2024
Future of Hospitality

최신 보안 위협 동향 및 대응방안

(주)태광네트웍정보 Total Network Solutions Provider with AhnLab

㈜태광네트웍정보

국내 최고의 보안 및 네트워크 솔루션 전문 기업으로 컨설팅에서 설계, 네트워크 구축 및 통합유지보수까지 **Total Network Service**를 제공합니다.

AhnLab
조달총판

kt Managed Service
네트워크/정보보안 공인협력사

RUCKUS COMMSCOPE
Elite Partner

사업영역

유 · 무선 / 정보보안 통합네트워크

주요고객사

24년 업력의 성공적인 구축 역량과 경험으로 고객의 IT 경쟁력과 가치를 향상 시킵니다.

호텔/공공/금융/일반기업/교육 등 다양한 분야의 우수한 기업들이 태광네트웍정보와 함께 하고 있습니다.

InterContinental Seoul COEX
Fairfield by Marriott
Sejong
metro HOTEL Myeongdong, Seoul
Henn na Hotel 東京ホテル
Mondrian Seoul Itaewon
Hotel Koreana
Hamilton Hotel

* 호텔 분야 주요 고객사

최신 보안 위협 동향 및 대응방안

안랩 솔루션컨설팅팀 원동현 팀장

CONTENTS

최근 악성코드 동향

악성코드 통계

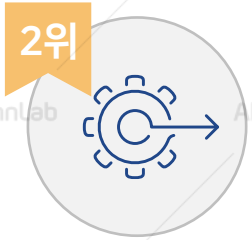
1위

Infostealer

44.6%

다양한 자격증명 정보를 탈취하는 악성코드

2위



Downloader

43.9%

다른 유형의 악성코드로 추가로
다운로드 받아 공격을 진행하는 악성코드

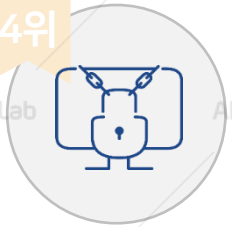
3위

Backdoor

9.5%

추후 악성 행위를 위해 시스템에
설치하는 악성코드

4위



Ransomeware

2.0%

데이터 암호화를 인질삼아 협박을 통해
금전을 갈취하는 악성코드

피싱 이메일 통계

1위

FakePage

36%

페이지 모방으로 계정 패스워드 입력 유도

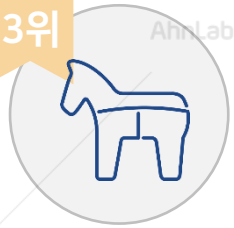
2위

Infostealer

27%

웹, 메일, FTP 등 자격증명 정보 탈취

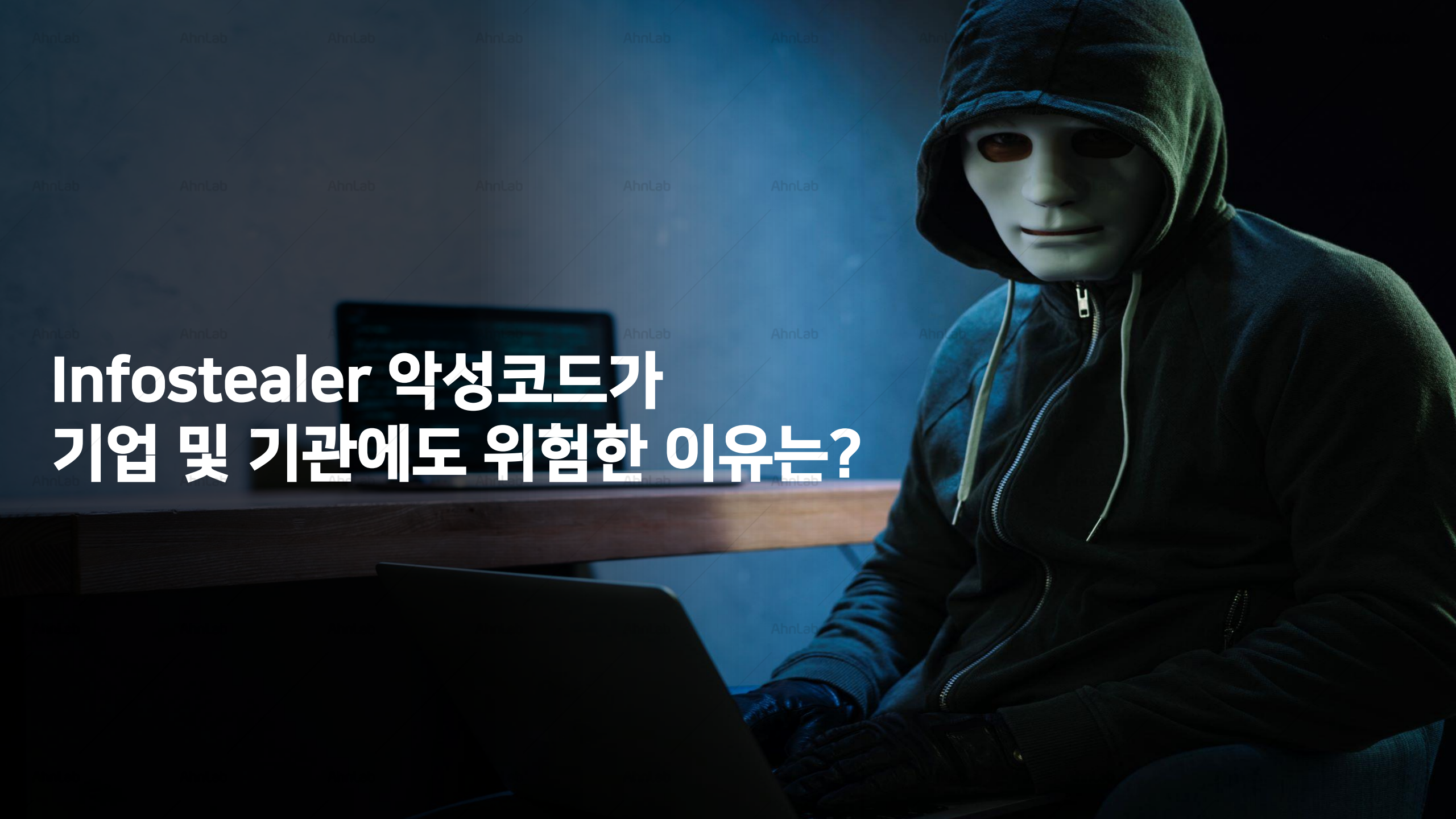
3위



Trojan

22%

정상으로 위장하여 다양한 악성행위 수행



Infostealer 악성코드가 기업 및 기관에도 위험한 이유는?

Malware as a Service

서비스 형태의 빌더 제작으로
Drakweb 등의 **해킹 포럼을 통해 판매**

Initial Access

단순 탈취에 그치지 않고
수집된 정보를 바탕으로 **조직 침투에 활용**

Credential Stuffing

탈취한 자격증명 정보를 활용하여
타 사이트의 암호 또는 **사용할 암호도 예측**

2차, 3차 공격 활용으로
대형 정보유출 사고로 이어지는 결과 초래

APT vs Ransomware

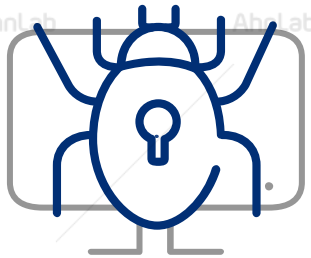
APT

- 은밀하게
- 장기간 잠복
- 주요 정보 유출

VS

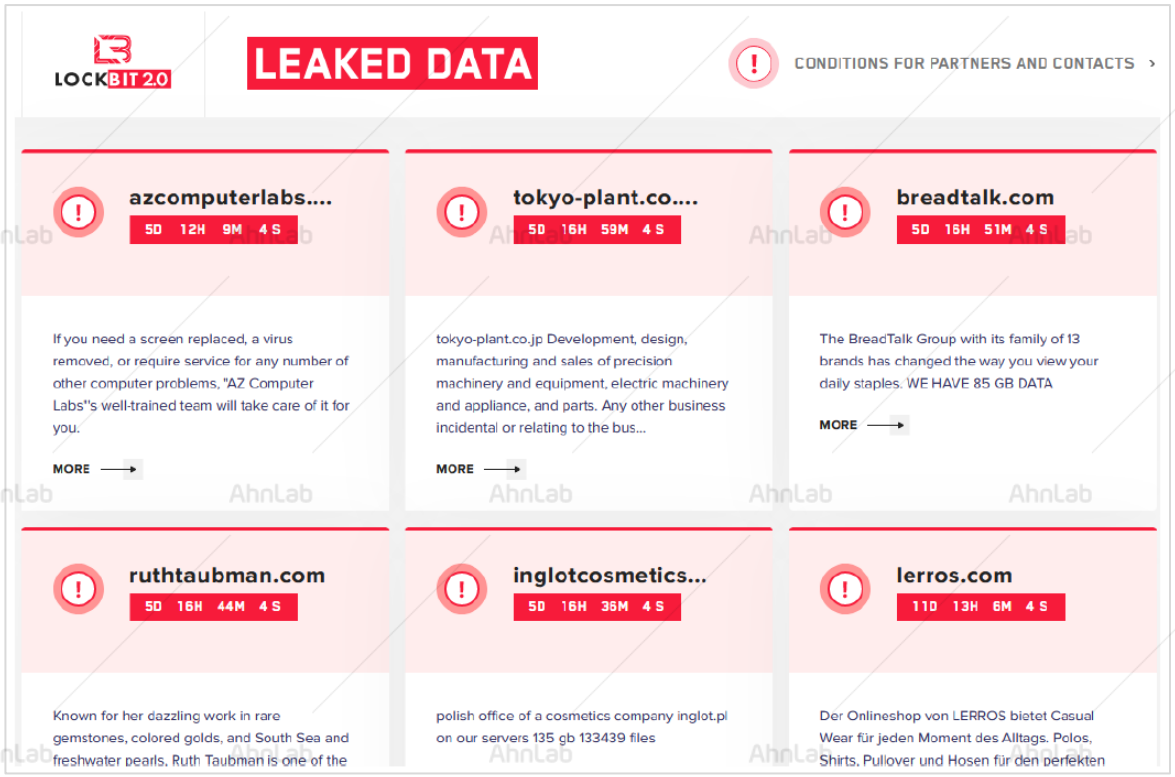
Ransomware

- 은밀하지 않게
- 단기간에
- 주요 정보 암호화



APT 공격 방식 + Ransomware 감염

2중 협박 (Double Extorsion)



탈취 정보 공개

금전적 보상 요구

APT Groups Techniques

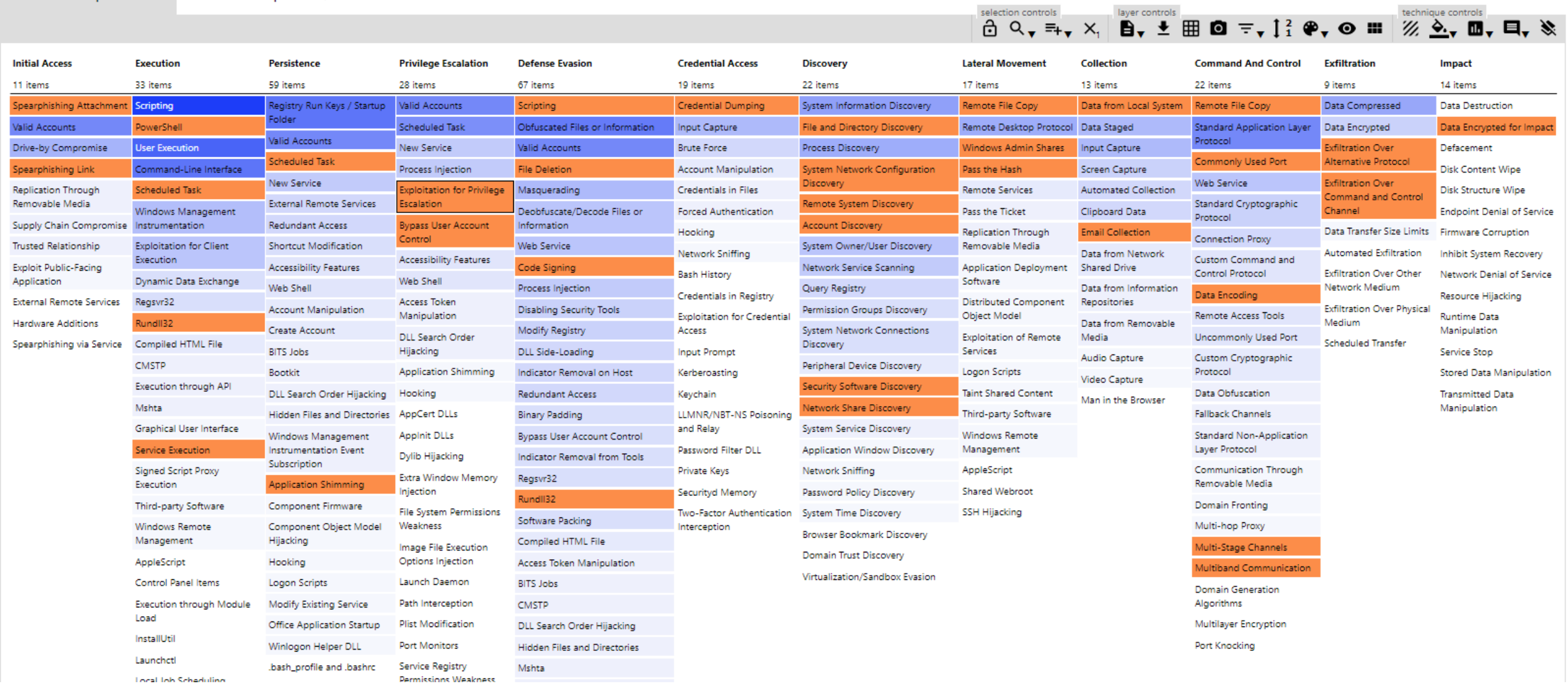
All APT Group + CLOP | All APT Group

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
Spearphishing Attachment	Scripting	Registry Run Keys / Startup Folder	Valid Accounts	Scripting	Credential Dumping	System Information Discovery	Remote File Copy	Data from Local System	Remote File Copy	Data Compressed	Data Destruction
Valid Accounts	PowerShell	Valid Accounts	Scheduled Task	Obfuscated Files or Information	Input Capture	File and Directory Discovery	Remote Desktop Protocol	Data Staged	Standard Application Layer Protocol	Data Encrypted	Data Encrypted for Impact
Drive-by Compromise	User Execution	Scheduled Task	New Service	Valid Accounts	Brute Force	Process Discovery	Windows Admin Shares	Input Capture	Commonly Used Port	Exfiltration Over Alternative Protocol	Defacement
Spearphishing Link	Command-Line Interface	New Service	Process Injection	File Deletion	Account Manipulation	System Network Configuration Discovery	Pass the Hash	Screen Capture	Web Service	Exfiltration Over Command and Control Channel	Disk Content Wipe
Replication Through Removable Media	Scheduled Task	External Remote Services	Exploitation for Privilege Escalation	Masquerading	Credentials in Files	Remote System Discovery	Remote Services	Automated Collection	Standard Cryptographic Protocol	Data Transfer Size Limits	Disk Structure Wipe
Supply Chain Compromise	Windows Management Instrumentation	Redundant Access	Bypass User Account Control	Deobfuscate/Decode Files or Information	Forced Authentication	Account Discovery	Pass the Ticket	Clipboard Data	Connection Proxy	Automated Exfiltration	Endpoint Denial of Service
Trusted Relationship	Exploitation for Client Execution	Shortcut Modification	Accessibility Features	Web Service	Hooking	System Owner/User Discovery	Replication Through Removable Media	Email Collection	Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Firmware Corruption
Exploit Public-Facing Application	Dynamic Data Exchange	Accessibility Features	Web Shell	Code Signing	Network Sniffing	Network Service Scanning	Application Deployment Software	Data from Network Shared Drive	Data Encoding	Exfiltration Over Physical Medium	Inhibit System Recovery
External Remote Services	Regsvr32	Web Shell	Access Token Manipulation	Process Injection	Bash History	Query Registry	Distributed Component Object Model	Data from Information Repositories	Remote Access Tools	Scheduled Transfer	Network Denial of Service
Hardware Additions	Rundll32	Account Manipulation	DLL Search Order Hijacking	Disabling Security Tools	Credentials in Registry	Permission Groups Discovery	Exploitation of Remote Services	Data from Removable Media	Uncommonly Used Port		Resource Hijacking
Spearphishing via Service	Compiled HTML File	Create Account	Application Shimming	Modify Registry	Exploitation for Credential Access	System Network Connections Discovery	Logon Scripts	Audio Capture	Custom Cryptographic Protocol		Runtime Data Manipulation
	CMSTP	BITS Jobs	Hooking	DLL Side-Loading	Input Prompt	Peripheral Device Discovery	Taint Shared Content	Video Capture	Data Obfuscation		Service Stop
	Execution through API	Bootkit	AppCert DLLs	Indicator Removal on Host	Kerberoasting	Security Software Discovery	Third-party Software	Man in the Browser	Fallback Channels		Stored Data Manipulation
	Mshta	DLL Search Order Hijacking	AppInit DLLs	Redundant Access	Keychain	Network Share Discovery	Windows Remote Management		Standard Non-Application Layer Protocol		Transmitted Data Manipulation
	Graphical User Interface	Hidden Files and Directories	Dylib Hijacking	Binary Padding	LLMNR/NBT-NS Poisoning and Relay	System Service Discovery	AppleScript		Communication Through Removable Media		
	Service Execution	Windows Management Instrumentation Event Subscription	Extra Window Memory Injection	Bypass User Account Control	Password Filter DLL	Application Window Discovery	Shared Webroot		Domain Fronting		
	Signed Script Proxy Execution	Application Shimming	File System Permissions Weakness	Indicator Removal from Tools	Private Keys	Network Sniffing	SSH Hijacking		Multi-hop Proxy		
	Third-party Software	Component Firmware	Image File Execution Options Injection	Regsvr32	Securityd Memory	Password Policy Discovery			Multi-Stage Channels		
	Windows Remote Management	Component Object Model Hijacking	Launch Daemon	Rundll32	Two-Factor Authentication Interception	System Time Discovery			Multiband Communication		
	AppleScript	Hooking	Path Interception	Software Packing		Browser Bookmark Discovery			Domain Generation Algorithms		
	Control Panel Items	Logon Scripts	Plist Modification	Compiled HTML File		Domain Trust Discovery			Multilayer Encryption		
	Execution through Module Load	Modify Existing Service	Port Monitors	Access Token Manipulation		Virtualization/Sandbox Evasion			Port Knocking		
	InstallUtil	Office Application Startup	Service Registry Permissions Weakness	BITS Jobs							
	Launchctl	Winlogon Helper DLL		CMSTP							
	Local Job Scheduling	.bash_profile and .bashrc		DLL Search Order Hijacking							
				Hidden Files and Directories							
				Mshta							

ALL APT Groups vs TA505

All APT Group + CLOP | All APT Group



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
Spearphishing Attachment	Scripting	Registry Run Keys / Startup Folder	Valid Accounts	Scripting	Credential Dumping	System Information Discovery	Remote File Copy	Data from Local System	Remote File Copy	Data Compressed	Data Destruction
Valid Accounts	PowerShell	Valid Accounts	Scheduled Task	Obfuscated Files or Information	Input Capture	File and Directory Discovery	Remote Desktop Protocol	Data Staged	Standard Application Layer Protocol	Data Encrypted	Data Encrypted for Impact
Drive-by Compromise	User Execution	Scheduled Task	New Service	Valid Accounts	Brute Force	Process Discovery	Windows Admin Shares	Input Capture	Commonly Used Port	Exfiltration Over Alternative Protocol	Defacement
Spearphishing Link	Command-Line Interface	New Service	Process Injection	File Deletion	Account Manipulation	System Network Configuration Discovery	Pass the Hash	Screen Capture	Web Service	Exfiltration Over Command and Control Channel	Disk Content Wipe
Replication Through Removable Media	Scheduled Task	External Remote Services	Exploitation for Privilege Escalation	Masquerading	Credentials in Files	Remote System Discovery	Remote Services	Automated Collection	Standard Cryptographic Protocol	Data Transfer Size Limits	Disk Structure Wipe
Supply Chain Compromise	Windows Management Instrumentation	Redundant Access	Bypass User Account Control	Deobfuscate/Decode Files or Information	Forced Authentication	Account Discovery	Pass the Ticket	Clipboard Data	Connection Proxy	Automated Exfiltration	Endpoint Denial of Service
Trusted Relationship	Exploitation for Client Execution	Shortcut Modification	Accessibility Features	Web Service	Hooking	System Owner/User Discovery	Replication Through Removable Media	Email Collection	Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Firmware Corruption
Exploit Public-Facing Application	Dynamic Data Exchange	Accessibility Features	Web Shell	Code Signing	Network Sniffing	Network Service Scanning	Application Deployment Software	Data from Network Shared Drive	Data Encoding	Exfiltration Over Physical Medium	Inhibit System Recovery
External Remote Services	Regsvr32	Web Shell	Access Token Manipulation	Process Injection	Bash History	Query Registry	Distributed Component Object Model	Data from Information Repositories	Remote Access Tools	Scheduled Transfer	Network Denial of Service
Hardware Additions	Rundll32	Account Manipulation	DLL Search Order Hijacking	Disabling Security Tools	Credentials in Registry	Permission Groups Discovery	Exploitation of Remote Services	Data from Removable Media	Uncommonly Used Port		Resource Hijacking
Spearphishing via Service	Compiled HTML File	Create Account	Application Shimming	Modify Registry	Exploitation for Credential Access	System Network Connections Discovery	Logon Scripts	Audio Capture	Custom Cryptographic Protocol		Runtime Data Manipulation
	CMSTP	BITS Jobs	Hooking	DLL Side-Loading	Input Prompt	Peripheral Device Discovery	Taint Shared Content	Video Capture	Data Obfuscation		Service Stop
	Execution through API	Bootkit	AppCert DLLs	Indicator Removal on Host	Kerberoasting	Security Software Discovery	Third-party Software	Man in the Browser	Fallback Channels		Stored Data Manipulation
	Mshta	DLL Search Order Hijacking	AppInit DLLs	Redundant Access	Keychain	Network Share Discovery	Windows Remote Management		Standard Non-Application Layer Protocol		Transmitted Data Manipulation
	Graphical User Interface	Hidden Files and Directories	Dylib Hijacking	Binary Padding	LLMNR/NBT-NS Poisoning and Relay	System Service Discovery	AppleScript		Communication Through Removable Media		
	Service Execution	Windows Management Instrumentation Event Subscription	Extra Window Memory Injection	Bypass User Account Control	Password Filter DLL	Application Window Discovery	Shared Webroot		Domain Fronting		
	Signed Script Proxy Execution	Application Shimming	File System Permissions Weakness	Indicator Removal from Tools	Private Keys	Network Sniffing	SSH Hijacking		Multi-hop Proxy		
	Third-party Software	Component Firmware	Image File Execution Options Injection	Regsvr32	Securityd Memory	Password Policy Discovery			Multi-Stage Channels		
	Windows Remote Management	Component Object Model Hijacking	Launch Daemon	Rundll32	Two-Factor Authentication Interception	System Time Discovery			Multiband Communication		
	AppleScript	Hooking	Path Interception	Software Packing		Browser Bookmark Discovery			Domain Generation Algorithms		
	Control Panel Items	Logon Scripts	Plist Modification	Compiled HTML File		Domain Trust Discovery			Multilayer Encryption		
	Execution through Module Load	Modify Existing Service	Port Monitors	Access Token Manipulation		Virtualization/Sandbox Evasion			Port Knocking		
	InstallUtil	Office Application Startup	Service Registry Permissions Weakness	BITS Jobs							
	Launchctl	Winlogon Helper DLL		CMSTP							
	Local Job Scheduling	.bash_profile and .bashrc		DLL Search Order Hijacking							
				Hidden Files and Directories							
				Mshta							

[공격과정] Ready

공격자

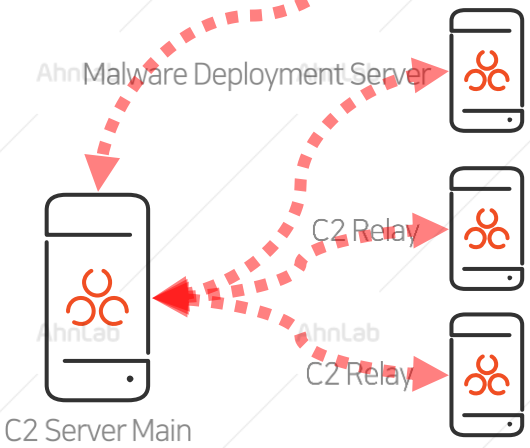
웹/이메일 서비스

인터넷망

내부망

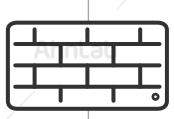
서버망

- 타깃 선정
- 타깃 정보수집
- 타깃 환경 분석
- 도구 준비
- 탐지 테스트

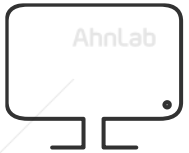


Email Server

PC1



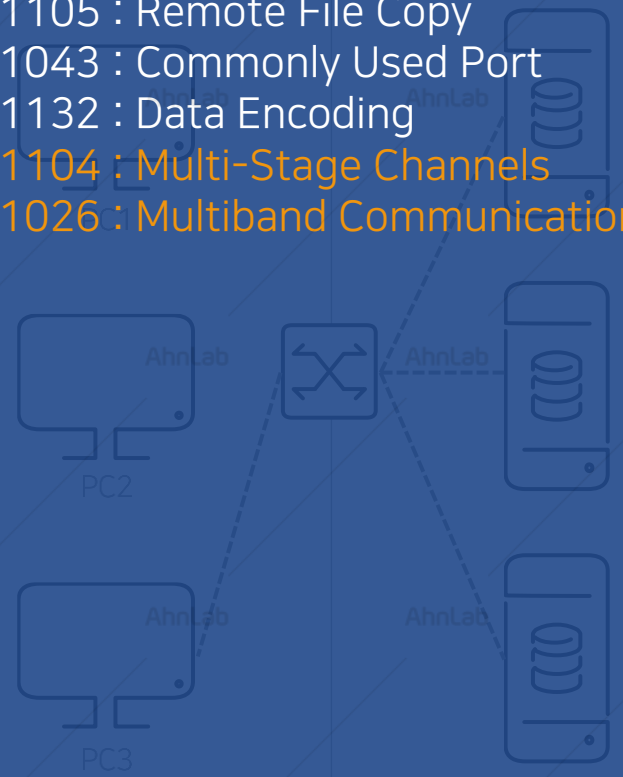
PC2



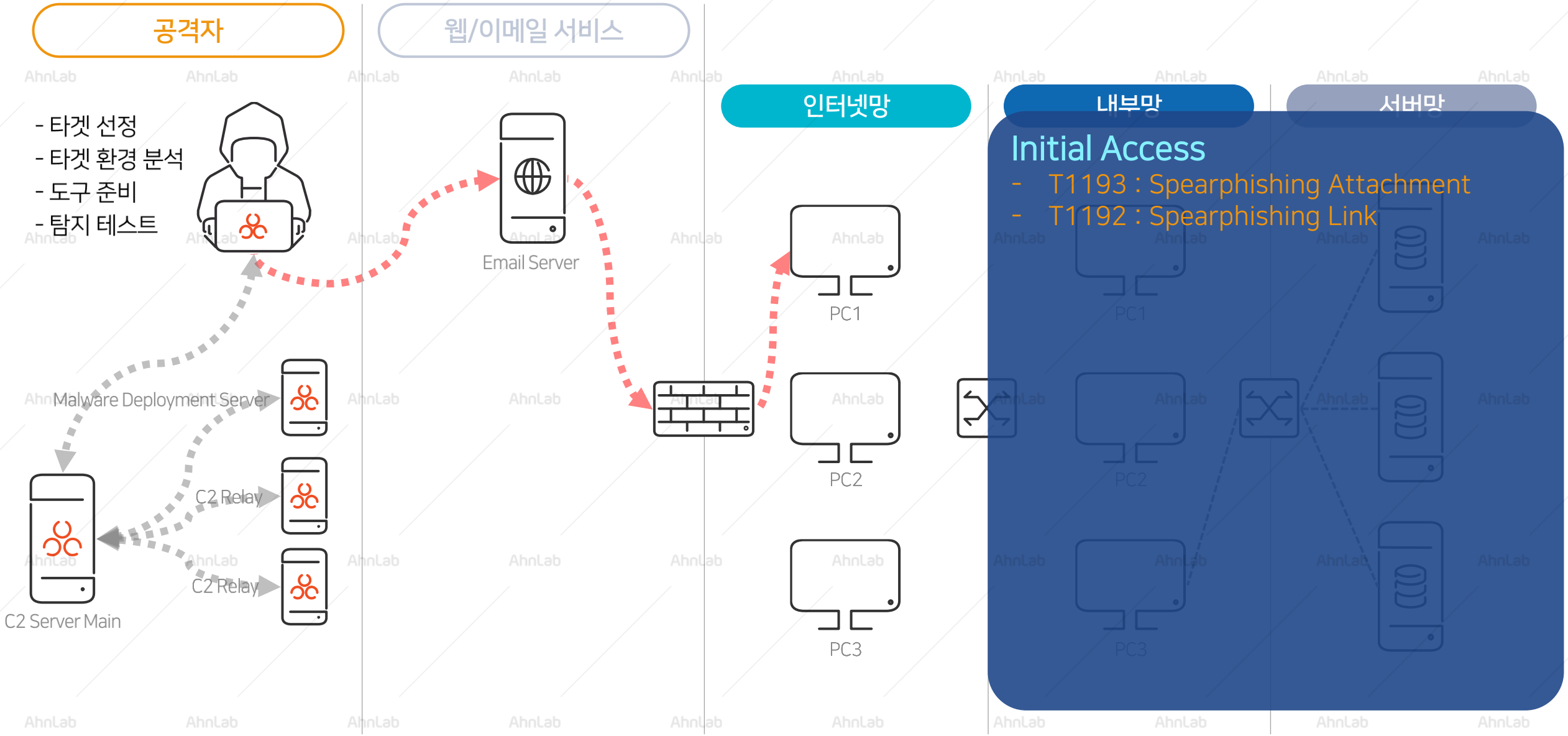
PC3

Command And Control

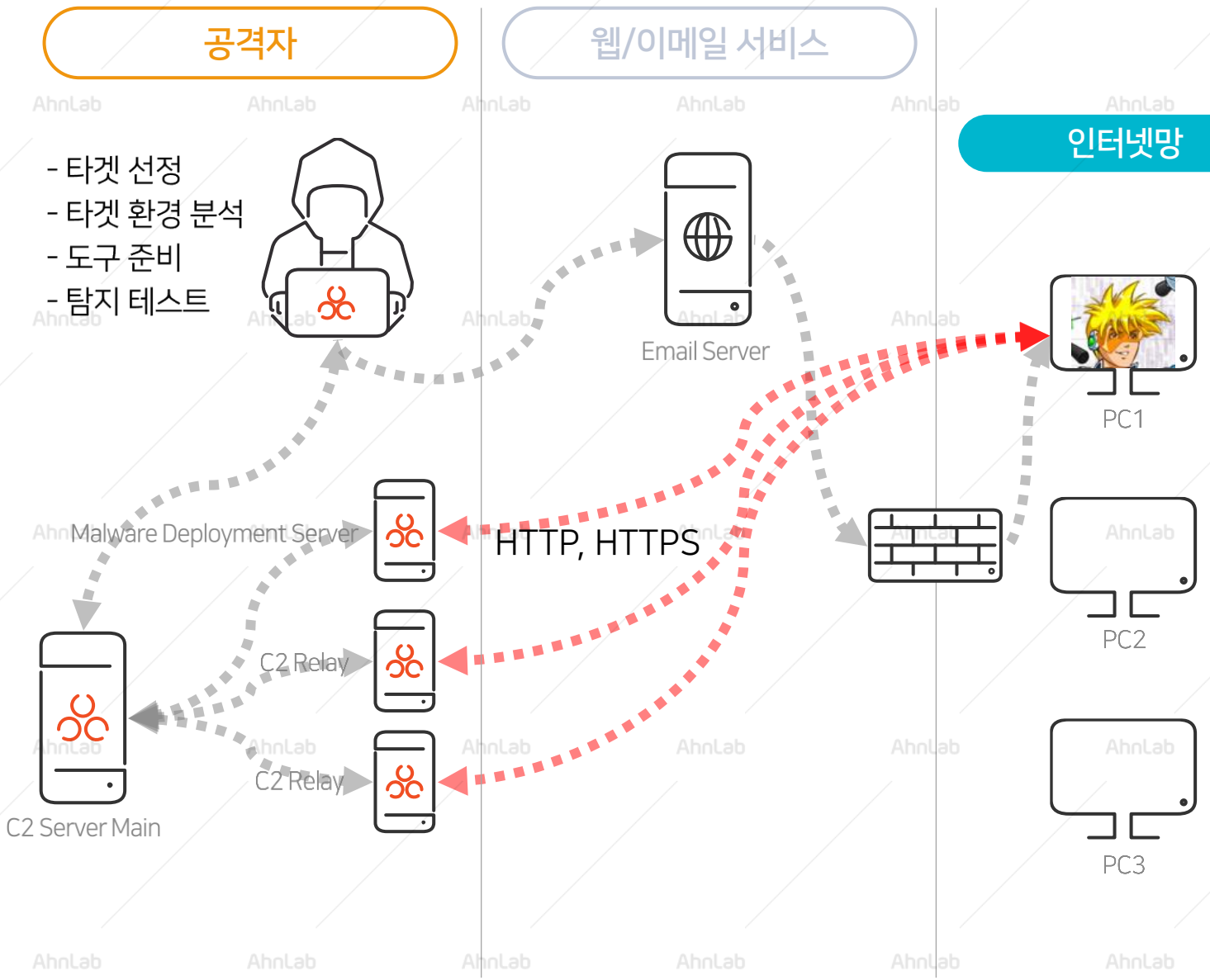
- T1105 : Remote File Copy
- T1043 : Commonly Used Port
- T1132 : Data Encoding
- T1104 : Multi-Stage Channels
- T1026 : Multiband Communication



{공격과정] Initial Access – Spear Phishing



{공격과정] Setting Foothold



Execution
- T1086 : PowerShell
- T1053 :Scheduled Task
- T1085 : Rundll32
- T1035 : Service Execution

Persistence
- T1138 : Application Shimming

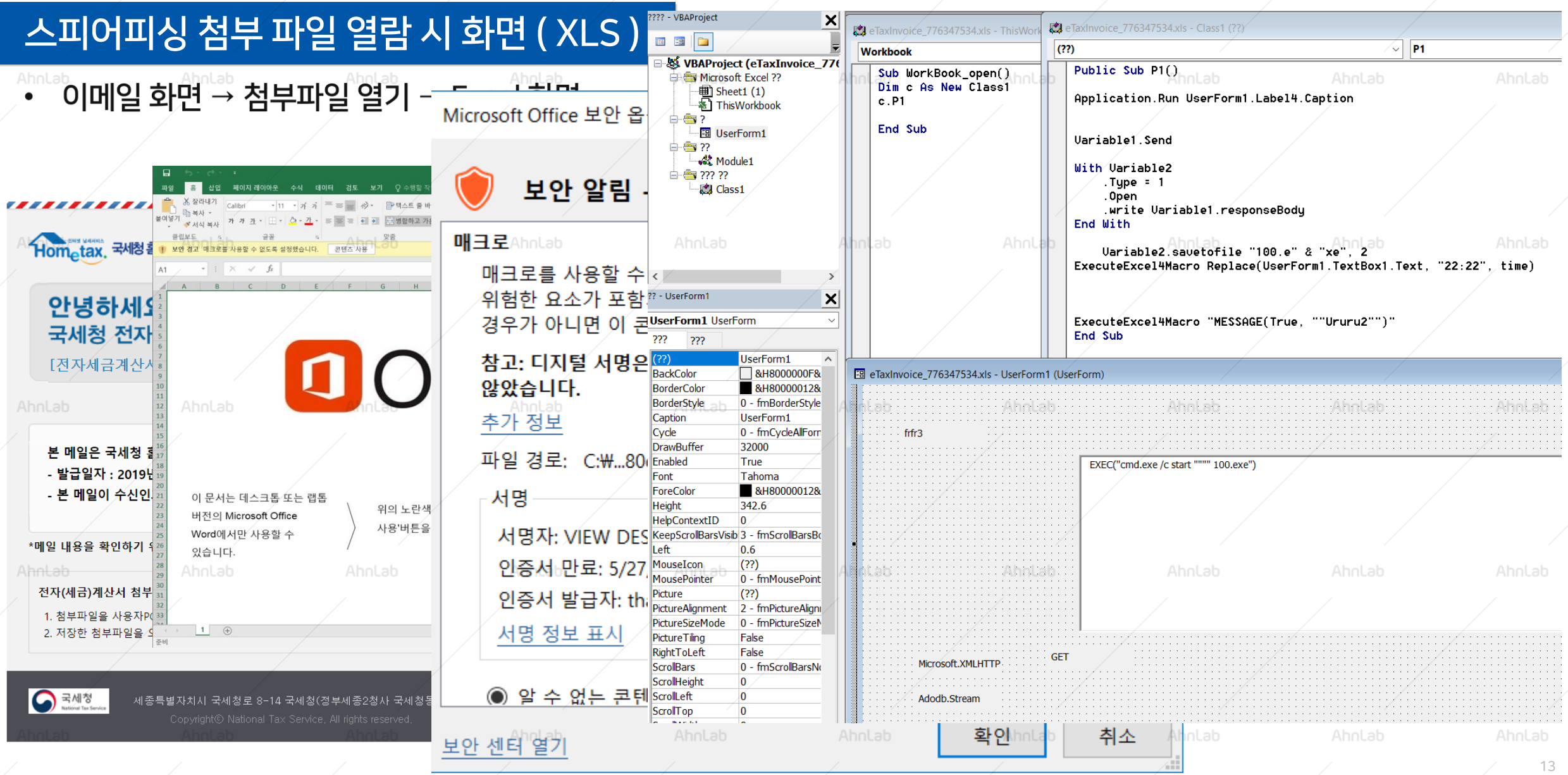
Privilege Escalation
- T1068 : Exploitation for Privilege Escalation(?)
- T1088 : Bypass User Account Control(?)

Defense Evasion
- T1064 : Scripting
- T1107 : File Deletion
- T1116 : Code Signing
- T1085 : Rundll32

[공격과정] Setting Foothold

스피어피싱 첨부 파일 열람 시 화면 (XLS)

- 이메일 화면 → 첨부파일 열기 –



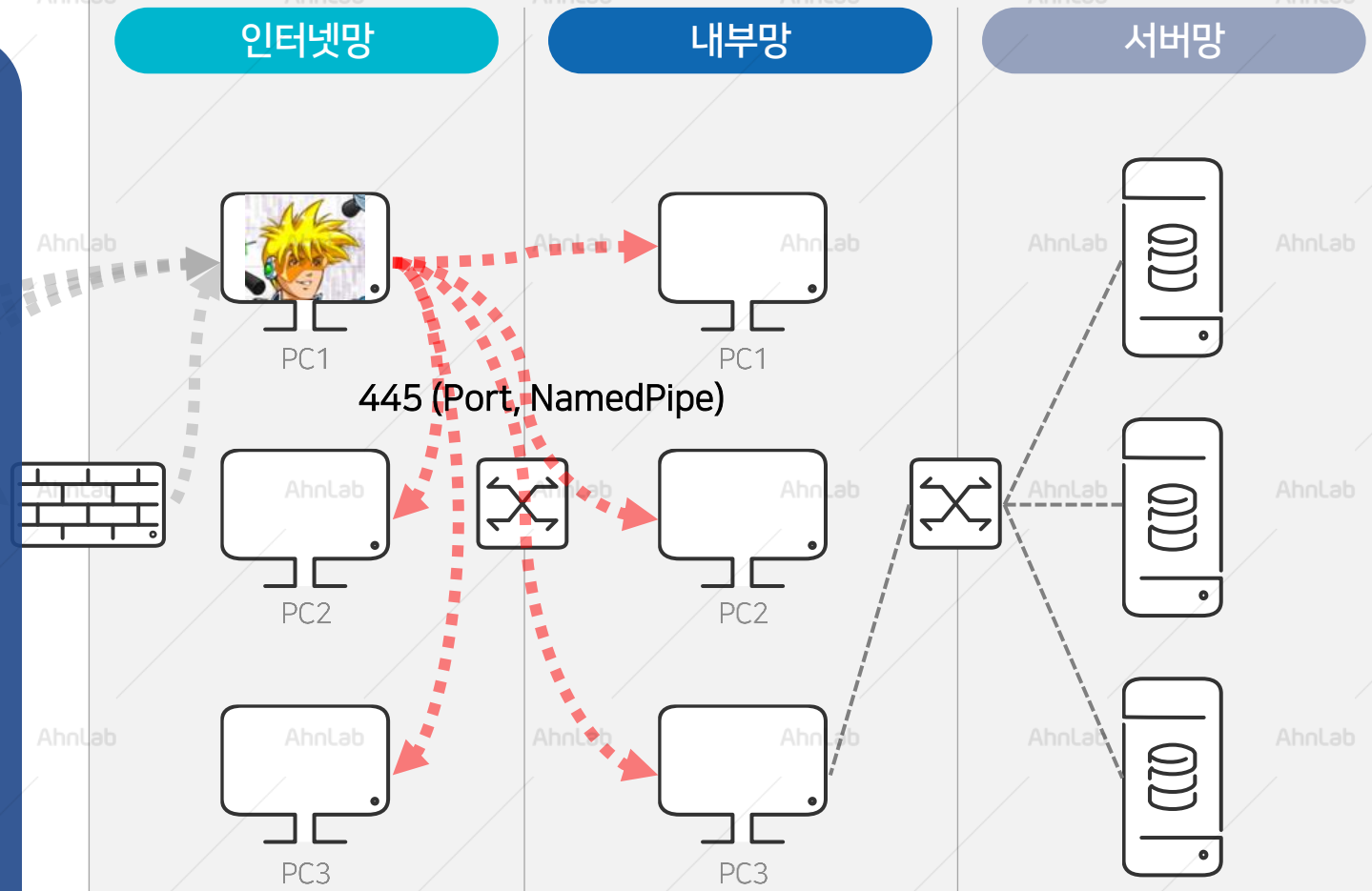
[공격과정] Lateral Movement

공격자 | 웹/이메일 서비스

Credential Access
- T1003 : Credential Dumping

Discovery
- T1083 : File and Directory Discovery

Lateral Movement
- T1105 : Remote File Copy
- T1077 : Windows Admin Shares
- T1075 : Pass the Hash



[공격과정] Impact

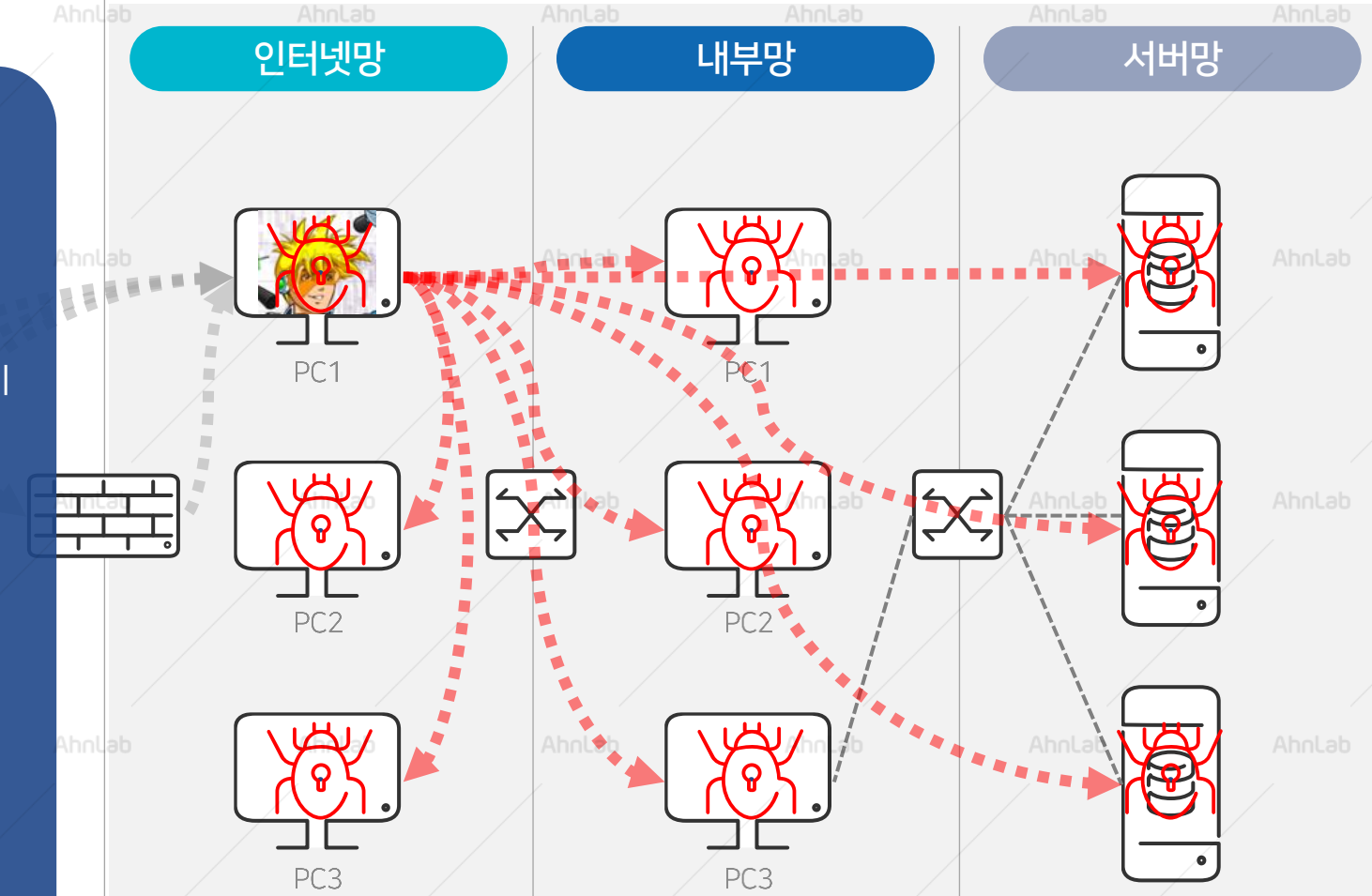
공격자

웹/이메일 서비스

Collection
- T1114 : Email Collection
- T1005 : Data from Local System

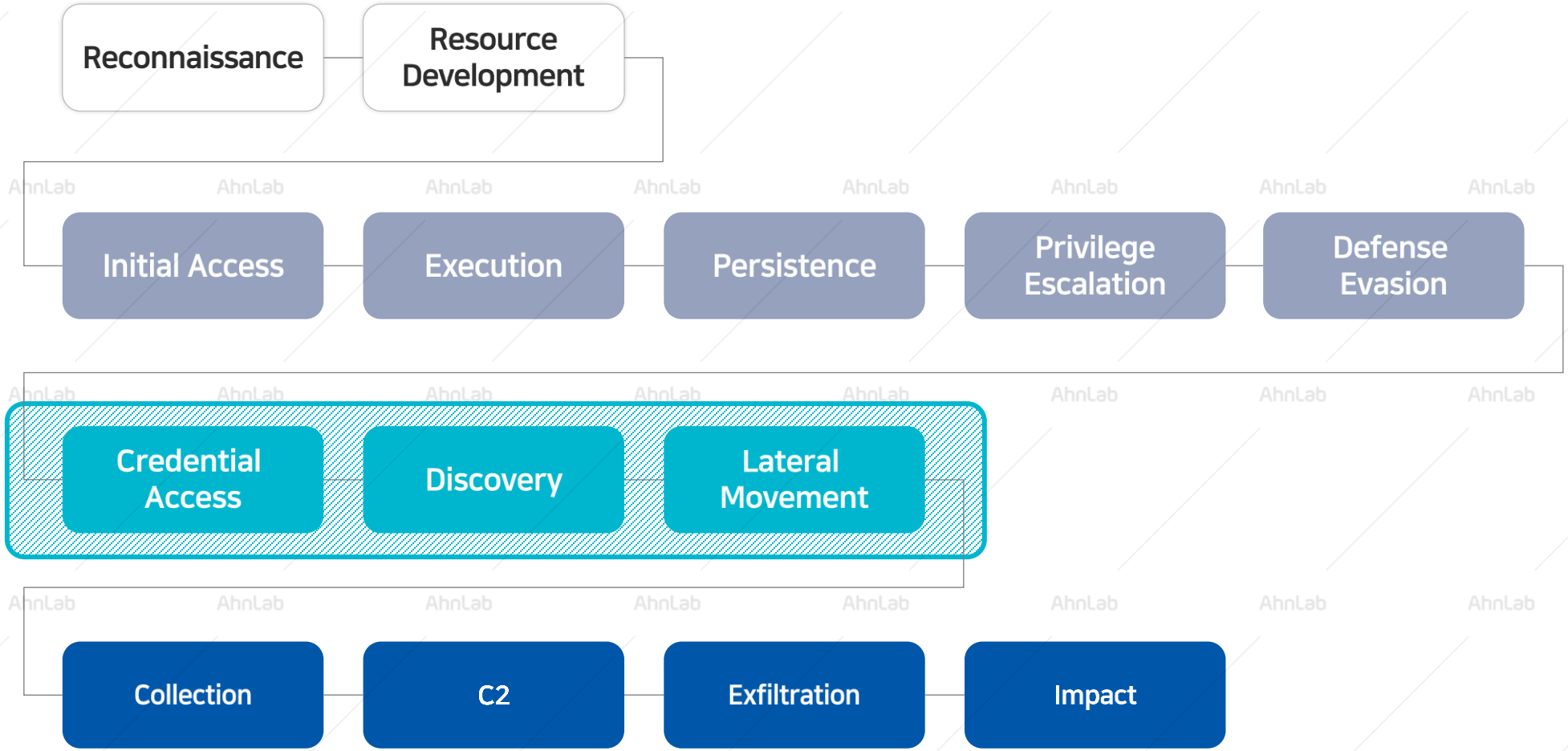
Exfiltration
- T1048 : Exfiltration Over Alternative Protocol
- T1041 : Exfiltratation Over Command and Control Channle

Impact
- T1486 : Data Encrypted for Impact



조직의 랜섬웨어 피해 단계

MITRE ATT&CK TACTICS



0 단계

피해 없음

1 단계

최초 침해 시스템 피해에 그침

2 단계

조직 전체로 피해 확산

3 단계

데이터 유출 및 랜섬웨어 감염

분석가 코멘트

조직 전체로 피해가 확산되는 Lateral Movement 단계에서 탐지 및 차단해야 한다.

0 단계

피해 없음

- 공격자의 준비 과정

공격자의 행위 파악이 어렵다.
최근 활동중인 공격그룹의 전략(TTP)과 타깃을 파악하는 것이 필요하다.

1 단계

최초 침해 시스템 피해에 그침

- 공격자의 최초 침해 시스템
  - 설정 미흡, 소프트웨어 취약점, 사용자의 실수
- **악성 코드에 감염되는 사건들이 대부분 여기에 해당**

완벽하게 막는 건 불가능하다.
하지만, 피해는 크지 않다.

2 단계

조직 전체로 피해 확산

- APT로 발전되는 단계
- 정상 행위와 악성 행위의 판별이 어려움
- 단일 보안 솔루션만으로 해결하기 어려움

하지만, 이 단계를 막아내면,
피해는 크지 않다.

3 단계

데이터 유출 및 랜섬웨어 감염

- 실질적 피해 발생

공격자가 2단계까지 성공했다면,
3단계를 막기는 어렵다.

그림출처 : http://m.inven.co.kr/board/powerbbs.php?come_idx=2097&l=1147581

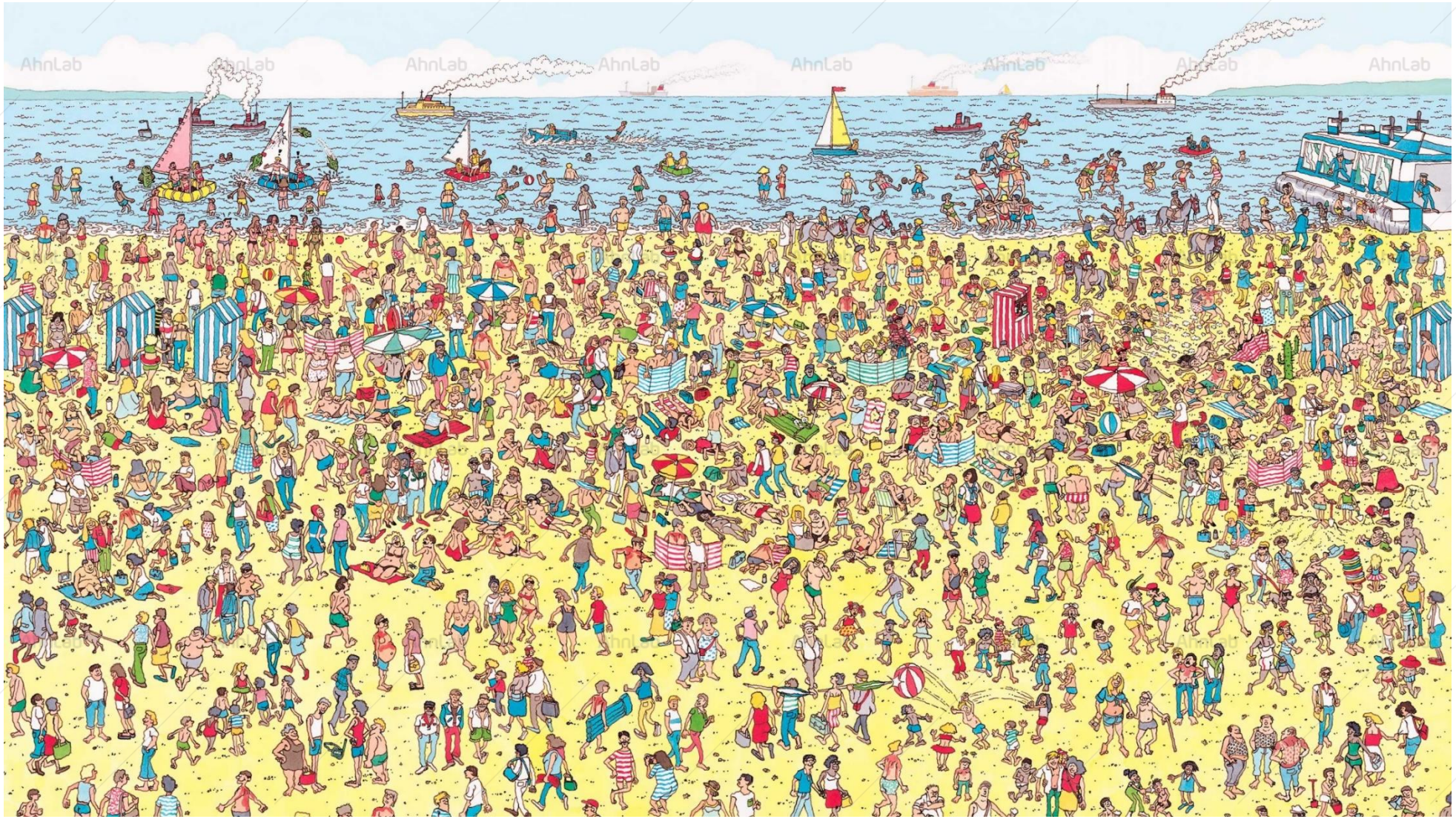
위협 완화 방안 > 가시성 확보

가시성 확보

공격자가 무슨 짓을 하고 있는지 알면 된다.

2022년 7월 James Webb Space Telescope이 실제 촬영한 용골 성운

Where's Wally



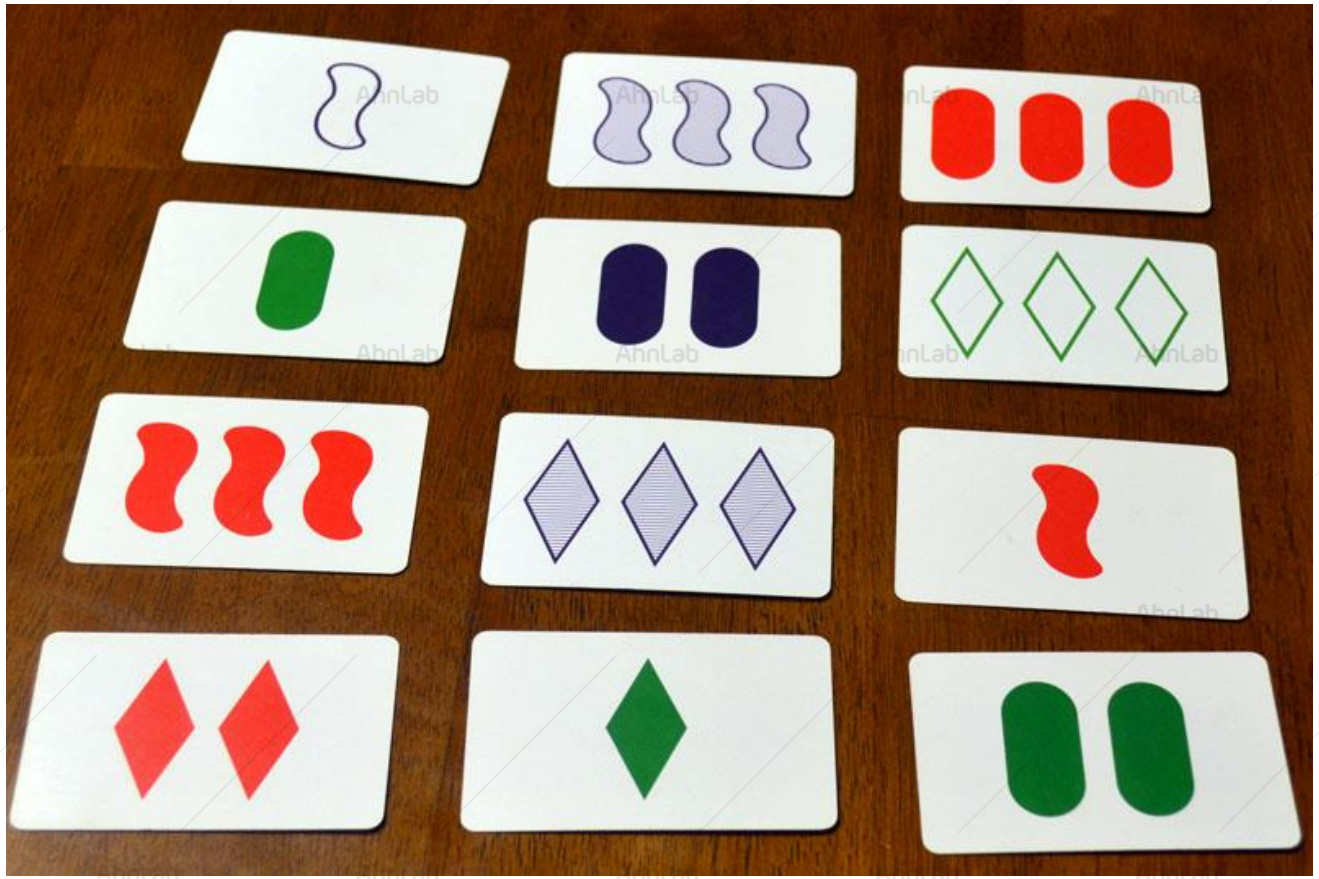
이미지 출처 https://www.wallpaperflare.com/waldo-cartoon-where-s-wally-water-sky-sea-day-nature-wallpaper-hrsym/download/3840x2160

SET Game

패턴이 모두 같거나, 모두 다른 것을 찾아내는 게임

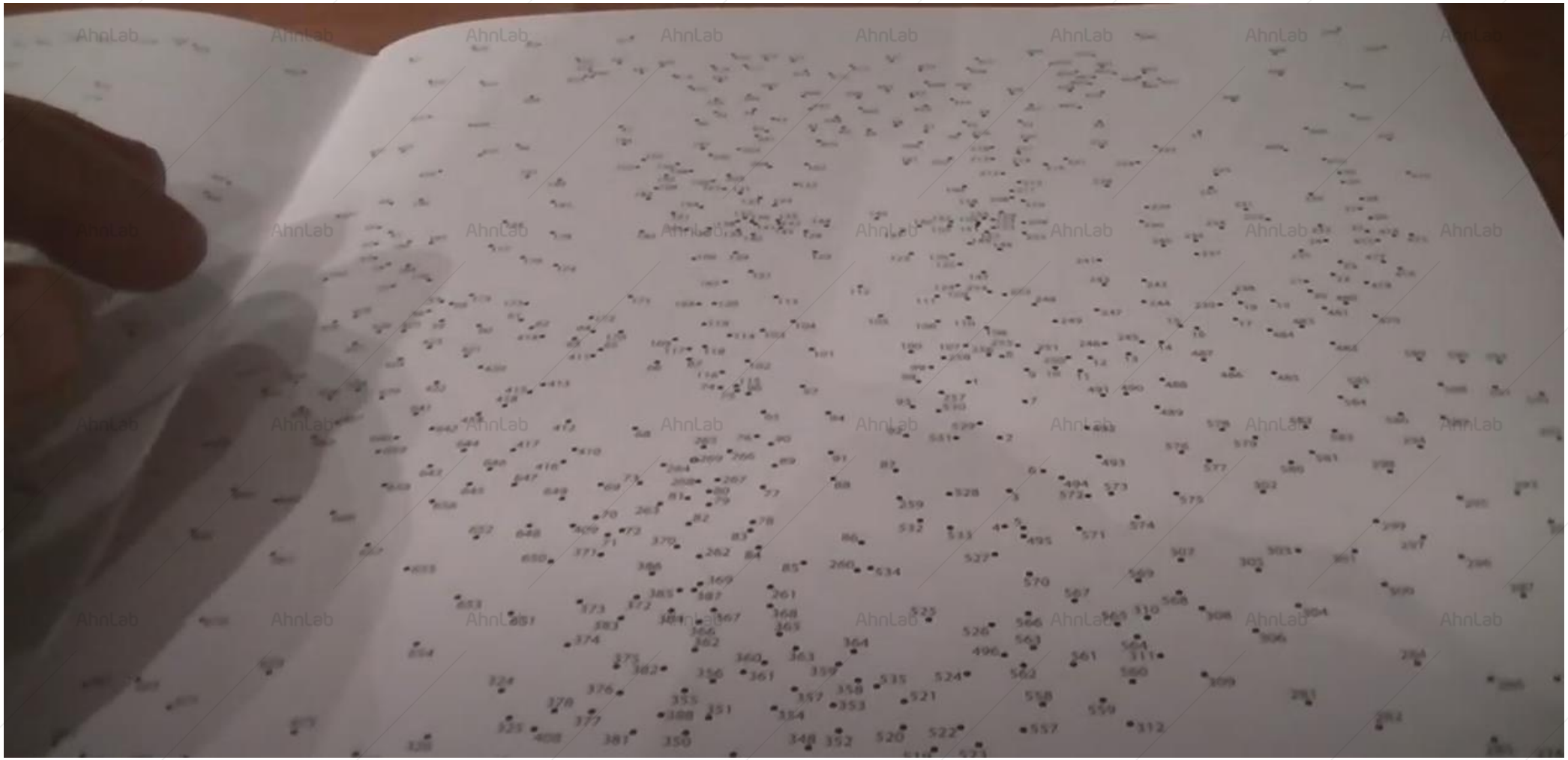
속성

- 모양 : 3가지 (물결, 알약, 다이아몬드)
- 색상 : 3가지 (빨강, 파랑, 초록)
- 무늬 : 3가지 (솔리드, 흐린, 비어있는)
- 개수 : 3가지 (1개,2개, 3개)



이미지출처 : https://www.gamesforyoungminds.com/blog/2018/1/4/set

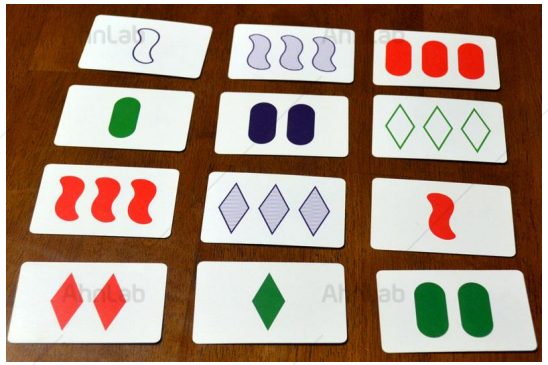
Dot to Dot Game



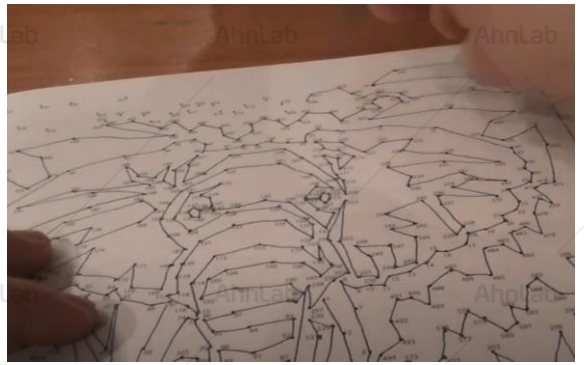
이미지 출처 : https://www.youtube.com/watch?v=rfvxxKcdNdI

의심 데이터 발견 > 패턴 발견 > 종합 상황 판단

의심 데이터 발견



의미, 패턴 발견



발견한 정보를 종합해 상황 파악

그런데 흔적이 남아 있을까?....

Dr. Edmond Locard (1877 ~ 1966)
프랑스의 법과학자 겸 범죄심리학자
프랑스의 셜록 홈즈로 알려짐

두 물체끼리 접촉이 있으면 반드시 물질 교환이 일어난다.

즉, "모든 접촉은 흔적을 남긴다"

- **현대의 과학수사는 이 법칙을 기본 전제로 함**
- **디지털 시대에도 유효할까?**

사고 발생 확률을 낮추기 위한
공격 표면 최소화

상시 행위 수집을 위한
CCTV 설치

사고를 추적하여
원인 파악 및 재발방지

사고 발생 인지 시간 단축을 통한
피해 범위 및 규모 축소

다양한 위협에 대한 복합적 대응방안 필요...

컨설팅, '객관적인 현황 분석'

- 공격자의 시각으로 취약점 분석
- 개선 및 보안 방안 제공

트레이닝, '쉽고 친근한 접근'

- 보안 담당자 및 일반 사용자에 대한 교육 등 다양한 종류의 트레이닝 포함
- 최신 보안 이슈와 트렌드를 지속적으로 접하고 업데이트 필요

솔루션, '자동화된 대응체계'

- 네트워크: 방화벽, IPS/IDS, APT 대응 솔루션의 조화 / 이메일: APT 대응 솔루션 활용
- 엔드포인트: 보안 플랫폼 연동을 통한 대응 / TIP: 최신 위협 정보 습득

전문 서비스, '보안 전문가의 지원'

- 보안 사고 발생 이후 피해 최소화 및 대응해 나갈지에 관한 가이드 제공
- 악성코드 전문가 분석 서비스 및 침해사고 분석 서비스 등

결론 : 기술과 사람의 협력 필요

01

현재까지는

- 짧은 기간에 효과적인 대응 방안을 마련하기 위해서는 솔루션을 검토하는 것이 가장 빠르지만,
- 상세 분석을 위한 컨설팅을 통해 외부에 노출된 위협부터 제거해 나가는 것이 더 합리적인 방안이며,
- 일반 구성원의 보안 인식 교육도 필요하다.

02

앞으로는

- 기술과 사람이 협력할 때 가장 효과적으로 대응할 수 있다.
- 대응을 위해 준비된 것이 무엇이며, 어떤 것을 더 보완해야 할지 지속적으로 검토하여,
- 더욱 견고한 방어 체계를 만들어 나가야 한다.

More security More freedom

안랩의 보안 아키텍처를 담은

AhnLab 통합 솔루션/서비스 맵

AhnLab

01 변화하는 보안 트렌드

지금까지 보안은 **경계 보안 중심**

AS-IS

외부위협의 **방어**와
내부유출의 **통제**에 포커스 …

Detection
외부 위협 방어

TO-BE

대응(Response) 중심
솔루션 **통합**과 **연동**

Prevention
내부 유출 통제

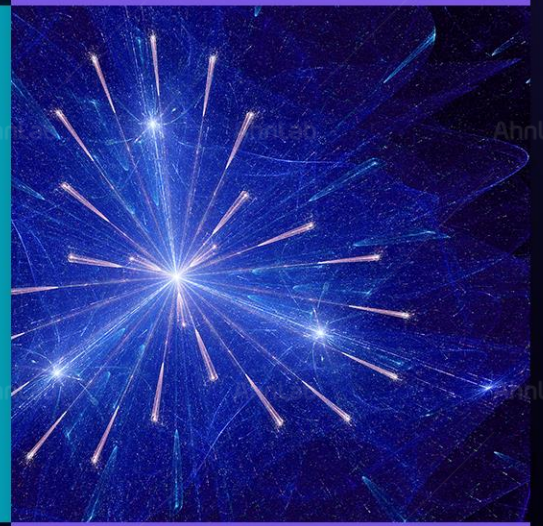
정보자산을 지키기 위한
Traditional 솔루션들 …

Unified Security

플랫폼과 플랫폼의 연동

Consolidation

솔루션들의 유기적인 통합



AhnLab

02 무엇이, 어떻게 변화하나?

위협의 예방

위협의 초기 **식별**과 **대응**

위협 완화

리스크 통제와 **거버넌스 확보**

Protect & Detect

Threat hunting & Respond

위협 원점에 대한
탐지-분석-대응

위협과 리스크에 대한
통합관리

Point Solution 간 정보 통합 + 연동을 통한

통합적인

Threat Detection & Response

레이어 별
포인트 솔루션 구성

오케스트레이션 및
거버넌스

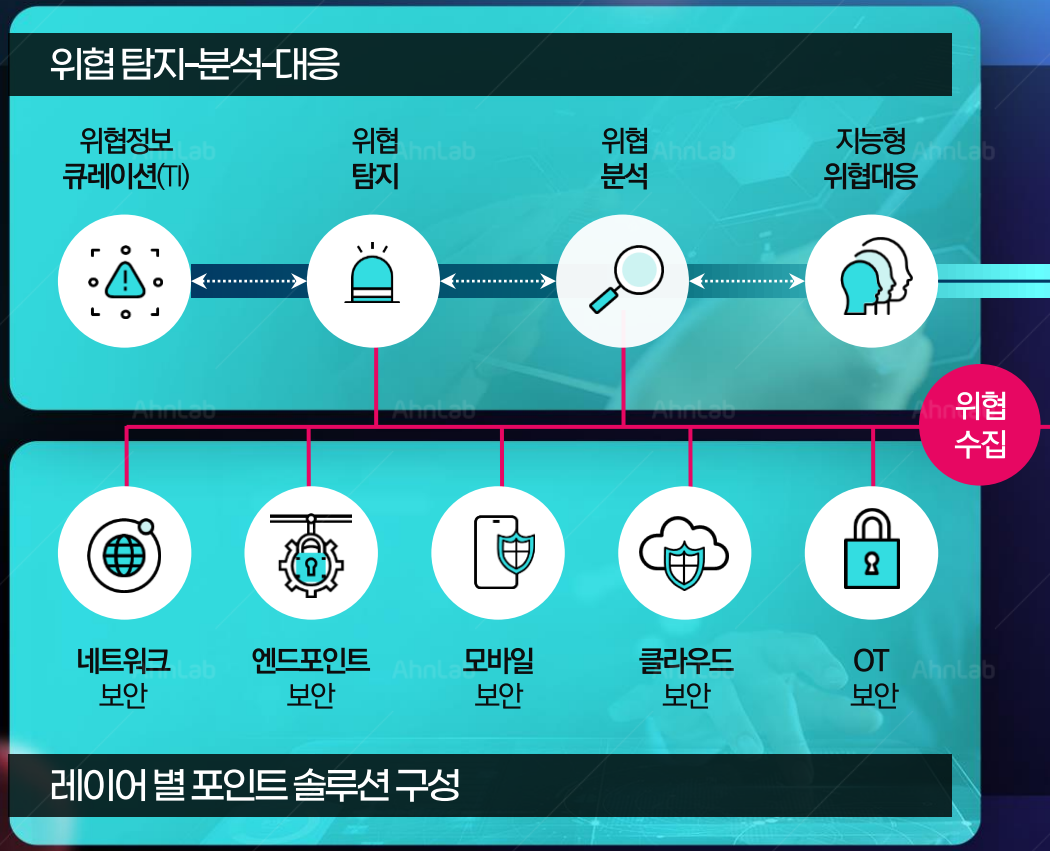
Resilience

Governance & Visibility

03 보안 영역의 결합

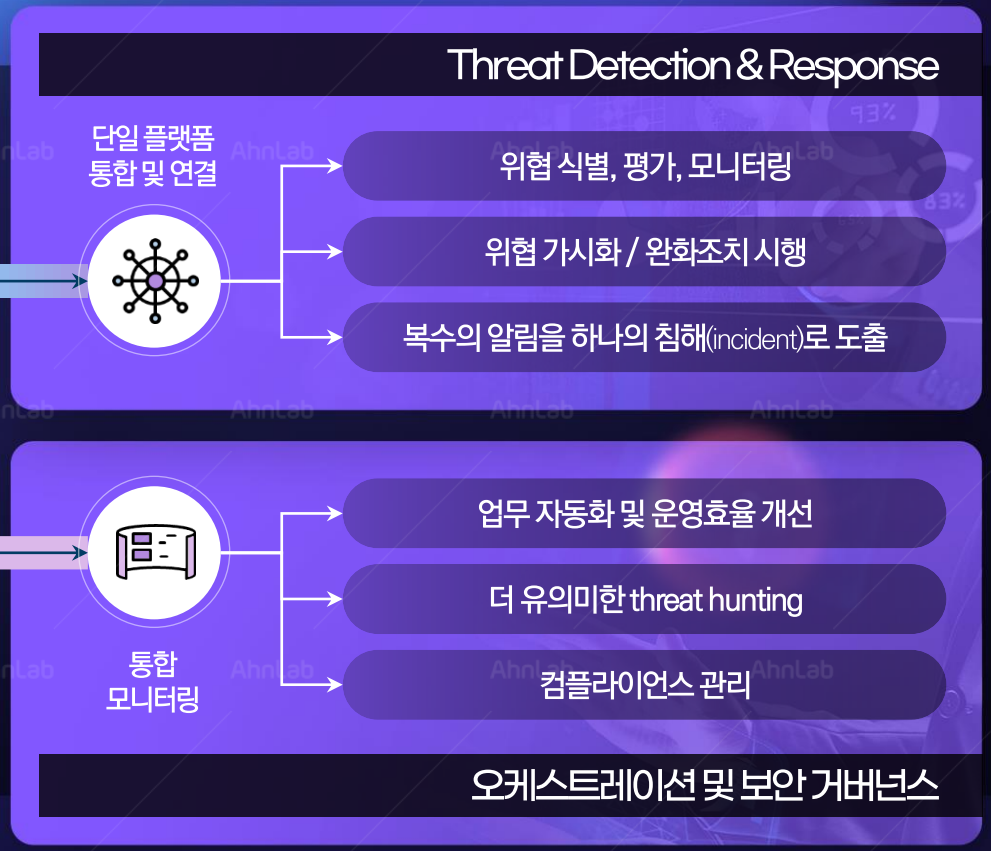
유기적 통합

효과적 대응을 위한 솔루션 유기적 **통합**



플랫폼 연동

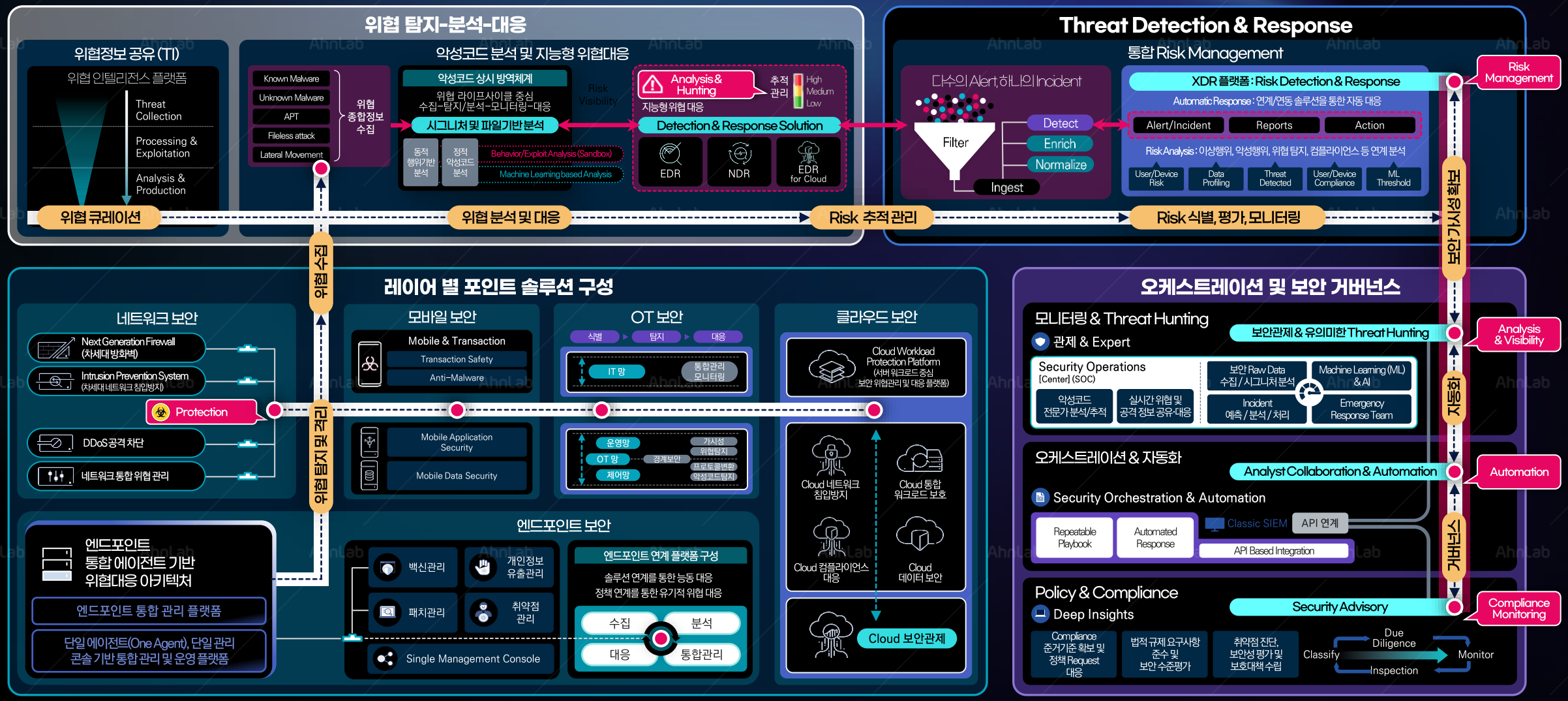
리스크 통제와 거버넌스 확보를 위한 플랫폼 **연동**



04 AhnLab이 그리는 보안 아키텍처

안랩의 보안 아키텍처를 담은 AhnLab 통합 솔루션/서비스 맵

More security / More freedom



AhnLab

05 AhnLab 보안 솔루션/서비스 매핑

네트워크 보안영역

차세대 네트워크 방화벽

차세대 방화벽 (NG Firewall)

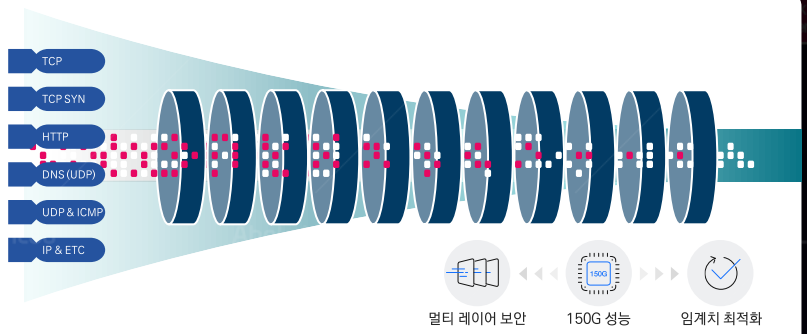
AhnLab TrusGuard

Firewall	IPS	Application Control	C&C 서버 탐지/차단
SSL VPN (PC / Mobile)	Proactive & Comprehensive	High Performance & Flexibility	Anti-Malware (파일 기반 / 패킷 기반)
DLP (Data Loss Prevention)			SSL Inspection (암호화된 트래픽 인지)
Anti-Spam			IPSec VPN
지역 기반 차단			Web Filtering

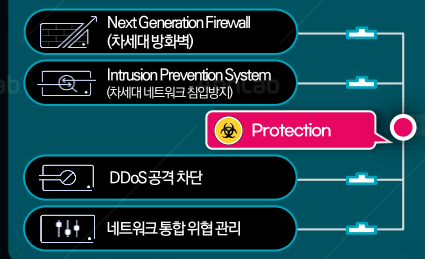
DDoS 공격 차단

DDoS 공격 차단 솔루션

AhnLab DPX



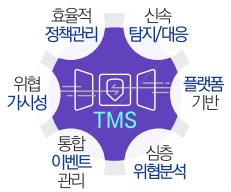
네트워크 보안



네트워크 통합 위협관리

네트워크 통합 위협 관리 시스템

AhnLab TMS



차세대 네트워크 침입방지

차세대 네트워크 침입방지

AhnLab AIPS

Next-Gen IPS
Anomaly Detection
High Performance
Malware
Threat Intelligence
Open API

네트워크 트래픽 분석

Network Detection & Response

Quad Miners
NETWORK BLACKBOX

100% Full 패킷 캡쳐
네트워크 행위 가시화
실시간 이상징후 탐지
고성능 패킷 스트림 저장

Web Application Firewall

AI WAF

MONITORAPP
AIWAF

모든 웹 트래픽 검사
비정상 접근 탐지 차단
Unkwown Attack 선제적 방어
Trafic Inspection 기술 기반

엔드포인트 보안영역

안티 멀웨어

안티멀웨어

기업 PC 보안	서버 보안
V3 Internet Security	V3 Net for Windows Server
V3 Endpoint Security	V3 Net for Unix/Linux Server
가정용 PC보안	**VDI 보안**
V3 365 Clinic	V3 for VDI

엔드포인트 보안 플랫폼

엔드포인트 플랫폼

단일 매니지먼트 기반의
차세대 엔드포인트 보안 플랫폼

중앙관리	패치관리
AhnLab EPP	EPP Patch Management
취약점관리 및 조치	**개인정보 유출 방지**
EPP Security Assessment	EPP Privacy Management

- 위협관리 및 대응을 위한 연계 정책 설정을 통해 조직의 환경에 최적화된 엔드포인트 보안 운영

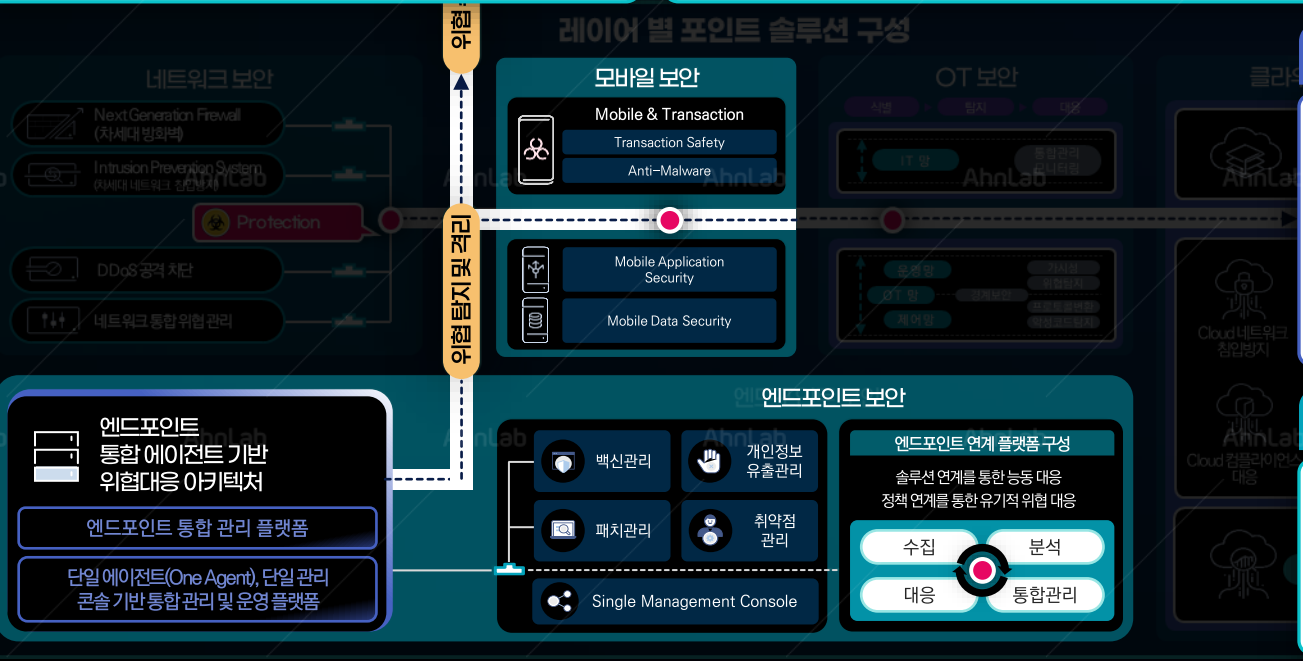
SMB 단말보안

엔드포인트 통합관리

다양한 엔드포인트
보안 솔루션의 통합 관리

SaaS형 보안관리
Office Security
SMB 보안
기업용 PC주치의

레이어 별 포인트 솔루션 구성



모바일 보안

모바일 AV	모바일 트랜잭션 보안
V3 Mobile Security	V3 Mobile Plus
모바일 오피스 환경 보안	**모바일 보안 엔진**
V3 Mobile Enterprise	Mobile Engine SDK

인증관리

Next Authentication Platform **Whykeykey**

Ydentity

생체기반 인증
Ydentity

개인정보보호

개인정보보호 통합관리

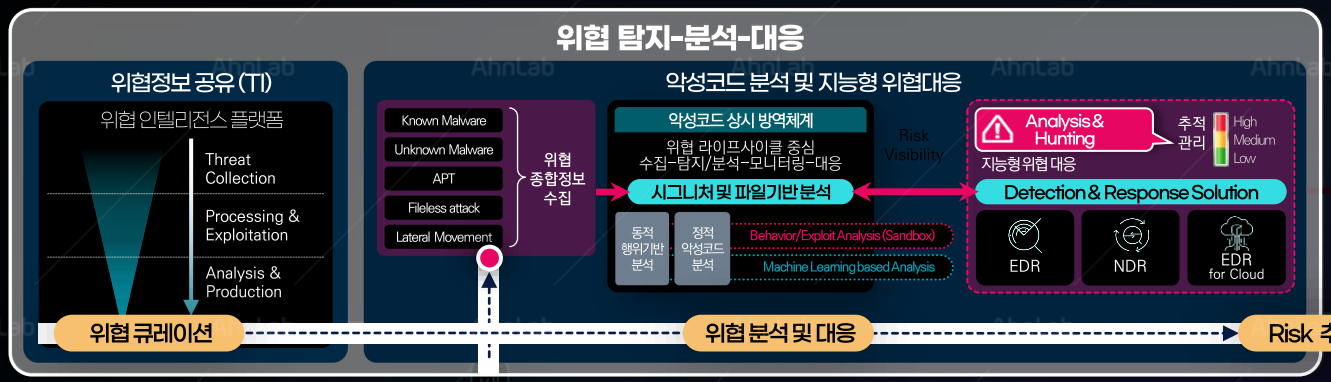
클라우드 기반의 더 강력한 **개인정보 유출 방지**

클라우드 개인정보 보호	Spiceware

개인정보수집·탐지·암호화
PII CDE
개인정보 가명·익명처리
PII ANP

지능형 위협대응 영역

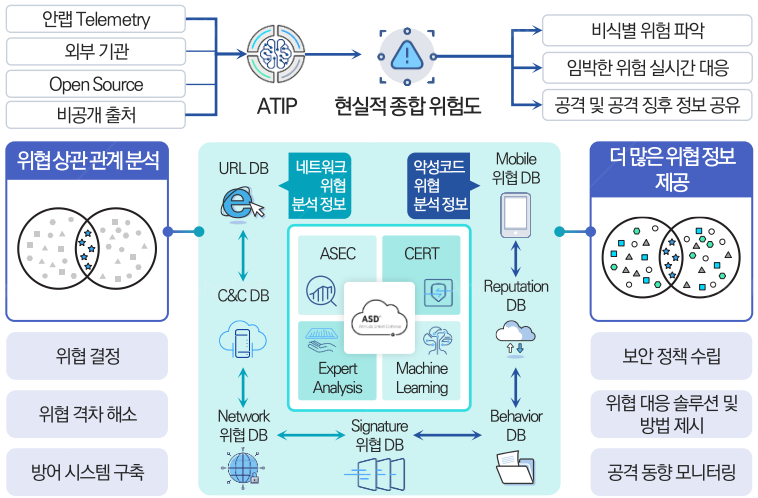
위협 탐지-분석-대응



위협 인텔리전스 플랫폼

AhnLab TIP

전문 기술 및 노하우가 결합된 시큐리티 인프라 기반
THREAT INTELLIGENCE PLATFORM



엔드포인트 위협탐지 및 대응

AhnLab EDR

행위 정보 탐지·분석을 통한
엔드포인트 가시성 확보 및 대응

간편한 구축, 손쉬운 운영
더 강력한 위협 대응

MDR (Managed Detection & Response)

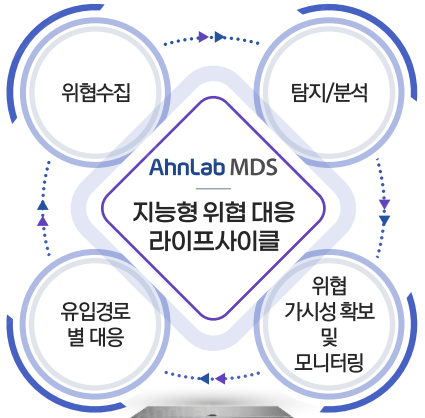
AhnLab MDR

설치된 EDR에서 탐지된 위협 이벤트를 위험도(경고, High) 기준으로
모니터링하여, **전문가가 원격에서 위협을 직접 분석 및 대응**

APT 대응

AhnLab MDS

샌드박스 기반
지능형 위협 대응



네트워크 기반 공격 대응	엔드포인트 기반 공격 대응	이메일 기반 공격 대응	망연계/ 파일 서버 대응
• 이상 트래픽 탐지 및 차단	• 악성코드 삭제 /실행 보류 • 의심 파일 추출 시스템 격리	• 이메일 격리 기능 • 이메일 필터링 연계	• 망연계 솔루션 연동 • 3rd party 솔루션 연계

- 주요 경로를 통해 유입되는 위협 수집
- 멀티엔진 기반의 다단계 분석 모듈 제공

수집 → 탐지/분석

APT 대응 절차

대응 → 모니터링

- 네트워크 에이전트 기반 위협 대응
- 직관적인 위협 가시성
- 지속적인 위협 모니터링

클라우드 영역

클라우드 보안 플랫폼

AhnLab CPP

클라우드 플랫폼 | 애플리케이션 제어 | 네트워크 침입 공격 방어 | 안티멀웨어

중앙관리	애플리케이션 실행 허용	네트워크 침입 방어·방화벽	악성코드 탐지·대응
CPP Management	Application Control	Host IPS	V3 Net

AhnLab vTrusGuard 클라우드 차세대 방화벽

NGFW for Cloud
클라우드 환경에 최적화된 차세대 방화벽 기술을 기반으로 위협을 최소화하여 클라우드 보호

AhnLab vAIPS 클라우드 위협대응시스템

클라우드 위협 탐지
클라우드 위협을 다양한 탐지 방법과 가속 기술을 바탕으로 정확하게 탐지하여 대응

AhnLab vTMS 클라우드 위협관리플랫폼

위협정보 모니터링 및 대응
위협대응시스템과 연동하여 다양한 클라우드 위협 정보를 모니터링하고 분석하여 대응

MONITORAPP AIONCLOUD 클라우드 WAF

클라우드 환경 최적화 웹 방화벽	
AIWAF-VE (VM)	AI ON CLOUD (SECaaS)

ASTRON SECURITY 클라우드 통합 워크로드 보호

CSPM + CWPP
ASTRON CWS

클라우드 데이터 보안

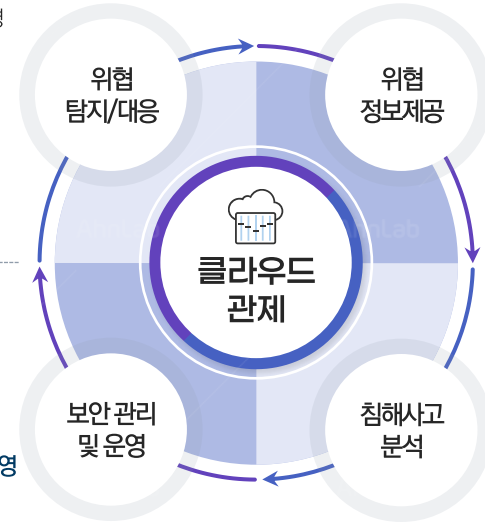
Spiceware One

클라우드 데이터 통합보안
Spiceware One

클라우드 관제

클라우드 환경 **실시간 보안 위협 탐지/대응**

안랩의 정보보안 **동향, 취약점 정보 제공**



효율적이고 체계적인 **클라우드 운영 지원**

클라우드 침해사고 발생 시 **정확한 원인 분석**

클라우드 컴플라이언스

클라우드 정보보호 컨설팅
클라우드 인프라 취약점 점검
클라우드 환경 모의침투 테스트
클라우드서비스 보안 인증(SaaS) 컨설팅
기업의 클라우드 서비스 이용 사전 컨설팅 및 클라우드 서비스 안전성 점검 및 확보조치

컴플라이언스 준수

전자금융거래법, 신용정보법 등에 따른 암호화, 데이터 위, 변조 방지 등

기술적, 관리적 보호조치를 준수

- 클라우드 환경 컴플라이언스와 클라우드 보안인증 획득 및 개인정보보호를 위한 Cloud Compliance Consulting

C3

클라우드 컴플라이언스 점검 자동화
Tatum C3
CSPM기반 클라우드 보안 컴플라이언스관리 자동화
Cloud Compliance Checker

클라우드 보안

Cloud Workload Protection Platform
(서버 워크로드 중심 보안 위협관리 및 대응 플랫폼)

- Cloud 네트워크 침입방지
- Cloud 통합 워크로드 보호
- Cloud 컴플라이언스 대응
- Cloud 데이터 보안

Cloud 보안관제

오케스트레이션 & 자동화

Analyst Collaboration & Automation
Security Orchestration & Automation
Repeatable Playbook
Automated Response
API 연계
API Based Integration
Automation

Policy & Compliance

Deep Insights
Security Advisory
Compliance Monitoring
Classify
Due Diligence
Inspection
Monitor

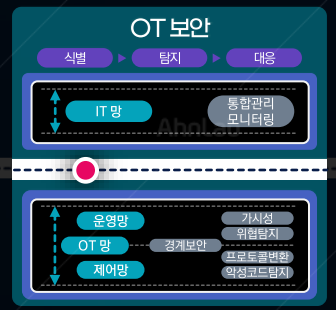
OT & ICS 영역

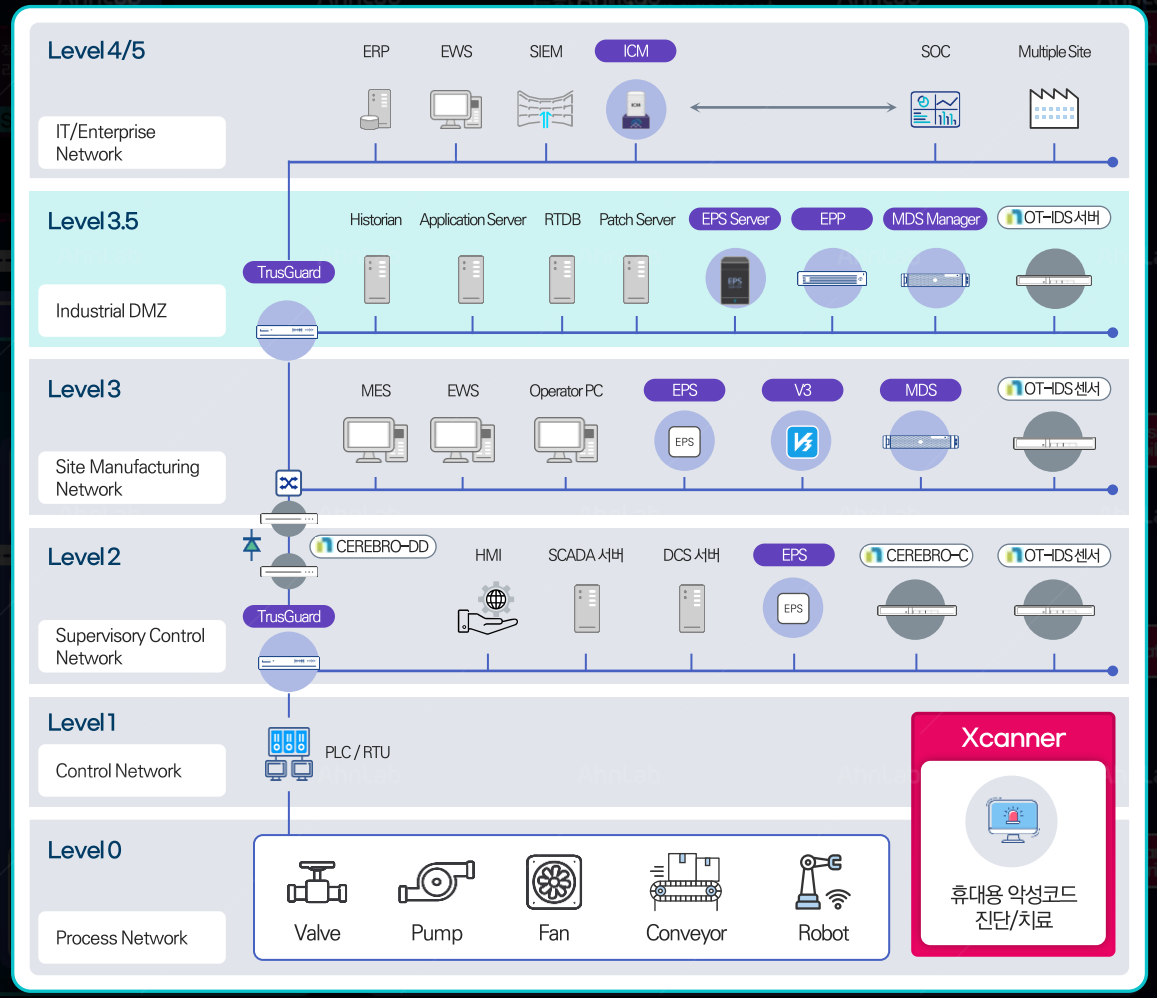
특수목적시스템 보안통제 및 산업용 서비스 제어

AhnLab 보안 위협 분석 기술 | NAONWORKS 산업용 프로토콜 분석

	식별	탐지	대응
OT 보안 > 운영망	**엔드포인트**		
	• AhnLab EPS (엔드포인트 자산/프로세스 식별)	• AhnLab EPS (악성코드 검사/비인가 프로세스 탐지)	• AhnLab EPS (Whitelist 제어/매체 제어) • AhnLab Xcanner (비상주형 악성코드 검사/치료)
	네트워크		
	• CEREBRO-XTD (OT자산/트래픽 식별)	• CEREBRO-XTD (보안 위협 탐지) • AhnLab MDS (생산망 파일 분석/감염장비 탐지) • AhnLab TrusGuard (비인가 트래픽 탐지)	• CEREBRO-DD (일방향 데이터 전송) • AhnLab TrusGuard (비인가 트래픽 차단)
OT 보안 > 제어망	**ICS 설비**		
	• CEREBRO-XTD (OT자산/트래픽 식별) • CEREBRO-C (OT프로토콜 변환)	• CEREBRO-XTD (OT프로토콜 분석/위협 탐지)	• ICS 설비 업체 대응

※ SCADA, HMI는 AhnLab EPS/Xcanner를 통한 엔드포인트의 식별/탐지/대응을 제공합니다.





06 아키텍처 레이어 구성

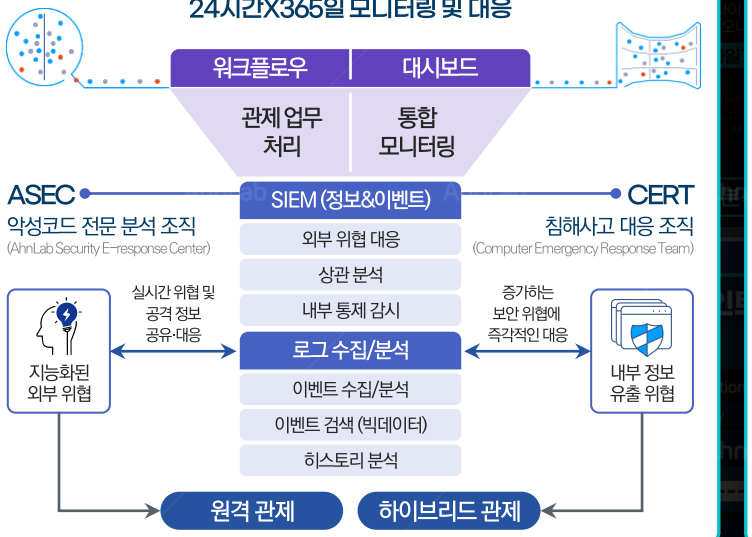
보안관제 / 자동화&오케스트레이션 영역

안랩의 보안 아키텍처를 담은 AhnLab 통합 솔루션/서비스 맵

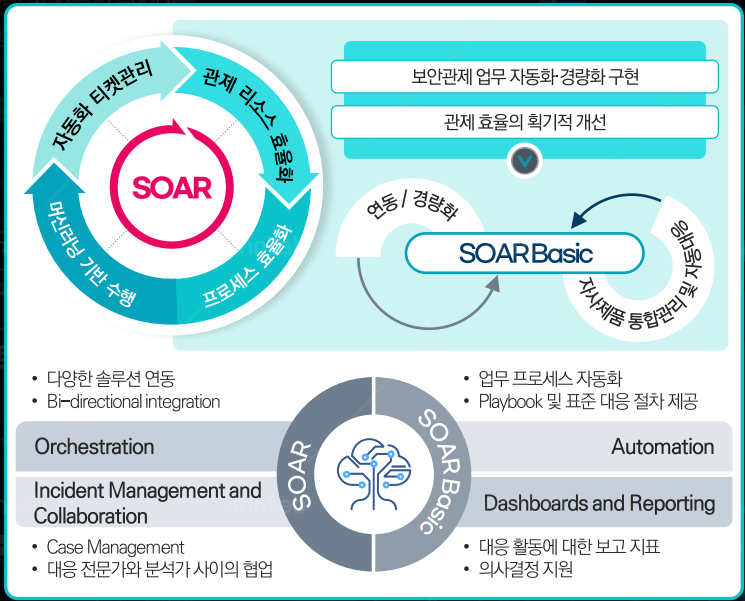
More security / More freedom

보안 관제

자체 시큐리티대응센터(ASEC)와 침해사고대응팀(CERT)을 통한
24시간X365일 모니터링 및 대응



자동화&오케스트레이션 (SOAR)

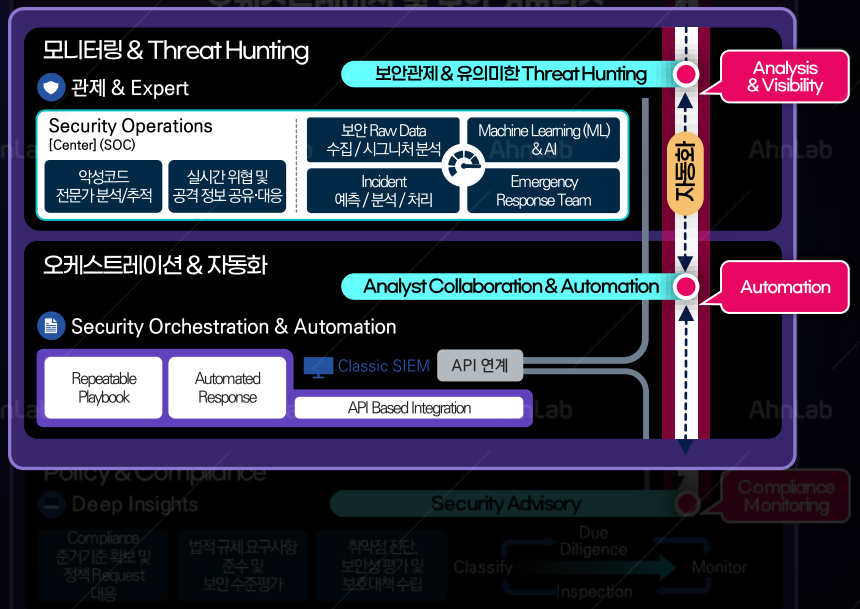


AI이상징후 탐지

JASON JMachine — AI 이상징후 탐지

빅데이터+AI

JMachine



Professional Service

보안 솔루션 운용 최적화

- 데이터 분석 서비스
- 전문가 온디멘드 서비스
- 보안 감사 사전 점검 서비스

보안 위협 분석·대응

- 의심 시스템 진단 서비스
- 악성코드 전문가 분석 서비스
- A-FIRST 포렌식 서비스

정보보안 교육

- AhnLab Professional Service
- 정보보안 교육 서비스

06 아키텍처 레이어 구성

정보보호 컨설팅 영역

안랩의 보안 아키텍처를 담은 AhnLab 통합 솔루션/서비스 맵

More security / More freedom

Secure Cloud, Sustainable Transformation