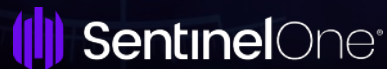


# 혼동스러운 EDR, NDR, XDR 마켓 트렌드, 기술적 정의 및 고려사항

[부제 : 위협 탐지/대응 솔루션, 어떻게 사용하면 좋은가?]



매니지드 위협 탐지 및 대응 전문기업



# 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



## NDR

Network Detection & Response



## XDR

eXtended Detection & Response



## SOAR

Security Orchestration, Automation & Response



## MDR

Managed Detection & Response



# 특징 및 트렌드

## EDR

Endpoint Detection & Response

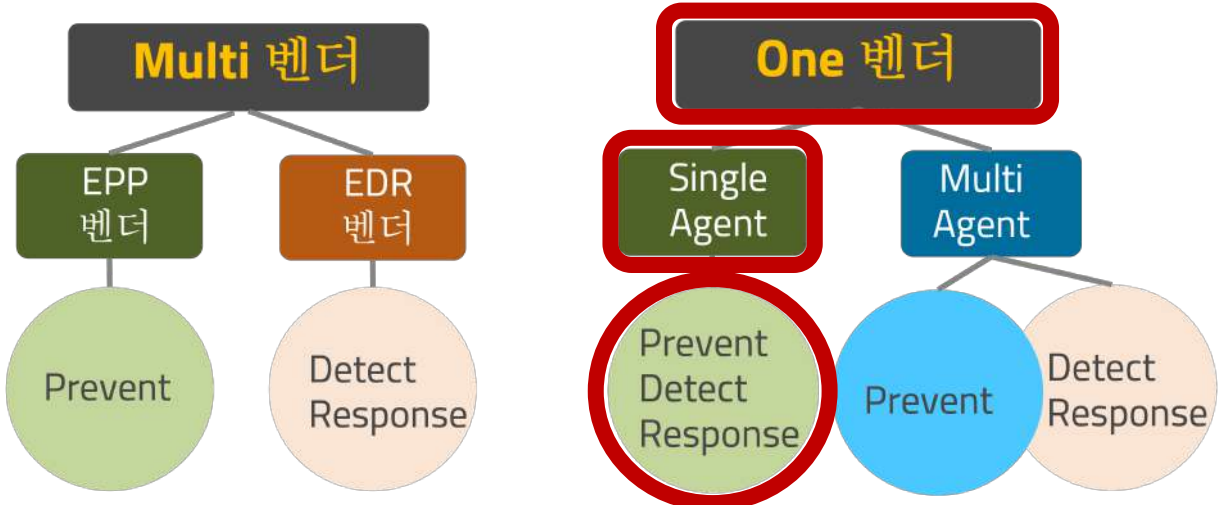


기업 정보보호 이슈 전망  
CONCERT FORECAST 2018

**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



### 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

Enable Deep Visibility [?](#)

Collect this Deep Visibility data

- |   |   |   |
|---|---|---|
| <input checked="" type="checkbox"/> Process <a href="#">?</a>                           | <input checked="" type="checkbox"/> File <a href="#">5/5</a> <a href="#">?</a>            | <input checked="" type="checkbox"/> URL <a href="#">?</a>                       |
| <input checked="" type="checkbox"/> DNS <a href="#">?</a>                               | <input checked="" type="checkbox"/> IP <a href="#">2/2</a> <a href="#">?</a>              | <input checked="" type="checkbox"/> Login <a href="#">2/2</a> <a href="#">?</a> |
| <input checked="" type="checkbox"/> Registry Keys <a href="#">9/9</a> <a href="#">?</a> | <input checked="" type="checkbox"/> Scheduled Tasks <a href="#">5/5</a> <a href="#">?</a> | <input checked="" type="checkbox"/> Behavioral Indicators <a href="#">?</a>     |
| <input checked="" type="checkbox"/> Command Scripts <a href="#">?</a>                   | <input checked="" type="checkbox"/> Cross Process <a href="#">4/4</a> <a href="#">?</a>   | <input checked="" type="checkbox"/> Driver Load <a href="#">?</a>               |

// 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
```



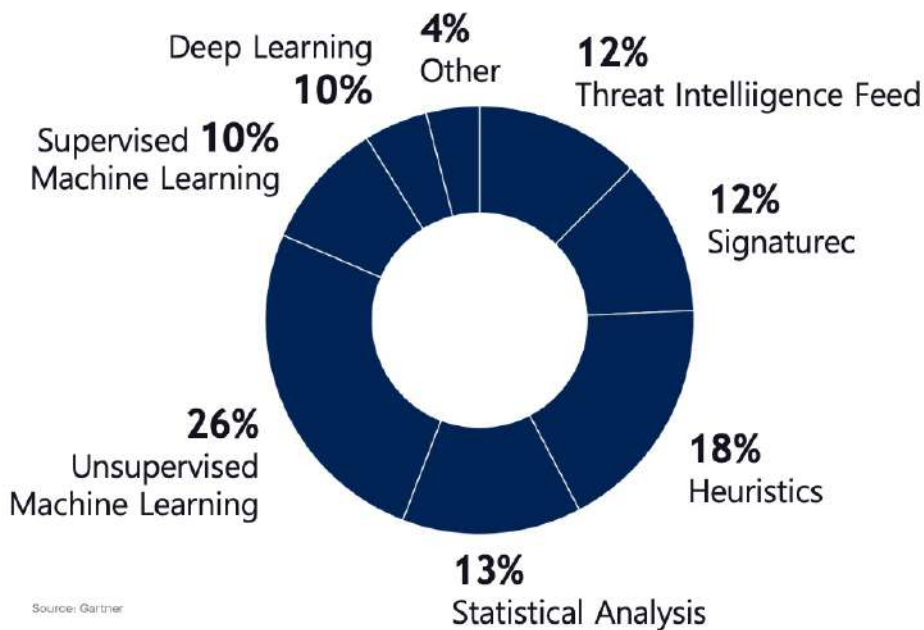
# 특징 및 트렌드

## NDR

Network Detection & Response



### NDR 위협 탐지 기술 (Gartner, 2022)



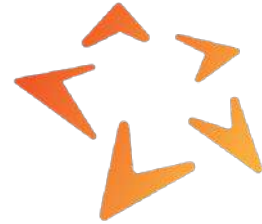
### 고려할 기술 특징

- 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 Threat Intelligence)
- **대응 연동** (Security Products 수동 / 자동)

# 특징 및 트렌드

## NDR

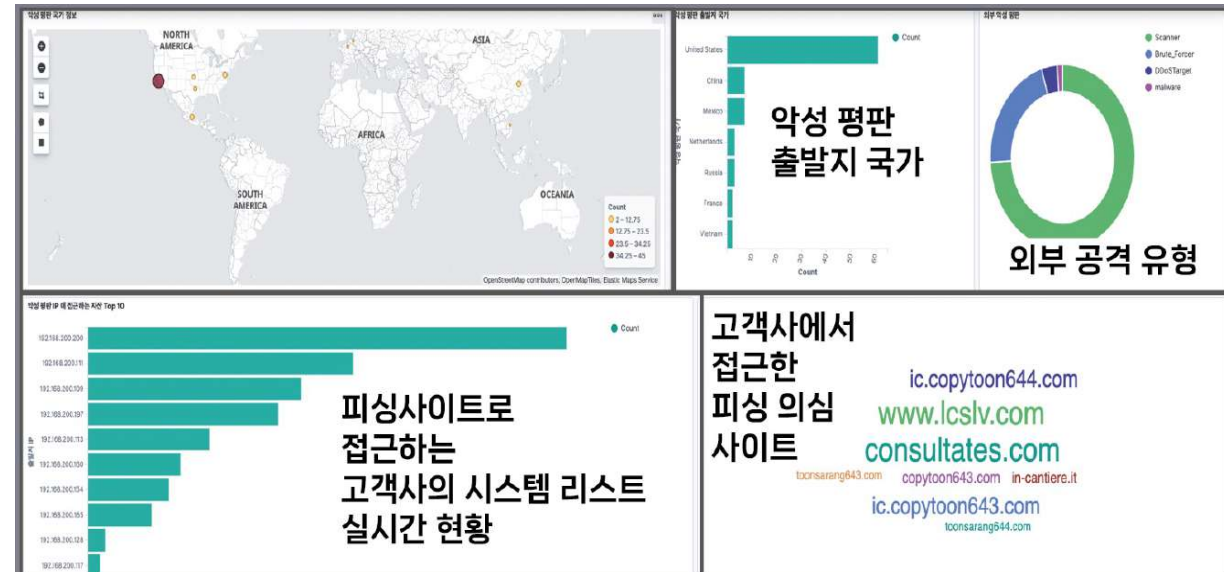
Network Detection & Response



## STELLAR CYBER®



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



## 위협 케이스 별, 커스텀 대시보드 생성 지속적인 업데이트 및 모니터링



# 특징 및 트렌드

## XDR

eXtended Detection & Response



STELLAR  
CYBER®



FORTINET®



EDR 기반, XDR

NDR 기반, XDR

SIEM 기반, XDR

Native XDR 벤더

Open XDR 벤더

얼라이언스

XDR Alliance®  
Open XDR ecosystem  
CROWDXDR ALLIANCE

### XDR Back End

Cloud  
Delivered

Data Lake

Automation

Threat  
Intelligence

APIs

Orchestration

Advanced  
Analytics

Incident  
Investigations

Response  
Workflow

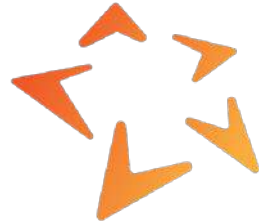
## 고려할 기술 특징

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

# 특징 및 트렌드

## 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 Clud 연동

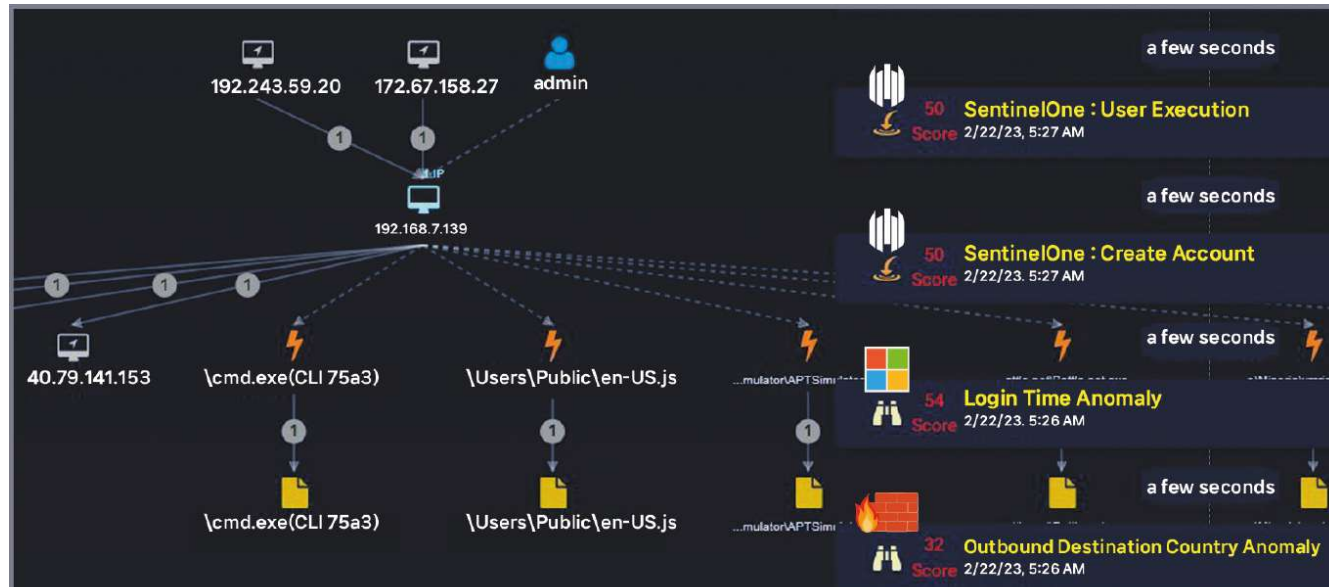
플랫폼 이벤트

#### 고객사 EDR 연동

보안 이벤트

#### 고객사 FW 플랫폼

Syslog (Allow, Deny)



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

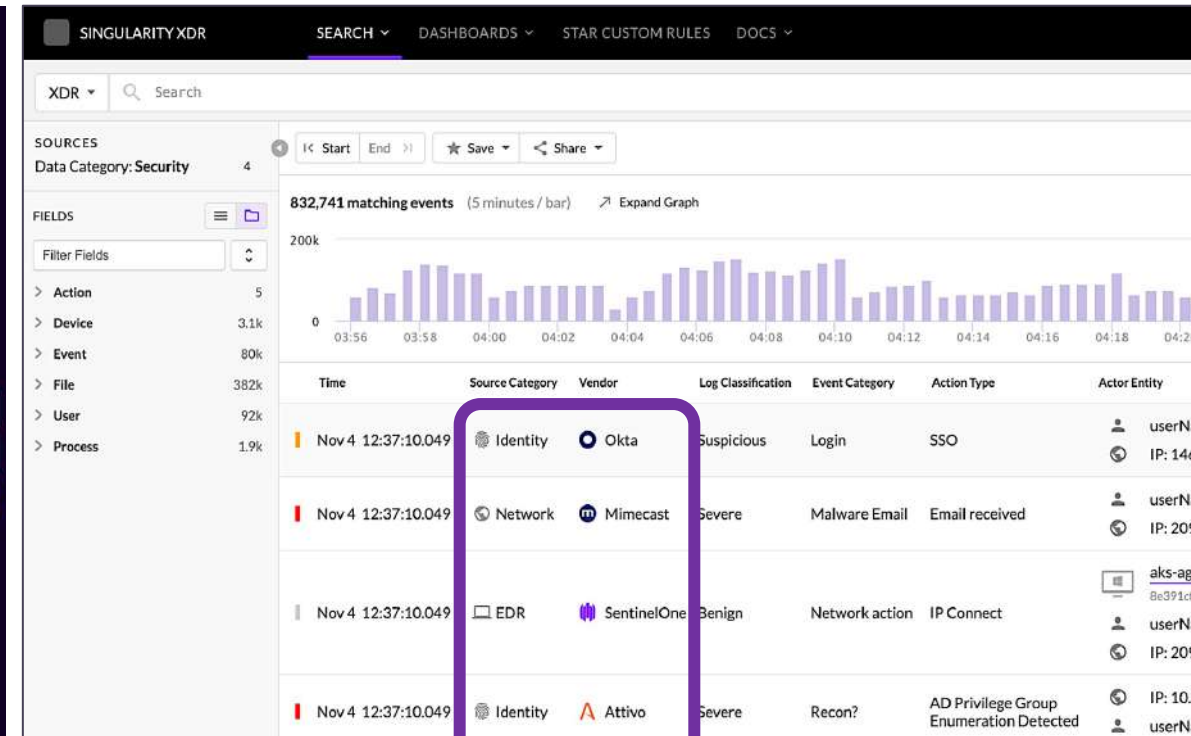
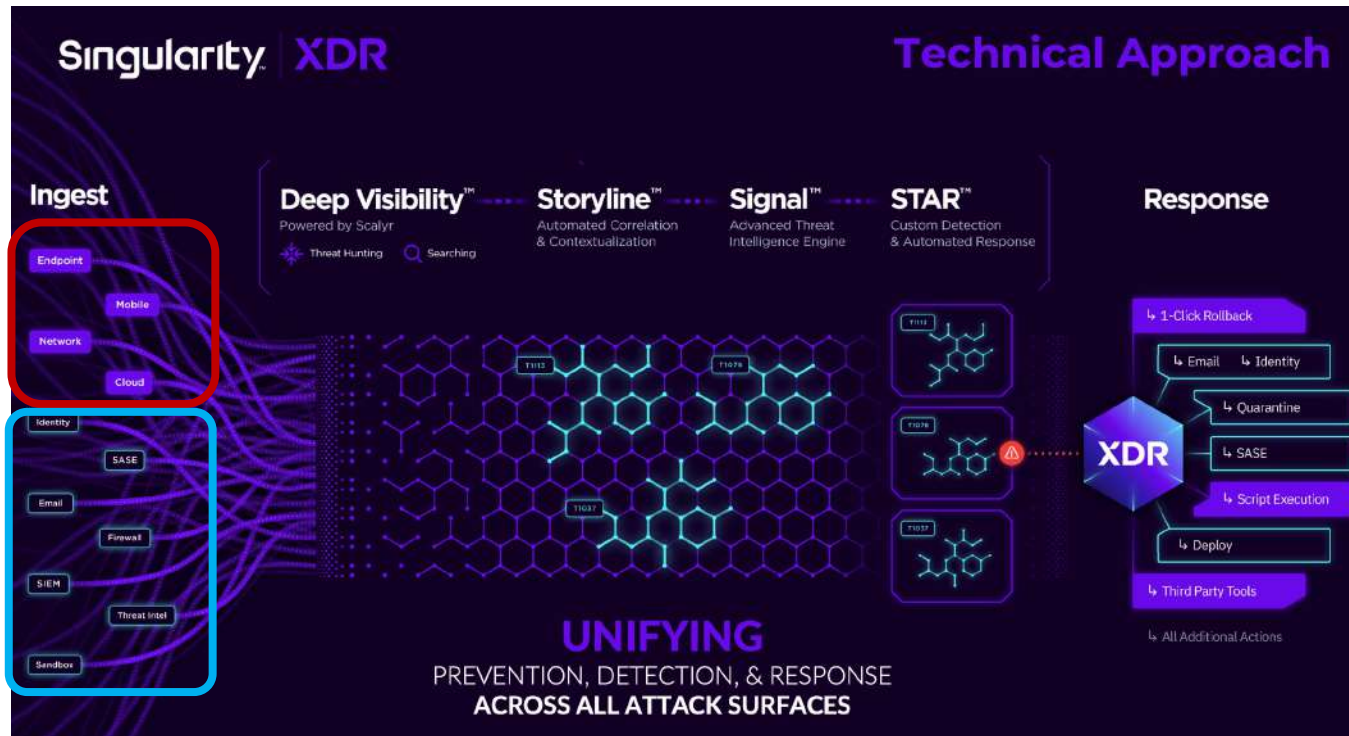
# 특징 및 트렌드

## XDR

eXtended Detection & Response



SentinelOne®





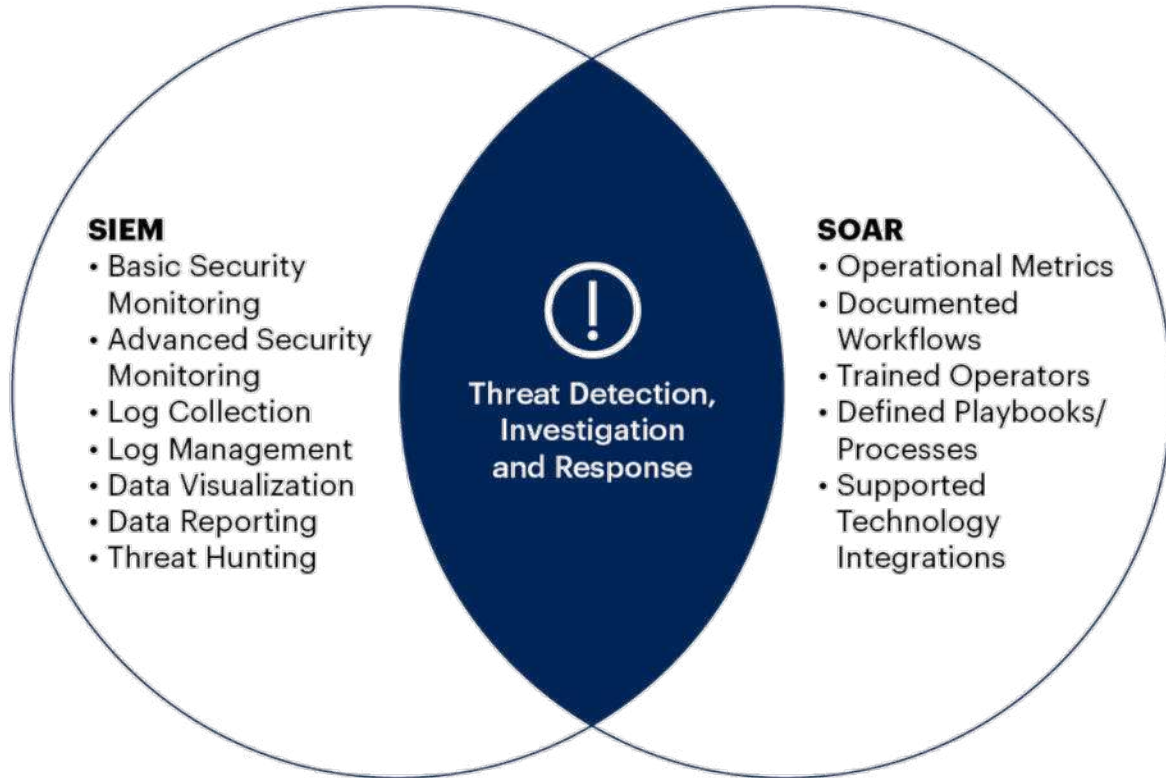
# 기술 특징.트렌드

## SOAR

Security Orchestration, Automation & Response



### Three 기술의 통합 (Gartner, 2022)



- 생산성
  - 효율성
  - 지속성
  - 시스템 연결
  - 팀. 협업
  - 프로세스화
  - 자동대응
  - 수동대응
  - 케이스. 관리
  - 에스컬레이션
- 
- 현재는 XDR 플랫폼 내부 기능과 일부 중복되기도 함

# 기술 특징.트렌드

## SOAR

Security Orchestration, Automation & Response



- 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



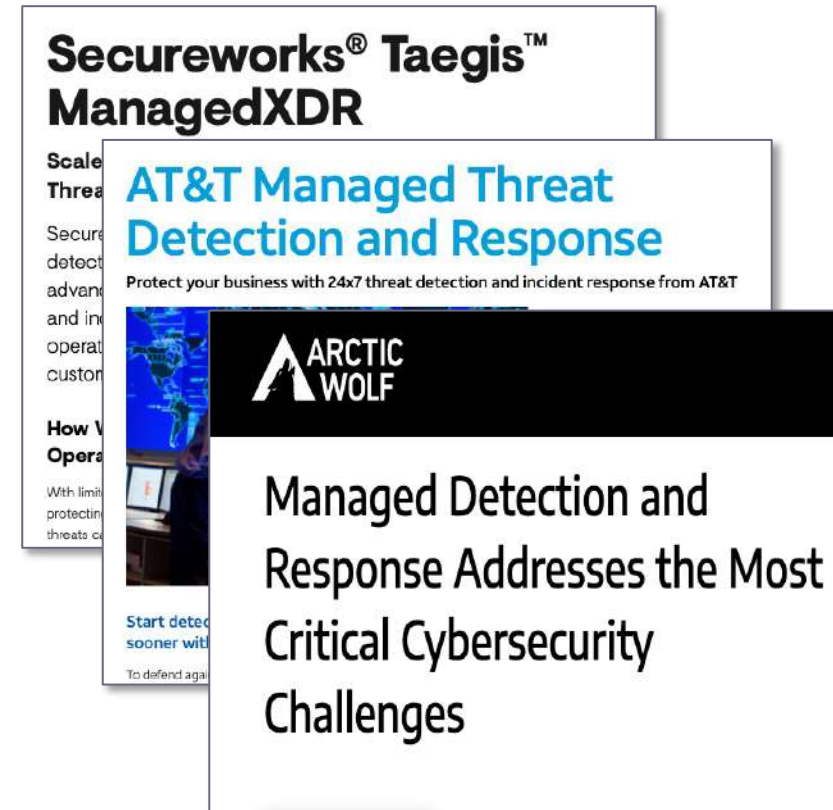
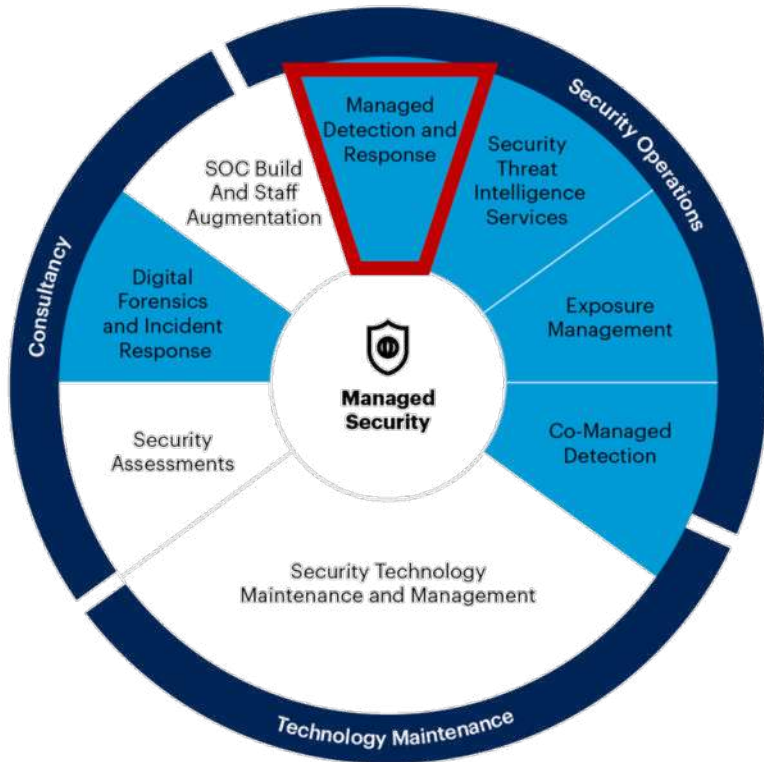
# 기술 특징.트렌드

## MDR

Managed Detection & Response



### Managed Security Service (Gartner, 2022)





# 기술 특징.트렌드



## MDR

Managed Detection & Response



## 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 Switch
- Log
- Containment
- Integration via API

고려할 사항.  
적용 쉽지 않다.  
도입 걸림돌.

전문가 관점  
프로세스 / 대응

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

# 위협 탐지 대응 솔루션

## 고려 사항

(어떻게 사용하면 좋은가?)



# PAGO DeepACT 매니지드 탐지/대응 목표

기업  
고객사

운영  
플랫폼

보호할  
정보 / 자산 / 인프라

위협  
"예방, 차단 // 탐지, 조사, 대응" 솔루션

EPP

EDR

NDR

XDR

SOAR

Threat Intelligence  
(위협 인텔리전스)

Threat Hunting  
(위협 헌팅)

Investigation  
(조사)

보안 운영팀 / 보안 기술팀 / 보안관제센터(SOC) / IR팀

능동 대응

공동 협업 체계

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

# 파고 자체 - SOAR / TI 플랫폼 구축 및 자동화

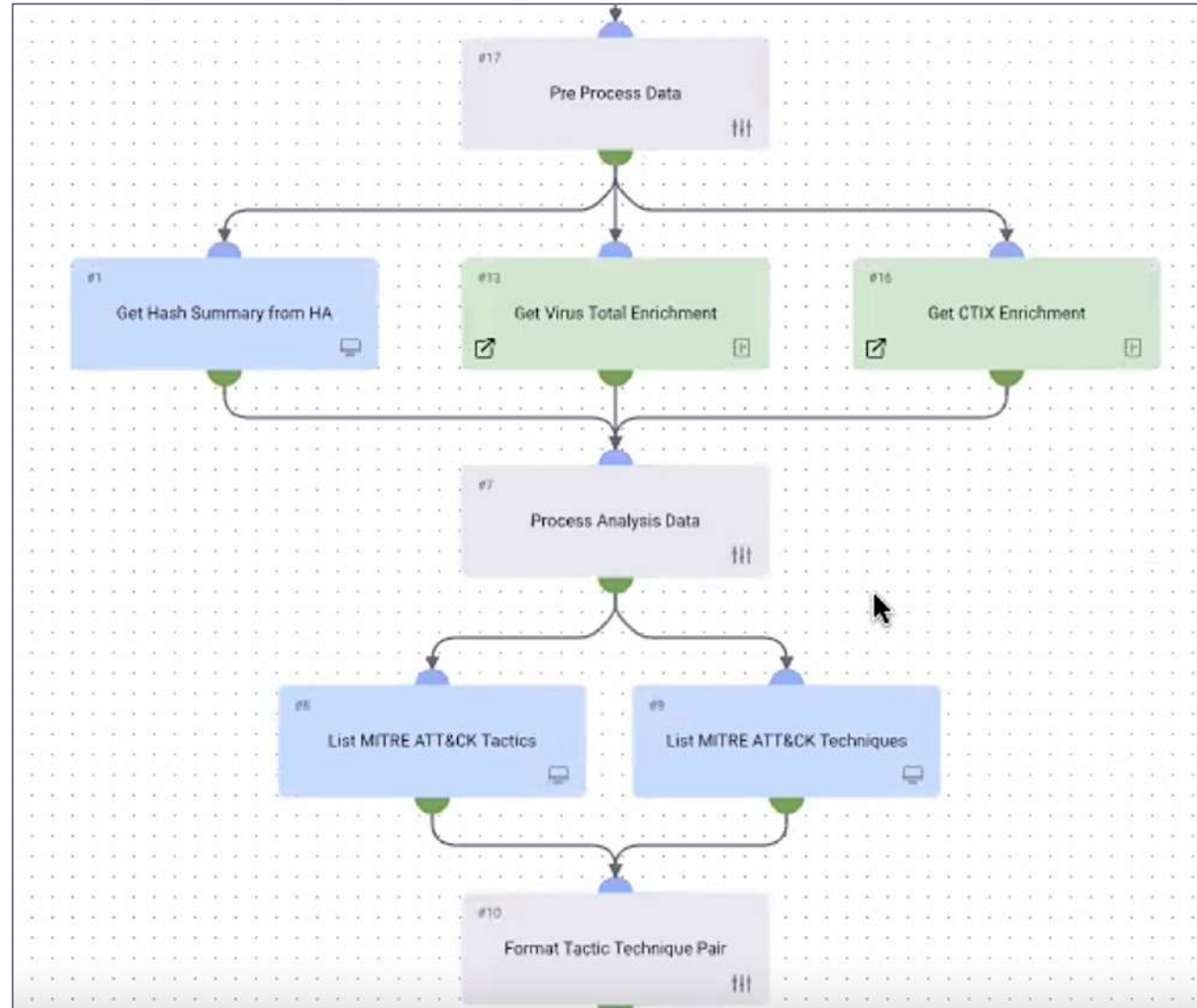
PAGO-CSOL

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

MALICIOUS

**Classifications**  
Ransomware | Wiper

**Threat Names**  
Trojan.MAC.MacRansom.K

**DYNAMIC ANALYSIS REPORT**

Created 3 days ago

tuexghs

macOS Executable

**Remarks (1/1)**

Anti-Sleep Triggered (0x0200000E): The overall sleep time of all monitored processes was truncated

Overview
Network
Behavior
Files
AV & YARA
IOCs

**VMRay Threat Identifiers (15 rules, 165 matches)**

Score	Category	Operation
5/5	Data Collection	Reads ssh keys
5/5	User Data Modification	Modifies content of user files
5/5	User Data Modification	Deletes user files
4/5	Antivirus	Malicious content was detected by he
3/5	Anti Analysis	Tries to evade debugger
3/5	Data Collection	Reads credential files of the keychain
2/5	Discovery	Checks for existence of ssh keys

MALICIOUS

**Classifications**  
Ransomware | Wiper

**Threat Names**  
Trojan.MAC.MacRansom.K

**DYNAMIC ANALYSIS REPORT**

Created 3 days ago

tuexghs

macOS Executable

**Remarks (1/1)**

Anti-Sleep Triggered (0x0200000E): The overall sleep time of all monitored processes was truncated from "1 day, 5 hours, 52 minutes, 40 seconds" to "3 seconds" to reveal dormant functionality.

Overview
Network
Behavior
Files
AV & YARA
IOCs
Environment

Filter 2771 Other Artifacts

Verdict 122 Results

Type	Value	Details Preview	Verdict	Actions
File	/Users/james/Downloads/tuexghs1	Dropped File, Binary	MALICIOUS	...
File	/Users/james/Downloads/tuexghs	Sample File, Binary	MALICIOUS	...
File	/Users/james/Library/.kp2f4H65N	Dropped File, Binary	MALICIOUS	...
File	/Users/james/Library/AppQuest/com.apple.questd	Dropped File, Binary	MALICIOUS	...
Process	tuexghs	/Users/james/Downloads/tuexghs	MALICIOUS	...



# 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

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

고객사에 즉각 공유한 결론 !!!

- 이 시스템은 랜섬웨어 공격에 계속 타겟팅되어 있는 상태이며, 취약점 점검 및 외부 통신 차단필요

**Jaden.kang** Jun 23rd at 12:28 PM

점검 결과 전달드립니다.

- 공격자의 공격 시도 정황이 포착되었으며, 백업/복구를 하지 못하도록 Commvault 서비스 종료
- CP가 공격에 사용되는 파일을 격리시켜 CP 서비스 중지, 에이전트 삭제를 시도했지만 정책에 의하여 막힘
- 에이전트는 정상 동작했으며, 모든 파일 격리 성공
- 권한 상승, 자산 스캔, 계정 탈취, 패스워드 평문 변경에 사용되는 툴부터 Lokilocker 랜섬웨어 까지 탐지된 것으로 보아 공격 시나리오가 예상 가능

**pyo.kwon** 1 day ago

ASM 보고서는 월요일 고객 유선 연락후 협의하겠습니다.

**Daniel.Choi** 14 hours ago

외부 노출 자산에 대한 조사는 방금 고객과 협의 완료하였습니다. 바로 진행하시면 될것 같습니다.

• 최근 3일 내 디바이스에서 탐지된 악성 파일 :

- PUP - 해킹툴 (Mimikatz / 각종 윈도우 계정 탈취 및 침투에 활용)
  - \\ [redacted] \c\$\NIA\mimikatz.exe
- PUP - 해킹툴 (JuicyPotato 관련 모듈 / 권한 상승 공격 툴)
  - \\ [redacted] \c\$\alock\9\ss.exe
  - \\ [redacted] \c\$\alock\SP.exe

# 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



Paul.Kwon 10:24 AM

@here

"YDark" 많이 들어보셨죠.

작년 5월 랜섬웨어 사태의 주요 악성코드입니다.

다른 시스템에도 전파될 가능성과 지속적인 우회공격 시도가 다분해 보이는군요. 고객사에 위험성을 알리는게 최우선 순위 일 것 같습니다.

AD 사용 환경이라면, 더더욱 위험하겠군요.

악성코드가 탐지/격리된 시스템의 마지막 User ID도 파악하 보세요.

# 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)

파고는 Critical 발동  
고객사 연락, 공동 대응

위험 탐지 조건별,  
ASM (Attack Surface Management)  
협의 및 수행

# 파고 DeepACT 자체 콘솔 (모든 고객사 위협 연동)



Report TIDB Administration PAUL.KWON P

Threat-Insights-Platform IOC (Indicator of Compromise)

IOC (Indicator of Compromise)

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

Show 25 entries

Classification	Category	Description
PUP	애드웨어	(도박 사이트 접속 모듈 / 112.213.118.50 통신 시도)
멀웨어	트로얀	(금융 정보 탈취 / Temp폴더에 자가복제 / 72.44.93.233 통신)
Malware	Trojan	(Lokibot / 자가복제 / rockmehard.co.uk 통신시도 / VT-63/72)
Malware	트로얀	(북한 트로얀(RAT) / 시스템 정보 수집 / 14.140.116.172 통신 시도 / by HIDDEN COBRA)
Malware	트로얀	(북한 트로얀(RAT) / msncone.exe 드롭 / 218.255.24.226 통신 시도 / by HIDDEN COBRA)
PUP	Keygen	(Techsmith Snagit 키젠 / by MESMERIZE / VT-40/72)
Malware	트로얀	(cmd132파일 및 실행 파일 드롭 / 79.134.225.71 통신 시도 / 자동 실행 등록)
멀웨어	랜섬웨어	(RaaS / 파일 암호화 / 103.28.12.103, 104.29.13.103 통신 / 파일 드롭(sdelete.exe))
Malware	트로얀	(북한 트로얀(RAT) / 자가복제 / 159.100.250.231 통신 시도 / 임베디드 셸코드 실행 / by HIDDEN COBRA)
PUP	P2P	(미투디스크 내부 모듈 / 각종 악성프로그램 다운로드 가능 / VT-2/68)
Malware	Trojan	(adobe파일로 위장 / 계정정보 탈취 / FTP(198.23.57.8) / VT-51/70)
Malware	Download	(트로얀 성향/googledrive를 이용한 암호화된 악성파일 다운로드 시도 / VT-11/72)
Malware	트로얀	(북한 트로얀(RAT) / 자가복제 / 159.100.250.231 통신 시도 / 임베디드 셸코드 실행 / by HIDDEN COBRA)



# SentinelOne 고객 - 분석가 코멘트 API 자동 연계

SENTINELS ENDPOINTS TAGS POLICY **BLACKLIST** EXCLUSIONS NETWORK CONTROL DEVICE CONTROL PACKAGES UPGRADE POLICY

All related scopes Description 열람이 X

Add new Delete selection

OS Hash Description

Win 2 [redacted] 멀웨어 - 크립토마이너 (XMRig 마이너 내부 모듈 / VT-57/69)  
 Win f [redacted] 멀웨어 - 트로얀 (Gh0st RAT 계열 / 드롭퍼 성향 / 서비스 레지스트리 등록 / C2통신(ct5.ftpvpn.info) / 추가 악성 코드 다운로드 / VT-45/52)  
 Win b [redacted] 멀웨어 - 트로얀 (Gh0st RAT 계열 / 드롭퍼 성향 / 서비스 레지스트리 등록 / C2통신(ct5.ftpvpn.info) / 추가 악성 코드 다운로드 / VT-45/52)  
 Win 2 [redacted] 멀웨어 - 웜 (트로얀 성향/Mofin계열/자가복제/문서 검색,정보탈취,MAC 주소 탈취/시스템 파일로 위장 및 시작프로그램 등록/dspyware2011@gmail/win7mailer)  
 Win 8 [redacted] 멀웨어 - 트로얀 (Powerghost 계열 / 파워셸 사용한 파일리스 공격 / DDoS 및 WannaMine 마이닝 공격 수행 / VT-Unknown)  
 Win 2 [redacted] 멀웨어 - 다운로더 (악성행위에 필요한 모듈 다운로드 파워셸 / C2서버(107.148.239.111:80) / VT-Unknown)  
 Win 8 [redacted] 멀웨어 - 트로얀 (Powerghost 계열 / 파워셸 사용한 파일리스 공격 / DDoS 및 WannaMine 마이닝 공격 수행 / VT-Unknown)  
 Win 0 [redacted] 멀웨어 - 랜섬웨어 (매그니베르 랜섬웨어 / 파일 암호화)  
 Win 2 [redacted] 멀웨어 - 랜섬웨어 (매그니베르 랜섬웨어 / 파일 암호화)

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

Powered by Stellar Cyber®

이벤트 경고 시각화 조사 대응 시스템

Full-screen Share Clone Edit

dstip: [redacted]

+ Add filter

220616-Traffic

Count

timestamp per 30 seconds

dstip

dstip: Descending	Count
17[redacted]0	1,229
17[redacted]30	386
17[redacted]	278
17[redacted]	32
17[redacted]90	15

Export: Raw Formatted

comment

- 어제 오후 시간대에 특정 서버/PC 인터넷이 갑자기 느려짐 - 서버/PC Net : 17[redacted]0/24
  - 1[redacted]4 대역 시간 특정 (220616-15:00 ~ 220617-18:00)
- 1.Victim 서버/PC 찾기
  - 1[redacted]
- 2.어떤 트래픽이 유입 되었는지 확인
  - icmp
- 3.어떤 공격 유형인지 추정해보기
  - Ping of Deatch [기본적인 ping(64bytes) 보다 크게 만들어(1440bytes) 전송 Dos공격의 일종]
- 4.대응 방안 생각해보기
  - [redacted]

srcip

srcip: Descending	Count
1[redacted]55	1

app

netbios-dgm

특정 상황 별, 즉각적인 커스텀 대쉬보드 생성 및 고객과 공유

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

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

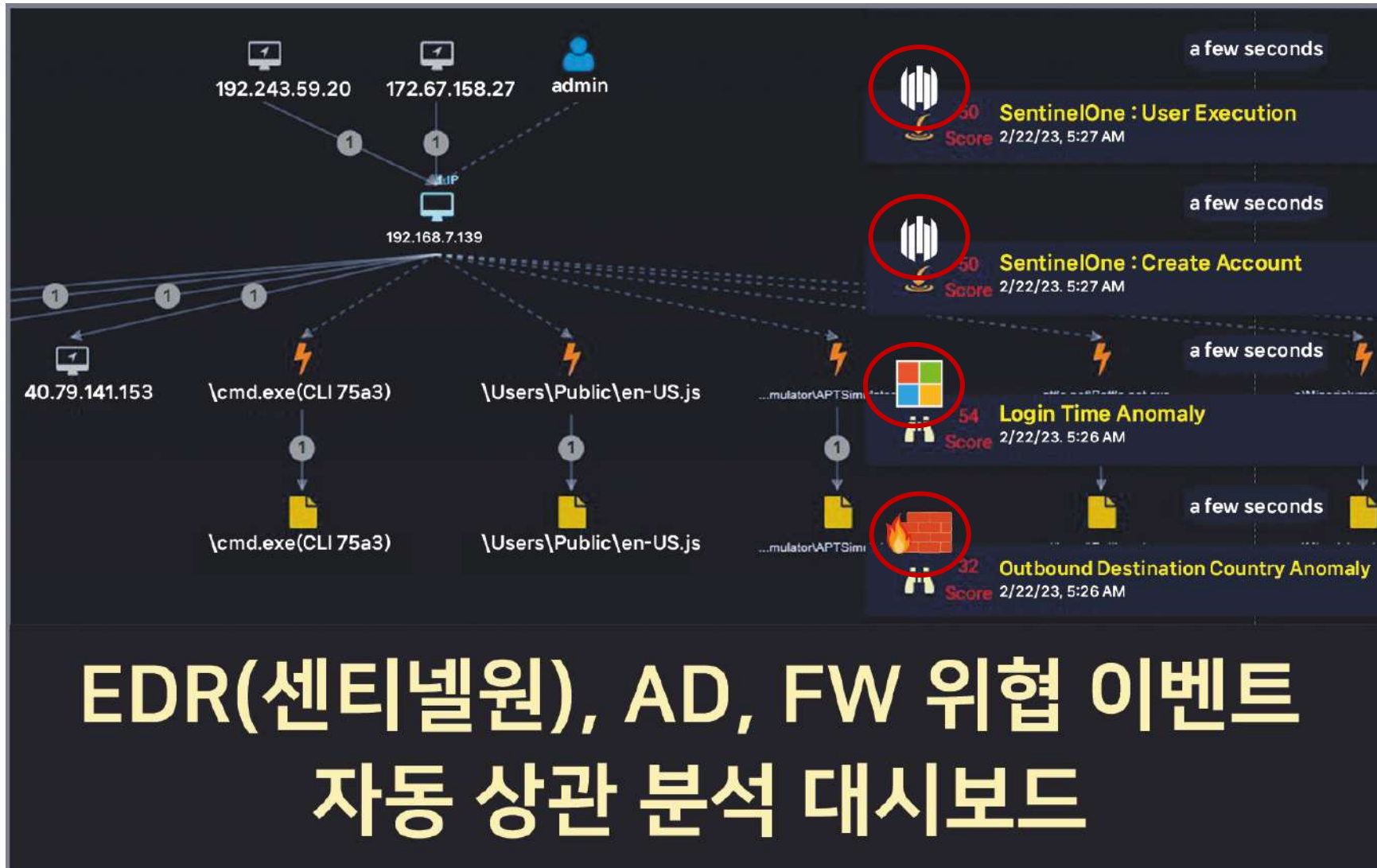
# Stellar Cyber XDR 고객 - 커스텀 대쉬보드



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

위협 케이스 별, 커스텀 대시보드 생성 지속적인 업데이트 및 모니터링

# 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





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](mailto:sales@PAGOnetworks.com)

기술 문의 : [tech@PAGOnetworks.com](mailto:tech@PAGOnetworks.com)