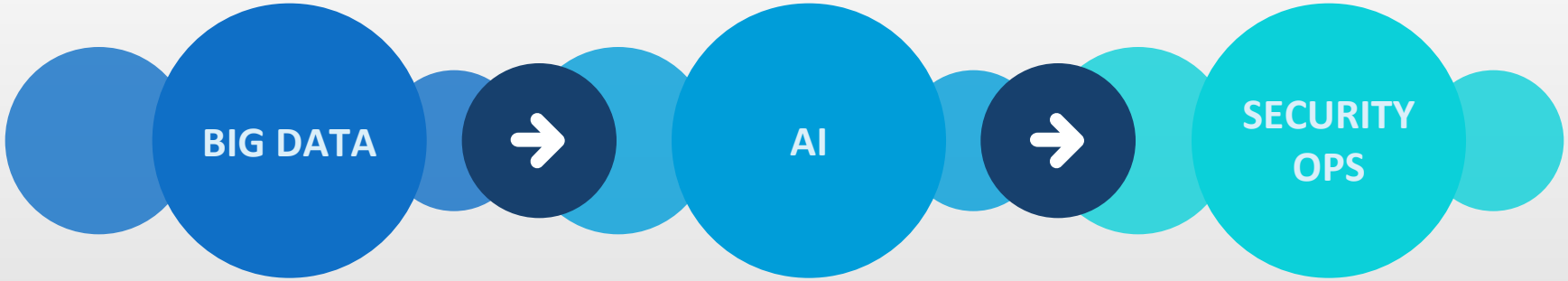
Seculayer
Company & Product Introduction

November 2018

We UNDERSTAND all data in the world !!

Contents

Cyber Security Operation Center
Platform Provider



Big Data

Big data platform that supports storage and collection from various sources with rapid search engine by clustering technology.

Artificial Intelligence

Artificial intelligence platform that detects unknown cyber attacks and threats as well as responds to potential risks with machine learning algorithms.

Security Operation Center

SOC platform that flags, categorizes, analyzes and responds to the standardized process of security events created from various systems.

Seculayer's Journey

2018
- AI integrated adaptive security system implementation at NIRS.

2017
- AI integrated adaptive security system ISP by NIRS

2016
- "School Net" system implementation in Seoul, Jeonbuk and Gangwon education agencies.
- eyeCloud IPS released. Intrusion detection/prevention sensor and analysis solution. EAL3 by CC certified.

2015
- INNO-BIZ certified.
- Bluebird released. Incident analysis and response solution (SOC platform).

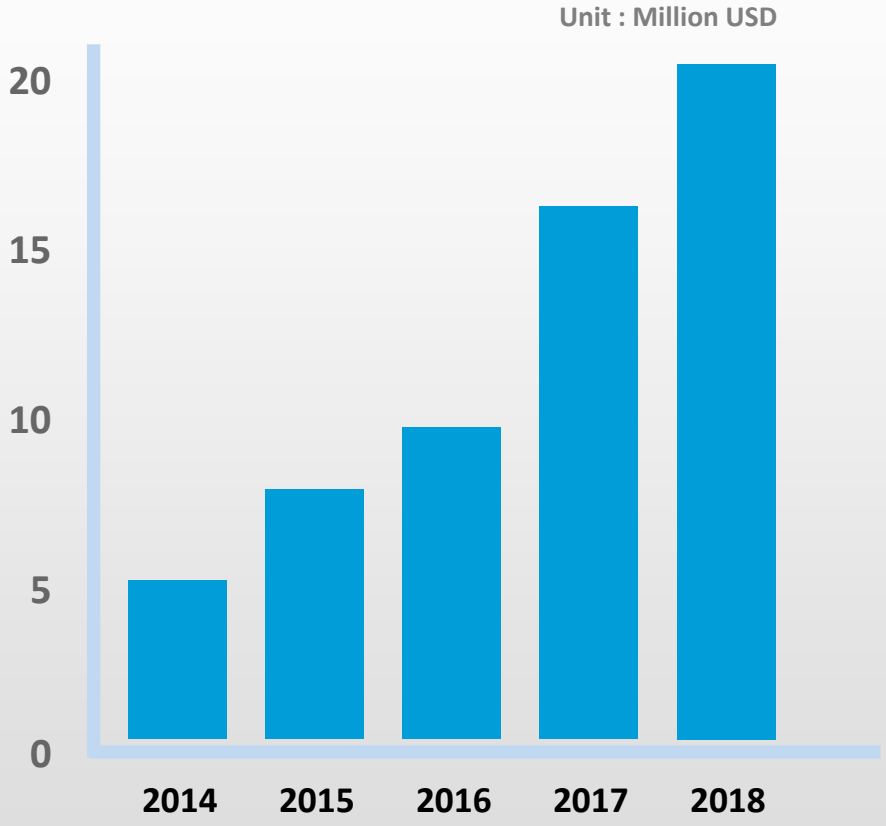
2014
- ISO27001:2013 (by Bureau Veritas certified organization)
- EAL2 (by Common Criteria) / Good Software (by Telecommunication Technology Association)

2013
- eyeCloudSIM v2.5 was implemented for integrated security control system at nation's largest data center, NIRS (formerly known as NCIA), under the name of nSIMS.

2012
- eyeCloudSIM released. Big data log management technology exclusively developed by Seculayer.
- Seculayer Inc. established by three co-founders in February.

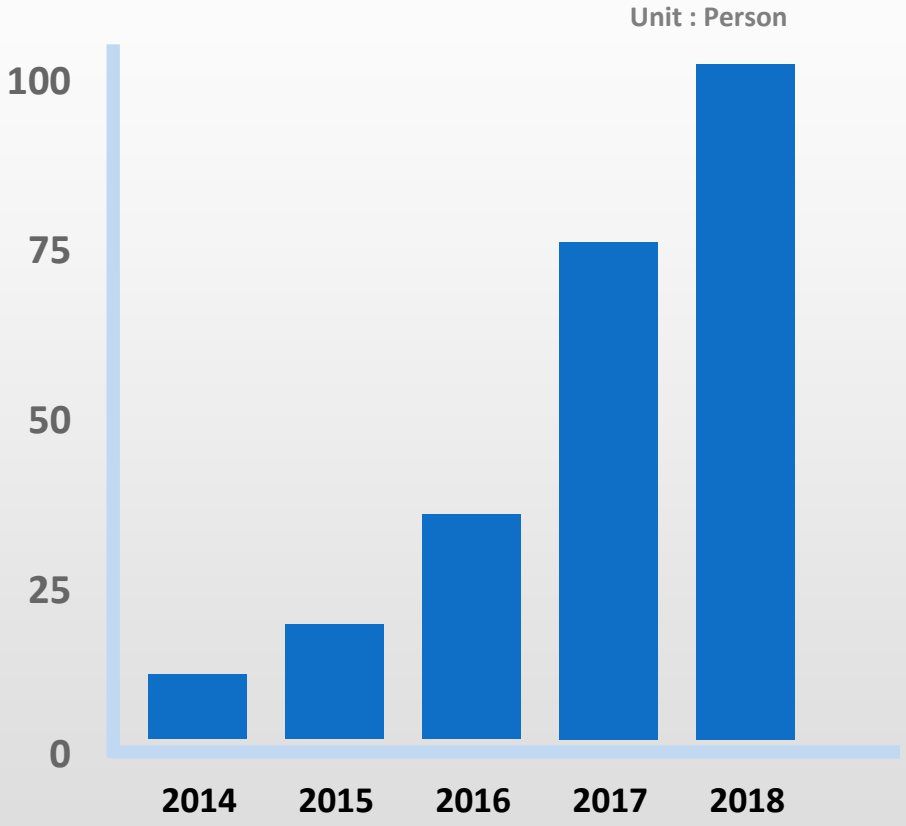
Company Growth

Financial Revenue



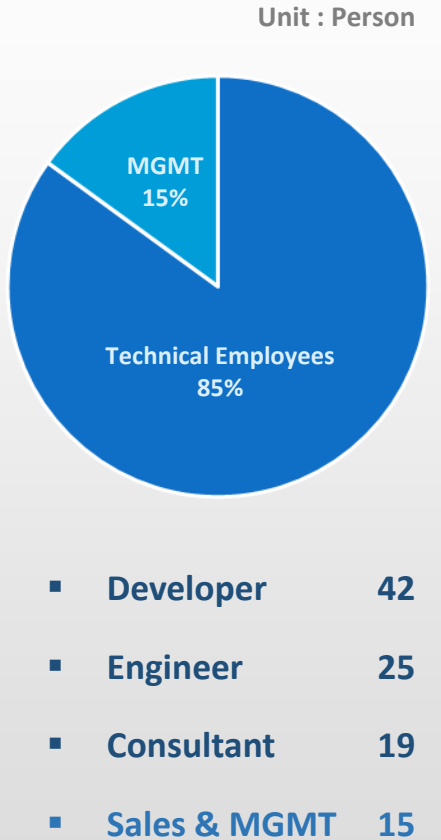
+ 300%
increased

Employees Size



+ 1,400%
increased

Employee Profile



- Developer 42
- Engineer 25
- Consultant 19
- Sales & MGMT 15

- TOTAL 101

> 200

Customers

> 300

Products Sold

Public/Govt. Sector

- National Information Resource Service
- Ministry of Unification
- Ministry of Strategy and Finance
- Ministry of Culture, Sports and Tourism
- Ministry of Land, Infrastructure and Transport
- Ministry of Employment and Labour
- Korea Electric Power Corporation
- Republic of Korea Army
- Supreme Court of Korea
- Police Agencies

Financial Sector

- Korea Development Bank (KDB)
- Jeonbuk Bank
- KB Insurance
- Korea Federation of Banks
- LIG Insurance
- Acuon Saving Bank
- Smart Saving Bank

Education/Healthcare

- Dongguk University
- Sangmyeong University
- University of Seoul
- Korea Natioinal Sport University
- Korea Aerospace University
- Kyungpook national university hospital
- Yeungnam University Medical Center

Enterprises

- Korea Telecom
- SK Telecom
- SK Hynics
- SK Broadband
- NHN Entertainment
- LS Automotive
- S1
- Ahnlab
- Lotte Home Shopping
- Hyundai PowerTech
- NICE dun & bradstreet

Awards & Certifications

12 Patents

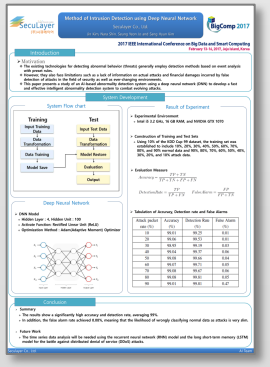
- **Real-Time Analysis by Artificial Intelligence**
- Risk MGMT by Advanced Analytics
- Unformatted Data Indexing Method
- **Real-Time Event Detection (US Patent)**
- **Performing Normalization of Unstructured Data (US Patent)**
- Malicious Code Analysis & Clustering and more

10 Certifications

- **ISO IEC 27000 : 2013**
- Good Software Certification
- Common Criteria
- Software Quality LEVEL 1 and more

8 Awards

- **Contribution Award by NIRS**
- Achievement Award by Ministry of the Interior and Safety
- Good Software Awards by TTA
- Good Software Awards by ETNews and more



2 Studies

- **Intrusion Detection using DNN(Deep Neural Network)Algorithm using KDD'99**
- Fraud Detection using Deep learning Algorithm

Product Lineup

Cyber Security Operation Center Platform

Security Control

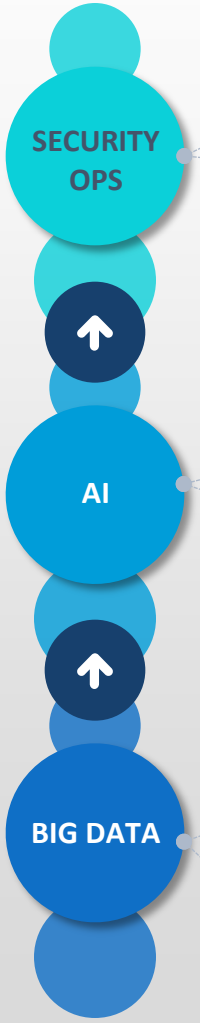
Security event processing, analysis, response, security policy establishment and distribution

Analyze all behaviors

Detect potential risks and anomalies using all data analysis (association analysis) and security information from Big Data

Big Data Gathering

Data collection / analysis from all data sources including security equipment, network, server, application, UBA, IOT and so on



eyeCloudSIM for Bluebird | S.O.C Portal

Refined Events

A.eye | AI Platform for Cyber Security

All Events & Logs

eyeCloudSIM | Security Info. & Event MGMT. Platform

guppy for Big Data | Big Data Analysis Platform

Response Command

Response Command

Security Info. (Vulnerability, Threats)

Collecting Logs

Security Info. Source

Security Automation

On the roadmap

Security Information Service

eye.C | Intelligence Center

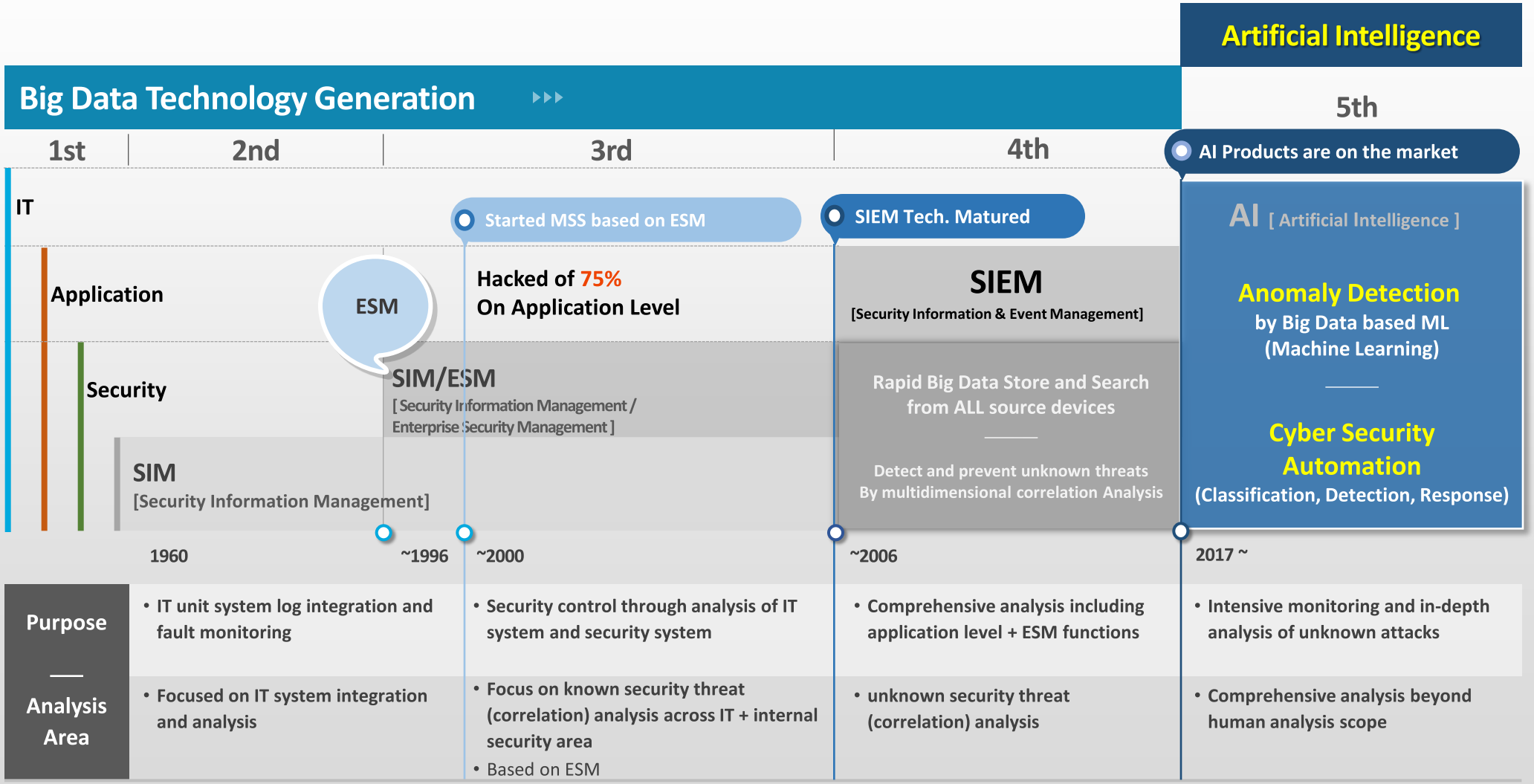
T.eye | Threat Intelligence

Data Source Devices

eyeCloudSIM for TtL | Network Packet Analysis System

eyeCloud IPS | Intrusion Prevention Sensor & analysis System

Contents


Artificial Intelligence
Big Data Technology Generation
5th
1st
2nd
3rd
4th
AI Products are on the market
IT
Started MSS based on ESM
SIEM Tech. Matured
AI [Artificial Intelligence]
Application
ESM
Hacked of 75%
On Application Level
SIEM
[Security Information & Event Management]
Anomaly Detection
by Big Data based ML
(Machine Learning)
Security
SIM/ESM
[Security Information Management /
Enterprise Security Management]
Rapid Big Data Store and Search
from ALL source devices
Cyber Security
Automation
(Classification, Detection, Response)
SIM
[Security Information Management]
Detect and prevent unknown threats
By multidimensional correlation Analysis
1960
~1996
~2000
~2006
2017 ~
Purpose
• IT unit system log integration and fault monitoring
• Security control through analysis of IT system and security system
• Comprehensive analysis including application level + ESM functions
• Intensive monitoring and in-depth analysis of unknown attacks
Analysis Area
• Focused on IT system integration and analysis
• Focus on known security threat (correlation) analysis across IT + internal security area
• Based on ESM
• unknown security threat (correlation) analysis
• Comprehensive analysis beyond human analysis scope

Contents

2 Product Introduction

- **eyeCloudSIM (SIEM)**
- A.eye (AI for Cyber Security)

eyeCloudSIM (SIEM) - Overview

See More!!

eyeCloudSIM v3.0

Integrated data collecting and analyzing system based on big data

Integrated log management system that collects and analyzing data through high speed search enabled by big data

Next Generation SIEM

- SIEM (Security Information & Event Management)
- Integrated control environment that provides collecting, analyzing, interlocking capability with user-friendly interface.

Log Searching

- Able to search more than 2 billion logs by combining keywords by tags
- Automatically creates user-defined search result

Log Collecting

- Log collection by methods of both installing agents and agentless
- Auto log parser tool allows to collect unformatted logs by formatting them

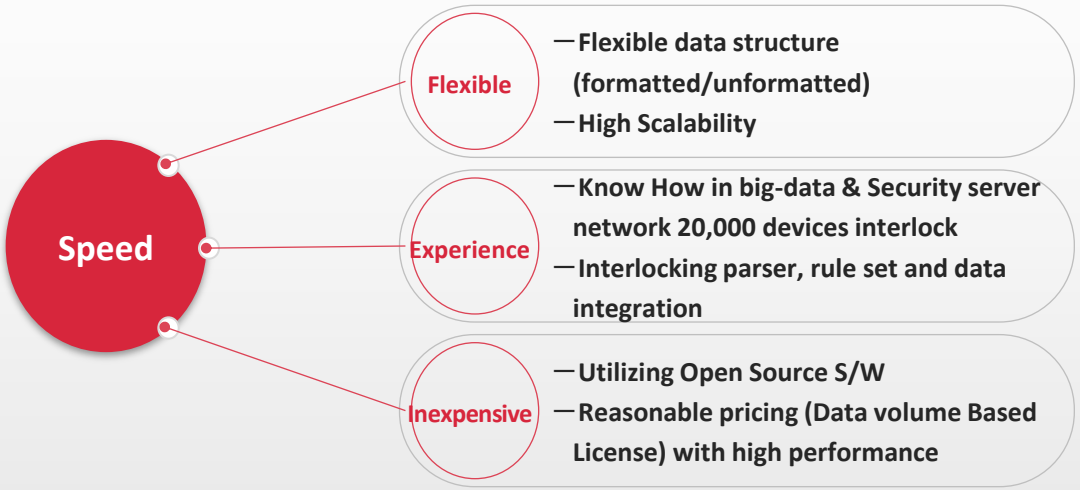
Dashboard

- Able to create, move and resize the components of collecting events
- Provides 2-5 columns

Event analysis

- Event analysis by assets based on each attributes of collecting logs
- Risk level calculation by the results of event analysis by assets and groups

Features



What to expect

- Big data log search and analysis with integrated log collection
- Appropriate analysis and response to cyber threats and attacks with real-time event and log correlation
- Shorten time to respond to security incidents by integrating logs
- Display the devices' current status in one place for brisk identification and response to the origin of incidents
- Automation and efficient work flow by combining multiple managing points
- Data integration increases efficient work process through share between departments

> 200,000 EPS	> 600,000 EPS	< 1 Sec In 2 Billion Logs
COLLECTION	STORAGE	SEARCH

Big Data Collection

Data collection system considering Big Data collection technology, large data transmission, operation stability and high availability

Rapid Indexing

Distributed architecture for few TB daily processing performance.

Data storage management for scalability, stability and possible deficiency from multi systems.

Distributed Search

Analysis module supports distributed search and real-time performance.

Intuitive visual analysis for event correlation, statistics, threshold, and forecasting

Contents

2 Product Introduction

- eyeCloudSIM (SIEM)
- **A.eye (AI for Cyber Security)**

A.eye (Artificial Intelligence)

A.eye
Big Data & Artificial Intelligence Platform

Big data-based next generation
AI integrated analysis system

Next-Generation AI Platform to support all functions like data gathering, pre-processing, Machine Learning for detection and analysis

AI Platform for detection and analysis

- Next-generation integrated artificial intelligence analysis system based on AI using reliable machine learning open source and in-house Dev. engine
- Implementation of professional analysis environment by providing artificial intelligence model creation function integrating with existing data

Data integration

- Supports standard Open API, Adapter, Provider for data collection and extract
- Rapid tickets processing by integration with SOC

Data pre-processing

- Provides optimized data transformation algorithms and functions for machine learning

Model Management

- Easy and intuitive UI/UX for Model creation wizard and workflow
- Provides an unified process from dataset selection to model creation

Monitoring & Feedback

- Intuitive monitoring with specialized visualization technology
- Elaborate learning model reinforcement with user's feedback

Features

Professional

Flexible
- Dynamic Cluster structure (Effectively sharing GPU resources)
- Dynamic Scalability

Experience
Security data Machine Learning expertise
1) Conduct AI verification project for NIRS
2) True/False Positive detection analysis, failure prediction, anomaly detection

Rationality
- Reliable open source utilization
- H/W configuration based on volume and model
- Build with SIM, SOC solutions

Benefits

Accurate detection and analysis through machine learning based system

Comprehensive data analysis by machine learning model of AI

Shorten task processing, accident response time and fault handling and do **real-time cyber threat monitoring**

Rapid response to failure prediction through gathering device's status information

Work efficiency and speedy decision making through machine learning model for improving work process

Systematic and transparent task processing by artificial intelligence and Information sharing and accuracy enhancement

100%	98%	94%	100%
Algorithm	True Positive Detection	Anomaly Detection (Normal Scope)	GPU Clustering

Flexible Application

Latest and on demand Machine Learning algorithms are supported in AI platform.

Any user-created algorithms as well as DNN, RNN, CNN, Ensemble GAN can be applied.

Detection Accuracy

Hyper parameter application suitable for each algorithms' features.

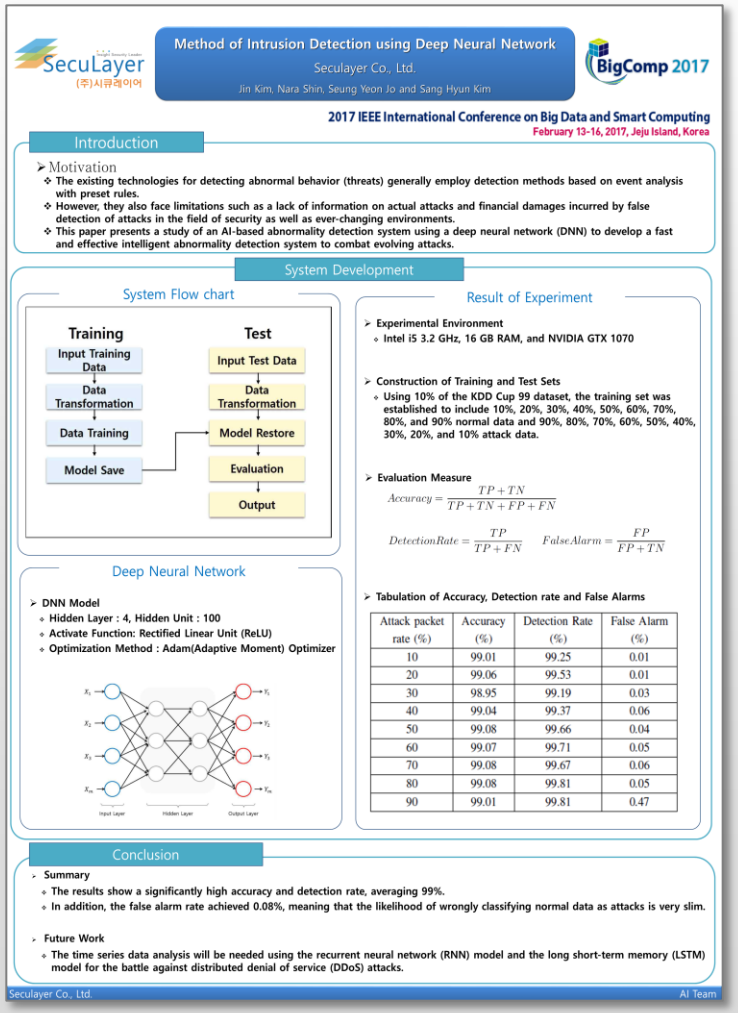
Optimized data conversion technology for collected, extracted then converted data to be used for machine learning.

GPU Clustering

Dynamic clustering architecture of GPU resources for effective data processing depending on the amount of data and complexity.

The study of the "Deep Neural Network using Method of Intrusion Detection" by Seculayer was adopted by the Big Comp,

IEEE International Conference.



2017 IEEE International Conference on Big Data and Smart Computing

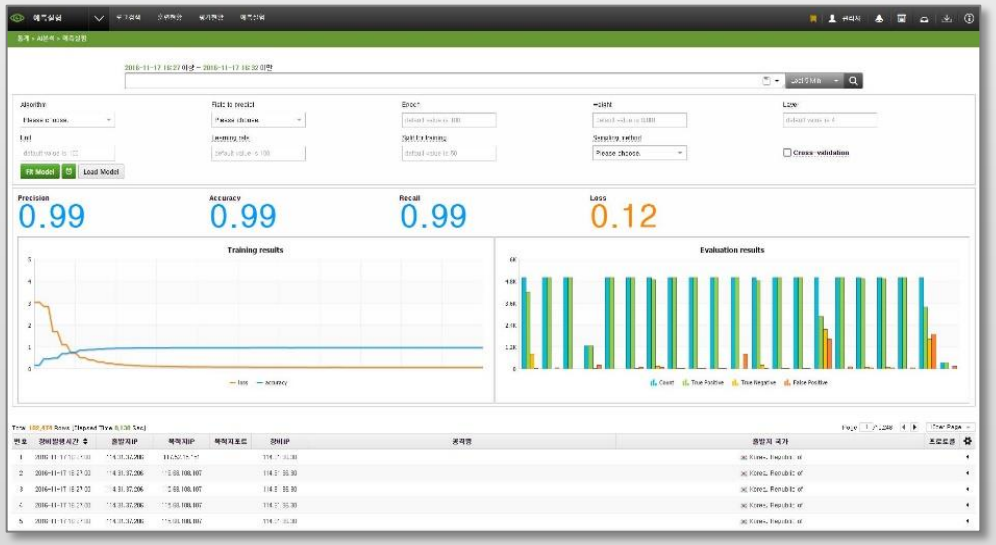
2017. 2. 13~16, Jeju Island, Korea

Method of Intrusion Detection using Deep Neural Network

- **Summary**

Data Accuracy is 99% on average and Detection Rate is 99% on average, confirming data detection rate and accuracy are very high.

False Alarm Rate is 0.08%. Confirmed false classification of the data is very low



Contents

Contents

3 Customer Use case

- **K-Gov. Agency - SIEM + SOC**
- **K-Gov. Agency - AI (Artificial Intelligence)**

K-Gov. Agency - 40 TB Daily Processing Data (800,000 eBooks volume)

Delaying response on security incident and system failure

Search item	Duration
Search on Firewall data	3 hours (Daily data) / 10 days (Monthly data)
Failure response	1 hour or so
Data analysis capacity	Tens of GB (limited)
Failure response time	Approximately 10 days
Control & MGMT scope	Visible security threats and system failures

Struggling with current ESM

Increasing operation systems to manage

- 30 Billion daily events (Volume : 30 ~ 38TB) to store and analyze
- Increasing every year

Tens of thousand of incoming data type

- Many different gathering data type
  - 7,426 meta data types
- Excessively variety of systems by open tender
  - Hard to standardize data structure

Narrow Control & MGMT scope

- Administrator has limitation to manage all systems in real time in terms of security and system operation status

Rapid spreading

- Spread and share security posture or system status with higher agency or correlation agency

SIEM+SOC - Performance improvement

Items	Duration (Before eyeCloudSIM) 2012	Duration (Current eyeCloudSIM) 2018
Search Performance (Daily / Monthly data)	3 hours / 10 days	1 Second / 20 Seconds
Data analysis capacity (6 Months)	Tens of GB	7 PB
System Failure Recovery	1 hour	5 Minutes
System Failure Analysis	10 days	3 Hours

Search Performance
For daily collected data
10,800%

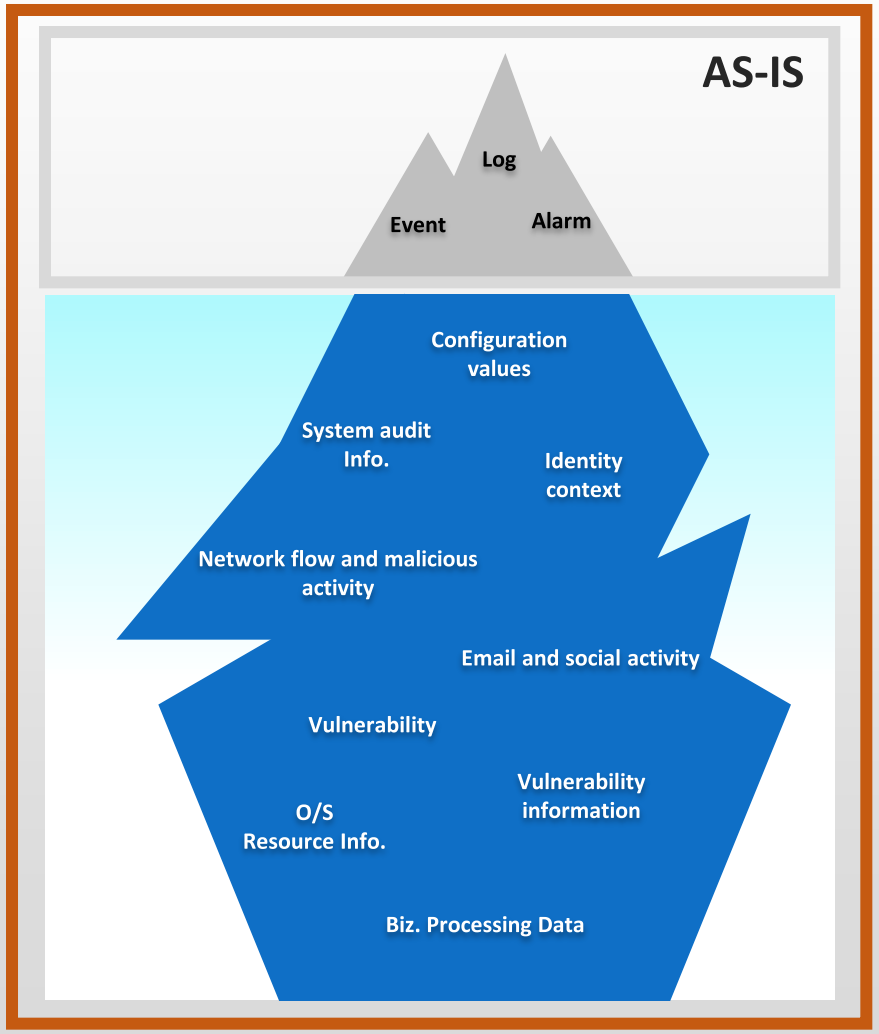
Storage Capacity
For data retention
70,000%

System Recovery
Time took to recover from incidents
120%

System Analysis
Time took to analyze resources and servers related to incidents
800%

▪ SIEM+SOC - Security Surveillance Scope

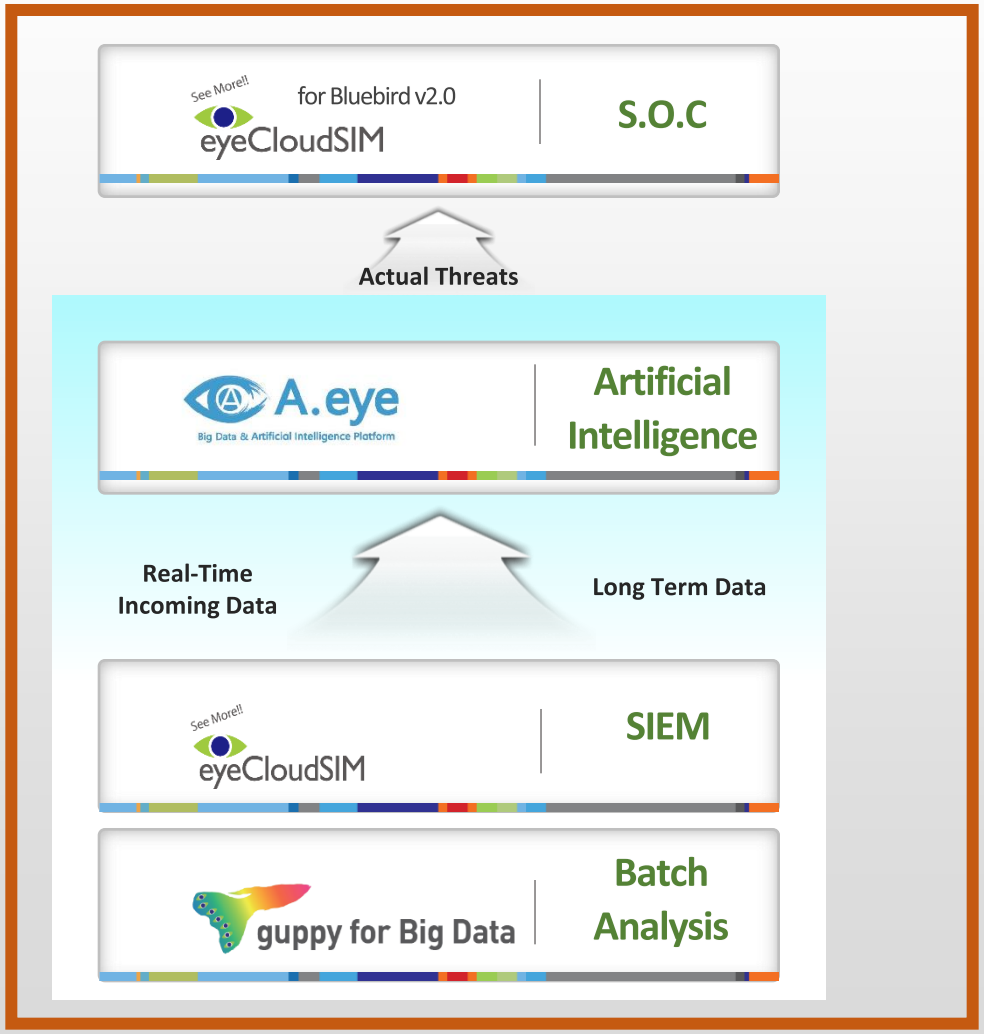
TO-BE (Security Surveillance Scope)



SEEN AREA

UNSEEN AREA

TO-BE (System Configuration)



Contents

3 Customer Usecase

- K-Gov. Agency - SIEM + SOC
- **K-Gov. Agency - AI (Artificial Intelligence)**

K-Gov. Agency - 40 TB Daily Processing Data (800,000 eBooks volume)

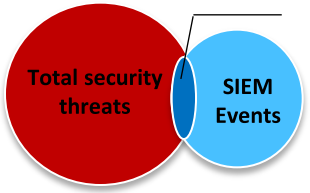
AS-IS

Diversification and Intelligence of Cyber Threats

Intelligence of malicious code technique	▪ Increased vulnerability attack with new obfuscation ▪ Simultaneous attacks
Korea targeted attack	▪ Increased spear phishing attacks combined with zero-day vulnerabilities
Large-scale Ransomware	▪ Intelligent / indiscriminate attacks ▪ Increase new attacks, like Ransomware

→ More organized, diversified and Evolving of cyber threats

Security Threat Response Limit



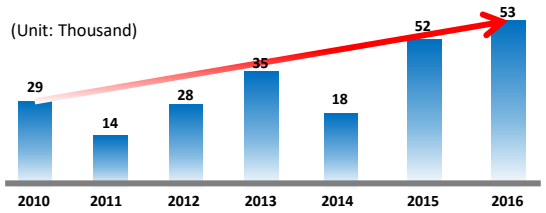
Control Security Event

▪ Building Big Data based security log collection system

▪ Signature-based countermeasures can not identify latent threats

→ Rule-based response system, Difficult to detect latent threats

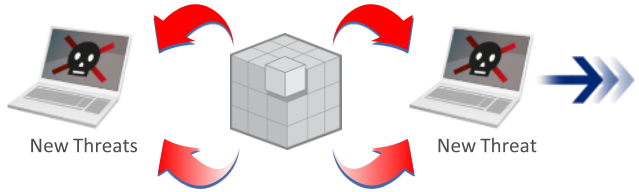
No. of response against cyber attack(2010~2016)



→ Significantly increases countermeasures

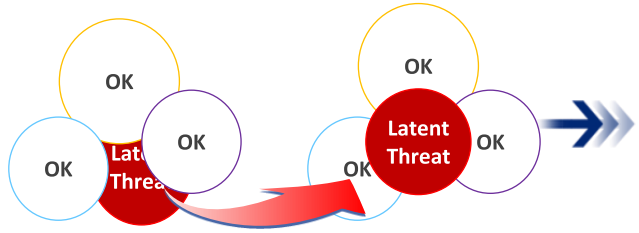
TO-BE

Requires preemptive response to new threats



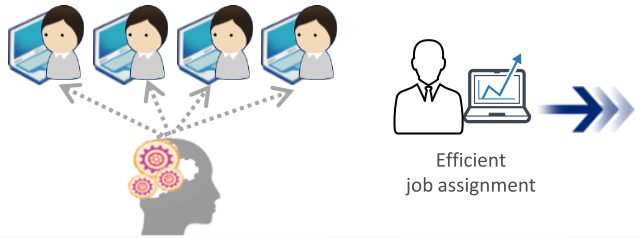
→ **Predicts new threats** to detect

Needs to detect latent threats



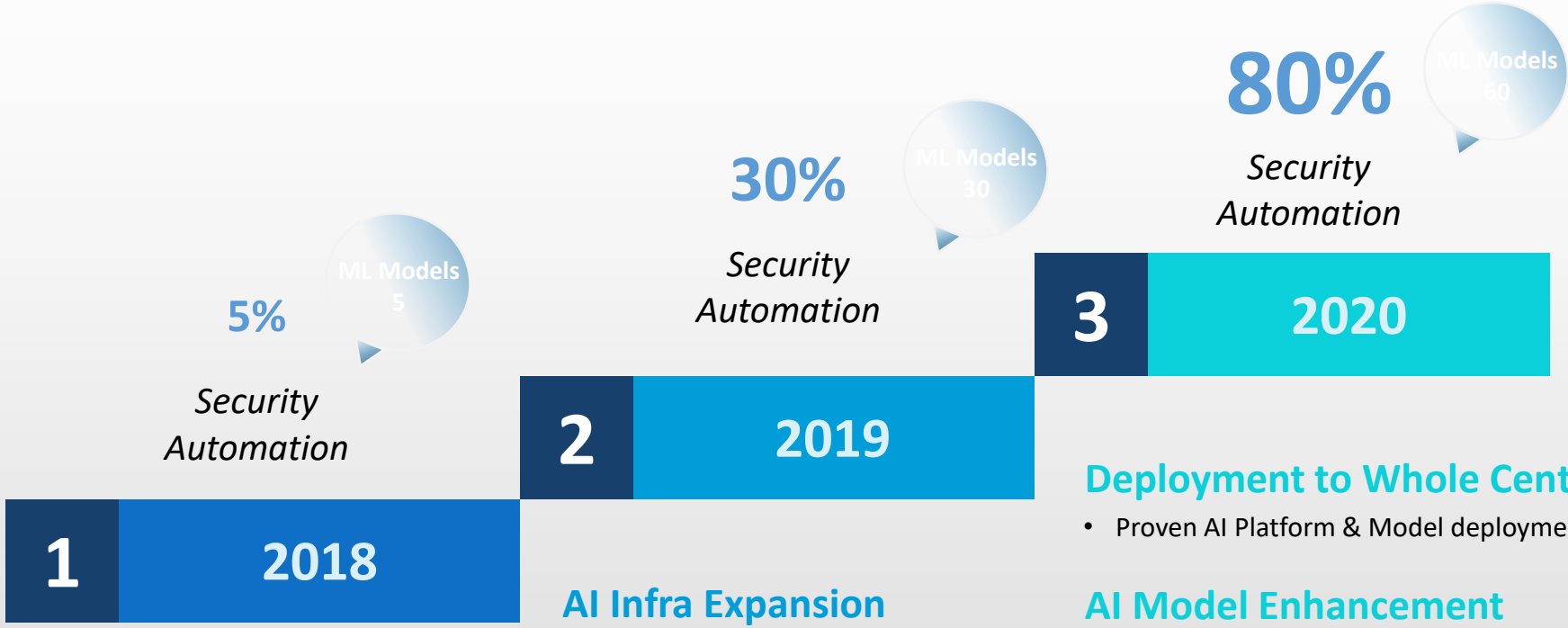
→ **Enhance security system** to detect latent threats

Needs Security automation



→ **Increase productivity** through task automation

AI - 3 Phases to complete the platform



Platform Implementation

- Knowledge Repository
- Machine Learning

Model Developemnt

- Security Detection & Anomaly models

AI Infra Expansion

- AI MGMT System
- AI Infra System

AI Model Enhancement

- Expansion of Model for Service

Security Intelligence

- Threat Intelligence Deployment

Deployment to Whole Center

- Proven AI Platform & Model deployment

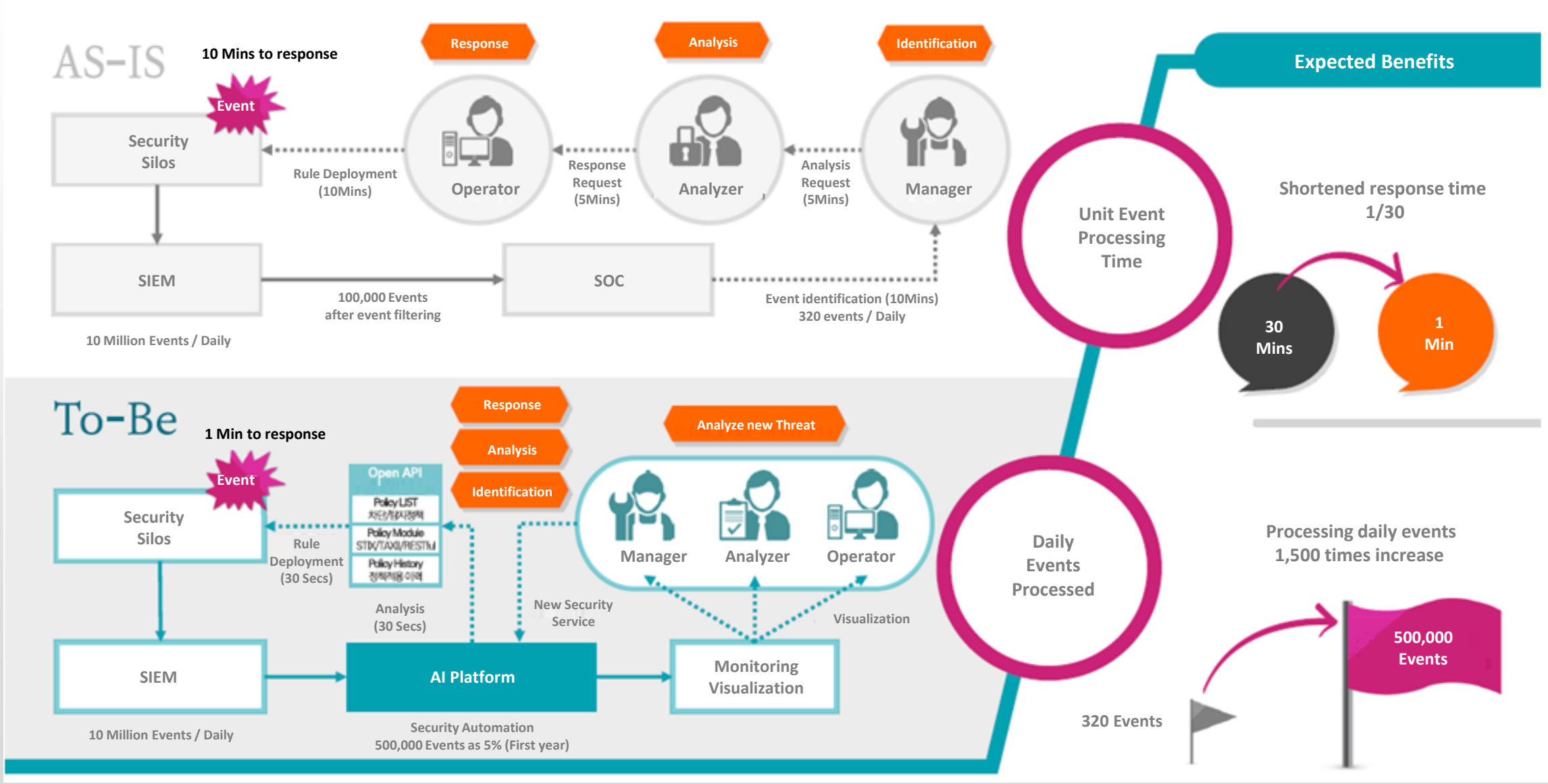
AI Model Enhancement

- Covers 1,5000 Public Services

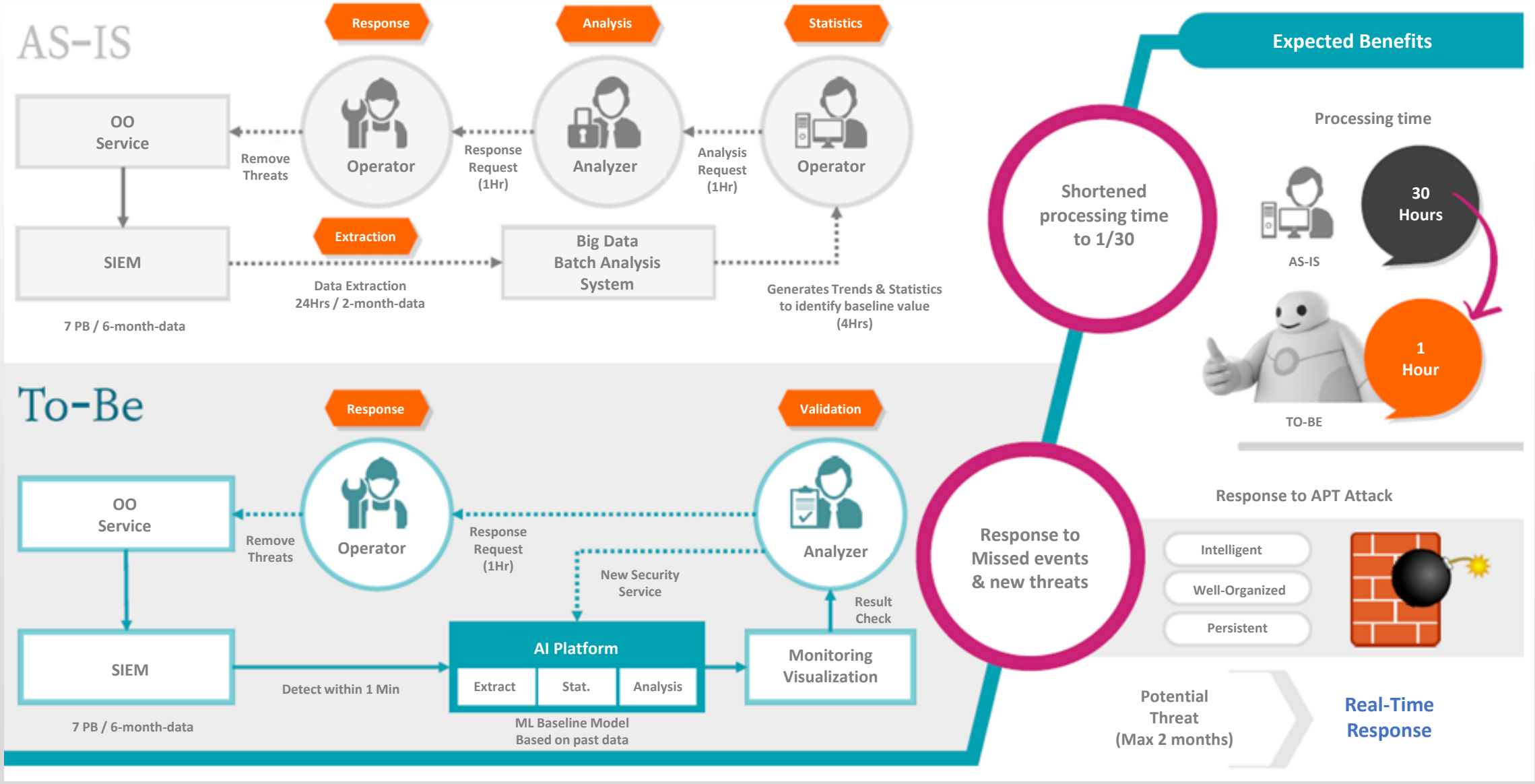
Interoperability to Silos

- For security automatic response

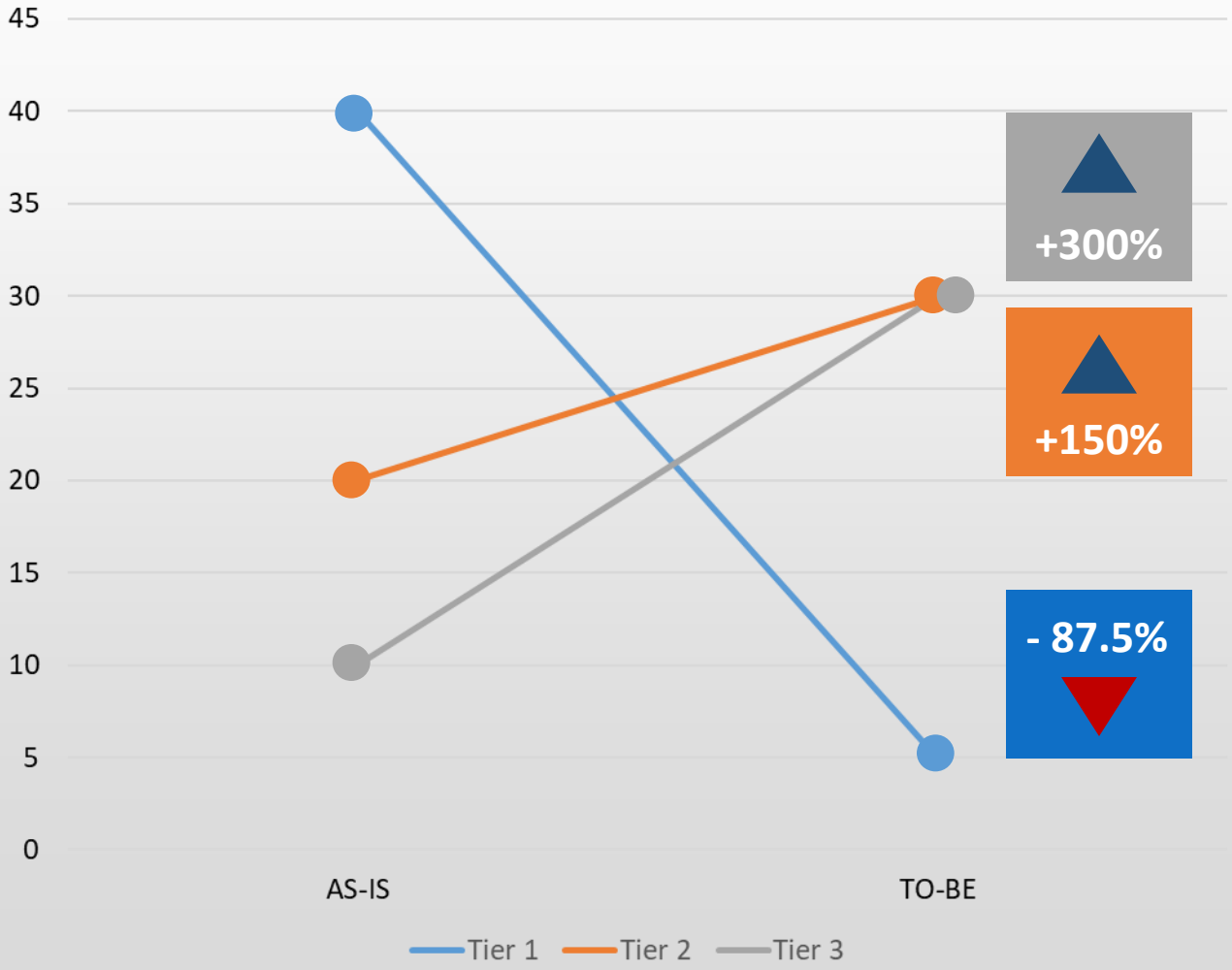
AI - Expected Outcome (Realtime Detection and Response)



AI - Expected Outcome (Anomaly Detection)



Much **reduce** simple monitoring Staff, **Enhance** Experts



Tier 1 (SOC Monitoring)

. Security Monitoring
. Security System Administrator

Tier 2 (SOC Triage)

. Senior Threat Response Analyst
. Threat Response Mitigation Analyst (Reactive)

Tier 3 (SOC Escalation)

. Threat Response Remediation Analyst (Proactive)
. Incident Case Manager

Why Seculayer?

Understanding Big Data

High understanding of security, systems, applications and big data gained from operating BIG DATA SYSTEM for 6 years.

Security-optimized AI platform

Differentiated and optimized AI platform rather than silo security AI, universal AI

Understanding Operating Environment

High understanding of public institution operating environment
(Policies, Security operations, cloud, servers & applications, etc.)

Thank you