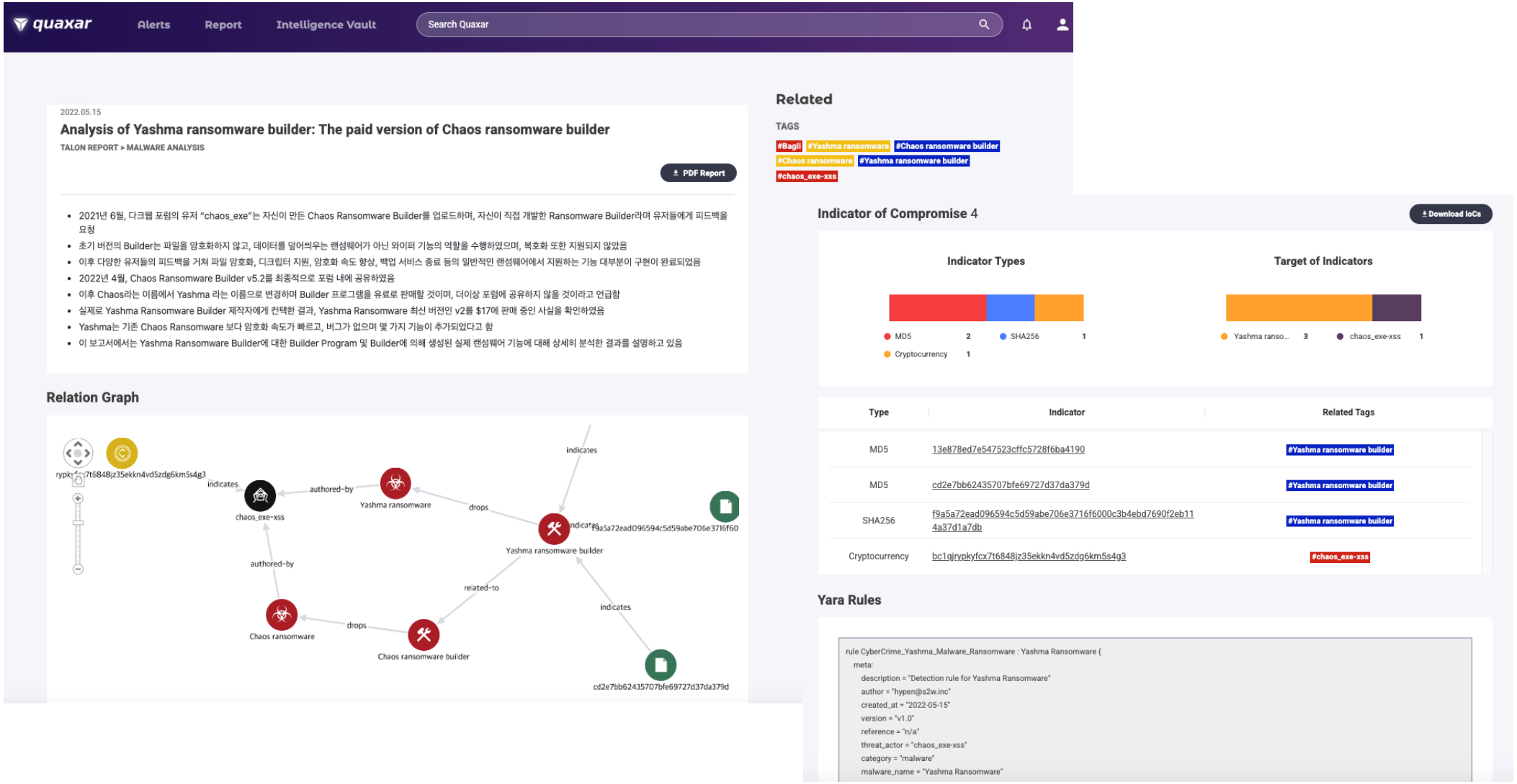
#CVE-2016-0099 #ConnectWise #BlackCat #Valid Accounts #Exploit Public-Facing Application #Data Encrypted for Impact #Inhibit System Recovery #Fileshredder #BlackCat #MEGAsync #LaZagne #Data Destruction #Cobalt Strike #WebBrowserPassView #GOST(GO Simple Tunnel) #PsExec #Mimikatz #Alphv #Noberus

Relation Graph



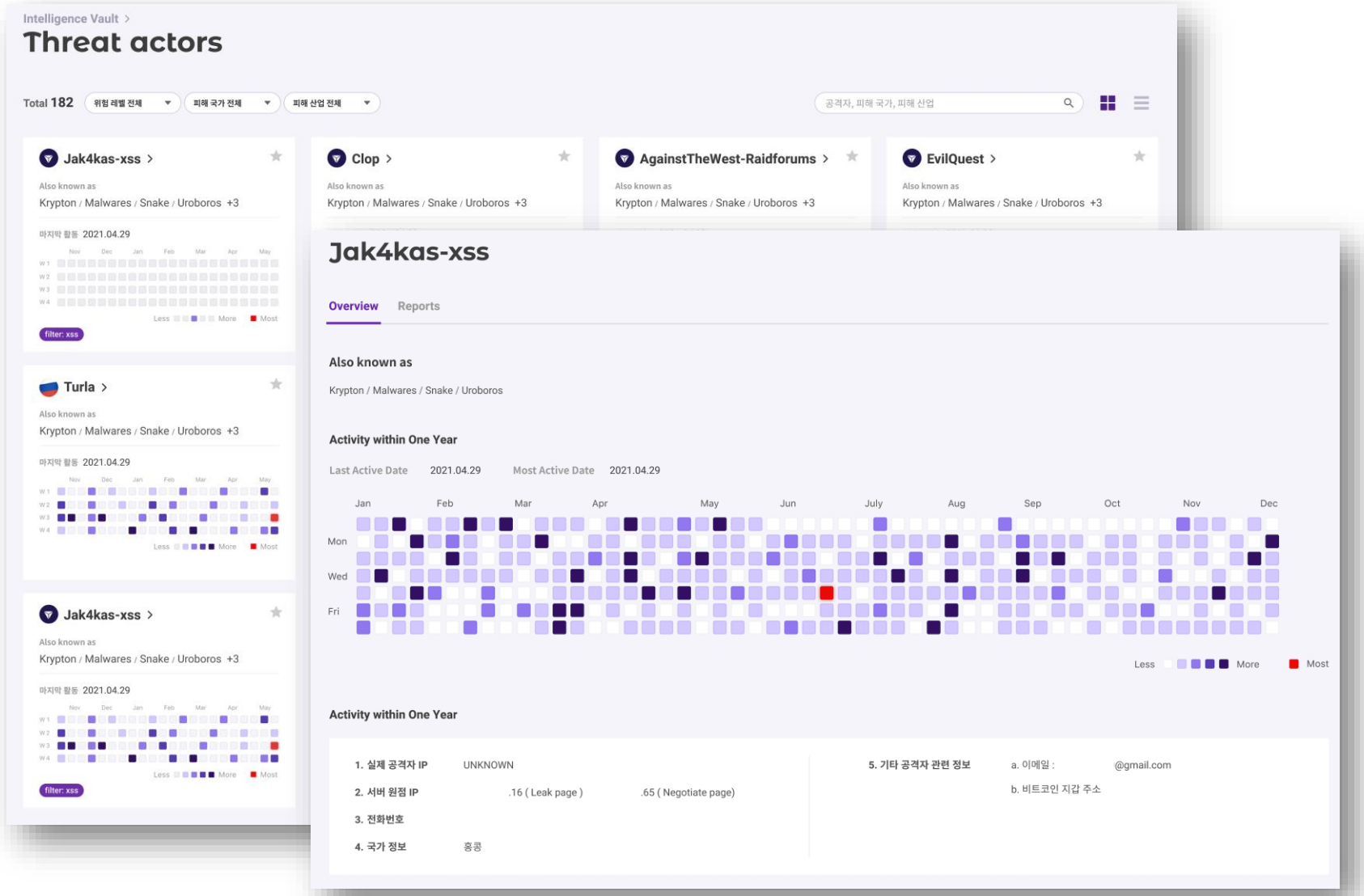
Talon Report: *Detailed Analysis of Ransomware, Botnet*

랜섬웨어 전문 분석가가 제공하는 상세 분석 REPORT를 통해 랜섬웨어 및 봇넷 별 주요 행위를 확인할 수 있습니다.



Active Threat and Vulnerability Management – *Threat actors*

기존 APT 그룹 뿐만 아니라 Deep & Darkweb에서 활동하는 사이버 범죄자 포함 100여개가 넘는 공격 그룹 정보를 제공합니다.



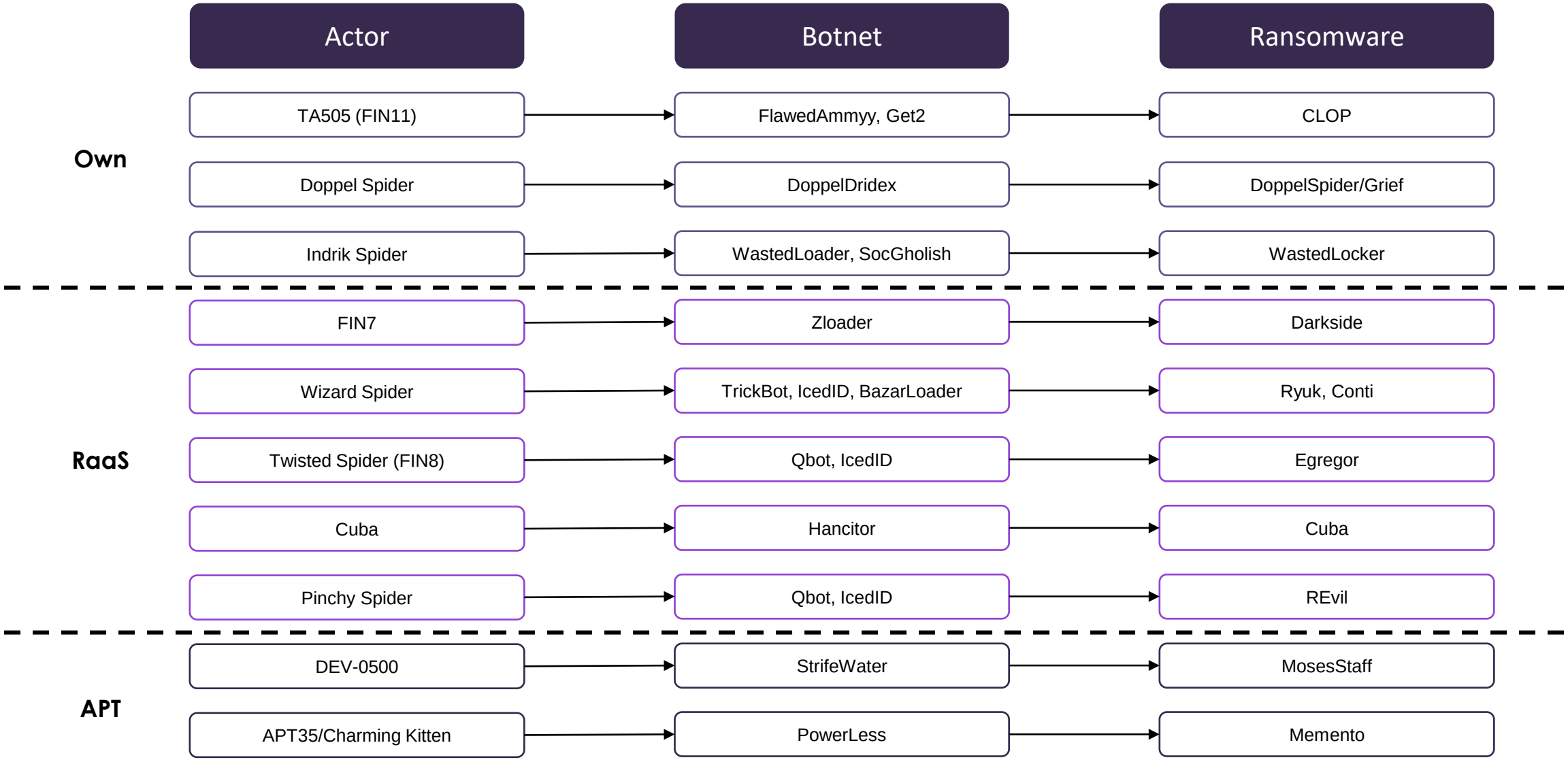
Active Threat and Vulnerability Management – *Threat actors*

기존 APT 그룹 뿐만 아니라 Deep & Darkweb에서 활동하는 사이버 범죄자 포함 100여개가 넘는 공격 그룹 정보를 제공합니다.

Cerber	>	GandCrab	>	**Sodinokibi/REvil**		
Lockbit	>	**Lockbit 2.0**				
BitPaymer	>	DoppelPaymer	>	Grief	>	**Entropy (Weak)**
Vasa Locker	>	Babuk	>	Payload.bin	>	**RAMP**
WastedLocker	>	Hades	>	Phoenix	>	**Macaw**
Darkside	>	BlackMatter	>	**BlackCat (Weak)**		
Prometheus	>	**Spook**				
SynAck	>	**El_Cometa**				
ThunderCrypt	>	**Lorenz**				
HERMES	>	RYUK	>	**Conti**		
MountLocker	>	Astro Team	>	XING Locker	>	**Quantum Team**
Haron	>	**MIDAS**				
Nemty	>	Nefilim	>	**Karma**		
Maze	>	Sekhmet	>	Egregor	>	**WhiteRabbit (Weak)**

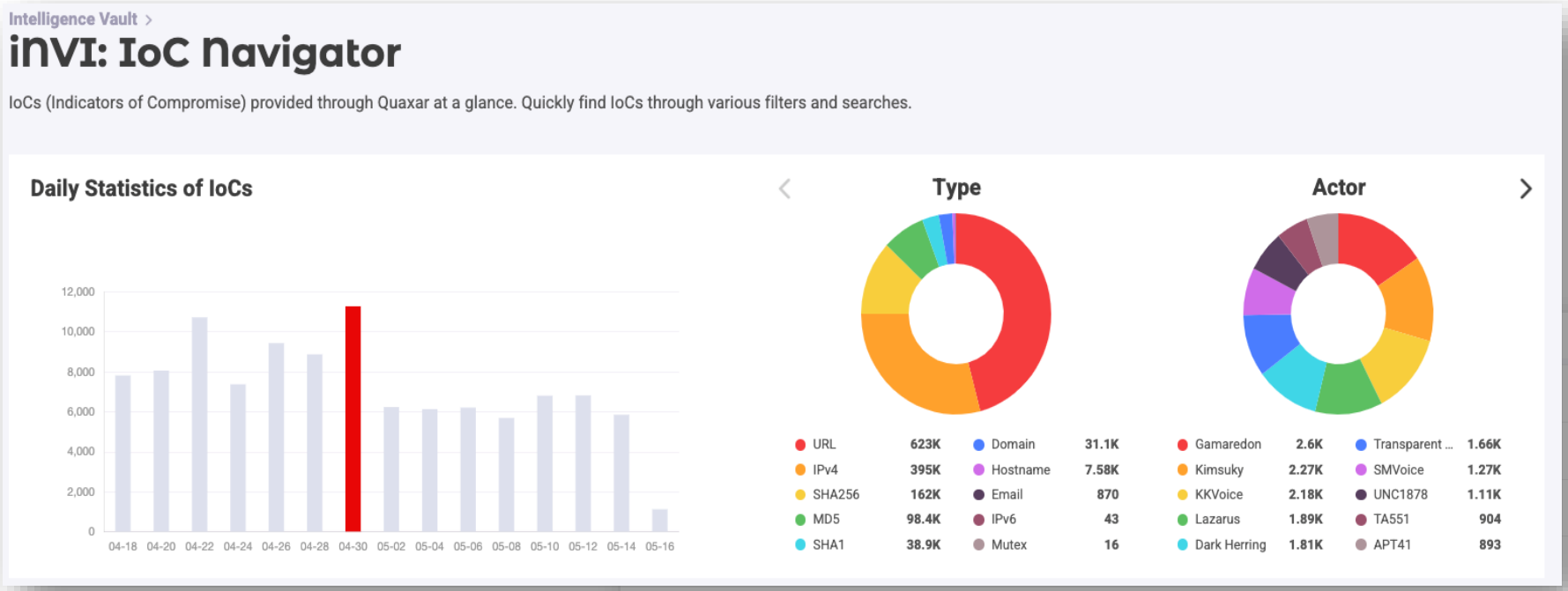
Active Threat and Vulnerability Management – *Threat actors*

기존 APT 그룹 뿐만 아니라 Deep & Darkweb에서 활동하는 사이버 범죄자 포함 100여개가 넘는 공격 그룹 정보를 제공합니다.



Active Threat and Vulnerability Management – *IOC Navigator*

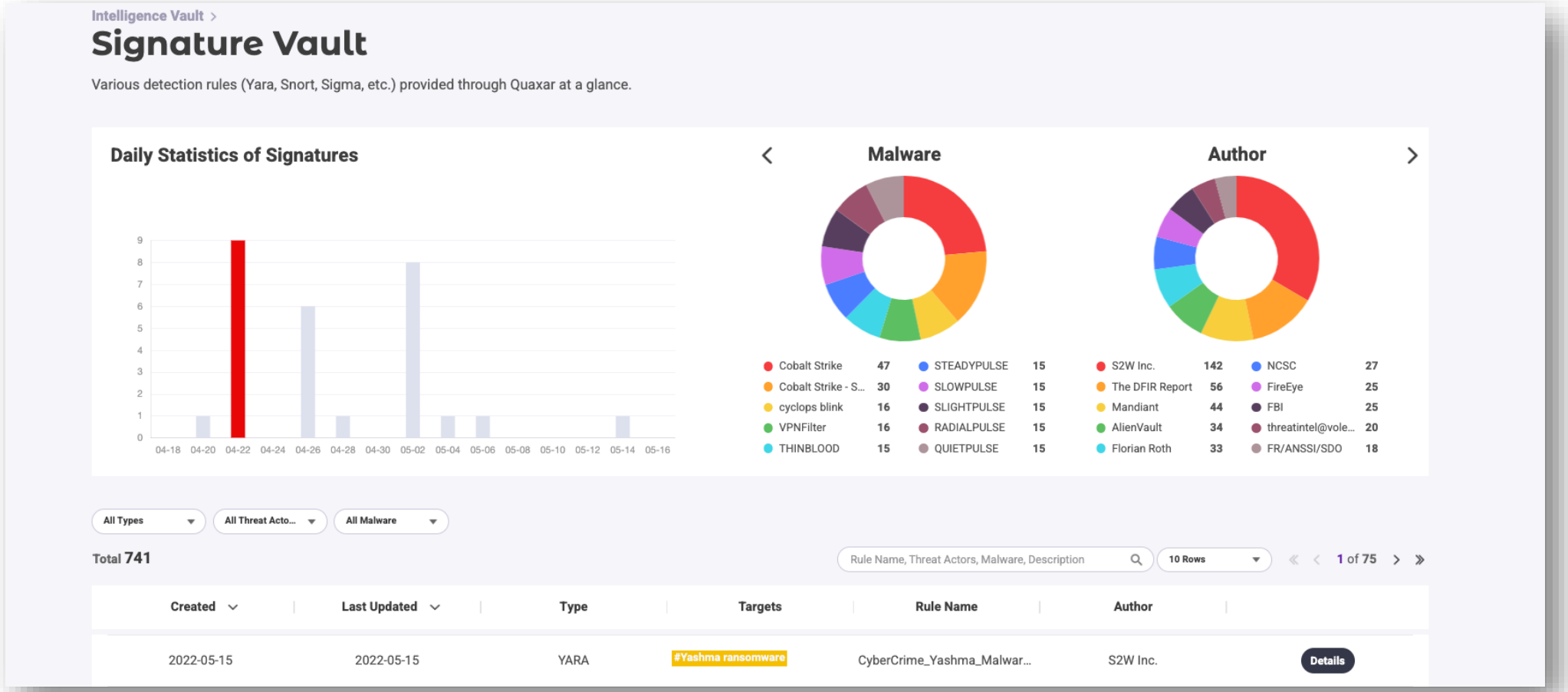
다양한 외부 위협에 대한 유의미한 대응책을 신속하게 제공합니다.



					Quaxar Score	Related Tags	Lifetime
2022-04-15	SHA256	5d517ff8488e88a58b10805294d72e90697aa92fc29c332b1edf913507356dfa		S2W Inc.	Level 5	#Makop Ransomware	30 / 30
2022-04-15	MD5	aa8ab4616d872f6e3024b75057fd0782		S2W Inc.	Level 5	#Makop Ransomware	30 / 30
2022-04-15	MD5	1ba7523c76e971353d27e9ea6ec8c524		S2W Inc.	Level 5	#Makop Ransomware	30 / 30
2022-04-13	SHA256	7594bf1d87d35b489545e283ef1785bb2e04637cc1ff1aca9b666dde70528e2b		S2W Inc.	Level 3	#Gwisin	30 / 30
2022-04-12	SHA256	4587e7d8e56a7694aa1881443312c1774da551459d3a48315acd0c694bcf87a0	[External] https://github.com/rivitna/Malware...		Level 5	#hive	30 / 30
2022-04-12	SHA256	e1b559fc7842194ffded24222f8c8d0cd84b3ce5093fec4a03152bbd56d0ea11	[External] https://github.com/rivitna/Malware...		Level 5	#hive	30 / 30

Active Threat and Vulnerability Management – *Signature Vault*

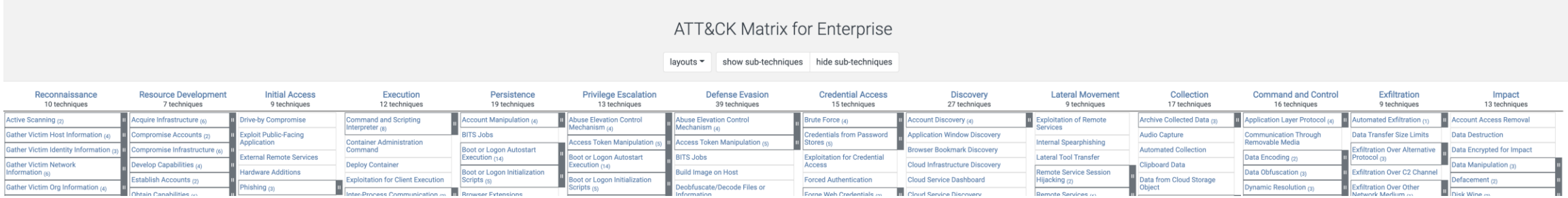
악성코드 및 공격 도구에 대한 탐지룰을 통해 위협에 선제적으로 대응합니다.



Active Threat and Vulnerability Management – *Signature Vault*

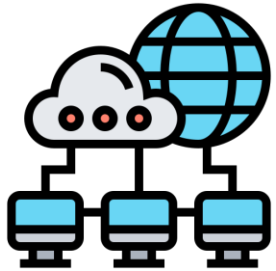
다양한 스테이지에서 악성 여부를 확인할 수 있도록 여러 종류의 탐지 시그니처를 제공합니다.

ATT&CK



Yara rule

Snort rule



Sigma rule

Quaxar의 특별함

S2W는 독자적인 데이터 수집 기술을 통해 외부 위협을 종합적으로 관제합니다.
더불어 관계 분석 그래프, 고도화된 NLP 기술 등을 이용해 신속하게 위협을 분석하고 정확한 원인을 파악합니다.

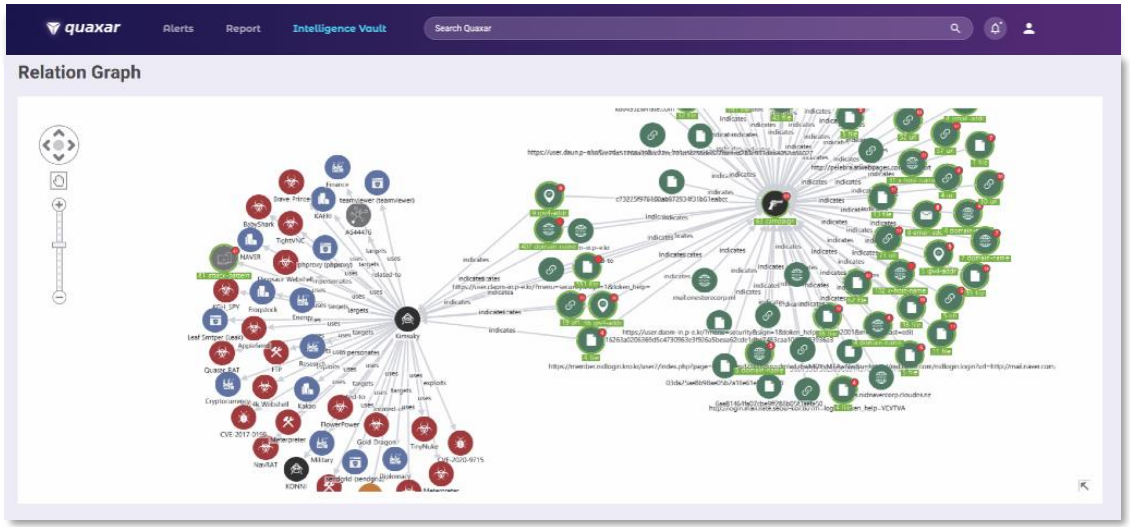
광범위한 모니터링 채널 및 데이터 수집

1 Internal Threat Intelligence

2 External Threat Intelligence: Surface Web

3 External Threat Intelligence: Deep/Dark Web

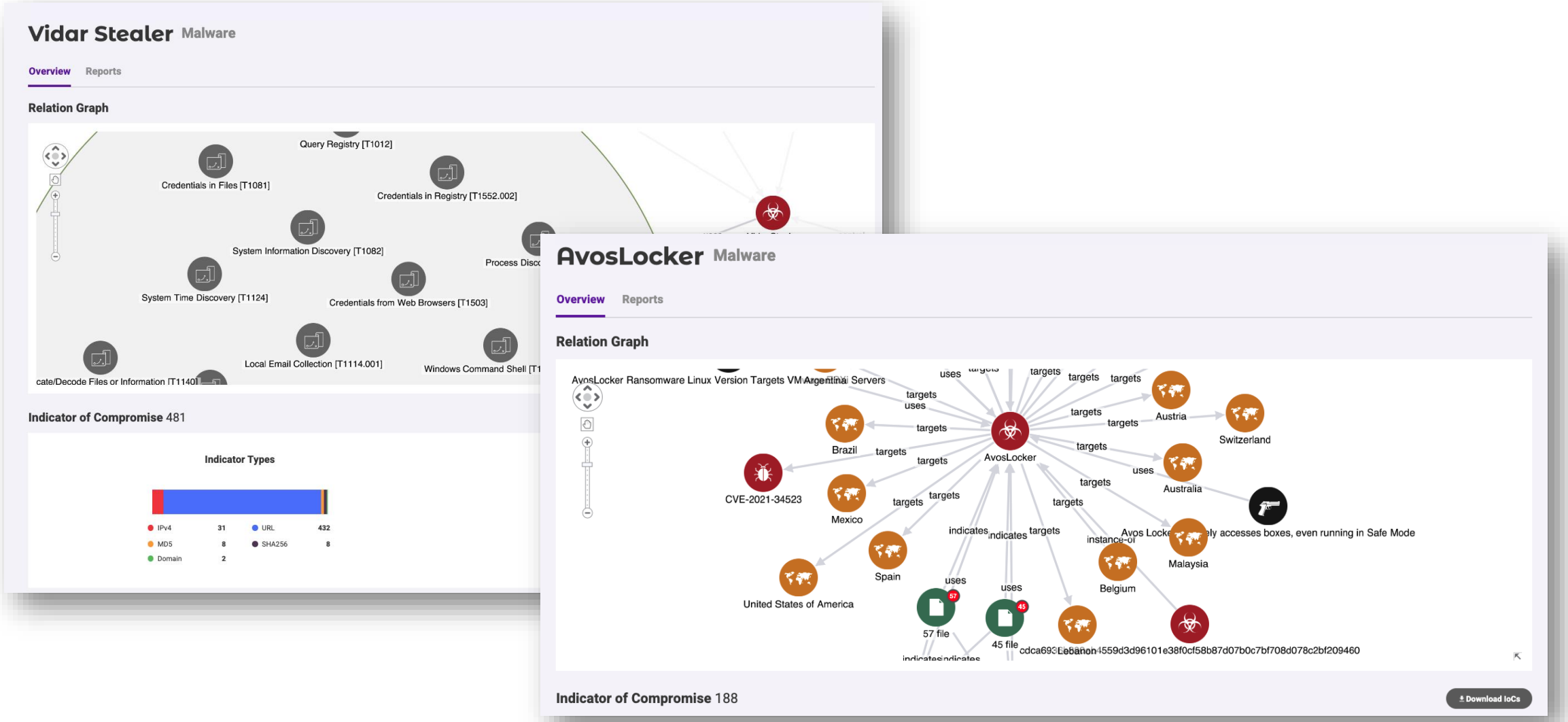
구체화된 관계 그래프를 통한 심층 분석



사이버 위협 표현 규격인 STIX를 이용해 CTI(Cyber Threat Intelligence) 정보 간의 관계를 일관성 있고 체계적으로 분석 가능

Quaxar Advanced Search

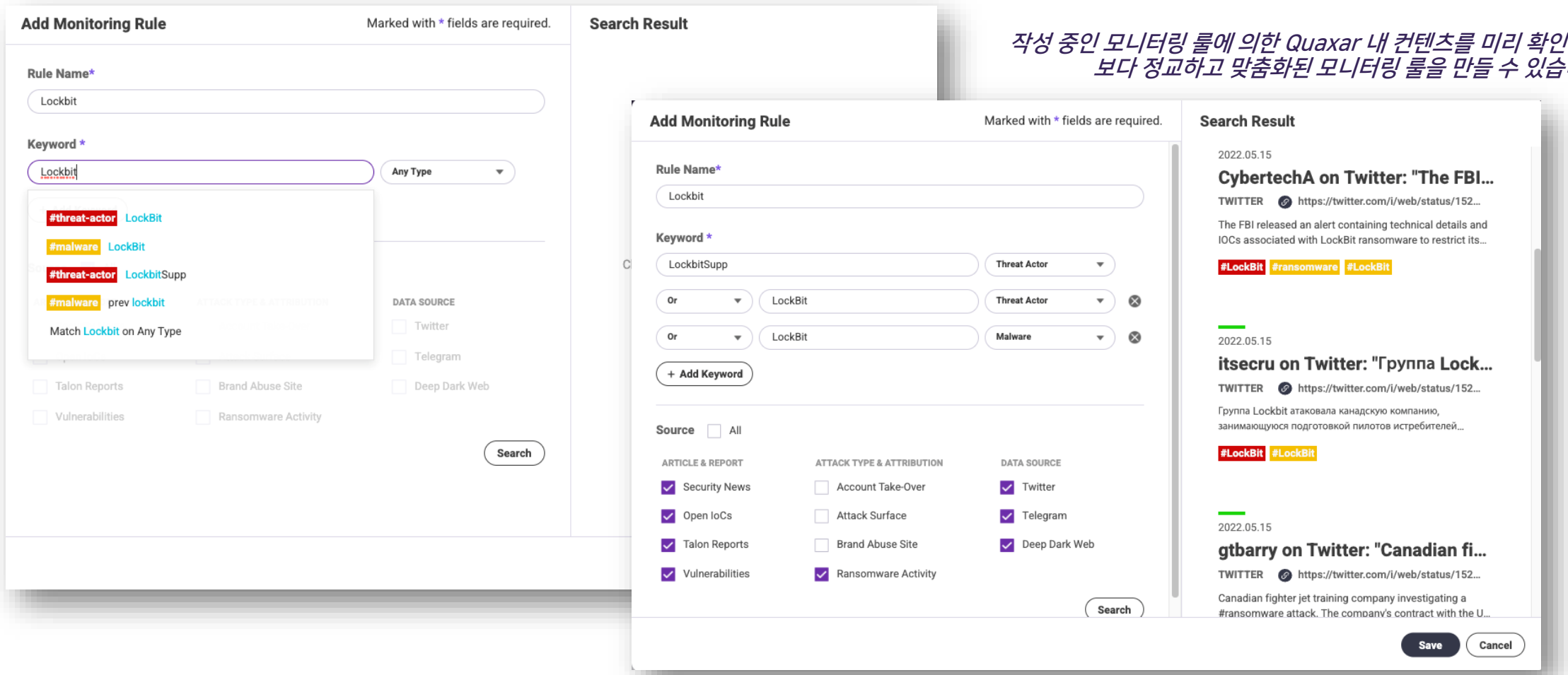
Quaxar는 STIX (Structured Threat Information Expression) 에 따라 분류된 위협 정보를
그래프 형태의 연관성 정보와 함께 직관적인 검색 결과를 제공합니다.



Monitoring Rule

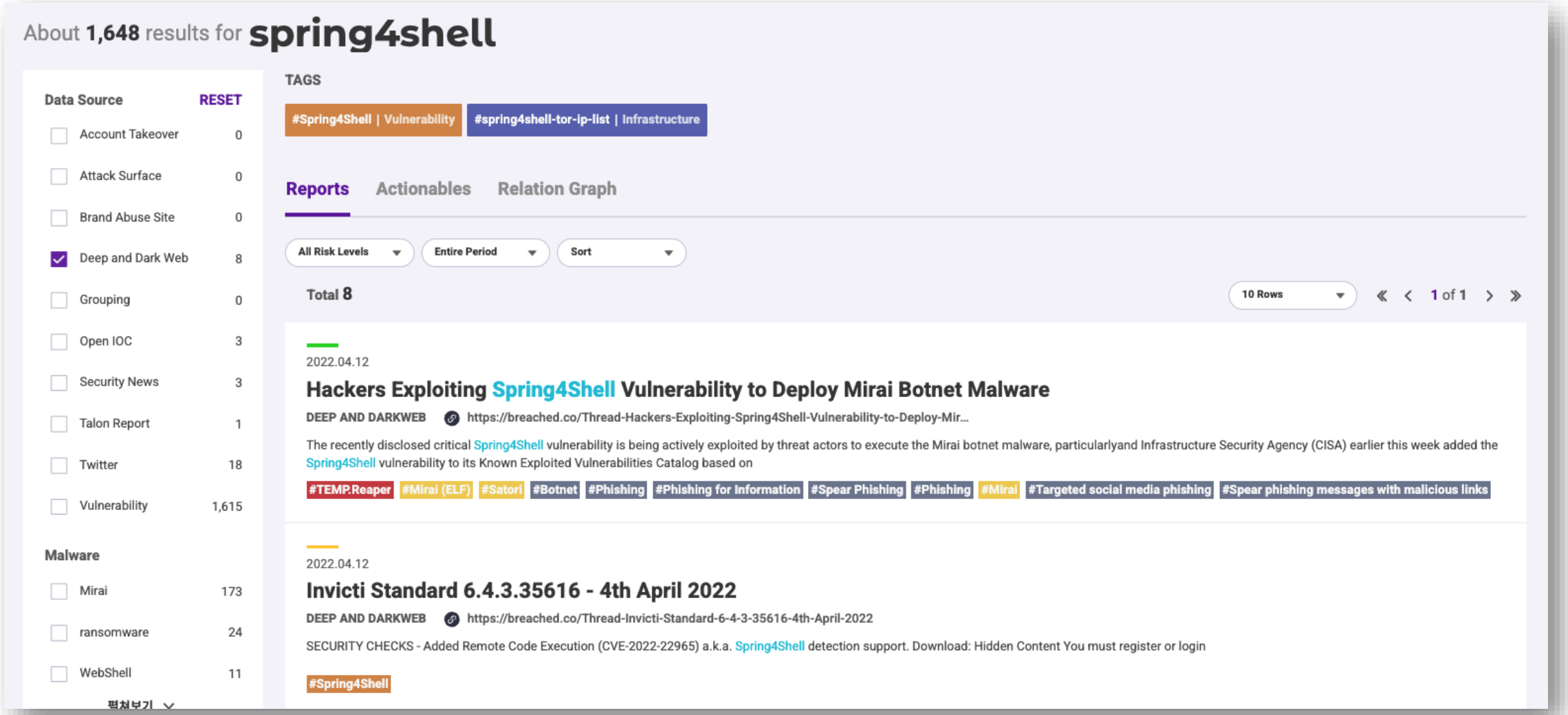
사용자는 Quaxar의 모니터링 룰을 통해 관심사항에 따른 주요 위협 정보를 정교하고 신속하게 확인 할 수 있습니다.

작성 중인 모니터링 룰에 의한 Quaxar 내 컨텐츠를 미리 확인하며,
보다 정교하고 맞춤화된 모니터링 룰을 만들 수 있습니다.



Advanced Search

Quaxar는 각종 자연어 처리 기술과 고도화된 데이터 정제 기술을 통해 최적화된 검색 결과를 제공합니다.



랜섬웨어 추적 관련 주요 업적

Cyclone 작전
Clop 랜섬웨어 검거 작전

- ✓ 원점 추적 위한 Clop 관련 인프라 정보 분석
- ✓ Clop 랜섬웨어 비트코인 자금흐름 분석
- ✓ 다크웹 내 Clop 랜섬웨어 오퍼레이터들의 활동 분석 및 프로파일링

INTERPOL EN ∨

INTERPOL deployed Operation Cyclone with the assistance of information provided by its private partners Trend Micro, CDI, Kaspersky Lab, Palo Alto Networks, Fortinet and Group-IB through INTERPOL's Gateway project.

Gateway boosts law enforcement and private industry partnerships to generate threat data from multiple sources and enable police authorities to prevent attacks.

Further illustrating the power of private sector cooperation in cybercrime investigations, two Korea-based cyber threat companies – S2W LAB and KFSI – also provided INTERPOL with valuable dark web data analysis throughout the operation.

Quicksand 작전
Gandcrab & Revil Sodinokibi 검거 작전

- ✓ 악성코드 관련 분석 정보
- ✓ 공격 그룹 관련 정보 제공

INTERPOL EN ∨

Bitdefender supported operations by releasing tailor-made decryption tools to unlock ransomware and enable victims to recover files. These innovative tools enabled more than 1,400 companies to decrypt their networks, saving them almost EUR 475 million in potential losses.

KPN, McAfee, S2W helped investigations by providing cyber and malware technical expertise to INTERPOL and its member countries.

Operation Quicksand continues to supply evidence that is feeding into further cybercrime investigations and enabling the international police community to disrupt numerous channels used by cybercriminals to launder cryptocurrency and commit ransomware crime.

온라인 아프리카 범죄 조직 분석

- ✓ 다크웹 내 아프리카 관련 범죄 분석 제공 (마약, 인신매매, 밀수 등)

INTERPOL enact

Online African organized crime from surface to dark web

- ✓ S2W가 제공한 분석 내용으로 발간한 인터폴 내부 보고서

ANALYTICAL REPORT

Quaxar 주요 서비스

Digital Risk Protection

브랜드 사칭 및 악용 사이트 등 잠재적 위협으로부터 브랜드를 보호합니다.

- 브랜드 어뷰징 사이트 탐지
- 기업 사칭 및 피싱 사이트 탐지
- 비정상적 모바일 앱 탐지
- 브랜드 악용 사이트/앱 테이크다운(Take down)

Active Threat and Vulnerability Management

다양한 외부 위협에 대한 유의미한 대응책을 신속하게 제공합니다.

- 다크웹에서 활동 중인 랜섬웨어 모니터링
- 취약점/IoC/Detection Rules
- Attack Surface Monitoring
- 위협 그룹 및 악성코드 관련 인텔리전스

Data Breach Detection

기업 핵심 자산정보 유출 여부를 실시간으로 탐지합니다.

- 기업 민감 정보 유출 탐지
- 재무 관련 정보 유출 탐지
- 개인정보 유출 탐지

Quaxar 주요 서비스

RFI (Request for Information) Report Support

특정 주제 (악성코드, 공격그룹, 암호화폐 등) 관련 고객 분석 요청에 대한 보고서를 신속하게 제공합니다.

Incident Response

침해사고 발생시 사고 조사를 지원합니다.

Take-down Service

고객사에 악의적인 컨텐츠 및 사이트 (도메인 등)에 대한 삭제 / (합법적인) 차단 작업을 진행합니다.

차별화된 기술력이 고객 만족도의 차이를 가져옵니다.

모니터링 커버리지

고객사 A

아직 활성화 되지 않은 피싱 사이트의 도메인 정보를 제공받고 있어요.

처음 받아보는 종류의 정보이고, 사고 예방 효과가 높아요.

진출한 적 없는 외국 앱스토어에서 피싱 앱 탐지 정보를 받았어요.

덕분에 브랜드 보호를 위해 필요한 조치를 취할 수 있었어요.

분석 역량

고객사 B

방대한 TI 데이터속에서 정확한 정보를 신속하게 알려줘요.

S2W는 상황과 대상에 맞춰 실효성 높은 고급 정보를 적시에 제공해줘요.

주요 위협 그룹 및 악성코드에 대한 풍부한 IoC 데이터를 보유하고 있어요.

또, 전담 분석가를 통해 신속한 추가 분석이 가능해요. 그리고 보고서의 수준이 아주 좋아요.

인텔리전스 실효성

고객사 C

S2W의 유출 계정 데이터 정확도는 75~100%로 타사 대비 현저히 높아요.

기존에 이용하던 타사 보안 서비스의 정확도는 20% 미만의 수준이었어요. 양/질적으로 차이가 굉장히 커요.

신속하고 압도적인 내부 주요 자산 및 계정 정보 유출 탐지량과 정확도를 갖췄어요.

유출 원인에 대한 S2W의 정확한 분석 덕분에 대응이 한결 수월해졌어요.

Beyond Security, Quaxar

Beyond Security

기업의 핵심 자산 보호를 넘어 지속적인 성장을 위한 비지니스 의사 결정에 도움을 줍니다.

Tailored Intelligence

기업의 최적화된 운영 환경을 위해 세밀하게 고안된 맞춤형 인텔리전스를 제공합니다.

Reframing Threat Response Process

위협 대응 프로세스에 Quaxar를 접목해 보다 신속하고 효과적인 위협 대응이 가능합니다.

S2W와 솔루션에 대해 더 알고 싶으신가요?

S2W의 문은 언제나 열려있습니다, 아래의 메일 주소로 문의주세요.

info@s2w.inc

www.s2w.inc
경기도 성남시 분당구 판교역로 192번길 12, 판교미래에셋센터 3층 | +82 07 5066 5277

랜섬웨어 대응을 위한 데이터 보호 전략

베리타스 천대영 이사

VERITAS

랜섬웨어 대응을 위한 검증된 데이터 보호 전략

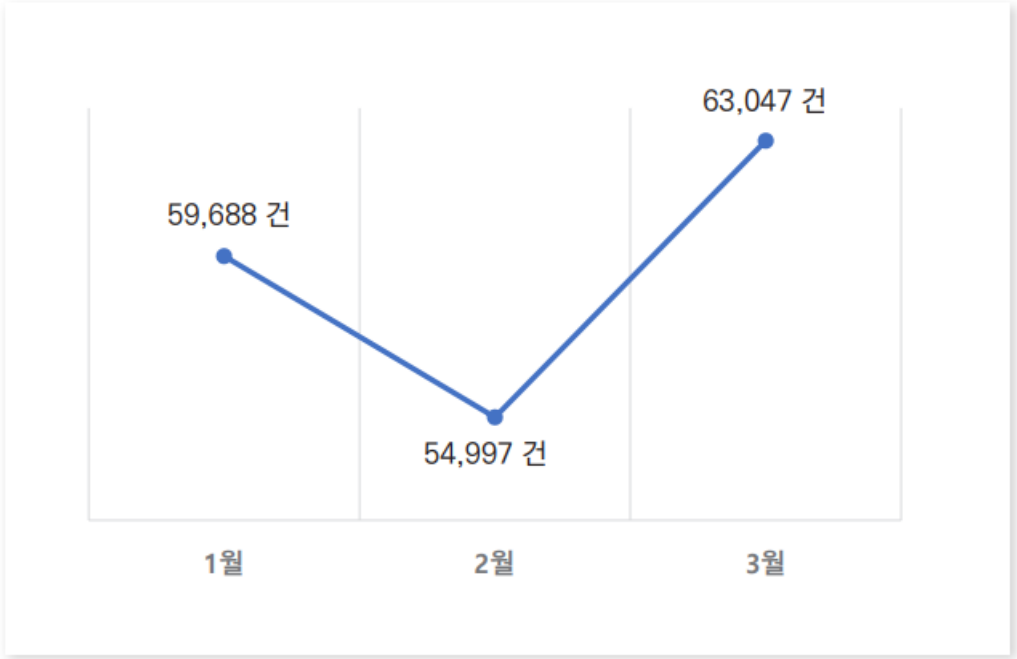
COMPREHENSIVE,
MULTI-LAYERED RANSOMWARE RESILIENCY

Veritas Korea

VERITAS

랜섬웨어 관련 국내/외 동향 및 대응

2022년 1분기 랜섬웨어 동향 보고서 – 한국인터넷진흥원



2022년 1분기 국내 랜섬웨어 탐지 건수 (이스트시큐리티)

미국 FBI, 지방 정부 대상 랜섬웨어 공격에 대한 권고사항

- 모든 운영 시스템과 소프트웨어에 대한 주기적인 업데이트
- 사용자 교육과 피싱 훈련 수행
- 모든 계정에 대한 강력한 비밀번호 설정
- 다단계 인증 사용(Multi-Factor Authentication)
- 오프라인 백업 생성
- 모든 백업 데이터 암호화
- RDP 또는 잠재적 위험성이 있는 서비스 사용 시 엄격한 모니터링 수행
- Linux 사용시 Linux용 보안 모듈 사용
- 네트워크 모니터링 도구를 사용하여 랜섬웨어의 비정상적인 동작에 대한 식별, 탐지, 조사

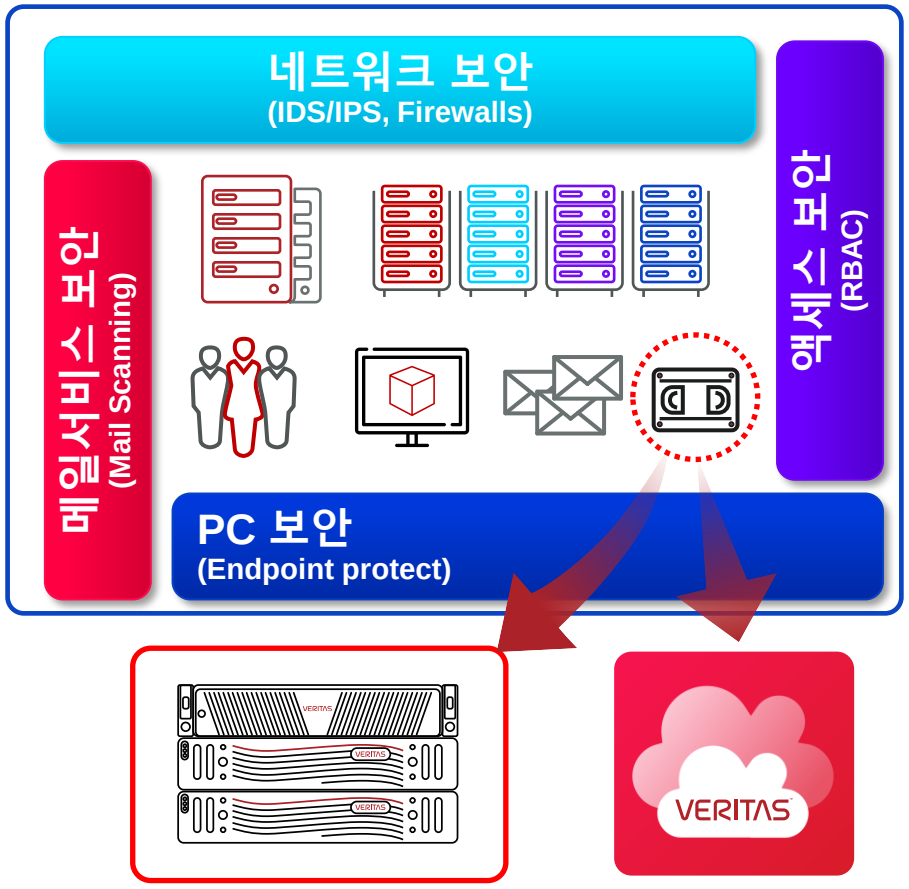
VERITAS

기존 운영환경에서의 보안 솔루션으로 랜섬웨어 공격을 100% 차단하는 것은 어려울 수 있습니다.

운영 환경과 격리된 별도의 보안된 백업 정책 필요

백업은 최후의 보루이며, 모든 재해상황에서 데이터 복구가 가능하도록 운영되어야만 합니다.

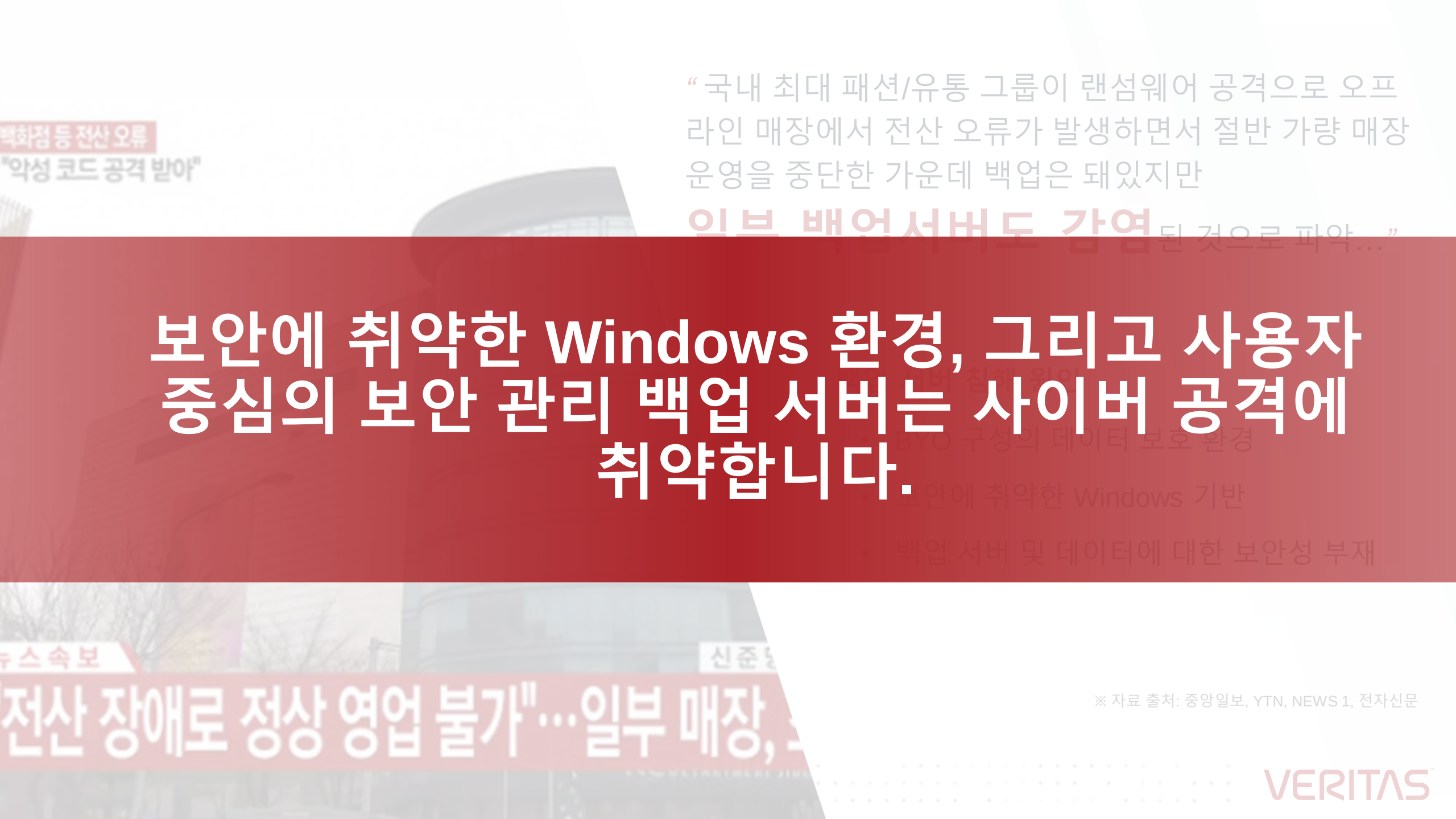
통합된 보안 정책



분리된 별도의
보안 정책

보안된 위치로의
Air-Gap

- **모든 조직에는 Hole이 있습니다.**
  - 해커들은 다양한 방법으로 조직의 보안 레이어를 공격하고, 모든 유형의 공격을 100% 차단하는 것은 사실상 불가능에 가깝습니다.
  - 모든 인프라는 공통된 보안 정책으로 운영이 되고 관리되므로, 피해 발생시 대규모로 피해규모가 확산될 수 밖에 업습니다.
- **백업은 최후의 보루입니다.**
  - 모든 보안이 무력화 되고, 대규모 재해 상황 발생시 마지막 수단은 백업으로부터 복구하는 것입니다.
  - 모든 가능성을 고려한 데이터 보호 정책이 필요합니다.
- **완전히 분리된 제 3자의 입장에서의 보안 정책이 필요합니다.**
  - 기존 사내 보안 정책과 다른 솔루션과 관점에서의 접근 전략이 필요합니다.
  - 보안 전문업체를 통한 중복 관제는 많은 비용을 필요로하고, 기존 보안 정책과 충돌하거나 중복 투자가 발생될 수 있습니다.
  - 사내에서 서로 다른 2가지 이상의 보안 정책을 자체 운영하는 것은 불가능에 가깝고, 많은 비용과 추가 인력을 필요로 합니다.



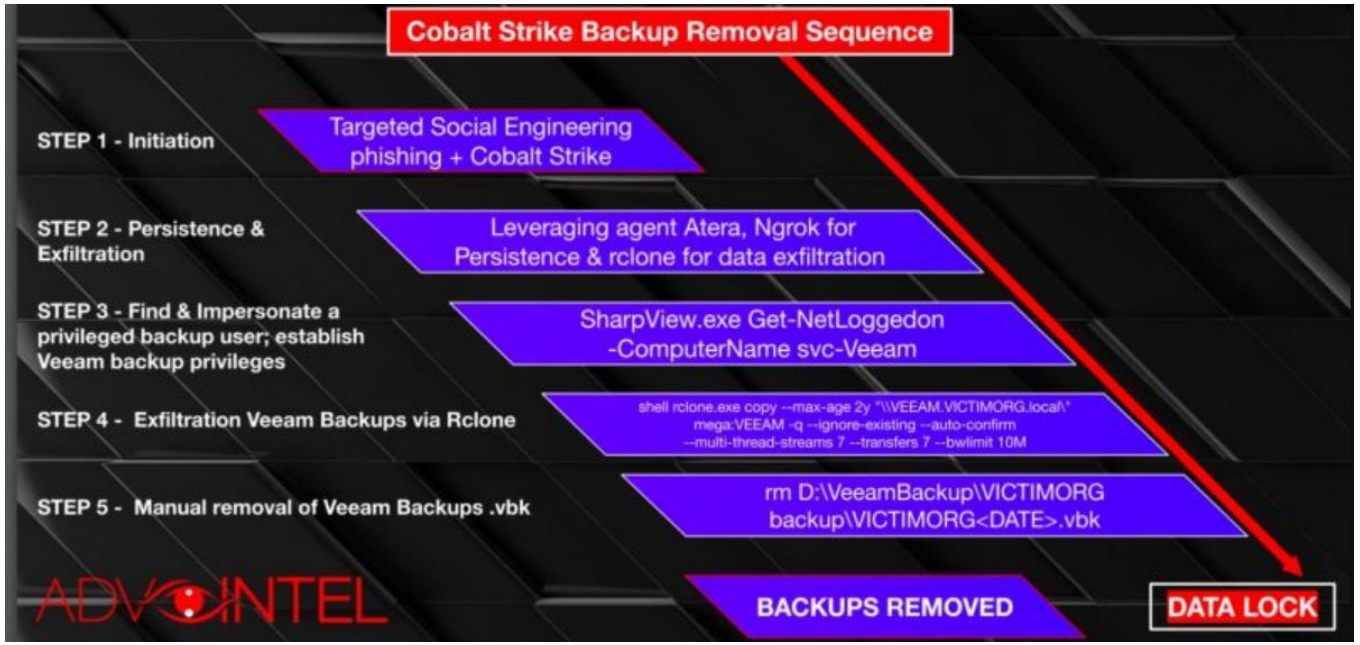
보안에 취약한 Windows 환경, 그리고 사용자 중심의 보안 관리 백업 서버는 사이버 공격에 취약합니다.

※ 자료 출처: 중앙일보, YTN, NEWS 1, 전자신문

VERITAS

Veeam을 target으로 하는 Conti Ransomware

신종 랜섬웨어 공격 형태는 **VTL/PTL의 내용까지도 모두 삭제할 수 있습니다.**



※ 출처: https://threatpost.com/conti-ransomware-backups/175114/

이슈 탈취한 AD 계정을 이용하여 백업 환경에 **정상적으로 Log-In 및 백업 데이터 삭제**

위험 잠재적으로 **모든 BYO 환경**은 **동일 위협에 직면**할 수 있음

대안 기존 보안 정책과 분리된 별도의 보안된 백업 인프라 운영 및 2단계 인증

Veritas NetBackup Appliance는 **완벽한 독립형 보안 솔루션 탑재** 및 **2단계 인증**을 통하여 Conti Ransomware 뿐만 아니라 **새로운 패턴의 공격 시도를 모두 차단**할 수 있습니다.

미국 IT서비스 업체 코그니전트, 랜섬웨어로 인한 손실 최대 7,000만 달러

"미국 IT서비스 업체 코그니전트(Cognizant)가 4월 '메이즈(Maze)' 랜섬웨어 공격으로 5,000만 달러에서 최대 7,000만 달러 사이의 손실을 예상하고 있다."

- IT World, 2020.05.12

- 지난 4월 코그니전트 인도 **데이터센터에 대규모 랜섬웨어 공격**
- **NetBackup(SW) + VTL로 Mix된 환경이며, 대규모 데이터센터(본사+DR센터)로 운영**
  - NetBackup Appliance 미사용
- **NBU Appliance 미사용으로 인한 랜섬웨어 피해 발생**
  - NetBackup BYO 서버 피해발생
  - 피해 복구에 상당한 시간 소요
- 피해 발생 이후 외부 보안업체를 통한 컨설팅 진행
  - 백업, 보안관제 및 방어, Compliance가 통합된 관리 체계 필요
  - 백업은 **NetBackup Appliance로 전량 교체 결정**
    (NBU Appliance 19대, Flex 5340 Appliance 29대 도입 결정)

대규모 데이터센터의 보안장벽도 해커의 APT 공격에는 무용지물입니다.

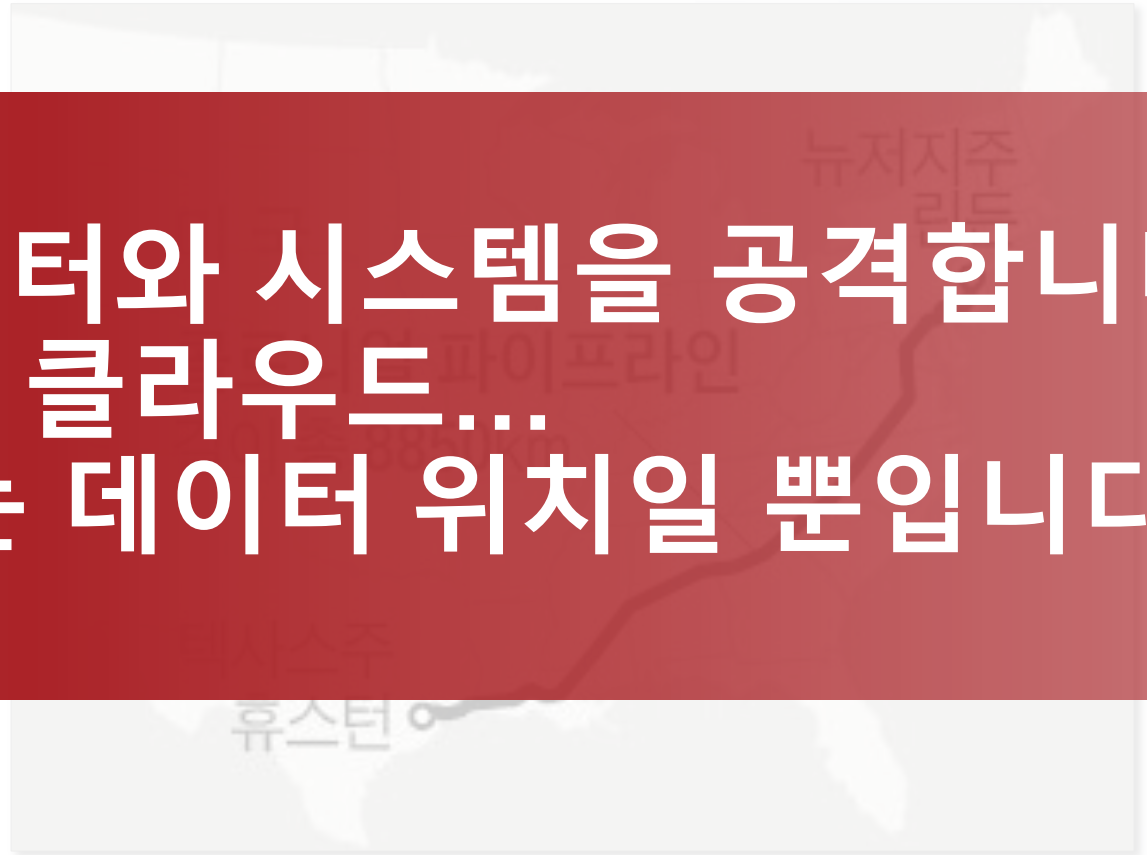
"랜섬웨어 공격을 받고 싶어하는 사람은 없습니다. 우리 [illegible] 그것도 그것을 완벽하게 [illegible] 않지만 대안은 당신이 [illegible] 그리고 우리는 그것을 [illegible] 노력했습니다."

- Cognizant CEO, Brian Humphries

- 전세계 270개 이상의 사무실 및 디자털 허브
- Fortune 500대 기업 중 194위
- 직원 수 : 약 30만명(2020년 중반)
- 년 매출 : $16.13 billion, 2019

미국 최대 송유관 랜섬웨어 공격 사건

영화 “다이하드 4.0 – Fire Sale”, 현실로…



해커는 모든 위치의 데이터와 시스템을 공격합니다.
폐쇄망과 클라우드…
그것은 그저 해커에게는 데이터 위치일 뿐입니다.

다음 타겟은 누구일까요?

랜섬웨어에 대해 알아야 할 5가지 중요 사항

1 공격의 진화

랜섬웨어 공격자는 지속적으로 전술을 바꿉니다.

2 낮은 신뢰도

해커에게 몸값을 지불한다고 해도 항상 데이터를 찾지 못합니다.

3 개인보다 기업

랜섬웨어는 개인보다 기업을 더 많이 공격합니다.

4 시스템이 표적

랜섬웨어는 데이터가 아닌 시스템을 목표로 합니다.

5 데이터의 위치

랜섬웨어는 데이터가 있는 모든 곳을 공격할 수 있습니다.

VERITAS

사이버 재해상황 대응을 위한 요건 – 데이터 보호 측면

백업 데이터 보호

- 원본과 다른 형식으로 보관
- 데이터 사본(시점)간 격리
- 사용자 액세스 제어 및 탐지/차단
- 백업 데이터 암호화
- 데이터 전송 및 미전송 상태 암호화
- 정합성 유지를 위한 검증 및 치유
- 위치 제약 및 종속성 없는 복제
- 2차 사본 유지 및 Air-Gap 환경 보관
- 위/변조 방지를 위한 WORM 또는 오프라인 보관
- OpenSource 및 3rd-party 기술 최소화

신속한 복구

- 백업 데이터 보호
- 카탈로그 및 메타데이터 보호
- 복구를 위한 보안된 환경 유지
  - 백업 소프트웨어 구성 변경 탐지/차단
  - 운영체제 구성 변경 탐지/차단
  - Whitelist 기반의 해킹시도 및 멀웨어 공격 탐지/차단
  - 취약점을 이용한 제로데이 공격 또는 익스플로잇 공격 차단 및 완화
- 하드웨어 안정성 확보를 위한 DR 유지
- 모든 위치에서 즉각적 복구 상태 유지
- 정기적인 복구 테스트 수행

VERITAS

많은 전문가들은 일관되게 보안된 백업은 필수라고 이야기합니다.

RANSOMWARE FREE

Enterprise Data Service Platform – Ransomware Resiliency

포괄적인 다계층 랜섬웨어 복원력

Protect

변조 불가능 모드(Immutability)
BYO, Appliance, Cloud, SaaS

제로 트러스트 기반의
임의 삭제 차단

Attack Surface 감소
(공격 받을 수 있는 범위 감소)

30+이상의 경험 기반
w/ 보안 엔지니어링 제품

16년 연속 Gartner Leadership

Detect

완전한 인프라 및 데이터 가시성
Edge to Core to Cloud

단일 제품 = 100% 가시성

실시간에 가까운
AI 기반 이상징후 탐지
및 악성코드 스캐닝

Recover

유연하고 신속한 복구
모든 규모의 환경과 모든 장애 규모에 대해 위치 제약 없이

객체 단위부터 전체 DC에 이르는 복구

재해 복구 리허설
비용 효율적인 무중단 기반

클라우드 효율성

VERITAS

RANSOMWARE FREE

랜섬웨어 완벽 대응 보안 백업 솔루션

보안된 백업만이 랜섬웨어에 완벽하게 대응할 수 있는 유일한 방법입니다.

- **침입 차단(IPS) 및 탐지(IDS) 기능** 기본 탑재
  - 랜섬웨어가 시스템에서 데이터를 삭제하거나 실행되는 것을 차단(랜섬웨어 실행파일 차단)
  - 해킹시도 원천적 차단
- 보안 위험 요소 탐지 및 예방 기능 제공

black hat USA

PASSED

* NetBackup 어플라이언스는 17,000번 이상의 해킹 시도를 모두 막아내 보안성을 입증하였습니다. –Black Hat USA

VERITAS

RANSOMWARE FREE

보안 요소별 제공 범위

데이터 보호 솔루션 제공 업체는 사용자 관점이 아닌 제품 관점에서의 보안 요소만을 제공합니다.

- 포인트 이슈에 대응하기 위한 과거의 데이터 보호 방법론은 최근 랜섬웨어와 같은 대규모 재해 상황 대응 중심으로 변화하고 있으며, 사이버 재해상황에서는 강력한 보안 백업만이 데이터를 보호할 수 있는 유일한 방안
- 사이버 침해사고는 기업의 존폐가 결정될 정도로 심각한 수준의 재해 상황이며, 대규모로 진행됨.

BYO
(사용자 중심)

낮은 보안 수준
(사용자 책임 높음)

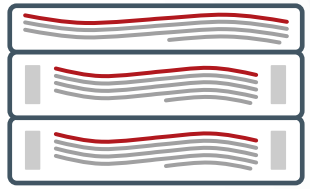
사용자
(미제공)

SW
기능

- 보안 강화된 OS
- NIST 표준 및 지침 준수
- STIG Guide에 기반한 하드닝
- IPS/IDS 기능 기본 탑재
- 2단계 인증 및 접근 제어
- 역할기반 사용자 액세스 제어
- 중복제거 저장소 암호화

자체 제공
(통합)

Appliance
(제조사 중심)



높은 보안 수준
(사용자 책임 최소화)

VERITAS

RANSOMWARE FREE

NetBackup Appliances 보안정책

NetBackup Appliance에 탑재된 IPS는 White-list 기반 정책으로써 패턴 업데이트가 필요하지 않습니다.

Intrusion Prevention

실시간 선제 대응

- 해킹 시도 차단 및 멀웨어 방지
- OS 강화(하드닝)
- 어플리케이션 제어
- 권한 없는 사용자 액세스 제어
- 취약성 및 패치 완화 (제로데이 공격 방어)

Intrusion Detection

실시간 모니터링 및 감사

- 호스트 침입 감지
- 파일 무결성 모니터링
- 환경구성 모니터링
- 사용자 액세스 추적 및 모니터링
- 로깅 및 이벤트 리포팅

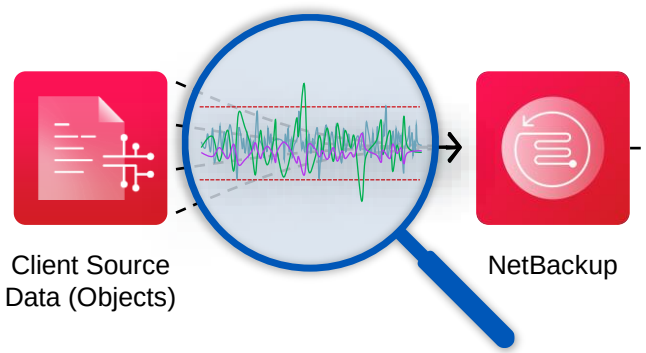
VERITAS

RANSOMWARE FREE

이상징후 탐지(Anomaly Detection) 및 멀웨어 검사

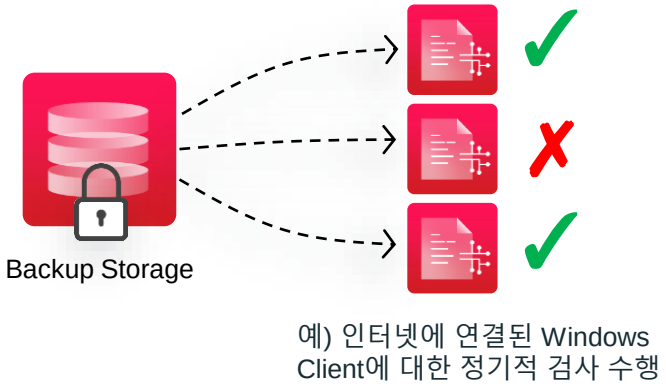
NetBackup 10에는 NetBackup 9.1에 도입된 AI 기반의 이상징후 탐지 기능과 함께 작동하는 새로운 자동화된 멀웨어 검사 기능이 포함되어 있습니다.

백업중



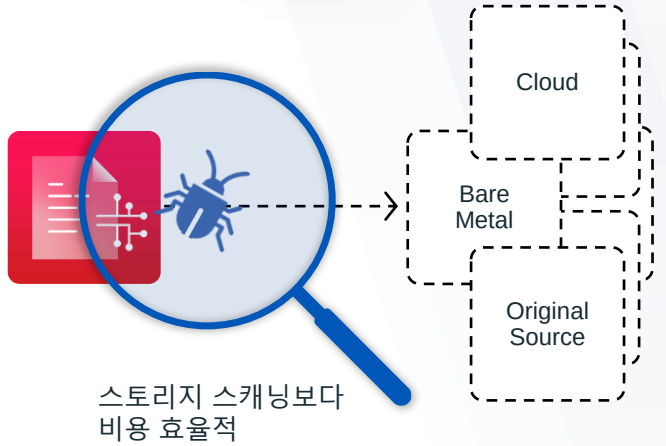
AI 이상징후 탐지
실시간에 가깝게…

백업후



자동화된 멀웨어 검사
이상징후 탐지 기반

복원전



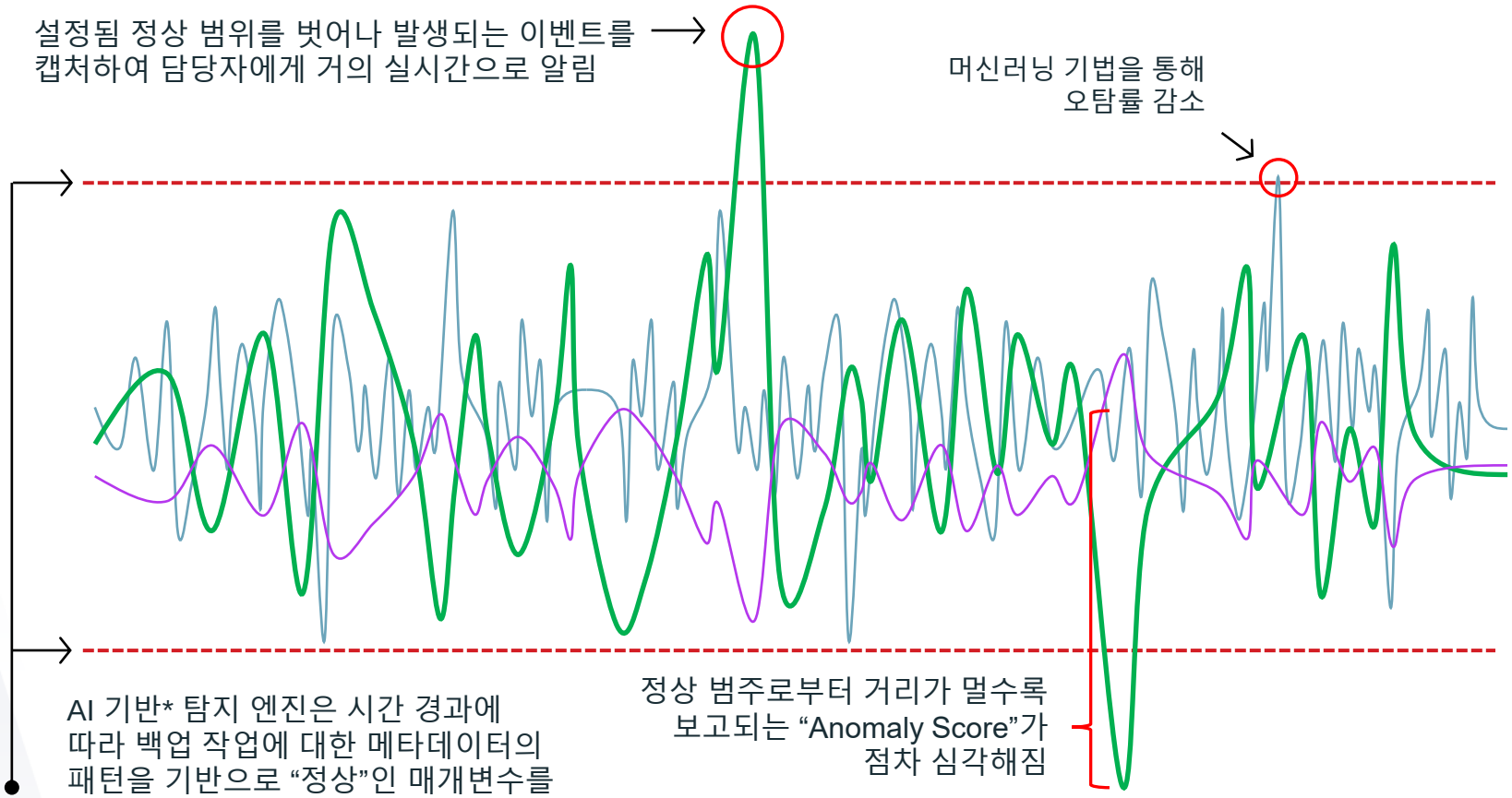
복원시 Scan을 통해
상태를 인식
데이터의 무결성 보장

VERITAS

RANSOMWARE FREE

이상징후 탐지(Anomaly Detection) 기법

AI 기반의 머신런닝 기법을 통해 이상징후를 탐지하고 자동으로 리포팅합니다.



NetBackup의 AI 기반 이상징후 탐지 엔진

- 방대한 양의 데이터 마이닝
- 모니터링 및 리포팅 자동화
- 실행 가능한 통찰력 확보
- 여러 기준에 따른 보고
- 공격에 대한 조기 경보 설정

* 머신런닝(ML) 모델은 nbdeployutil을 사용하여 데이터 pre-seeding를 활용하고, AI는 DBSCAN 알고리즘으로 구동됨.

VERITAS

WORM 스토리지 기능 지원 – Immutable Storage

5250/5350 Appliance 하드웨어 기반에서 제공되며, Flex S/W 플랫폼으로 구성되어야 합니다.

변조 불가능 스토리지 모드 지원

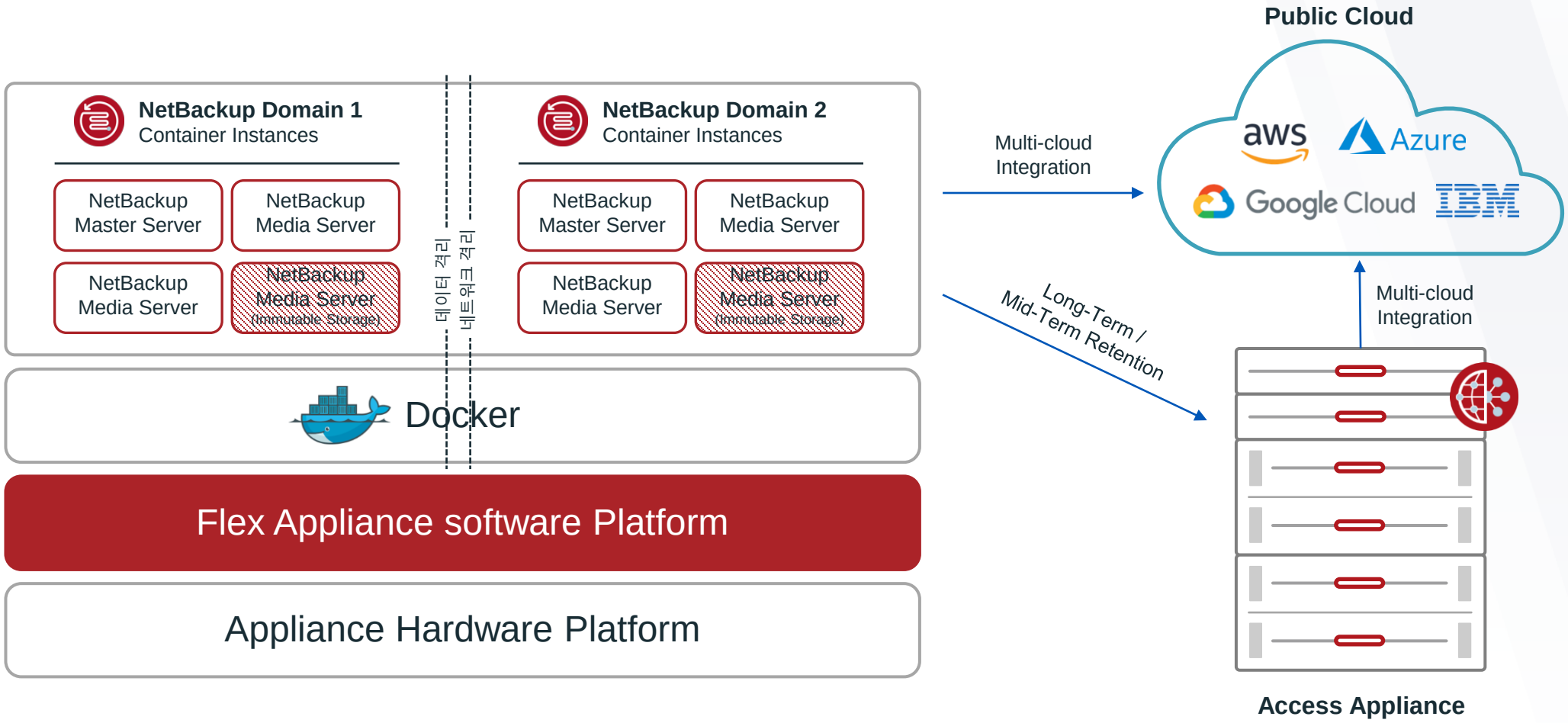
- NetBackup Flex Appliance
- OS 시간과 무관한 자체 Compliance Clock을 통해 불변 기간 설정
- 2가지 WORM 기능 제공
  - Compliance: WORM 보존 기간 동안 삭제 불가능
  - Enterprise: WORM 보존 기간 중 삭제 가능

지원 환경

- NetBackup v8.3 이상
- Flex Appliance
  - Flex S/W v2.0 이상
  - Flex 5250/5350 Appliance H/W에서 제공
  - 중복제거 저장볼륨에 대해서 WORM 설정 가능

Flex Appliance high-level architecture

Flex Appliance는 여러 NBU 호스트를 운영할 수 있으며, WORM 기능을 추가적으로 제공합니다.



VERITAS

장기보존 데이터에 대한 멀티 스토리지 옵션

NetBackup Appliance
빠른 복구, 온프레미스 30~90일

프라이빗 클라우드 선호 고객

As-a-service 선호 고객

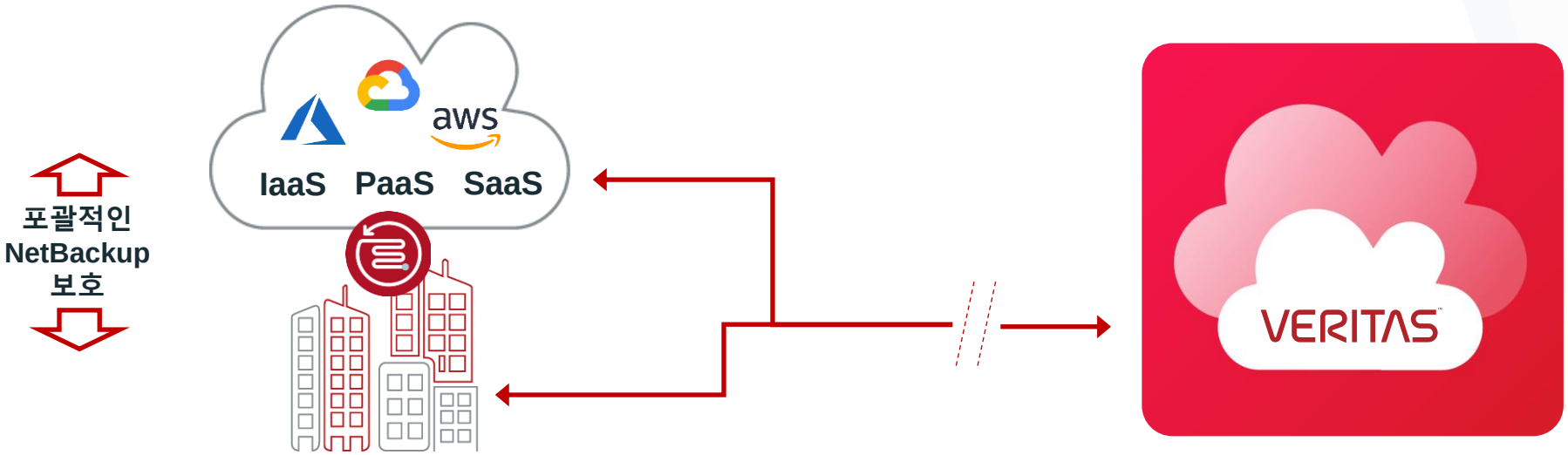
Long-Term Retention

Access Appliance
고객 관리
경제적인 LTR

NetBackup Recovery Vault
Storage-as-a-service
Subscription
Air-Gap
무제한 규모
Veritas의 클라우드 경험

NetBackup Recovery Vault

모든 워크로드 데이터 격리(Air-Gap)를 위한 클라우드 기반 Storage-as-a-Service를 제공합니다.



온프레미스 DC 또는 클라우드 테넌트

- NetBackup 내에서 안전하게 프로비저닝
  - RBAC 인증
  - Subscription 기반
  - 소비량 리포팅
- 자동화된 회복력

NetBackup Recovery Vault

- Air-Gap 랜섬웨어 보호
- 클라우드 또는 데이터 센터로 복구
- 무제한 규모
- 예측 가능한 비용
- Azure, AWS S3

참고: 스토리지 소비량 또는 데이터 작업에 대한 초과분이 측정되는 경우 추가적인 월별 청구가 적용될 수 있습니다.

일반백업과 보안백업을
모두 제공하는 제품은
NetBackup Appliance가 유일합니다.

랜섬웨어보험 국내외 운영사례 공유

캐롯손해보험 김우석 매니저

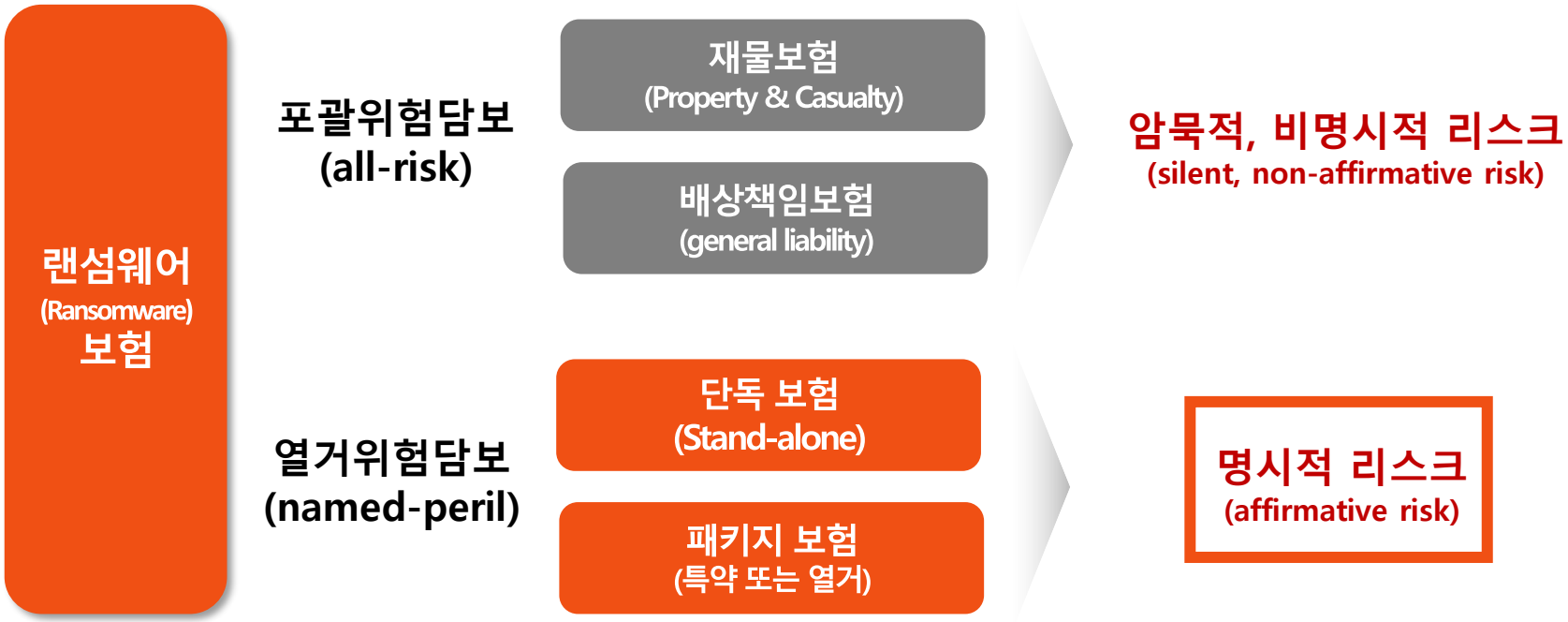
Carrot

랜섬웨어 보험 국내외 운영사례 공유

Content

01 랜섬웨어보험 상품 구분

- 랜섬웨어 위험을 보장하는 보험은 담보 방식에 따라 아래와 같이 구분
- 사이버 보험 시장이 가장 활성화된 미국의 경우, 명시적 리스크 보험이 활성화되어 있음



- 사이버 보험 담보의 경우 아래와 같은 내용을 담보 가능
- 랜섬웨어 보험의 주 목적인 '사이버 협박'이외에, 실질적으로 보상할 수 있는 상품 구성 필요

당사자		제3자
직접손실	비용	
• 금융 도난 및 사기 • 지적재산 도난 • 영업중단손해 • 사이버협박 • 평판손실 • 물적 자산 손실	• 법률비용 • 계약상 벌과금 • IT 포렌식 • 통지 • 데이터 및 소프트웨어 손실 • 평판손실 관리 • 물적 자산 손실로 인한 비용	• 데이터침해 배상책임 • 금융 도난 및 사기 배상책임 • 네트워크 서비스 실패 배상책임 • 지적재산 도난 배상책임 • 인격권 침해 배상책임 • D&O 배상책임 • 일반자산손실 배상책임

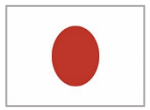
자료: Wrede, D., Stegen, T., and Johann-Matthias Graf von der Schulenburg(2020), "Affirmative and Silent Cyber Coverage in Traditional Insurance Policies: Qualitative Content Analysis of Selected Insurance Products from the German Insurance Market", *The Geneva Papers on Risk and Insurance-Issues and Practice*, 45, pp. 657~689

03 국내외 보험 운영 쟁점 – 담보 정의의 불확실성

- **랜섬웨어 피해를 명시적 리스크로 담보하더라도, 약관 해석에 따라 논쟁이 있음.**
- **국내의 경우 개인정보유출 및 제3자 배상으로 담보가 한정된 경우가 대부분으로, '보장 공백'이 존재**

■ 2017년 워너크라이 랜섬웨어 사건 : 보험 가입 기업이 보안 취약성 문제에 대한 대응을 게을리 했다는 보험회사 주장 -> 손해배상 담보에 대한 보상 여부에 대한 논의 중.

■ 사이버 보험 관련 보험금 분쟁이 빈번하지 않으나, 해커에게 지급한 비트 코인이 재산권(Property)에 해당한다는 판결이 있음.



■ 21년부터 4개 대형손해보험사에서 기존의 전통적인 '배상책임보험'에서 '사이버손해배상' 특약을 신설했으나, 배상책임만 담보한다는 데 있어 한계가 있음.

■ 2017년 가상화폐거래소 랜섬웨어 피해 사건 : 피해 기업에서 각기 다른 두 손해보험사의 사이버종합보험, 개인정보유출 배상책임보험에 각각 30억원 한도의 보험을 가입했으나 재산(Property) 담보 미가입으로 피해 보상을 받지 못함.

- **일반적으로 대부분의 보험에서 '테러 및 전쟁 행위'은 면책 조항을 두어 보상하지 않음.**
- **랜섬웨어와 같은 사이버 위협을 테러 혹은 전쟁 행위로 보느냐에 대한 논의가 세계적으로 진행 중**

■ 2017년 낫페트야 사건 : 해당 사건의 배후가 러시아 정부 차원의 공격 행위로 발표하자, 보험회사에서 약관에 규정된 전쟁 면책 적용을 주장하며 보험금 지급 거절.

- 식품 대기업 몬델레즈(Mondelez) : 보험사 'Zurich Insurance'를 상대로 1억 달러 소송 진행 중이며, 법원 계류 중.
- 제약회사 머크(Merck & Co) : 보험사 'Ace America'를 상대로 한 소송 결과, 해당 사건의 경우 물리적 전쟁이 아니었으므로, 전쟁행위로 보기 어렵다는 뉴저지 법원의 판결로 승소함.

■ 영국 대표 보험사 로이드는 지난 21년 11월 국가 단위 사이버 전쟁과 작전은 사이버 보험 보장 범위에서 제외한다는 새로운 약관을 발표.

■호주 재무부에서 운영 중인 테러리즘 전용 재보험 기구에서 랜섬웨어 등 '사이버 위협'에 대하여 재보험 담보 및 지급 보증 제공을 검토했으나, 랜섬웨어 비용을 정부에서 지불하는 것에 대한 논의 진행 중.

■ 다국적 보험사 악사(AXA)는 프랑스의 사이버 보험 정책에 따라 프랑스 내 랜섬웨어 피해 보상 서비스를 중단함. -> 사이버 테러 세력에 강경노선을 펼치는 프랑스 정책에 의한 중단

랜섬웨어 보험 시장에 대한 수요 및 공급은 확대될 전망이지만, 여전한 '보장 공백' 및 논의 사항 존재

차세대 '랜섬웨어 보험'의 개발 필요성

- 피해 기업에게 '실질적인' 보상이 가능한 보험 상품 개발
- 전문가 그룹의 데이터 공유로 '보장 공백' 최소화

References

■ 송윤아 외 1인 공저(2021), 주요국 정부의 사이버보험 공급 지원 동향 및 시사점, KIRI 리포트 포커스, 8p.

■ 송윤아(2021), 사이버사고의 진화와 사이버보험 시장 동향, KIRI 리포트 포커스, 13p.

■ 권진홍 외 1인 공저(2021), 사이버보험의 주요 내용 및 쟁점, BFL 제105호, 39p.

랜섬웨어 사고 관련 법적 쟁점

법무법인 화우 최용호 변호사

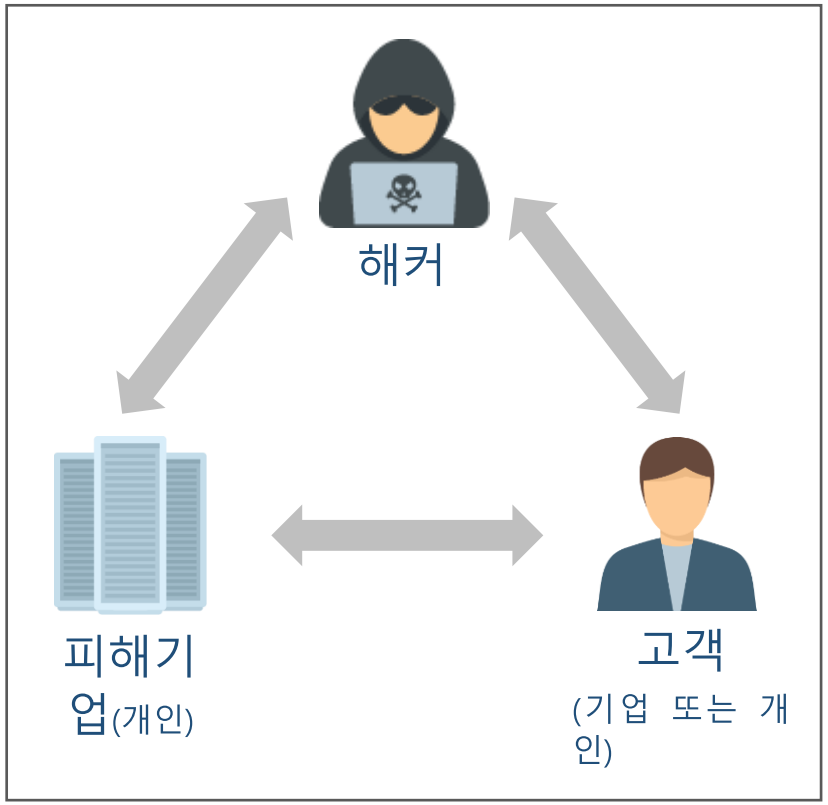
법무법인(유) 화우
YOON & YANG

Contents

I 랜섬웨어 사고 관련 주요 쟁점

법무법인(유) 화우
YOON & YANG

❖ 랜섬웨어 사고 관련 당사자 및 주요 쟁점



- 사고발생시 가장 먼저 무엇을 해야 하나?
- 사고 신고를 해야 하나?
- 몸값을 지불해야 하나?
- 고객(피해)는 어떻게 해야 하나?

Ⅱ 해커와 피해기업 사이의 법률관계

법무법인(유) 화우
YOON &YANG

❖ 형사 관련 쟁점

1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반

제48조(정보통신망 침해행위 등의 금지)

② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실 · 변경 · 위조하거나 그 운용을 방해할 수 있는 프로그램(이하 “악성프로그램”이라 한다)를 전달 또는 유포하여서는 아니된다.

제70조의2(벌칙)

제 48조 제2항을 위반하여 악성프로그램을 전달 또는 유포하는 자는 7년 이하의 징역 또는 7천만원 이하의 벌금에 처한다.

➡ 랜섬웨어 공격은 장치 또는 시스템에서 데이터를 암호화는 것이 기본, 이를 위해서는 암호화를 위해 필요한 악성 프로그램이 장치나 시스템에 탑재되어야 함

❖ 형사 관련 쟁점

2. 형법상 업무방해죄

제314조(업무방해)

② 컴퓨터등 정보처리장치 또는 전자기록등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자도 제1항의 형(5년 이하의 징역 또는 1천 500만원 이하의 벌금)과 같다.

➡ 암호화로 인해 전자기록 자체가 멸실되는 것은 아니지만 접근 불가능하게 변경훼손되어 정보처리에 장애가 발생하여 손괴*에 해당

* '손괴'란 물질적인 파괴행위로 인하여 물건을 본래의 목적에 공할 수 없는 상태로 만드는 경우뿐만 아니라 일시적으로 그 물건의 구체적 역할을 할 수 없는 상태로 만드는 것도 효용을 해하는 경우에 해당

❖ 형사 관련 쟁점

3. 형법상 공갈죄

제350조(공갈)

① 사람을 공갈하여 재물의 교부를 받거나 재산상의 이익을 취득한자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

➡ 몸값으로 요구하는 비트코인은 재물에 해당(2018도3619 판결)

➡ 타인의 정보를 볼모로 삼고, 해당 정보를 사용할 수 없도록 하는 것은 재물의 교부에 응하지 아니한 때에는 부당한 불이익을 초래할 위험이 있다는 위구심을 야기한 경우로서 공갈(해악의 고지)에 해당(2012도7461 판결 등)

❖ 민사 관련 쟁점

① 몸값 지불 여부에 대한 결정

- 다른 방법으로는 복구 불가능한 중요 파일에 접근해야 하는 경우, 인명 피해가 예상되거나 즉시 운영이 정상화되지 않으면 회사 존립이 위태로워지는 경우 등

② 몸값 지불이 복구를 보장하지는 않음

- 신뢰할 수 없는 상대방인 해커에게 몸값을 주는 것임.
- 대부분의 해커가 몸값이 지불되면 파일을 해독할 수단을 제공하지만, 범자인 상대방(해커)가 몸값을 챙긴 후 약속을 지키지 않을 가능성도 상당함.

③ 몸값 지불이 즉각적인 복구를 의미하지도 않음

- 해독키를 받더라도 해당 해독키를 사용하여 당장 복구할 수 있는 것은 아님. 수작업을 통해 해독을 하여야 하고 개별적으로 해독해야 하는 관계로 복구에 시간이 오래 걸리는 경우가 많음

④ 몸값 지불 자체가 불법에 해당할 수 있음

Ⅲ 피해기업과 고객 사이의 법률관계

법무법인(유) 화우
YOON &YANG

Ⅲ. 피해기업과 고객(기업) 사이의 법률관계

❖ 형사 및 행정 관련 쟁점

- 피해기업과 고객(기업) 사이에 형사적으로 문제가 될 사항은 없음
- 랜섬웨어 공격에 따라 고객(기업)이 보유하고 있는 개인정보가 유출되는 경우에는 개인정보보호법 등에 따른 개인정보 유출 관련 신고 및 고지의무를 이행하여야 하며, 관련 법령에 따라 과징금 등 부과처분의 대상이 될 수 있음

❖ 민사 관련 쟁점

- 서비스 마비 등에 따른 고객(기업)의 피해에 대한 손해배상 의무
- 피해기업이 서버호스킹을 제공하는 경우, 서버호스팅을 이용하는 고객(기업) 뿐만 아니라 해당 고객(기업)의 고객에 대한 손해배상 의무까지 부담하게 될 위험
- 개인정보가 유출되었을 경우에는 집단소송 등의 위험성 있음

Ⅳ 결론

Ⅳ. 결론

랜섬웨어 공격의 피해자가 되지 않도록 적절한 예방조치(접근권한 제어, 잠재적 악성코드 노출 모니터링 등)를 취하고, 랜섬웨어 공격에 대해 적정한 복구 계획을 수립할 필요

향후 랜섬웨어 공격에 따라 고객(기업)에게 금전적 손해가 발생하게 되더라도, 선제적인 예방조치를 통해 소송리스크를 최소화할 필요

정확한 로그 분석 등 전문가를 통한 초기 대응을 통해 피해를 최소화

랜섬웨어 사고신고 및 개인정보 유출이 확인된 경우에는 관련 신고를 이행

몸값 지불은 지양하되, 부득이 몸값을 지불해야 할 경우에는 전문가의 조력을 받을 필요

About 민간 보안 협의체 ‘KARA’

KARA (Korea Anti-Ransomware Alliance)는 안전한 사이버 환경을 조성하고 랜섬웨어 공격에 대한 체계적인 대응 프로세스를 마련하기 위해 구성된 랜섬웨어 대응 민간 협의체다.
SK쉴더스의 주도로 트렌드마이크로, 지니언스, 맨디언트, S2W, 베리타스, 캐롯손해보험, 법무법인 화우 등 국내 외 각 분야의 전문 기업들이
정기적인 랜섬웨어 최신 트렌드 및 피해 실태와 관련한 정보를 공유하며 사고 접수와 대응, 복구, 대책까지 원스톱으로 대응하는 프로세스를 제공한다.
또한 고도화된 랜섬웨어의 위협에 맞서 정부 기관 및 글로벌 협의체와의 다양한 외부 활동과 공동 세미나 등을 전개하고 있다.