혼동스러운 EDR, NDR, XDR
마켓 트랜드, 기술적 정의 및 고려사항

[부제 : 위협 탐지/대응 솔루션, 어떻게 사용하면 좋은가?]

PAGO NETWORKS | DeepACT Managed Detection and Response

매니지드 위협 탐지 및 대응 전문기업

SentinelOne CYLANCE STELLAR CYBER

보안시장

위협 탐지 대응

"솔루션 . 플랫폼. 서비스"

탐지 대응 - “솔루션 / 플랫폼 / 서비스” 유형

EDR
Endpoint Detection & Response

엔드포인트 탐지 및 대응 솔루션

NDR
Network Detection & Response

네트워크 탐지 및 대응 솔루션

XDR
eXtended Detection & Response

익스텐디드(확장) 탐지 및 대응 솔루션, 플랫폼

SOAR
Security Orchestration, Automation & Response

보안 운영 자동화 및 대응 솔루션, 플랫폼

MDR
Managed Detection & Response

매니지드 탐지 및 대응 서비스

탐지 대응 - "주요 벤더"

EDR
Endpoint Detection & Response

SentinelOne · CROWDSTRIKE · kaspersky · Carbon Black · TREND MICRO · FIREEYE · Trellix · Microsoft Security · NETWITNESS

NDR
Network Detection & Response

STELLAR CYBER · DARKTRACE · ExtraHop · cisco · NETWITNESS · Trellix · TREND MICRO · VECTRA · corelight

XDR
eXtended Detection & Response

STELLAR CYBER · paloalto NETWORKS · FORTINET · NETWITNESS · SentinelOne · CROWDSTRIKE · TREND MICRO · Microsoft Security · Trellix

SOAR
Security Orchestration, Automation & Response

paloalto NETWORKS · FORTINET · splunk> phantom · SWIMLANE · Microsoft Security · ThreatConnect · CYWARE · RAPID7 · tines · torq

MDR
Managed Detection & Response

Secureworks · ActZero · ARCTIC WOLF · ESENTIRE · expel · SentinelOne · CROWDSTRIKE · MANDIANT · RAPID7 · PAGO NETWORKS

특징 및 트렌드

EDR
Endpoint Detection & Response

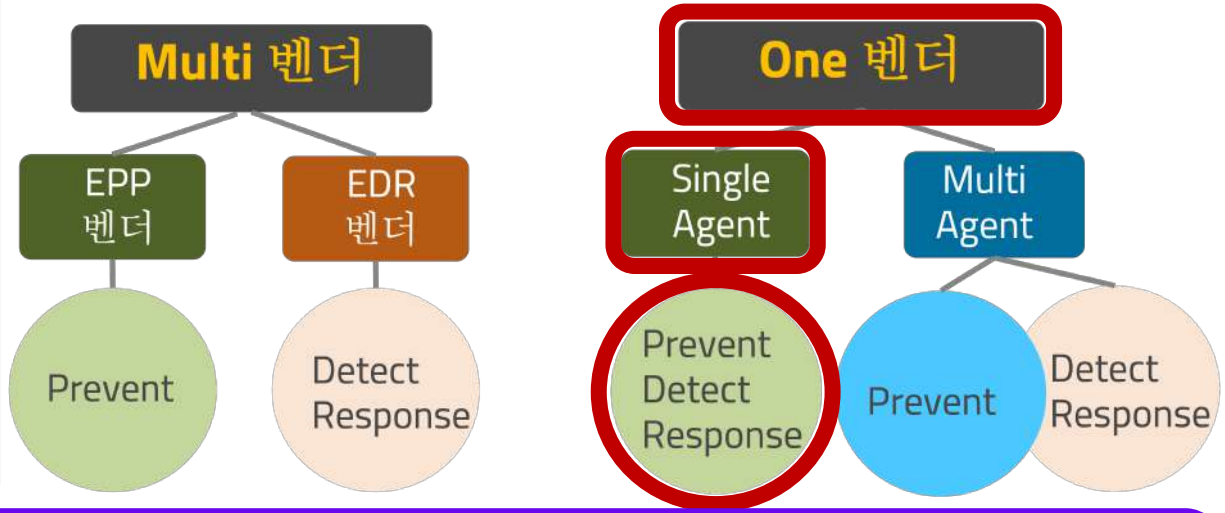
SentinelOne · CROWDSTRIKE · kaspersky · Carbon Black · TREND MICRO · FIREEYE · Trellix · Microsoft Security · NETWITNESS

기업 정보보호 이슈 전망
CONCERT FORECAST 2018

Prevent
Detect
Response

변화하는 기술 적용 / 엔드포인트 보안의 방향성

고객사 EPP . EDR 다양한 구성 방향성



추가 특징

- 통합 엔드포인트 보안 • 위협헌팅 (Threat Hunting) • 사고 대응 (Incident Response)
- MITRE ATT&CK • 복구 (Rollback) • 다중 OS (Windows, Linux, Mac, CWPP, Cloud Linux)

특징 및 트렌드

EDR
Endpoint Detection & Response

SentinelOne®

EXAMPLE

Detection Engines

- Reputation
- Static AI
- Static AI - Suspicious
- Behavioral AI - Executables
- Documents, Scripts
- Lateral Movement
- Anti Exploitation / Fileless
- Potentially Unwanted Applications
- Application Control (Containers only)

Deep Visibility Configuration

Collect this Deep Visibility data

Enable Deep Visibility

Process		File	5/5	URL	
DNS		IP	2/2	Login	2/2
Registry Keys	9/9	Scheduled Tasks	5/5	Behavioral Indicators	
Command Scripts		Cross Process	4/4	Driver Load	

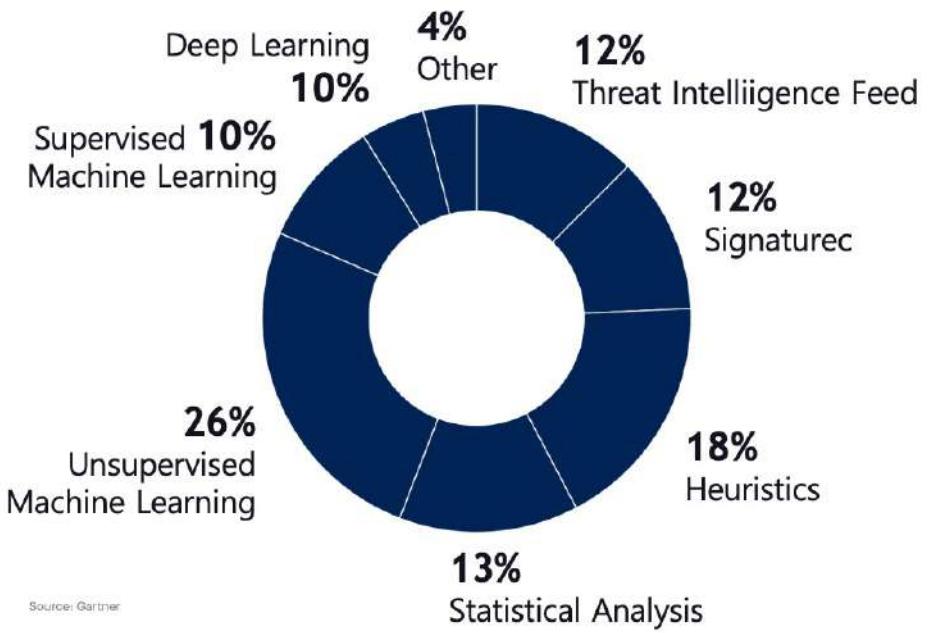
```
// Query for Outbound communications, grouped and sorted by IP with count across the environment
src.process.name matches "powershell" dst.ip.address = *
| let rfc1918 = not ($dst.ip.address matches "((127\\..*)|(192\\.168\..*)|(10\\..*)|(172\\.1[6-9]\\..*)|(172\\.2[0-9]\\..*)|(172\\.3[0-1]\\..*)).*")
| filter rfc1918 = true
| group hits = count(src.process.name), endpoints = hacklist(endpoint.name) by dst.ip.address
| sort -endpoints
```

특징 및 트렌드

NDR
Network Detection & Response

STELLAR CYBER® DARKTRACE ExtraHop cisco
NETWITNESS Trellix TREND MICRO VECTRA corelight

NDR 위협 탐지 기술 (Gartner, 2022)



고려할 기술 특징

- Real-time Law Network Packet / Traffic Metadata 분석
- 내부 트래픽 **(East-West)** / 퍼블릭 트래픽 **(North-South)**
- **위협 유발** 내부시스템 / **위협 대상** 내부시스템 동시 식별
- Signature / Heuristic 이외, **AI / Big Data 이상행위분석** 필수
- On-Prem / Cloud 기반, 모니터링 센서 유연한 통합
- Live Customized Dashboard **(쿼리기반 위젯 대쉬보드 생성)**
- Human Readable 위협 알람
- 위협 **알람 내용 강화** (Enrichment using Thrteat Intelligence)
- **대응 연동** (Security Products 수동 / 자동)

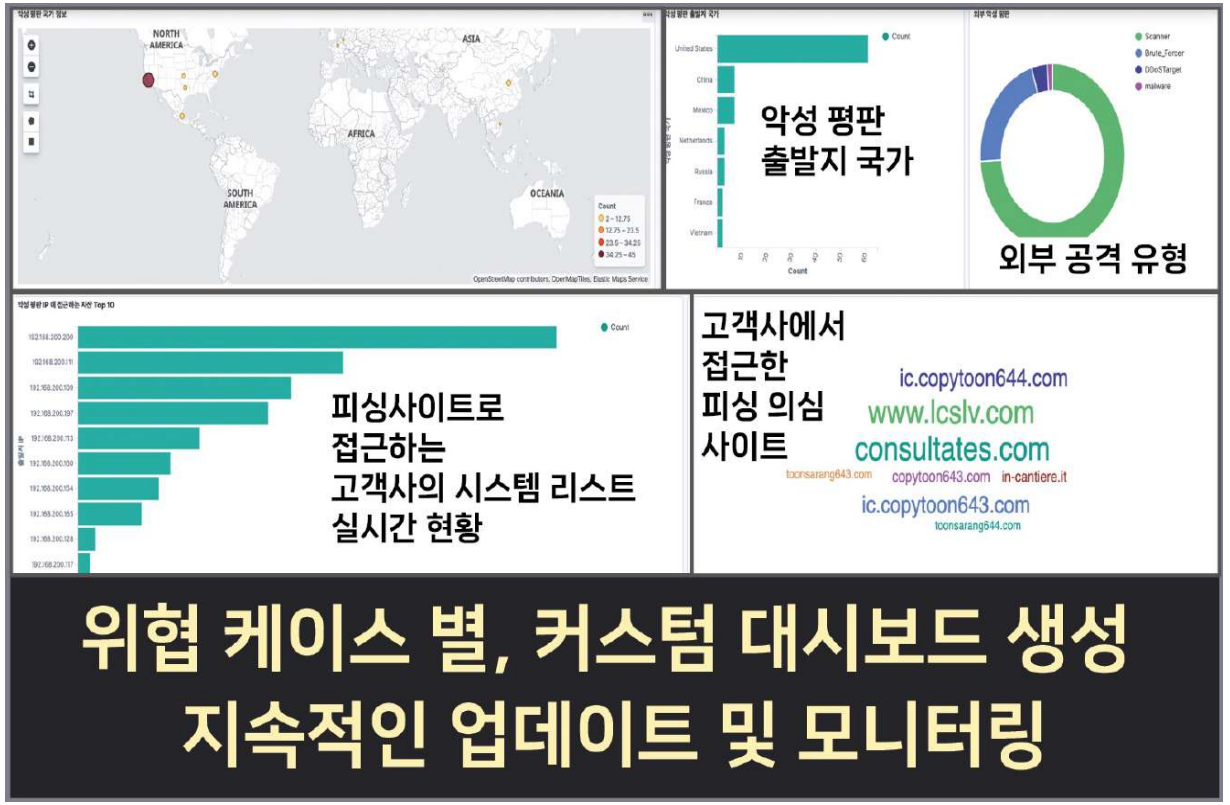
특징 및 트렌드

NDR
Network Detection & Response

STELLAR CYBER®

EXAMPLE

All Login Failures 783k Total	Plain Text Passwords 3M Total	Remote Access 278k Total	Remote Login via Unencrypted Traffic 515k Total
Brute-Forced Successful User Login 4 / 4 Critical / Total	Cryptojacking 45 / 45 Critical / Total	Exploited C&C Connection 8 / 8 Critical / Total	SYN Flood Attacker 0 / 6 Critical / Total
Private to Private Exploit Anomaly 9 / 9 Critical / Total	Private to Public Exploit Anomaly 22 / 22 Critical / Total	Public to Private Exploit Anomaly 7 / 7 Critical / Total	User Login Failure Anomaly 30 / 1k Critical / Total
Possible Unencrypted Phishing Site Visit 0 / 18 Critical / Total	Possible Phishing Site Visit from Email 56 / 56 Critical / Total	Credential Stuffing 30 / 33 Critical / Total	SMB Username Enumeration 26 / 26 Critical / Total



특징 및 트렌드

XDR
eXtended Detection & Response

STELLAR CYBER® paloalto NETWORKS FORTINET NETWITNESS
SentinelOne CROWDSTRIKE TREND MICRO Microsoft Security Trellix

EDR 기반, XDR
NDR 기반, XDR
SIEM 기반, XDR
Native XDR 벤더
Open XDR 벤더

얼라이언스

XDR Alliance
Open XDR ecosystem
CROWDXDR ALLIANCE

고려할 기술 특징

- **탐지 대응 소스 최대한 확장**
- 확장된 소스 통합, 탐지, 액션
- **탐지 대응 소요시간 최소화**
- **약한 신호들 -> 강한 보안 알람**
- 위협 알람 내용 강화
- **크로스 쿼리기반 위젯/대쉬보드**
- 위협 인텔리전스 동시 공유
- **빅데이터 기반 분석 기술 내장**
- AI (ML, DL) 탐지 기술 내장

특징 및 트렌드

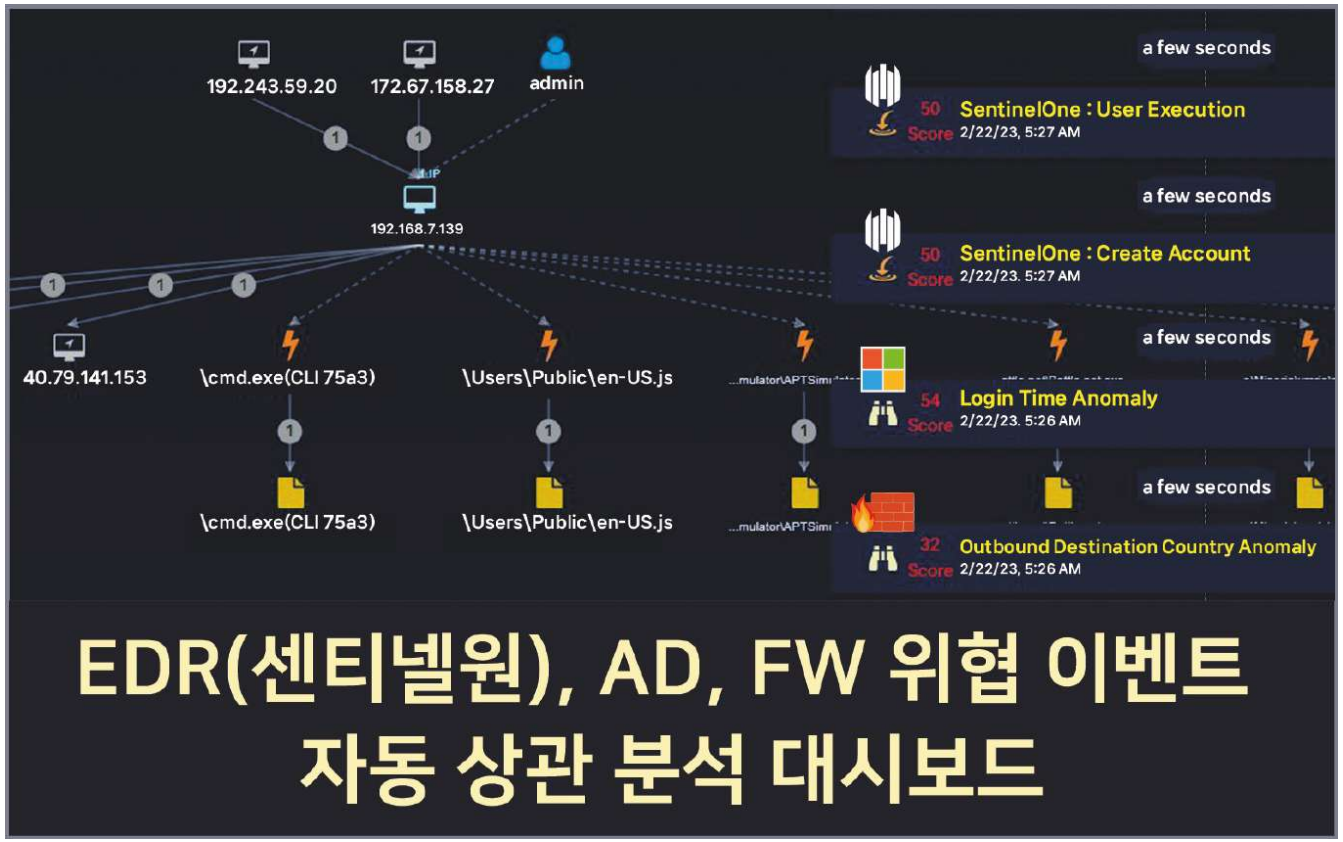
EXAMPLE

XDR
eXtended Detection & Response

STELLAR CYBER®

스텔라 사이버 오픈 XDR

- 자체 NDR 어플라이언스
  네트워크 트래픽 이벤트 수집
  대형, 중형, 소형 장비
- 고객사 인증 플랫폼
  OKTA, Google 등
- 고객사 AD서버 연동
  사용자 정보 이벤트
- 자체 엔드포인트 에이전트
  시스템 이벤트 수집
- 보안 운영 분석 자동화 플랫폼
- 고객사 Cloud 연동
  플랫폼 이벤트
- 고객사 EDR 연동
  보안 이벤트
- 고객사 FW 플랫폼
  Syslog (Allow, Deny)



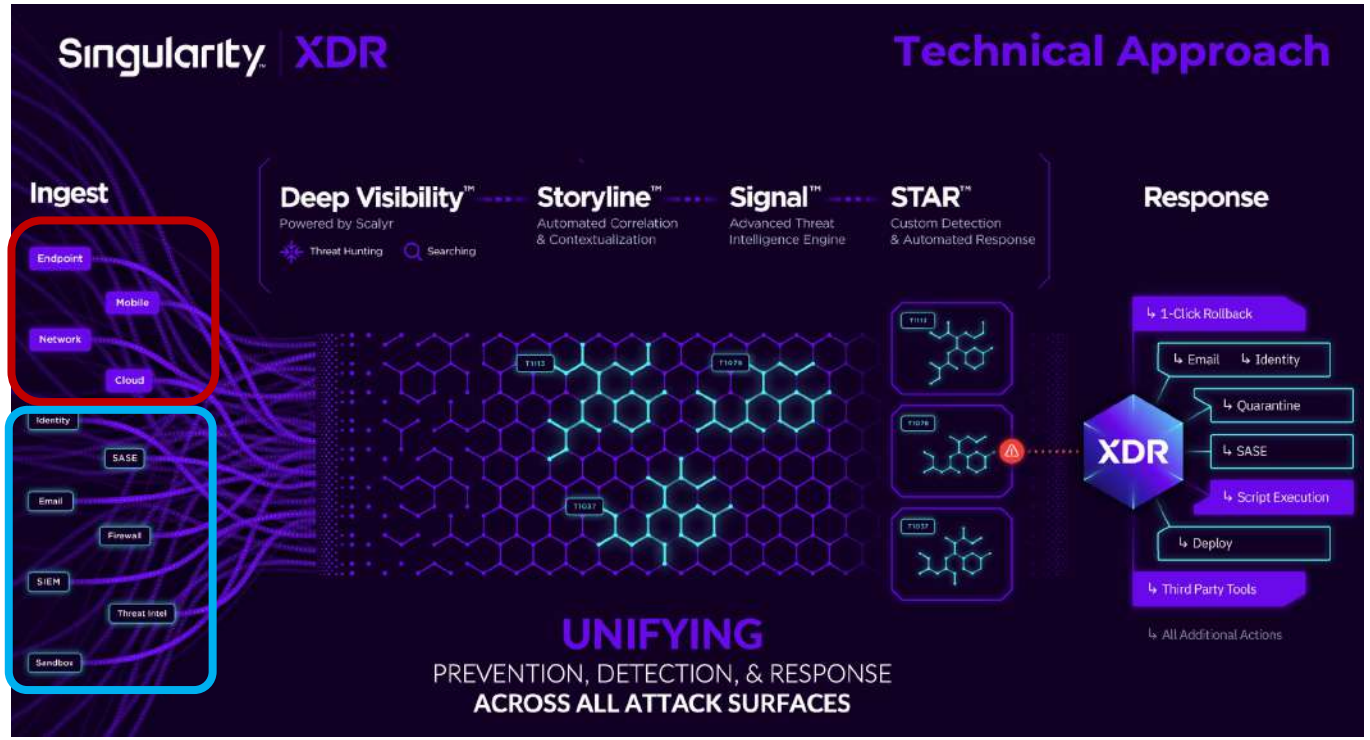
EDR(센티넬원), AD, FW 위협 이벤트 자동 상관 분석 대시보드

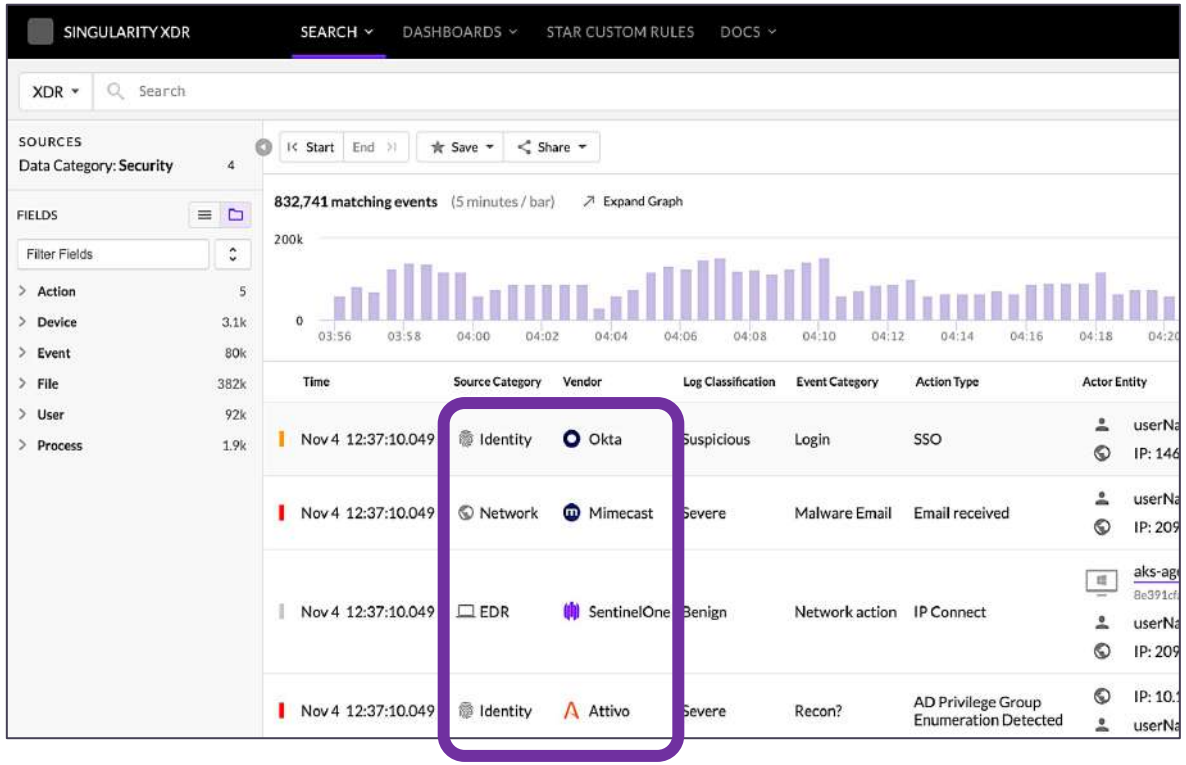
특징 및 트렌드

XDR
eXtended Detection & Response

SentinelOne®

EXAMPLE





기술 특징.트렌드

SOAR
Security Orchestration, Automation & Response

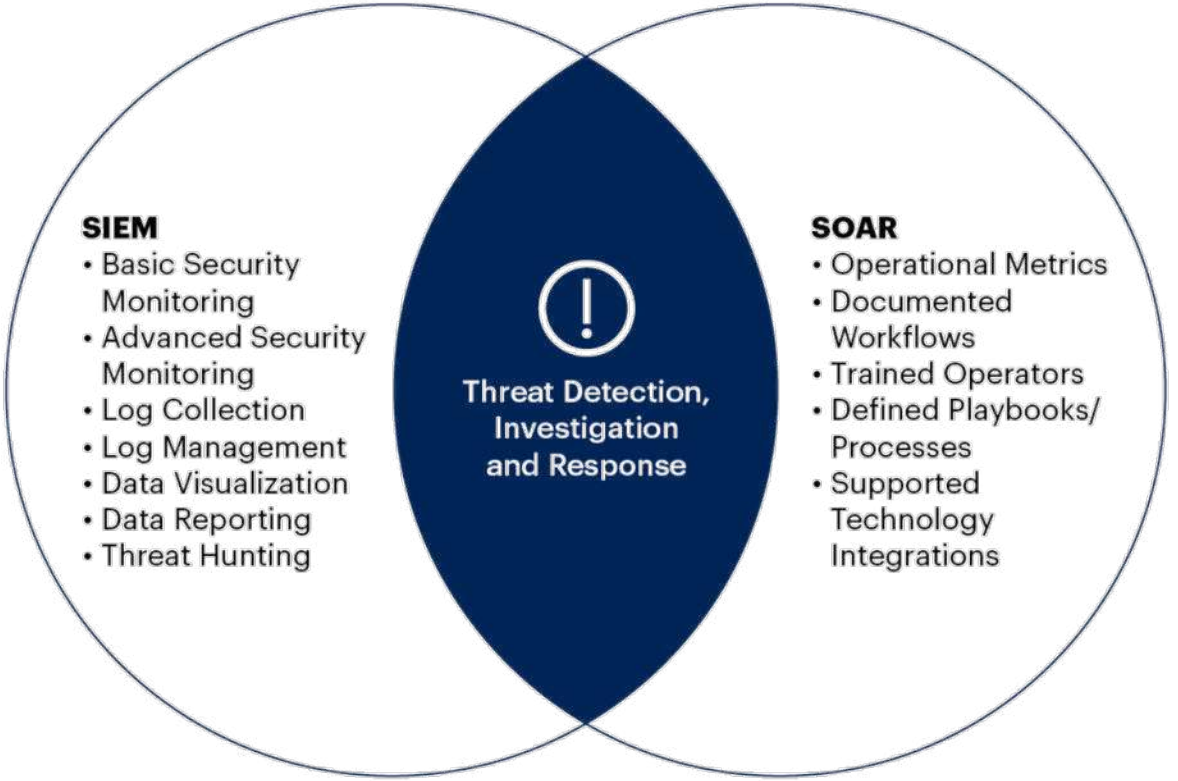
paloalto NETWORKS FORTINET splunk> phantom SWIMLANE Microsoft Security
ThreatConnect CYWARE RAPID7 tines torq

Three 기술의 통합 (Gartner, 2022)

Security Incident Response Platforms (SIRPs)
- Case/Incident Management
- Workflows
- Incident Knowledgebase

Security Orchestration and Automation (SOA)
- Integrations
- Play/Process/Workflow Automation
- Playbook Management

Threat Intelligence Platforms (TIPs)
- TI Aggregation, Curation, Distribution
- Alert Enrichment
- TI visualization



- 생산성
- 효율성
- 지속성
- 시스템 연결
- 팀. 협업
- 프로세스화
- 자동대응
- 수동대응
- 케이스. 관리
- 에스컬레이션

- **현재는 XDR 플랫폼 내부 기능과 일부 중복 되기도 함**

기술 특징.트렌드

SOAR
Security Orchestration, Automation & Response

paloalto NETWORKS FORTINET splunk> phantom SWIMLANE Microsoft Security
ThreatConnect CYWARE RAPID7 tines torq

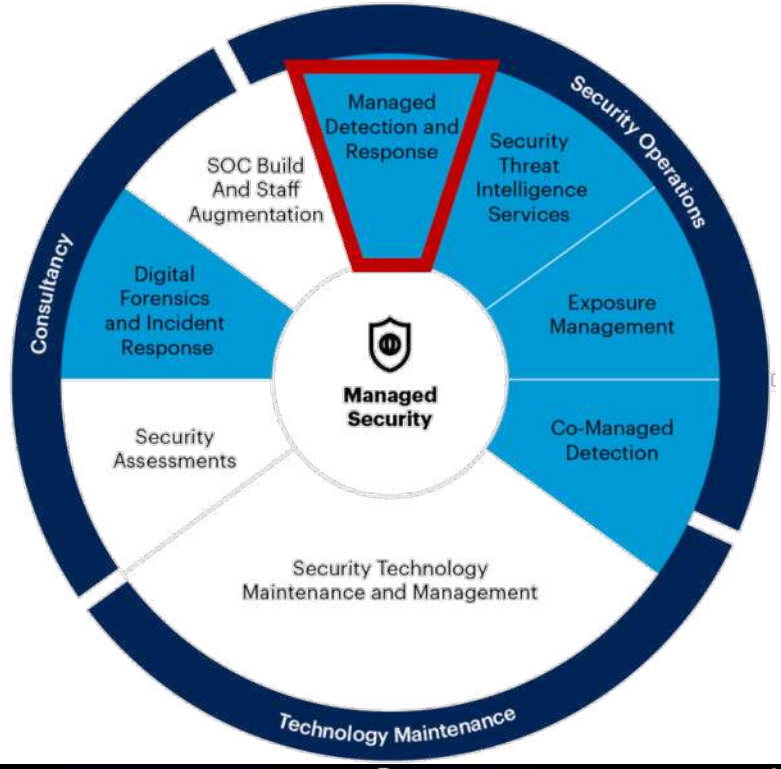
- Workflow / Playbook 이 "완전 자동화를 의미하는 것이 아님.
- 특정 보안솔루션에서 위협 IOC 취합 후,
  다른 보안솔루션에 정책적용 자동화 시키는 것이, SOAR 최종 목표가 아님.
- Low-Code / No-Code SOAR 플랫폼 등장으로 복잡성 해제 움직임
- 앞에서 다룬,
  EDR / NDR / XDR 등의 이벤트 등을 처리하는 SOC 운영 프로세스

기술 특징.트렌드

MDR
Managed Detection & Response

Secureworks · ActZero · ARCTIC WOLF · eSENTIRE · expel · SentinelOne · CROWDSTRIKE · MANDIANT · RAPID7 · PAGO NETWORKS

Managed Security Service (Gartner, 2022)



기술 특징.트렌드

EXAMPLE

MDR
Managed Detection & Response

PAGO NETWORKS

CYLANCE
SentinelOne
STELLAR CYBER®

제품별 매니지드 서비스

- **Managed EDR**
- **Managed NDR**
- **Managed XDR**

- 위협 유효성 검증
- 전문분석가 심층 분석
- 빠른 판단 및 대응
- 위협 인사이츠 요약
- 고객 에스컬레이션
- 위협 제거, 고립, 대응

전문 MDR 서비스 추가 모듈

- 리모트 가상 CERT / SOC 역할
- 사고 대응 (Incident Response)
- 위협 헌팅 (Threat Hunting)
- 위협 노출 점검 (Attack Surface Mgmt)
- 위협 IOC 추출 / 공유
- 침해여부 진단 (Compromise Assess)

MDR 서비스 자동화

- 위협 인텔리전스 시스템
- 위협 자동 분석 시스템
- 자체 SOAR (플레이북, 워크플로우)
- 상용툴 / 오픈소스툴 / 자체 개발

탐지 대응 솔루션 도입, 고려 사항 (왜 어려운가?)

EDR
Endpoint Detection & Response

NDR
Network Detection & Response

XDR
eXtended Detection & Response

SOAR
Security Orchestration, Automation & Response

MDR
Managed Detection & Response

전제조건

위협은 이미 침투했다

위협은 이미 진행중이다

R

시스템 관점
Response

- Alert
- Playbook
- Quarantine
- Kill process
- Logout
- Containment
- Integration via API

고려할 사항.
적용 쉽지않다.
도입 걸림돌.

전문가 관점
프로세스 / 대응

- Investigation
- Threat Hunting
- Forensic
- Actionalble Answer
- Manual Response
- Automatic Response

위협 탐지 대응 솔루션

고려 사항

(어떻게 사용하면 좋은가?)

PAGO DeepACT 매니지드 탐지/대응 목표

파고 자체 - SOAR / TI 플랫폼 구축 및 자동화

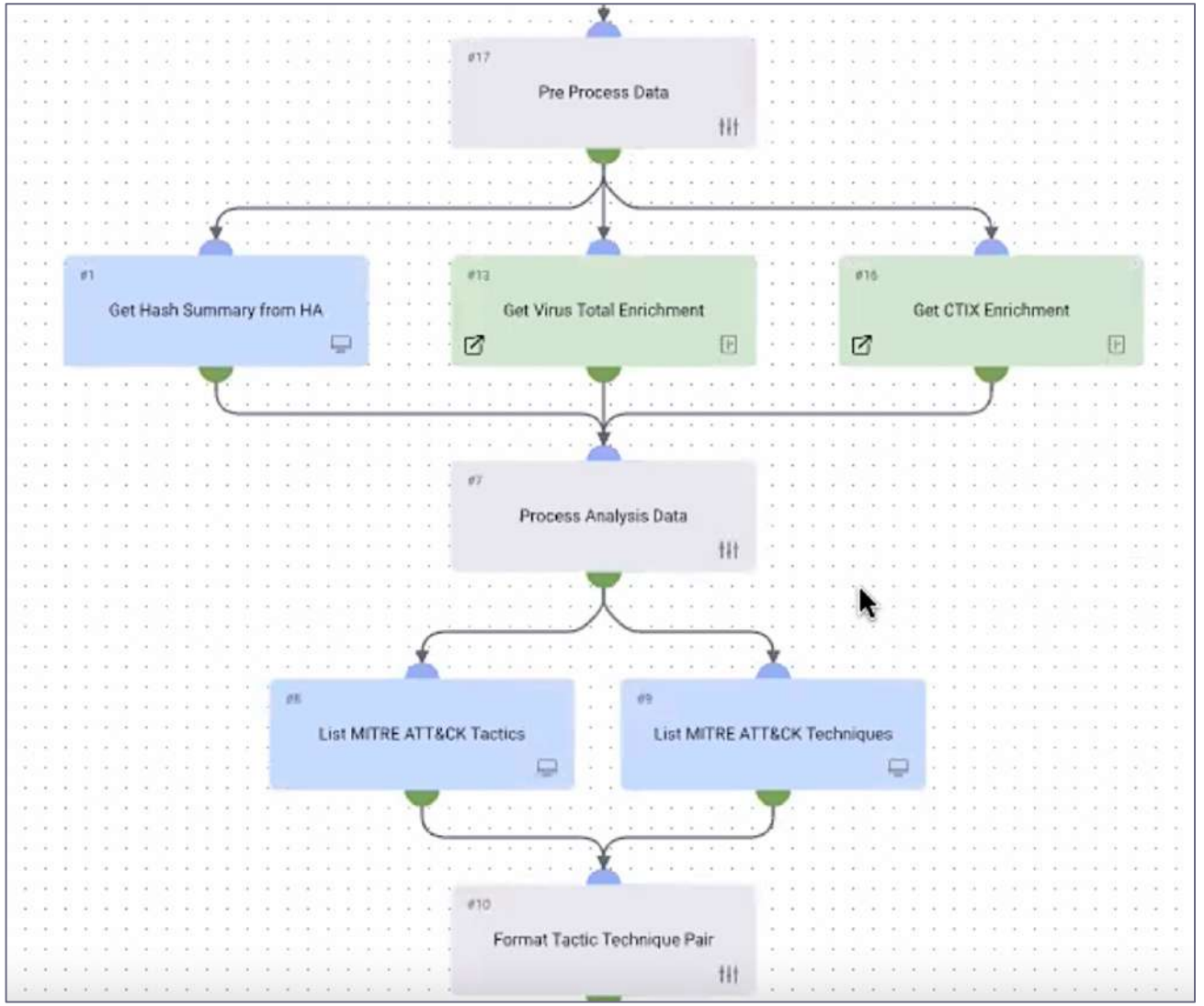
PAGO-CSOL

Playbooks (20) Custom System

All Active Inactive

Search or filter results

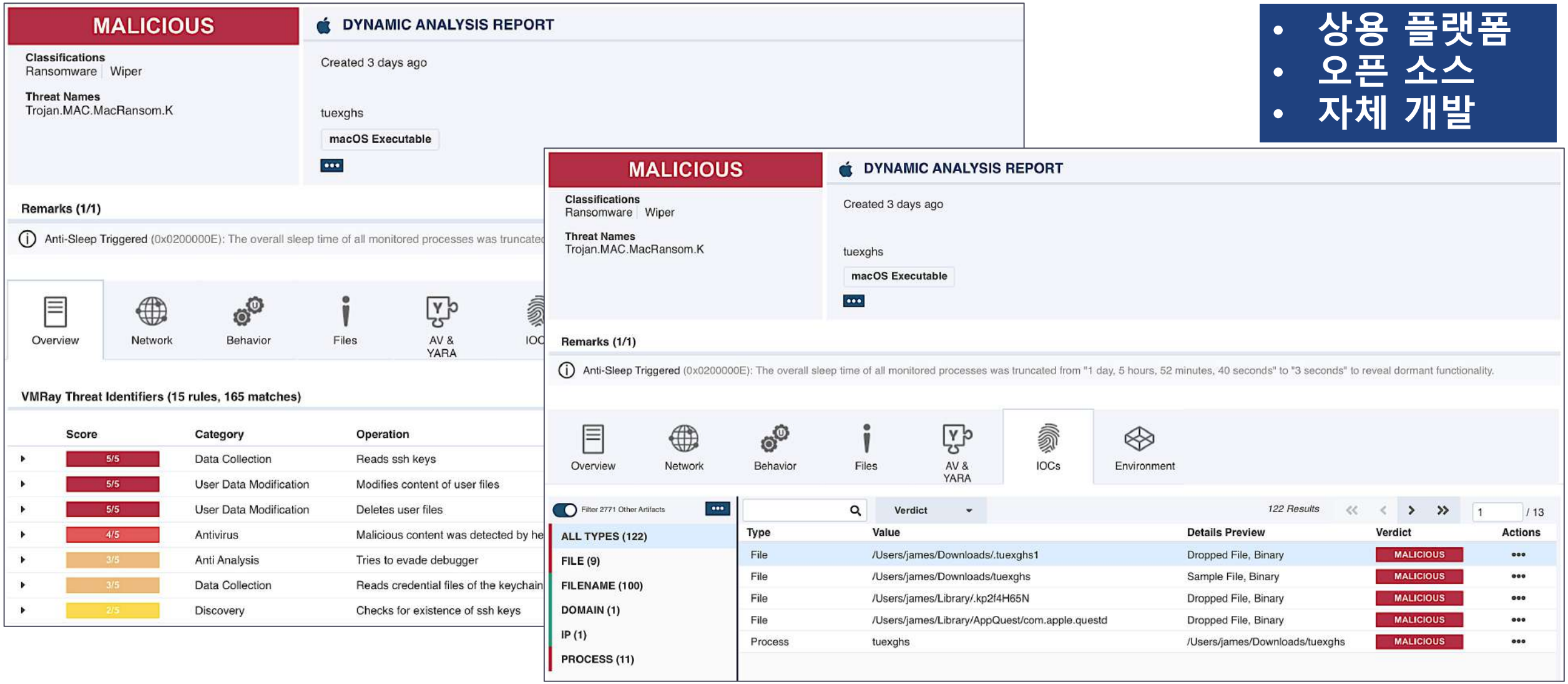
ID	Playbook Name
PLB109	Onboard Alerts from Cylance Protect
PLB110	Fetch Alert Details
PLB117	Move Hash to GlobalSafe List
PLB101	Test
PLB111	Fetch Devices Associated with a Threat
PLB119	CTIX :: Enrich IOCs
PLB118	CTIX :: Update Block Details
PLB124	CTIX :: Process IOCs Reported by CFTR
PLB114	Enrich IOC - Hashes



- 상용 플랫폼
- 오픈 소스
- 자체 개발

파고 자체 – 프로세스에 의한 위협분석 자동화

- 상용 플랫폼
- 오픈 소스
- 자체 개발



파고 자체 대응 협업 프로세스 (고객 요청 이전)

특정 고객사에서,
악성코드 탐지, 격리 성공후
추가 조사 프로세스 발동

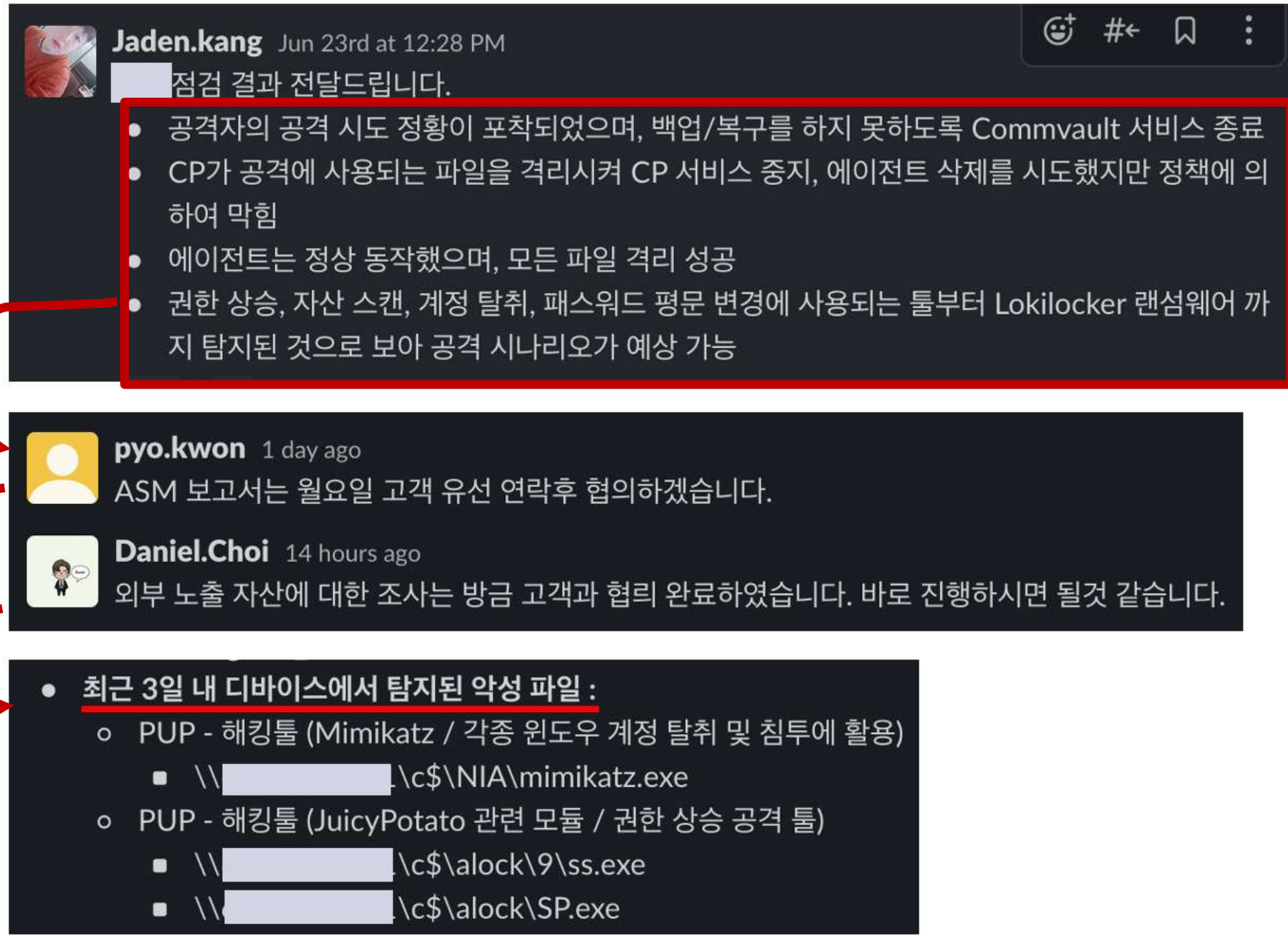
- 보안에이전트 비활성화 정황
- Commvault 서비스 종료
- 다수 악성코드 탐지 / 격리

외부에서 취약점이 보이는지
Attack Surface Management
고객사와 협의 완료

위협분석대응팀에서,
최근 3일 이내 탐지/격리된
추가적인 악성코드 업데이트

고객사에 즉각 공유한 결론 !!!

- 이 시스템은 **랜섬웨어 공격**에 계속 타겟팅되어 있는 상태이며, 취약점 점검 및 외부 통신 차단필요



분석된 2차 정보 바탕, 고객사 타겟공격 논의

- 탐지된 파일 정보 (총 16개)
  - Gmer - 안티루트킷 / 프로세스 강제 종료 가능 / 2개
  - YDArk - 안티루트킷 / AV 무력화 툴 / 2개
  - Processhacker - 프로세스 강제 종료 가능 / 4개
  - 트로얀 - 다운로더 성향있는 트로얀으로 인터넷 환경이 적합하면 악성파일 다운로드 후 크리티컬한 멀웨어 기능 수행 간으성 존재 / 8개

이번 경우는, 그 다음 프로세스가 ....

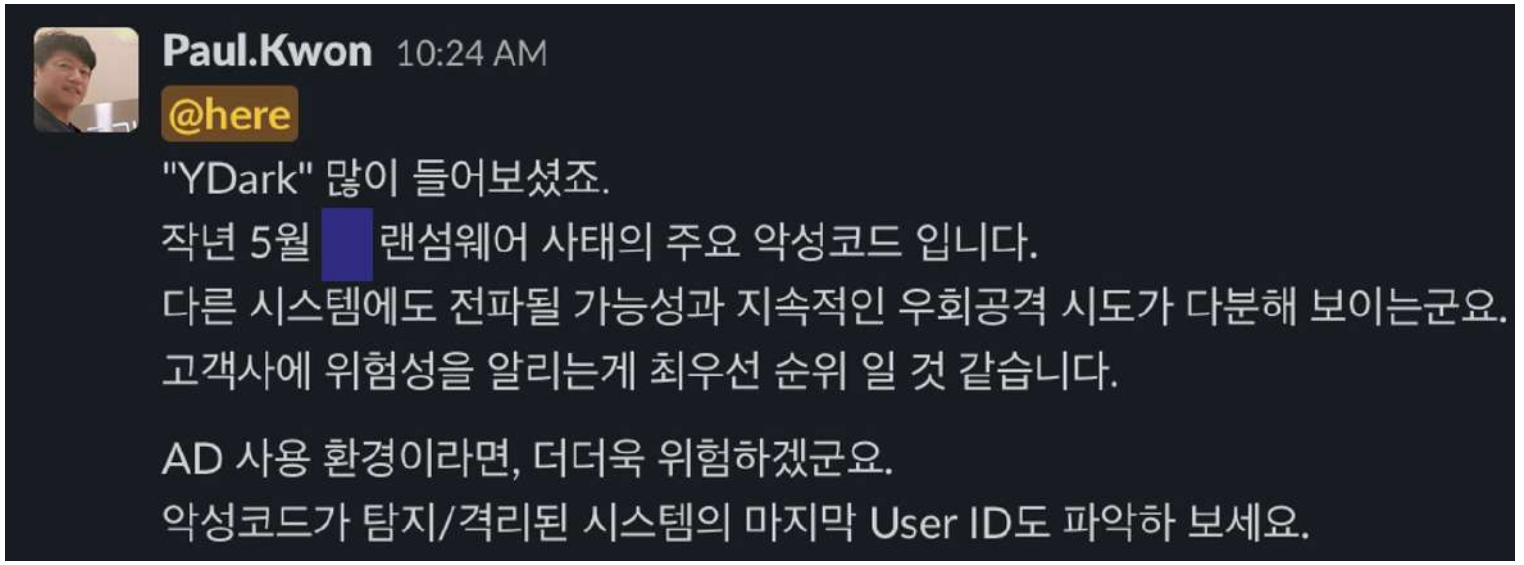
- 전형적인 랜섬웨어 드롭 단계
- 고객이 "타겟팅" 되었다는 의미 (**)
- 고객사와 즉시 공유
- 고객사와 추가 조사, 헌팅, 방어 논의

❑ 분석가 요약

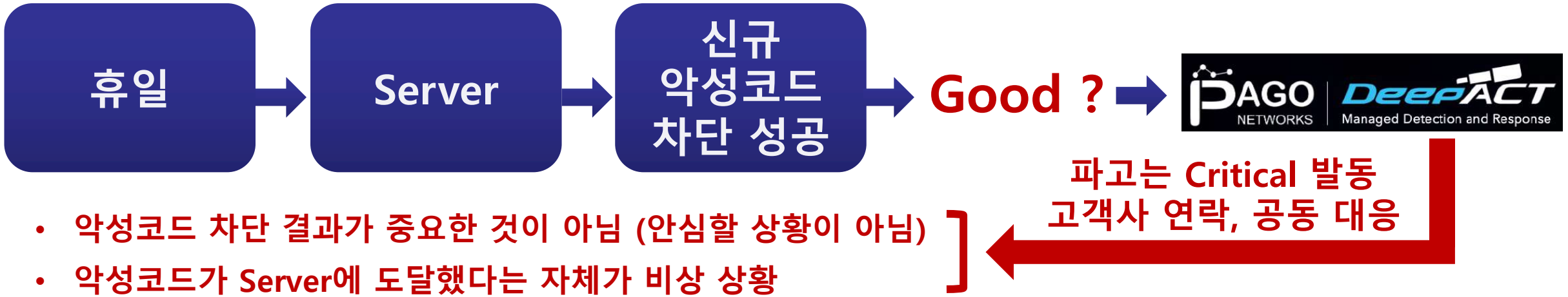
- 전형적인 "랜섬웨어" 과정
- 어떤 공격이 차단되었는지 공유하는 것은 아주 중요

- 차단된 악성코드 그룹을 2차 분석하는 필요성 입증 (**)

소통



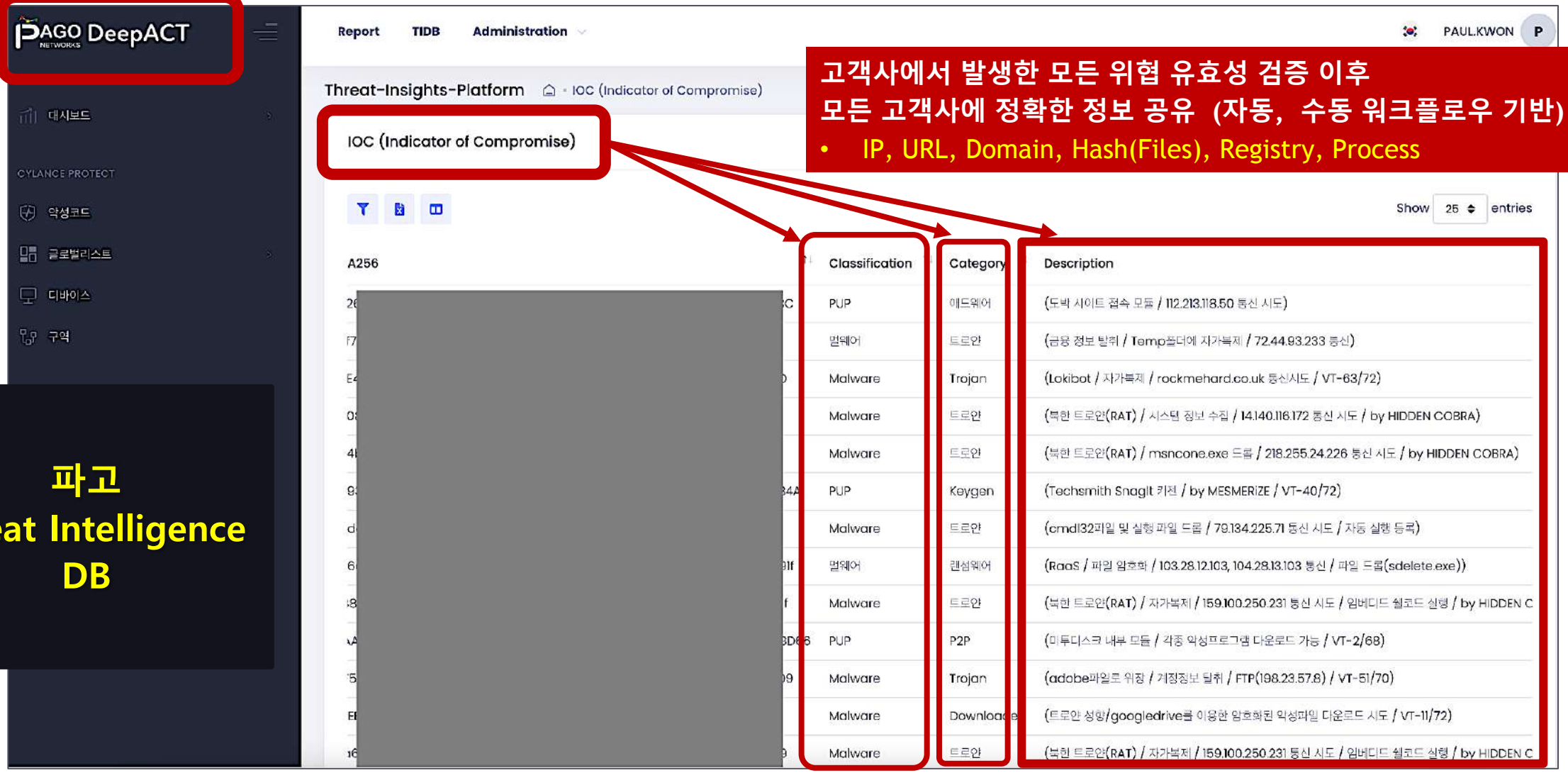
악성코드 차단성공 했는데, 비상 상황 발동 !!



- **악성코드 차단 결과가 중요한 것이 아님 (안심할 상황이 아님)**
- **악성코드가 Server에 도달했다는 자체가 비상 상황**
  - ✓ Exploit ? / 정상 경로 ? ➔ 조사 (Investigation) 프로세스 돌입 필요
  - ✓ 사용자 Login / 원격 접속 유무
  - ✓ AD 조인 여부
  - ✓ 서버 관련, NW 트래픽 조사
  - ✓ 서버 최근 탐지되었던 모든 악성코드 / PUP 종류 파악
  - ✓ FW Rule 점검
  - ✓ **외부 인터넷, 또는 내부 NW에서, 이 서버로 접근 가능한 취약 포인트 조사 (Port, Protocol, Service)**

위협 탐지 조견별,
ASM (Attack Surface Management)
협의 및 수행

파고 DeepACT 자체 콘솔 (모든 고객사 위협 연동)

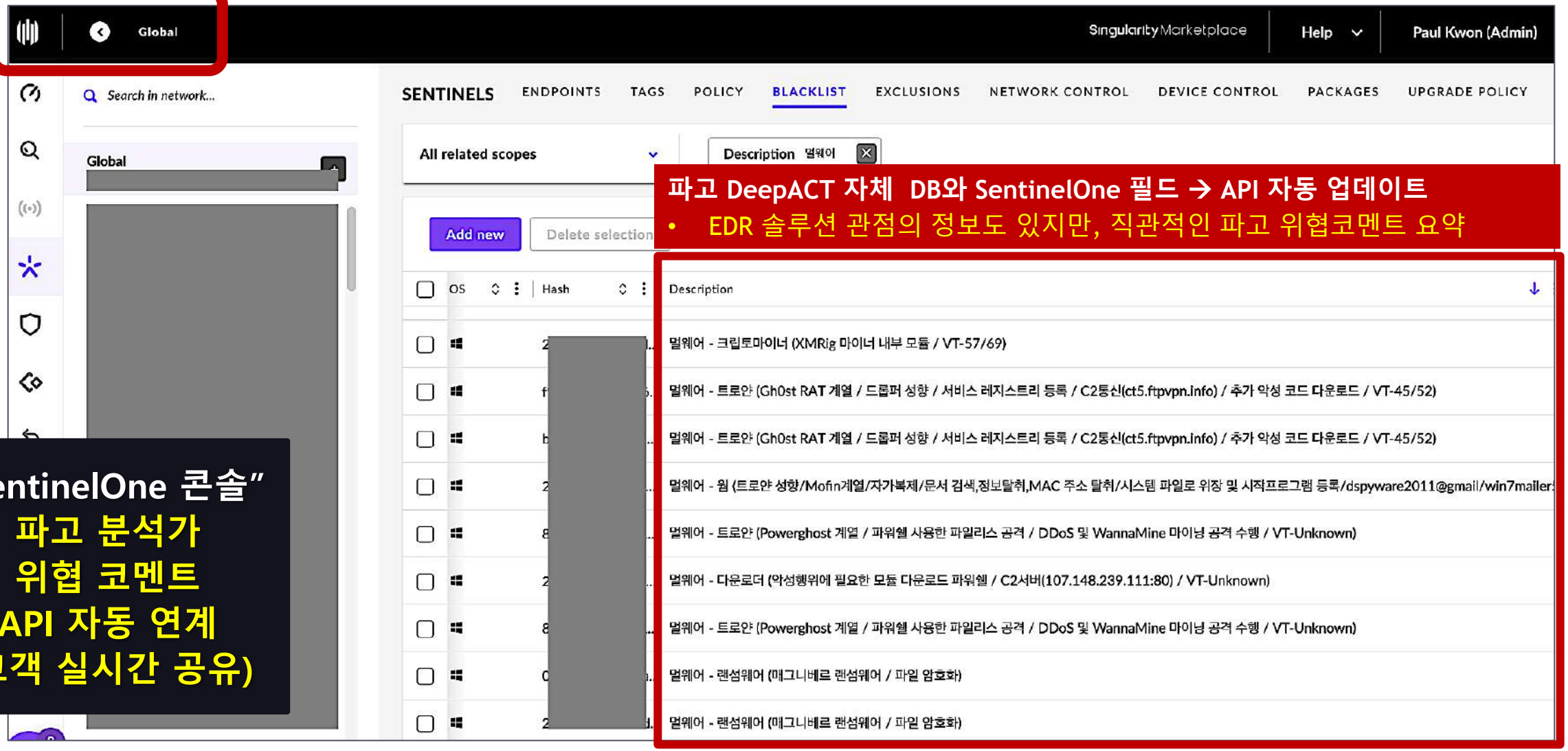


고객사에서 발생한 모든 위협 유효성 검증 이후
모든 고객사에 정확한 정보 공유 (자동, 수동 워크플로우 기반)

- IP, URL, Domain, Hash(Files), Registry, Process

파고
Threat Intelligence
DB

SentinelOne 고객 – 분석가 코멘트 API 자동 연계



파고 DeepACT 자체 DB와 SentinelOne 필드 → API 자동 업데이트

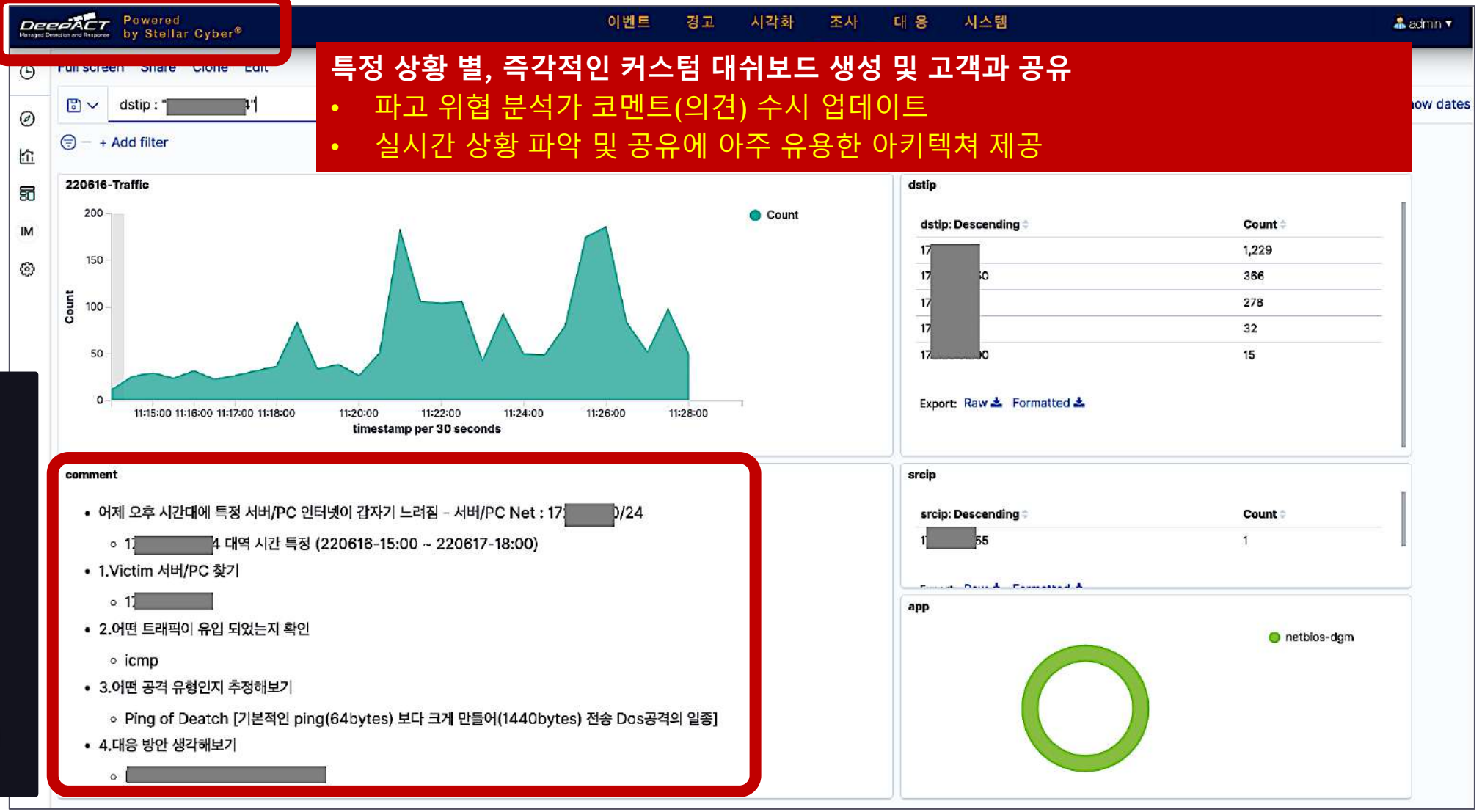
- EDR 솔루션 관점의 정보도 있지만, 직관적인 파고 위협코멘트 요약

"SentinelOne 콘솔"
파고 분석가
위협 코멘트
API 자동 연계
(고객 실시간 공유)

Stellar Cyber XDR 고객 – 커스텀 대쉬보드 분석가 의견 API 자동 연계

특정 상황 별, 즉각적인 커스텀 대쉬보드 생성 및 고객과 공유

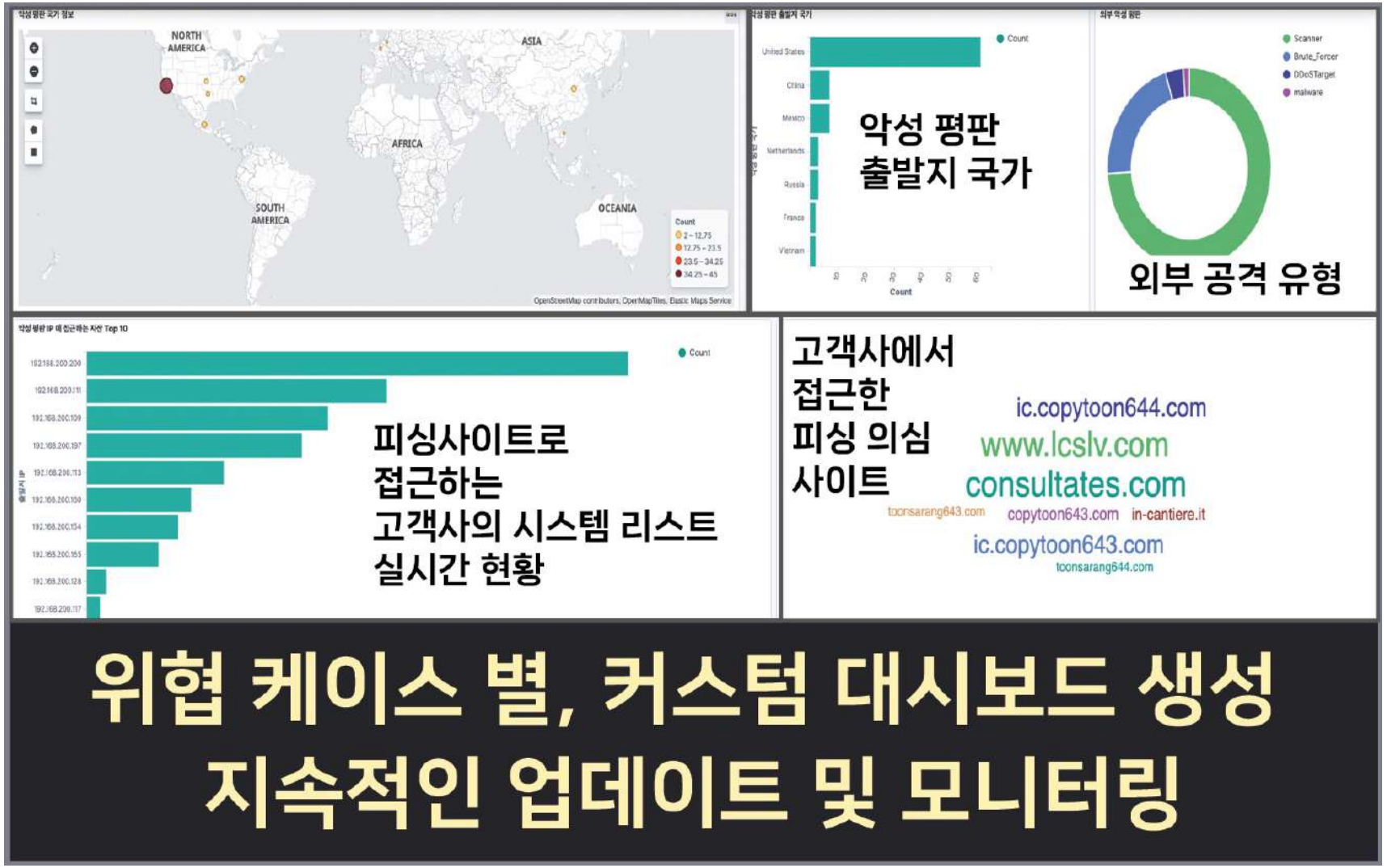
- 파고 위협 분석가 코멘트(의견) 수시 업데이트
- 실시간 상황 파악 및 공유에 아주 유용한 아키텍쳐 제공



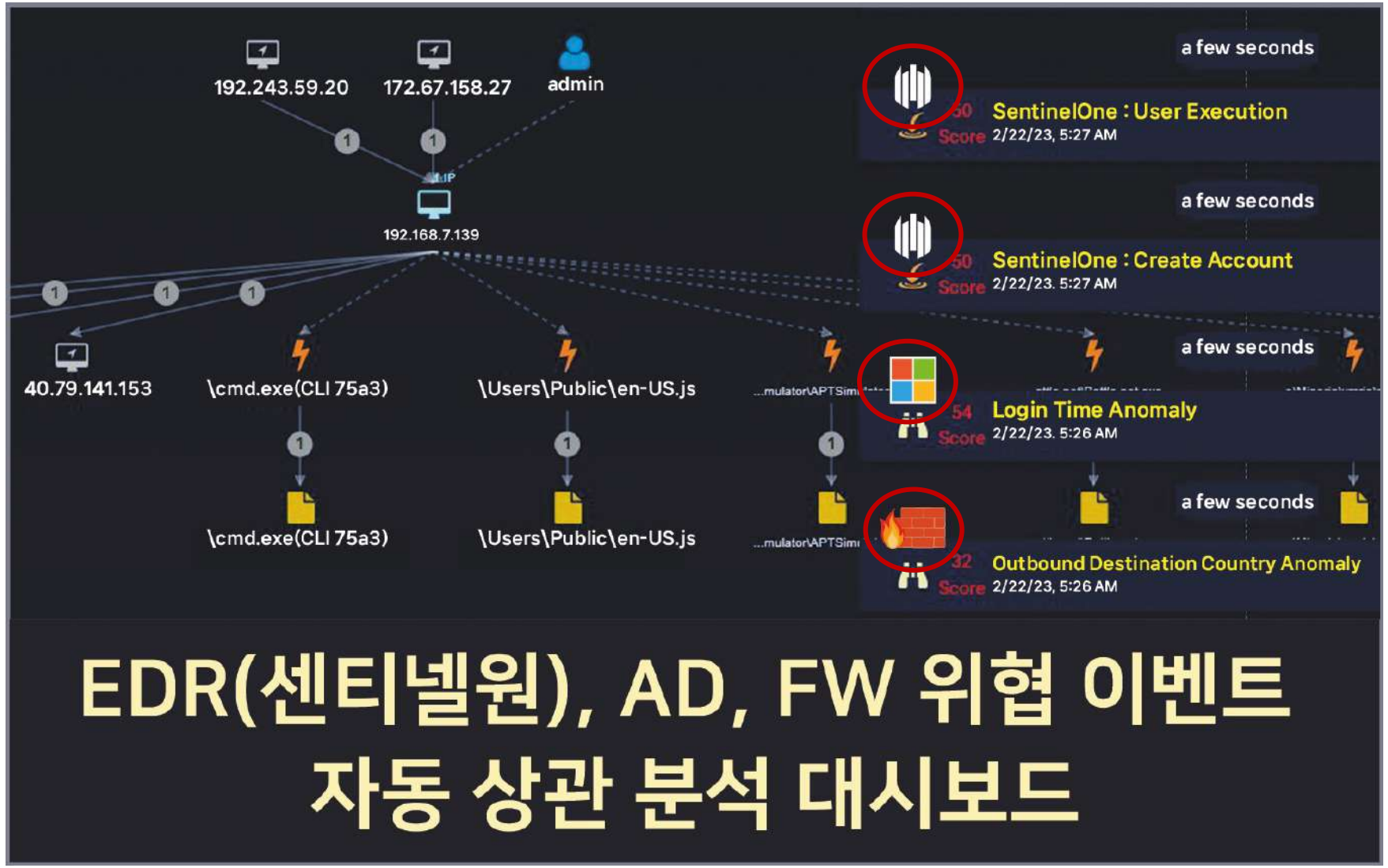
"Stellar Cyber XDR 콘솔" 커스텀 대쉬보드 **파고 분석가 위협 코멘트 API 자동 연계 (고객 실시간 공유)**

Stellar Cyber XDR 고객 – 커스텀 대쉬보드

"Stellar Cyber XDR 콘솔"
커스텀 대쉬보드
실제로
당장 모니터링
필요한 내용 관련
대쉬보드 생성
(고객 실시간 공유)



Stellar Cyber XDR 고객 – 자체 NDR + 타 보안 솔루션 이벤트 연동



매니지드 탐지/대응(MDR) 서비스 대상 고객

보안에 투자할
여력이 없는
SMB (중소기업)

기존
NW보안 위주
보안관제서비스
중견 / 대기업

기존
SIEM / Event 위주
모니터링
중견 / 대기업

“고객 내부 전문가 & MDR 서비스 프로바이더”

공동 위협 대응 프로세스 정립시키는 과정

급변하는 위협에 대한, 실질적인 탐지 및 방어 서비스 상호 협력

지능형 위협 탐지.대응 고도화 – 우리가 원하는 것

이미
침투해 있는
위협, 악성코드
탐지/격리, 능동대응

새로이
침투 진행중인
위협, 악성코드
탐지/격리, 능동대응


PAGO
NETWORKS

PAGO NETWORKS | DeepACT Managed Detection and Response

매니지드 위협 탐지 및 대응 전문기업

MDR-as-a-Service / SOC-as-a-Service / CERT-as-a-Service

Protecting Enterprise For "IT, Cloud, OT/ICS" Infrastructure

(주) 파고네트웍스
매니지드 탐지 및 대응 전문 기업
서울시 강남구 강남대로 382, 강남역 메리츠타워 18층

PAGO DeepACT 매니지드 위협 탐지 및 대응 센터
MDR (Managed Detection & Response) Center
경기도 안양시 동안구 시민대로 361, 에이스평촌타워 1003호

https://www.PAGOnetworks.com
영업 문의 : sales@PAGOnetworks.com
기술 문의 : tech@PAGOnetworks.com