Why Cloud SIEM?

| ISEC 2024 x Logpresso |

LOGPRESSO

Hybrid Environment

On-premises

Public Cloud

SaaS

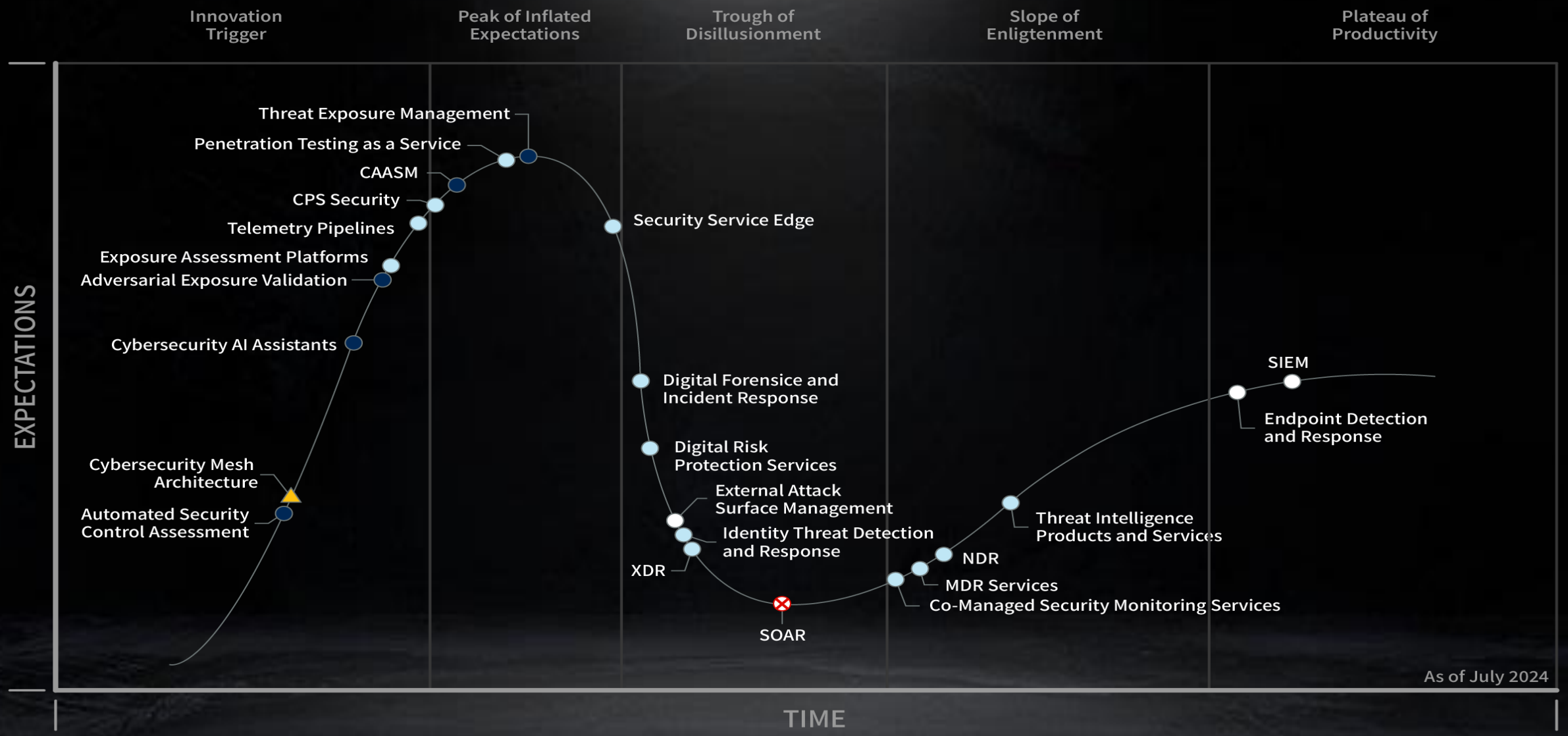
Requirements

Threat Detection and Incident Response

Complete Visibility

Meet Compliances and Regulations

Hype Cycle for Security Operations 2024



Plateau will be reached: <2 yrs. 2-5 yrs. 5-10 yrs. >10 yrs. Obsolete before Plateau

Gartner

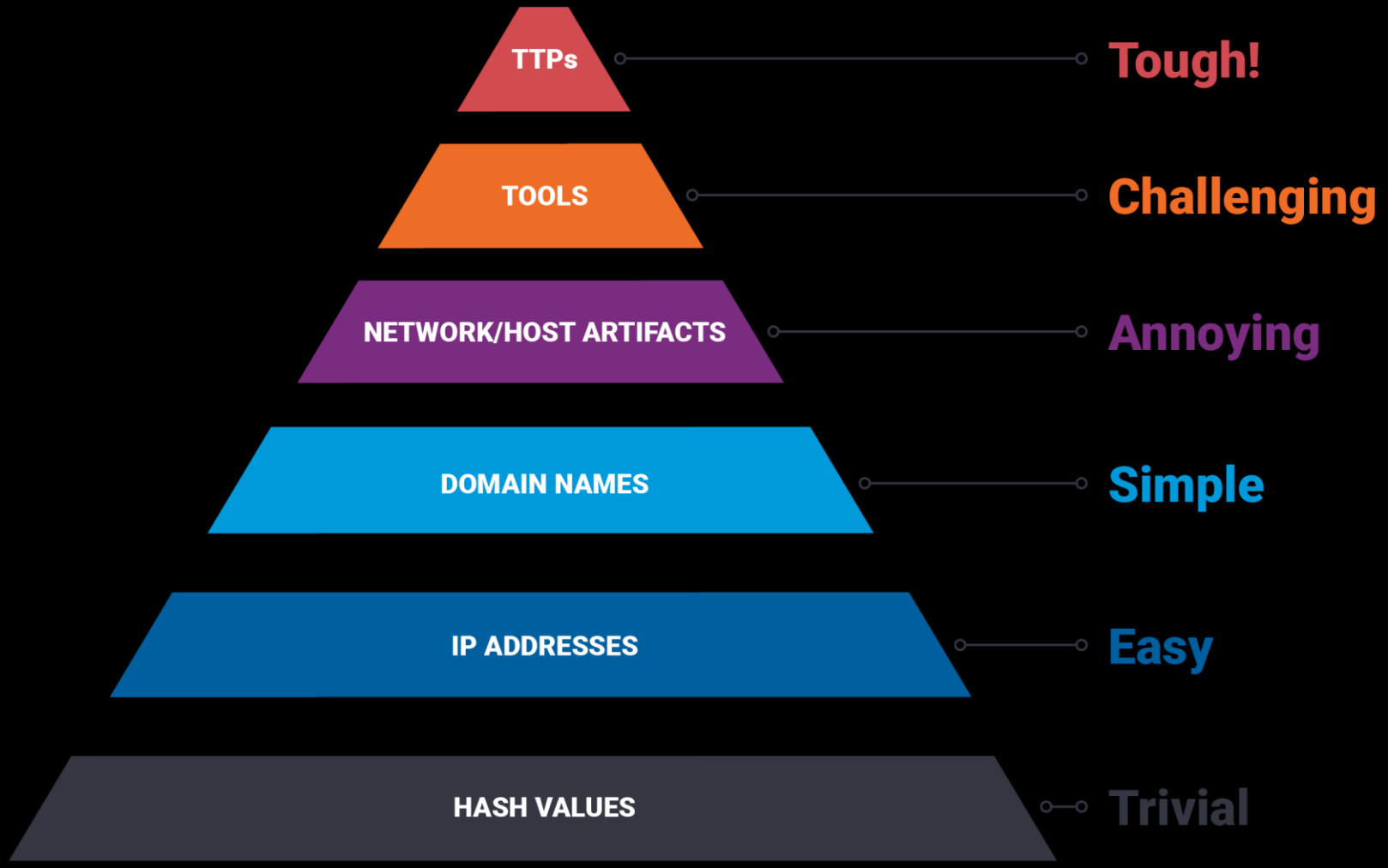
Legacy SIEM

Hard to Integrate

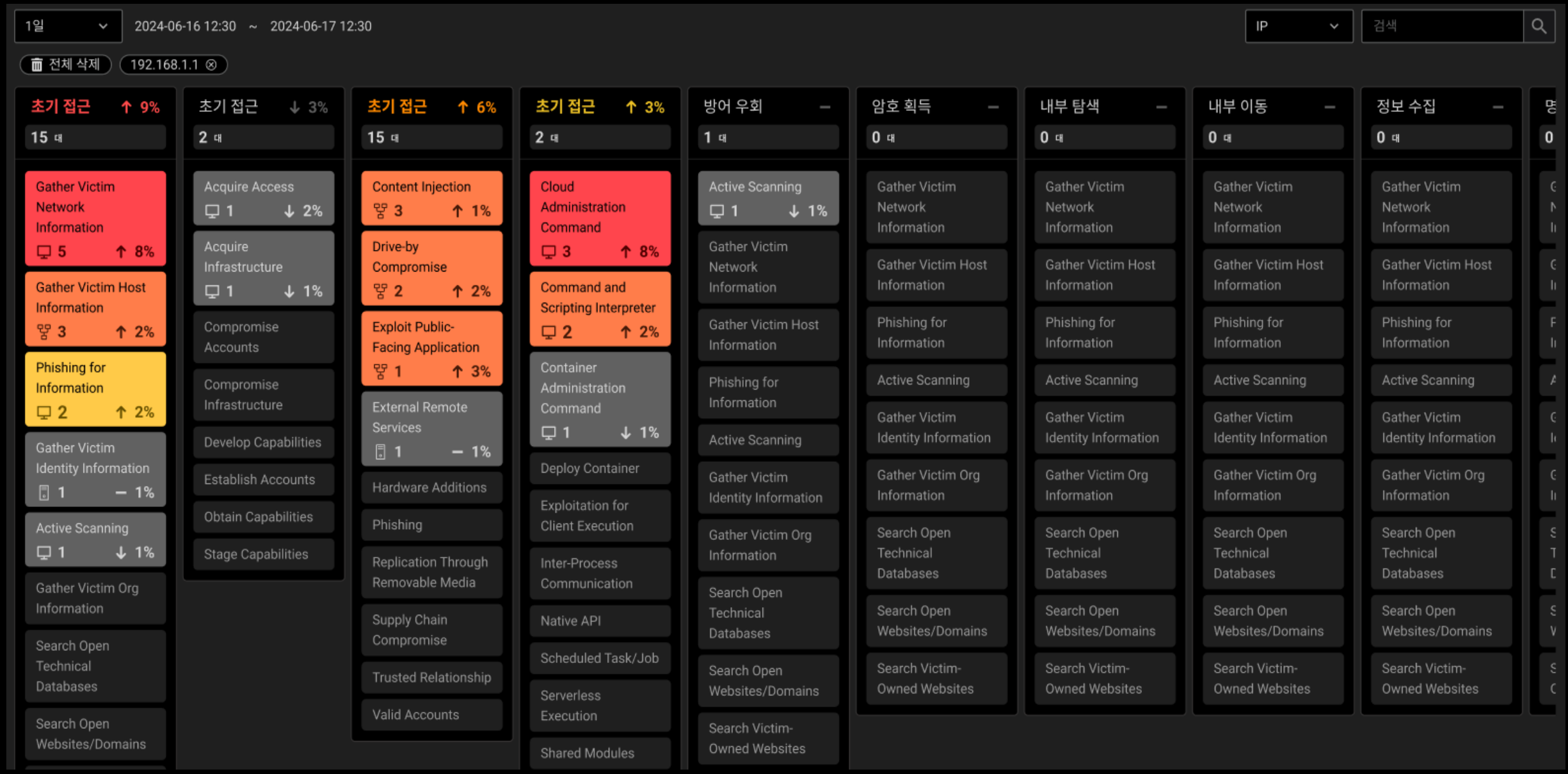
Too Many Alerts

Limited Data Sources

The Pyramid of Pain



MITRE ATT&CK Coverage



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

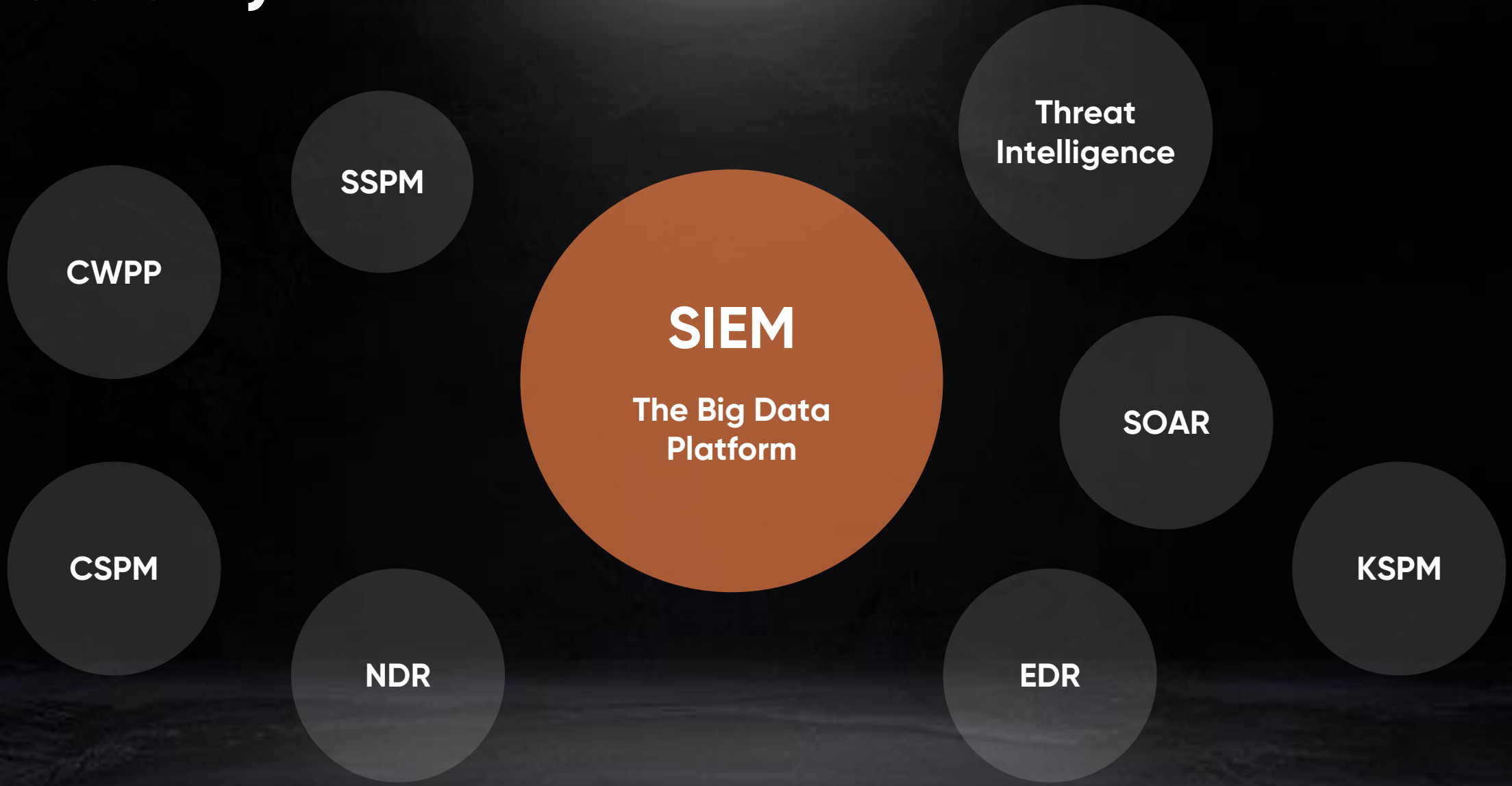
Open XDR

Fragmented UX

Weak Integration

Just Modernized SIEM

Data Gravity



Modernized SIEM

AI Assistant

Plugin Architecture

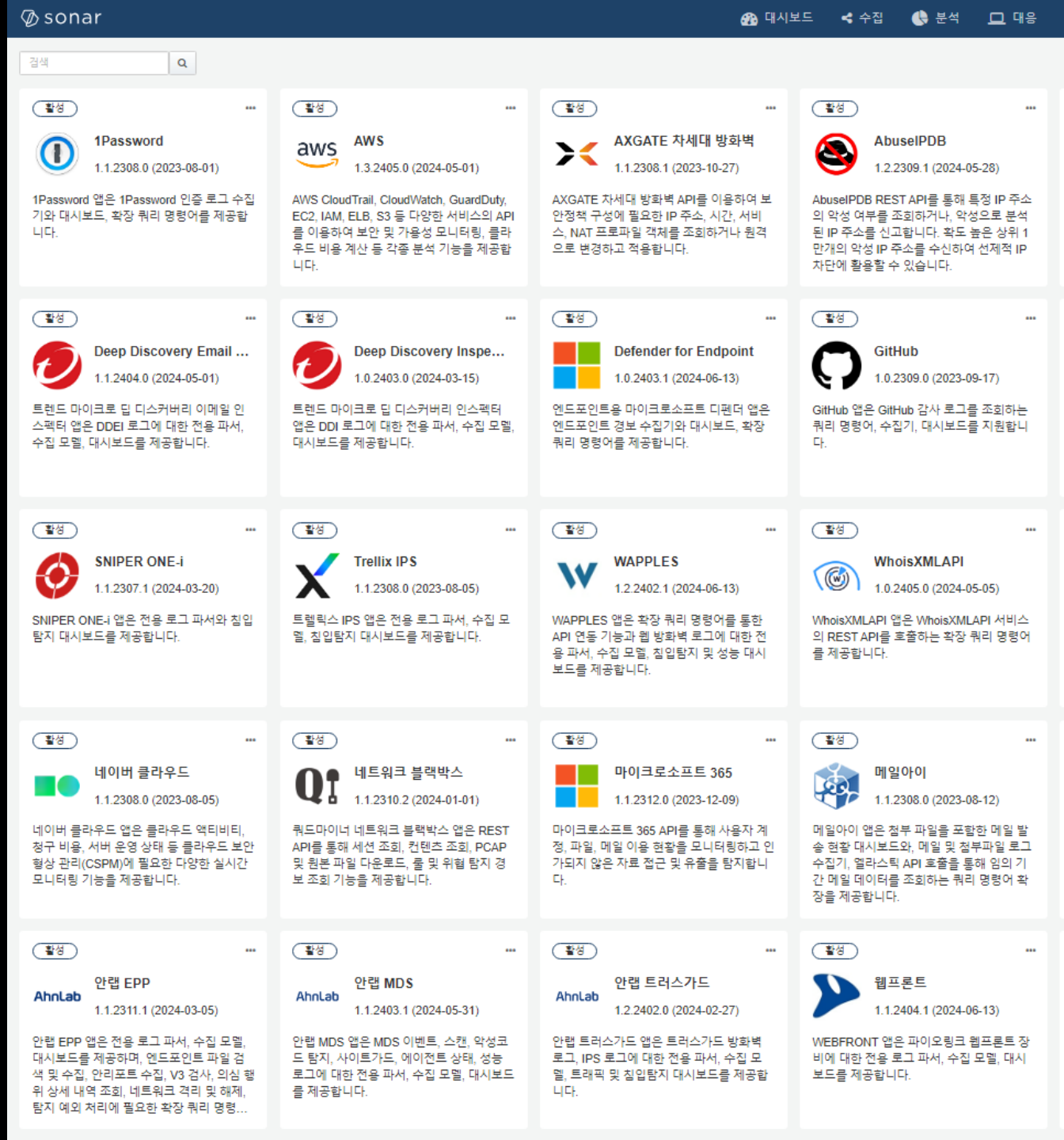
Auto Correlation and Response

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



Auto Correlation

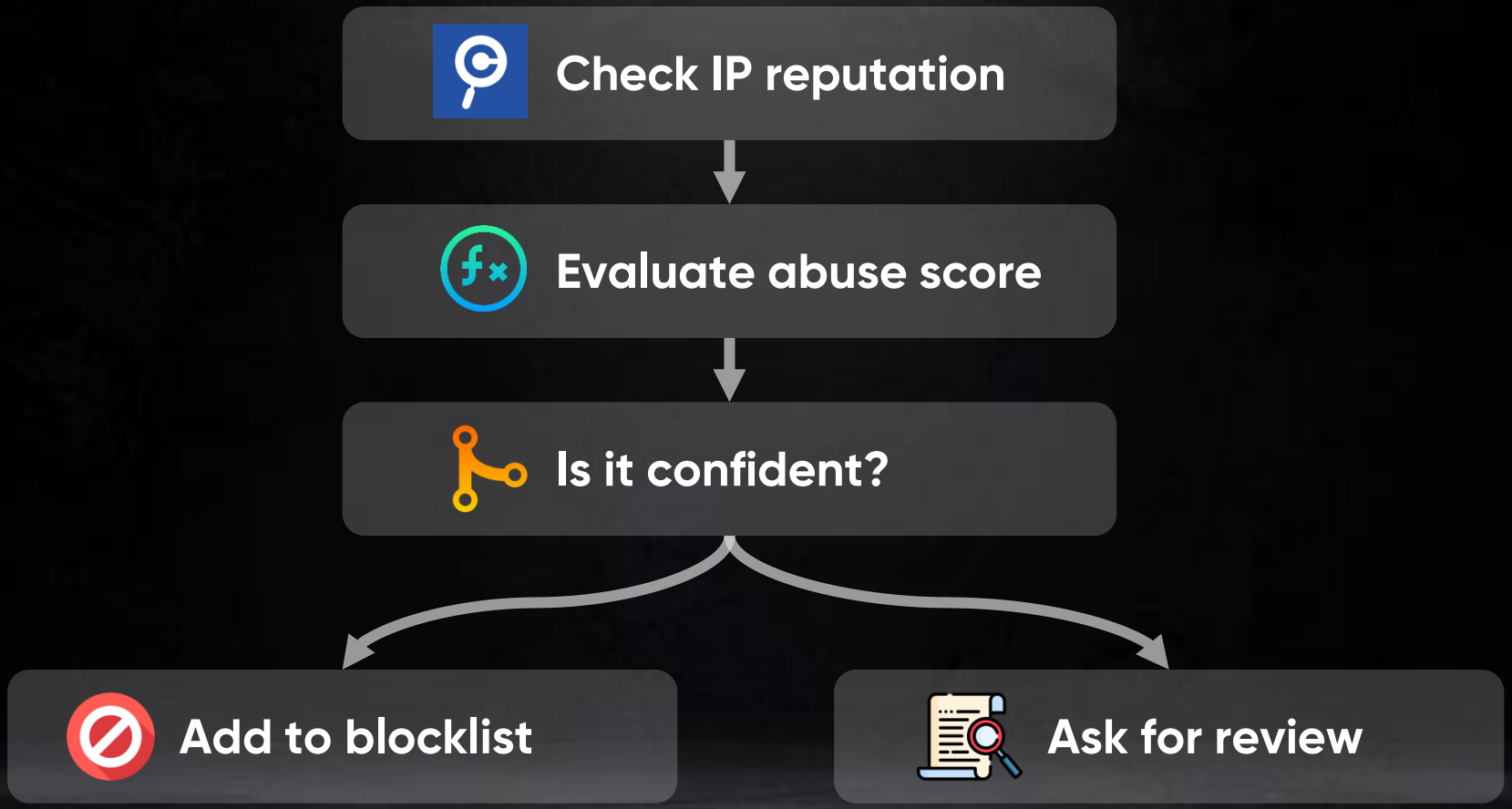
T1566 Phishing +20

T1059 Command and Scripting Interpreter +50

T1039 Data from Network Shared Drive +10

T1048 Exfiltration Over Alternative Protocol +20

Automated Response



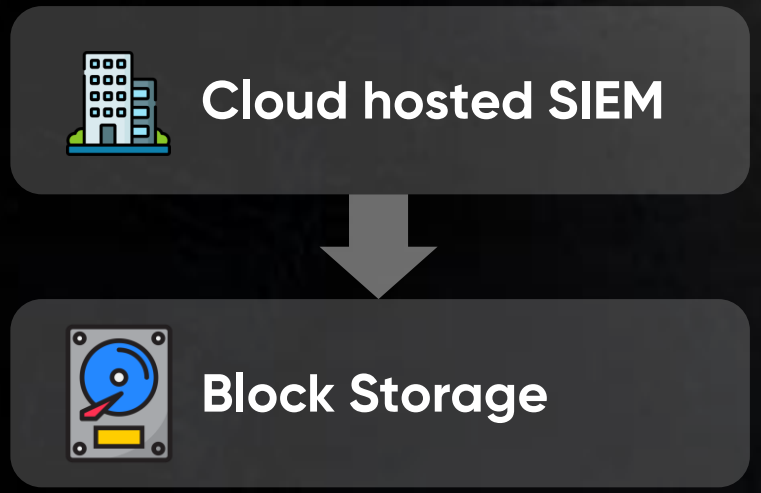
Why Cloud SIEM?

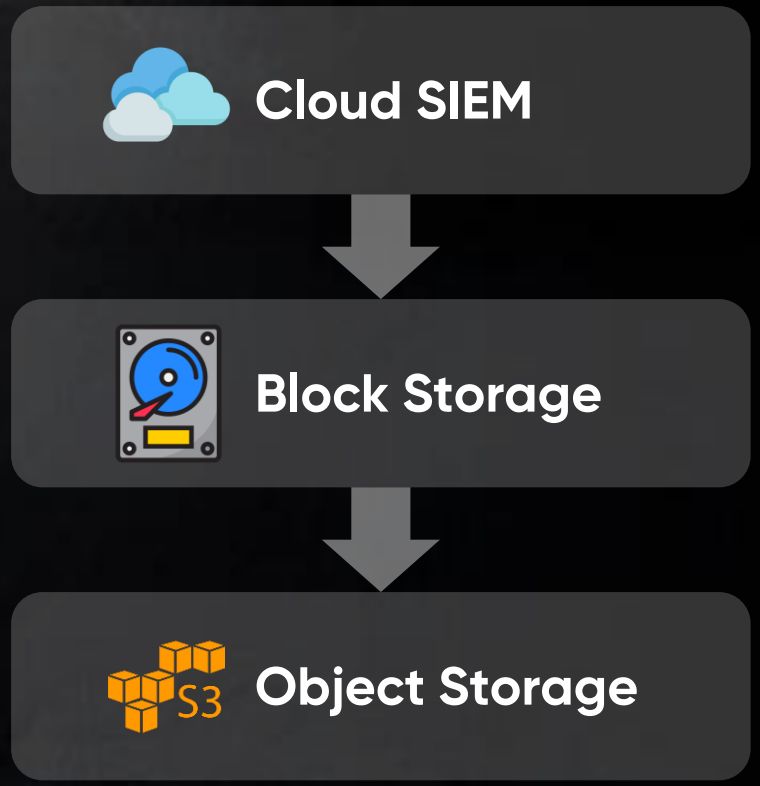
Scalability

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

LOGPRESSO