PASCON 2019
2019 공공기관·기업 개인정보보호&정보보안 컨퍼런스
Public institution·Affiliated organization Information Security Conference 2019

BlackBerry | CYLANCE

# AI / 머신러닝 기반, 엔드포인트 보안 프로젝트 적용 방법론 및 성공 사례


권영목 대표 / Paul Kwon, CEO

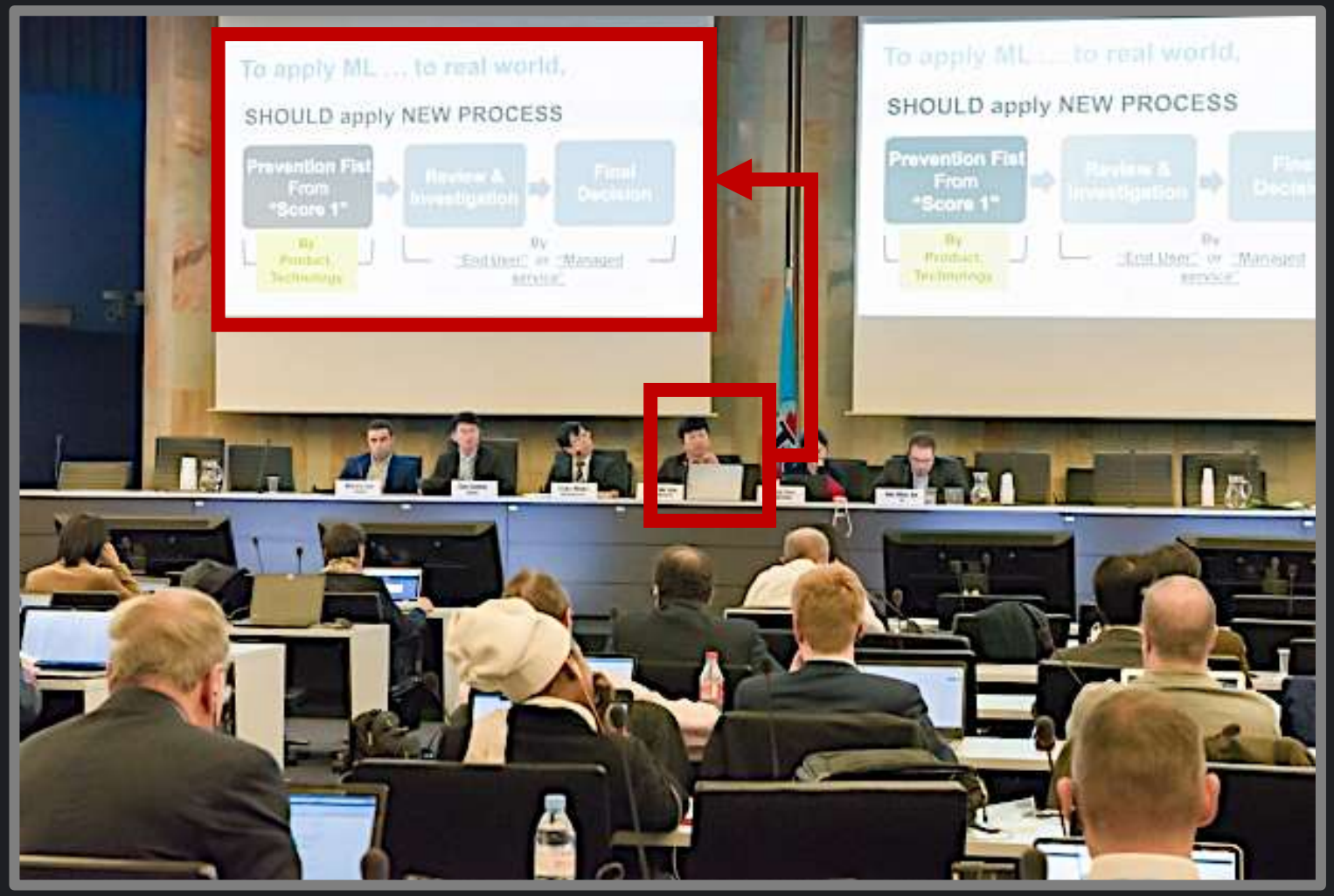
파고네트웍스 / PAGO Networks, Inc

블랙베리 사일런스 한국총판

# ITU 워크샵 (제네바/스위스, 2019년 2월)

- AI / 머신러닝을..
  실제 보안환경에
  적용하려면 ?

- **완전히 새로운**
  **보안 프로세스 방법론**
  적용 필요 !!!




BlackBerry | CYLANCE

PAGO NETWORKS

왜 …

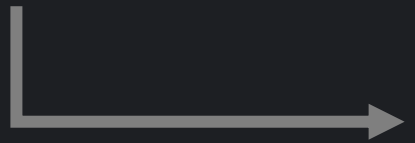
AI / ML 엔드포인트 보안은

완전히 새로운 프로세스 필요한가?

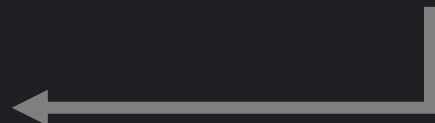
BlackBerry | CYLANCE PAGO NETWORKS

# 엔드포인트 보안 화두

**E**NDPOINT
**P**ROTECTION
**P**LATFORM



- 시그니쳐
- 휴리스틱
- URL 블랙리스트
- 호스트 행위기반
- 네트워크 샌드박스
- 클라우드 샌드박스
- 외부 IOC 연동
- 평판조회
- 안티익스플로잇
- 주기적인 스캐닝
- 머신러닝



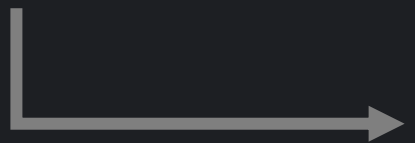
**E**NDPOINT
**D**ETECTION
**R**ESPONSE

BlackBerry | CYLANCE

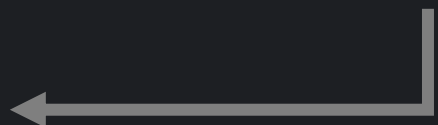
PAGO NETWORKS

# 엔드보인트 보안 화두

**E**NDPOINT
**P**ROTECTION
**P**LATFORM



- 시그니쳐
- 휴리스틱
- URL 블랙리스트
- 호스트 행위기반
- 네트워크 샌드박스
- 클라우드 샌드박스
- 외부 IOC 연동
- 평판조회
- 안티익스플로잇
- 주기적인 스캐닝
- **AI / 머신러닝**

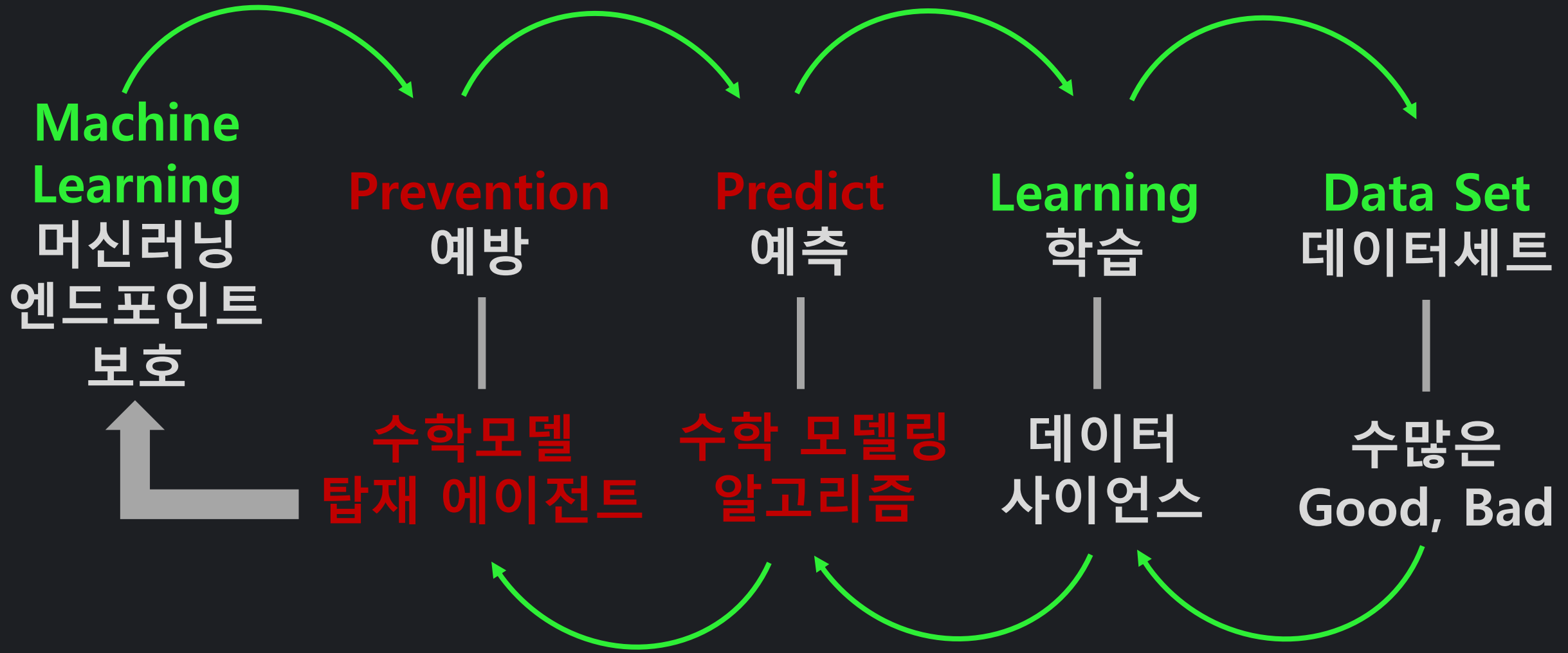


**E**NDPOINT
**D**ETECTION
**R**ESPONSE

BlackBerry | CYLANCE

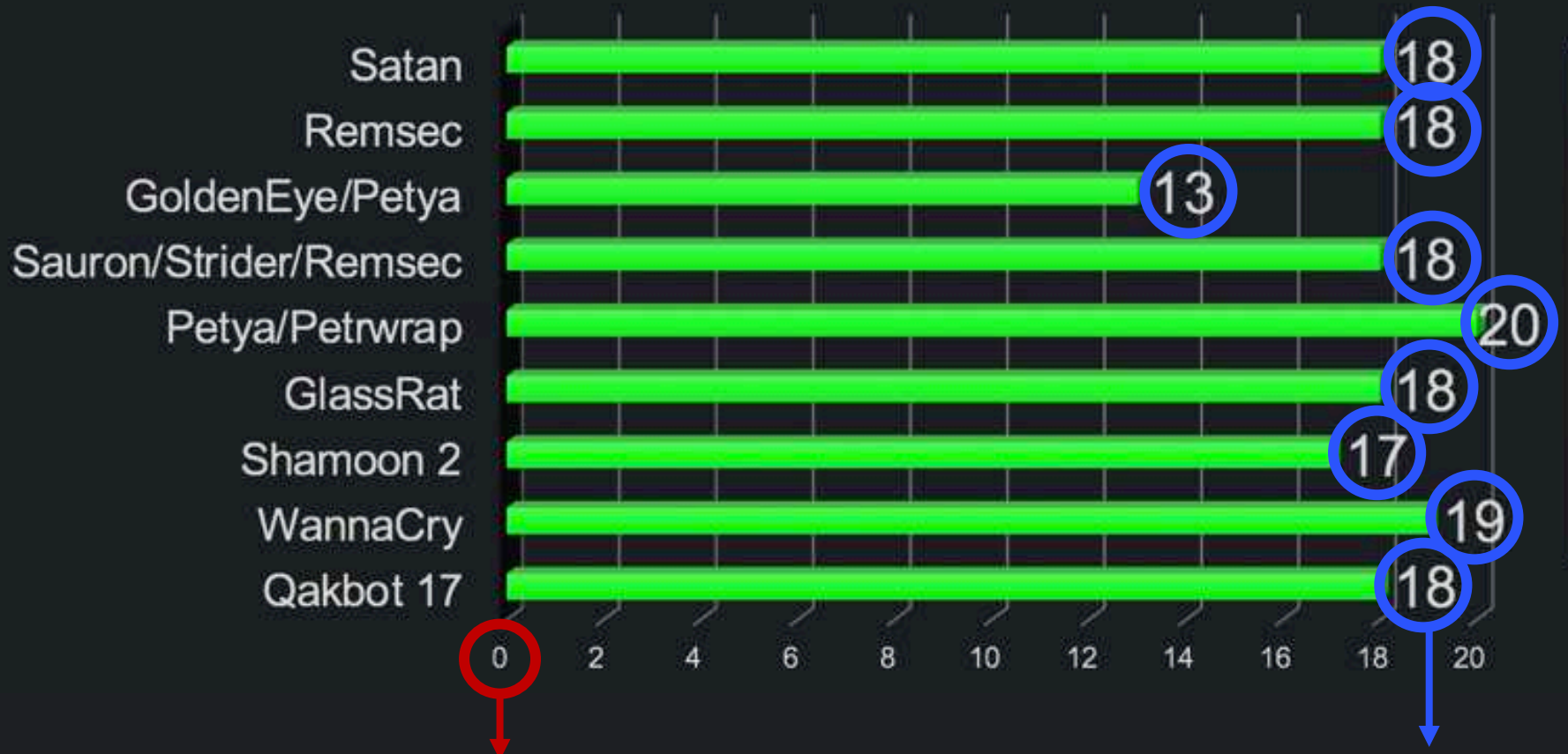
PAGO NETWORKS

# 짚어보겠습니다 – AI / ML 엔드포인트 보안 기술




BlackBerry | CYLANCE
PAGO NETWORKS

# AI / ML - 보안관점 예측/예방 실효성 있나?

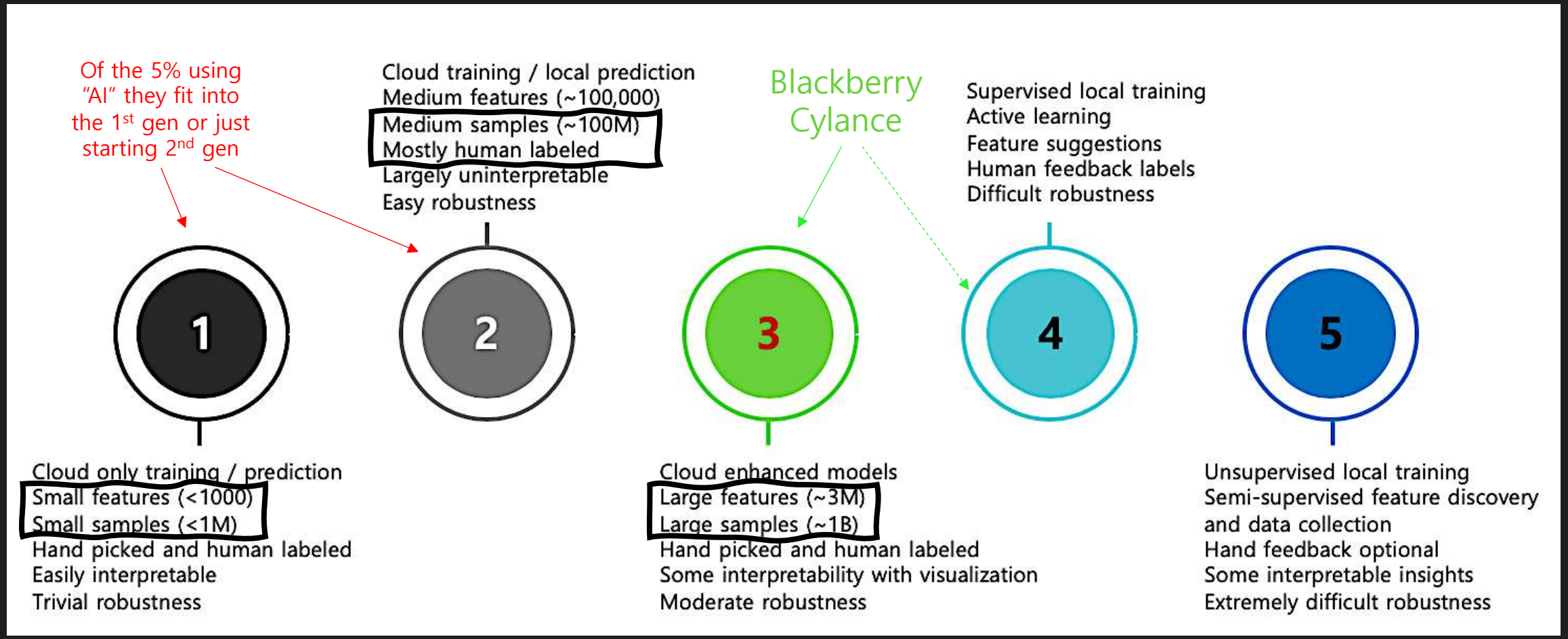



2015년
수학모델 빌드 시점


수학모델 빌드 시점 대비,
수개월 후에 출현한 멀웨어 방어 유무 테스트
(2018년, SE Labs, 예측기반 멀웨어 방어 테스트)

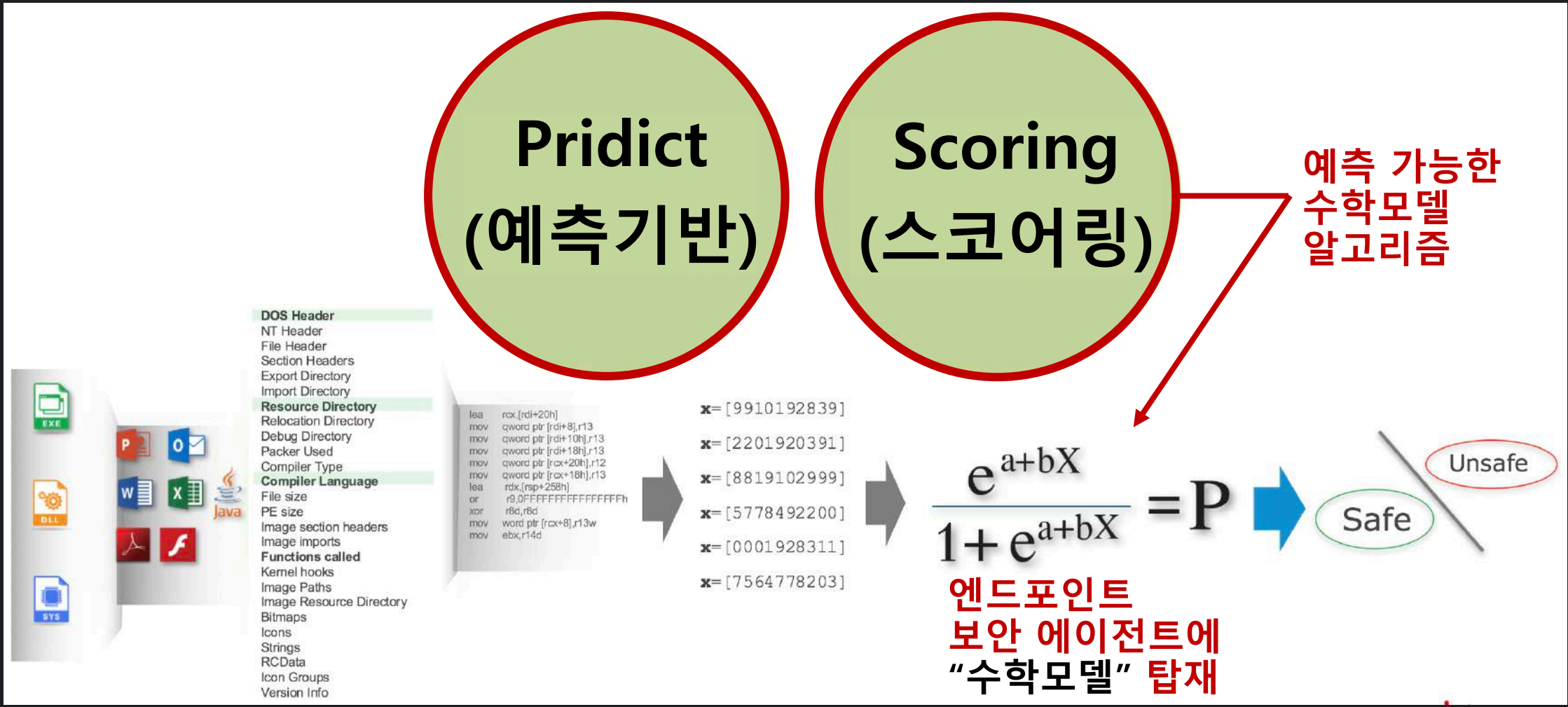
BlackBerry | CYLANCE
PAGO NETWORKS

# 각 엔드포인트 보안 AI / ML – 차이점은?
## 학습량 / 데이터세트 / 수학모델 알고리즘




BlackBerry | CYLANCE. PAGO NETWORKS

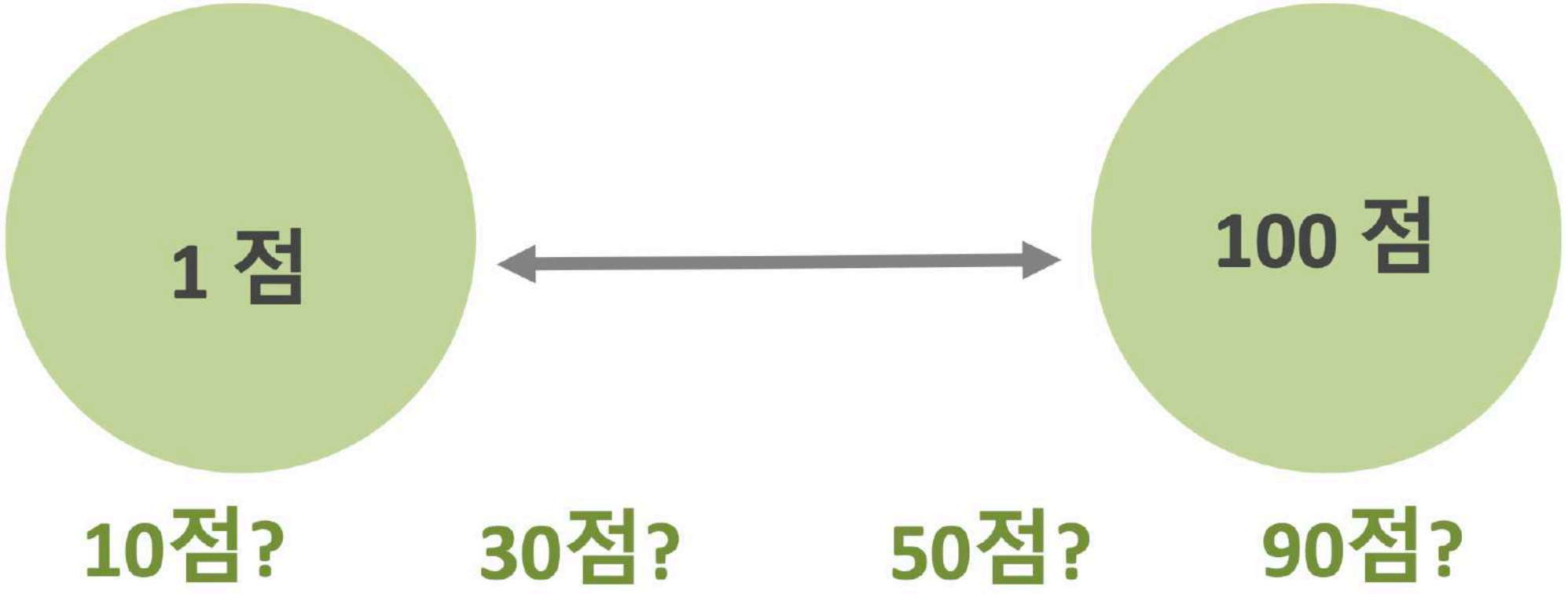
# AI (인공지능)을 엔드포인트 보안에 적용 의미




BlackBerry | CYLANCE

PAGO NETWORKS

# 그렇다면, 예측기반 스코어는 몇점부터 차단?




머신러닝을 적용했다면,
1점부터 차단하는 것을 권고합니다.

1점부터 차단?

FALSE POSITIVE (오탐)” 은?

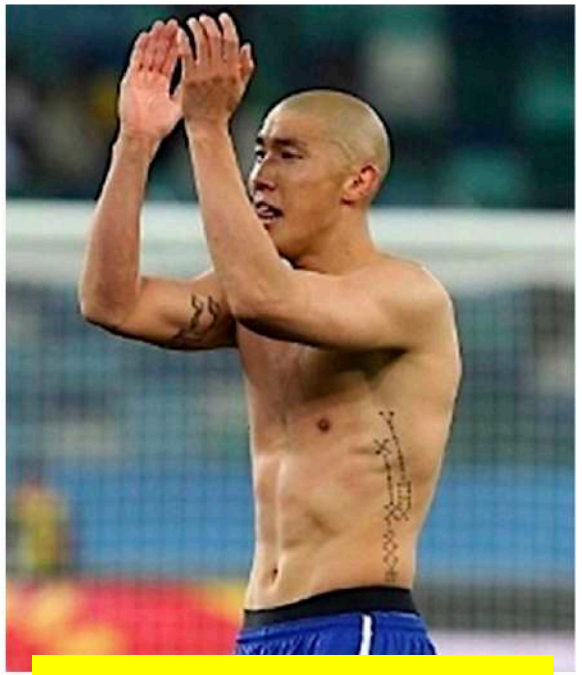
---

모든 머신러닝 보안프로젝트는

이 질문에 해답을 제시해야 합니다.

# 공격적인 질문
# 1점부터 차단? / FALSE POSITIVE는?

## 먼저, 머신러닝 관점 스코어링 이해 필요 (케이스 1)



Scoring = 15

Vs.

Scoring = 100

BlackBerry | CYLANCE

PAGO NETWORKS

# 공격적인 질문
# 1점부터? / FALSE POSITIVE?

## 먼저, 머신러닝 관점 스코어링 이해 필요 (케이스 2)

정상적인
보안 SW

제품 이름: USIM 스마트인증
설명: USIM 스마트인증
버전: 1.5.1.1
회사 이름: [redacted]
저작권: [redacted]
파일 크기: 14.8 MB

서명됨: True
서명 상태: → 인증서 유효기간 만료
발급자: Thawte Code Signing CA - G2
게시자: [redacted]
주제: [redacted]
타임스탬프: 2015-12-28 오후 7:55:00
지문: [redacted]

Scoring = 50

보안 SW
"인증서 탈취"
코드싸이닝
악성코드 공격

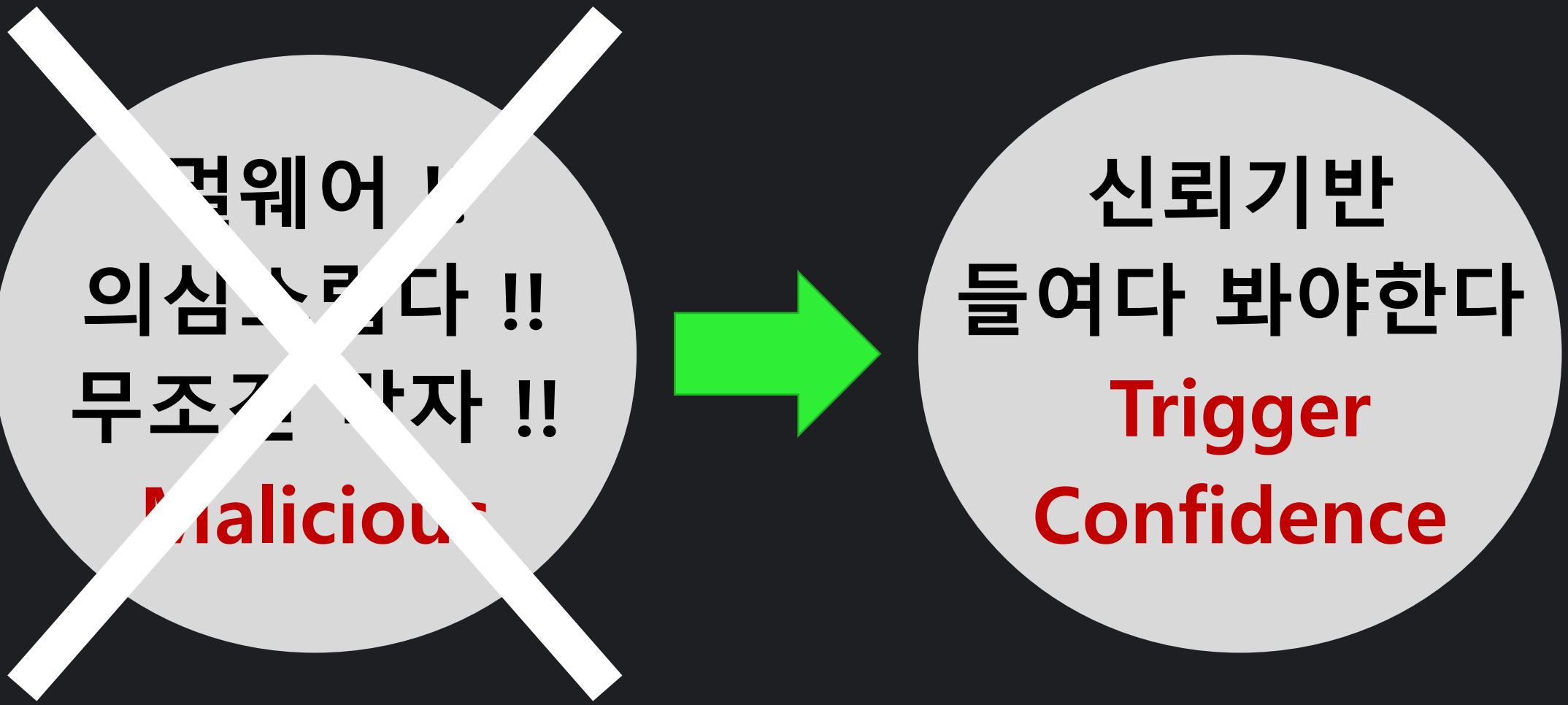
제품 이름:
설명:
버전:
회사 이름:
저작권:
파일 크기: 46.8 KB

서명됨: True
서명 상태: 만료됨 → 인증서 유효기간 만료
발급자: VeriSign Class 3 Code Signing 2010 CA
게시자 [redacted]
주제: [redacted]
타임스탬프: 2016-01-17 오후 8:32:00
지문: [redacted]

Scoring = 100

BlackBerry | CYLANCE
PAGO NETWORKS

# AI / ML 적용 및 예방/예측/스코어링 의미?



# 머신러닝 엔드포인트 보안 – 새로운 접근법 제시

"새로운 방식의 보안 접근법 적용 필요"

머신러닝 기술 도입을 원하신다면 …

스코어링 통한

- Prevention First
- Investigation
- Final Decision

BlackBerry | CYLANCE

PAGO NETWORKS

# 잠시 ..

# 블랙베리 사일런스
# 머신러닝 엔도포인트 보안 솔루션
# 한국시장 성장속도
# 살펴 보겠습니다.

BlackBerry | CYLANCE PAGO NETWORKS

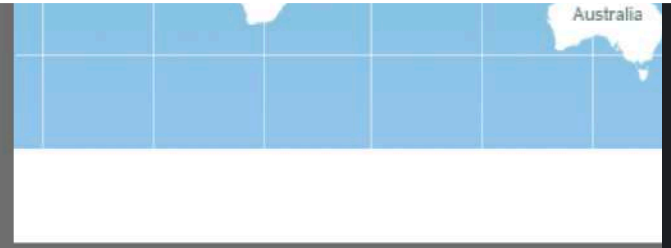
# 2017년 말 !!!

# 2019년 10월 현재 !!!

대한 최적의 대응을 지원하는 보안 서비스로, 과다한 노이즈로 인
했다.

= “파고네트웍스는 2017년 설립 당시부터 MDR 서비스를 적극
에 이르기까지 다양한 규모의 고객 350여곳에 사일런스 머신러닝
넌스에서도 파고네트웍스의 이러한 경험을 호평해 한국 총판으로

PAGO NETWORKS




- 350개 고객사
- 높은 기술력 제공
- 한국 시장에서 인정받는 매니지드 서비스 능력
- 제품 / 서비스 공급력 안정화

BlackBerry | CYLANCE | PAGO NETWORKS

# 머신러닝 하면...
# FALSE POSITIVE 를
# 제일 먼저 걱정했는데...

2017년

10

어떻게?

2019년

350

BlackBerry | CYLANCE

PAGO NETWORKS

# “만약, 아래 내용이 해결된다면 … ?”
# FALSE POSITIVE를 계속 걱정할 필요가 있을까요?

| 시스템 관점 | 일반 사용자 관점 | 운영 관리자 관점 |
| --- | --- | --- |
| 충돌 이슈 X<br>격리 이슈 X<br>APP 가용성 O | 업무 가용성 O<br>업무 중단 X | 예외처리업무 X<br>Helpdesk 콜 X<br>보안성 O |

BlackBerry | CYLANCE PAGO NETWORKS

무엇이 증명되었기에..

고객수가 급격히 늘어나는지

좀 더 구체적으로 살펴보겠습니다.

BlackBerry | CYLANCE PAGO NETWORKS

# 1. 제품의 효율성, 안정성, 보안성 극대화

Stop
The Unknown

Prevent
0-Day Attacks

Light
Performance

Fast
Protection

Predict
to Prevent

No
Signature Update

Easy & Rapid
Deployment

**CPU**
**평균 1~3%**

**메모리**
**평균 30~70MB**

BlackBerry | CYLANCE

PAGO NETWORKS

# 2. 다양한 적용 플랫폼

PC

노트북

서버

POS

ATM

키오스크

헬스케어 장비


무인택배 시스템


공공장소 광고 판넬

산업제어/생산 시스템(PC/서버)

# 3. 다양한 적용 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

BlackBerry | CYLANCE
PAGO NETWORKS

# 4-1. 머신러닝 프로젝트 방법론 FOR 모든 고객

"새로운 방식의 보안 접근법 적용 필요"

머신러닝
기술 도입을
원하신다면 ...

스코어링
통한

- Prevention First
- Investigation
- Final Decision

# 4-2. 머신러닝 프로젝트 방법론 FOR 모든 고객

## 블랙베리 사일런스
## 보안 제품

Prevention is Possible
인공지능 머신러닝 기반
차세대 엔드포인트 보안

CYLANCE PROTECT **EPP**

CYLANCE OPTICS **EDR**

+

## 파고네트웍스
## 탐지/대응 서비스

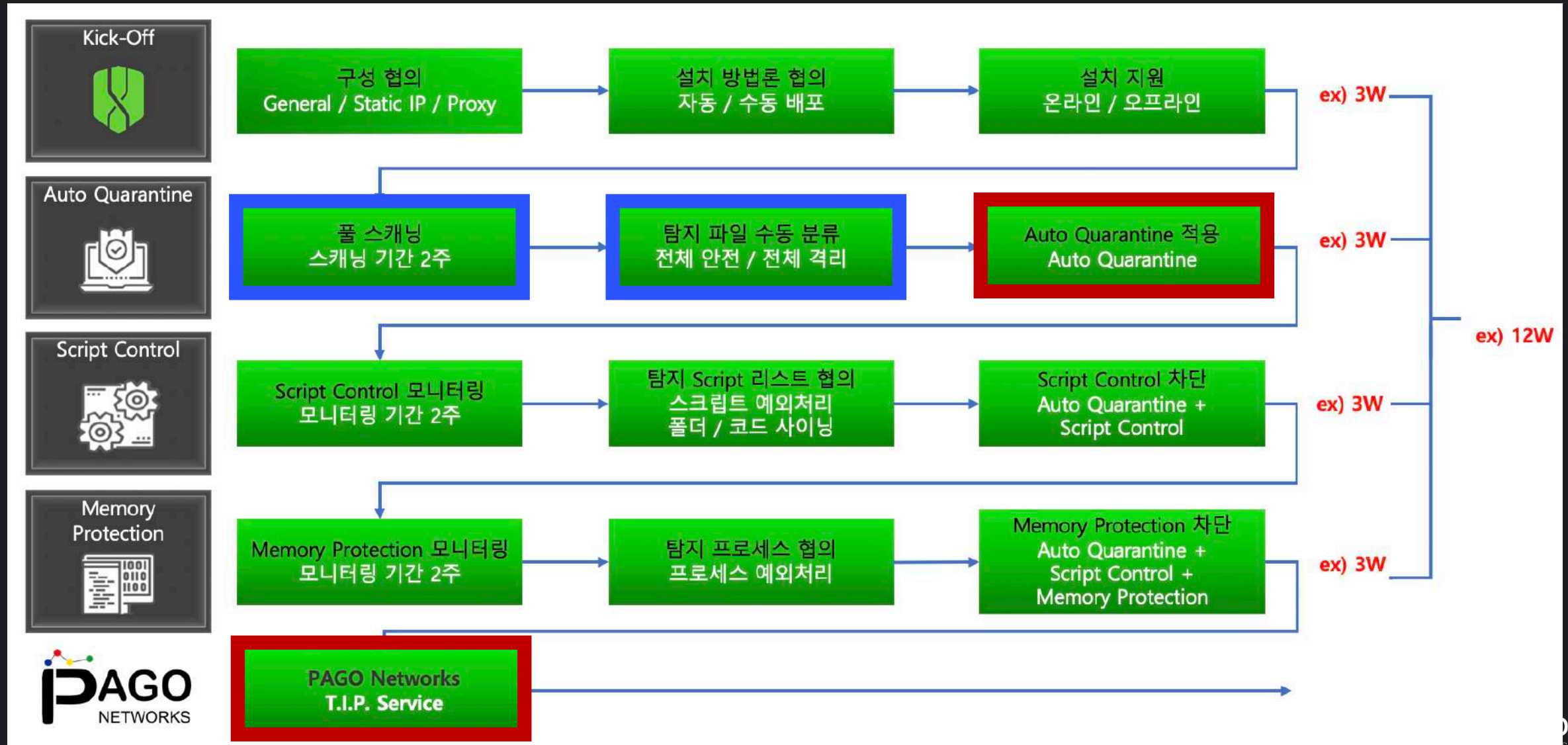
PAGO NETWORKS

***Threat Insights Platform***

- 탐지 / 차단된 모든 멀웨어 / 악성행위 분석
- 긴급 위협정보 공유 서비스
- 온디맨드 멀웨어 상세 보고서
- 대시보드 / 자동 레포팅 자체 연동 제공
- 스크립트 / 매크로 탐지 및 차단 보고서
- 고객 3rd Party 보안솔루션 IOC 연동

BlackBerry | CYLANCE PAGO NETWORKS

# 4-3. 일반 IT 환경 - 프로젝트 방법론 개발



# 4-4. 공장 생산망 / OT 환경 - 프로젝트 방법론 개발

## OA Network CylancePROTECT 사전협의단계

| 1 | 네트워크 구성 | → | 2 | 방화벽 사양 체크 | → | 3 | 방화벽 허용 | → | 4 | Zone 설정 |
|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | 일반 클라우드 통신?<br>✓ Proxy 구성 통신? | | ✓ | 예상 세션 발생 수<br>✓ 방화벽 영향도 체크 | | ✓ | URL 허용?<br>✓ IP 허용? | | ✓ | 분류 기준<br>✓ Zone 네이밍룰 |
| • | 구성 아키텍처 문서 | | • | 세션 관련 기술문서 | | • | 방화벽 허용 정보 | | • | 에이전트 패키징 |

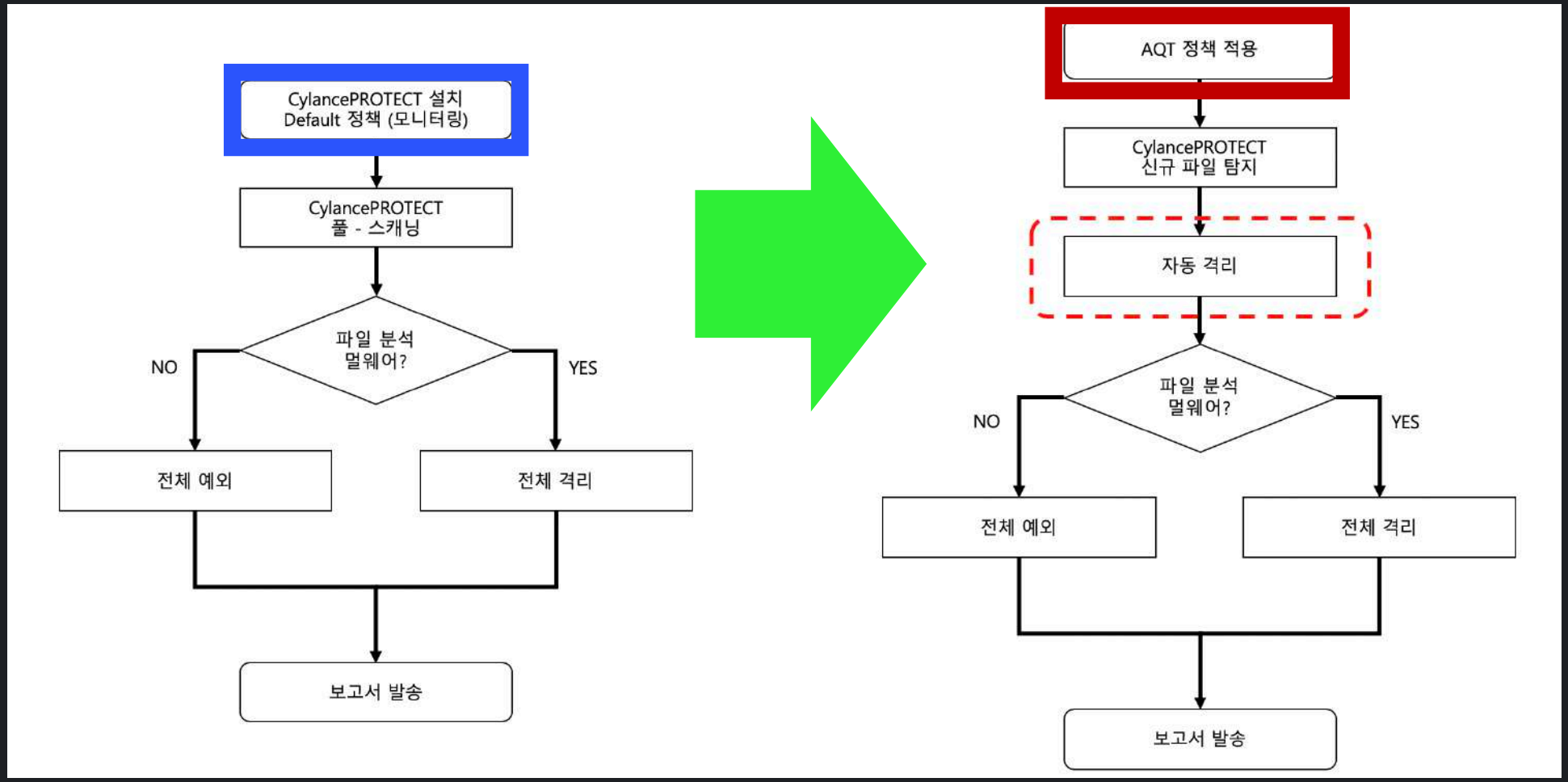
## OA Network CylancePROTECT 구축 단계

| 1 | 에이전트 배포 | → | 2 | 풀 스캐닝/파일 분류 | → | 3 | 운영자 교육 | → | 4 | 정책 적용 |
|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | 운영자 배포<br>✓ 솔루션 배포 | | ✓ | 풀 스캐닝<br>✓ 파일 분류 | | ✓ | UI 이해<br>✓ 서비스 이해 | | ✓ | AQT 적용<br>✓ Script Control 적용 |
| • | 설치 / 배포 가이드 | | • | 위협 보고서 | | • | 교육 자료 | | • | 격리 파일 리스트 |

BlackBerry | CYLANCE

PAGO NETWORKS

# 5. 프로젝트 방법론 – 고객 밀착 프로세스 / 자동화



BlackBerry | CYLANCE

# 프로젝트 성공 사례

# 최초 전제 조건

시스템에서 이미 사용중이던,
기존 엔드포인트 보안 솔루션은... 100% 그대로 유지 !!

사용자 PC
---
기존백신 유지

머신러닝 에이전트
추가 설치

Server
---
기존백신 유지

머신러닝 에이전트
추가 설치

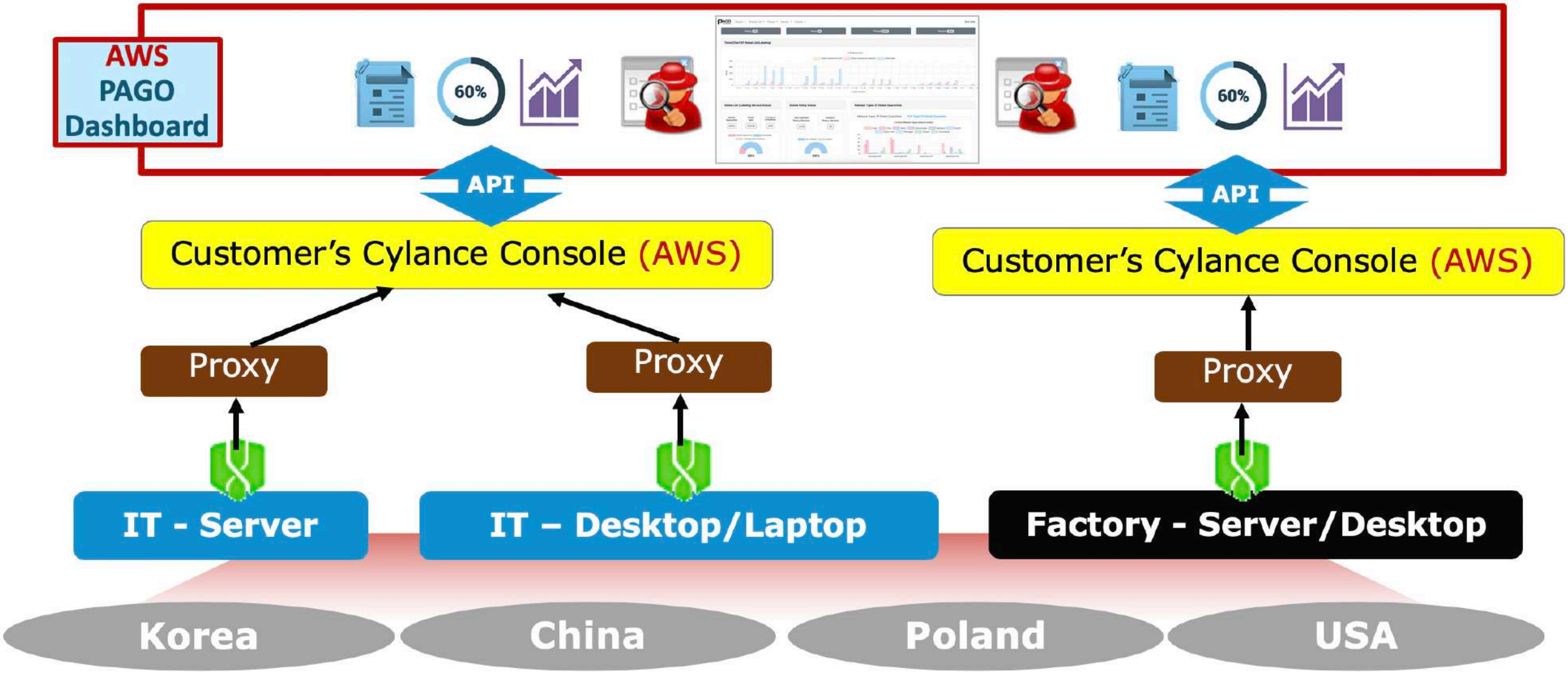
공장 생산망
---
공정용 백신 유지

머신러닝 에이전트
추가 설치

BlackBerry | CYLANCE

PAGO NETWORKS

# 적용아키텍쳐 샘플


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

# 테스트 / 실망운영 - 체크 부문

## 시스템 성능 영향도

- Cylance 설치시, 리부팅 여부 체크
- 시스템 부하 체크
- 시스템 운영시, 장애 발생여부 체크

## 추가적인 “보안성” “탐지/차단” 능력 확인

- 기존 보안솔루션이 탐지하지 못했던 멀웨어를 탐지해 내는가?
- 신종 Unknown 멀웨어 탐지 부문?

## PAGO 매니지드 서비스 레포팅

- 탐지된 멀웨어 추가 상세분석 후, 주요 정보 레포팅
- 온디멘드 요청시, 멀웨어 분석 역량

BlackBerry | CYLANCE

PAGO NETWORKS

# ZERO-DAY 방어 사례 1

기존 AV 존재 및
시그니처 존재 함에도
불구하고,

AI / 머신러닝 엔드포인트 보안
악성 멀웨어/바이러스
추가 탐지 및 격리

| 멀웨어 차단 이유 | 멀웨어 / 바이러스 파일명 | 탐지 / 차단 일시 |
|---|---|---|
| Malware - VirusTotal 57 / 60 | vok90D4.tmp | 2017-06-05 오후 4:14:14 |
| Malware - VirusTotal 57 / 62 | 49916778 | 2017-06-05 오후 4:01:55 |
| Malware - VirusTotal 47 / 62 | ACA0VHWT3.exe | 2017-06-05 오후 4:01:56 |
| Malware - VirusTotal 24 / 27 | 972464524 | 2017-06-05 오후 4:01:59 |
| Malware - Unknown (Fake Microsoft File / Original File - win.exe) | icsys.icn.exe | 2017-08-14 오전 3:30:28 |
| Malware - Trojan / Worm (Virus Total - 57 / 61) | language.exe | 2017-06-13 오전 4:40:25 |
| Malware - Unknown (Product name - Barack Hussein Obama) | 7004[1].exe | 2017-06-05 오후 4:02:02 |
| Malware - Virus | serverx.exe | 2017-07-25 오후 5:56:31 |
| Malware - Trojan | lsmosee.exe | 2017-07-25 오후 5:08:15 |
| Malware - VirusTotal 27 / 61 | Pqrstuvwx.exe_ | 2017-06-05 오후 4:02:02 |
| Malware - Trojan (Bitcoin Miner / VT-50/63) | systens.exe | 2017-08-03 오전 9:34:29 |
| Malware - VirusTotal 58 / 62 | 972904088 | 2017-06-05 오후 4:02:03 |
| Malware - Downloader | 罗马窗口化.exe | 2017-07-27 오전 10:36:29 |
| Malware - Trojan (VT-45/60) | winhlp32.exe | 2017-08-03 오전 9:43:10 |
| Malware - VirusTotal 42 / 54 | 184636652_IEFile.exe | 2017-06-05 오후 2:55:23 |
| Malware - Backdoor (Not Microsoft File) | tv000040.upd | 2017-08-02 오전 4:58:46 |
| Malware - VirusTotal 47 / 59 | -748373528 | 2017-06-05 오후 10:37:23 |

BlackBerry | CYLANCE
PAGO NETWORKS

# ZERO-DAY 방어 사례 2 (PREVENTION 증명)

**CylancePROTECT**
인공지능
머신러닝모델 생성일
**2017년 3월20일**

**CylancePROTECT**
멀웨어 최초
발견 및 차단 일자
**2017년 6월6일**

**A**
시그니처
생성여부 확인
**2017년 7월10일**

과거 3/20
수학모델 이용
Unknown
멀웨어 차단

**7004[1].exe**
**멀웨어 차단**

**A**
**시그니처**
**(없음)**
**방어 실패**

**제로데이**
**35일**

**A**
**시그니처**
**(생성확인)**

# ZERO-DAY 방어사례 3

유럽지부, 부사장 PC

---

기존 AV 설치된 상황

- 고객사 대표이사님과 업무상, 긴급 영상회의 필요
- PC CPU 성능 이슈 발생 (100% Full)
- 영상통화 불가능

유럽지부, 부사장 PC

---

기존 AV 설치된 상황

**CylancePROTECT 즉각 설치**

- 설치 직후, 멀웨어 탐지 및 격리
- 멀웨어 유형 ➔ Unknown 크립토 마이너
- 영상통화 즉시 가능

BlackBerry | CYLANCE

PAGO NETWORKS

# 성과 사례 4 (매니지드서비스 / 상세분석보고서)

…2019. 3. 14. 오후 6:08

PAGO_TECH, PAGO_SALES에게

안녕하세요?

저희가 오늘 몇 군데 분석을 요청했는데 타 업체와는 정성과 수준 면에서 비교할 수 없이 좋은 결과 리포트이네요.

많은 도움이 되었습니다.

수고 많이 하셨고 감사드립니다.

### 3. 분 석 내 용

#### 1. PDF 파일 분석

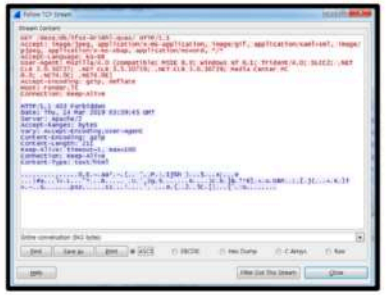
<그림 1. pdfid 로 PDF 파일 스크립트 삽입 여부 결과>

PDF 파일 내부에 악성 스크립트를 삽입하여 공격하는 경우가 존재하여 파일 내부 스크립트 삽입여부를 검사하는 툴인 pdfid 로 해당 파일을 검사한 결과이다.
스크립트는 보통 JavaScript 로 삽입되며 EmbeddedFile 항목 결과로도 삽입 여부를 판단할 수 있는데, 전부 결과값이 0 으로 스크립트가 삽입되지 않았음을 알 수 있다.

#### 2. PDF 에 존재하는 URL 접속 결과 분석

해당 PDF 에 존재하는 URL 주소 관련 정보는 다음과 같다.

1) http://render.lt/deze/db/5fxz-6r58hl-quex/



<그림 2. 접속 시도시 응답받는 패킷 정보>

BlackBerry | CYLANCE PAGO NETWORKS

# 성과 사례 5 (매니지드서비스 / 긴급위협정보 공유)



BlackBerry | CYLANCE

PAGO NETWORKS

# 성과 사례 6 (매니지드서비스 / 긴급위협정보 공유)

Threat-Insights-Platform • 글로벌리스트 • 전체 격리 목록

전체 격리 목록

Show 10 entries

| 테넌트 이름 | SHA256 | Score | Reason | 추가된 날짜 |
|---|---|---|---|---|
| 테넌트1 | A6E2CDC0E9426D50BD72D866BFC80E0FBA941EFB3AE6D1C564D409F57D1EB117 | 100 | PUP - 키젠 / 크랙 (윈도우 라이센스 크랙 / VT-37/69) | 2019-07-03 16:13:59 |
| 테넌트10 | 1FBCAD0B256E6E7059C116E0E8CE4A8B4BE4A0C78956F1AE7F3768EF3430A099 | 100 | 멀웨어크립토마이너 (모네로 CPU 마이너 프로그램 / 임시 파일 / VT-19/71) | 2019-04-17 04:34:28 |
| 테넌트11 | 7A8F38290BE17DC1A7CB3C9B71DE32F884E69BE7A823BC17C08F00A1D8C14314 | 94 | 멀웨어트로얀 (Loki Bot 특성 / 프로세스 상주하며 시스템 및 사용자 정보탈취 / 통신IP 47.254.133.231 / VT-12/72) | 2019-04-17 04:00:31 |
| 테넌트12 | B39BFA60A994BFBD1312BEB1633B1A4DD9698B62285975DD212613EC7E4873E0 | 96 | 멀웨어트로얀 (정보탈취 멀웨어인 Formbook계열 / 키로깅 특성, IE브라우저, 시스템 파일에 코드인젝션 행위 수행 / VT-30/72) | 2019-04-11 11:59:30 |
| 테넌트13 | C960E34CDED8E25652094A241874B1AE7F1C5B43E632CD41EC622360155EAB56 | 94 | 멀웨어트로얀 (Loki Bot Mailspam / 시스템 경로에 bvbvbbvbv.exe 생성 / 이메일, 웹 브라우저, FTP 정보 탈취) | 2019-03-29 18:04:55 |
| 테넌트14 | 326F47611B243256798C45BFA106FBF0A2D6285EC85BA0D4DAD3DC6454421045 | 48 | 멀웨어트로얀 (백도어,봇 특성 내포 / 안티디버깅,시작프로그램 등록기능 스크립트 실행,레지스트리 변경,서비스 생성 / VT-38/71) | 2019-03-26 17:53:07 |
| 테넌트15 | B1C51D4039D15F55E4536F934A6372B8190067E833AFEFCAA2DDFDFB61E19CEF | 42 | 멀웨어트로얀 (백도어,봇 특성 내포 / 안티디버깅,시작프로그램 등록기능 스크립트 실행,레지스트리 변경,서비스 생성 / VT-24/71) | 2019-03-26 17:53:05 |
| 테넌트16 | 526B7A7E80F691F7FCBC4C1E08DB350C6DB9651C8514004D75212FB46956C31E | 89 | 트로얀드롭퍼 (PDF파일확장자로 위장 / Autorun기능 VBS스크립트,스파이웨어 파일 드랍 / VT-18/64) | 2019-03-22 19:50:25 |
| 테넌트17 | D383CEE6586F23BC1DCDD4D1E8638D58E795C0833111BCBD94AE1FB883AAE988 | 99 | 랜섬다운로더 (문서파일 위장 / VBA사용해 갠드크랩 다운로드 / CnC IP 107.173.49.208) | 2019-03-22 15:28:59 |
| 테넌트18 | 5CC274135AFA318C2FB805BFB2DB17748BEBBD42D31C5FE14A182E383EA1B851 | 100 | PUP - 애드웨어 (검색도우미 에이전트의 내부모듈 / 각종URL(indyproject.org)내포) | 2019-03-14 21:43:58 |

BlackBerry | CYLANCE

PAGO NETWORKS

# 도입 이후, 평가 (고객사 A)

- **엔드포인트 Agent 안정성 / 성능**

  "지금까지 사용했고, 테스트 해봤던 엔드포인트 보안 제품 중,
  타 소프트웨어와 **단 한건의 충돌** 또는 **에이전트 자체 이슈를 보지 못했던 유일한 제품**이다"

  "기존 AV와 비교해서, **압도적으로 성능이슈를 제거** 해 준다.
  매일 시그니쳐 업데이트가 필요 없고, 매일 풀-스캐닝도 필요없다.

- **기존 AV 탐지 못한 "Known / Unknown 멀웨어 / 바이러스" 탐지 차단**

  "**기존 AV가 있는데도**, "이렇게  많은 Known / Unknown 멀웨어가 탐지되는지 미처 몰랐다"

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

  "AV를 사용하면서, 이렇게 가치 있는 매니지드 서비스를 받는 경험은 처음이다.

**블랙베리 사일런스 제품과, 파고네트웍스의 매니지드 서비스는**
**"단순 Anti-Virus 대체 제품이 아니며, 그이상의 가치를 제공한다"**

# 도입 이후, 평가 (고객사 B)

- **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.**

# 아래 이슈 / 고려사항을 경험하고 계십니까?

- 기존 **성능이슈** 경험
- AV 기능을 100% 활성화 시키지 못하는 경우 (**성능/충돌** 이슈로 인해)
- 설치 / 제거 시, **장애이슈** 존재
- 신규/변종 멀웨어 **시그니쳐 업데이트** 업무에서 해방이 필요한 경우
- **풀-스캐닝** 업무에서 해방이 필요한 경우
- **WINDOWS XP, 2003** 시스템을 여전히 운영하는 경우
- 탐지/격리된 **멀웨어 정확한 정보** 필요한 경우
- 기존 대비 **보안성능(PROTECTION)** 비율을 높이고 싶은 경우

# 머신러닝 기술 + MDR 서비스의 만남

## 블랙베리 사일런스
## 보안 제품

Prevention is Possible

인공지능 머신러닝 기반
차세대 엔드포인트 보안

CYLANCE PROTECT — EPP

CYLANCE OPTICS — EDR

+

## 파고네트웍스
## 탐지/대응 서비스

PAGO NETWORKS

***Threat Insights Platform***

- 탐지 / 차단된 모든 멀웨어 / 악성행위 분석
- 긴급 위협정보 공유 서비스
- 온디맨드 멀웨어 상세 보고서
- 대시보드 / 자동 레포팅 자체 연동 제공
- 스크립트 / 매크로 탐지 및 차단 보고서
- 고객 3rd Party 보안솔루션 IOC 연동

BlackBerry | CYLANCE  PAGO NETWORKS

# Questions

+

# Answers