OT / ICS 보안 웨비나

BlackBerry Protect with 파고네트웍스 MDR 서비스

(PAGO TIP - Threat Insights Platform)

(주) 파고네트웍스
블랙베리 마스터 총판
MDR (Managed Detection & Response) 서비스 전문 기업

OT / ICS 보안 개요

About OT / ICS Security

OT / ICS 보안의 다양한 영역

Network Visibility

Risk Assessment

Endpoint Protection

IOT Firewall

Vulnerability Assessment

Asset Management

Whitelisting

OT Security Management

OT / ICS Consulting

OTCSA 출범 – 2019년 10월22일

OT CSA

OT Cyber Security Alliance

“

OT / ICS 인프라를
IT 장비로 제어하는 기업 대상
" 보안 가이드라인 / 안전수칙”

Not What-To, But How-To

”

OTCSA 멤버


ABB


BlackBerry
CYLANCE


Check Point
SOFTWARE TECHNOLOGIES LTD


FORESCOUT


FORTINET


Microsoft


MOCANA


nccgroup


Qualys


SCADAfence


splunk>


WÄRTSILÄ


WESCO®

OTCSA – IT vs. OT

특징	IT	OT
보호 대상	정보	물리적 프로세스
위험 영향도	정보 유출, 금융 악화	안전, 건강, 환경, 금융
주요 보안 목표	기밀성	가용성, 무결성
가용성 요구 사항	보편적으로 중간, 딜레이 수용 (산업군에 따라서 "아주 높음")	아주 높음
실시간 처리 요구 사항	딜레이 수용 (산업군에 따라서 "아주 높음")	크리티컬 / 아주 높음
컴포넌트 라이프 사이클	3년 ~ 5년 ~ 7년	15년 ~ 20년 이상
애플리케이션 패치	상시, 스케쥴링	느림, 가끔 (상황에 의해 못함)
보안 테스팅 / 보안 감사	상시, 규제	아주 가끔
현장 보안 교육	높음, 성숙	이제 증가 시작

OTCSA – 증가하는 위협

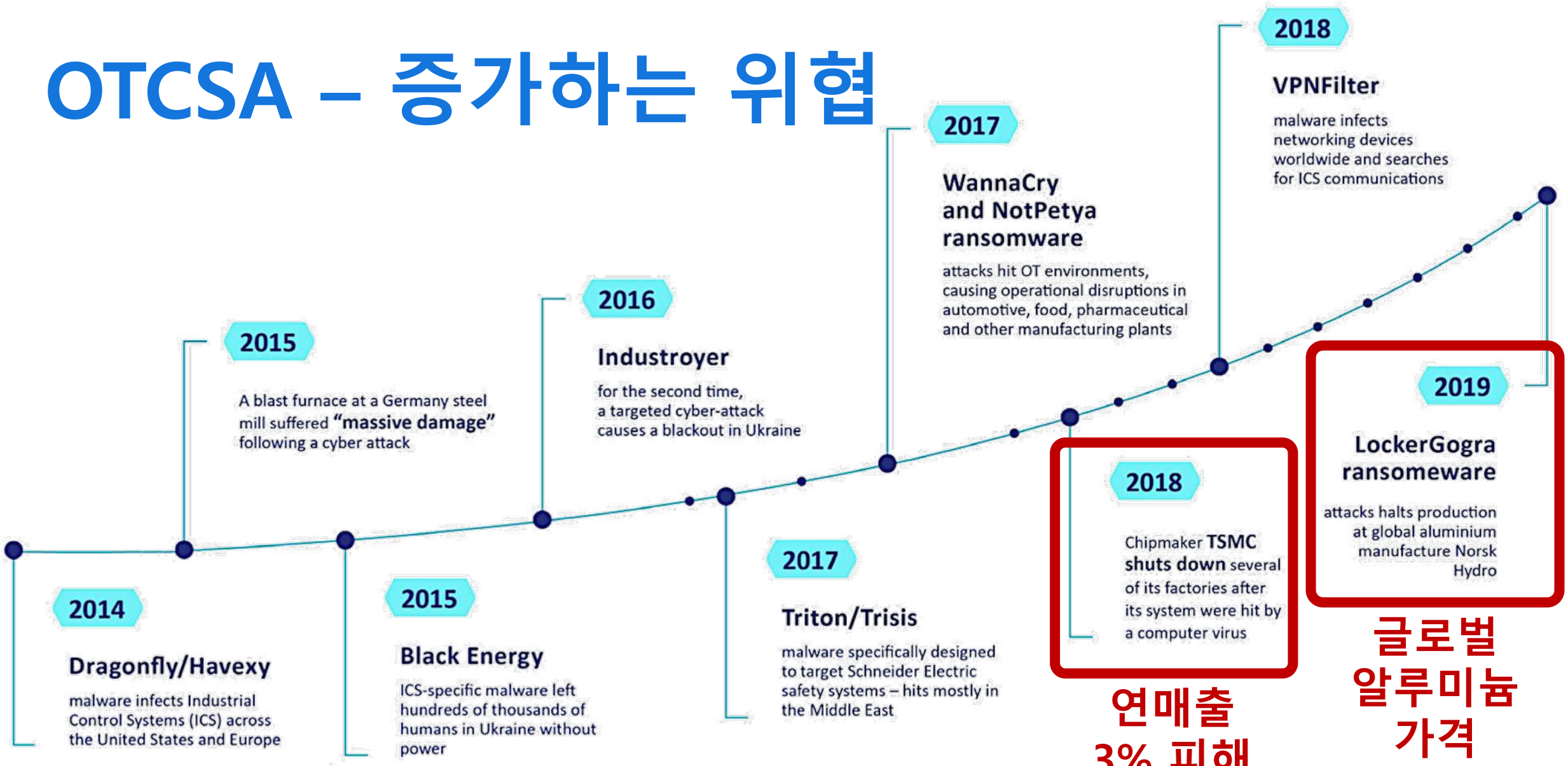
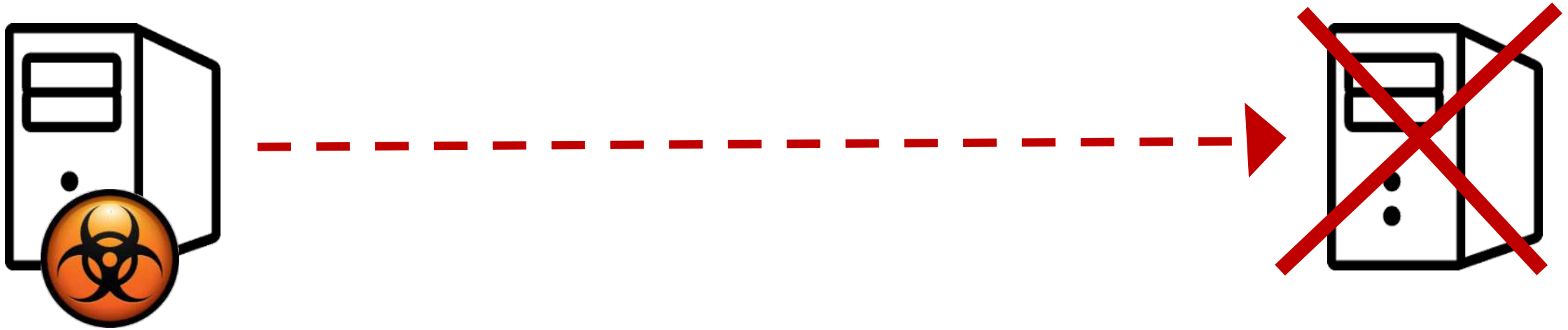


Figure 1. Threats to critical infrastructure and industrial automation are increasing in severity and frequency

TSMC WannaCry 변종 … 2018 한국은 ??

파고네트웍스 BlackBerry Protect 고객 다수 (OT 제조망 환경)



WannaCry
변종
(단, 데이터 암호화 없음)

제조망 동일 네트워크
시스템 다수
크래쉬(Crash) 발생
"모두 SMB 포트 오픈됨"

TSMC WannaCry 변종 … 2018 한국은 ??

파고네트웍스 BlackBerry Protect 고객 다수 (OT 제조망 환경)

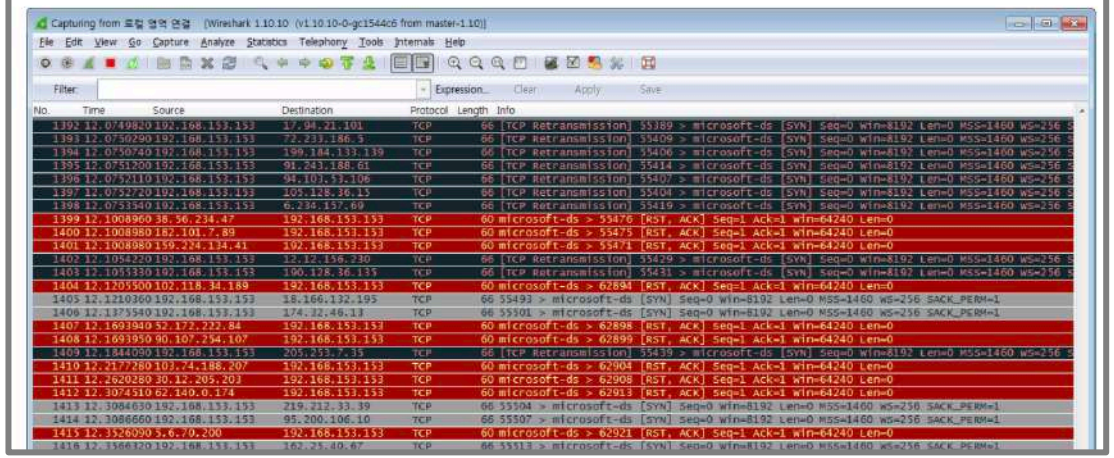
WannaCry 변종 암호화 모듈 손상 (일부러 ???) → DDoS 공격 툴 변화

해당 WannaCry 변종은 암호화 라이브러리 및 수행 코드를 가지고 있는 것으로 확인 되었으나,
암호화를 수행하는 프로세스가 실행되지 않는 것을 확인함.
원인은 PE구조의 Manifest 영역이 손상되었음.

해당 Malware 유입되기 전부터 해당 영역이 손상된 것이기 때문에 손상된 이유에 대해서는 분석할 수 없습니다.

굳이 손상된 이유에 대해서 추측 하자면, 외부적인 환경 요인에 의해서 손상되었거나, **Malware 개발자가 일부러 손상시켜 Eternal Blue SMB 취약점을 통한 DDoS 공격이 목적이 되도록 의도**된 변종일 수 있음.

Microsoft Security Center (2.0) Service 서비스가 시작되면, 무차별적으로 다른 대상으로 SMB 연결을 시도하는 패킷을 확인할 수 있습니다.



WannaCry 변종 (단, 데이터 암호화 없음) → **결과론적으로는 WannaCry 변종 제작후 DDoS 유형의 타겟 공격** → **제조망 동일 네트워크 시스템 다수 크래쉬(Crash) 발생 "모두 SMB 포트 오픈됨"**

OTCSA – Working Groups 레벨

WG	Objective	Focus	Work Products
WG1 Long-term Vision	To define the desired target to ensure safer and more secure OT and cyber-physical operations	• Brown and green fields • Industry and vendor agnostic	• Scope, challenges, and use cases (problem statement) • C-level communication about risk management and maturity • Architecture blueprints and operational and management processes as needed
WG2 Visibility, Intelligence, and Response	To define a comprehensive solution to risk management based on asset inventory and monitoring, situational awareness, and response management	• Brown fields • Industry and vendor agnostic initially, then selected industries and vendors to show feasibility	• Overall architecture • Data model/common API demonstrator • Response playbooks and threat intelligence
WG3 Protection for Inherently Vulnerable Devices	To define mitigating controls for protecting devices that today do not include, or include only limited, security controls	• Brown and green fields • Industry and vendor agnostic initially, then selected industries and vendors to show feasibility	• Inventory of mitigating controls • Risk-analysis-driven, cost-conscious selection process for mitigating controls • Tools to assess the trustworthiness of implemented controls and their resilience against vulnerabilities

OTCSA – Work Product

Domain	Reach	Focus	Guideline objectives
Technology	Includes architectures and design principles	• Industry- and vendor-agnostic WPs • WPs specific to selected industries • Verified instantiations of secure OT systems based on industry- and vendor-agnostic WPs	• Provide a desired/target status as well as guidance on reaching that status in a risk-based fashion and with a step-wise approach • To be based on standard reference architectures, models, and protocols • Provide additional details with respect to other security frameworks (e.g., describing how)
+			
Process	Includes workflow steps as well as roles and responsibilities	• Design, engineer, install, and decommission OT solutions • Deploy, operate, and manage technology, people, and information for better security • Align to IT processes	• Aligned with technology WPs • Leverage existing process frameworks • Follow similar approach to technology WPs for desired vs. transitional state, step-wise approach, generic vs. agnostic, and multiple levels of detail
+			

Compliance	Measure, test, and audit for compliance	• Focus on compliance and conformity assessments of:
		  ○ Specific OT systems and their operations to the technology and process WPs
		  ○ A member's product to the technology and process WPs
			• Enable easy mapping of technology and process WPs to standards and regulations while highlighting gaps

Not just focus on "What to do",

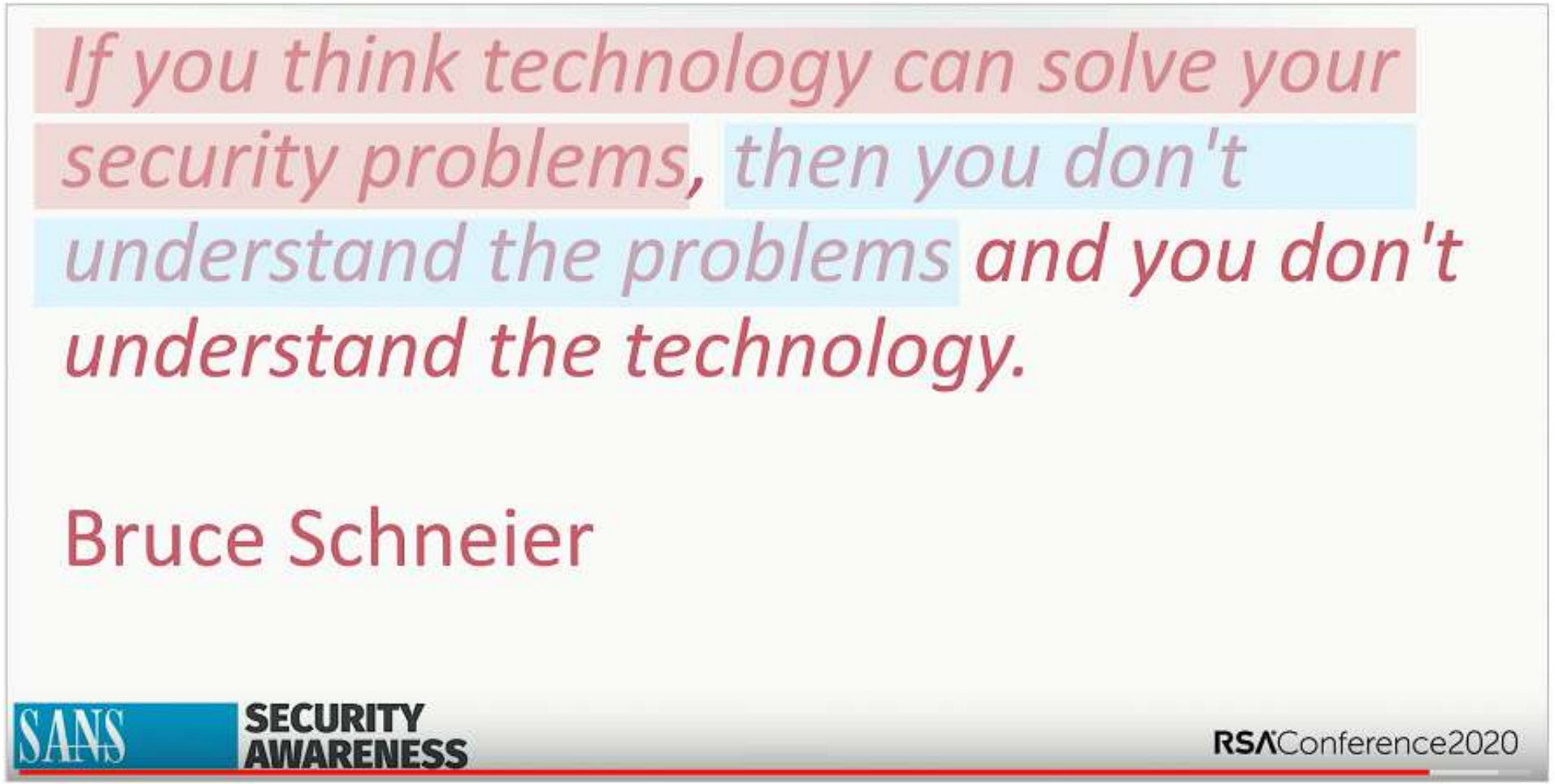
But more on "How to do"

지난 2월

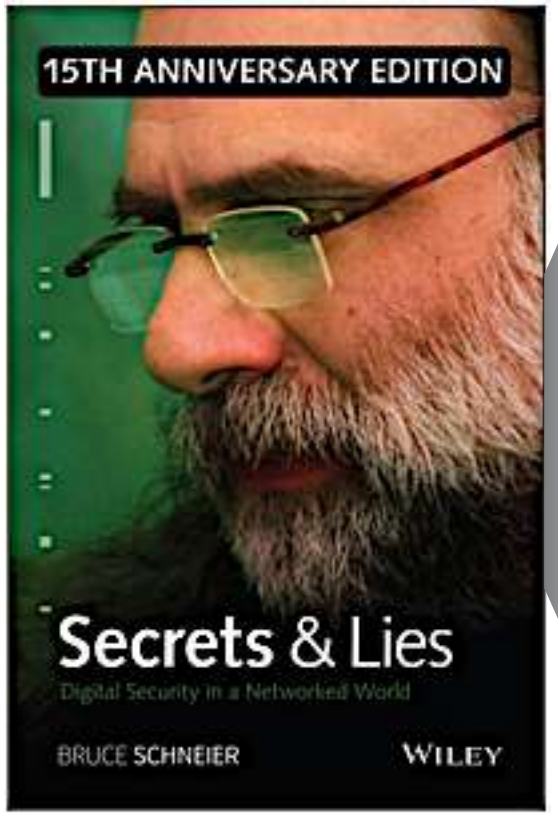
RSA Conferece 2020 으로

잠시 돌아가 보겠습니다.

RSAC 2020 – SANS 의 발표 내용



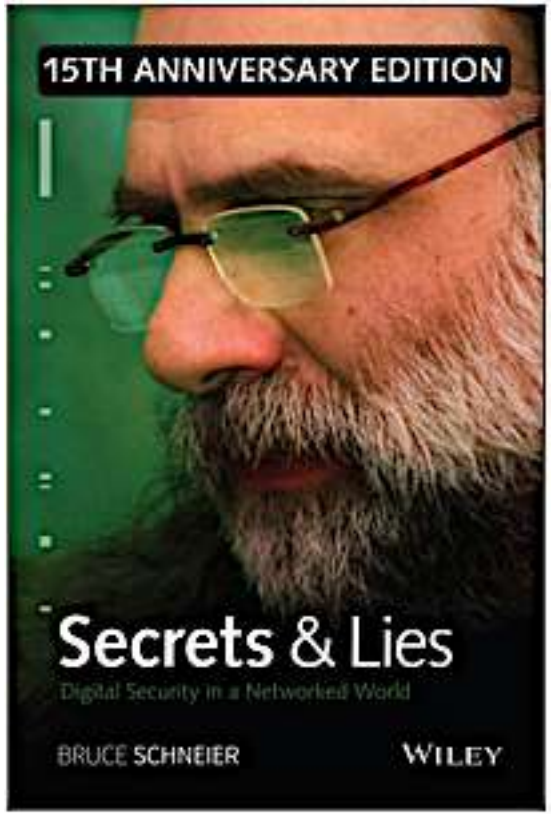
Security is a Process, not a Product



This is obvious to anyone involved in real-world security. In the real world, security involves processes. It involves preventative technologies, but also detection and reaction processes, and an entire forensics system to hunt down and prosecute the guilty. Security is not a product; it itself is a process. And if we're ever going to make our digital systems secure, we're going to have to start building processes.

A few years ago I heard a quotation, and I am going to modify it here: If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

IT, OT/ICS – 보안 공통점



Security is not a product, it itself is a process

OT CSA

Technology

+

Process

+

Compliance

OTCSA – 멤머 유형, 목표 산업군

파고네트웍스
with
블랙베리

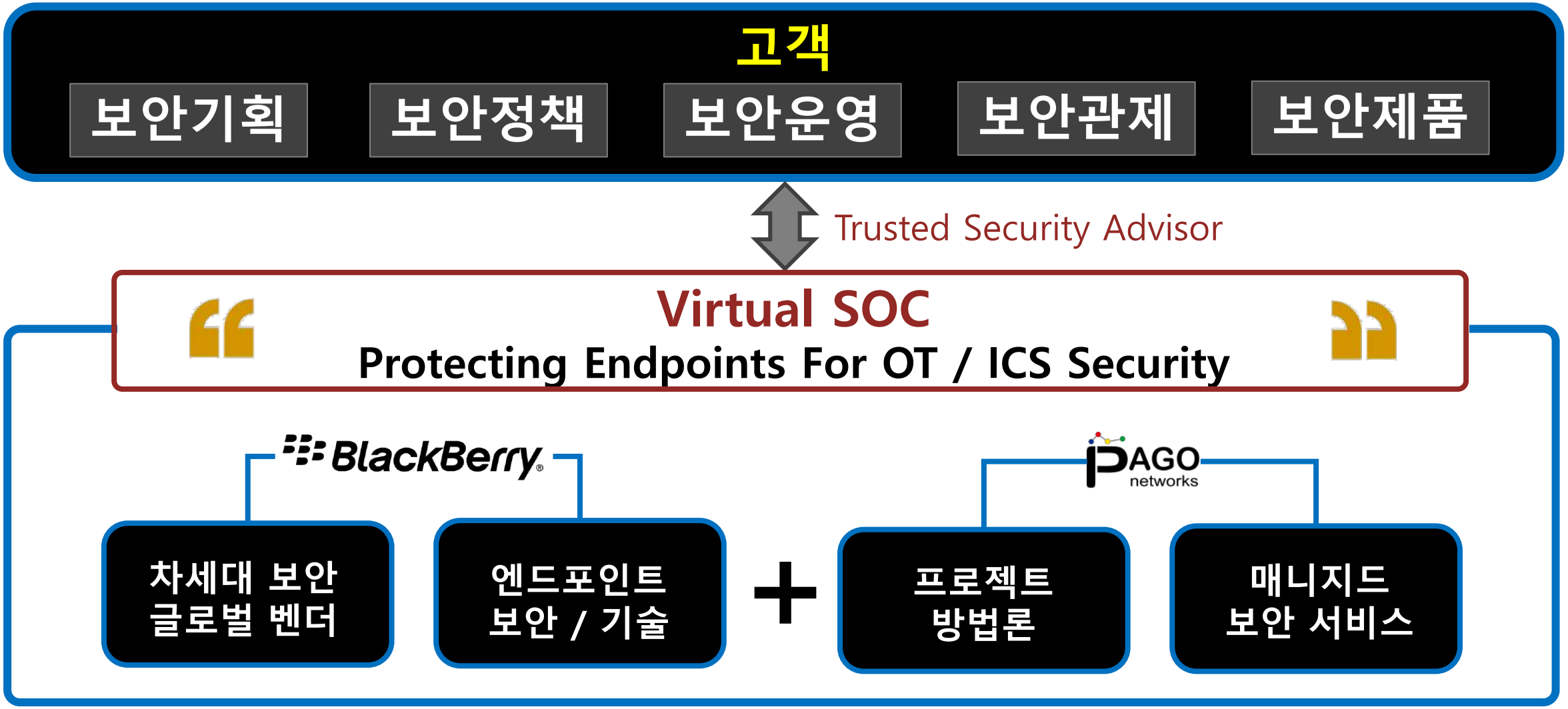
Target member types
OT operators in the target industries
Endpoint protection solution provider
Enterprise software product vendor
Enterprise Resource Planning vendor
Firewall vendor
Identity and Access Management solution provider
Incident Response Management service and solution provider
Security services provider
Consulting services provider
Cloud provider
Industrial Control Systems vendor
Security Information & Event Management solution provider

Target industry representation areas
Automotive & transportation
Buildings & infrastructure
Energy & utilities
Food & beverage
Life sciences
Marine & ports
Metals & mining
Semiconductor
Oil, gas & chemicals
Pulp & paper
Banking
Telecommunications

제품
+
기술
+
프로젝트
방법론
+
프로세스

차세대 엔드포인드 보안 플랫폼
with 매니지드 위협대응 서비스 제안
For OT / ICS Security

파고네트웍스 제안 방향성



Hybrid개요 : 제품 + 서비스

BlackBerry

BlackBerry Protect

AI endpoint protection.

BlackBerry Optics

Detection and response solution.

Threats

- Detected
- Notified
- Alerted
- Killed
- Quarantined

- **Prevention First**
- **Detection & Response**
- **More Higher Protection**

PAGO networks "MDR Service"

Threat Research

For All Threats ...

- Analysis
- Investigation
- Response
- Remedition
- Extracting IOC
- Communication

- **100% threats**
- **100% validation**
- **Lower False-Positive**

Threat-Insights-Platform

Provide ...

- Details Inofrmation
- 고객을 위협한 실제 위협 정보 요약
- Threat Category
- IOC
- Summary Reports
- Guideline

- **More threat insights**
- **Threat Insights DB**
- **IOC, Knowledge 공유**
- **위협공유 커뮤니티**

IOC 연동 w/ 보안 제품

- 방화벽
- 이메일 보안
- 자산관리 솔루션
- 네트워크접근제어
- 인사DB
- AD

For all Threats

- Details Inofrmation
- Threat Category
- IOC
- Summary
- Guideline
- Reports

- **Unmanaged Devices**
- **Invisible Devices**

IOC Feed

- For Non-BlackBerry Protect 고객

TIDB Feed Service

- Threat Insights DB
- IOC DB
- Threat Reports

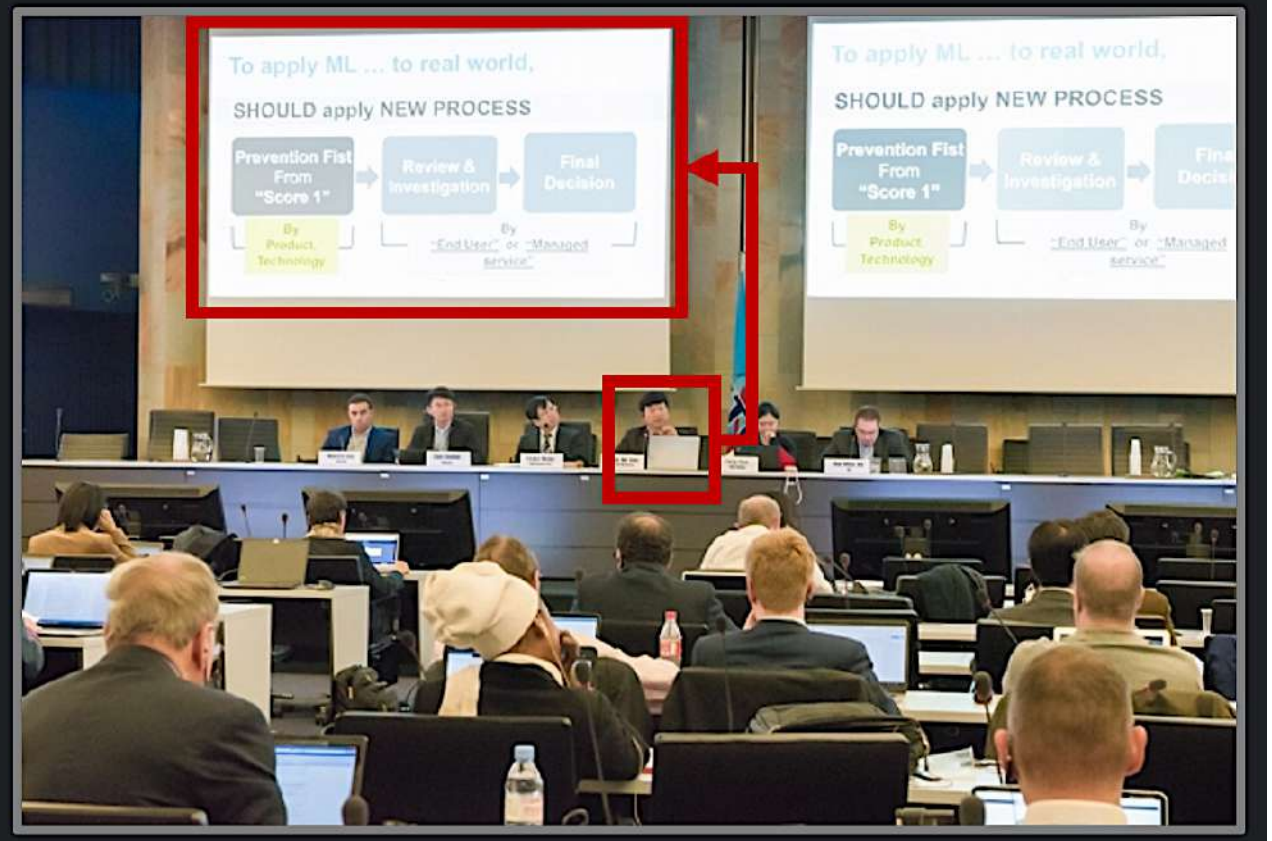
- **Cyber Security Echo-System**

파고네트웍스 활동 – AI + 엔드포인트 보안

ITU 워크샵 (제네바 / 스위스, 2019년 2월)

- AI / 머신러닝을.. 실제 보안 환경에 적용하려면 ?

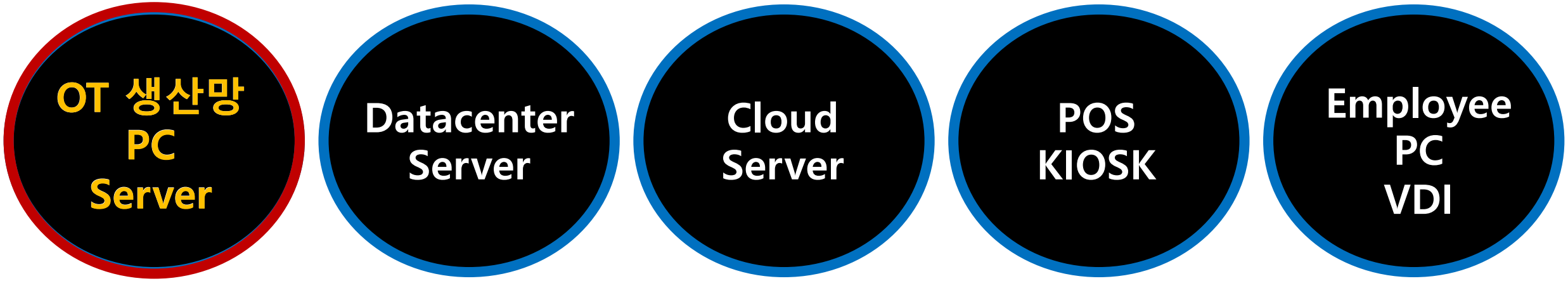
- **완전히 새로운 보안 프로세스방법론** 적용 필요 !!!



제품/기술 - BlackBerry Protect

AI 기반 차세대 엔드포인트 보안 플랫폼

(기존 엔드포인트 AV / APT 대체)



블랙베리 적용 대상 for OT / ICS

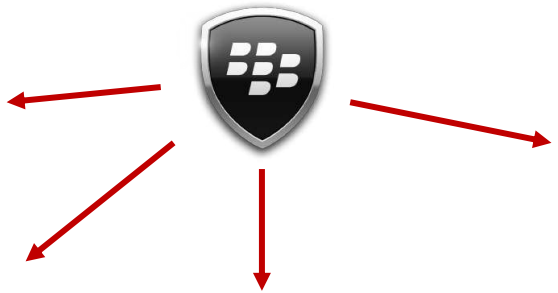
무인택배 시스템

공공장소 광고 판넬

산업제어/생산 시스템(PC/서버)

블랙베리 적용 대상 for OT / ICS

블랙베리 적용 대상 for OT / ICS



블랙베리 지원 OS

에이전트 공식 지원 운영체제

Microsoft

Windows XP SP3
Windows Vista
Windows 7 (Embeded 포함)
Windows 8 / 8.1
Windows 10
Windows Server 2003 SP2
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows 2016 Standard, Datacenter, Essential
Windows 2019
(*Windows XP, 2003 공식지원)

MacOS

OS X 10.9 (Mavericks)
OS X 10.10 (Yosemite)
OS X 10.11 (El Capitan)
OS X 10.12 (Sierra)
OS X 10.13 (High Sierra)
OS X 10.14 (Mojave)
OS X 10.15 (Catalina)

redhat

RedHat Enterprise 6.6 ~ 7.6
CentOS 6.6 ~ 7.6
Ubuntu 14.04 ~ 18.04
SUSE 12, SP1, SP2, SP3

---

amazon web services Linux

Amazon Linux AMI 2017.9
Amazon Linux AMI 2018.3
Amazon Linux 2 2017.12

블랙베리 에이전트 스펙 for OT / ICS

- 보안 에이전트 / 콘솔 – 멀티 랭귀지 지원
- 보안 에이전트 지원 OS – "XP, 2003" 필수 지원 (아직 EOS OS system 많음)
- 특수 환경을 제외하고, 보안 에이전트 설치 시, 시스템 리부팅 하면 안됨
- 보안 에이전트 운영 단계에서, 기능 업데이트 등이 발생 시, 시스템 리부팅 하면 안됨
- 보안 에이전트의 시스템 충돌성 최소화 부문 증명 필요 (모든 충돌 사례를 사전에 오픈해야 함)
- 보안 에이전트의 시스템 리소스 사용 최소화 부문 증명 필요 (Memory / CPU)
- 보안 에이전트 수량에 따른 "네트워크 대역폭 사용량" 증명 (해외 공장의 대역폭 고려 위해)
- 보안 에이전트 수량에 따른 "세션수의 구체적인 수치" 증명 (낮은 스펙의 NW/방화벽 고려 위해)
- 제안사 / 제조사의 기술 지원 역량과 범위 확인 (OT 환경의 중요성 때문)
- 보안 에이전트의 다양한 배포 방안 제시 확인 (32/64bit 자동확인, 필요 모듈 존재여부 자동체크)
- Known / Unknown 멀웨어 상관 없이, 높은 탐지 및 방어율 증명
- 보안 에이전트에 의해 방어된 멀웨어의 "정확한 유형, 작동방식, IOC추출, 영향도" 정보 제공
- 이미 방어된 멀웨어에서 추출된 IOC 를 고객사의 기존 보안제품에서 사용하도록 대응 방안 제공
- 보안 에이전트가 설치되지 않은, OT 엔드포인트에 멀웨어 감염시, 영향도 최소화 방안

EPP – BlackBerry Protect 개요

Artificial Intelligence Real Threat Prevention

Prevent-First / Protect-First

인공지능 머신러닝 기반 - 차세대 엔드포인트 프로텍션 플랫폼

Known 악성코드 탐지 / 실행 차단	**No** 시그니처 (업데이트)
Un-Known 악성코드 탐지 / 실행 차단	**No** 휴리스틱
메모리 공격 차단	**No** 샌드박스
스크립트 공격 차단	**No** 행위기반
애플리케이션 LockDown	**No** 주기스캔

Vs.

BlackBerry Protect

인공지능 / 머신러닝 에이전트

- 실효성 증명
- 엔진 가벼움
- PC / Server 성능에 영향 없음
- Known / Unknwon 멀웨어에 대한 탐지, 차단 기술 증명
- SW 충돌 사례 보고되지 않음
- 한국 고객 증명 완료

기존, 신종, 변종

상관없이

실시간

사전 차단

기술 증명 완료

- **기존 AV기반, 멀티 레이어 엔드포인트 보안**
- **기존 APT 샌드박스 보안**

- 실효성많이 떨어짐
- 엔진 무거워짐
- 스캐닝 수행 시, 성능 이슈
- Known / Unknown 모두 놓치는사례 상당수 발견

AI 기반 – Unknown 랜섬웨어 방어 (2020)

Hash	분석 내용	Score	탐지/격리 일시
6AF129876F78A6CADF5B53E5F1236B3E86BBEC8258D97014882D54857DB53640	멀웨어 - 랜섬웨어 (Sodinokibi / 파일 암호화 및 암호화폐 요구 / VT-Unknown)	98	2020-04-07 15:37:00
8C24D9D97FB5B4949D1EAF74F731DC25833F0CECE4BA616250CC270BD260FD0C	멀웨어 - 랜섬웨어 (Blackout / 파일 암호화 및 암호화폐 요구 / VT-Unknown)	70	2020-04-07 15:36:37
292BF92948A288E21727A1995A0BD004474832BD5854087FD2E7560D792D5460	멀웨어 - 랜섬웨어 (Crypt0L0cker / 파일 암호화 및 암호화폐 요구 / VT-Unknown)	89	2020-04-07 15:36:16
2B817CCB7589646DD588B6740D1F58973E31AF1873CF3691FDEDE4ACF67595C6	멀웨어 - 랜섬웨어 (Jest / 파일 암호화 및 암호화폐 요구 / VT-Unknown)	98	2020-04-07 15:35:35
AB3A2E24FA7C2186525BF8EB70C06B10A54905E551347B890C4ADDE2FC46E460	멀웨어 - 랜섬웨어 (Ryuk 랜섬웨어 / 숨김형태로 자가복제 / 볼륨섀도카피 삭제 / VT-Unknown)	94	2020-03-19 09:52:46
C0FC409F7695F15E358C20941BBDA7B318767791DA1CB2F54B5530930AE354C9	멀웨어 - 랜섬웨어 (Makop / 이메일 통해 유포 / 확장명 makop 변경 / VT-Unknown)	94	2020-03-17 17:16:08

- 현재 BlackBerry Protect는 **2019년도 AI 수학모델 적용 및 운영중**
- BlackBerry Protect로 탐지/격리된 실제 내역이며, 해당 일시 기준 바이러스 토탈에 등록된 모든 보안솔루션에서 Un-Known 확인

AI 기반 – Unknown 멀웨어 방어 (2020)

Hash	분석 요약	Score	탐지/격리 일시
730BD3C283C2895FC0FBF0D80035B3F6162561BA26A5837D8CE9AC1D575D313E	멀웨어 - 트로얀 (APT6 해커그룹의 정보유출성 멀웨어 특성(enigma)을 지닌 임시파일 / VT-Unknown)	60	2020-05-20 20:24:18
5CBD1C9E60D2C72153AAB0CC8EB0F7797006C183ADA576EA6087E33072F3E0D2	멀웨어 - 바이러스 (Sality 계열 / 서비스 등록 / 프로세스 인젝션 / VT-Unknown)	98	2020-05-20 15:52:36
13104640F0398248DFACD2FFFB667C0BF2F3B51770FAE3E6855F0C829608D586	멀웨어 - 트로얀 (시스템 OS정보 수집 / Autoit 제작 / pdf 위장 / VT-Unknown)	93	2020-05-20 11:11:35
D8C3A3CD16C65FCF3F7497F0103CAC67C20D4F65C4E21A778353C65344559F7A	멀웨어 - 트로얀 (APT6 해커그룹의 정보유출성 멀웨어 특성(enigma)을 지닌 임시파일 / VT-Unknown)	59	2020-05-19 20:20:14
D0B6E78EF22833617DC905750DC3536E15B86F3A03932C5AE9519F72606D205B	멀웨어 - 트로얀 (APT6 해커그룹의 정보유출성 멀웨어 특성(enigma)을 지닌 임시파일 / VT-Unknown)	77	2020-05-19 20:20:14
CDECC422BB677EE909F1989B1DBF4D0428B53098AD9601CCA72724F7A3C9845E	멀웨어 - 트로얀 (APT6 해커그룹의 정보유출성 멀웨어 특성(enigma)을 지닌 임시파일 / VT-Unknown)	60	2020-05-19 20:20:14
6129EE7DAA04B4C67E0B9C6607A55B48D75F04A33B4483DCEE81E57227BF0265	멀웨어 - 트로얀 (APT6 해커그룹의 정보유출성 멀웨어 특성(enigma)을 지닌 임시파일 / VT-Unknown)	59	2020-05-19 20:20:14
1898481E21B1FBF9B1666BE254C7245C97E1B8B548F3964466C3FA8D3C3E1952	멀웨어 - 트로얀 (APT6 해커그룹의 정보유출성 멀웨어 특성(enigma)을 지닌 임시파일 / VT-Unknown)	66	2020-05-19 20:20:14
6E37AE565CA9D0840B63C83FE1B7F0EA5507E47E072DBA63070D7142EE5F312A	멀웨어 - 트로얀 (APT6 해커그룹의 정보유출성 멀웨어 특성(enigma)을 지닌 임시파일 / VT-Unknown)	86	2020-05-19 20:20:14
ED97DB9B36417293A4AF468B4390F60FD58FE4B683454AA7B56476CC3A75B7D8	멀웨어 - 크립토마이너 (XMR모네로마이너 v5.6 / 128.199.183.160 통신 / VT-Unknown)	89	2020-05-18 20:33:16
F64504FDD5E035058494DCFB487F25D02F7EF6660A74D7862D3C7A25380F03E0	멀웨어 - 크립토마이너 (XMR모네로마이너 v5.6 / 128.199.183.160 통신 / VT-Unknown)	89	2020-05-18 20:32:05
005F9471FEEB0047D099B569C4C73B448218A8B2E24B4BFFCC1E91B324ADC61E	멀웨어 - 트로얀 (시스템 정보 수집 / MSBuild 인젝션 / VT-Unknown)	92	2020-05-15 10:09:53
5086FC76C032EE380731BF90731B71E9D354AF4DE26ACE719B26122EA47F1BE7	멀웨어 - 다운로더 (트로얀 성향/googledrive를 이용한 암호화된 악성파일 다운 시도 / VT-Unknown)	100	2020-05-14 11:18:05
D4E2036C4FA81147BFB84A685460739DD43C4A9B58051BA9053DB3E4C09395D2	멀웨어 - 트로얀 (Lokibot / 45.143.138.72통신 / 악성파일 다운 시도 / VT-Unknown)	93	2020-05-14 10:04:03
F886C8AD7F06A34874BD0C3B818FD0EBC254A6B4C8125C006EC8DF9632DB8E31	멀웨어 - 크립토마이너 (트로얀 성향/ 윈도우 test.dll로 위장 / 모네로(XMR) 마이너/VT-Unknown)	16	2020-05-14 05:53:29
812A891639798AD6B73E72742B18C8F535CC17717D5DED5EFC23B050506DA580	멀웨어 - 크립토마이너 (XMR모네로 마이너 실행파일 / 128.199.183.160 통신 / VT-Unknown)	89	2020-05-13 10:57:26

- 현재 BlackBerry Protect는 **2019년도 AI 수학모델 적용 및 운영중**
- BlackBerry Protect로 탐지/격리된 실제 내역이며, 해당 일시 기준 바이러스 토탈에 등록된 모든 보안솔루션에서 Un-Known 확인

일반적인 Application White Listing 비교

레거시 애플리케이션 화이트 리스트 솔루션

- 고객이 직접 "화이트리스트"에 포함할 애플리케이션 선별
- 필수 SW가 " 이미 감염된 상태"에서도, 화이트리스트에 추가

생각보다 많은

"File Share / SMB프로토콜, USB사용"

- 새로운 파일 설치 또는 업데이트 시, 일시적으로 **"시스템 unlock"**
- 그리고, 때로는 **"시스템 unlock 상태" 계속 유지**

- 이미 많은 파일이 감염된 상태에서, "시스템 Locknig Mode" 돌입

BlackBerry Protect

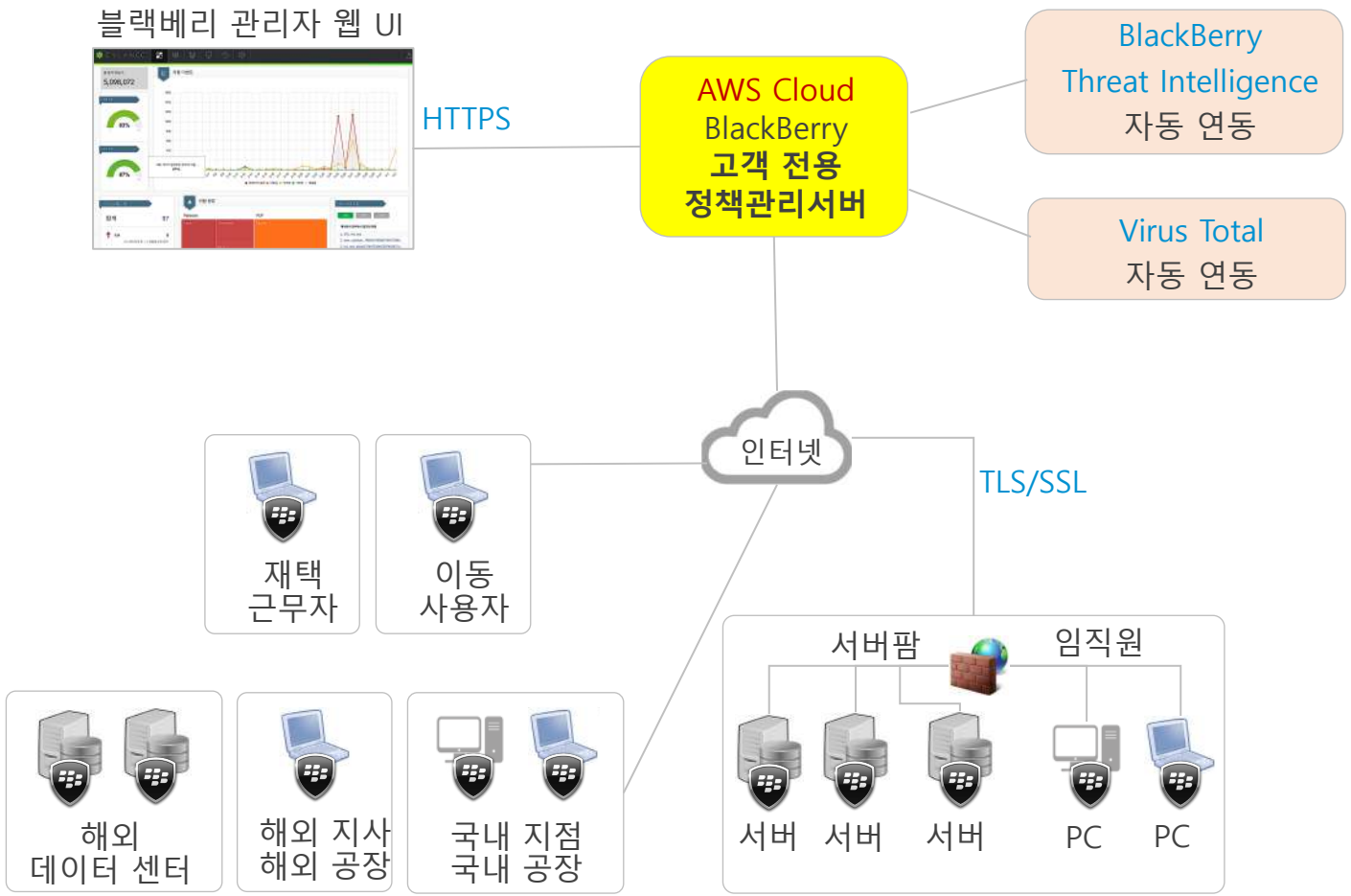
왜 "사일런스" OT 보안에 두각을 보이나?

- ✓ **특화된 OT보안 프로젝트 방법론과 프로세스 제공**
- ✓ 낮은 리소스 사용
- ✓ 경량 에이전트
- ✓ 기존 SW와 시스템 충돌 최소화 (현재 생산망 0%)
- ✓ 높은 OT 시스템 가용성 보장
- ✓ 높은 보안성 제공 (Known / Unknown 멀웨어 대상)
- ✓ No 시그니쳐 업데이트, No 정기적 풀-스캐닝
- ✓ **Managed Detection & Response 서비스 제공**

도입 또는 타 AV 대체 효과

- ✓ **OT 엔드포인트 시스템의 "보안 강화"**
- ✓ 안정성 / 가용성을 동시에 유지
- ✓ 보안 에이전트 관리 방식의 쉬움
- ✓ **Virtual SOC** 제공

블랙베리 아키텍쳐

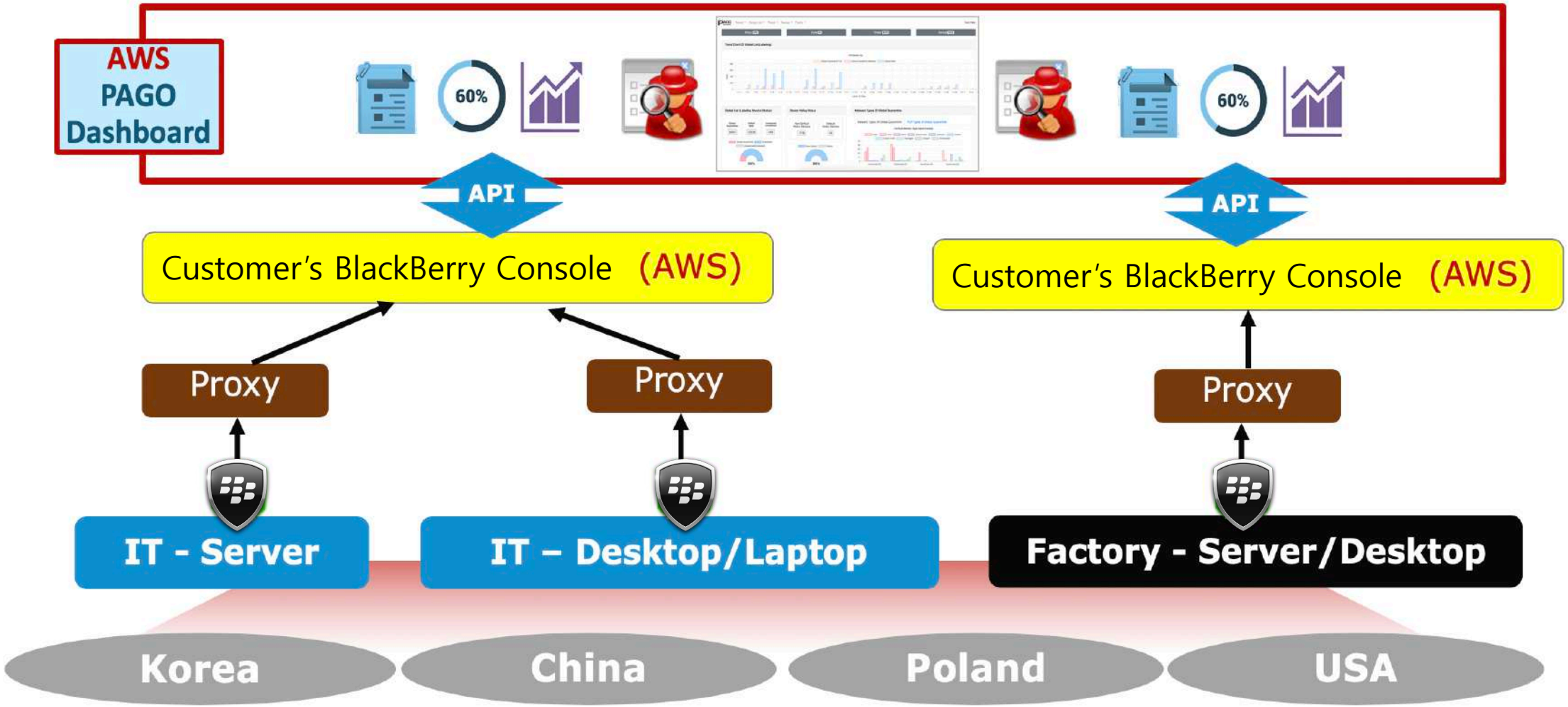


- **BlackBerry Protect 정책 관리 서버 (AWS 클라우드에 위치)**
  - AWS 구성, 확장, 이중화, 자동 Replication 지원
  - 별도 비용 부담 없음
    (최초 도입 이후, 에이전트가 늘어나도 비용부담 없음)
  - **BlackBerry에서 100% 비용 지원**

- **BlackBerry Protect 에이전트**
  - 공식 지원 OS에, 에이전트 설치
  - 경량 / 성능이슈 최소화 / 구역기반 관리
  - 정책관리 서버와 TLS/SSL 암호화 통신

- **Proxy 서버 구성 가능 (옵션)**
  - 고객 환경에 따라,
    BlackBerry Protect 에이전트는 고객사의 Proxy 서버를 통해서, AWS 정책관리서버와 통신하도록 구성 지원
  - Proxy 설정은 에이전트에서 구성됨
    (OS 또는 웹브라우저 구성이 아님)

블랙베리 구성 사례


AWS
PAGO
Dashboard
60%
60%
API
API
Customer's BlackBerry Console (AWS)
Customer's BlackBerry Console (AWS)
Proxy
Proxy
Proxy
IT - Server
IT – Desktop/Laptop
Factory - Server/Desktop
Korea
China
Poland
USA

일반적인 엔드포인트 보안 고도화 개요

EPP

훨씬 더 높은 Protection 기술 고도화

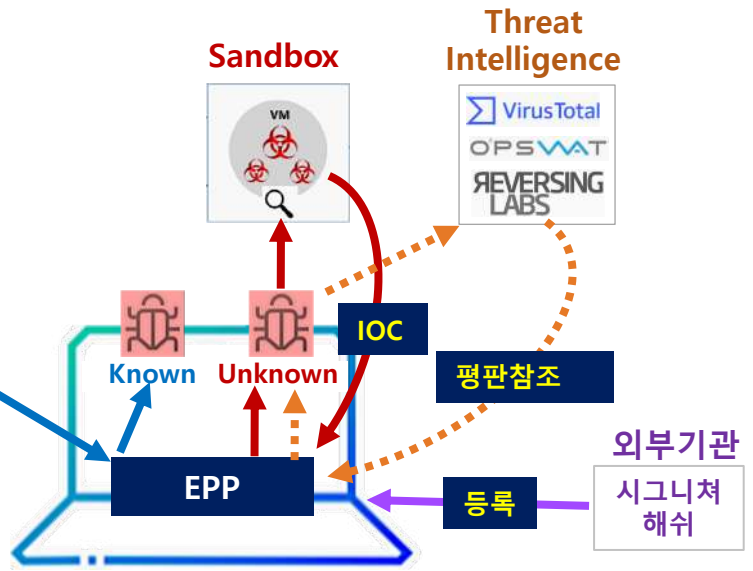
- Multi-Layered 기술
- 일부 선택 기술
- 외부 전문기관 협력
- 머신러닝 단독 기술

- 시그니쳐
- 휴리스틱
- URL 블랙리스트
- 호스트 IPS
- 안티익스플로잇

Known Malware

- 호스트 행위기반
- 네트워크 샌드박스 전송 IOC 생성
- 외부 IOC 연동
- 평판조회
- 주기적인 스캐닝
- 머신러닝

Un-known Malware



일반적인 EPP 고도화 목적

- EPP 설치된 시스템의, 자체보호
- EPP 설치된 다른 시스템에, IOC 공유

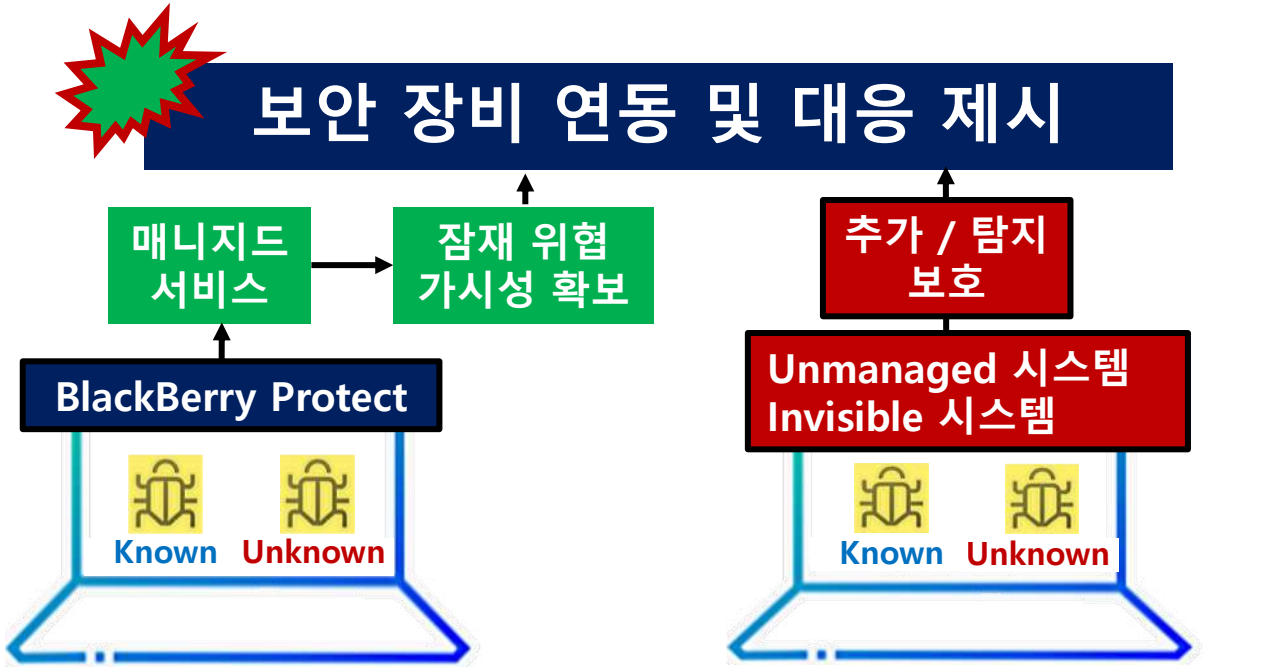
OT / ICS 제조망
EPP 미설치 시스템
엔드포인트 고도화 사각지대 존재

Unmanaged, Invisible 시스템

파고네트웍스 서비스 제안 방향성

- **고객사에서 실제로 차단된 모든 멀웨어 추가정보 추출**
  - 구체적인 멀웨어 종류 / 목적 파악
  - IOC 추출
    - IP, URL, C2
    - 프로세스
    - 스크립트
    - 레지스트리
    - 특정 파일
    - 파워쉘

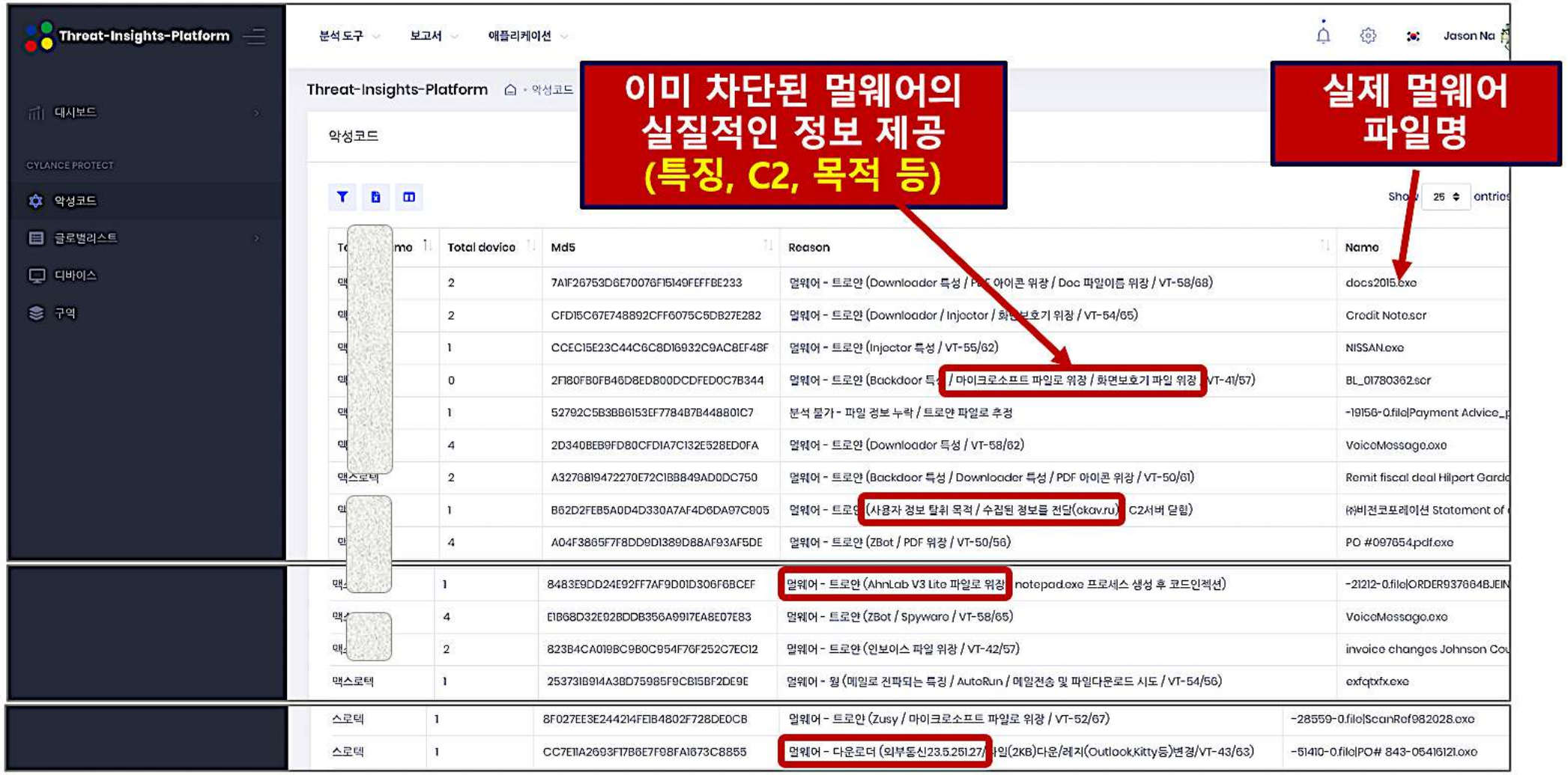
- **고객사 보안솔루션과 실질적인 위협정보 연동/대응 제시**
  - Firewall
  - NAC
  - 자산관리 솔루션
  - 패치관리 솔루션



EPP + 매니지드 서비스 목적

- 성공적으로 차단된 멀웨어의, 구체적인 정보 추출
- 공격 시도한(차단된) 위협의 구체적인 가시성 제공
- EPP 미설치된, 시스템 보호를 위한 대응방안 제시
- 실질적인 IOC 창출 및 공유 체계 완성

이미 방어 완료된 멀웨어 – 추가 인사이츠 추출



파고네트웍스 위협 대응 서비스

- **이미 고객사에서 방어된 멀웨어 고객사 추가 대응 관점에서 접근**
- 분석된 침해지표(IOC) 제공
- 기존 보안솔루션 – 정책 적용
- **Unmanaged / Invisible 디바이스 멀웨어 침해 조기 탐지 방어 프로세스**

PAGO TIP (Threat Insights Platform) – 위협 대응 서비스

- 멀웨어에서 추출된 침해지표(IOC) 및 고객사 보안솔루션 대응 권고 방안

시스템	종류	침해지표	대응 방법
방화벽	URI	xmr.crypto-pool.fr	- 아웃바운드 차단
	IP:Port	IP : 163.172.226.137 163.172.226.114 163.172.207.69. 195.154.62.247 163.172.203.178 163.172.206.67	
		Port : 7777,80	
Anti Virus	HASH	C697792BDA83E572120047CC8A5F3A8411C645539F0C831D169D0A1FFDEB17FC 47BFB9EB0005C86AE1D7F2F65271DEEDD30BF47840E557288917BD1F39A9CD4D FBBEAA0FE0F204D4908CC288BCE6F0B7EEACAAF6419F50F41F3FD28962B33984 260E8A8F2104702D3ED2BC0043DDCE85CDE1B6D56CB77DCF50A5F0215D7CEE2B	- 시그니처 업데이트
자산관리 솔루션	레지스트리	키 : 해당 사항 없음	해당 사항 없음.
		데이터 : 해당 사항 없음	
	파일	C:₩Windows₩fonts₩process.exe C:₩Windows₩fonts₩Notepad.exe C:₩Windows₩temp₩spoolsv.exe C:₩Windows₩syswow64₩xensvc.dll	- 파일 삭제
	서비스	서비스 명 : Host for Windows Services 실행 파일 경로 : [Notepad.exe 파일의 경로]	- 서비스 중지 - 시작 유형 '사용 안함' 변경

※ 자산관리 솔루션을 사용하시는 경우 침해지표(레지스트리, 파일, 서비스)로 Group 을 설정해서 감염 의심 디바이스 리스트를 확인할 수 있습니다.

실제 발송되는 보고서 샘플

Emergency-Threat Information Service

Upatre

문서번호

Ver. 1.4

PAGO NETWORKS

1.4.1 사용자 관점 대응방안

대응 항목	대응방법의 근거	대응 방법
메일 수신	Upatre 는 스팸메일을 통해 들어오며 다른 악성 Botnet 을 다운로드 및 실행한다.	불분명한 발신자의 메일 첨부 문서 열람 자제
파일 및 폴더 정리	악성 파일은 사용자가 확인하기 어려운 폴더에 잠입하여 실행된다.	AppData 폴더 정리

1.4.2 시스템 대응방안

시스템	종류	침해지표	대응 방법
Anti Virus	HASH	47f217c552240a72780ec3595ab7fa801288895b9168b9b6c2410559709be7b1 | b543e040616f55b49da2f274fa053f5c059195f16bf27bbd92995d625a77e5b2	시그니처 업데이트
방화벽	IP:Port	94.23.247.202:80 | 213.239.209.50:80 | 216.22.25.145:80	아웃바운드 차단
	URL	Borbonchia.ge | barkunlimited.com	
자산관리 솔루션	파일	C:₩Users₩[사용자]₩AppData₩Local₩Temp₩iooooj.exe	파일 삭제

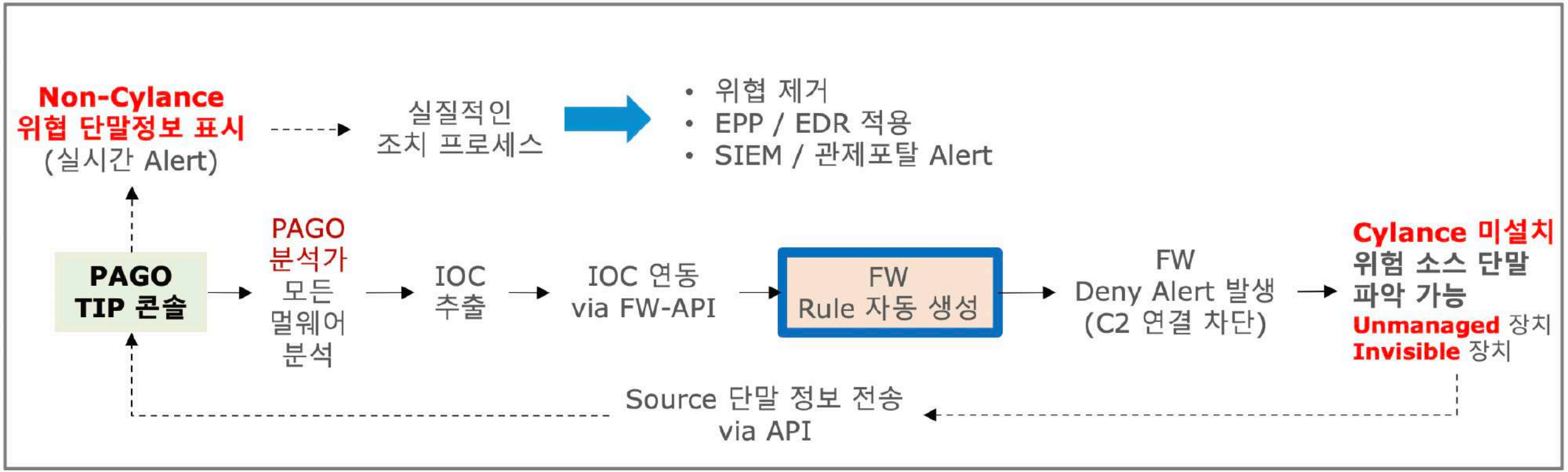
파고네트웍스 위협 인사이츠 DB (TIDB)

PAGO TIP Console – TIDB that are added by TIP Analyst

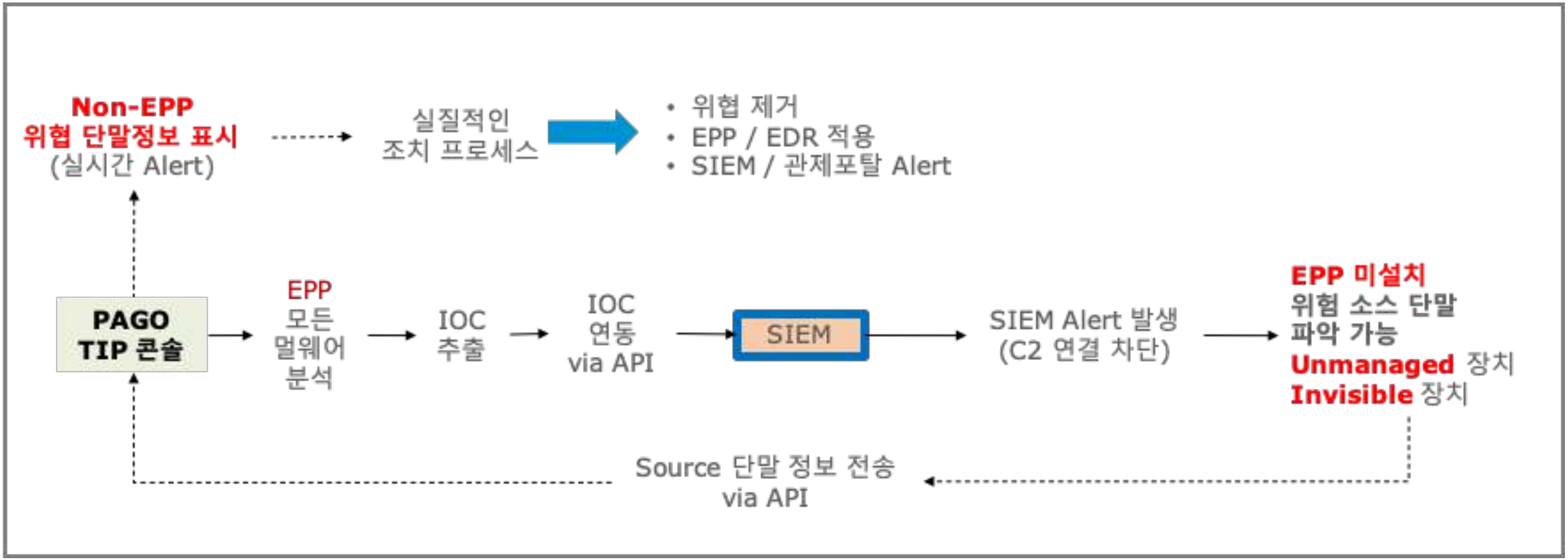
TIDB
(Threat Insights DB)

- Malware – Hash / Category / Comment in details
- C&C – IP
- C&C – URL
- Service Name (멀웨어가 추가한)
- Service Path (멀웨어가 추가한)
- Registry Key (멀웨어가 추가한)
- Scheduler (멀웨어가 추가한)

파고네트웍스 위협 인사이츠 DB (TIDB) 연계

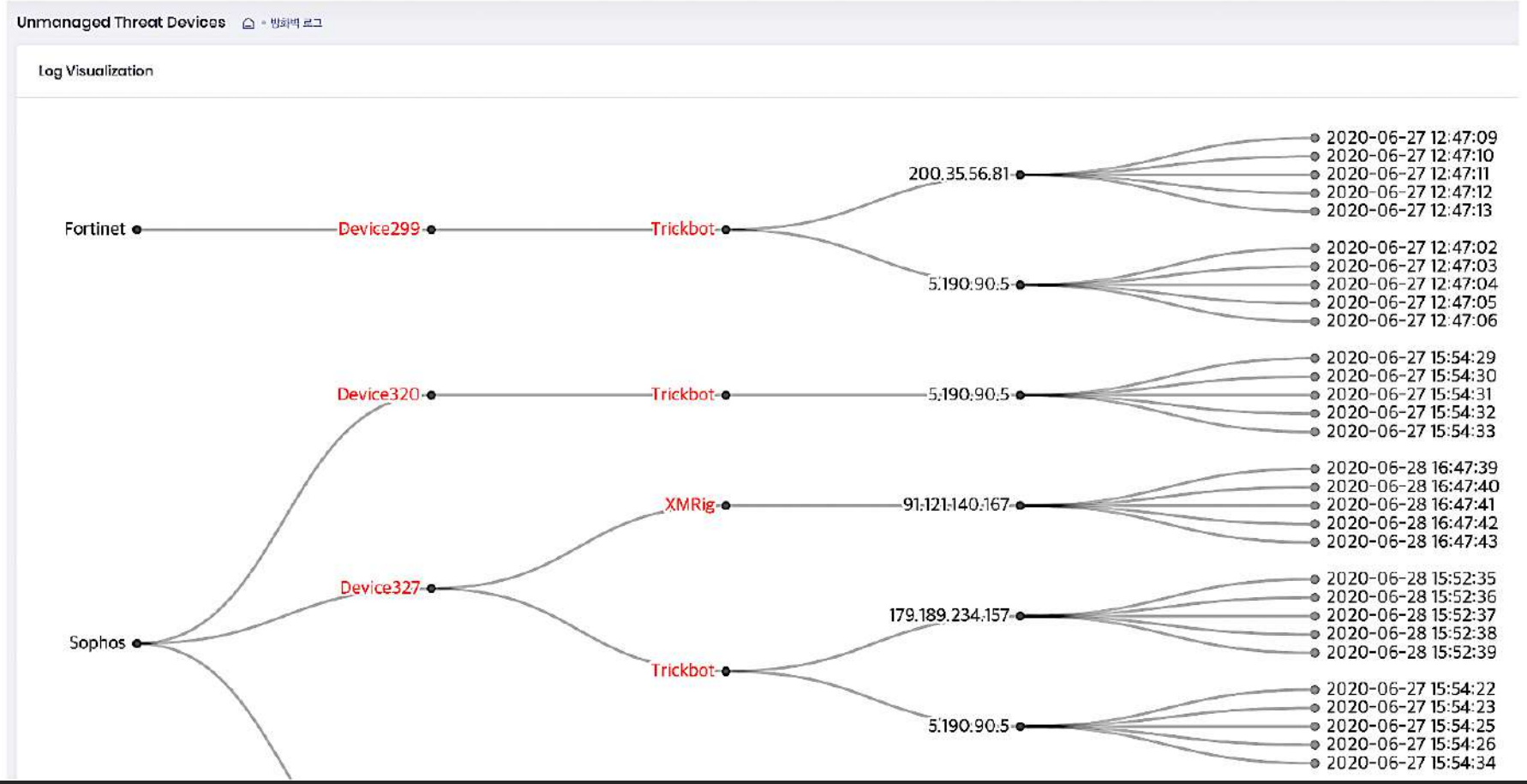


파고네트웍스 위협 인사이츠 DB (TIDB) 연동



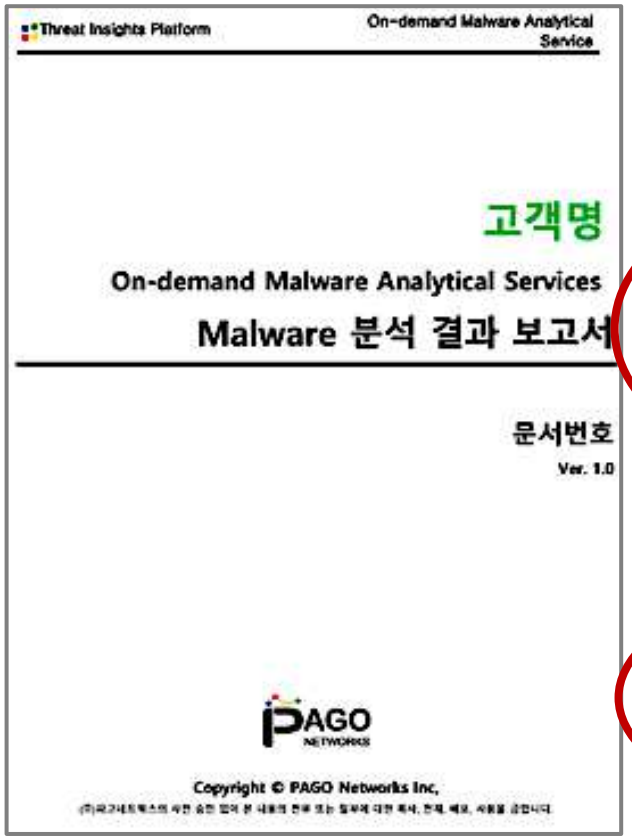
위협 인사이츠 DB (TIDB) 연동 이후.. 결과는

PAGO TIP Console – Infected devices (unmanaged / invisible)



온-디맨드 멀웨어 분석 보고서 서비스

고객사 전달되는, 상세 보고서
실질적인 "위협 목적 / 대응 방안 / 영향도" 위주


Threat Insights Platform
On-demand Malware Analytical Service

고객명

On-demand Malware Analytical Services

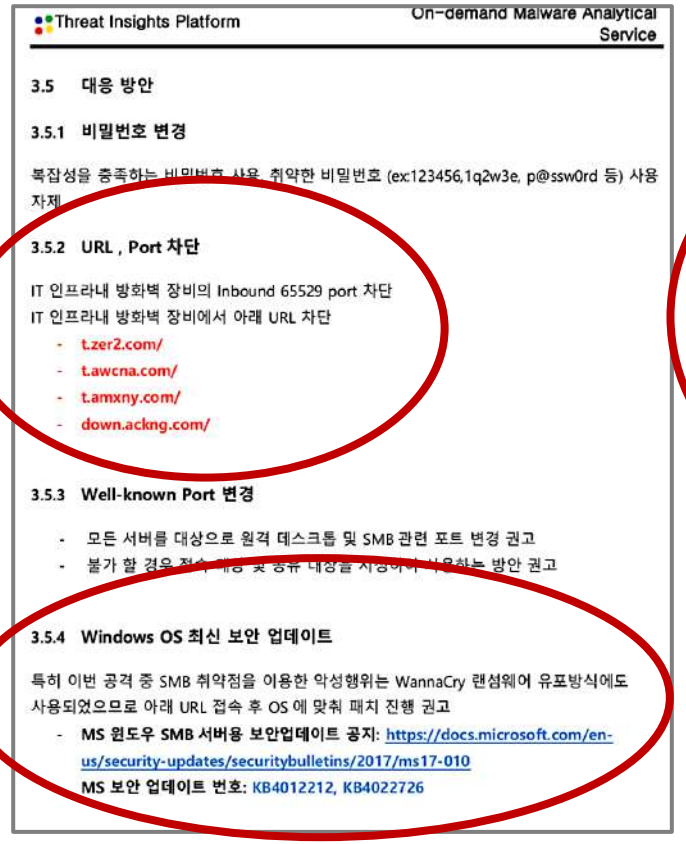
Malware 분석 결과 보고서

문서번호

Ver. 1.0

PAGO NETWORKS

Copyright © PAGO Networks Inc,


Threat Insights Platform
On-demand Malware Analytical Service

3.5 대응 방안

3.5.1 비밀번호 변경

복잡성을 충족하는 비밀번호 사용. 취약한 비밀번호 (ex:123456,1q2w3e, p@ssw0rd 등) 사용 자제

3.5.2 URL , Port 차단

IT 인프라내 방화벽 장비의 Inbound 65529 port 차단
IT 인프라내 방화벽 장비에서 아래 URL 차단

- t.zer2.com/
- t.awcna.com/
- t.amxny.com/
- down.ackng.com/

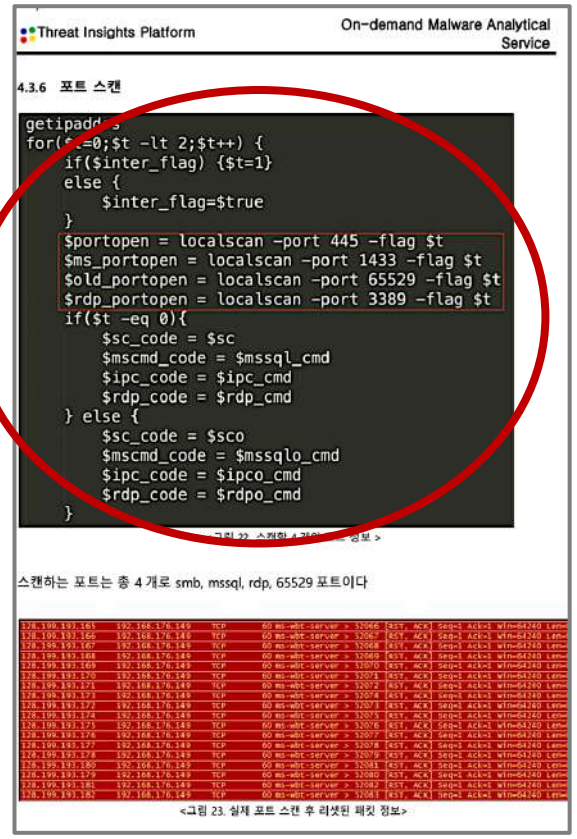
3.5.3 Well-known Port 변경

- 모든 서버를 대상으로 원격 데스크톱 및 SMB 관련 포트 변경 권고
- 불가 할 경우 접속 대상 및 공유 대상을 지정하여 사용하는 방안 권고

3.5.4 Windows OS 최신 보안 업데이트

특히 이번 공격 중 SMB 취약점을 이용한 악성행위는 WannaCry 랜섬웨어 유포방식에도 사용되었으므로 아래 URL 접속 후 OS 에 맞춰 패치 진행 권고

- MS 윈도우 SMB 서버용 보안업데이트 공지: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
  MS 보안 업데이트 번호: KB4012212, KB4022726


Threat Insights Platform
On-demand Malware Analytical Service

4.3.6 포트 스캔

```
getipaddr
for($t=0;$t -lt 2;$t++) {
    if($inter_flag) {$t=1}
    else {
        $inter_flag=$true
    }
    $portopen = localscan -port 445 -flag $t
    $ms_portopen = localscan -port 1433 -flag $t
    $old_portopen = localscan -port 65529 -flag $t
    $rdp_portopen = localscan -port 3389 -flag $t
    if($t -eq 0){
        $sc_code = $sc
        $mscmd_code = $mssql_cmd
        $ipc_code = $ipc_cmd
        $rdp_code = $rdp_cmd
    } else {
        $sc_code = $sco
        $mscmd_code = $mssqlo_cmd
        $ipc_code = $ipco_cmd
        $rdp_code = $rdpo_cmd
    }
```

스캔하는 포트는 총 4 개로 smb, mssql, rdp, 65529 포트이다

<그림 23. 실제 포트 스캔 후 리셋된 패킷 정보>

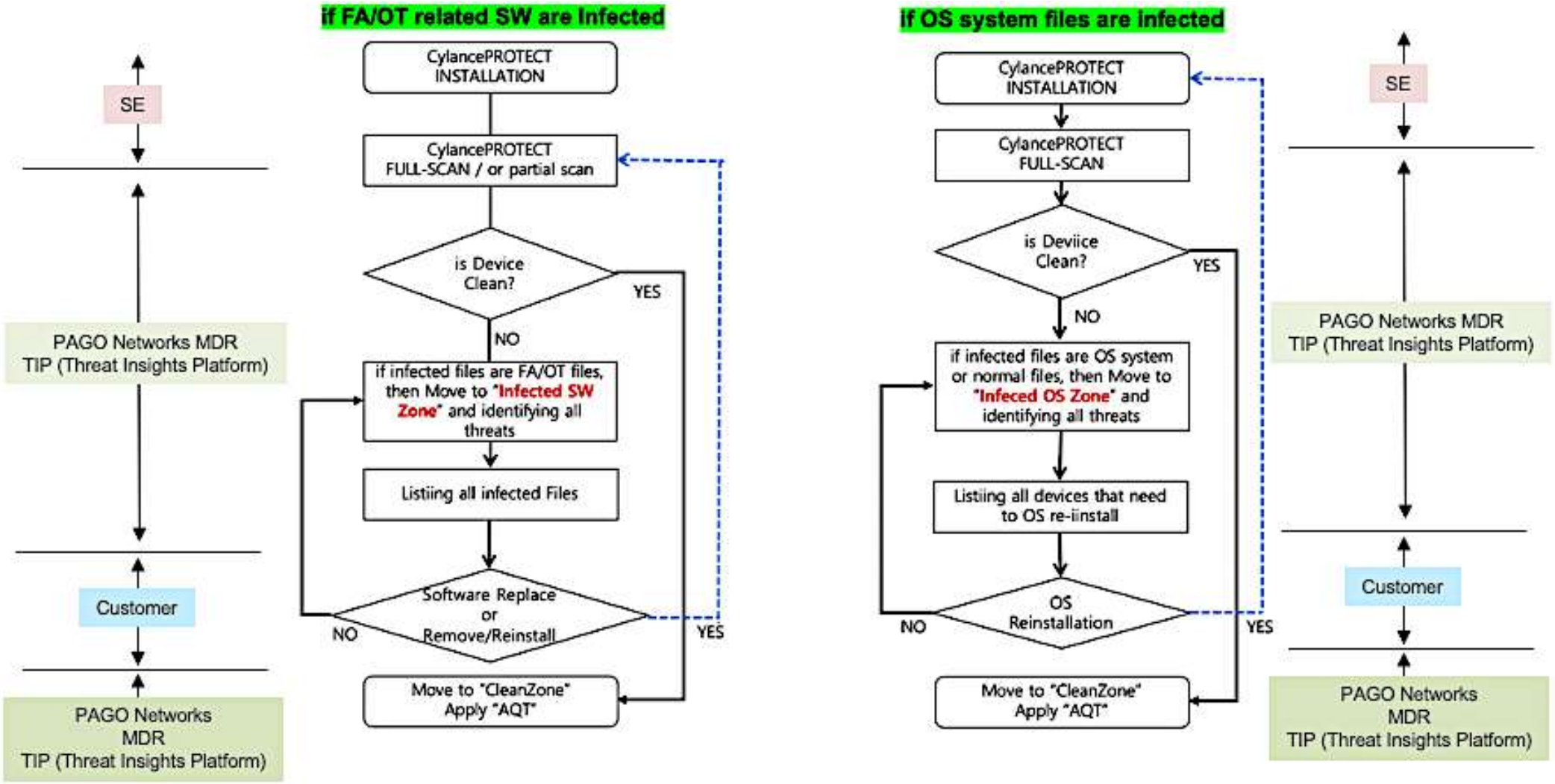
OT / ICS – 엔드포인트 보안 프로세스 1

- **구역 "TestBED (최초 보안에이전트 설치시) → 그 이후, 실제 운영환경 전환**

구역 이름	설명	멀웨어 격리 정책
TestBED_Installation	CylancePROTECT 최초 설치 이후, "TESTBED_Installation" 구역으로 이동 → 최초 1회 "Slow-풀스캐닝 수행"	Default
TestBED_Infected_SW TestBED_Infected_OS	"Slow-풀스캐닝 완료 이후", 만약 " 생산망_SW 또는 OS_파일"에서 머신러닝 기반으로 스코어링 될 경우, "TESTBED_Infected" 구역으로 이동.	Default
TestBED_CleanZone	Virtual SOC 위협분석대응팀에 의해, OT엔드포인트 시스템의 멀웨어가 모두 "Clear"된 상태에서, "TESTBED_CleanZone" 구역으로 이동.	FA_PC_Quarantine

- **목적**
  - 고객 / 프로젝트 팀은 " 시스템 충돌, 안정성 부문, 리소스 사용부문" 등을 체크
  - CylancePROTECT에 의해 탐지된 모든 스코어링 파일 분석 및 현황 공유 (상당히 많은 멀웨어 추가 탐지됨)
  - Virtual SOC 위협분석대응팀 서비스 역량 테스트
  - 위 단계에서, "클리닝 단계 완료 후" → "**Production 단계**" 로 진입

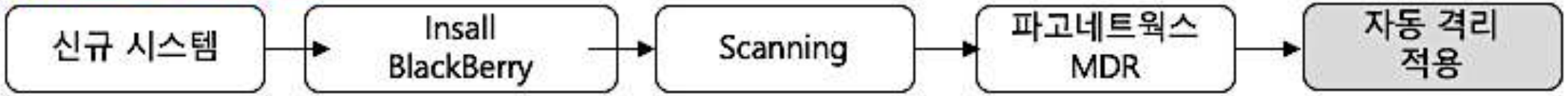
OT / ICS – 엔드포인트 보안 프로세스 2



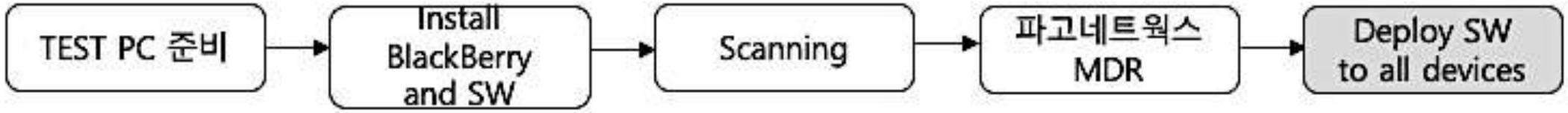
OT / ICS – 엔드포인트 보안 프로세스 3

※ 실제 많은 OT 엔드포인트 보안에서, BlackBerry Protect 가 실제 운영되는 단계

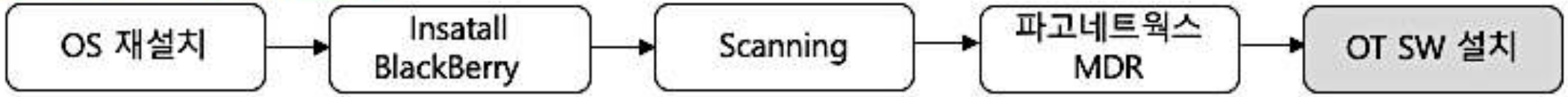
- New PC/Endpoint



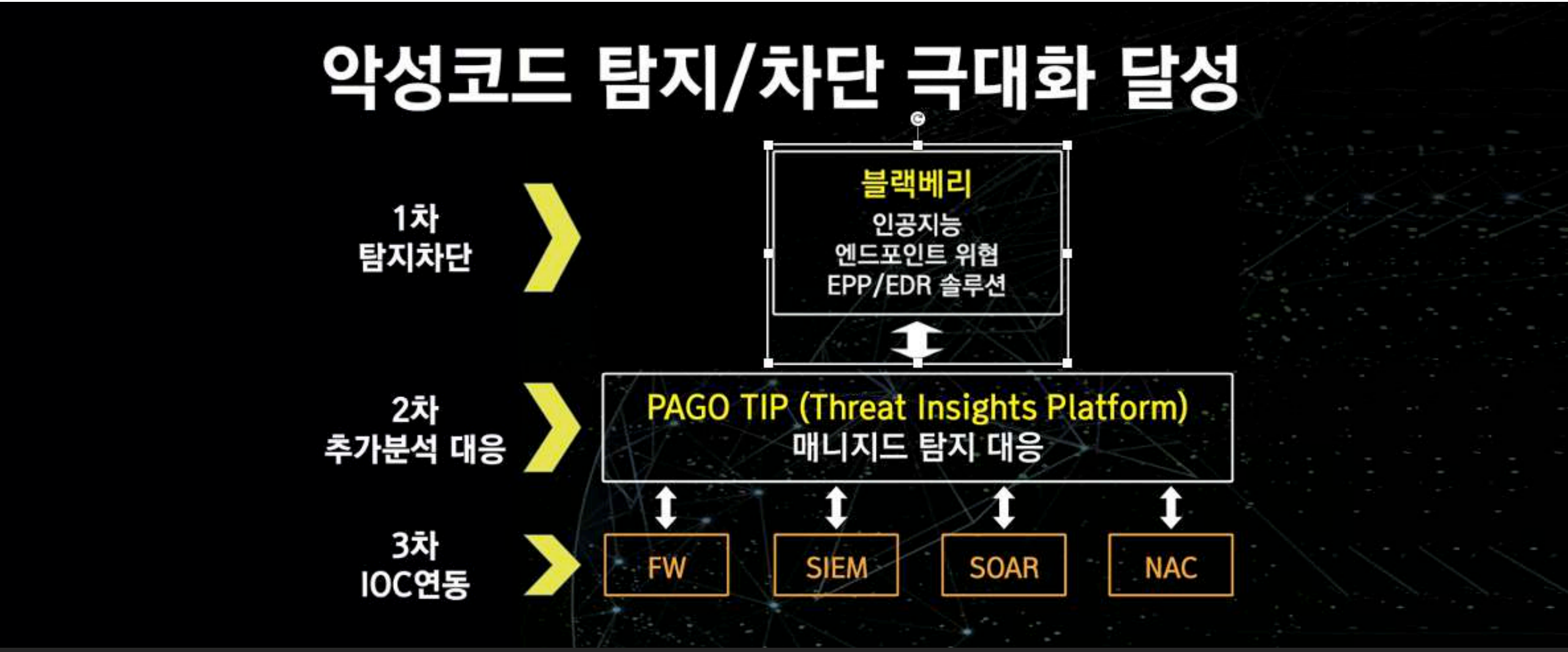
- New Software Installation or updatinig



- PC OS Re-installiing



파고네트웍스 / 블랙베리 전략



고객 피드백 – OT / ICS 엔드포인트 보안

Efficiency

Simplicity

Prevention

엔드포인트 Agent 안정성 / 성능

서로 **운영 환경이 다른 모든 시스템**에서 **동일한 수준의 안정성**과 **성능이슈가 없음**을 확인했다.

멀웨어의 종류에 상관없이, Known/Unknown 탐지 성능이 탁월하다

"다양한 종류의 멀웨어 관련, **기존 AV 대비**.. Known / Unknown 멀웨어 탐지/격리 비중이 훨씬 높다"

생산망에서 AV 가, 안전하게 작동하는 것이 믿겨지지 않는다.

기존 애플리케이션 화이트리스트 솔루션 대신, 머신러닝 EPP와 매니지드 서비스의 조합은 탁월했다.

파고네트웍스 "매니지드 서비스 (TIP – Threat Insights Platform)"

파고네트웍스의 매니지드 서비스는
"단순 레포팅 서비스가 아니고, **새로운 보안운영 프로세스를 정립**시켜 준다."

블랙베리 사일런스 제품 - "기대 이상의 보안성을 극대화" 시켰고,
파고네트웍스 서비스 - "가상 SOC 대응팀"으로 활동한다.

Q & A

감사합니다

Sales@pagonetworks.com

블랙베리 마스터 총판

MDR (Managed Detection & Response) 전문 기업