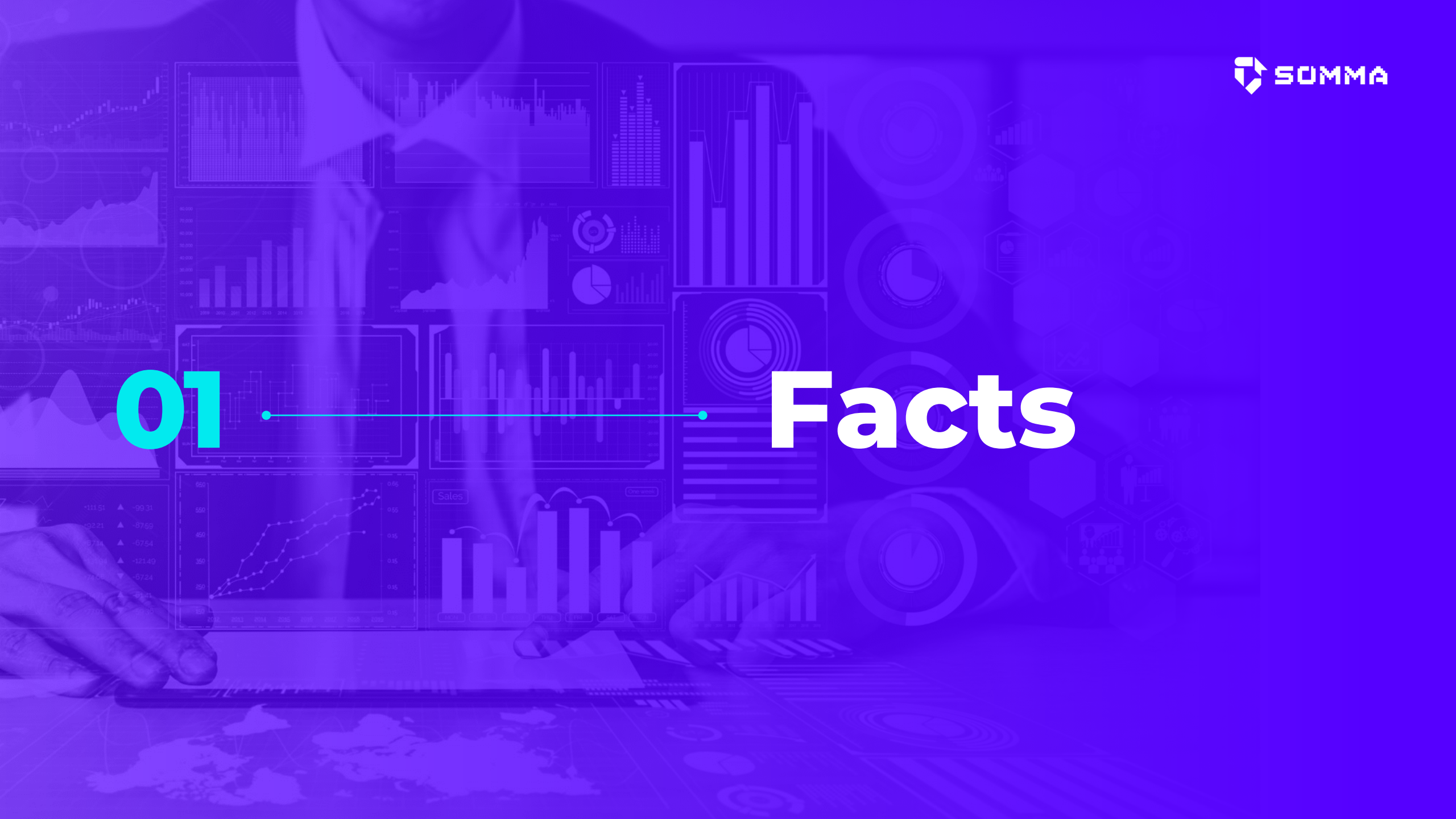
The best THREAT HUNTERS+ ever!

# Overview about

# SOMMA



# 01 Facts

# 01 Facts


**CEO/Founder**

## Mr. Yong-Hwan Roh

**Pre-A**

**Finance level**

**6**

**years running**

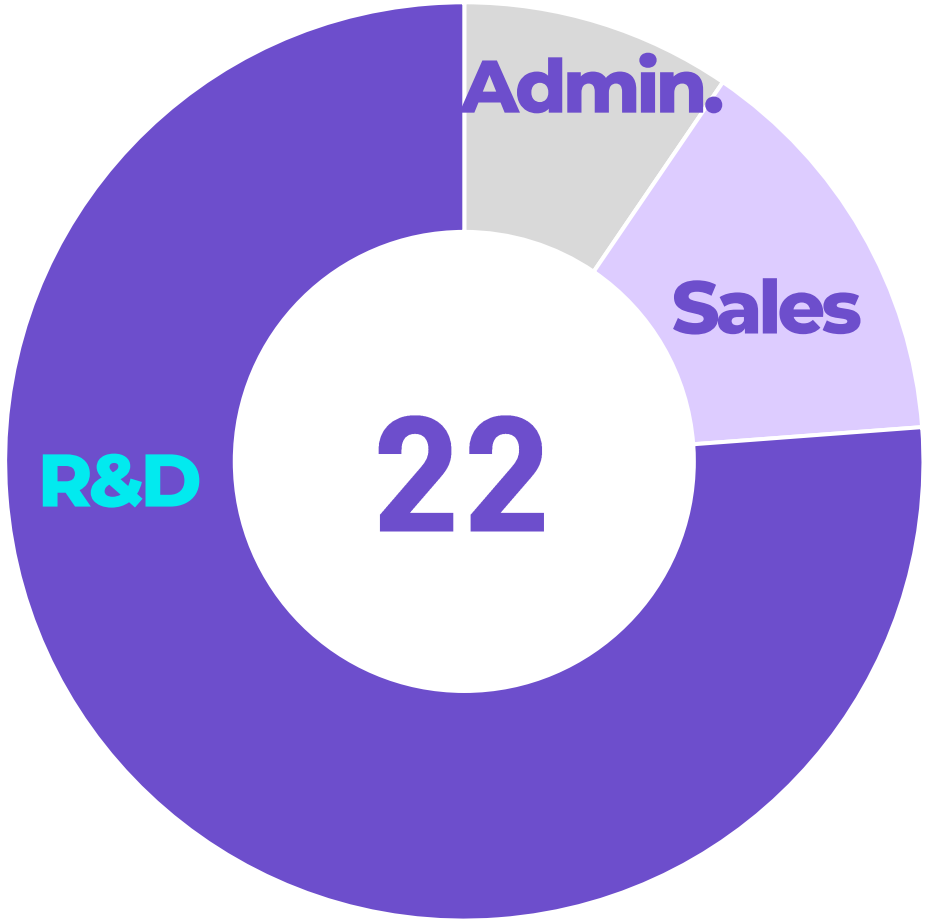
**22**

**hunters working**

# 02 Teams

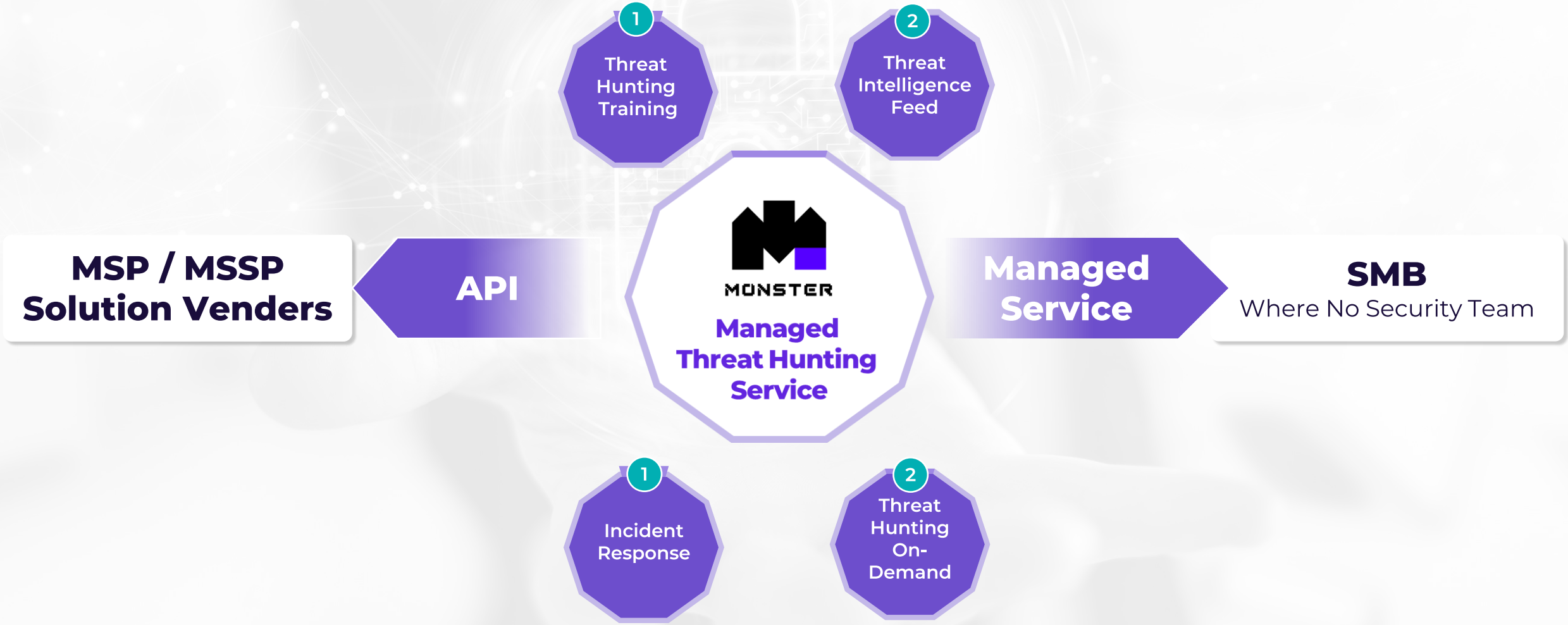
# 02 Teams


CEO
Administration
Sales & Marketing
R&D Lab.
Intelligence
Platform
Threat hunting


Admin.
Sales
R&D
22


SOMMA
03
Business

# Target


1
Threat Hunting Training
2
Threat Intelligence Feed
MSP / MSSP Solution Venders
API
MONSTER
Managed Threat Hunting Service
Managed Service
SMB
Where No Security Team
1
Incident Response
2
Threat Hunting On-Demand

# Achievement

## Customers

**Consumer**

AhnLab · JIRANSECURITY · SAINT SECURITY

**Military**

Hanwha Systems · LIG Nex1 · Agency for Defense Development · R.O.K CYBER COMMAND

**Public**

LH KOREA LAND & HOUSING CORPORATION · INNOPOLIS Foundation 연구개발특구진흥재단 · KISA Korea Internet & Security Agency · NSR 국가보안기술연구소 National Security Research Institute

**Overseas**

uppsalasecurity

| | | |
|---|---|---|
| 2018 | ADD Korea | developed intelligent cracking inference and cyber threat analysis system |
| | Saint Security | agreed technique interlocking for commercial threat intelligence to detect malignant code |
| | ADD Korea | developed APT attack simulator |
| 2019 | Ahn Lab. | agreed to share malignant detection technique and database usage |
| | Uppsala security | developed UppWall with Monster platform |
| | ADD Korea | Threat data creation to evaluate threat detection system |
| | NIS Korea | supplied Monster as platform |
| | ADD Korea | developed predict technique and intelligent analysis of cyber threat |
| 2020 | ADD Korea | developed technique of APT attack detection and real-time memory analysis |
| | KISA | nominated entrepreneur for cloud security advanced service |
| | Innopolis Foundation | nominated entrepreneur to consolidate capability for technical transfer business |
| | KISA | Bigdata AI dataset build for cyber security |
| | KISA | System build for active cyber threat information mining and supplied Monster as platform |
| | LH Korea | Bigdata platform project with Monster |
| 2021 | Korea cyber CMD | build structure for cyber threat analysis and development research |
| | ADD Korea | Cyber war simulation project, Cyber cracking inference project and etc. |
| | Ashin I | Co-developed agent for Nanny-On based Monster |

SOMMA

# 04 Technology

# Core technology

SOMMA

End-point agent

## Real-time data collection

- Monitoring all activity on the system in real-time
- Collecting behavioral data for threat analysis
- Scrapping volatile data

## High capability

- Light monitoring engine with 0.2Mil case per Min.
- Minimization system loading with data reduction
- Patent registered in Korea & the United States

## Response and liaison

- Real-time network control with connecting server and online policy
- Immediate response on incident threat

## Solution

ANY-Office

### Any-Office (Threat management for remote-working)

- Threat solution for remote-work management
- Control end-points based on White-list/black-list
- Cyber threat detection solution in remote-working system
- Bridge cyber security solution with ordinary enterprise solution

Nanny-On | AhnLab SMB PLACE

DocuONE | OfficeKeeper

## Business

- Pilot implementation for Korea Land & Housing Corporation for outsourcing management
- Prospective continuous adaption

LH 한국토지주택공사

- Security solution provider in Singapore
: End-point monitoring & control for Sentinel (2019)

uppsalasecurity

- Used for AI learning data set creation
Provided end-point monitoring agent to active honeypot system building

KISA

# Core technology

SOMMA

## Behavioral data analysis

### Data processing & storing

- Create and save meta data
- Manage data pipeline

### High-capacity distribution processing

- Monster data platform API
- API to access independent data
- Horizontally extendable distributed database
- Enhanced bigdata processing

### Threat detection

- Real-time, persistent & repeated threat detection
- Detection based threat intelligence and TTP(Tactics, Techniques, Procedures)
- Search anomaly behavior with Machine Learning/AI
- Transferred 2 patents
- Registered 1 Korean patent
- Applied 1 U.S. patent

## Threat intel.

### Technique advancement with intelligence

- Hold technical property with national security lab. ( 2 patents & 1 TTA cert. )
- Intelligence service associated with Saint security and malwares.com
- Malicious code data-sharing agreed with Ahnlab.

### Detection/Response advancement with Data

- R&D projects with military and national defense cybersecurity
- Cloud security service enhancement project with KISA
- MITRE Attack Evaluation participation

AhnLab | NSR | SAINT SECURITY | 한화시스템/시스템 | 국방과학연구소 Agency for Defense Development | LIG Nex1 | KISA 한국인터넷진흥원

## Business

### End-point threat management service (Pilot)

- Self-counter threat security management service (Lotte Data Comm.)
- SOC security service association in SMB (Ahnlab)
- Threat management service on systems by partner (LH)
- MOU on end-point threat management service to US (WeBridge, Inc.)

AhnLab | uppsalasecurity | webridge | 롯데정보통신 | CM | KISA 한국인터넷진흥원 | LH 한국토지주택공사

# Core technology

SOMMA

## Adversary emulation

### Single attack simulation

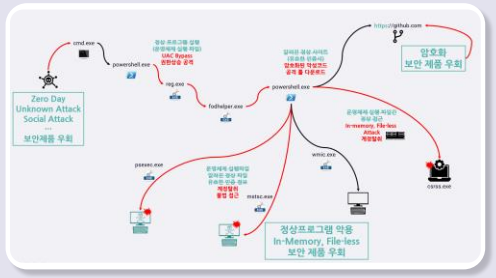
- Single attack simulation in MITRE ATT&CK matrix

### Attack scenario simulation

- Attack TTP(Tactics, Techniques, Procedures) simulation in Cyber range according to actual APT attack

### Data collection on attack behavior

- Improvement of vulnerability and creating threat analysis data through attack behavioral simulation




## Solution

CHEIRON

### Attack simulation based on MITRE ATT&CK

### Simulation on APT attack scenario

- Utilized in MONSTER platform for detection engine advancement
- Remediation adaptive UI/UX to scale up private and commercial

국방과학연구소 Agency for Defense Development | LIG Nex1 | AhnLab
한화시스템/시스템 | ATT&CK® | KAI

## Business

### Applied to dataset creation service

- Participants in Military cyber security R&D projects
- Cybersecurity Bigdata AI dataset build-up (KISA, 2020)

국방과학연구소 Agency for Defense Development

### Education of advanced cyber threats

- Applied military cybersecurity education & training programs
- Cyber threat hunting training on MITRE ATT&CK

# Why Data on Cloud is BETTER?

**Data on Cloud** is authentic power of SOMMA.


## Threat visuality

- Incident response readiness on attack
- Precise analysis and trail of breach

## Persistent threat detection

- Search past threats in reverse with the latest intelligence
- **Analyse the past data with present technique**

## One take, Multiple shot

- Detection with intelligence
- Threat detection with TTP
- Application based on ML/AI

SOMMA

# Reference

# Monster As A Platform (Custom Endpoint Threat Detection and Response)

SOMMA

## MONSTER End-Point Agent

Behavioral / Volatile data acquisition

- Original binary file
- System artifact

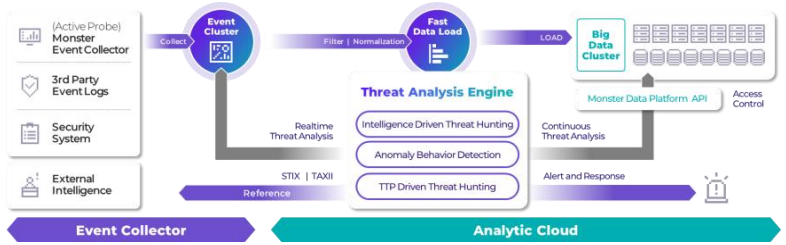
## MONSTER Dashboard

Threat detection and monitoring with incident analysis

Real-time data collection

**Interworking ordinary analytic system**

## MONSTER analytic server




## Existing analytic system

- OOO detection sys.
- OOO analytic sys.
- OOO analytic sys.

# Monster As A Platform (AnyOffice, Management for Remote work)

SOMMA

ANY-Office

## Control agent to executable range

### Process control

Opt.

Block

### Network control

Access

Block

### Threat response

Response anomaly behavior

## Policy management (On-premise)

ANY-Office

Security guidance

Setup & policy DB

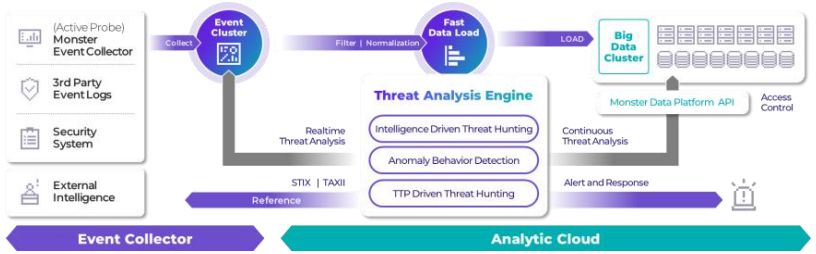
Management monitoring

- Monitoring dashboard
- Configuration management
- Policy management

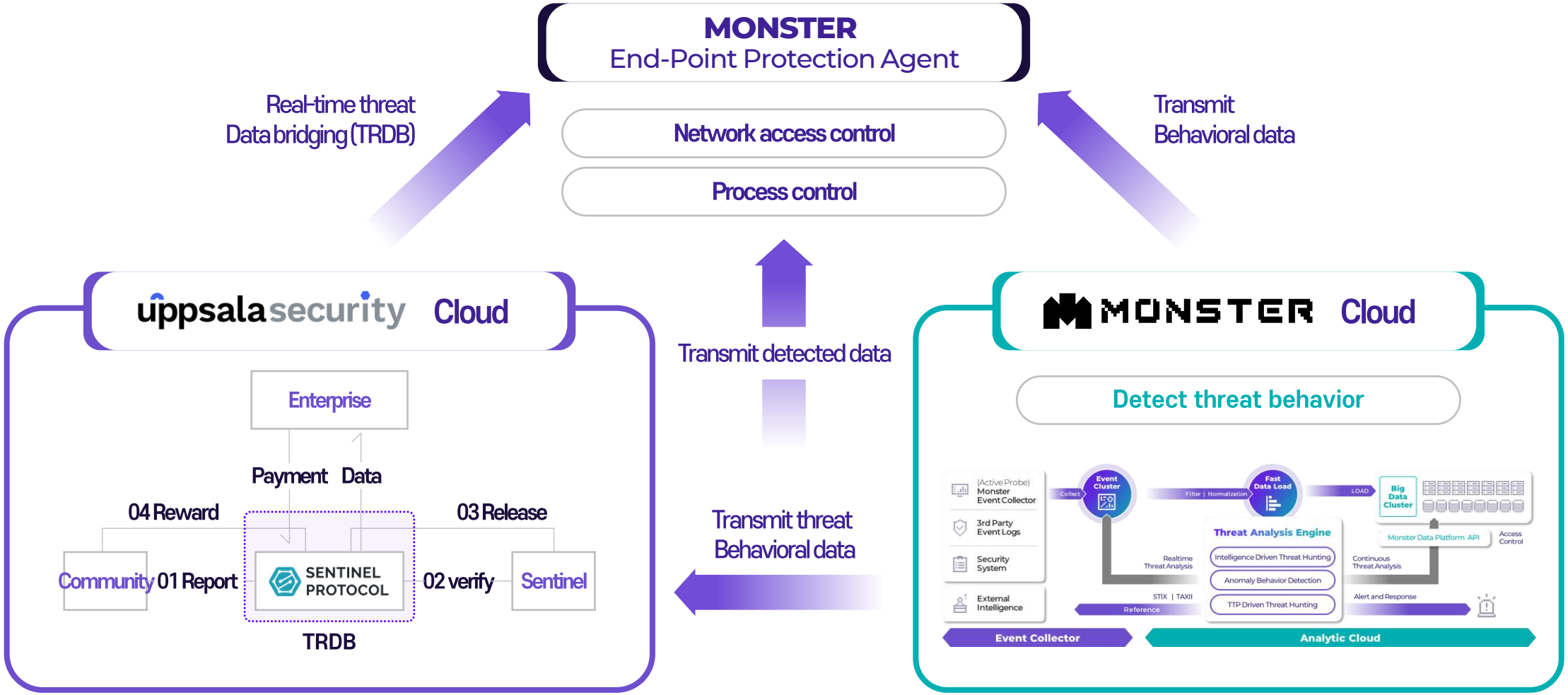
## End-point threat management (SaaS)

MONSTER

Behavioral data



# Monster As A Platform (Uppwall EPP with Uppsala security Inc.)



The Best Threat Hunters Ever ! SOMMA

# Thank you

MONSTER
CHEIRON
ANY-OFFICE

SOMMA https://www.somma.kr