CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

EDR, XDR 및 Attack Surface Risk Management의 상호 보완적 통합 전략

Trend Micro 윤명익 이사

XDR – SOC 요구사항과 Incident 대응

SOC Team Challenges

복잡한 기업 환경과
진화하는 위협

경고의
오버헤드

제한적이고
단편적인
가시성

SOC 요구 사항

Detection and Response

Correlation

Categorization

Analysis

Visibility

IOC’s

Automation

MITRE ATT&CK framework

Incident Response

XDR Coverages

Extended Detection & Response (XDR)

Playbooks

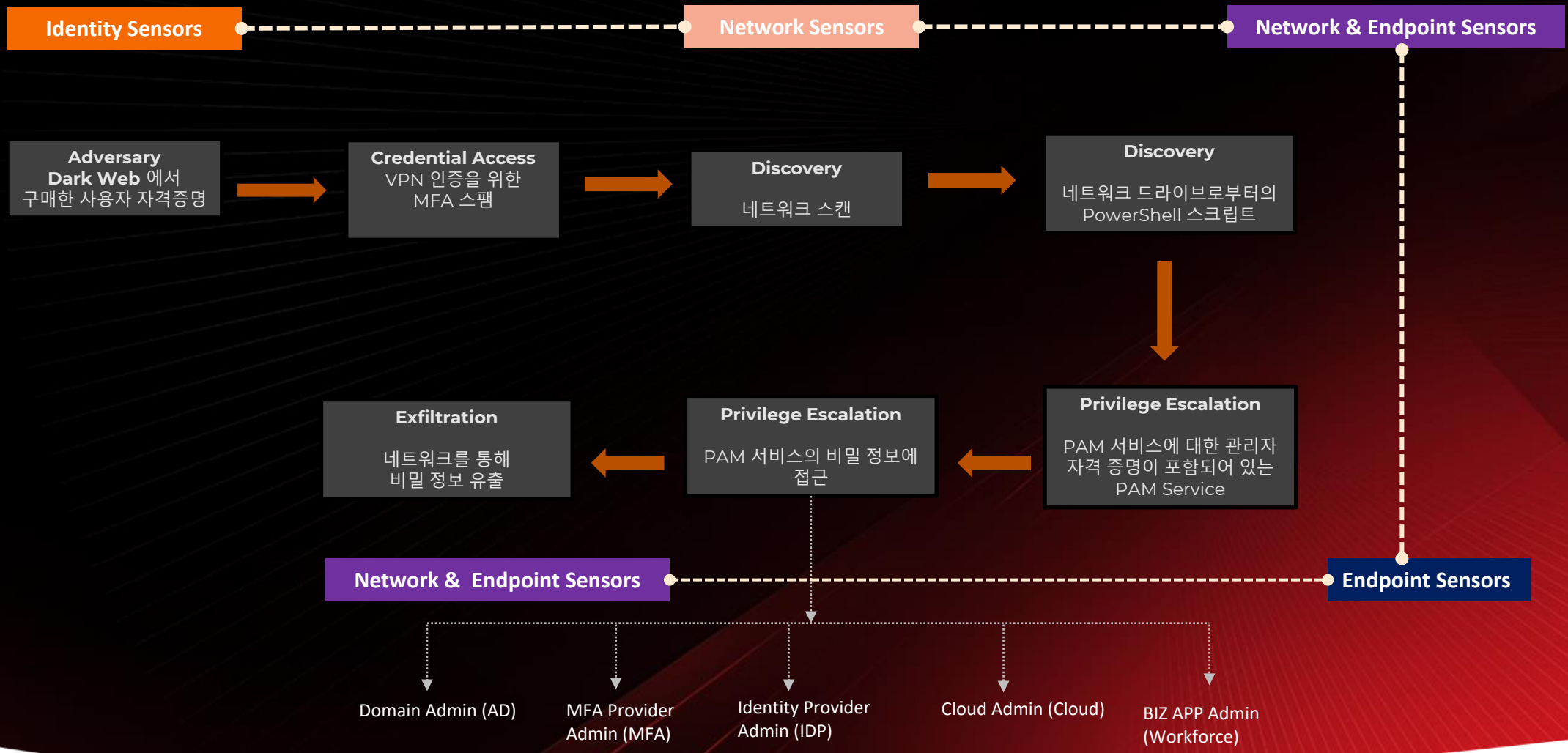
Forensics and Incident Response

Identity | Data | OT/CT | Network | Cloud | Email | Endpoint | 3rd Party

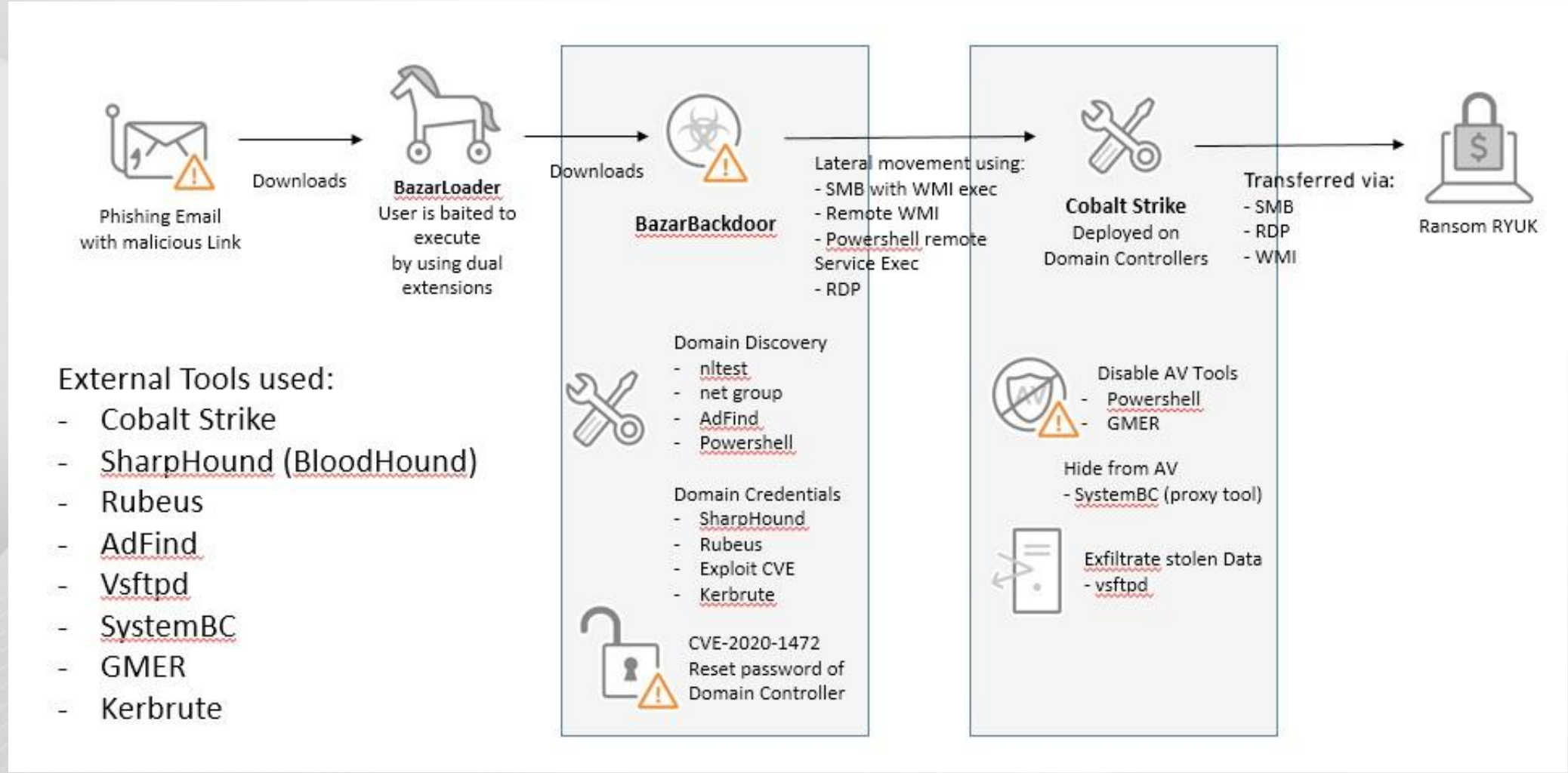
Broadest sensor coverage in the market

Real-Life Use Case : Uber 침해 사고 사례 (2022년 9월)

Mean Time To Detection and Response = Time Sensitive



Ryuk Ransomware Infection Path

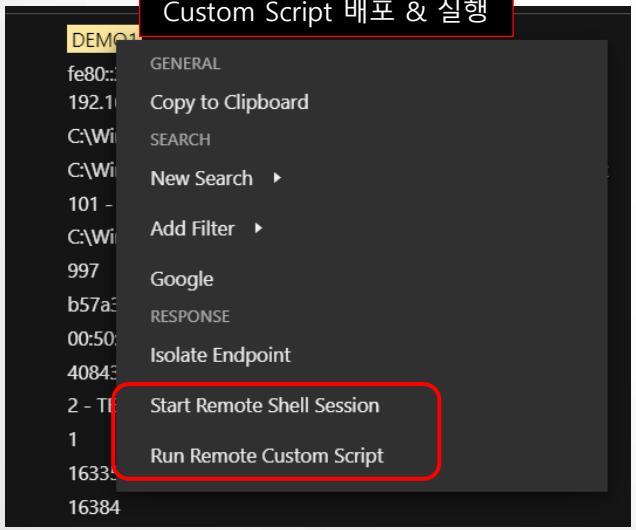


Trend Vision One
Ryuk Ransomware Incident
Detection & Response Demo

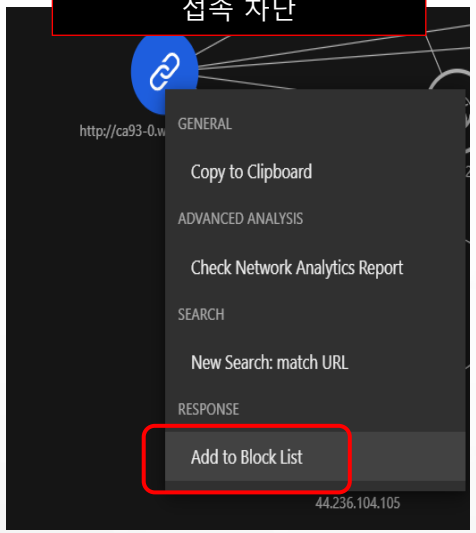
Vision One XDR의 다양한 대응(Response) 기능

파일 실행 차단
파일 수집

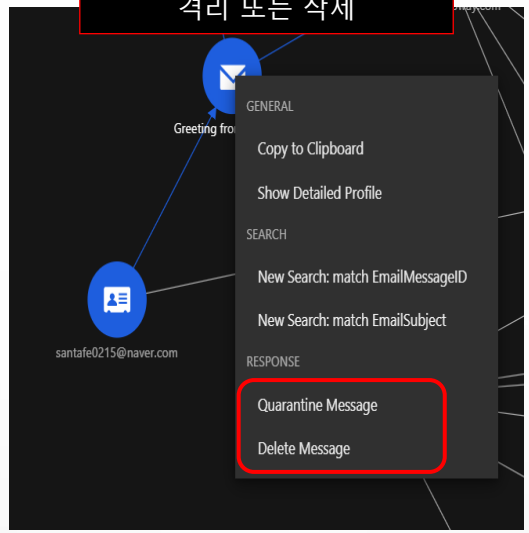
원격셸 접속/
Custom Script 배포 & 실행



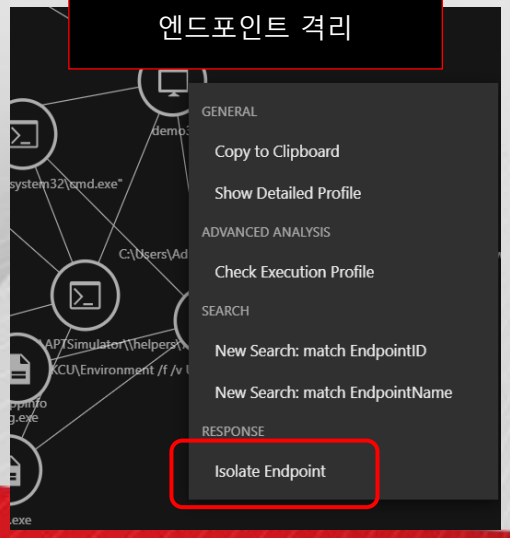
URL 또는 IP주소
접속 차단



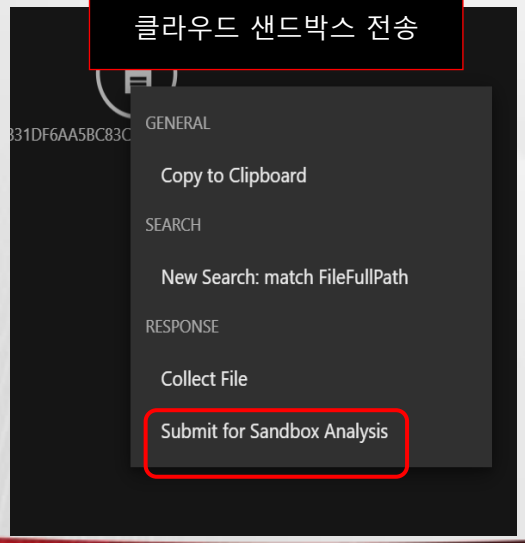
메일 메시지
격리 또는 삭제



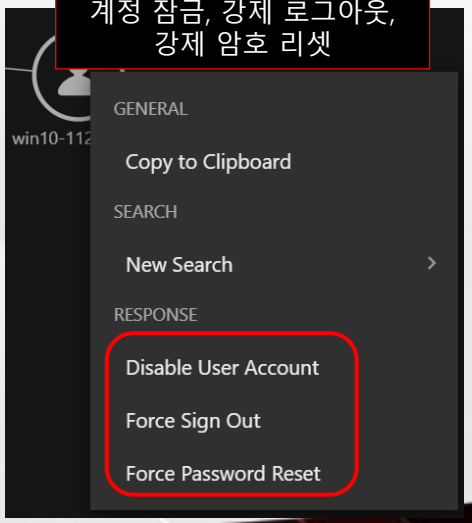
엔드포인트 격리



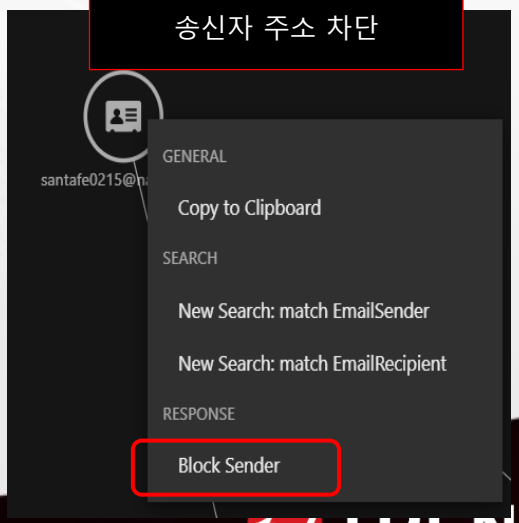
클라우드 샌드박스 전송



계정 잠금, 강제 로그아웃,
강제 암호 리셋



송신자 주소 차단



XDR을 통해 탐지된 Ryuk Ransomware 행위

MITRE ATT&CK® Mapping for Enterprise

App: Observed Attack Techniques | Criteria ⓘ

Go to App | Last 7 days

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact	TA0042 Resource Development	TA0043 Reconnaissance
128	90	5	11405	11407	1895	52	9390	167	0	1060	6	0	0
T1190 127	T1059 38	T1053 2	T1548.002 3801	T1548.002 3801	T1110 858	T1087 8	T1021 4671	T1056 50		T1071 930	T1486 4		
T1133 1	T1203 30	T1053.005 2	T1134 3800	T1134 3800	T1110.001 858	T1018 7	T1021.001 4670	T1056.001 50		T1105 45	T1485 2		
	T1204.002 14	T1133 1	T1134.001 3800	T1134.001 3800	T1056 50	T1087.002 7	T1570 45	T1056.004 50		T1071.003 30			
	T1047 4		T1053 2	T1036 3	T1056.001 50	T1482 7	T1210 2	T1115 11		T1071.001 24			
	T1053 2		T1053.005 2	T1140 1	T1056.004 50	T1016 6	T1021.002 1	T1005 5		T1071.004 19			
	T1053.005 2			T1218 1	T1555.003 29	T1069 6	T1021.006 1	T1560 1		T1571 8			
				T1218.003 1		T1069.002 6				T1095 4			
						T1033							

공격 Demo 스크립트에 포함되지 않았음

XDR과 ASRM 결합의 기대효과


공격 표면 위험 관리 솔루션이 XDR 기술과 통합되면 우리 팀에 많은 가치를 가져올 수 있어요. 예를 들어 공격 표면 위험 관리(ASRM)가 모든 자산에 대한 더 많은 컨텍스트와 가시성을 제공한다면 우리는 많은 시간과 노력을 절약할 수 있을 거에요.
그리고 우리 팀이 이미 작업하고 있는 동일한 여건에서 대응의 우선 순위를 지정하는데 도움을 줄 겁니다. XDR과 공격 표면 위험 관리를 연결할 수 있다면, 우리 조직 환경의 모든 다양한 유형의 위험과 위협에 대해서 포괄적인 단일 가시성을 갖게 될 겁니다.
GREG KRASINSKY
SOC Manager


그것은 우리가 이미 가지고 있는 사일로의 수를 줄일 수도 있어요. 데이터를 수집하는 시스템과 플랫폼이 너무 많아서 무슨 일이 일어나고 있는지 완벽하게 파악하기가 정말 어렵거든요.
RANDALL STEVENS
Chief Information Security Officer


이 두 가지 솔루션을 결합해서 Risk해결 작업을 자동화할 수도 있습니다. 우리는 전반적인 Risk 수준을 효과적으로 측정해야 합니다. 취약성과 잘못된 보안 설정을 찾아내야 하는 거죠.
저도 동의해요. 데이터 사일로를 무너뜨릴 수 있는 기회가 있다고 생각해요. 우리 팀이 대응해야 하는 사건과 Alert를 줄이는 것에도 도움이 될 겁니다. 우리가 SOC에서 매일같이 보는 탐지 정보들도 위험을 평가하는 데 도움이 됩니다.

XDR의 기대 효과

Extended Detection & Response (XDR)

ASRM과 XDR 결합의 기대효과

Attack Surface Risk Management (ASRM)

확장된 가시성

더 나은 Risk 컨텍스트

신속한 완화(Mitigation)

Extended Detection & Response (XDR)

상호 보완하는 ASRM과 XDR

Attack Surface Risk Management (ASRM)

Extended Detection & Response (XDR)

Trend Vision One

Attack Surface Risk Management Demo

예방

대응

ASRM

Attack Surface Risk Management

- Discover
- Assess
- Mitigate

XDR

Extended Detection and Response

- Detect
- Investigate
- Respond

보안 툴에서 통합 사이버 보안 통합플랫폼으로의 전환

Trend Micro One - Unified Cyber Security Platform

EDR, XDR, Attack Surface Management, Zero Trust, Threat intel, Assessment

Prevention

Endpoint
EPP

Detection
Only on
Managed
Devices

EDR

Multi Layers: Endpoint, Network, Cloud Workloads, and E-mail

Cross Threat Detection, Correlation & Response

EDR

XDR

Attack Surface Management

Zero Trust

Security Playbooks

CTI

Mobile Devices

3rd Party Integrations

Next New Requirements

TREND MICRO™ | Global Leader in Cybersecurity

Edward_yoon@trendmicro.com