

+

One Step  
**Ahead**

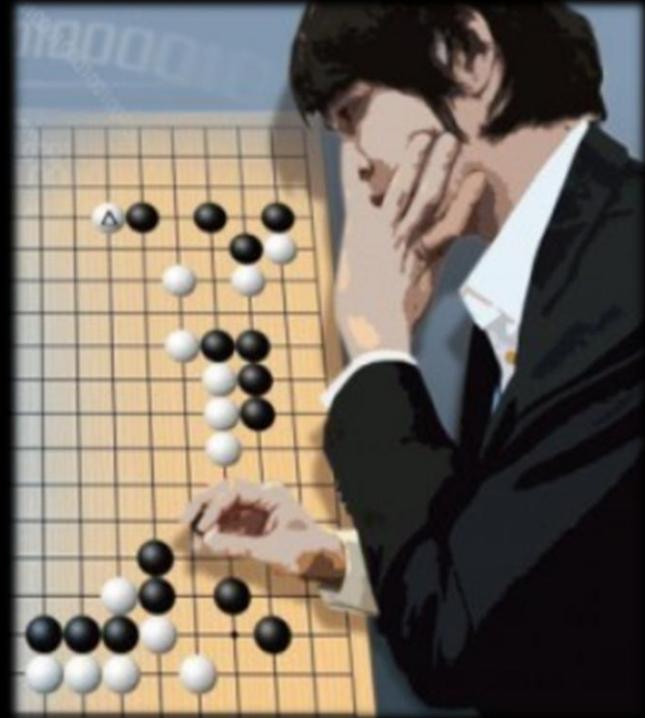
이글루시큐리티의 새로운 관제 전략  
**Security Intelligence Service**

2016. 04

# 세기의 바둑 대결



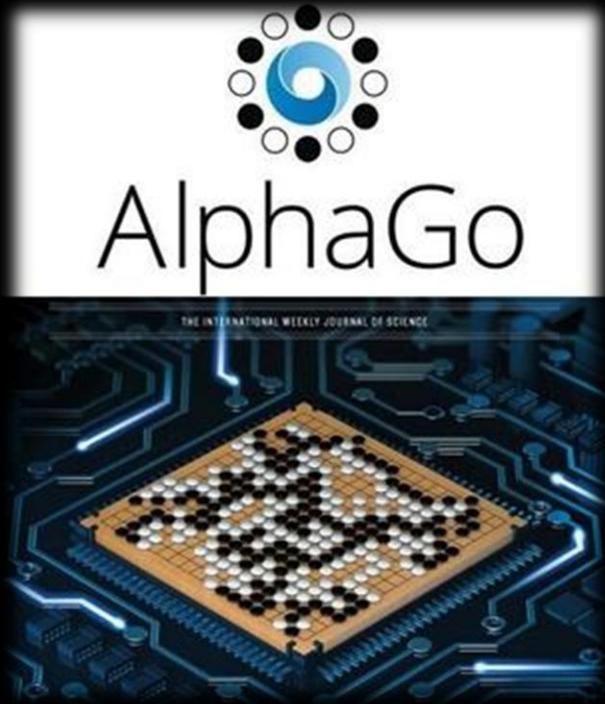
VS



AlphaGO

이세돌 9단

D-5, D-4, D-3, D-2, D-1



0



5

# Trends

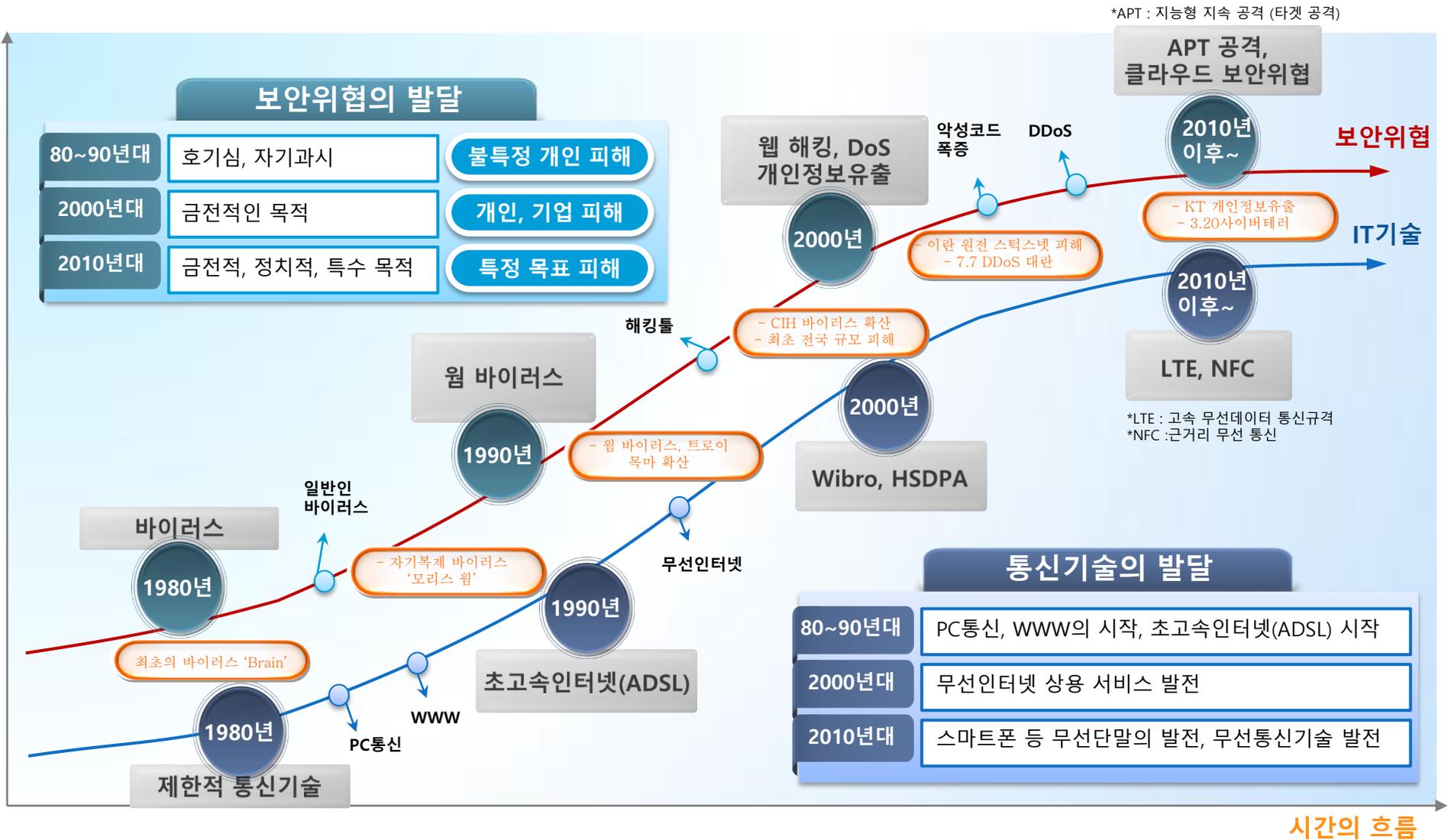




**Attacks Evolves**

# Cyber Attack Evolves

기술의 발달



# External – Internal – Trust - Complex



외부 공격(External Attack)은 경계를 보호하는 것이었습니다. 보안을 성으로 비유한다면 성문을 닫고 들어오는 길목을 차단 했다면 적을 막을 수 있었습니다. 아군과 적군의 구분이 확실 했었습니다.



# External – Internal – Trust - Complex



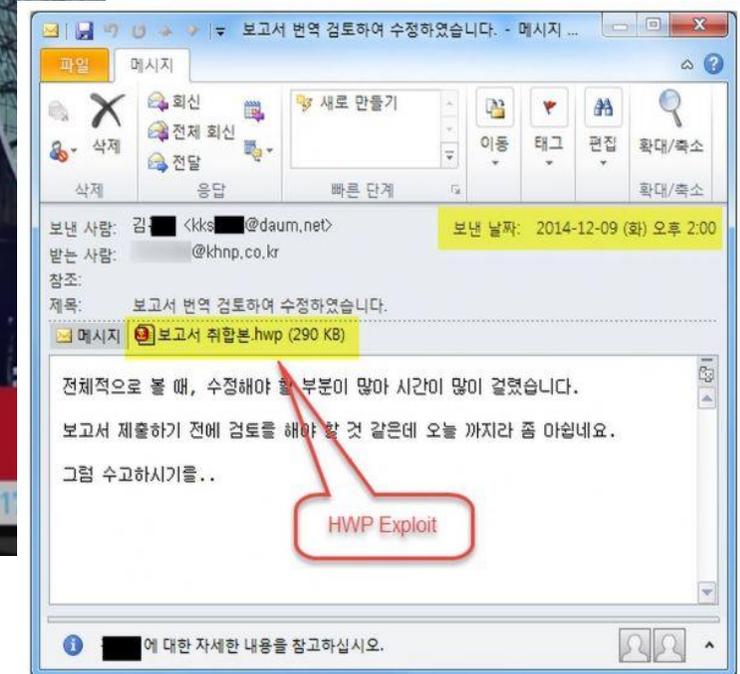
내부 공격(Internal Attack)은 아군과 적군이 불확실 해 저서 성 밖에서도 적이 있지만, 성 안에도 내부의 적이 존재 하였습니다. 그래서 성문을 지키는 것 뿐만 아니라 자산, 즉 Data를 지키는 것으로 변화하였습니다.



# External – Internal – Trust - Complex



- 그 어느 곳도 안전한 망은 없다.
- 이메일(스피어피싱)을 통한 악성코드 유포





신뢰 공격(Trust Attack)은 다양한 신뢰 또한 신뢰 할 수 있는 방법을 이용하여 자산을 보호하고 있으나 또한 해커의 표적 대상이 되었고 더 이상 신뢰 할 수 없게 되는 공격이 발생하고 있습니다.

## 보안업체 전자서명 해킹...악성 코드 유포 우려

한 보안업체가 은행과 공공기관에 제공하는 보안 프로그램이 해킹당한 사실이 확인됐습니다.

누군가 이를 통해 악성 코드를 유포하려고 했던 것으로 보이는데요.

국정원과 검찰이 수사에 나선 가운데 북한과의 관련성도 거론되고 있습니다.

임성호 기자입니다.

[기자]

해킹된 사실이 밝혀진 건 한 금융보안업체의 '코드 서명' 프로그램입니다.

지난해 10월 발급돼 시중은행과 증권사 등 8개 금융회사와 5개 공공기관이 쓰고 있었습니다.

코드 서명은 '인터넷의 인감 증명'과 같은 역할을 합니다.

인터넷 사이트에서 어떤 프로그램을 내려받을 때, 게시자가 누구인지를 알려줘 믿고 설치할 수 있게 해줍니다.

코드 서명이 없는 프로그램은 경고창을 띄우거나 아예 설치를 차단해 사용자를 보호해줍니다.

따라서 해킹한 코드 서명을 악성 코드를 심은 프로그램에 붙이면 손쉽게 금융과 공공기관 전산 시스템에 침투시킬 수 있습니다.



SSL 보안인증서 발급



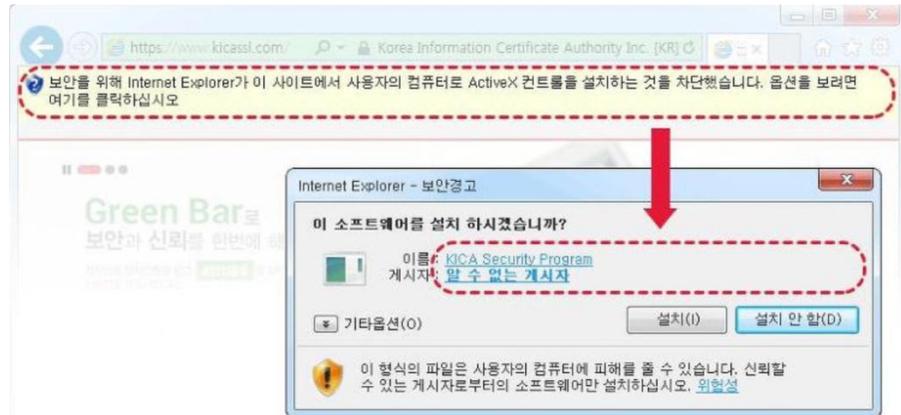
SSL 외부침입차단, 개인정보 보호



보안서버인증기관

운영자의 웹서버

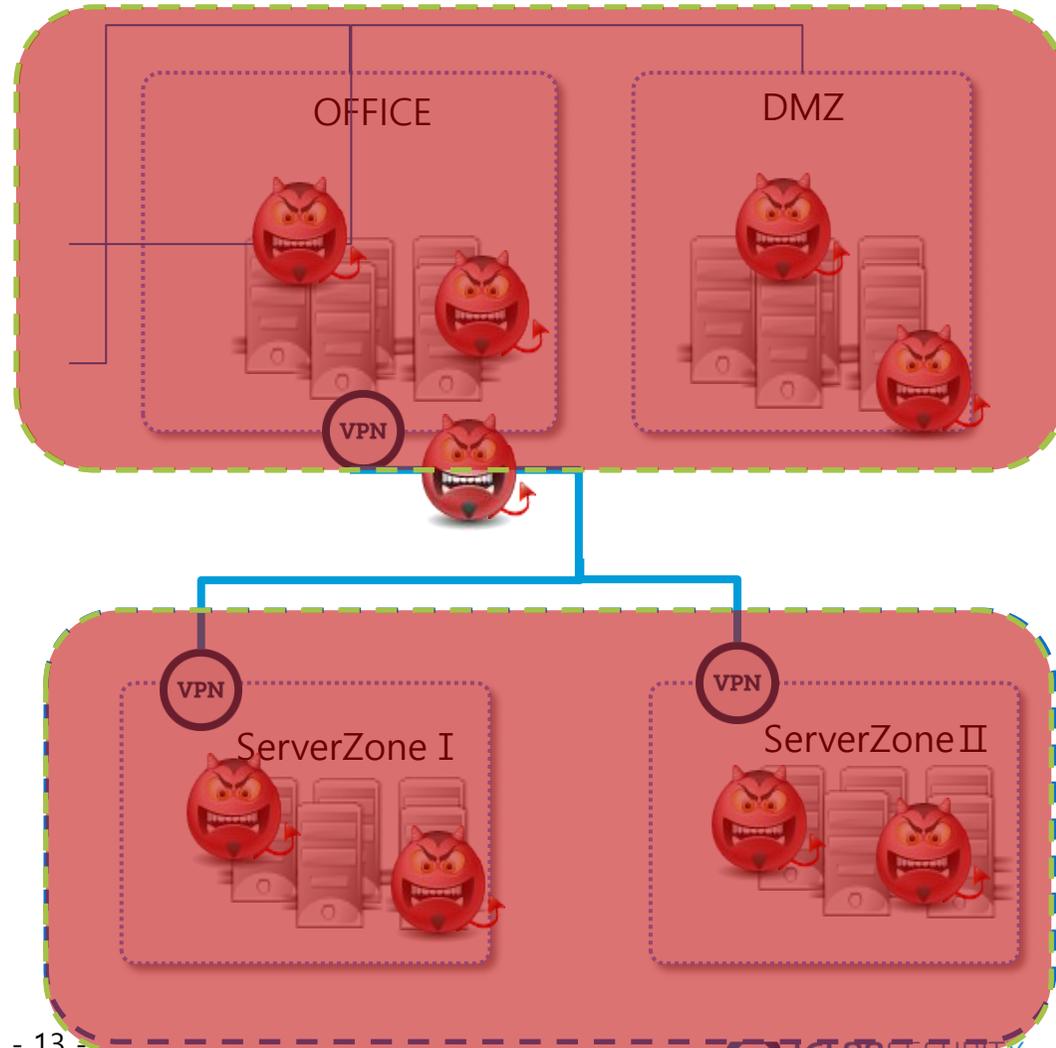
사용자의 웹브라우저



# External – Internal – Trust - Complex



복합 공격(Complex Attack)은 단순 사이버공격에서 외부, 내부, 신뢰 등 복합적인 공격 방법을 사용하며 진화되고 단순히 컴퓨터에 바이러스만 감염되는 수준에서 정보유출, 시스템파괴 등 지능화, 고도화되고 있습니다.

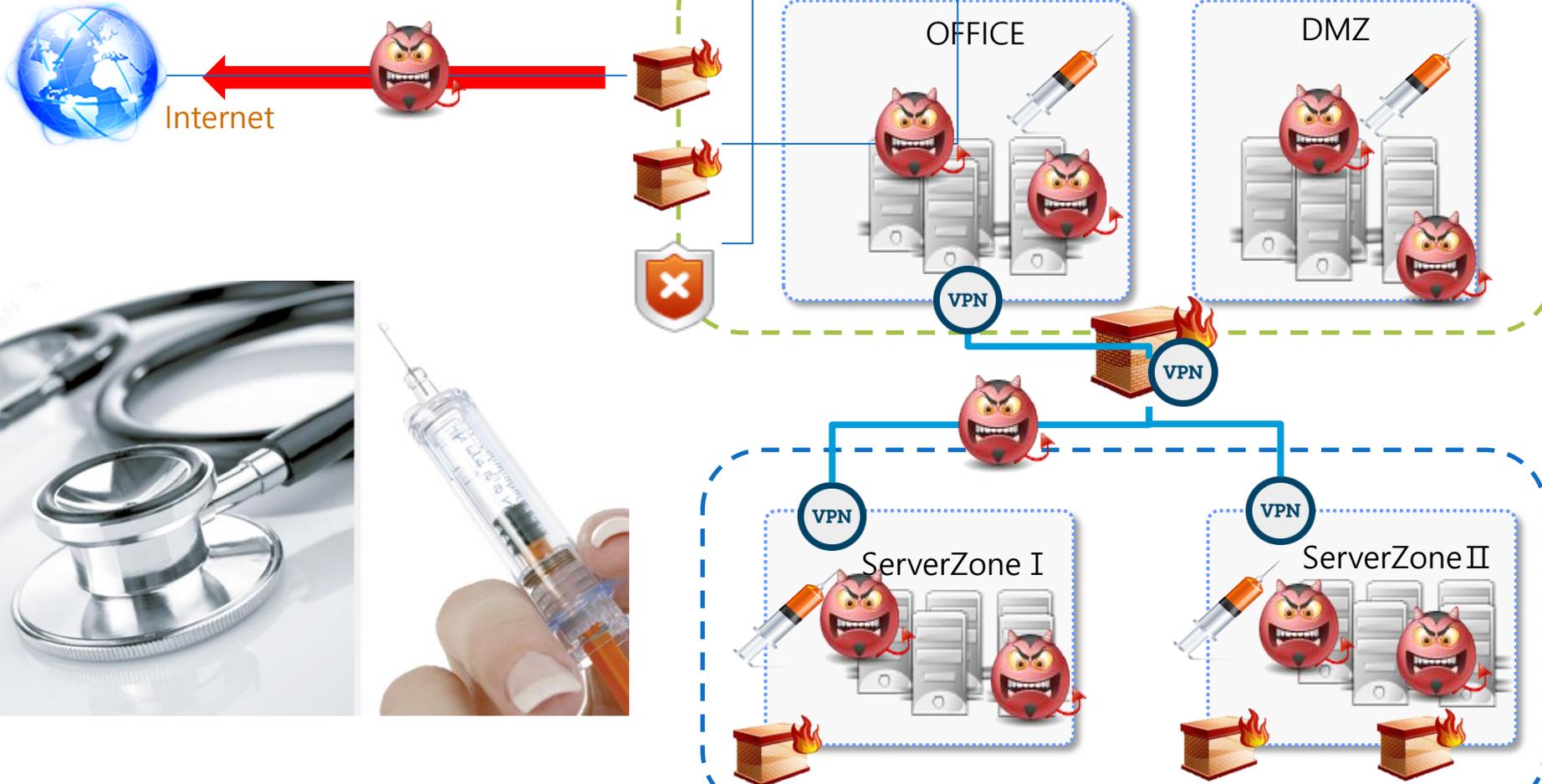


**Now**

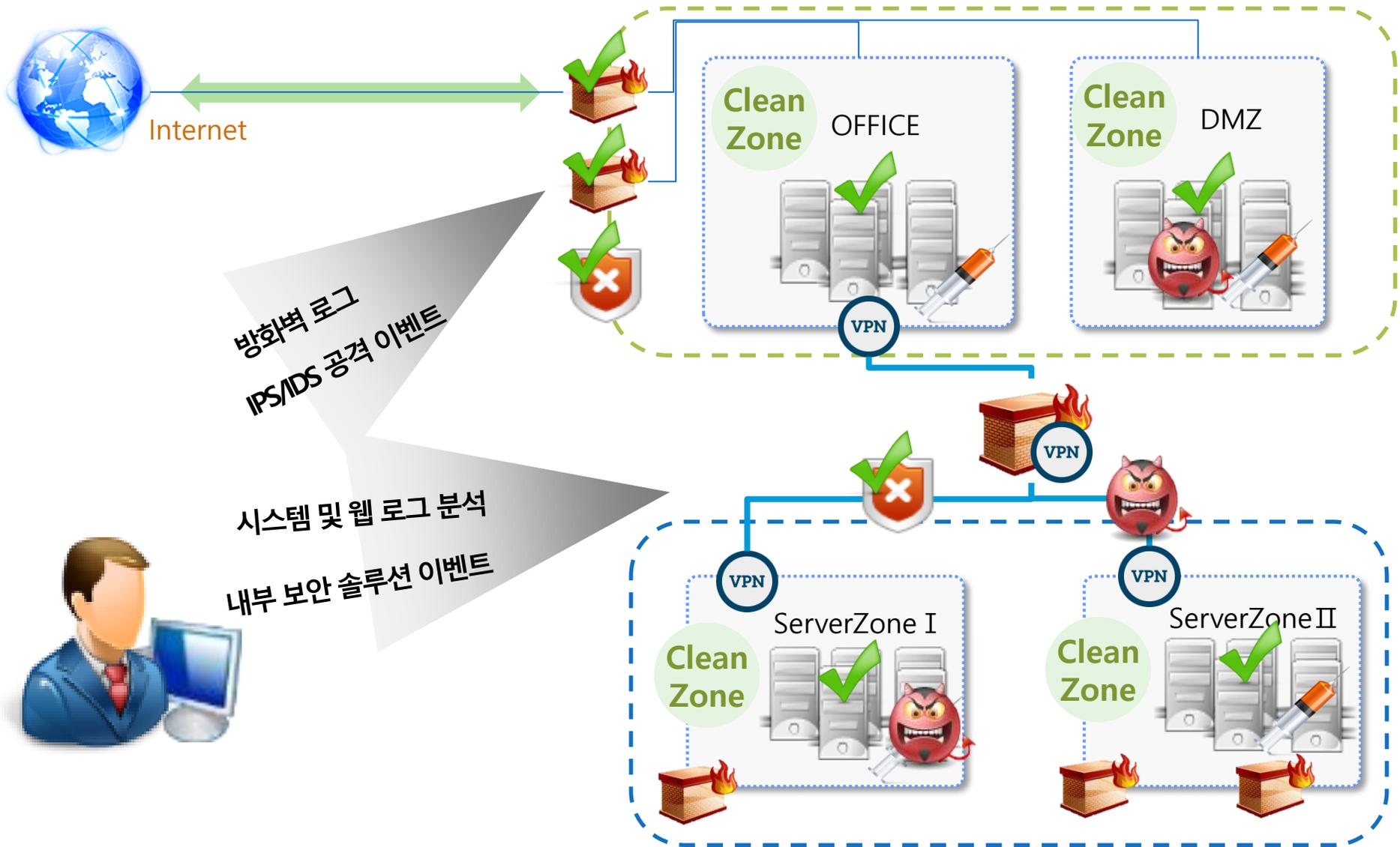
# Cyber Attack에 전쟁을 선포 합니다.



- ❖ Cyber Attack에 대응하기 위해 보안장비를 구축하여 외부에서 들어오는 침해 시도를 사전에 차단 하겠습니다.
- ❖ 내부에서 발생 되는 악성코드 감염등은 백신 등 내부 보안 솔루션으로 침해 예방/대응을 하겠습니다.
- ❖ 또한, 사전에 관리적, 기술적 보안에 대한 취약점이 존재 하는지 전문 보안컨설턴트에게 의뢰하여 예방하겠습니다.



# Cyber Attack에 대응하고 있습니다. 어떻게?



# 보안장비만 있으면 무엇이든 막을 수 있다?

장비는 많은데 뭘  
해야 할까?



이게 공격인가?  
괜히 막아서 장애 생기면?

나는 도대체 누구?

공격이 들어오면 뭘 해야 하지?

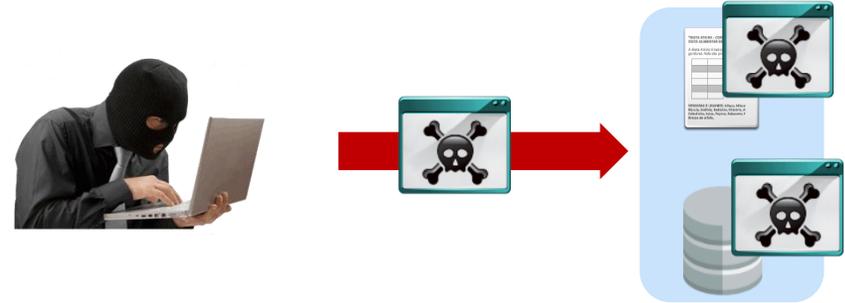
**Why?**

# 침해사고 특징

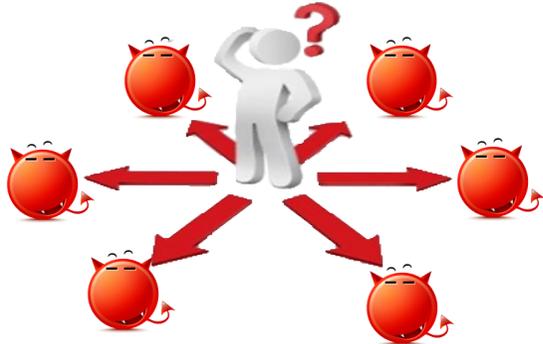
특정 시설 또는 기관 위협



지능형 지속공격 (APT 공격)



End User 를 이용한 공격



공격 방식의 다양화



‘08년  
옥션 해킹

‘10년 이란 핵발전소 Stuxnet

‘11년 SK컴즈 해킹

‘13년 3.20 사이버테러

‘14년 한수원 해킹

‘11년 NH농협 전산망 마비 ‘11년 RSA 해킹

‘13년 6.25 사이버테러 ‘14년 카드3사 정보유출 ‘15년 금융기관 DDoS 공격



사이버테러 위협 및  
침해사고 지속적 발생

# 북한 핵 도발 사이버테러 확산

대북 확성기 방송 재개...사이버 경보도 '관심' 격상

北 수소탄 실험 발표...사이버상 긴장감도 고조되나?

남북관계 악화일로...사이버위기경보 한 단계 또 격상

발생년도	사회적 이슈	사이버 공격	발생기간	피해 사례
2009	북한 2차 핵실험	7.7 DDOS	2개월	청와대와 국회 등 정부기관 전산망 마비
		.20 전산대란	1개월	금융사 및 언론사 전산망 마비
2014		원 해킹	-	한수원 정보유출 사건

사이버위기경보단계

등급안내 >

국내테러경보단계

등급안내 >



▪ 국가전반에 보안태세 강화 필요

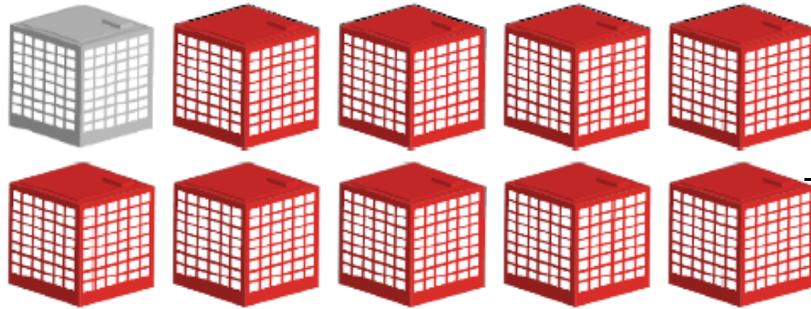


▪ 테러가 발생할 수 있는 일정 수준의 테러 위협 징후가 나타나는 상태

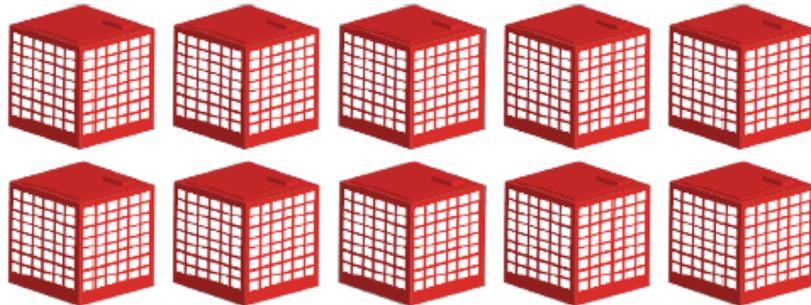


# 사이버 위협은 100% 막을 수 없다

- ~~방어자 : 털린 조직, 털리지 않은 조직~~
- 공격자 : 털린 것을 아는 조직과 모르는 조직
- 방어에서 대응으로.....



**95% of Companies are Compromised**



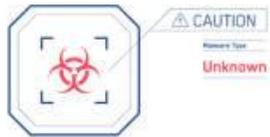
“There are two kinds of big companies in the United States. There are those who’ve been hacked....and those who don’t know they’ve been hacked”

- James Comey, Director FBI

# 랜섬웨어라는 무차별 공격에 완전 초토화 되고 있습니다.

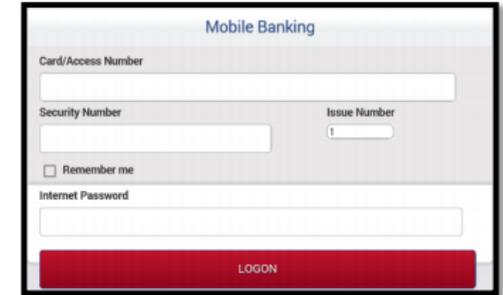
- ④ 매일매일 진화하는 랜섬웨어
- ④ 가장 오래됐고, 가장 쉬운 공격 중 하나 스팸 → 가장 지능화된 공격으로 진화

알려지지 않은 신종 악성코드가  
침해 사고에 핵심적인 역할 수행  
**지능형 악성코드**



**랜섬웨어**

지능화된 랜섬웨어 악성코드로  
금전 피해 및 중요 정보자산 이용 불가



**Mobile Ransomware**



[RSA Conference 2016 발표자료 중]

# 아직 해커는 진화를 시작도 안했습니다.

- ◀ 공격의 방법이나 형태는 변한 게 맞다.
- ◀ 하지만, 아직 인프라 변화는 시작도 안했다. (TCP/IP, IPv4)

Morris Worm  
Buffer Overflow

1988

CVE-2016-1287  
Buffer Overflow

2016

We're still introducing the same old bugs in our code



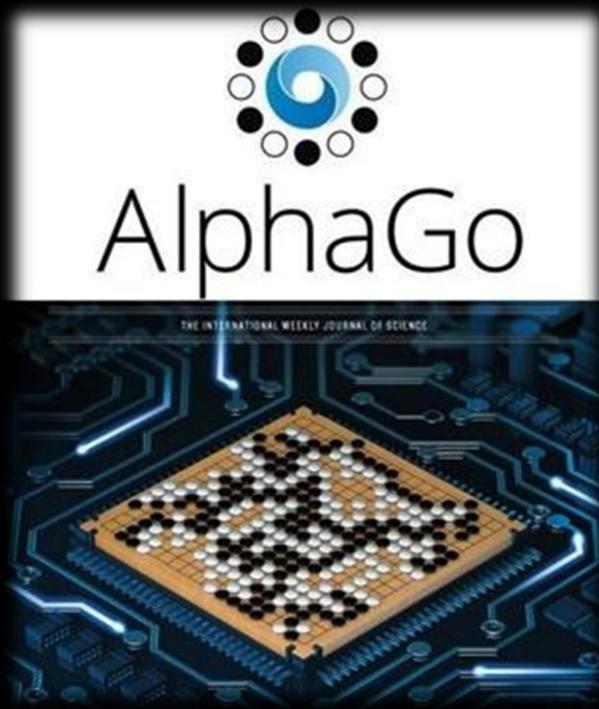
## DEP & ASLR makes exploitation more difficult

Plenty of programs/libraries/systems still not supporting ASLR/DEP

[RSA Conference 2016 발표자료 중]

[중간 결과]

0 : 3



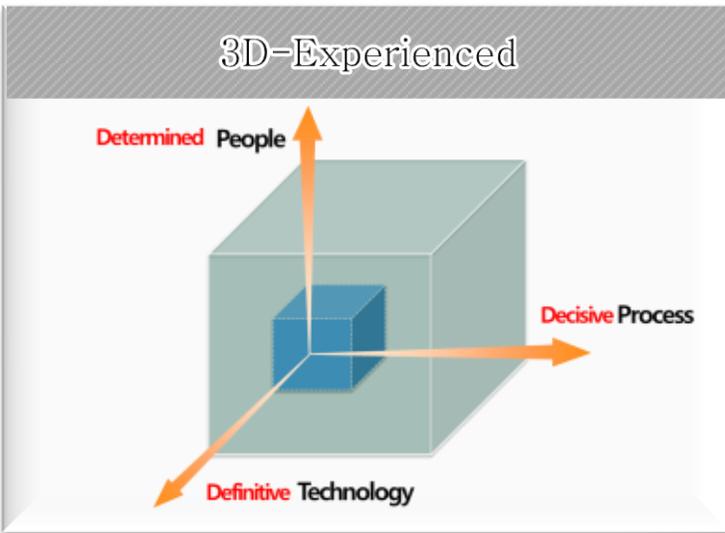
“If you know the enemy  
and know yourself, you  
need not fear the result  
of a hundred battles.”

— **Sun Tzu, The Art of War**



# 3E(Experienced – Enabled – Expected) Security Framework

이글루시큐리티의 **경험**이 반영된 모듈을 통한 **맞춤형 서비스** 제공



현황 분석 & 서비스 단계

	모듈1	모듈2	모듈3	모듈4	모듈5	모듈6	모듈7
서비스 1 [개인정보 관제]	○						
서비스 2 [웹서비스 관제]	○	○					
서비스 3 [보안관제]	○	○	○				
서비스 4 [종합보안관리/관제 1]	○	○	○	○			
서비스 5 [종합보안관리/관제 2]	○	○	○		○	△	
서비스 6 [융복합 관제]	○	○	○				○

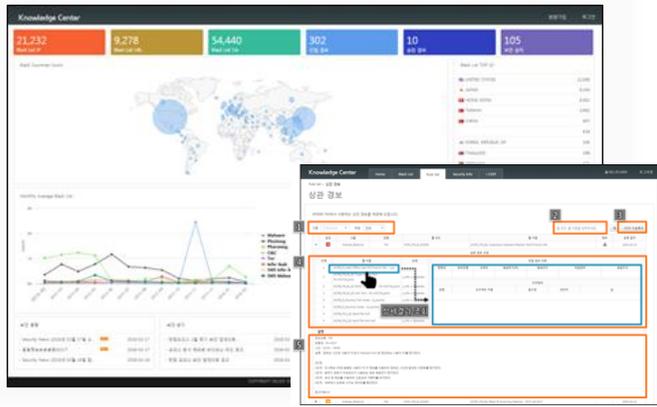
## 이글시큐리티 모듈화된 보안관제 서비스

구축/유지	보안관제	운영/관리	진단/예방	인증/교육	패키지 서비스
ESM 구축/연동	상황전파 /공유	보안장비 운영	취약점 점검	ISMS	종합보안 Care 패키지
WEB-MON 구축	보안이벤트 모니터링	보안정책 적용·관리	모의해킹	PIA/PIPL	개인정보 Care 패키지
ISMS 구축/인증	침해대응	이력관리	모의훈련	이글루스쿨 (기술교육)	홈페이지 Care 패키지
유지관리	침해분석	지침/매뉴얼 개정	악성메일 훈련	집체교육 (일반교육)	보안장비 Care 패키지
	홈페이지 위변조 탐지	SLA	소스코드 진단		침해대응·분석 패키지
	개인정보 유출 탐지	헬스체크	보안실태 점검		보안인식 강화 패키지
		유지관리	보안수준 점검		...

# 3E(Experienced – Enabled – Expected) Security Framework

이글루시큐리티의 **경험+분석**이 반영된 정책을 통해 **맞춤형 서비스** 제공

## K-Center 사이버위협 분석정보



## 위협에 대한 예측과 실행 가능한 관제 정책(Rule) 제공

### 300여개의 검증된 관제 Rule

The screenshot shows a table of rules with columns for Name, Severity, and Description. A list of 5 numbered callouts points to specific rule details and configuration options.

### 다양한 시나리오기반의 상관분석

The screenshot displays a correlation analysis interface with a table of related events and a detailed view of a specific correlation rule, including its logic and associated assets.

## 위협정보 상황 전파 체계



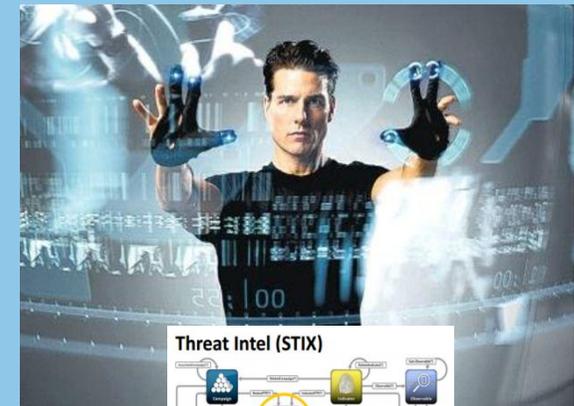
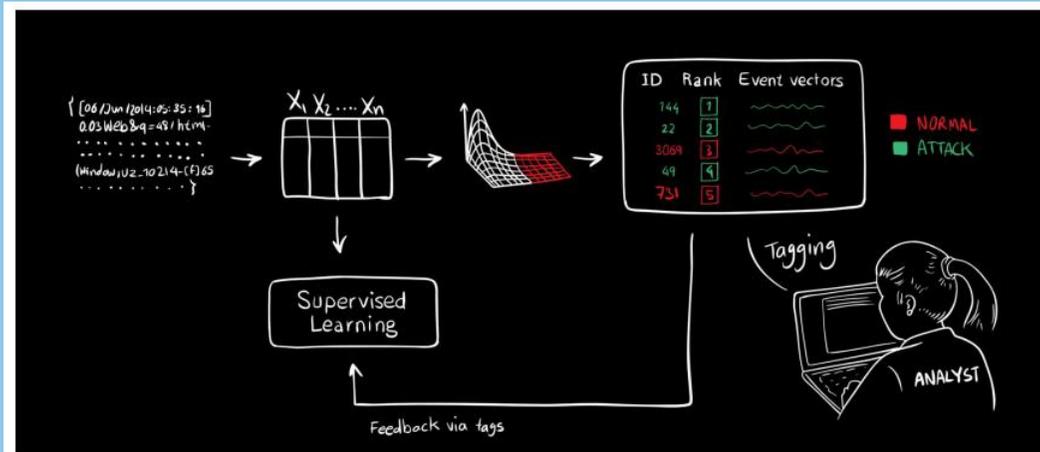
## 각 Rule에 대한 상세한 설명 및 활용방안 제시

Two detailed cards provide specific information for rules: 'NCS FW (R) Web PortAllow: OUT ->R(OUT)(1.ppt)' and '용이름 - ICRS FW (R) Web PortAllow: OUT(1.ppt) ->R(OUT)(1.ppt)'. Each card includes a description, configuration details, and a diagram of the rule's logic.



# 3E(Experienced – Enabled – Expected) Security Framework

이글루시큐리티의 **경험+ 분석+ 예측**이 반영된 정보를 통한 **맞춤형 서비스** 제공



[Data Scientist]



[Security Analyst]

- ④ 보안관제 프로세스가 녹아 있는 Platform
- ④ Big Data 기반 분석, Full Packet 처리, 다양한 보안이벤트와의 유연성

**SPIDER™** WHOIS 검색에 입력

Administrator님 환영합니다  
대시보드 홈 메뉴변경 로그아웃

모니터링 | 사이버위기관제 | **보안관제** | 침해사고대응 | 네트워크 | 집중 관계 | 예방활동 | 정보공유 | 보고서 | 관리

사이버위기관제 | **보안관제** | 침해사고대응 | 네트워크 | 집중 관계 | 예방활동 | 정보공유 | 보고서 | 운영관리 | 설정관리

사이버위기관제 | 관계현황 | 침해사고대응 | 네트워크 | 집중 관계 | 예방활동 | 정보공유 | 보고서 | 자산관리 | 알림설정

관제요약 | 관계요약 | 사고접수 | 트래픽 종합정보 | 위기관제별 관계 | 유해 IP 관리 | 보안뉴스 | 관계보고 | 자산관리 | 알림설정

경보단계 | 로그수집현황 | 사고이관 | DDoS 트래픽현황 | 최근이슈대응경이후현 | 유해 URL 관리 | 공지사항 | 관계보고통계 | 예외처리 | SMS발송시간

경보발령 | 실시간 관계 | 사고대응 | 세션현황 | 모의 훈련 | FAQ | 일일보고서 | 감사로그 | 임계치설정

위협도 현황 | 통합관계 | 승인처리 | 트래픽 통계 | DDoS 대응 훈련 | Q&A | 통계 | 주의관계IP | 위협속성감소설정

단계판단 | 상관분석 | 사기처리현황 | 실시간 유해 IP | 자료실 | 사용자정의 보고서 | 위험등급판단기준 | 지속시간설정

종합위협도 | 사용자중심 위반행위 | 실시간 로그 | 시스템점검 | 관련법령 | 악의적 보안 취약점 | SMS발송내역 | 메뉴관리

침해사고 접수 | 대응현황 | 상세분석 | 경보분석 | 로그추적분석 | 사용자정의분석 | 통계분석 | 정보감시 | 원시로그감시 | 통계감시 | 사용자정의감시 | 감사로그감시

2015년 1월

SPIDER™

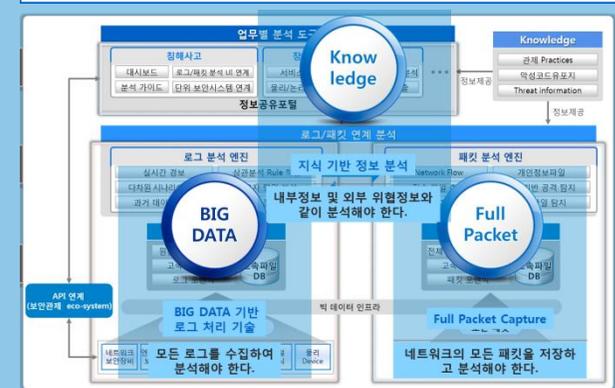
관리자 화면

Spam 차단

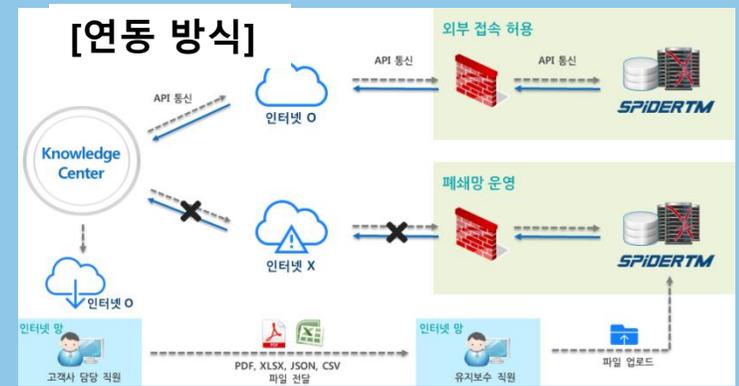
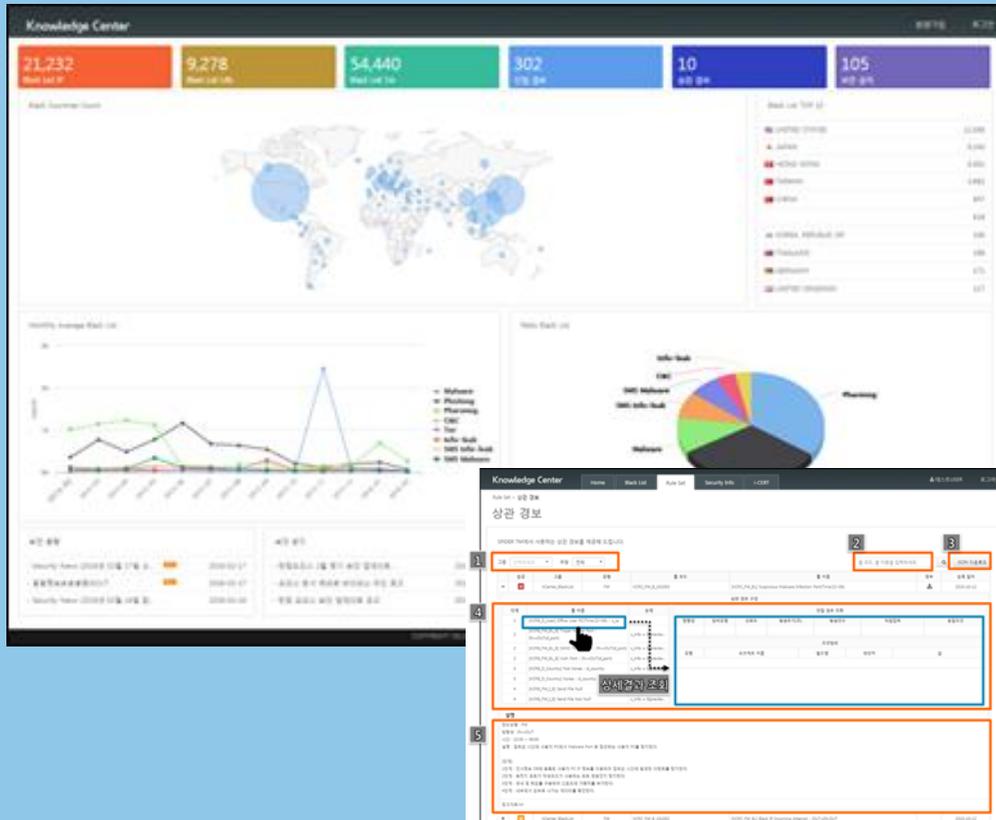
동일 Rule ID

메인 제목

동일 발신자



- SPiDER TM 과의 연동(API)을 통한 지속적인 위협에 대한 대응 가능
- 최신의 보안동향 및 기법을 알려줄 뿐 아니라 실제적인 관제 Rule 제공



### [SPiDER TM 연동화면]

No	설명
1	접속 URL : http://kcenter.igloosec.com/kcenter/api/dataSync/json/ 접속 Port : 80
2	KCenter 회원 가입한 계정 가입
3	API 방식으로 연동할 데이터 표현 접속 정보를 저장할 다음, [검색 테스트]를 클릭하면 "검색 성공" 일 경우, 정상적인 API 통신이 가능함.
4	

- ③ 다양한 사이버테러를 통해 검증된 비상대응체계
- ③ i-CERT (IGLOO Security Cyber Emergency Response Task Force)

**사이버침해위협 정보 공유, 분석 및 대응**

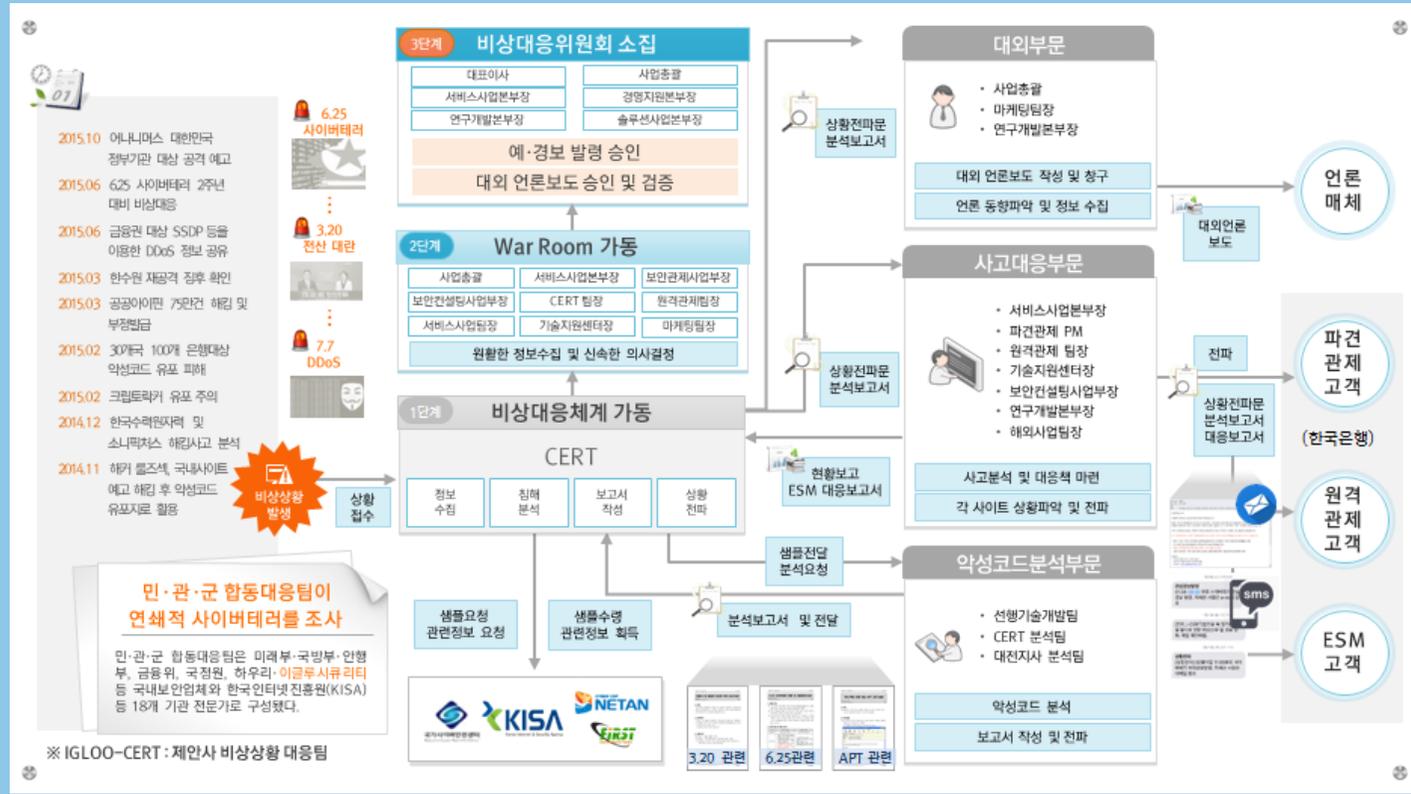
**민·관·군 합동 대응팀**

**국내·외 최신 보안동향, 위협, 기술 정보 제공**

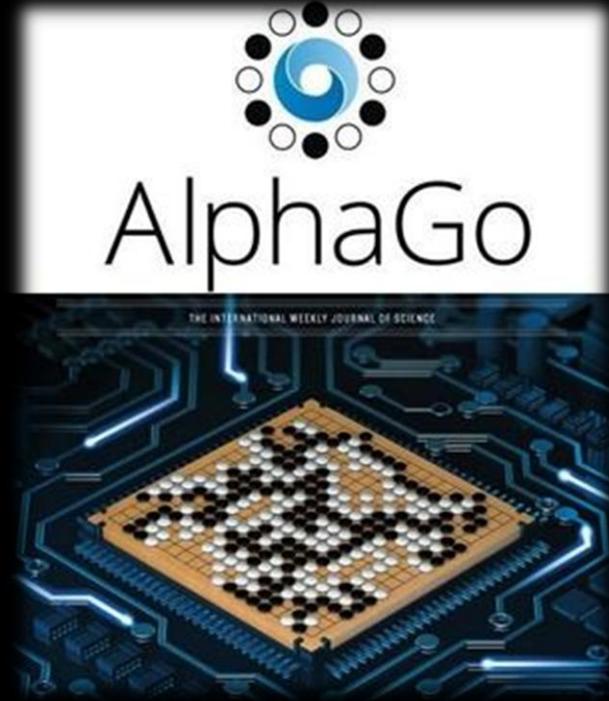
**전문 연구 기관**

**보안위협 정보 공유**

**250여개 이상의 보안관제 수행 중**



1 : 4



감사합니다.

