We Know Security

생각하는 보안관제

AI 보안관제 소개

2019. 04. 24.

이글루시큐리티 손보형 팀장

IGLOOSECURITY

Cyber Attack Trends

What about recent Cyber Attack?

2019 RSA Theme : Better

〃 신뢰 환경이 무너지고 있고 사이버 보안 전문가들은 Risk를 관리함으로써 다시 신뢰를 되살리는데 집중해야 한다. 〃

(RSA 2019, Niloofar Razi Howe)

〃 AI는 사이버보안을 강화 할 수 있으나, 공격에도 사용 될 수 있다. “

(RSA 2019)

“ AI의 잘못된 결과는 심각한 비용과 재앙적인 결과를 초래 할 수 있다. ”

(RSA 2019)

THE TRUST CRISIS

Great Cyber Attack

외부에서 들어오는
공격에 대한 방어

기반시설을 노려
파괴하는 공격

사용자에게 은밀하게 접근
하여 정보를 탈취

사이버 테러 전쟁을
야기하는 공격 거대화

과다 공격으로 인한
서비스 마비

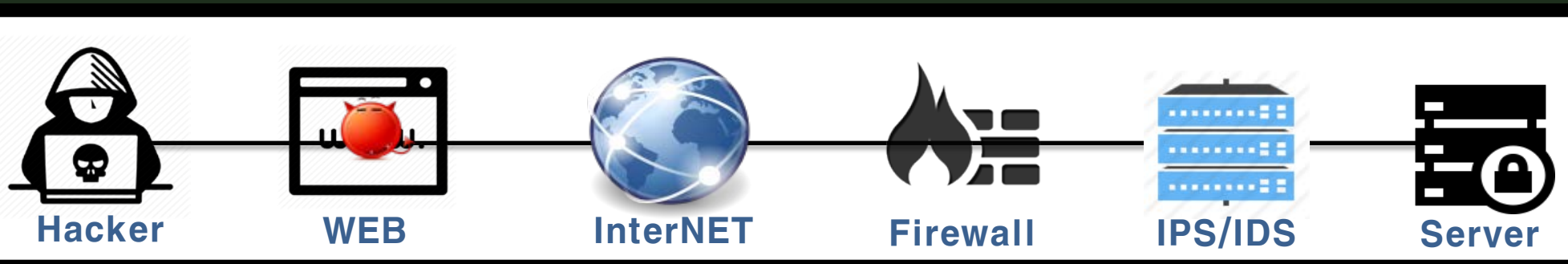
데이터를 인질로 삼아
금전을 요구

MSS Development Stage

What is the MSS and what is its limit?

보안관제의 변화 – 1세대 단위보안관제

Perimeter Security



Scanning

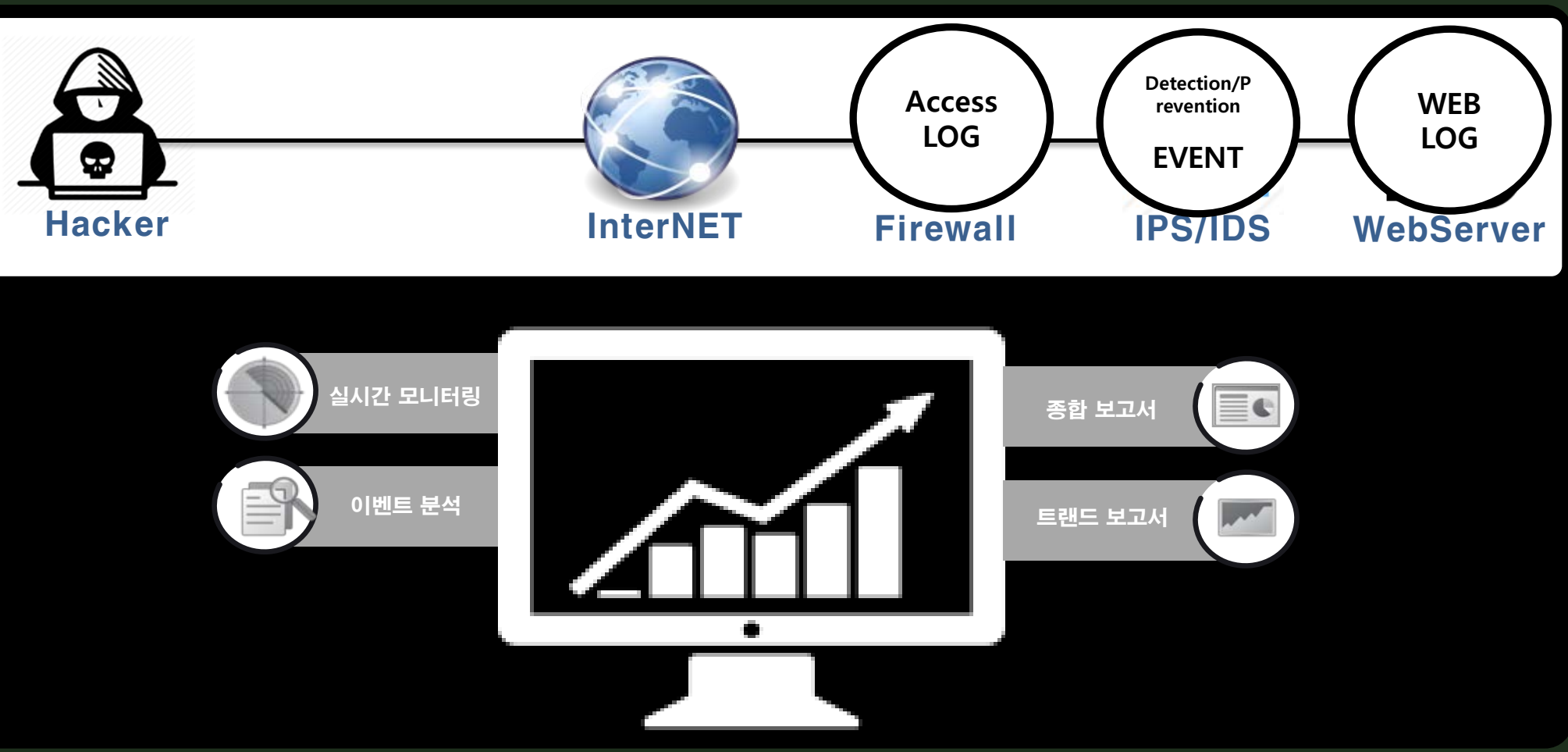
SQL Injection

Webshell

Web page defacing

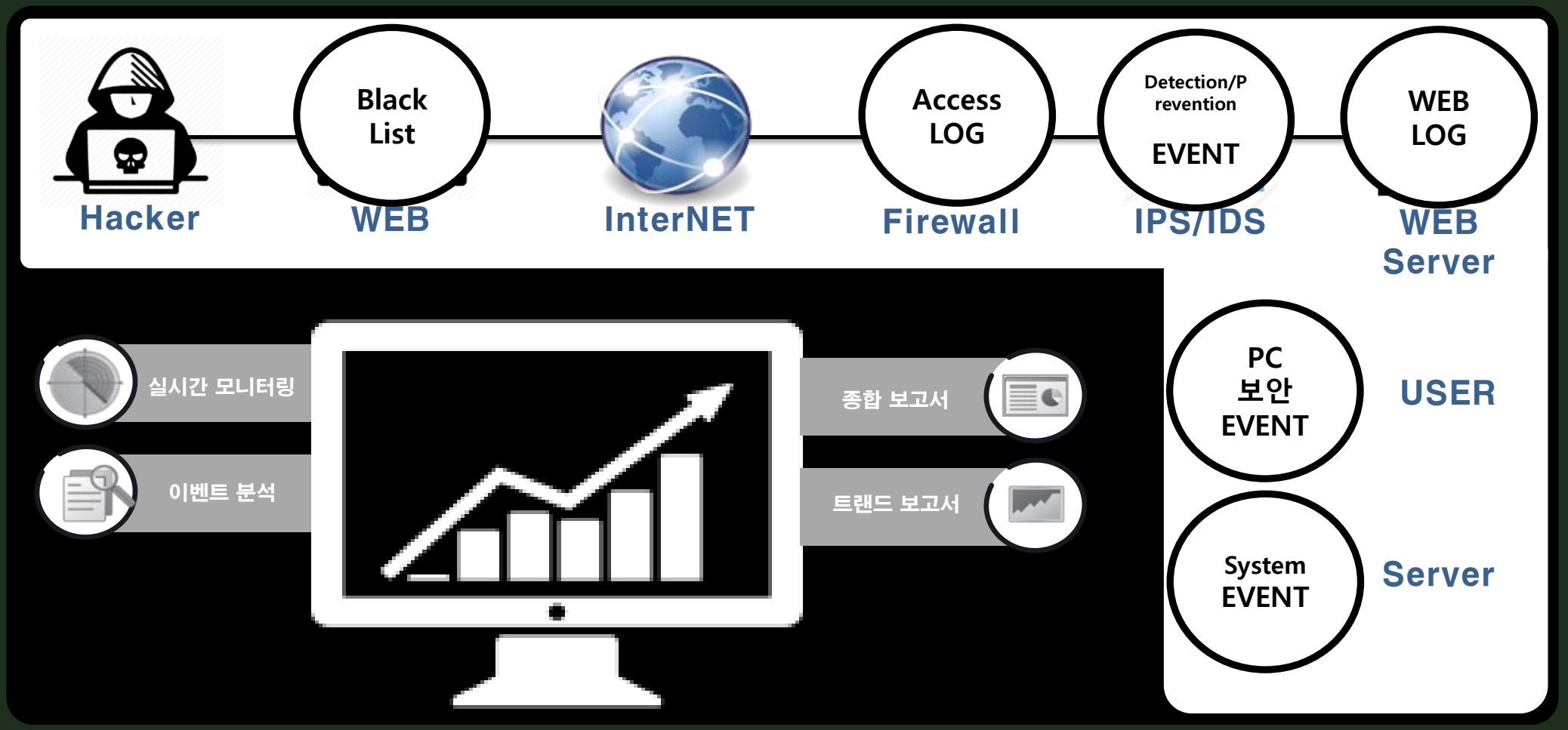
보안관제의 변화 – 2세대 통합보안관제

Data Security



보안관제의 변화 – 3세대 빅데이터 보안관제

Trust Security




36% report that they have "lots of customer data" but "don't know what to do with it"

Limitations of MSS

Attack Event
130,000

Security LOG
210G, 7billon

SIEM Warning Alarm
13,432

Incident Report
371

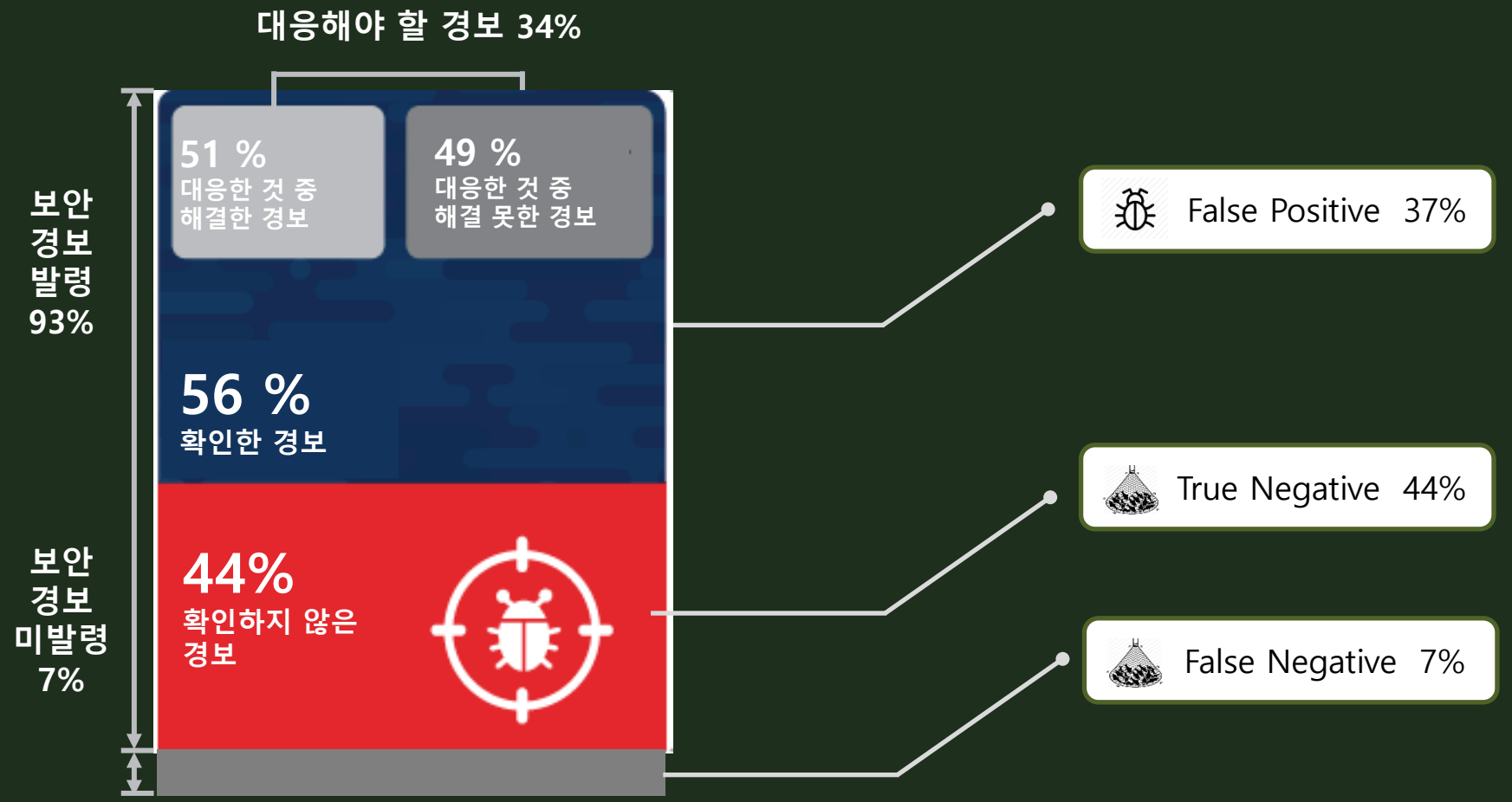
Blind attack

Increase in Security threat

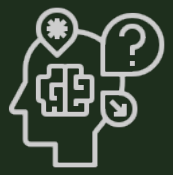
Automation of hacking

Image Loss of Business

Limitations of MSS



[source : Cisco 2018 Security Capabilities Benchmark Study]



Thinking AI MSS

How do I get to AI?

Resolve the Problem

인공지능 공격 탐지/차단

인공지능화 된 공격 탐지를 통하여 신속하고 정확한 공격 탐지 수행

분석가의 직관력 + 머신러닝

정확한 인공지능 공격 탐지를 위해 분석가의 직관력이 필요하며,
이를 바탕으로 한 학습을 통해 AI 최적화 수행

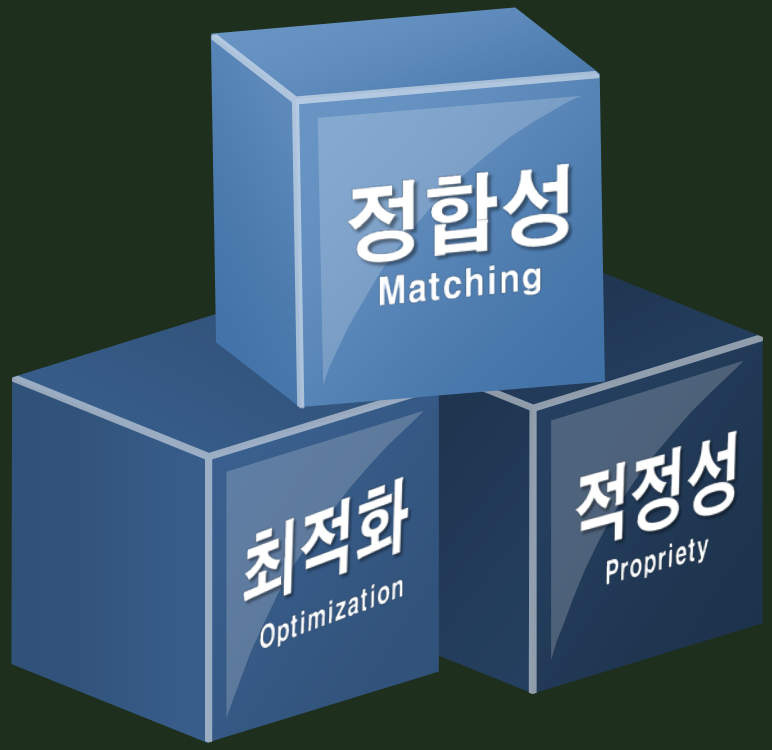
정합성/최적화/적절성

효과적인 공격 탐지를 위해 수집된 빅데이터에 대한 정합성을 수행 하고 탐지 룰을 최적화 하며, 인프라 환경에 적합한 탐지 룰 정책 생성

빅데이터 기반의 보안관제

단일 System에서 발생 되는 로그 및 이벤트를 SIEM을 통해 수집하여 빅데이터 기반의 공격 데이터 가공

AI 보안관제 사전 준비



정합성(Matching)

"많다고 좋은 것은 아니다"
BigData로 분석된 정확한 DATA만을 근거로 유효성을 극대화 하는 DATA 필요

최적화(Optimization)

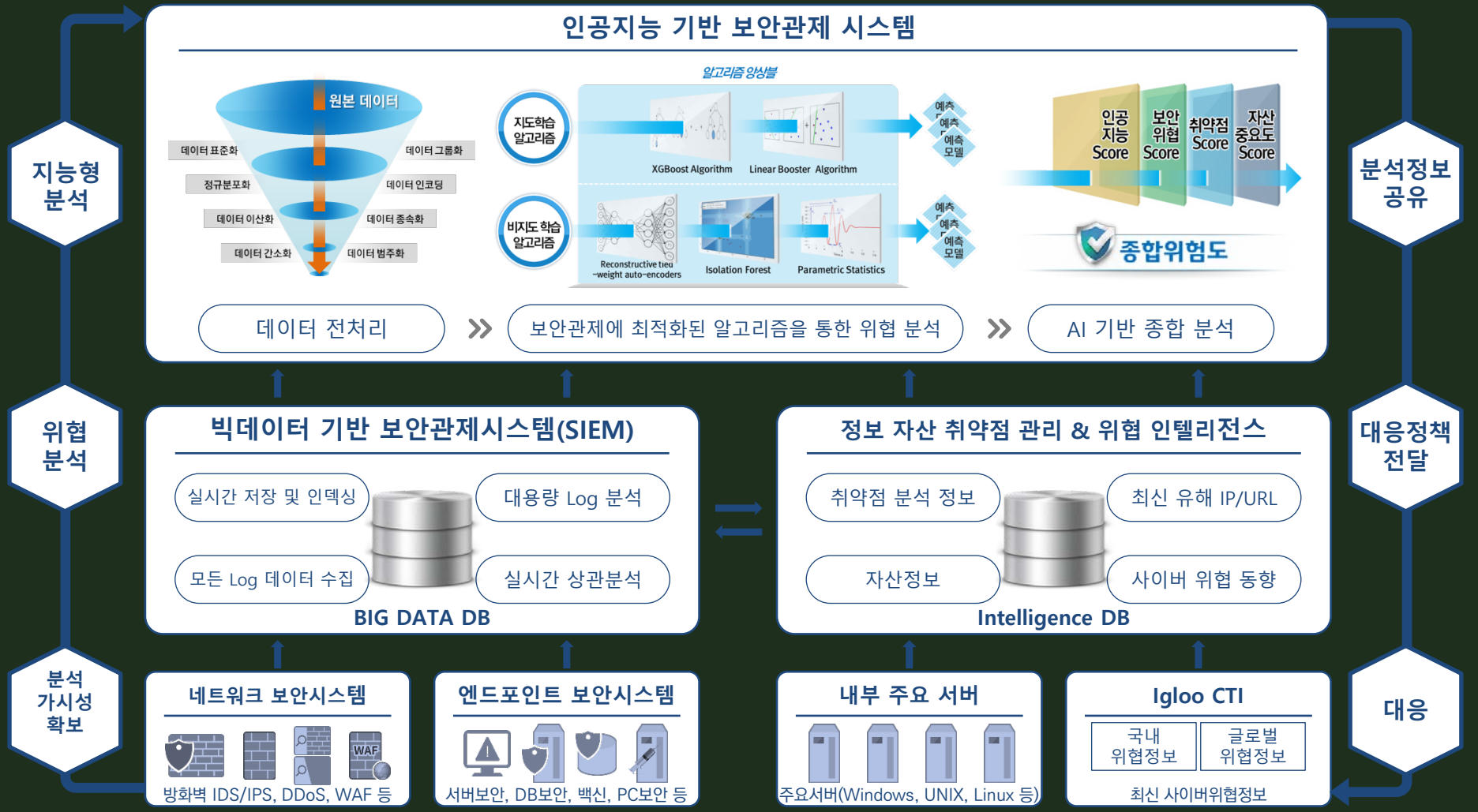
"공격은 지속적으로 변화한다"
탐지 Rule도 중요하지만 현재 환경에 최적화된 Rule과 지속적인 관리 필요

적정성 (Propriety)

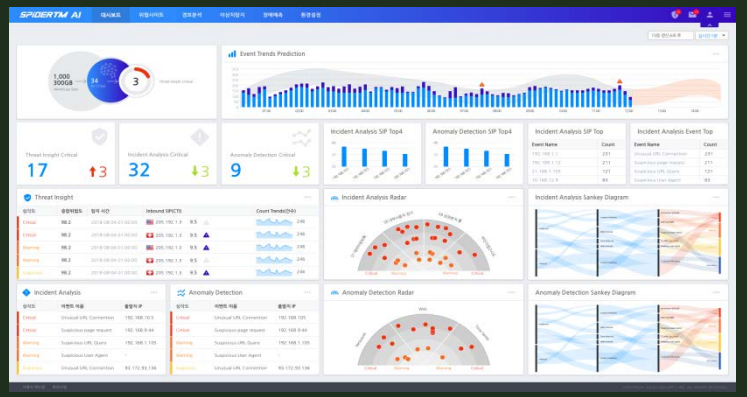
"잘못된 DATA의 조합은 더욱 더 잘못된 결과를 초래한다"
인프라 환경에 적절한 DATA의 조합으로 효율적인 공격 탐지가 필요

Thinking of IGLOOSECURITY MSS

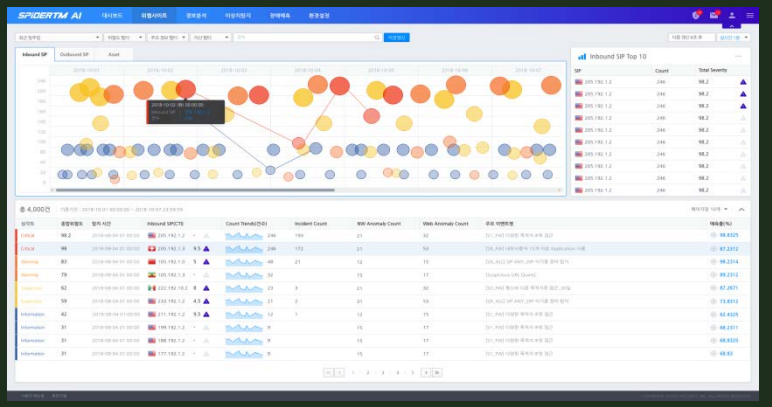
SIEM에 AI를 결합한 빅데이터 기반 지능형 보안관제 체계의 완성



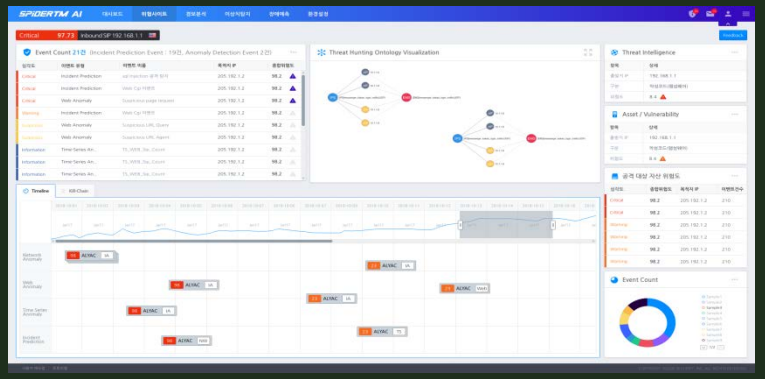
Thinking of IGLOO SECURITY AI



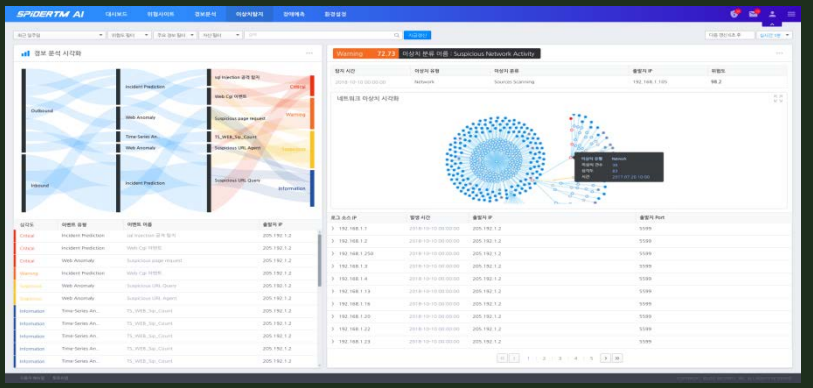
DashBoard
직관적이고 신속한 공격 파악



Threat Insight
경보와 이상치 종합 분석 시각화



Threat Insight Detail
지도학습을 통한 심각도와 예측률 기반 분석



Incident Analysis
지도학습을 통한 심각도와 예측률 기반 분석

We Know Security

THANK YOU

경청해주셔서 감사합니다.

IGLOOSECURITY