



# Why Cloud SIEM?

| ISEC 2024 x Logpresso |



# Hybrid Environment



**On-premises**



**Public Cloud**



**SaaS**

# Requirements



**Threat Detection and Incident Response**

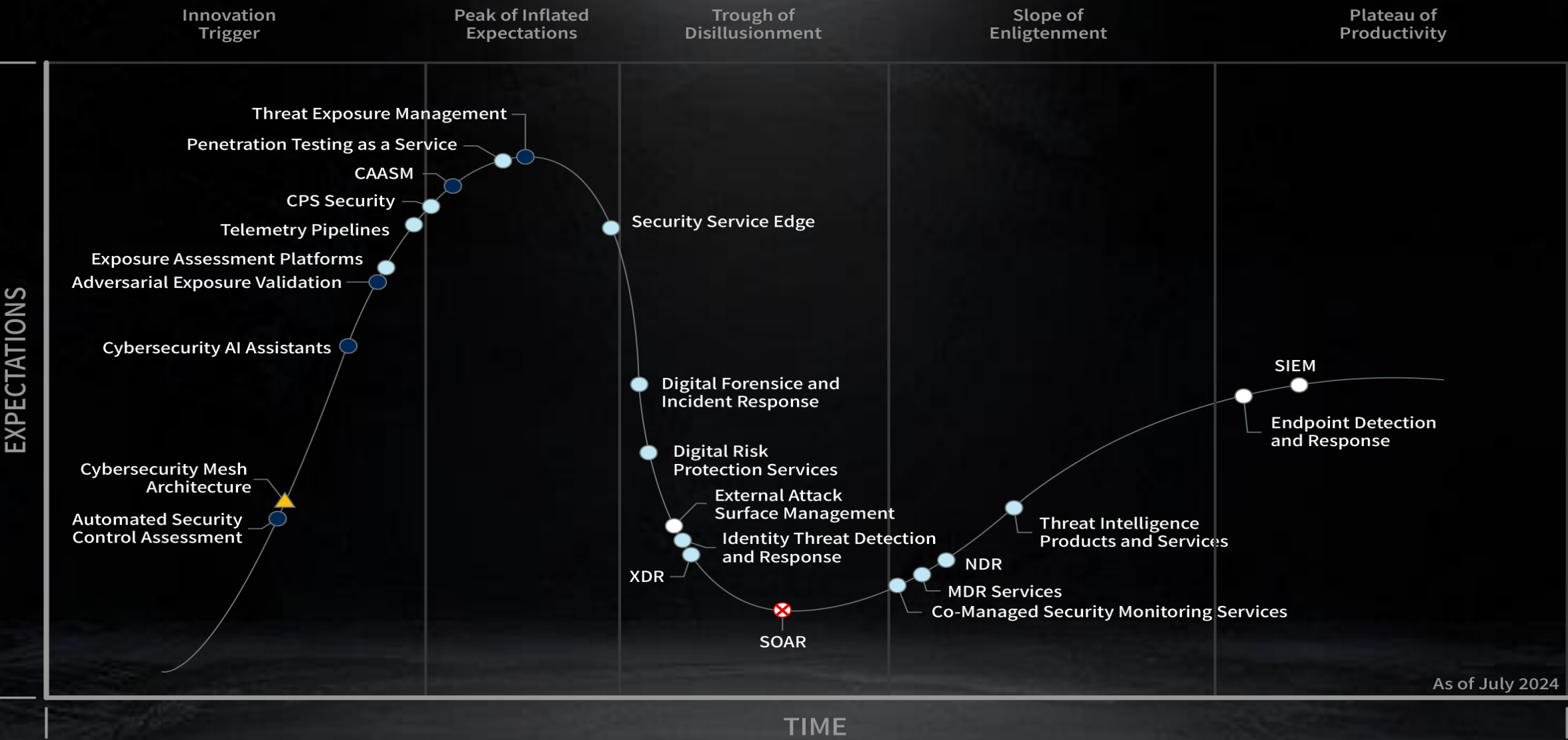


**Complete Visibility**



**Meet Compliances and Regulations**

# Hype Cycle for Security Operations 2024



# Legacy SIEM



**Hard to Integrate**

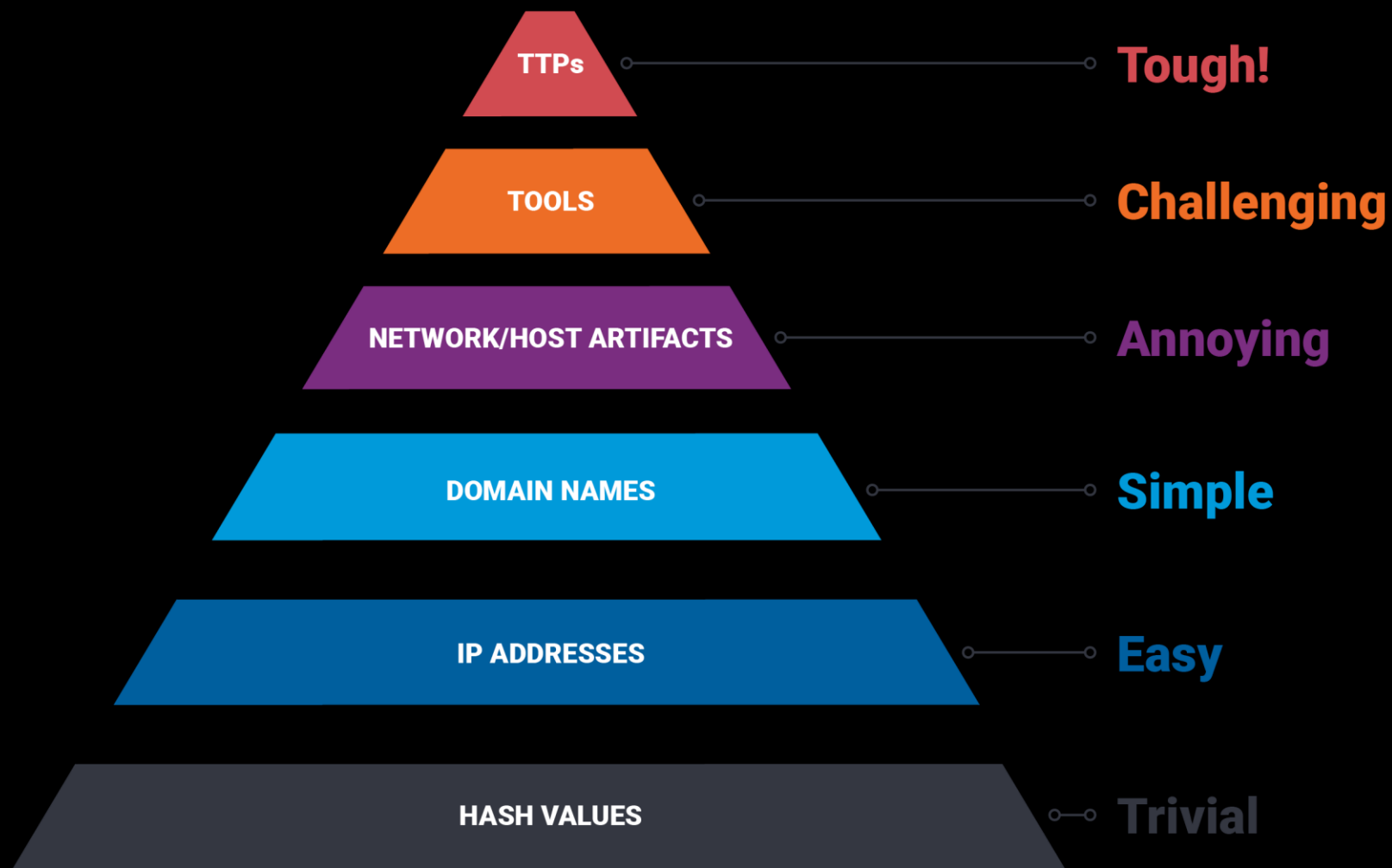


**Too Many Alerts**



**Limited Data Sources**

# The Pyramid of Pain





# XDR Approach



**Single Package**



**Automated Detection and Response**



**Extensive MITRE ATT&CK Coverage**



# XDR Landscape

Native  
XDR



Open  
XDR



# Native XDR Issues

**Native  
XDR**



**Existing Invested Security Assets**



**No Silver Bullet**



**Ideal for SME**

# Open XDR Issues

Open  
XDR



Fragmented UX

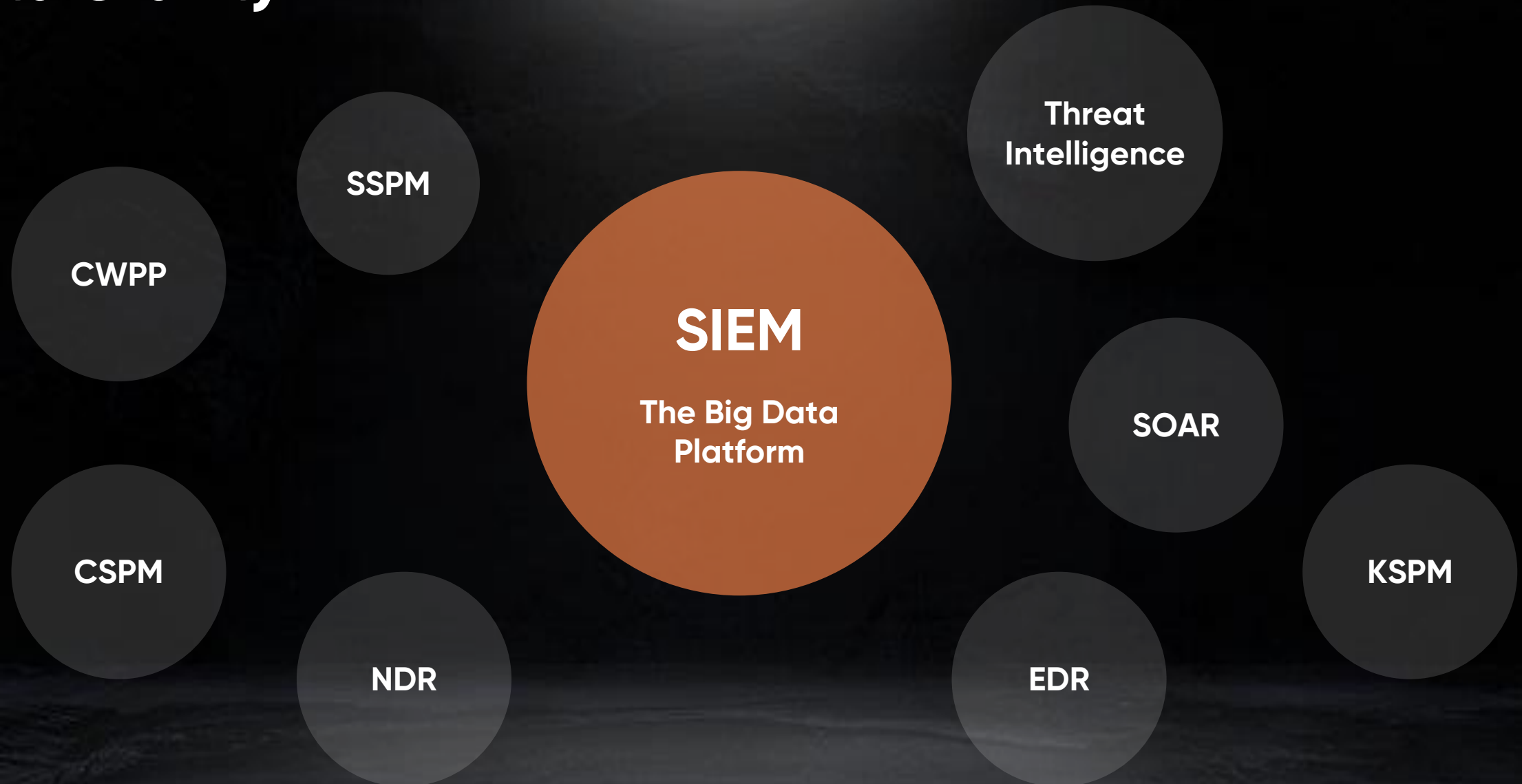


Weak Integration



Just Modernized SIEM

# Data Gravity



# Modernized SIEM



**AI Assistant**



**Plugin Architecture**



**Auto Correlation and Response**

# AI Assistant



Log Normalization



App Recommendation



Threat Intelligence Search



Hunting Rule Generation



Ticket Summarization



Report Generation



IP Blocking



Dashboard Generation

# Plugin Architecture

Parser

Log Schema

Logger

Logger Model

Dataset

Behavior Profile

Widget

Dashboard

Pattern Group

Address Group

Port Group

Detection Rule

ML Model

CTI Feed

Playbook

Report

AI Prompt

Query Command

대시보드

수집

분석

대응

검색

Q

활성

1Password

1.1.2308.0 (2023-08-01)

1Password 앱은 1Password 인증 로그 수집기와 대시보드, 확장 쿼리 명령어를 제공합니다.

활성

aws AWS

1.3.2405.0 (2024-05-01)

AWS CloudTrail, CloudWatch, GuardDuty, EC2, IAM, ELB, S3 등 다양한 서비스의 API를 이용하여 보안 및 가용성 모니터링, 클라우드 비용 계산 등 각종 분석 기능을 제공합니다.

활성

AXGATE 차세대 방화벽

1.1.2308.1 (2023-10-27)

AXGATE 차세대 방화벽 API를 이용하여 보안정책 구성에 필요한 IP 주소, 시간, 서비스, NAT 프로파일 객체를 조회하거나 원격으로 변경하고 적용합니다.

활성

AbuseIPDB

1.2.2309.1 (2024-05-28)

AbuseIPDB REST API를 통해 특정 IP 주소의 악성 여부를 조회하거나, 악성으로 분석된 IP 주소를 신고합니다. 확도 높은 상위 1만개의 악성 IP 주소를 수신하여 선제적 IP 차단에 활용할 수 있습니다.

활성

Deep Discovery Email ...

1.1.2404.0 (2024-05-01)

트렌드 마이크로 딥 디스커버리 이메일 인스펙터 앱은 DDEI 로그에 대한 전용 파서, 수집 모델, 대시보드를 제공합니다.

활성

Deep Discovery Inspe...

1.0.2403.0 (2024-03-15)

트렌드 마이크로 딥 디스커버리 인스펙터 앱은 DDI 로그에 대한 전용 파서, 수집 모델, 대시보드를 제공합니다.

활성

Defender for Endpoint

1.0.2403.1 (2024-06-13)

엔드포인트용 마이크로소프트 디펜더 앱은 엔드포인트 경보 수집기와 대시보드, 확장 쿼리 명령어를 제공합니다.

활성

GitHub

1.0.2309.0 (2023-09-17)

GitHub 앱은 GitHub 감사 로그를 조회하는 쿼리 명령어, 수집기, 대시보드를 지원합니다.

활성

SNIPER ONE-i

1.1.2307.1 (2024-03-20)

SNIPER ONE-i 앱은 전용 로그 파서와 침입 탐지 대시보드를 제공합니다.

활성

Trellix IPS

1.1.2308.0 (2023-08-05)

트렐릭스 IPS 앱은 전용 로그 파서, 수집 모델, 침입탐지 대시보드를 제공합니다.

활성

WAPPLES

1.2.2402.1 (2024-06-13)

WAPPLES 앱은 확장 쿼리 명령어를 통한 API 연동 기능과 웹 방화벽 로그에 대한 전용 파서, 수집 모델, 침입탐지 및 성능 대시보드를 제공합니다.

활성

WhoisXMLAPI

1.0.2405.0 (2024-05-05)

WhoisXMLAPI 앱은 WhoisXMLAPI 서비스의 REST API를 호출하는 확장 쿼리 명령어를 제공합니다.

활성

네이버 클라우드

1.1.2308.0 (2023-08-05)

네이버 클라우드 앱은 클라우드 액티비티, 청구 비용, 서버 운영 상태 등 클라우드 보안 향상 관리(CSPM)에 필요한 다양한 실시간 모니터링 기능을 제공합니다.

활성

네트워크 블랙박스

1.1.2310.2 (2024-01-01)

쿼드마이너 네트워크 블랙박스 앱은 REST API를 통해 세션 조회, 컨테츠 조회, PCAP 및 원본 파일 다운로드, 줄 및 위법 탐지 경보 조회 기능을 제공합니다.

활성

마이크로소프트 365

1.1.2312.0 (2023-12-09)

마이크로소프트 365 API를 통해 사용자 계정, 파일, 메일 이용 현황을 모니터링하고 인가되지 않은 자료 접근 및 유출을 탐지합니다.

활성

메일아이

1.1.2308.0 (2023-08-12)

메일아이 앱은 첨부 파일을 포함한 메일 발송 현황 대시보드와, 메일 및 첨부파일 로그 수집기, 엘라스틱 API 호출을 통해 임의 기간 메일 데이터를 조회하는 쿼리 명령어 확장을 제공합니다.

활성

안랩 EPP

AhnLab

1.1.2311.1 (2024-03-05)

안랩 EPP 앱은 전용 로그 파서, 수집 모델, 대시보드를 제공하며, 엔드포인트 파일 검색 및 수집, 안리포트 수집, V3 검사, 의심 행위 상세 내역 조회, 네트워크 격리 및 해제, 탐지 예외 처리에 필요한 확장 쿼리 명령...

활성

안랩 MDS

AhnLab

1.1.2403.1 (2024-05-31)

안랩 MDS 앱은 MDS 이벤트, 스캔, 악성코드 탐지, 사이트가드, 에이전트 상태, 성능 로그에 대한 전용 파서, 수집 모델, 대시보드를 제공합니다.

활성

안랩 트러스트가드

AhnLab

1.2.2402.0 (2024-02-27)

안랩 트러스트가드 앱은 트러스트가드 방화벽 로그, IPS 로그에 대한 전용 파서, 수집 모델, 트래픽 및 침입탐지 대시보드를 제공합니다.

활성

웹프론트

1.1.2404.1 (2024-06-13)

WEBFRONT 앱은 파이오닝 웹프론트 장비에 대한 전용 로그 파서, 수집 모델, 대시보드를 제공합니다.

# Auto Correlation



**T1566 Phishing**

**+20**



**T1059 Command and Scripting Interpreter**

**+50**



**T1039 Data from Network Shared Drive**

**+10**

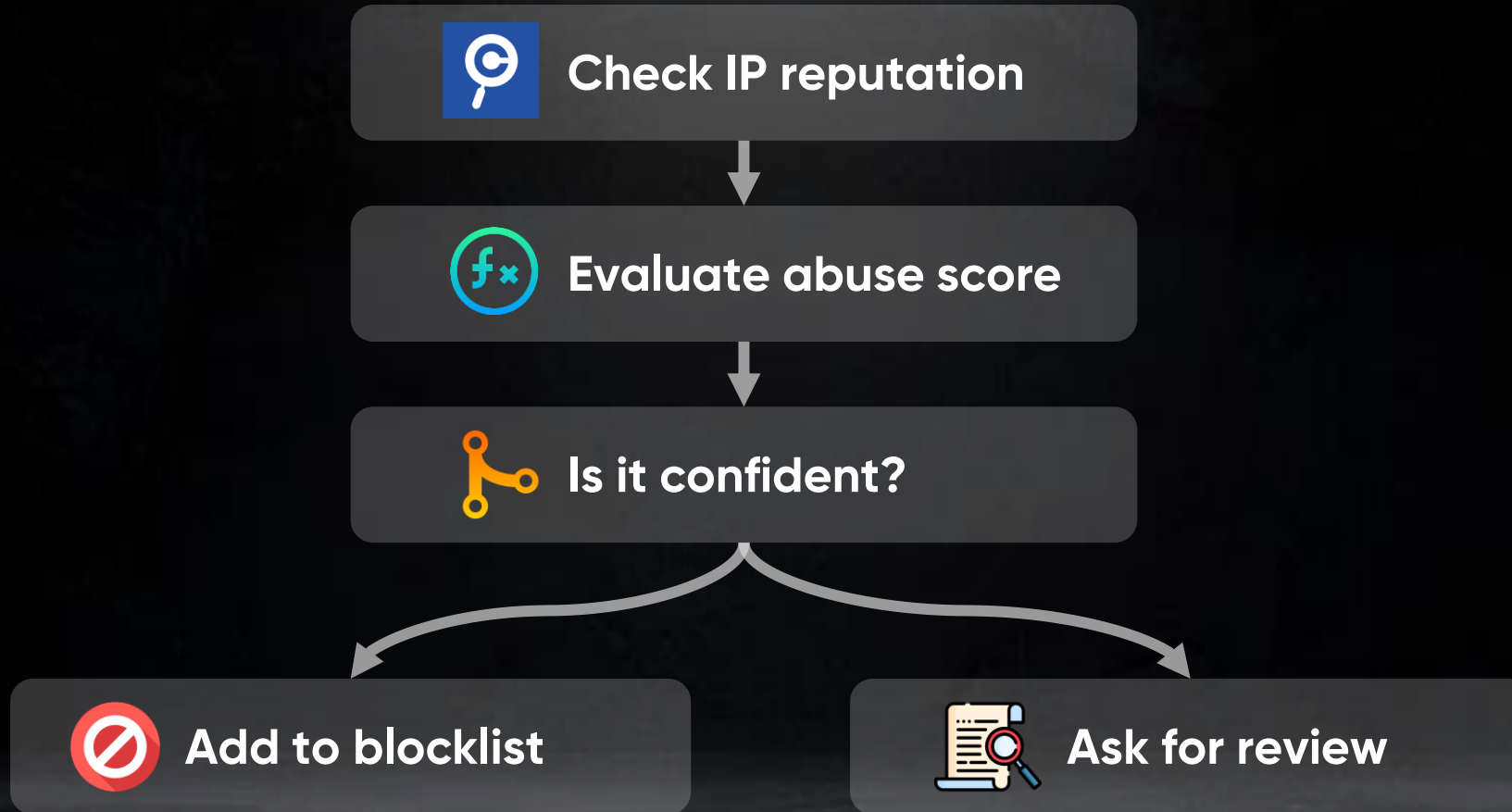


**T1048 Exfiltration Over Alternative Protocol**

**+20**



# Automated Response



# Why Cloud SIEM?

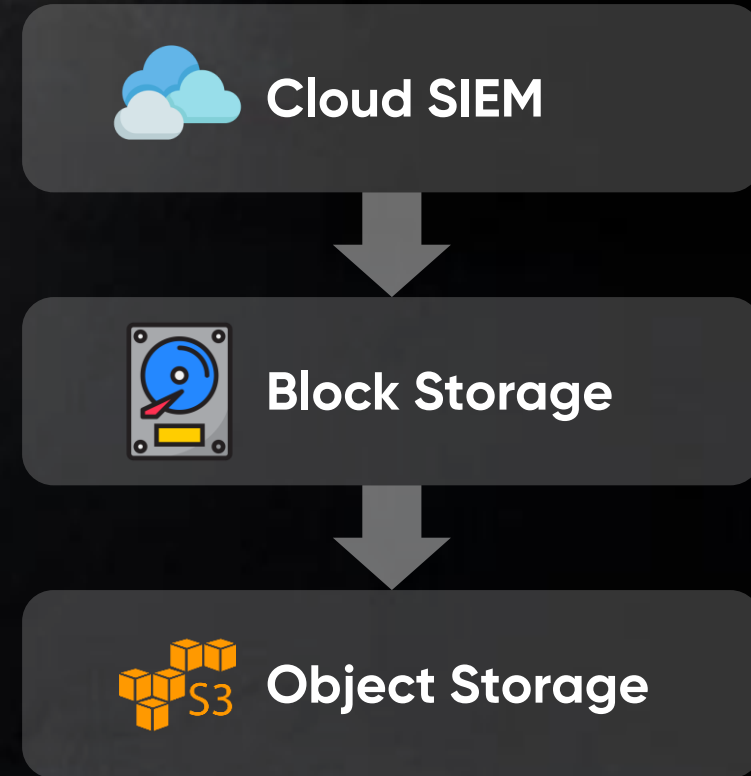
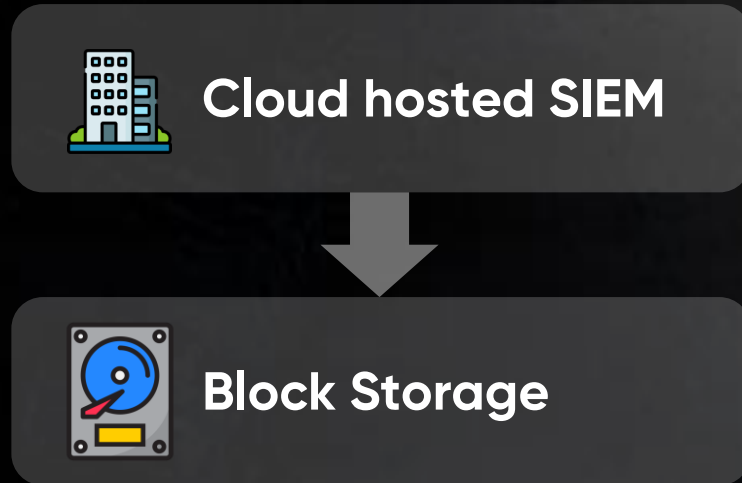


**Scalability**

**Threat  
Intelligence**

**Ease of  
Management**

# Cloud SIEM != Cloud hosted SIEM



# Cost Simulation

200GB per day



On-premises



Cloud hosted

Item	HDD 32TB RAID5 (A-A)	AWS EBS 25TB
1 year	¥4,000,000	¥20,400,000
3 years	¥4,000,000	¥61,200,000

**15 times  
higher**

# Cost Simulation

200GB per day



On-premises



Cloud SIEM

Item	HDD 32TB RAID5 (A-A)	AWS S3 Glacier 25TB
1 year	¥4,000,000	¥1,755,000
3 years	¥4,000,000	¥4,387,500

**small  
up-front  
cost**

# Log Ingestion from Public Cloud Services



# Future-Proof

## Hybrid Environment



**Logpresso  
Sonar**



**Logpresso  
Cloud**



# Thank You



9F, 7, Saechang-ro, Mapo-gu, Seoul, Republic of Korea  
02-6730-7249 [contact@logpresso.com](mailto:contact@logpresso.com)

