



STELLAR  
CYBER®

# Ai를 통한 보안분석체계 강화 및 제로트러스트 환경 구축

## 차세대 보안분석/관제

왕정석 지사장 (JS Wang)  
Korea Country Manager  
[jswang@stellarcyber.ai](mailto:jswang@stellarcyber.ai)  
+82-10-8629-4418

[WWW.STELLARCYBER.AI](http://WWW.STELLARCYBER.AI)

Making Security  
Operations Simpler



# Open XDR Security Platform

솔루션 기반 대처에서 플랫폼 기반의 분석/대응으로 진화

**X (eXtended)**



다양한 장비, 보안기술 및 위협 인텔리전스(TI)와 연동하여 확장된 기술 연동을 통해 최대한 많은 정보를 수집

**D (Detection)**



수집된 정보를 기반으로 머신러닝(M/L), AI 등의 최신 기술을 이용하여 연관관계를 분석하여 보안 위협을 탐지

**R (Response)**



SOAR 기능 등을 통해 탐지/분석된 보안위협에 대해 즉각적인 대응을 수행

# XDR 플랫폼을 통한 가시성 확보 및 분석



# 스텔라사이버의 자동 위협 탐지 및 대응 플랫폼



## 1. 다양한 정보 수집

## 2. 정보의 정규화 및 강화

## 3. 공격별 특화된 ML로 탐지

## 4. 탐지된 각 공격의 상관관계 분석 및 위협도 점수

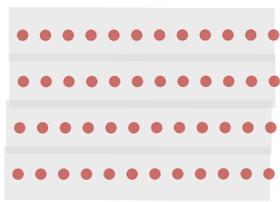
## 5. 다양한 솔루션과 연동하여 자동 / 반자동 위협 대응

### AI + ML의 보안 이벤트 분석

- 이벤트별 상관관계 분석
- 자산의 위협도 분석
- 위협도 + 신뢰도 + TI 점수에 따른 이벤트 위협 점수
- 사이버 킬체인 대시보드에 분류

### AI / ML에 의한 탐지

- 사이버 킬체인
- MITRE ATT&CK
- 서버/유저/트래픽 행위
- 탐지 정확도 극대화



16개의  
TI 평판 조회

공인 IP주소  
위치 조회

자산 정보  
분석

네트워크



엔드포인트



스텔라 NDR

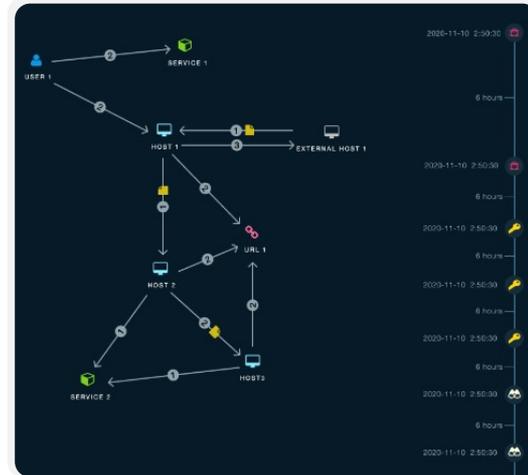
- 4300+ 프로토콜 분석
- 45만+ IDS 시그니처



사용자인증



클라우드



now.

Jira



Active Directory



NG-SIEM



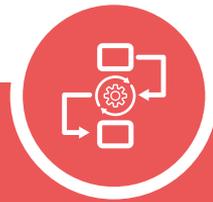
Threat  
Intel



NDR



IDS &  
Malware  
Analysis



SOAR



Open XDR Platform

Making Security  
Operations Simpler



## 제로 트러스트 구축 – 어디까지 어떻게?

- 제로 트러스트 네트워크 환경 구축
- 국내외 지사, 재택/원격 근무에 대한 모니터링 체계 구축
- 내부 감염 전파, 공격 확산에 대한 보안

# 피어 연결의 어려움

UnTrusted Zone



SaaS



Public Cloud

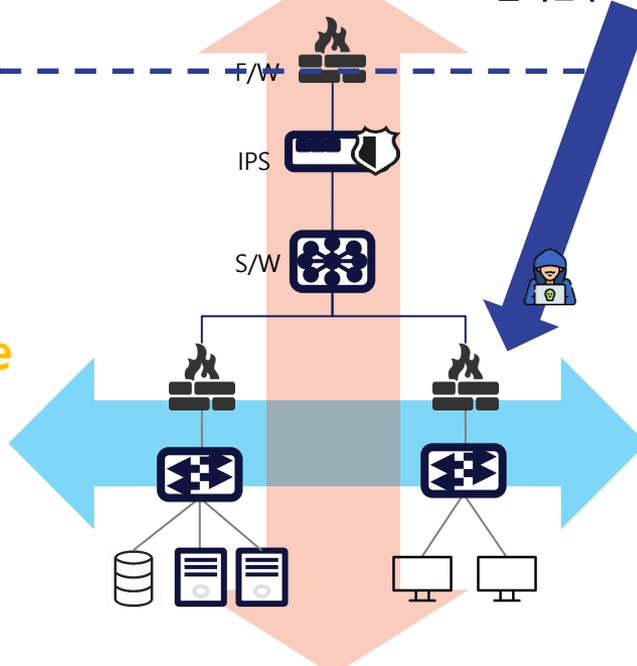


원격근무



IoT, BYOD

UnTrusted Zone



Never Trust, Always Verify!  
신뢰하지 말고 항상 검증하라

# 제로트러스트 도입을 위한 6가지 핵심 요소



 **Identities (식별자/신원)** – 식별자 관리, 인증, 위험도 평가, 가시성 및 분석, 자동화 및 통합

 **Devices (기기 및 엔드포인트)** – 정책 준수 모니터링, 데이터 접근제어, 자산 관리, 가시성 및 분석, 자동화 및 통합

 **Applications (응용 및 워크로드)** – 접근인가, 위협보호, 접근성, 응용보안, 가시성 및 분석, 자동화 및 통합

 **Data (데이터)** – 데이터 목록관리, 접근 결정방법, 암호화, 가시성 및 분석, 자동화 및 통합

 **Infrastructure (시스템)** – 접근통제, 시스템 계정관리, 시스템 보안 및 정책관리, 가시성 및 분석, 자동화 및 통합

 **Network (네트워크)** – 네트워크 세분화, 위협 대응, 암호화, 가시성 및 분석, 자동화 및 통합

# 제로트러스트 도입을 위한 6가지 핵심 요소



 **Identities (식별자/신원)** – 식별자 관리, 인증, 위험도 평가, 가시성 및 분석, 자동화 및 통합

 **Devices (기기 및 엔드포인트)** – 정책 준수 모니터링, 데이터 접근제어, 자산 관리, 가시성 및 분석, 자동화 및 통합

 **Applications (응용 및 워크로드)** – 접근인가, 위협보호, 접근성, 응용보안, 가시성 및 분석, 자동화 및 통합

 **Data (데이터)** – 데이터 목록관리, 접근 결정방법, 암호화, 가시성 및 분석, 자동화 및 통합

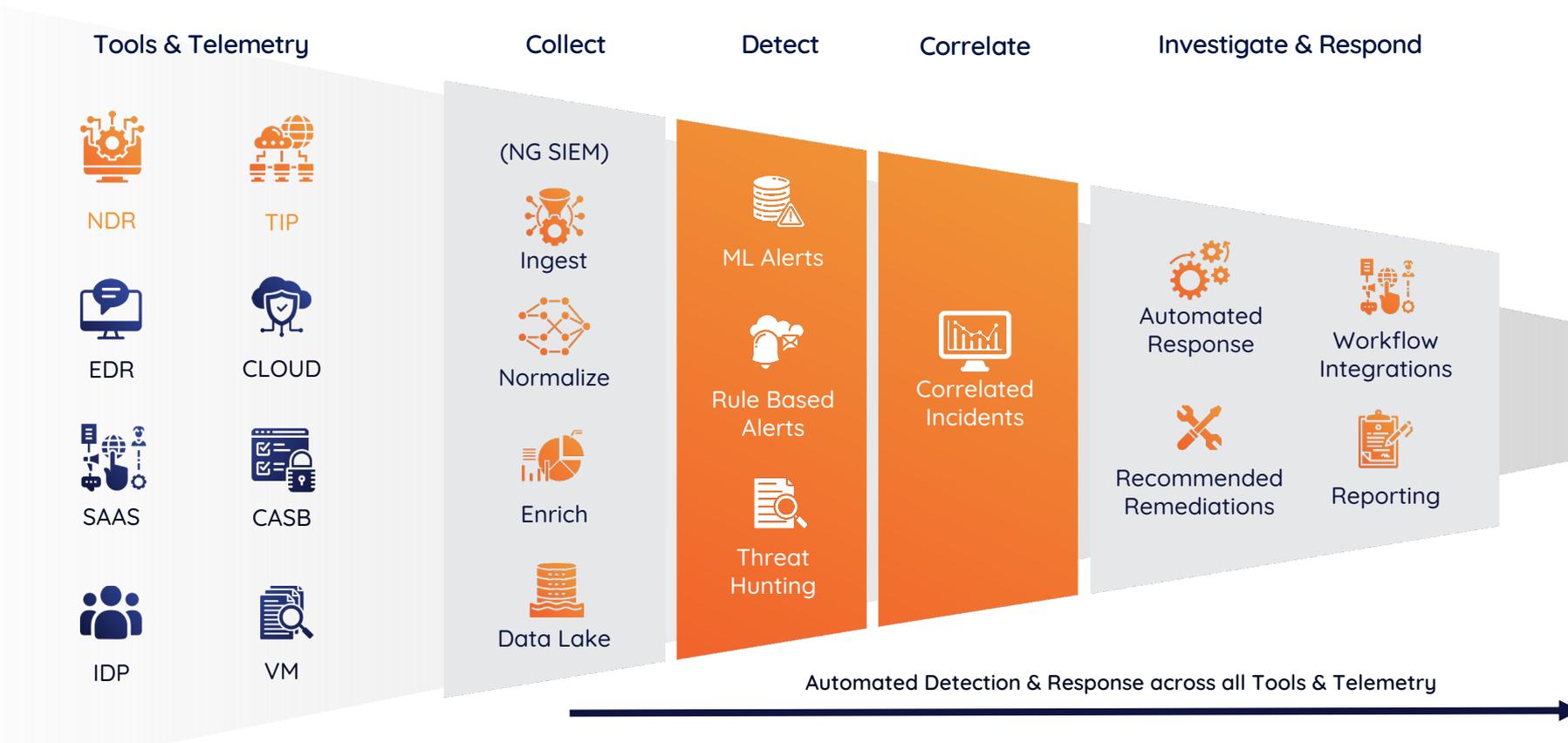
 **Infrastructure (시스템)** – 접근통제, 시스템 계정관리, 시스템 보안 및 정책관리, 가시성 및 분석, 자동화 및 통합

 **Network (네트워크)** – 네트워크 세분화, 위협 대응, 암호화, 가시성 및 분석, 자동화 및 통합

# Single Platform and Single License for Security Operations



Native Components to Stellar Cyber's Open XDR Platform



## 머신러닝을 통한 사용자 행위 분석

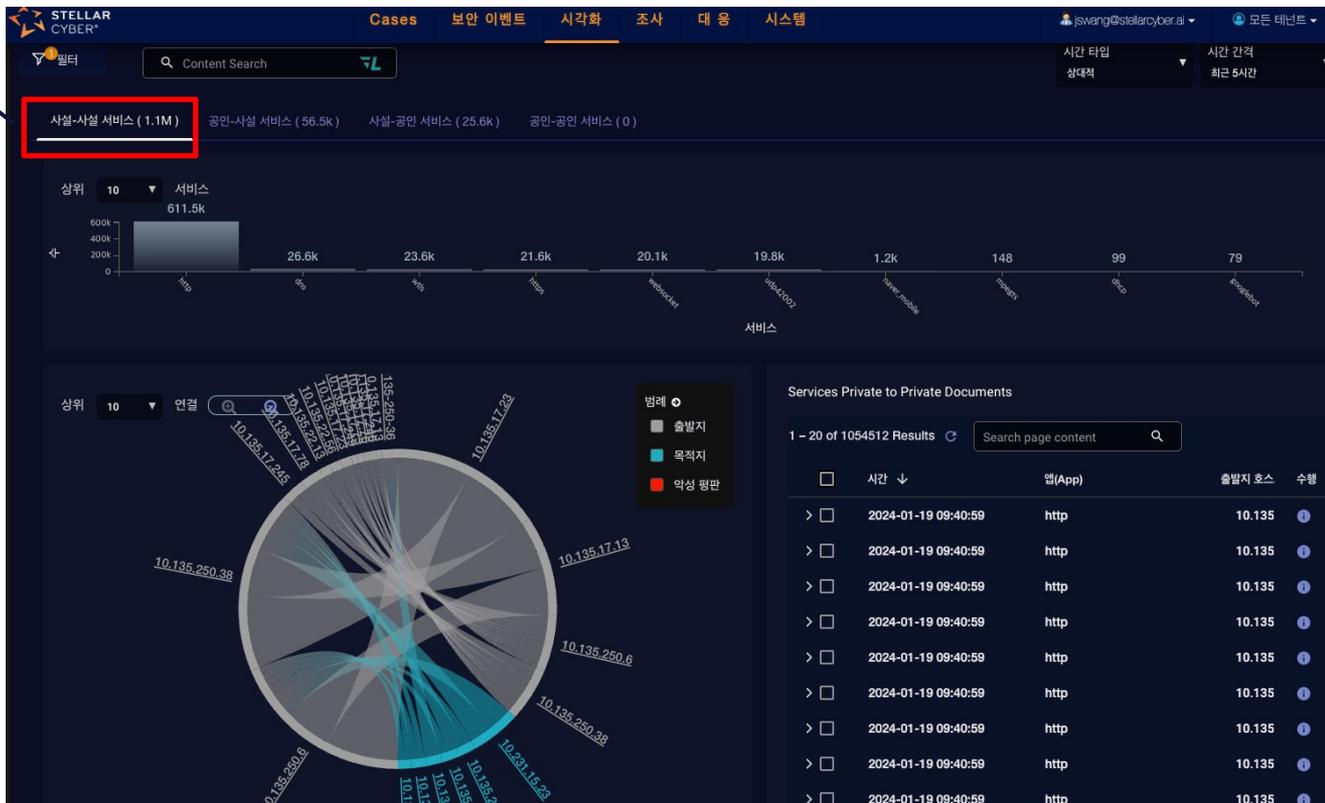
실제 상황	사용자의 접속 행위 발생 시, 모든 접속 및 이후 행위에 대한 학습 수행. 로그인 시간 및 위치의 변화, 트래픽 사용 패턴 등에 대한 이상행위 탐지를 통해 계정 정보 유출, 접속 보안 체계에 대한 관리 수행
상관분석 매트릭스	NTA, UBA, VPN, Windows Agent, 지리 정보
실제 경보 결과 (사례)	 <p>미국 버지니아에서 두번째 로그인 시도</p> <p>독일 프랑크푸르트에서 처음 로그인 시도</p>

# 업무망, 연계망에 대한 가시성 확보

## 사설, 외부 망 통신

- 내부망 시스템의 외부 통신 여부
- 망 내 트래픽 종류와 비 인가 트래픽 여부
- 내부망 자산에 대한 지속적인 모니터링

가시성 및  
증적자료 확보

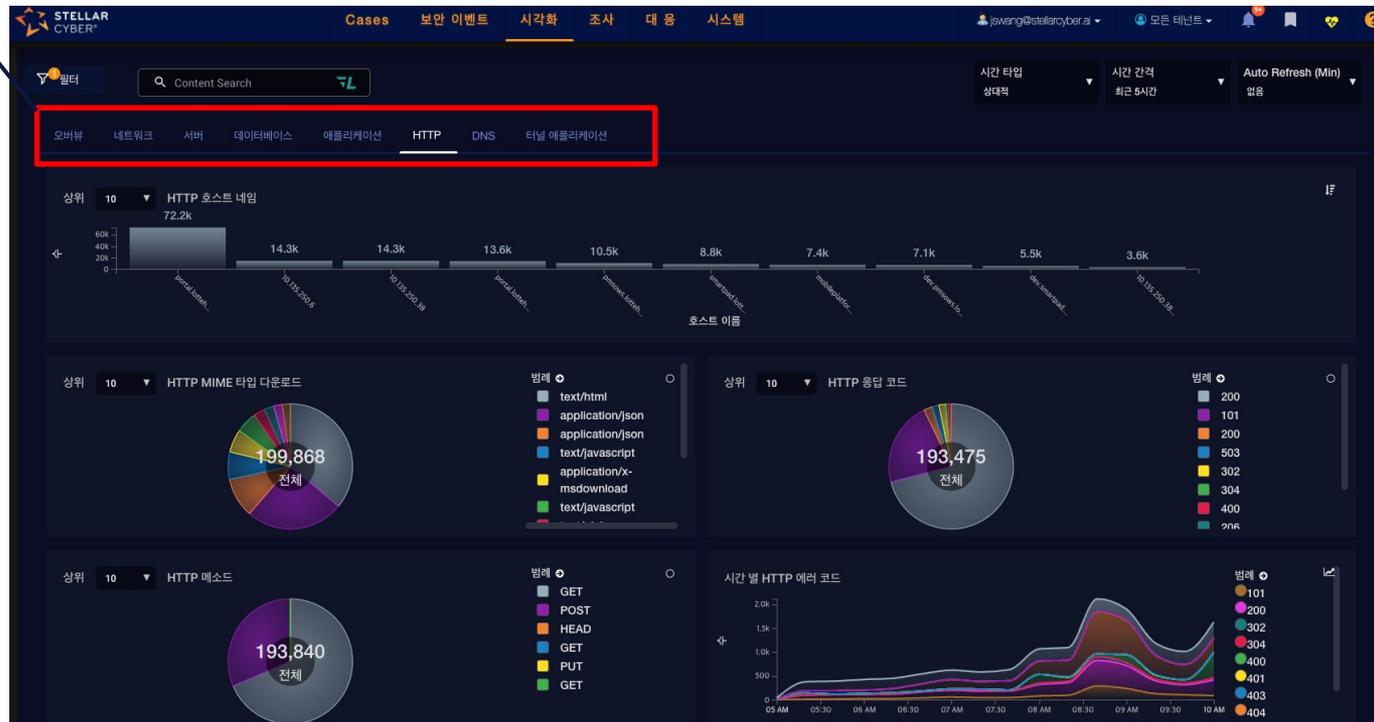


# 업무망, 연계망에 대한 가시성 확보

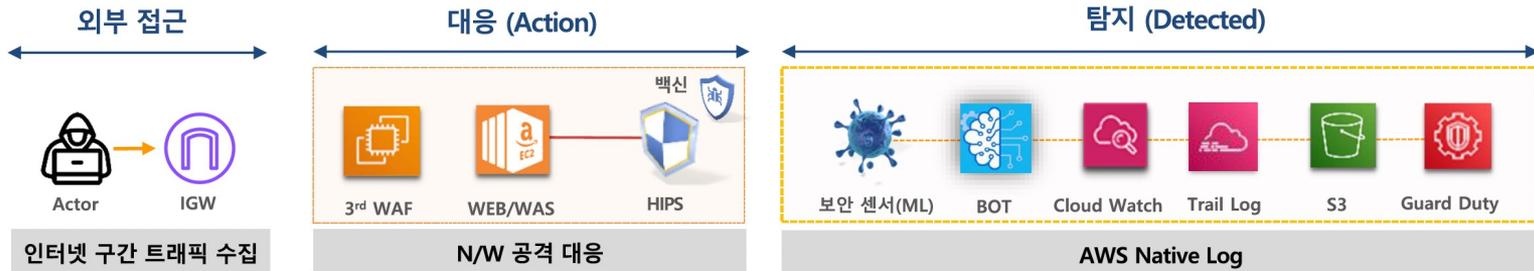
## 서비스 모니터링

- 각 어플리케이션 서비스 상태 확인
- 주요 서비스 변화 감시
- 서버 자산에 대한 지속적인 모니터링

공격 및 장애 현황에  
대한 데이터 확보



# 클라우드 서비스 관제 및 가시성 확보



클라우드 환경 연계 분석

AI 기반 위협 탐지

인터넷 구간 트래픽 탐지

## 통합 수집 관리(XDR)



광범위 데이터를 수집하여 연계 분석을 통해 실제적인 보안 위협 탐지

XDR 동작

광범위 데이터 수집

빅데이터 프로세싱

위협 이벤트 탐지

인공지능 (AI)

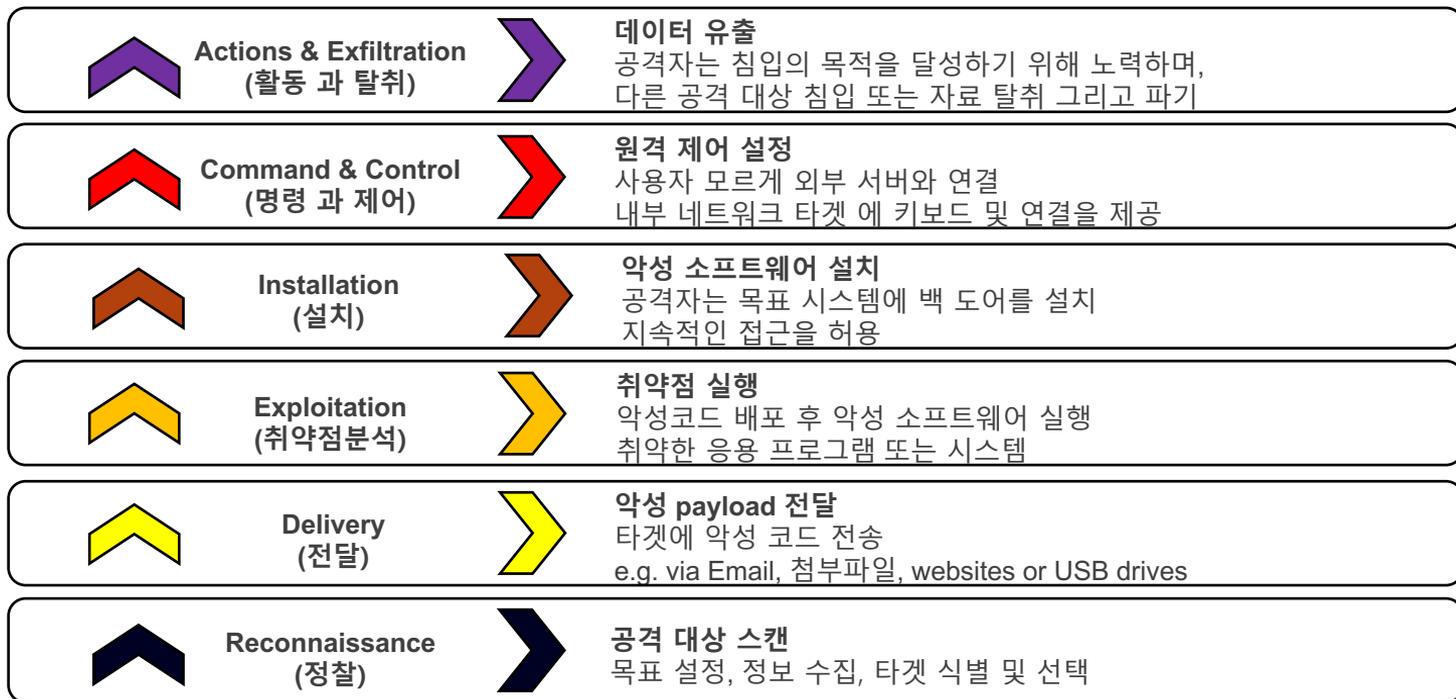
인시던트 생성

# AI 보안 분석 체계 대응

- AI에 대한 보안 이벤트 탐지 이후의 분석 체계로의 확대 적용

# 사이버 시큐리티 킬체인

사이버 공격을 프로세스 상으로 분석해 각 공격 단계에서 조직에게 가해지는 위협 요소들을 파악하고, 공격자의 목적과 의도, 활동을 분쇄, 완화시켜 조직의 회복탄력성을 확보하는 전략



## Adversarial Tactics, Techniques & Common Knowledge(적대적인 전술/기술 & 일반 지식)

특정 플랫폼에 한정하지 않고, PC에서부터 모바일, 서버, 클라우드 시스템까지 광범위한 사이버 보안 분류 기술을 통해 공격행위 전반을 단계별로 분류하고, 각 단계 별 탐지 기술 및 방어 전략을 제공.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Supply Chain Compromise	Control Panel Items Service Execution	Security Support Provider	Access Token Manipulation	Access Token Manipulation	Input Capture	Password Policy (T1056) Score: 5	Logon Scripts	Input Capture	Domain Fronting	Data Compressed	Endpoint Denial of Service
Drive-by Compromise	PowerShell	AppCert DLLs	Extra Window Memory Injection	Control Panel Items	Credential Dumping	Metadata: Applicable to: client endpoints -Detection score: 4 -Overlay: Detection	Pass the Hash	Data from Network Shared Drive	Uncommonly Used Port	Data Encrypted	Network Denial of Service
Spearphishing Attachment	Regsvr32	Logon Scripts	Process Injection	Extra Window Memory Injection	Credentials in Registry		Application Deployment Software	Email Collection	Remote Access Tools	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
Exploit Public-Facing Application	Rundll32	Image File Execution Options Injection	Process Injection	Masquerading	LLMNR/NBT-NS Poisoning and Relay	System Owner/User Discovery	Distributed Component Object Model	Audio Capture	Commonly Used Port		
External Remote Services	Scripting	AppCert.DLLs	Process Injection	Process Injection				Automated Collection	Data Obfuscation	Automated Exfiltration	Data Destruction
Hardware Additions	Scheduled Task	Application Shimming	Image File Execution Options Injection	Regsvr32	Account Manipulation	Account Discovery	Exploitation of Remote Services	Clipboard Data	Standard Application Layer Protocol	Size Limits	Defacement
Replication Through Removable Media	User Execution	Scheduled Task	Image File Execution Options Injection	Rundll32	Brute Force	Process Discovery	Pass the Ticket	Data from Information Repositories	Communication Through Removable Media	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Link	CMSTP	Accessibility Features	Application Shimming	Scripting	Credentials in Files	System Network Configuration Discovery	Remote Desktop Protocol	Data from Local System	Custom Contr	Exfiltration Over Other Protocol	Disk Structure Wipe
Spearphishing via Service	Command-Line Interface	Account Manipulation	Application Shimming	Image File Execution Options Injection	Exploitation for Credential Access	Application Window Discovery	Remote File Copy	Data from Removable Media	Man in the Browser	Screen Capture	Firmware Corruption
Trusted Relationship	Compiled HTML File	Appinit DLLs	Scheduled Task	Timestomp	Forced Authentication	Browser Bookmark Discovery	Replication Through Removable Media	Data Staged	Data		
Valid Accounts	Dynamic Data Exchange	Authentication Package	Accessibility Features	Obfuscated Files or Information	Hooking	Domain Trust Discovery	Network Service Scanning	Video Capture	File and Directory Discovery		
	Execution through API	BITS Jobs	Appinit DLLs	Binary Padding	Input Prompt	File and Directory Discovery	Network Share Discovery		Network Service Scanning		
	Execution through Module Load	Bootkit	Bypass User Account Control	Bypass User Account Control	Kerberoasting	Network Service Scanning	Shared Webroot		Network Sniffing		
	Exploitation for Client Execution	Browser Extensions	DLL Search Order Hijacking	Code Signing	Network Sniffing	Network Sniffing	Taint Shared Content		Peripheral Device Discovery		
	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Compile After Delivery	Password Filter DLL	Private Keys					
	Component	Firmware	Compiled HTML File	Compiled HTML File							
	InstallUtil										

**legend**

- #f9cece Tech. ref. for 1 group
- #f90000 Tech. ref. for 1 groups
- #ff8f00 Tech. in group + detection
- #bbc34a Tech. in detection

## ■ 스텔라사이버 Machine Learning Model

- Supervised M/L (지도학습)
  - 사전에 정의된 Label 및 유사도를 기준으로 학습 및 탐지 수행
- Unsupervised M/L
  - 입력되는 데이터를 기준으로 학습하여 패턴을 찾고 그에 대한 비정상적 편차를 학습하여 탐지 수행
- 세분화된 머신러닝 탐지 모델
  - 각각의 탐지 맞게 학습범위 및 내용이 세분화된 탐지 모델을 사용 -> **오탐 감소**
- 머신러닝 기반 인시던트 상관관계 분석
- 자산 분류 및 시각화 제공

Detection Name	Detection Name	Detection Name	Detection Name
비정상 상위/하위 프로세스	DNS 터널링 이상	프로토콜 계층 로그인 실패 비정상	비정상적인 SQL
계정 로그인 실패 비정상	파일 수정 이상	공인-공인 취약점 공격	흔하지 않은 어플리케이션 비정상
여카운트 MFA 로그인 실패 비정상	파일 생성 이상	RDP Brute Force 공격	흔하지 않은 프로세스 비정상
센서에서 수집 한 비정상적인 데이터 양	비정상 방화벽 차단	RDP Outbytes 비정상	URL 정보수집 이상
애플리케이션 사용 비정상	방화벽 정책 비정상	스캐너 동작 이상	사용자 에이전트 비정상
악성 목적지 평판 비정상	불가능한 왕래 비정상	스캐너 평판 이상	비정상 사용자 애플리케이션 사용
악성 출발지 평판 비정상 행위	IP / 포트 스캔 이상	센서 상태 비정상	사용자 자산 접근 비정상
Carbon BlackXDR Anomaly	로그인 시간 비정상	SMB 읽기 비정상	사용자 데이터 볼륨 비정상
C&C 평판 비정상	장시간 웹 세션 비정상	SMB 쓰기 비정상	사용자 로그인 실패 비정상
커맨드 이상	Mimikatz DCSync	비정상적인 SQL	사용자 로그인 위치 비정상
크리덴셜 스텔링	비표준 포트 비정상	흔하지 않은 어플리케이션 비정상	사용자 프로세스 사용 이상
CylanceOPTICS:XDR Anomaly	아웃바운드 목적지 국가 비정상	흔하지 않은 프로세스 비정상	웹방화벽 정책 위반 비정상
데이터 수집량 비정상	기형 아웃바이트	URL 정보수집 이상	
	프로세스 이상		

< 스텔라사이버 머신러닝 탐지 모델 >



## 사용자의 비정상 행위 탐지

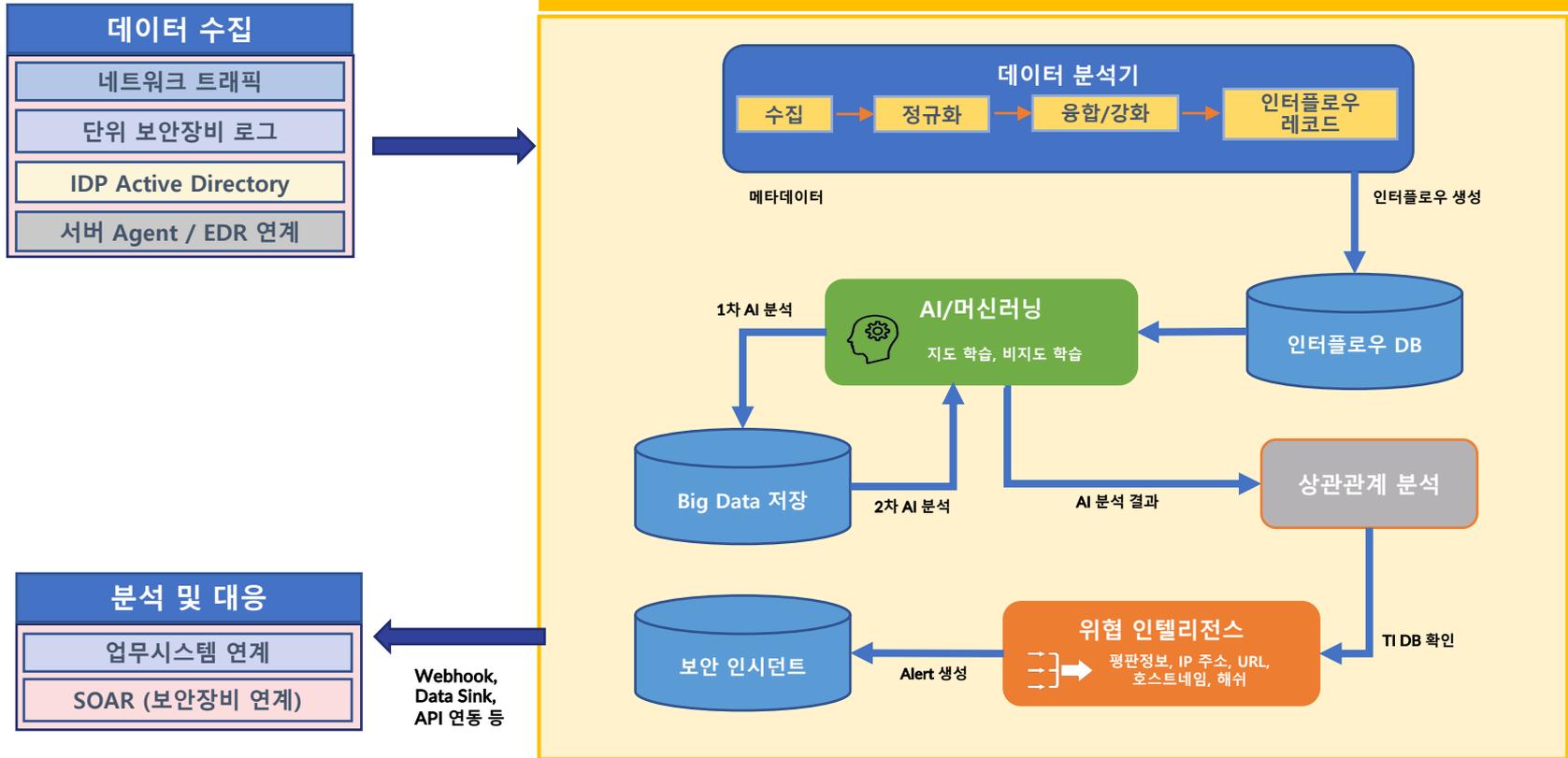
- 시스템 로그 및 다양한 보안 솔루션의 로그와 연관 분석을 통한 행위 탐지
- 별도의 룰이나 정책 없이 자동화된 위협 기준 수립
- 비정상적인 로그인 시도/어플리케이션 사용/트래픽 증가 등의 사용자 이상 행위 탐지



## 사용자 및 시스템간 연관성 분석

- 다수의 사용자PC, 업무 시스템 간 연관 분석을 통해 보안 리스크 정보 제공
- 중요 정보의 이동 경로 및 제공자, 수신자 등의 가시성 확보
- 감염된 PC를 통한 내부 시스템 감염 경로 추적

# 스텔라사이버 데이터 학습 및 강화 아키텍처



# 차세대 AI의 방향?



- Machine Learning / AI 적용
  - 보안 이벤트 탐지 / Short term analysis 레벨
  - 상관관계 분석 / Long term analysis 레벨
  - UI 및 사용자(관리자) 표현 레벨

Help Version: 4.3.x ▾ Quick Start Support ↗ Alert Coverage ↗ Learning Portal ↗ Product Roadmap

Welcome to the Stellar Cyber Knowledge Base

A screenshot of the Stellar Cyber Chat interface. At the top, it says "Stellar Cyber Chat" and "Powered by GPT". Below that is a prompt "Ask anything or try an example". There are three example questions in grey boxes: "What is DNS Tunneling?", "How do I assign a Windows agent sensor to a tenant?", and "What are XDR kill chain stages?". Below these is a disclaimer: "AI Chat is powered by GPT. Inaccurate info is possible. Please check responses." At the bottom, there is a text input field with the placeholder "Type a new question" and a blue arrow button. A footer note says "Sessions are currently limited to 0 questions per day." The interface is enclosed in a white box with a close button (X) in the top right corner.

Stellar Cyber Chat  
Powered by GPT

Ask anything or try an example

What is DNS Tunneling?

How do I assign a Windows agent sensor to a tenant?

What are XDR kill chain stages?

AI Chat is powered by GPT. Inaccurate info is possible.  
Please check responses.

Type a new question

Sessions are currently limited to 0 questions per day.

# 스텔라사이버 오픈 XDR 도입효과



## 전체 보호 공격 표면

바로 사용할 수 있는 위협 탐지  
기능으로 온프레미스, 클라우드,  
IT/OT 환경에 대한 위협을 식별



## 보안 운영 향상 성능 향상

MTTD를 8배 이상, MTTR을 20배  
이상 개선.  
직원들은 가장 잘하는 일에만 집중  
하고 나머지는 AI 기반 자동화가  
처리



## 비용 절감과 동시에 보안 운영 간소화

유연한 배포 옵션과 개방형 접근  
방식이 결합된 유연한 배포 옵션  
으로 고객이 투자 전략을 제어할  
수 있음



Making Security  
Operations Simpler

감사합니다.

왕정석 지사장 (JS Wang)  
Korea Country Manager  
[jswang@stellarcyber.ai](mailto:jswang@stellarcyber.ai)  
+82-10-8629-4418

[WWW.STELLARCYBER.AI](http://WWW.STELLARCYBER.AI)