One Step
Ahead

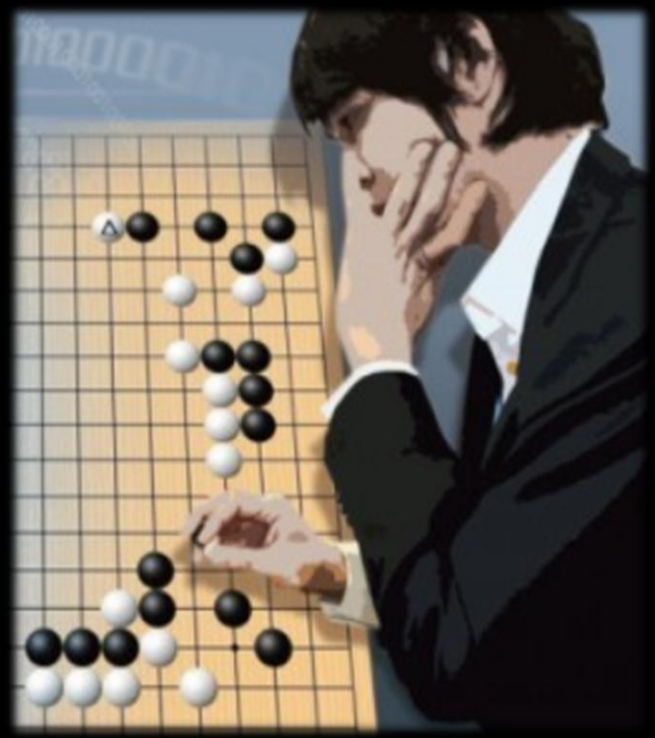
이글루시큐리티의 새로운 관제 전략
Security Intelligence Service

2016. 04

IGLOOSECURITY

세기의 바둑 대결

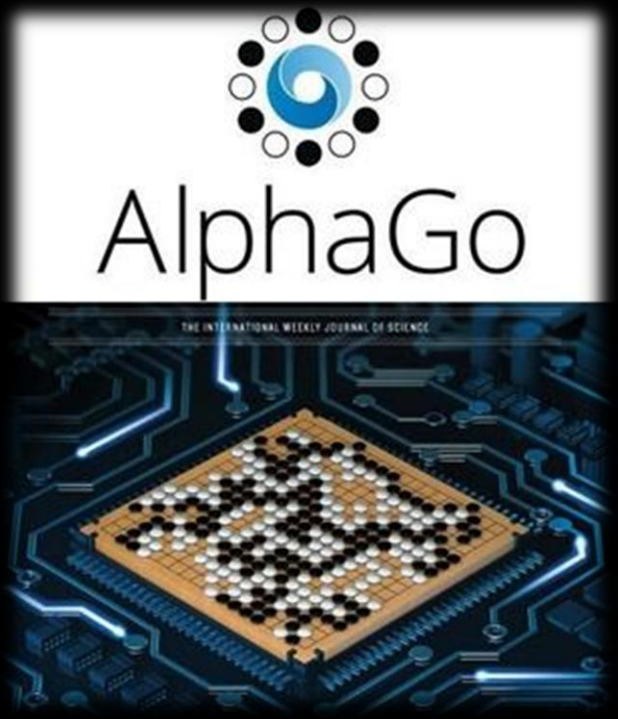
VS



AlphaGO

이세돌 9단

D−5, D−4, D−3, D−2, D−1



0

5

Trends

2008, 2015 Keyword+ Hot Topic

- 2008년과 2015과의 Submission Titles + Quick Abstract

[출처 : RSA Conference 2016]

IGLOOSECURITY

2016 Keyword+ Hot Topic

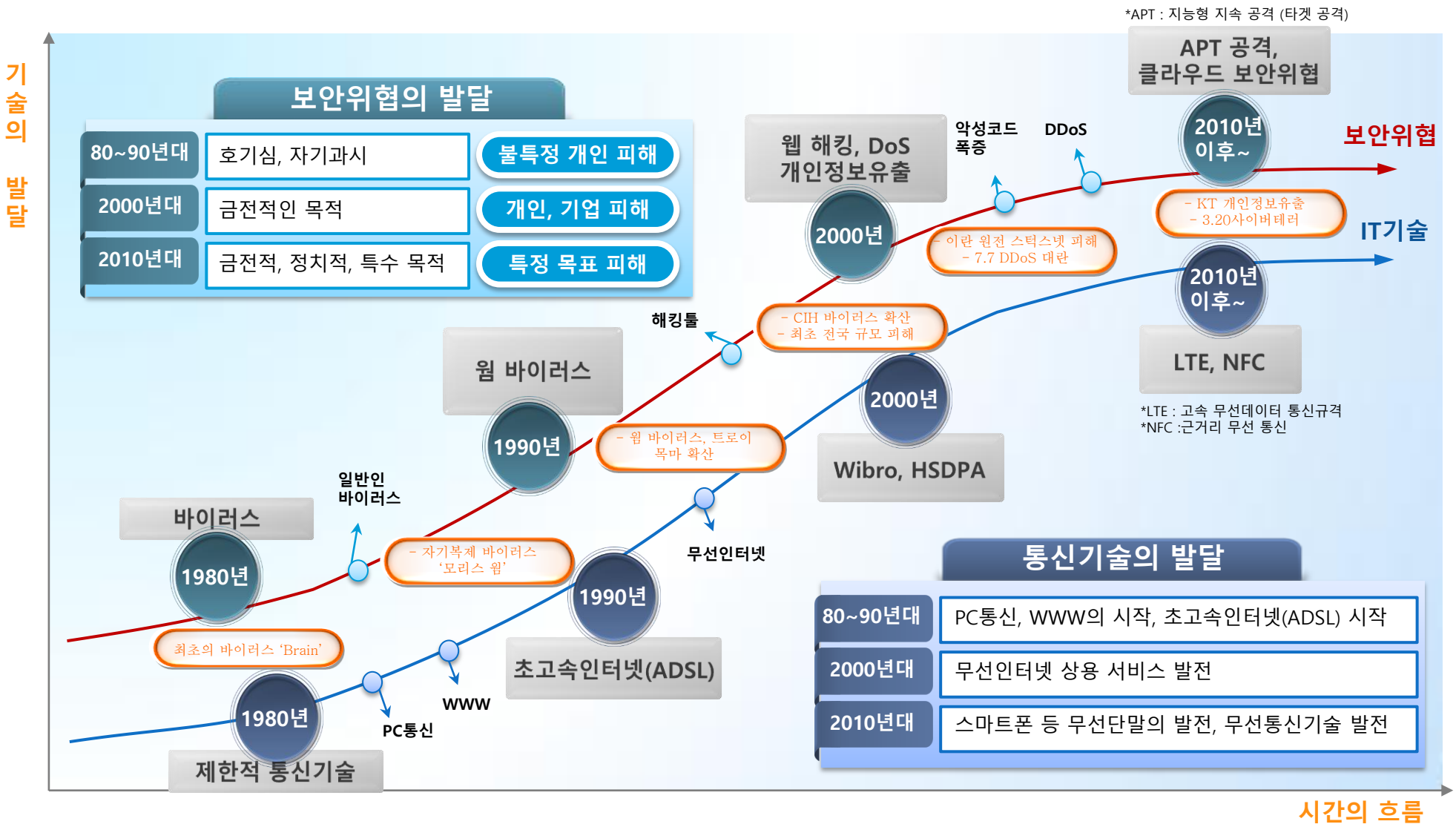
- DATA, CyberSecurity, RISK, intelligence, Threat, Learn
- Internet of Things(IoT), Cloude Security
- Data sovereignty and legislative volatility , Cyber Insurance, Privacy vs Security

[출처 : RSA Conference 2016]

IGLOOSECURITY

Attacks Evolves

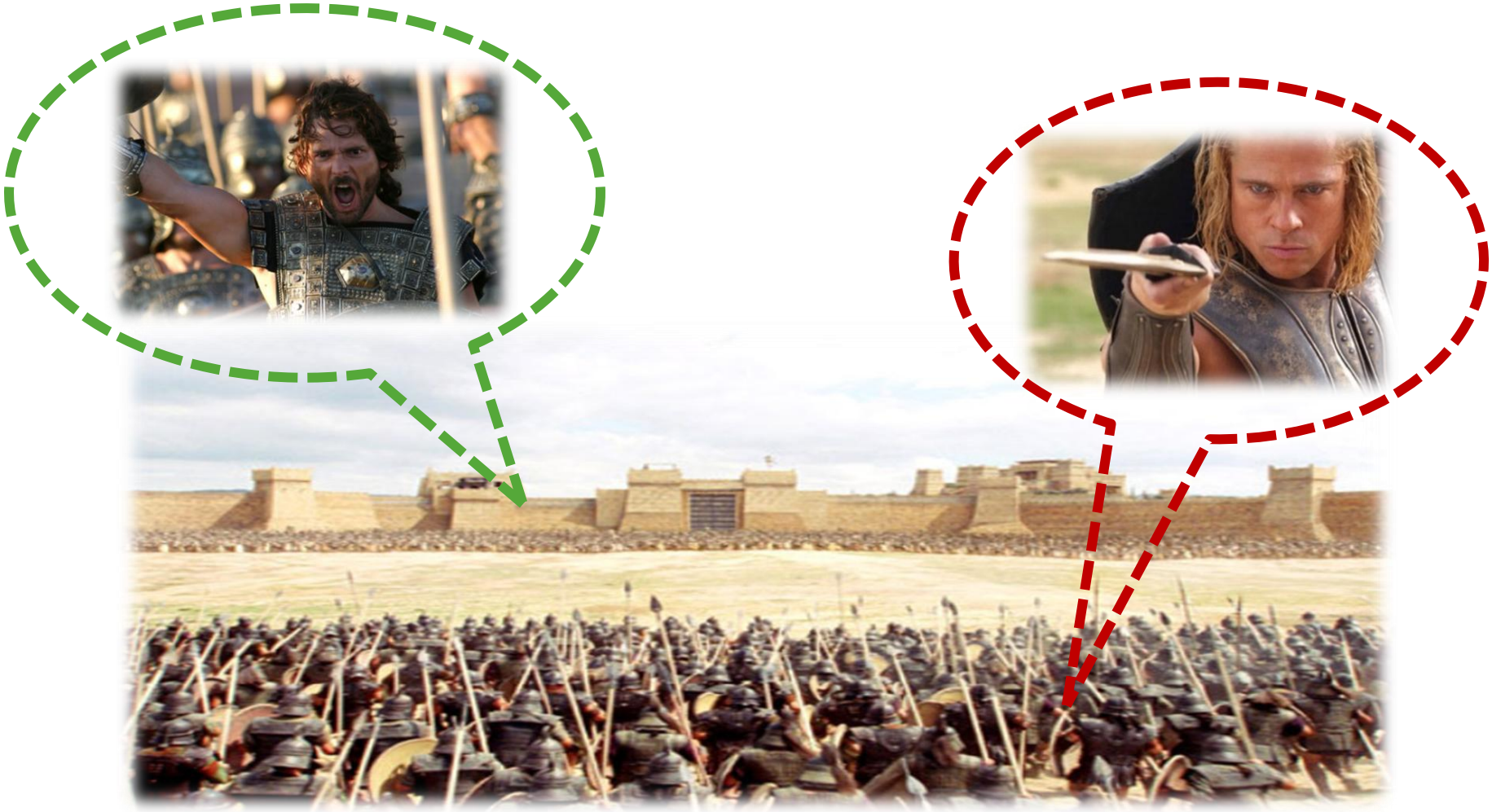
Cyber Attack Evolves



IGLOOSECURITY

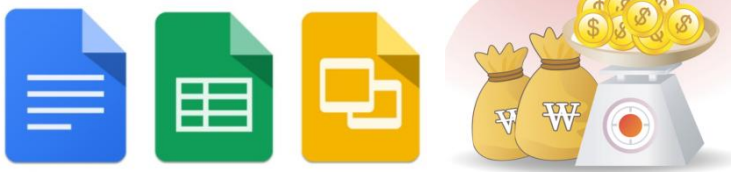
External – Internal – Trust - Complex

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

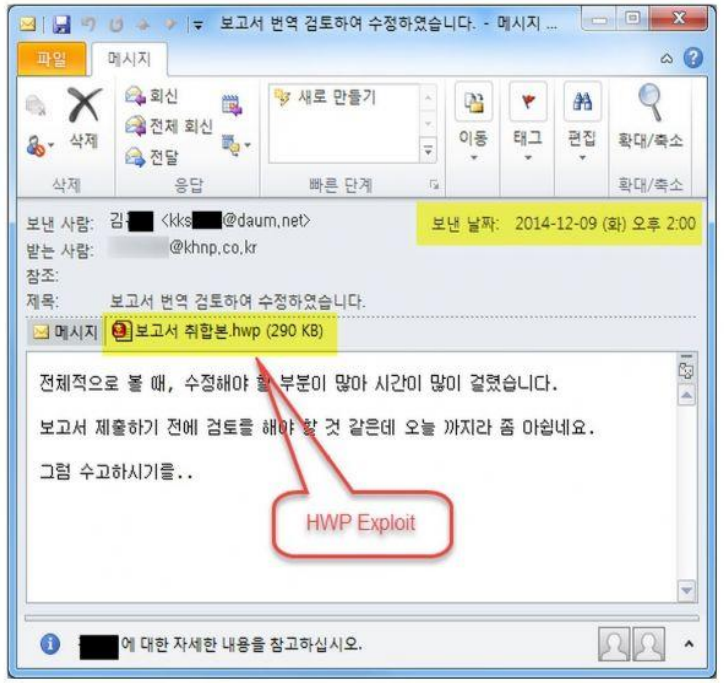
내부 공격(Internal Attack)은 아군과 적군이 불확실 해 져서 성 밖에서도 적이 있지만, 성 안에도 내부의 적이 존재 하였습니다. 그래서 성문을 지키는 것 뿐만 아니라 자산, 즉 Data를 지키는 것으로 변화하였습니다.



IGLOOSECURITY

External – Internal – Trust - Complex

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



IGLOOSECURITY

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 었습니다.

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.

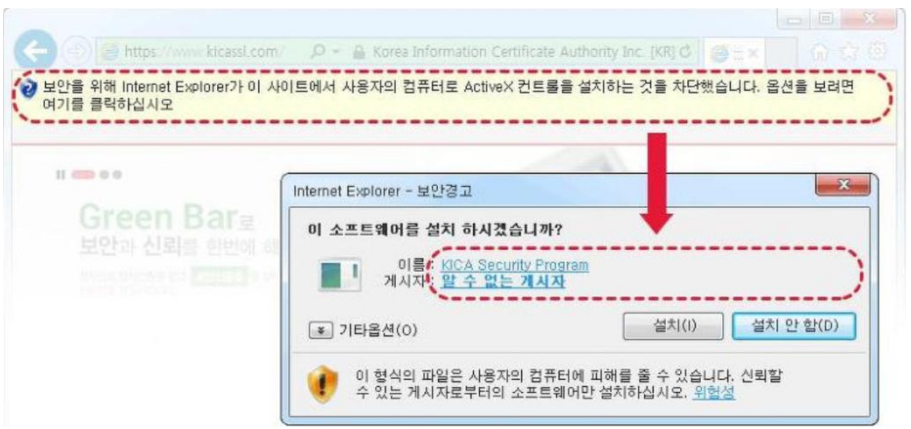
지난해 10월 발급돼 시중은행과 증권사 등 8개 금융회사와 5개 공공기관이 쓰고 있었습니다.

코드 서명은 '인터넷의 인감 증명'과 같은 역할을 합니다.

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

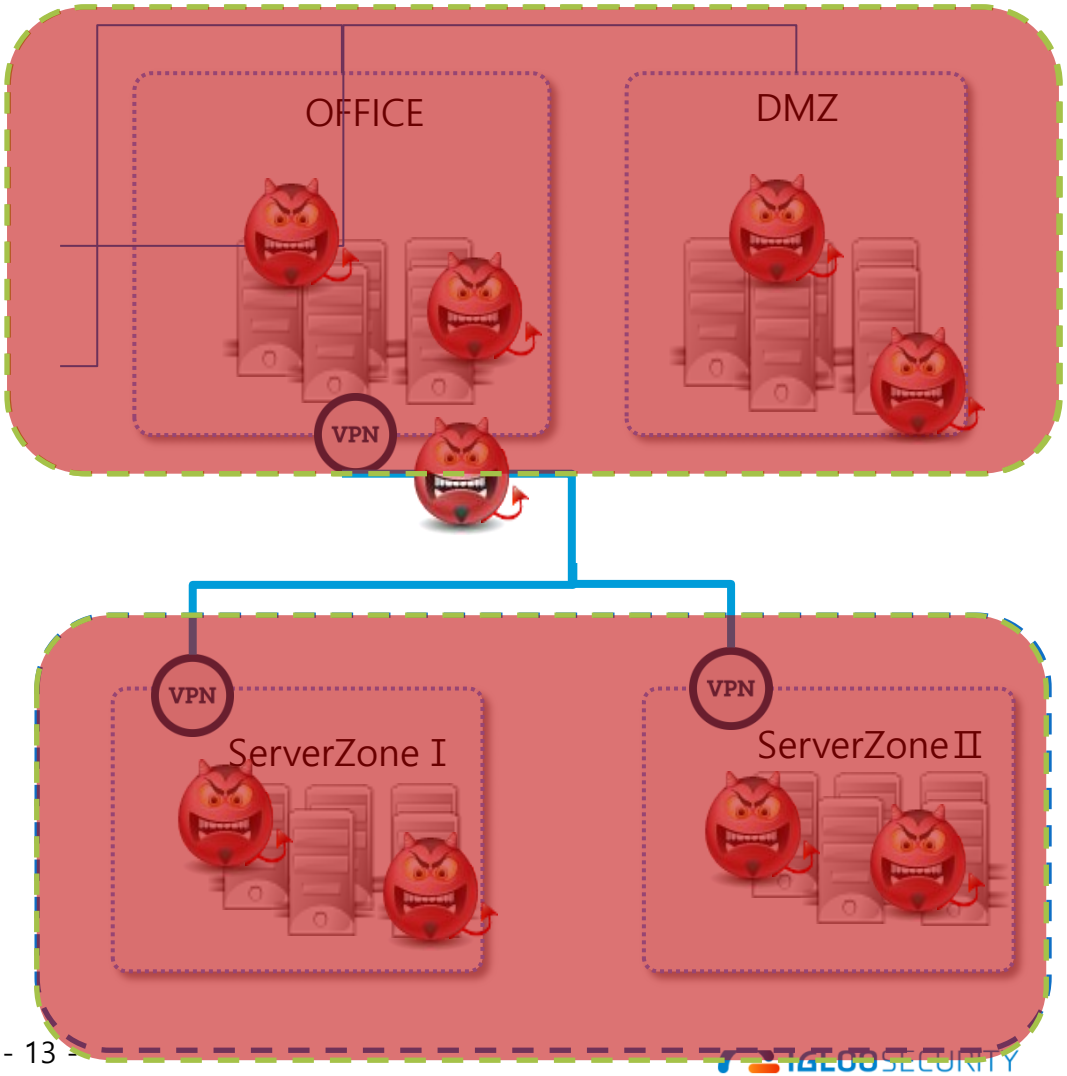
코드 서명이 없는 프로그램은 경고창을 띄우거나 아예 설치를 차단해 사용자를 보호해줍니다.

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



External – Internal – Trust - Complex

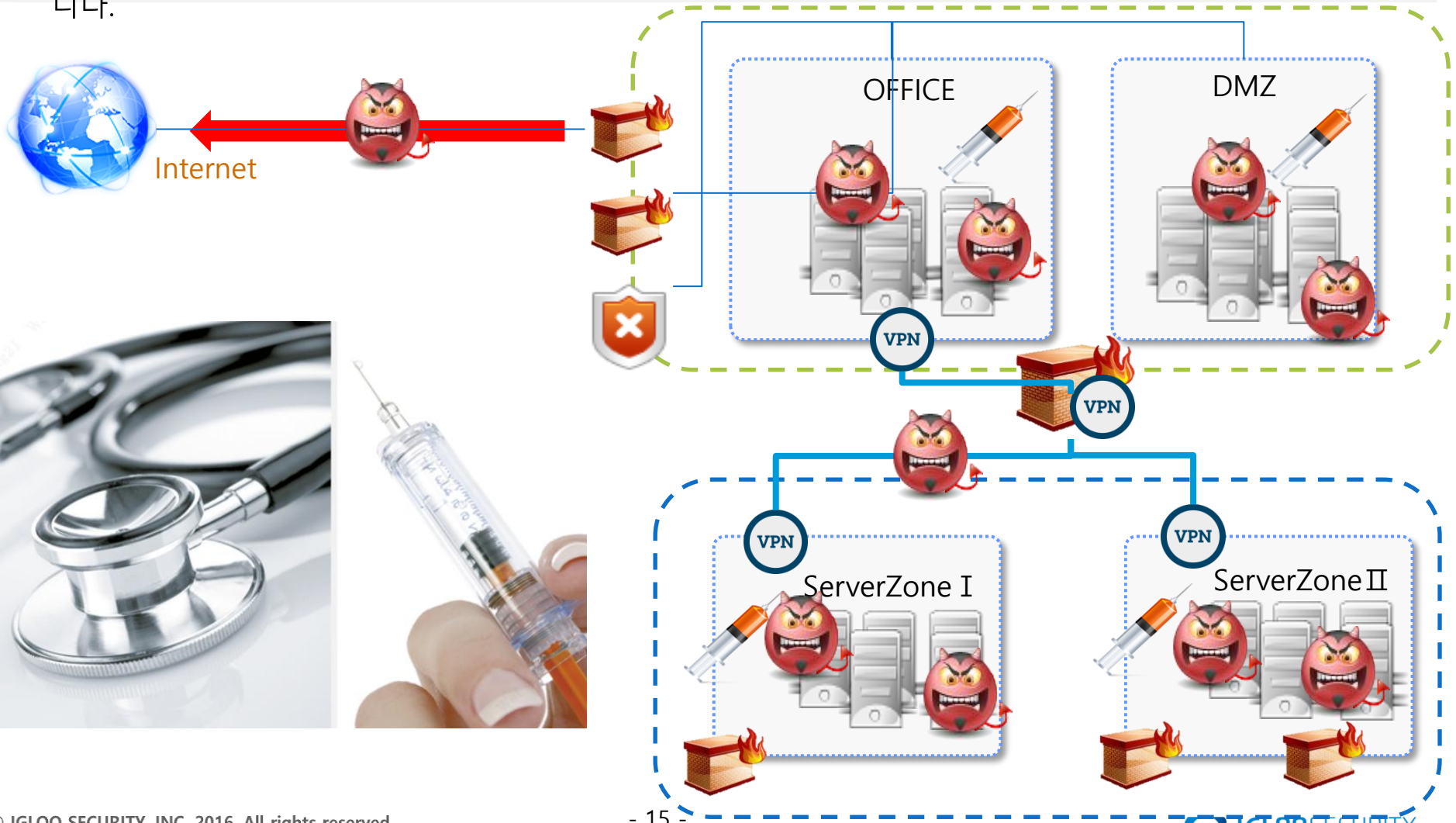
복합 공격(Complex Attack)은 단순 사이버공격에서 외부, 내부, 신뢰 등 복합적인 공격 방법을 사용하며 진화되고 단순히 컴퓨터에 바이러스만 감염되는 수준에서 정보유출, 시스템파괴 등 지능화, 고도화되고 있습니다.



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?

IGLOOSECURITY

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?

IGLOOSECURITY

Why?

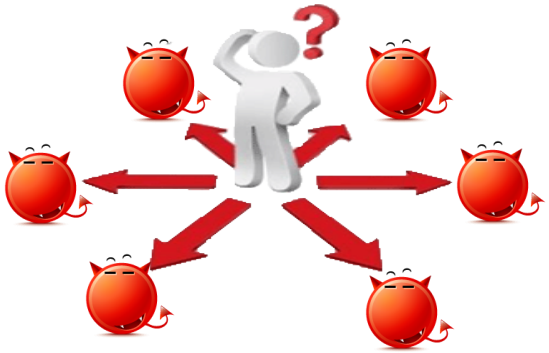
침해사고 특징

특정 시설 또는 기관 위협

TARGET

지능형 지속공격 (APT 공격)

End User 를 이용한 공격



공격 방식의 다양화

IGLOOSECURITY

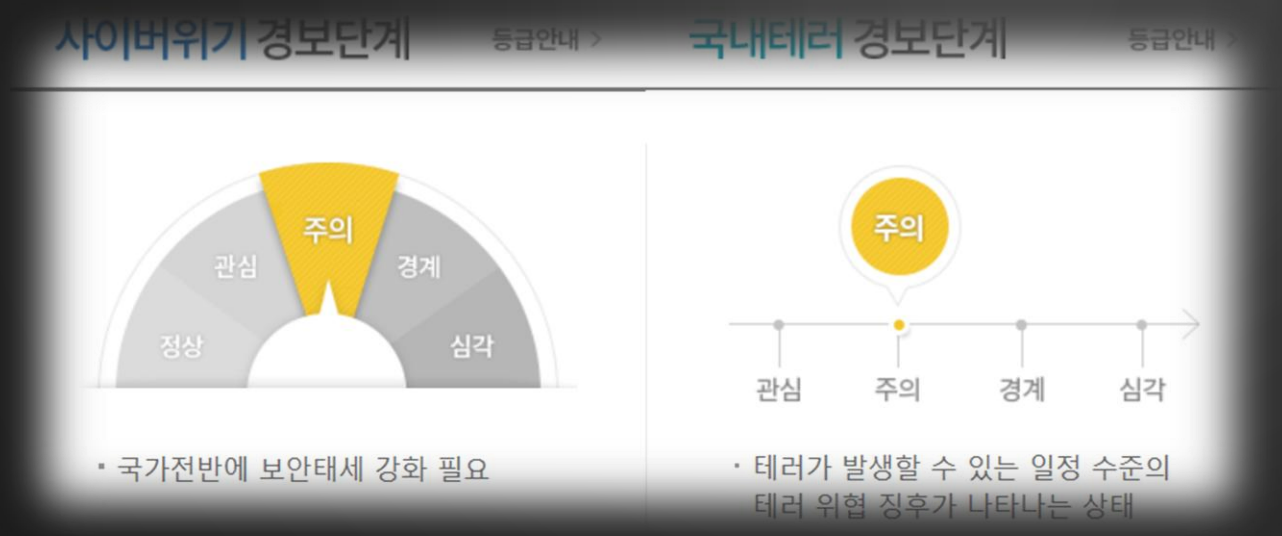
북한 핵 도발 사이버테러 확산

대북 확성기 방송 재개...사이버 경보도 '관심' 격상

北 수소탄 실험 발표...사이버상 긴장감도 고조되나?

남북관계 악화일로...사이버위기경보 한 단계 또 격상

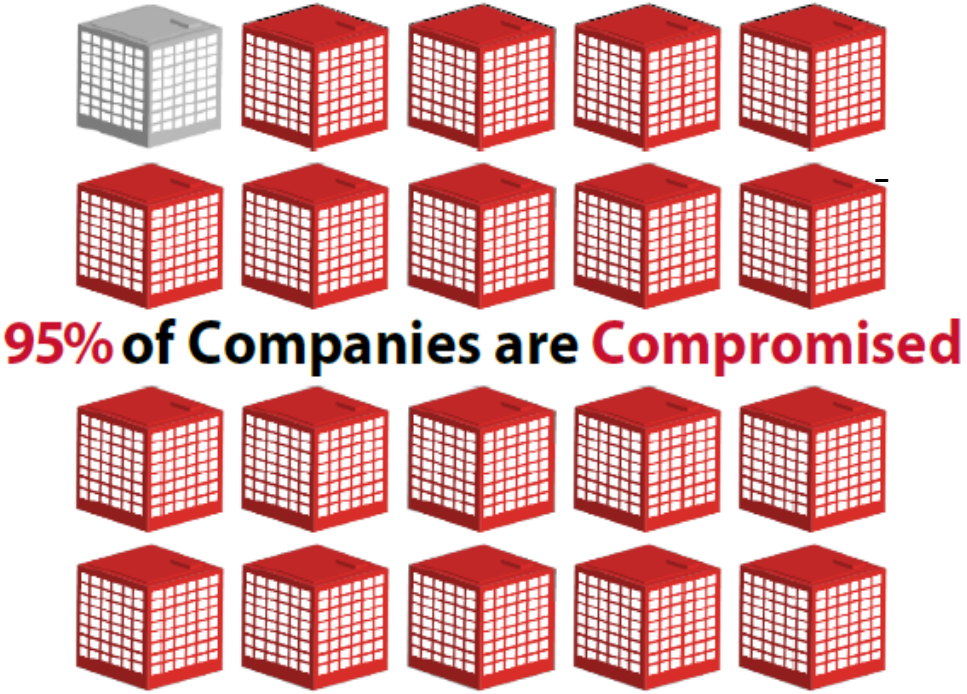
발생년도	사회적 이슈	사이버 공격	발생기간	피해 사례
2009	북한 2차 핵실험	7.7 DDOS	2개월	청와대와 국회 등 정부기관 전산망 마비
		.20 전산대란	1개월	금융사 및 언론사 전산망 마비
2014		원 해킹	-	한수원 정보유출 사건



IGLOOSECURITY

사이버 위협은 100% 막을 수 없다

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



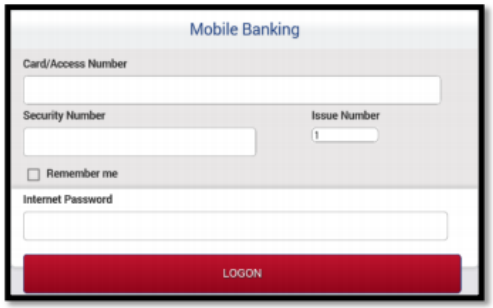
"There are two kinds of big companies in the United States. There are those who've been hacked....and those who don't know they've been hacked"

- James Comey, Director FBI

IGLOOSECURITY

랜섬웨어라는 무차별 공격에 완전 초토화 되고 있습니다.

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



Mobile Ransomeware

[RSA Conference2016 발표자료 중]

IGLOOSECURITY

아직 해커는 진화를 시작도 안했습니다.

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

Morris Worm
Buffer Overflow

CVE-2016-1287
Buffer Overflow

1988 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 Conference2016 발표자료 중]

[중간 결과]

0 : 3

AlphaGo

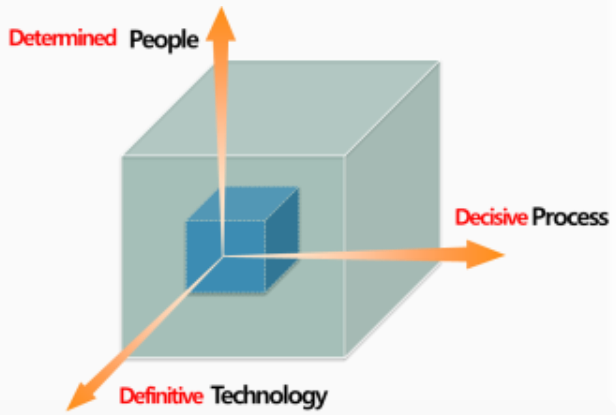
"If you know the enemy and know yourself, you need not fear the result of a hundred battles."

— Sun Tzu, The Art of War

3E(Experienced – Enabled – Expected) Security Framework

이글루시큐리티의 경험이 반영된 모듈을 통한 맞춤형 서비스 제공

3D-Experienced



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

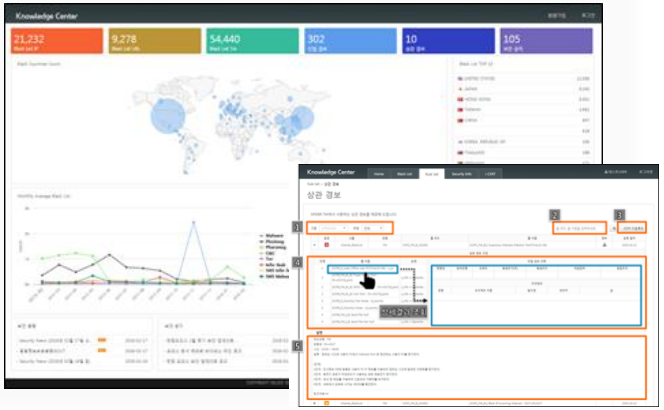
구축/유지	보안관제	운영/관리	진단/예방	인증/교육	패키지 서비스
ESM 구축/연동	상황전파/공유	보안장비 운영	취약점점검	ISMS	종합보안 Care 패키지
WEB-MON 구축	보안이벤트 모니터링	보안정책 적용·관리	모의해킹	PIA/PIPL	개인정보 Care 패키지
ISMS 구축/인증	침해대응	이력관리	모의훈련	이글루스쿨 (기술교육)	홈페이지 Care 패키지
유지관리	침해분석	지침/매뉴얼 개정	악성메일 훈련	집체교육 (일반교육)	보안장비 Care 패키지
	홈페이지 위변조 탐지	SLA	소스코드 진단		침해대응·분석 패키지
	개인정보 유노출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

IGLOOSECURITY

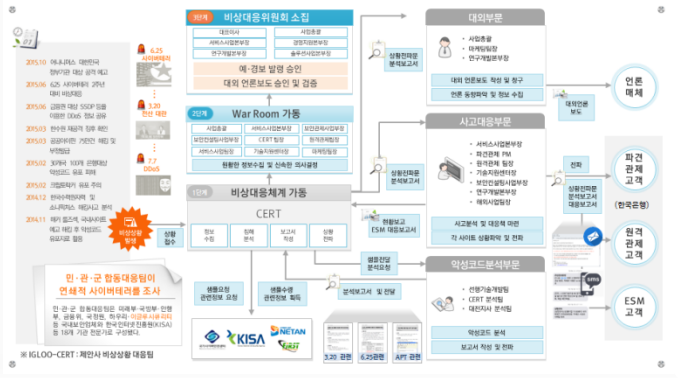
3E(Experienced – Enabled – Expected) Security Framework

이글루시큐리티의 경험+분석이 반영된 정책을 통해 맞춤형 서비스 제공

K-Center 사이버위협 분석정보

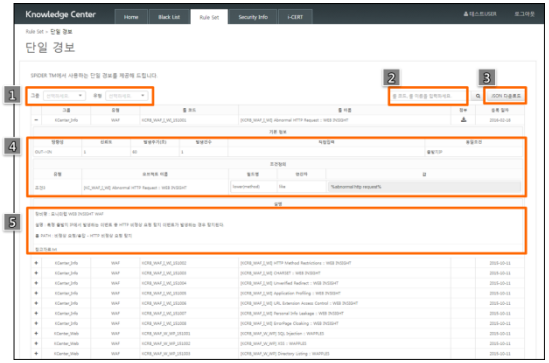


위협정보 상황 전파 체계

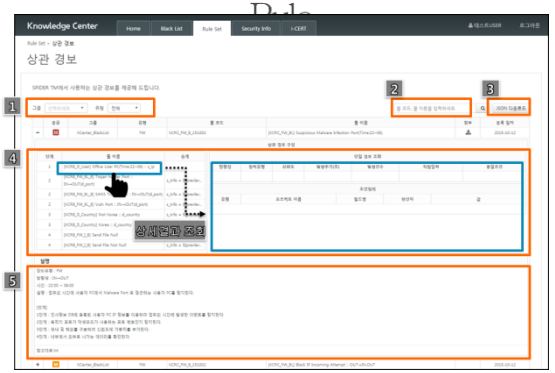


위협에 대한 예측과 실행 가능한 관제 정책(Rule) 제공

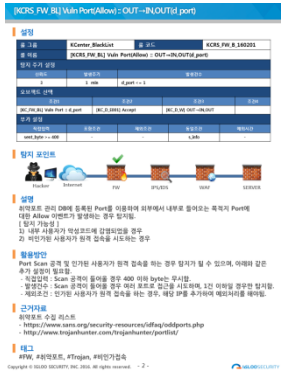
300여개의 검증된 관제 Rule

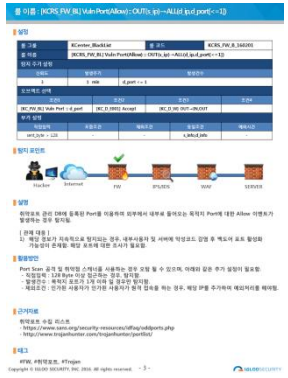


다양한 시나리오기반의 상관분석 Rule



각 Rule에 대한 상세한 설명 및 활용방안 제시

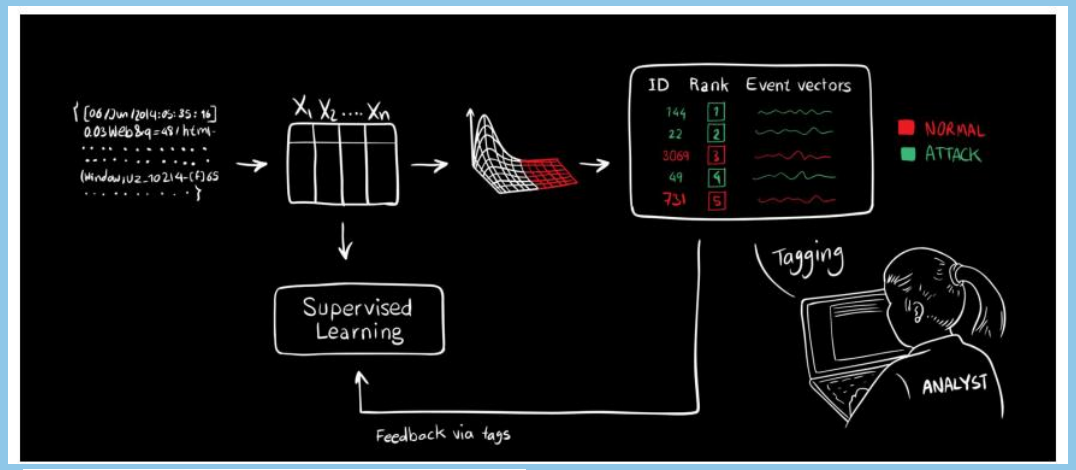




IGLOOSECURITY

3E(Experienced – Enabled – Expected) Security Framework

이글루시큐리티의 경험+ 분석+ 예측이 반영된 정보을 통한 맞춤형 서비스 제공

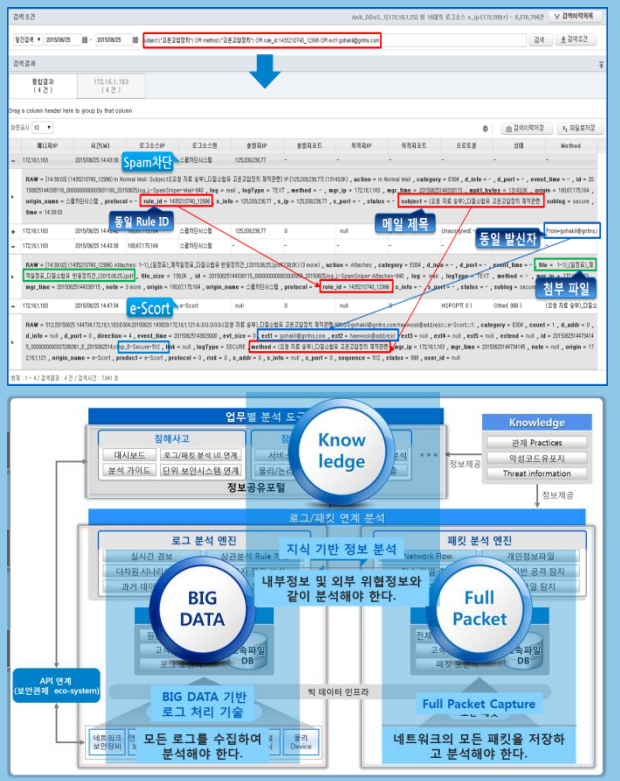


[Data Scientist]

[Security Analyst]

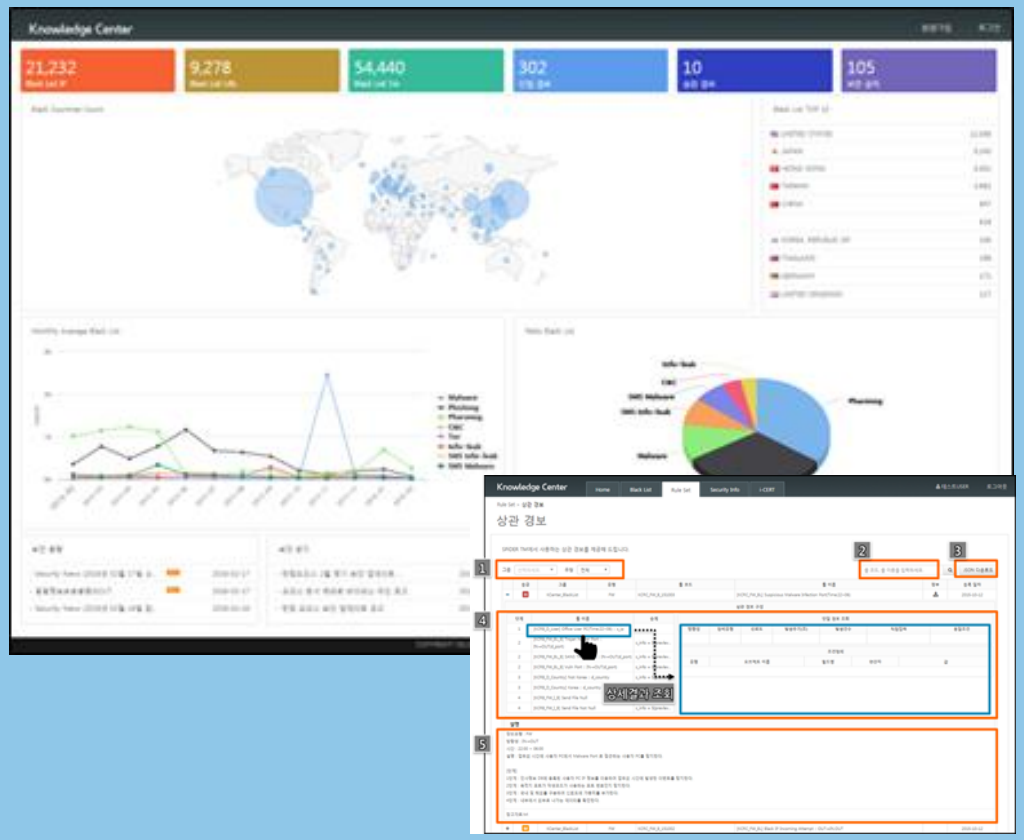
IGLOOSECURITY

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

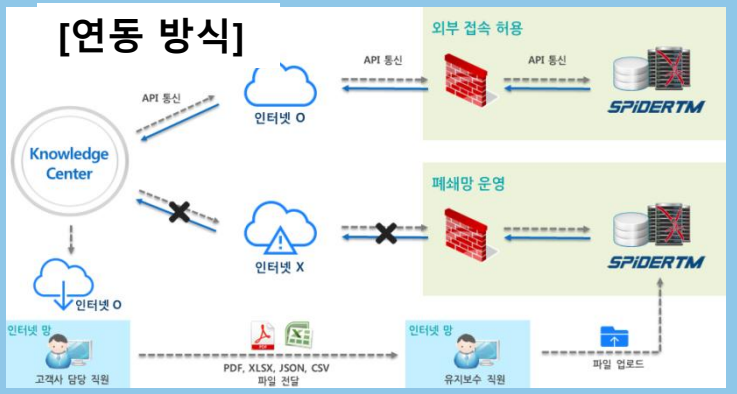


IGLOOSECURITY

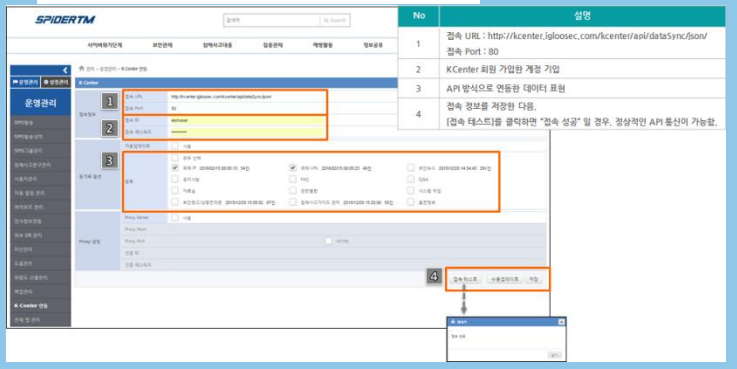
- SPiDER TM 과의 연동(API)을 통한 지속적인 위협에 대한 대응 가능
- 최신의 보안동향 및 기법을 알려줄 뿐 아니라 실제적인 관제 Rule 제공



[연동 방식]

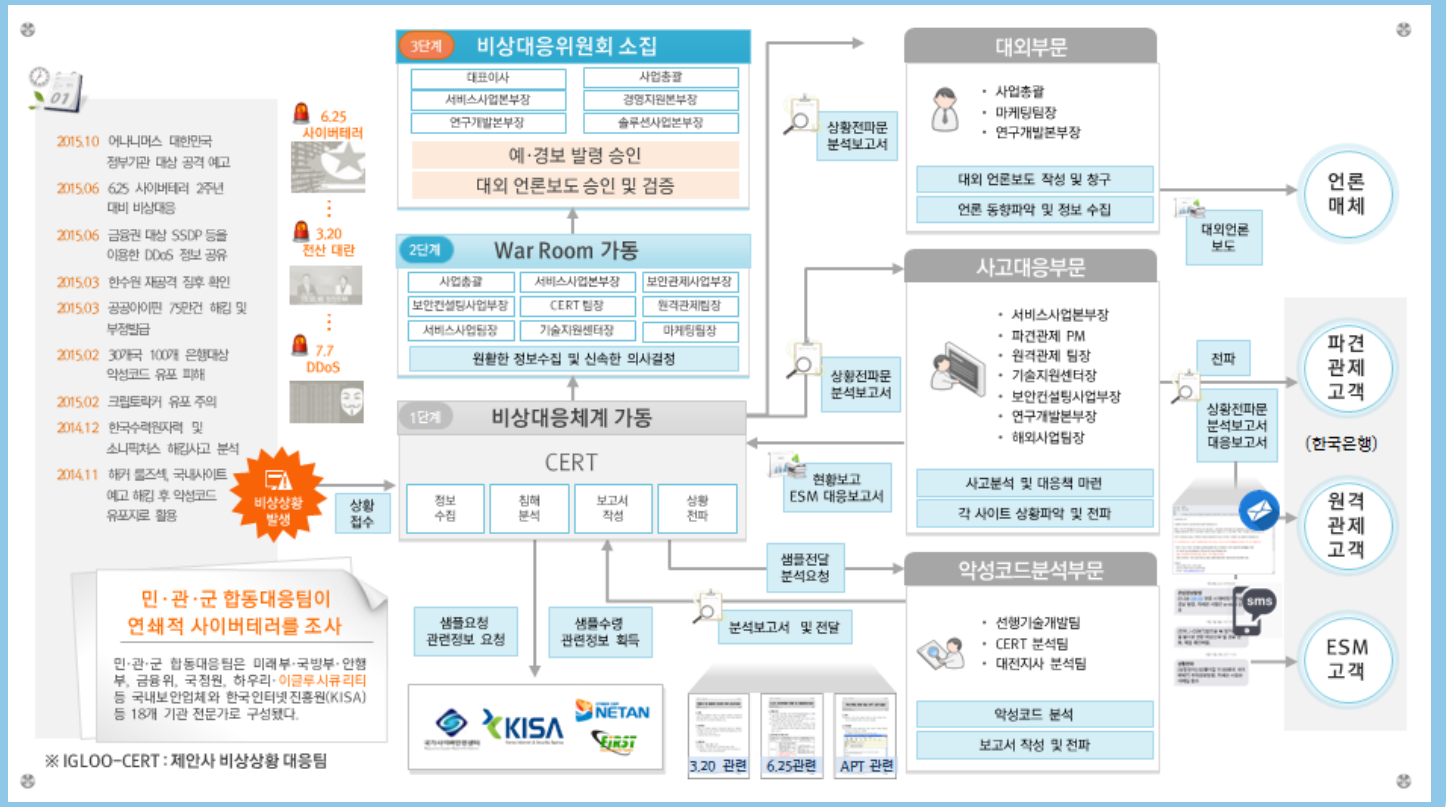


[SPiDER TM 연동화면]



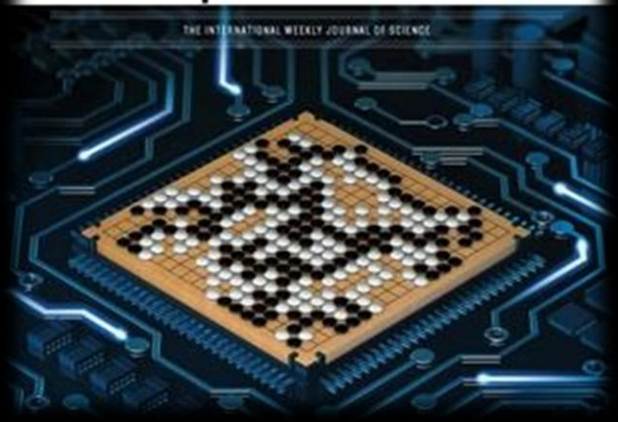
IGLOOSECURITY

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



1 : 4

AlphaGo



감사합니다.

IGLOOSECURITY