AhnLab Managed Security Service for MS Azure

Jan. 2019

COMPANY AT A GLANCE

Microsoft Azure

Name	AhnLab, Inc.
Foundation	March 15, 1995
Headquarters	South Korea
Revenue	USD 147.6 Mil. (2017)
KOSDAQ-listed	Sep. 13, 2001
CEO	Chijung Kwon
Employees	1090
Global Operations	China, Japan
Business Portfolio	Endpoint security for enterprises and consumers Network appliance solutions Web security solutions Transaction security solutions **Managed Security Services**

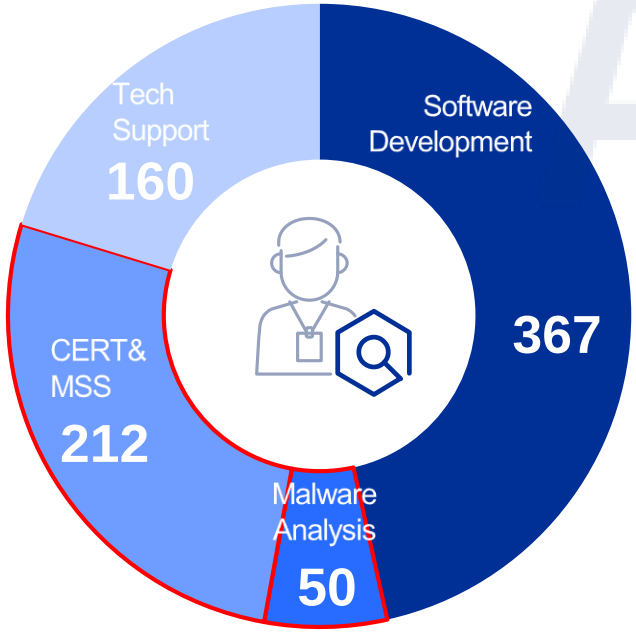
© AhnLab, Inc. All rights reserved.

Employees

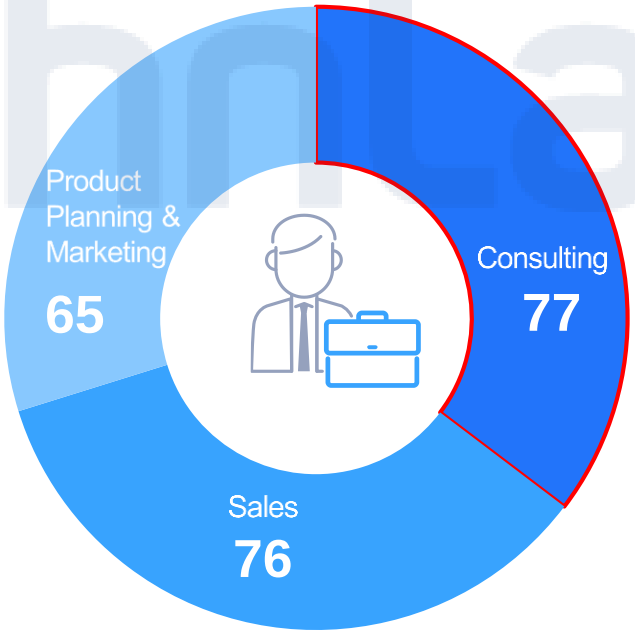
1,090 Total Employees

Over 70% of all employees are dedicated to research and development

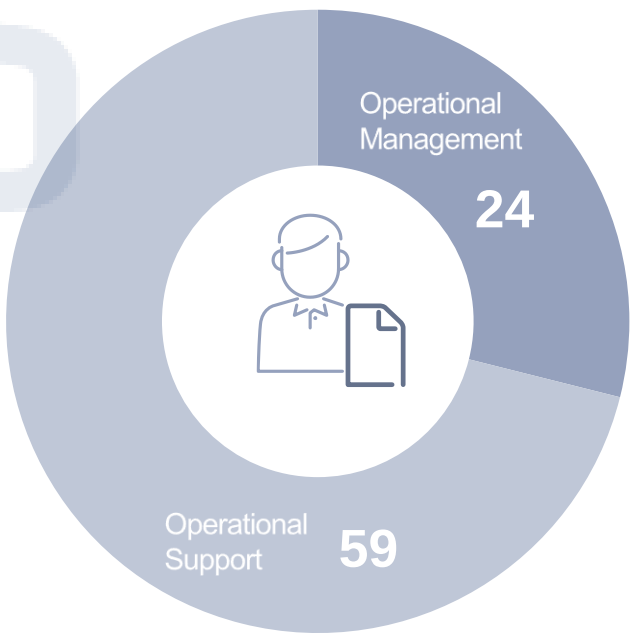
789 R&D Personnel



218 Business Personnel



83 Support Team Personnel



* As of August, 2018

© AhnLab, Inc. All rights reserved.

AhnLab's Security Infrastructure

24/7 Threat Monitoring and Response

through in-house malware analysis team and computer emergency response team (CERT)

ASEC

In-depth Malware Analysis

(AhnLab Security E-response Center)

- Collects and analyzes the latest malware
- Updates V3 engine, AhnLab's AV
- Monitors and analyzes network traffic
- Provides threat intelligence

Cooperates to respond to threats and attacks in real-time

CERT

Security Incident Response

(Computer Emergency Response Team)

- Monitors threats in customer field
- Collects threat information in real-time
- Responds to the reported incidents
- Offers managed security services

© AhnLab, Inc. All rights reserved.

Shared Responsibility for Cloud Security

Microsoft Azure

There are certain area belongs to customers in the Security Responsibility defined by Azure. It should be prepared and covered by yourself. How do you make it work?

On-Premises	IaaS	PaaS	SaaS
Users	Users	Users	Users
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network	Network	Network	Network
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Customer Responsibility

Cloud Provider Responsibility

© AhnLab, Inc. All rights reserved.

Managed Security Area

Microsoft Azure

Based on security responsibility model Azure offered, AhnLab defined managed security area to provide qualified services to our customers.

Customer	AhnLab	Cloud Service Provider
Platform, Applications, Identity	Network security policy settings	Data Center
Customer Data	Network security Solutions install and maintain	Network, CDN Infra
Server Side Encryption (File System And / Or Data)	Network security Solutions Monitoring	Cloud Basic Infra Services (Compute, Storage, Database)
Client Side Data Encryption & Data Integrity Authentication	Customer's network intrusion detection and response	
Network Traffic Projection	Optimize signature	

Detection Coverage

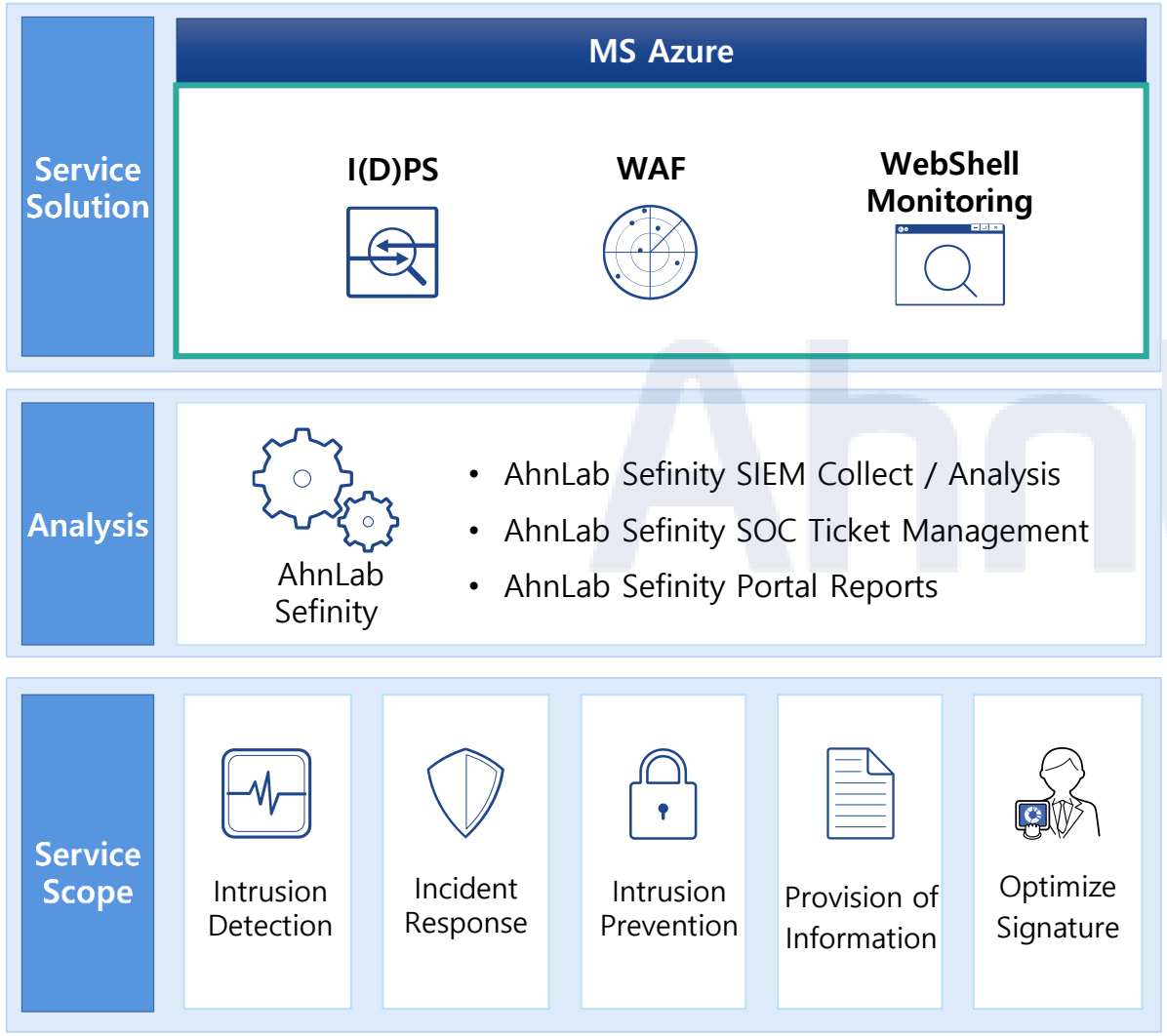
Next Generation Firewall (Available in 1Q, 2019)	IDS / IPS	WAF	Web Shell
L2~L7 Layer	The overall detection network (L3~L7 Layer)	Optimized detecting Web attacks (only L7 Layer)	Specialized services in detecting Web Shell

© AhnLab, Inc. All rights reserved.

AhnLab MSS Model & Scope

Microsoft Azure

In order to detect cyber attacks possibly lead to serious incidents, AhnLab MSS observe security threats and incidents real-time basis.



Service Scope	Service details
Intrusion Detection	- 24X365 Security Control - Event Monitoring/Analysis
Incident Response	- 24X365 Event monitoring - Analyzing & Responding Event - Responding Security Issues
Intrusion Prevention	- Various threat information - Terms of outsiders open port, check
Provision of Information	- Regular Security Trend & Incident Cases - Security Contents, Zero Day vulnerabilities etc.
Optimize Signature	- Intrusion prevention which are tailored precisely to customer systems

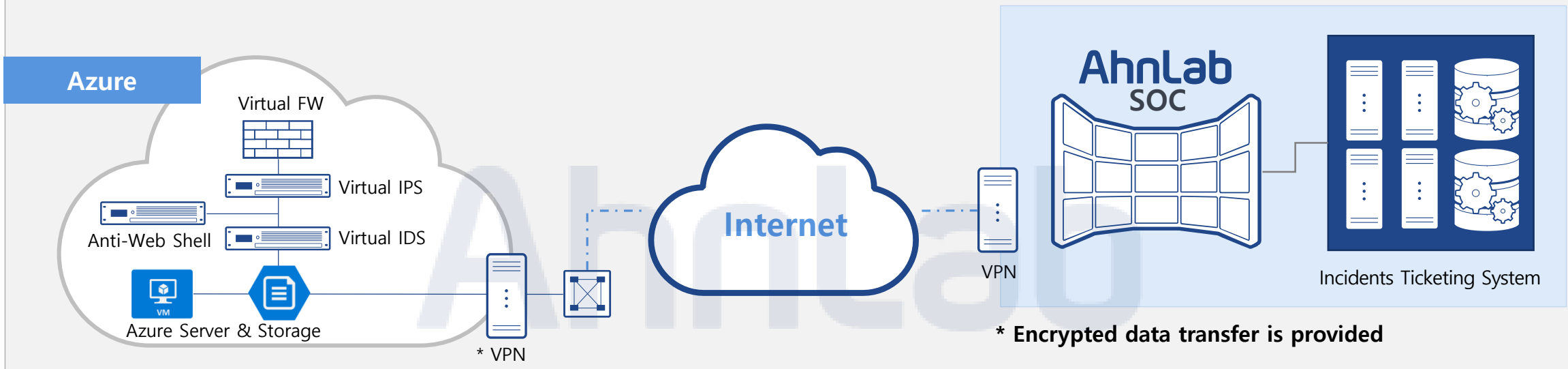
© AhnLab, Inc. All rights reserved.

General Configuration of Managed Security Services for Cloud

Microsoft Azure

AhnLab log collector on the Cloud collects data from solutions(virtual FW, IPS, and Anti-Webshell) and transfers to AhnLab Sefinity SIEM, which provides real-time data for intelligence analytics.

Service Configuration



Major Supported Venders

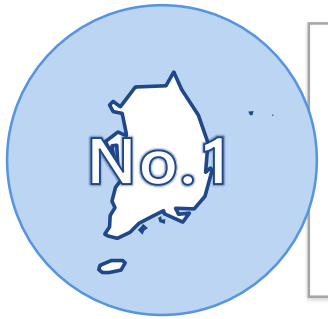
TREND MICRO, FORTINET, umv, MONITORAPP, Penta SECURITY, f5, Barracuda, paloalto NETWORKS, SSR Security Strategy Research, INSUNG 인성디지털

© AhnLab, Inc. All rights reserved.


AhnLab
Security Operation Center

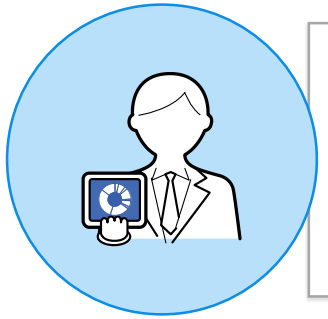
Competitive Forces

Microsoft Azure



First-Mover In Korea,

- AhnLab launched MSS for the Cloud as a first mover in Korea (Oct 2015)
- Providing MSS with Media, Games, Contents, Manufacturing, more than 20 Various Industry Customers
- **Deliver MSS to Global Enterprises with 300 Cloud computing severs**



Cloud Native MSS
Experts

- **AS for a Cloud native MSSP, AhnLab has a self-made response system against a variety of attacks**
- AhnLab has a specialty for monitoring threats and incidents on the public Cloud
- By embracing Third-Party Solutions on the Cloud, **AhnLab has multiple detection scenarios and own methodology**

Dedicated R&D for
Analytics and MSS Platform

- AhnLab A-CERT provides **premium services** like penetration test, malware analysis, forensic, incident response, etc)
- **Develop Machine Learning/AI-based Analytics** for intelligent automatic response (Minimize Human Errors)

© AhnLab, Inc. All rights reserved.

AhnLab MSS Platform, Sefinity

Microsoft Azure

AhnLab Managed Security Service delivered by Sefinity SIEM • SOC • Portal • Threat Intelligence.

External Systems

- QRadar
- Arcsight
- Splunk
- VirusTotal
- IBM X-Force
- Infra Manager
- Monitoring
- Scanner
- LogServer
- Knowledge System

External System Interface

Sefinity

Repository (Oracle, Elastic search)

Transaction	Console	SOC	SMS	E-Mail
Event Analysis	Log Verification		Aggregation	
	Impact Analysis		Focus Recognition	
	Scenario Modeling			
Event Collection	Status Checker		Log Collector	
	Flow Detection		ASD Connected Eng	
Log Normalization	Creating Regular Expressions for about 80 security devices			

Message Queue (Kafka)

AhnLab Internal System Interface

Automation
(Incident Response, FW Rules)

Malicious File Analysis

Malicious URL Analysis
(ActiveHoneyPot)

Alive Check
(SSM,HostMonitor)

Network
- NG Firewall/IPS WAF/DDoS
- Traffic Flow, Packet

Server /DB/App
- WEB/WAS
- OS/Application
- DB transaction

End-Point
- Integrated account Management
- Device Control
- Anti-Virus

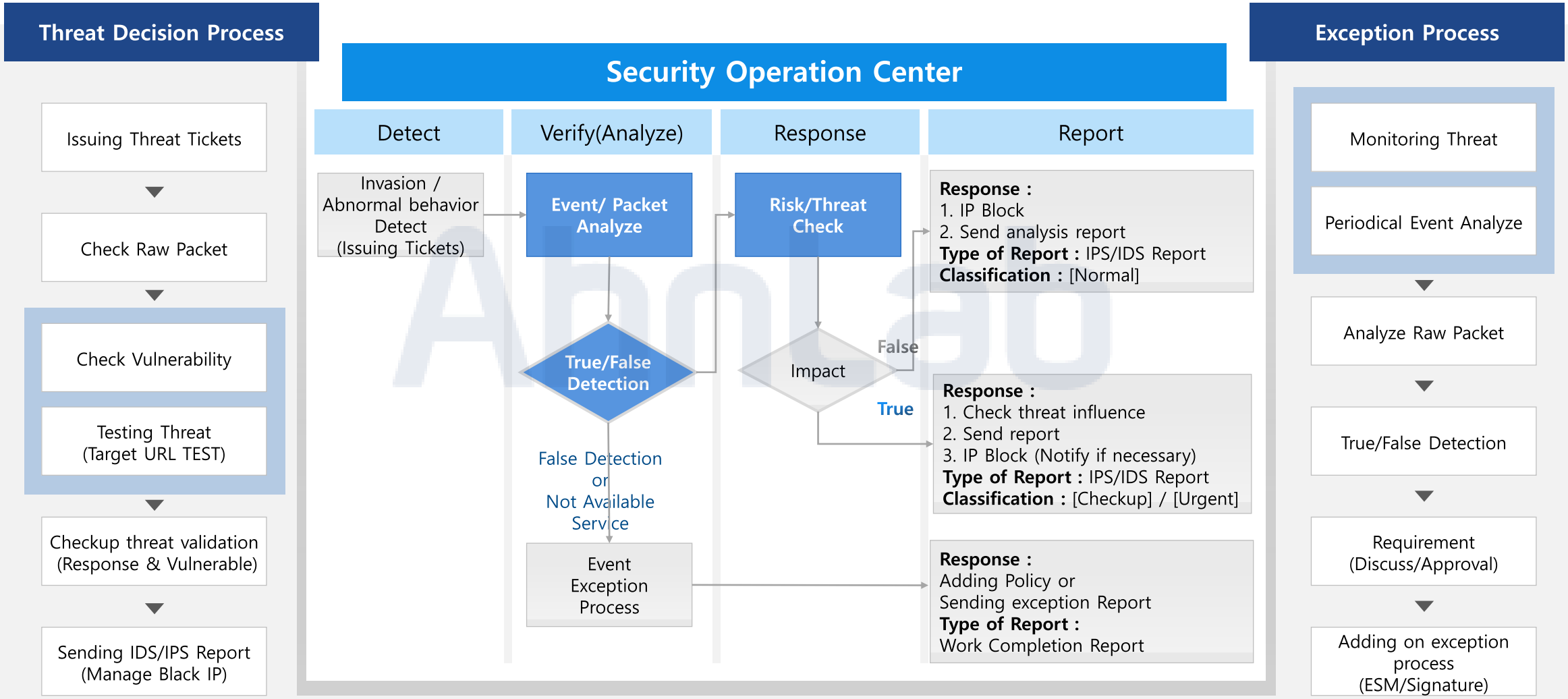
Compliance
- Personnel Info.
- Access Control
- Printed Documents

© AhnLab, Inc. All rights reserved.

Threat Response Process

Microsoft Azure

Decide risk level and analyze threats on the knowledge-based system. We are enhancing our service with AI-based correlation analytics.

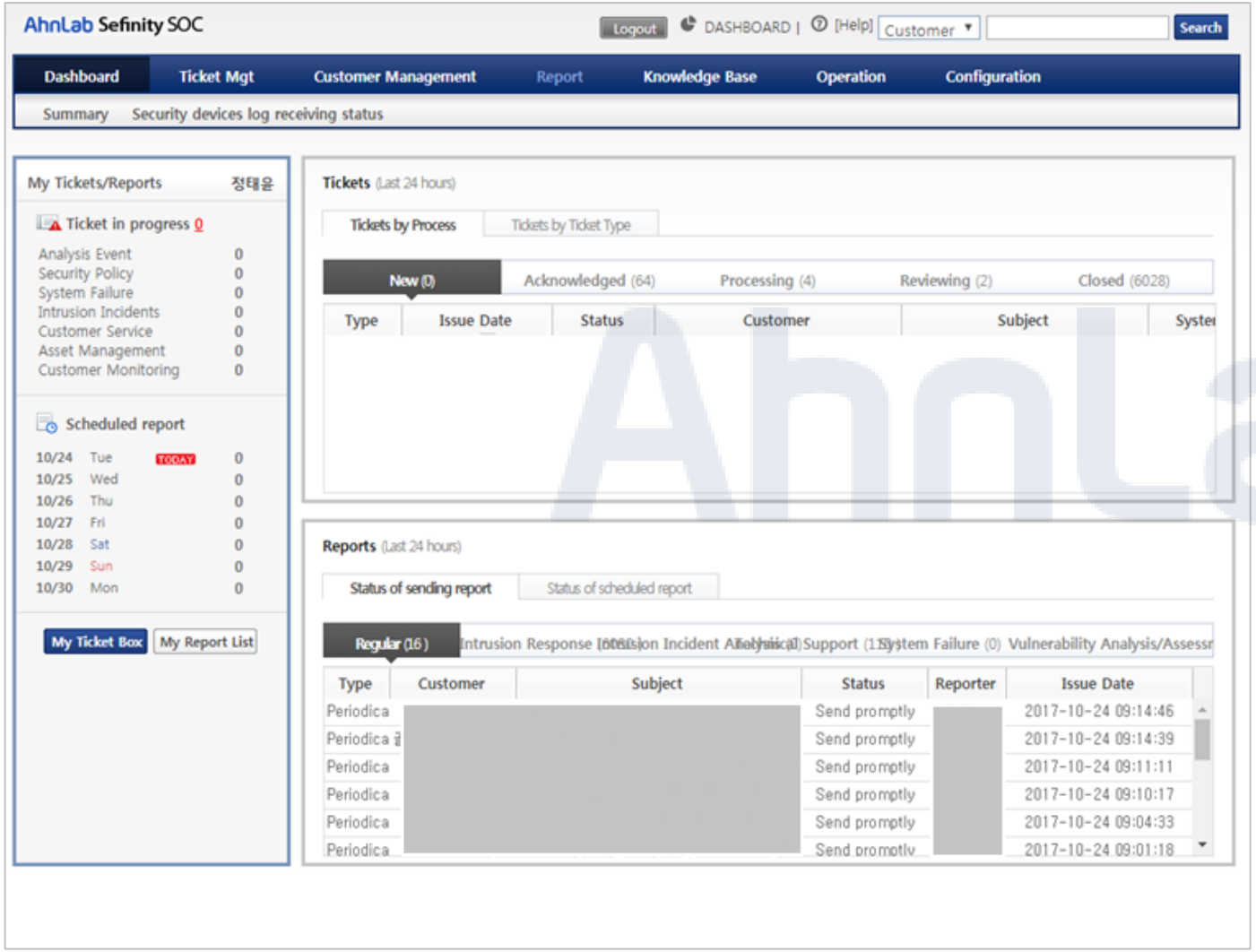


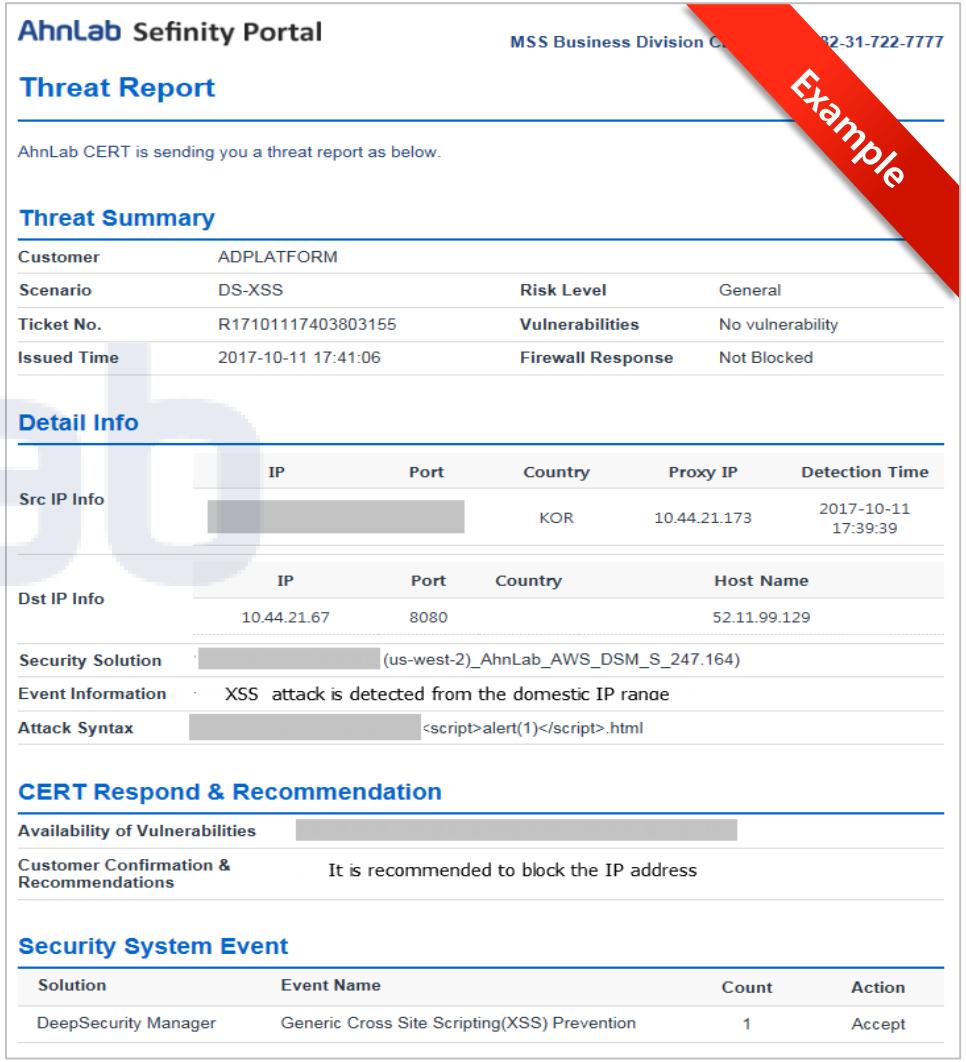
© AhnLab, Inc. All rights reserved.

Threat Response Process

Microsoft Azure

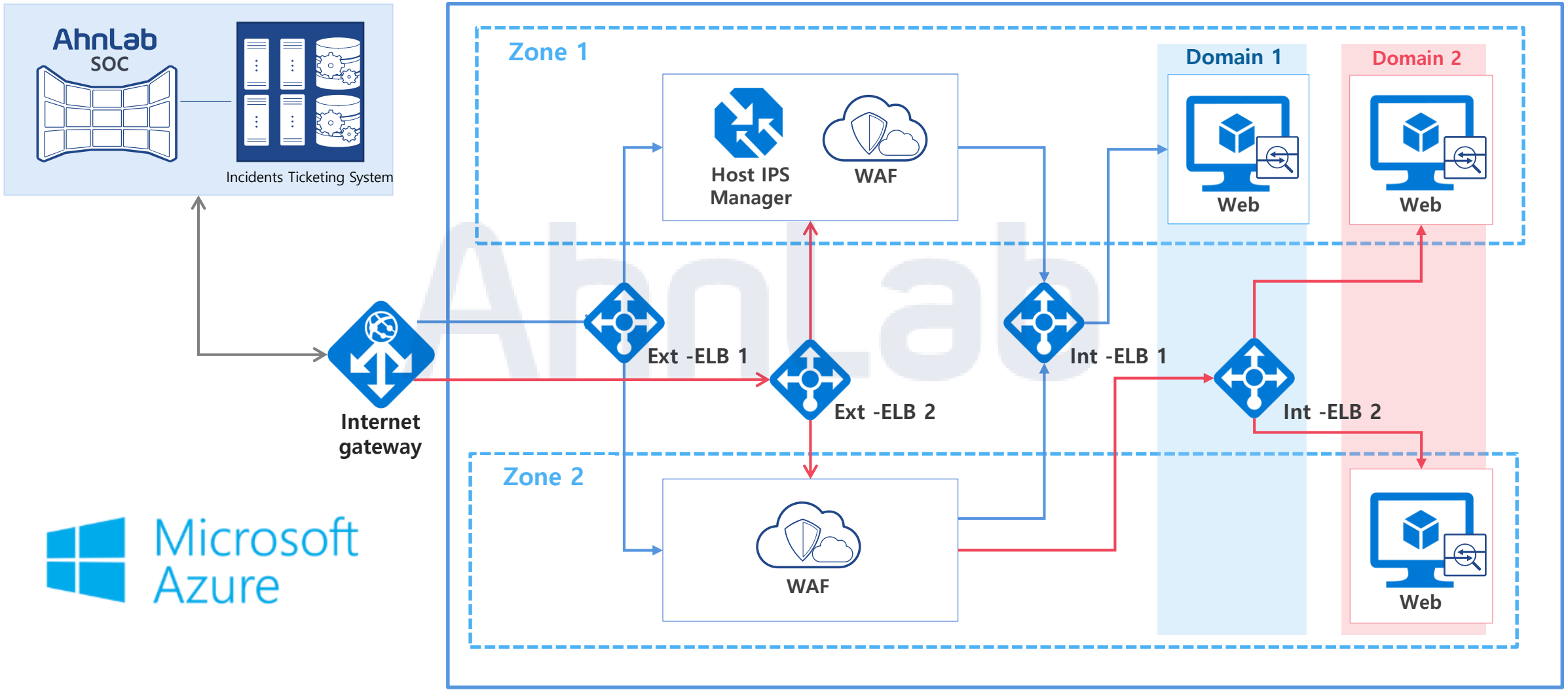
AhnLab developed Ticket Management System is developing with automation and orchestration technology.





© AhnLab, Inc. All rights reserved.

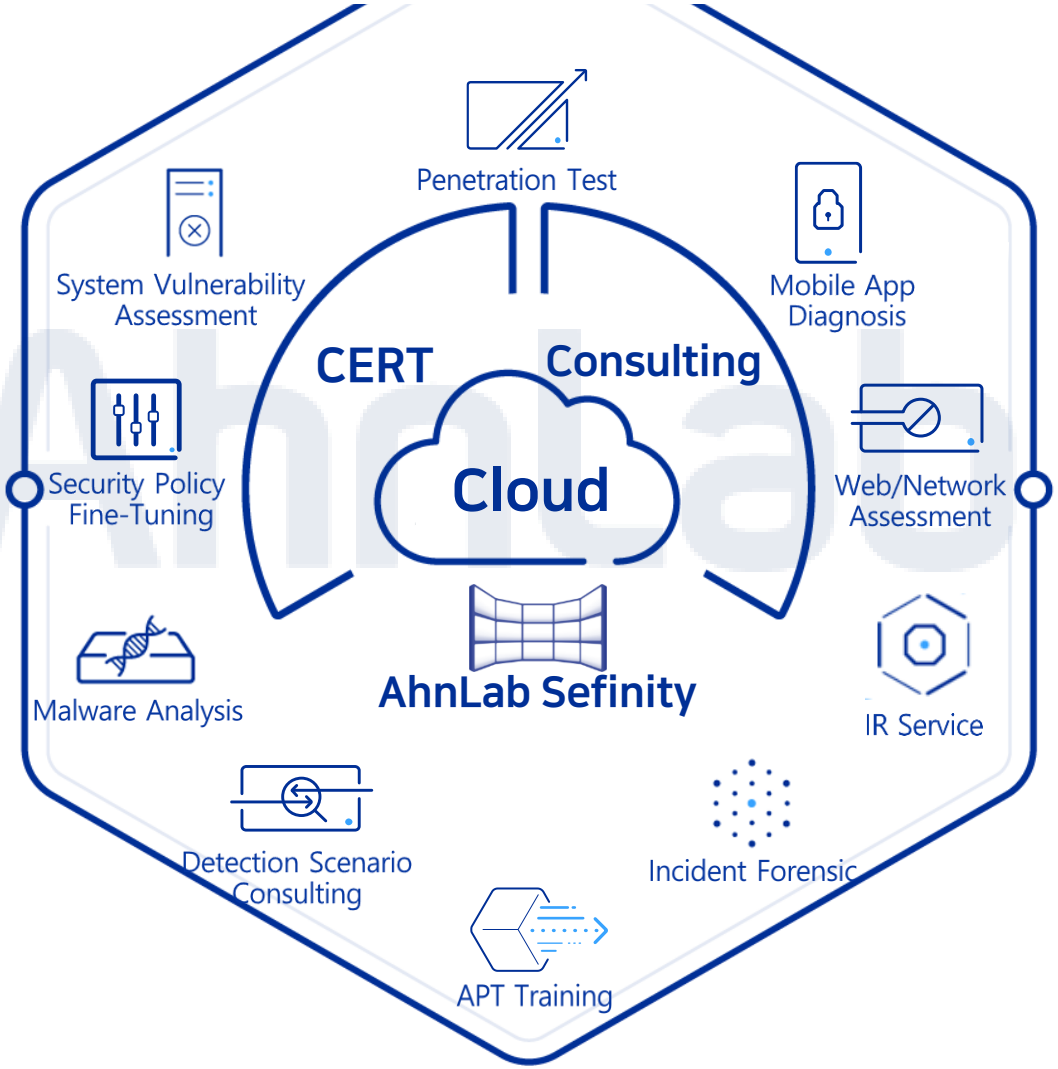
Azure Configuration



© AhnLab, Inc. All rights reserved.

AhnLab MSS Eco-System

Microsoft Azure



© AhnLab, Inc. All rights reserved.

Thank you.

More Security More Freedom

AhnLab