Goodus
Breathing Life into Technology

Vectra Cognito 제품소개

AI based Inside Threat Hunting Solution

VECTRA®

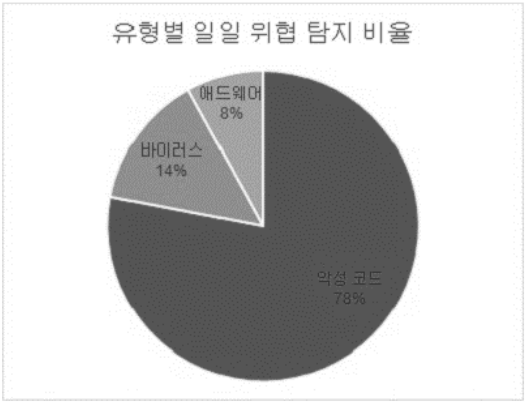
- 신종 공격 대응 한계 -

2017년 하루 36만 개 신종 악성파일 탐지...
2016년 대비 11.5% 증가

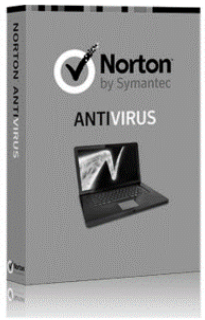
2017년 연간 보안위협 통계에서 주목할 사항

길민권 기자 mkgil@dailysecu.com 2017년 12월 21일 목요일

댓글 0 폰트 + −



시만텍 부사장 "백신소프트웨어는 죽었다"



노턴안티바이러스 등 보안 소프트웨어를 판매하는 시만텍 간부가 "안티바이러스 소프트웨어는 죽었다"는 발언을 해 눈길을 끈다.

이렇게 스스로를 부정하는 듯한 충격 발언을 한 인물은 시만텍 수석 부사장을 맡고 있는 브라이언 드예(Brian Dye)다. 그는 1980년대 안티바이러스 소프트웨어를 개발하는 한편 지금도 시만텍에서 제품 관리와 데이터센터 보안, 데이터 손실 방지 등 폭넓은 분야를 총괄하고 있다.

그는 기존 안티바이러스 소프트웨어에 대해 "죽었다(dead)"는 표현을 하며 안티바이러스 소프트웨어가 수익성 있는 제품은 아니라고 본다고 덧붙였다. 이 같은 발언은 보안 분야의 과제가 바뀌어야 한다는 점을 시사하는 것.

그가 밝힌 바에 따르면 현재 안티바이러스 소프트웨어가 바이러스 공격을 탐지할 수 있는 건 전체 중 45% 수준이다. 나머지 55% 공격은 감지하지 못하고 그냥 지나친다는 얘기다. 이런 문제가 발생하는 건 해킹 수법이 갈수록 지능화되고 있어 기존 방법에는 한계가 있다는 걸 스스로 인정한 것이다.

그가 밝힌 바에 따르면 현재 안티바이러스 소프트웨어가 바이러스 공격을 탐지할 수 있는 건 전체 중 45% 수준이다. 나머지 55% 공격은 감지하지 못하고 그냥 지나친다는 얘기다. 이런 문제가 발생하는 건 해킹 수법이 갈수록 지능화되고 있어 기존 방법에는 한계가 있다는 걸 스스로 인정한 것이다.

1. 기존 기술 – SIEM (Security Information Event Management)

- TI(Threat Intelligence), 시나리오 생성/관리, 트래픽 분석 한계 -

TI 한계

- 데이터 수집, 저장, 처리, 검색에 집중 → **TI (탐지시나리오, 평판 정보) 제공 X or 부족**
- 악성코드 행위 분석 시나리오 자체 제작 / 관리 어려움 → **악성코드 전문가 필요**

Traffic?

- 로그 데이터를 대상 분석 시스템 한계 → **로그 수집 불가 단말/시스템은?**
- 일부 SIEM들은 트래픽 데이터 수집/분석 → **수집 양=가격↑, Payload 부분 full 탐지 X**

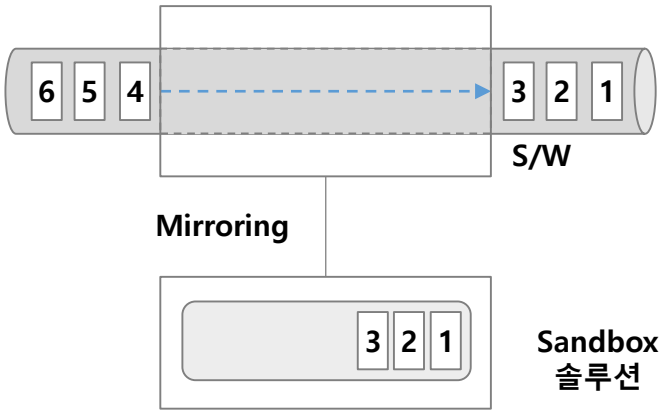
임계값 문제

- 시나리오 내 임계값(Threshold)은 고정 값을 정의하고 수정•관리 → **임계값 조정/관리 공수↑**

Ex) (평소에 접속)하지 않았던 (외부 호스트)로 (대량)의 데이터를 전송

1. 기존 기술 – Sandbox 기반 탐지

- 구조상 신종 악성코드 감염, 다수의 우회 방법 존재 -



[파일 유입 및 캡처 원리]

항목	내용
하드웨어 탐지	Sandbox 장치 디바이스 정보 인지
디버거 확인 및 무력화	감시 디버거 여부 확인, 일부 디버거 무력화
SW, OS 버전 확인	IE, 오피스, OS 등 특정 버전에서만 동작
실 사용자 행위 확인	실제 사용자 행위를 확인하고 활동
시간차 활동	실행 후 장기간 대기 후 악성 행위 동작
암호화 통신 이용 우회	SSL 통신으로 파일 캡처 불가

[가상화 환경 무력화 방법]

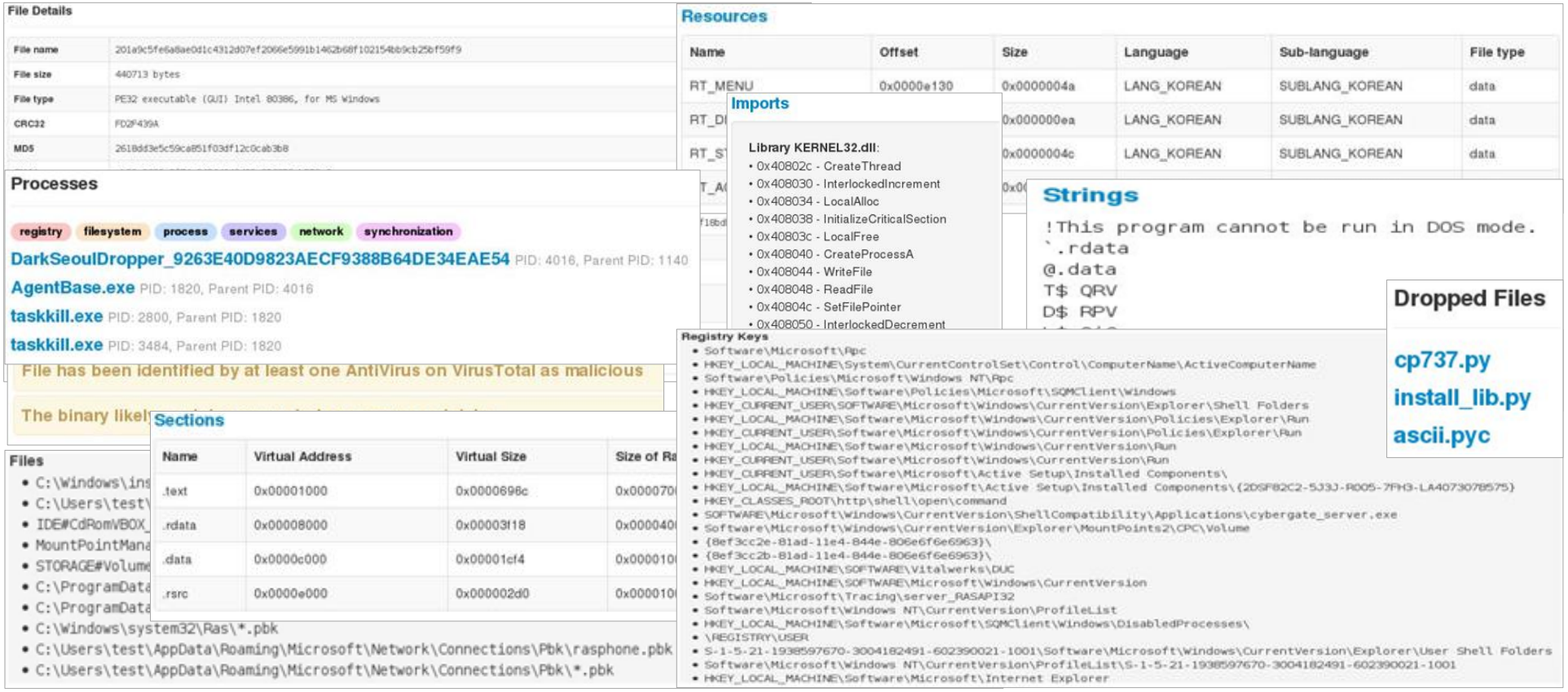
- 처음 보는 파일을 내부로 우선 보내고 파일을 sandbox에서 실행·오픈하여 검사

→ 신종 악성코드는 한번은 내부 감염 불가항력

→ 다수의 우회/회피 방안 존재

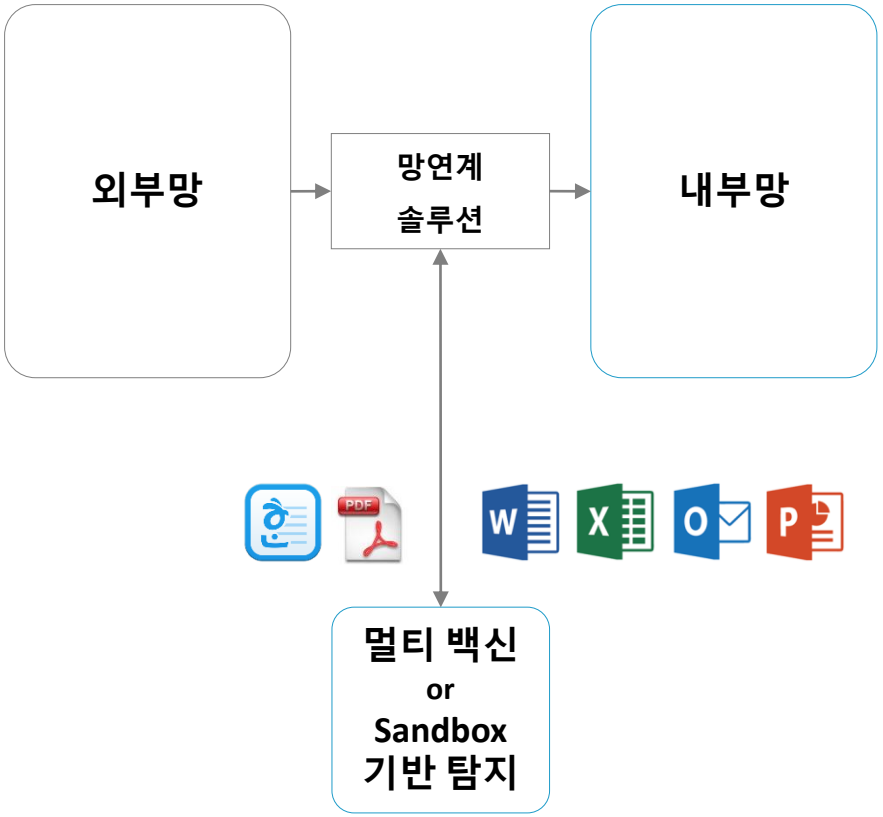
1. 기존 기술 – Sandbox 기반 탐지

Sandbox 탐지 결과 스스로 분석하실 수 있나요?

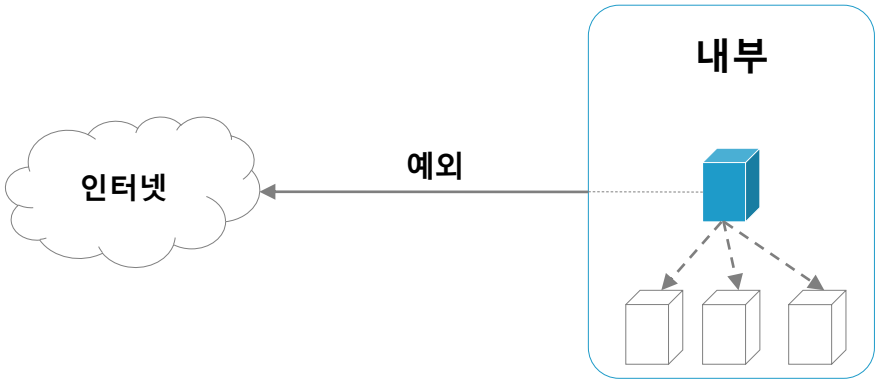


[Cuckoosandbox 포렌식 화면]

1. 기존 대응 기술 - 망분리



→ 내부 유입 파일 탐지가 상대적으로 취약



→ 예외 룰, 예외 단말기로 인한 내부 감염

2. 주요 이슈 – 내부 보안 홀(Hall)

Dwell Time for Cyber Intrusion

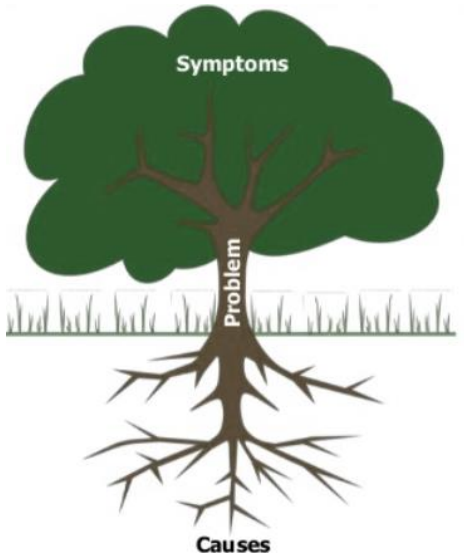
99
Global

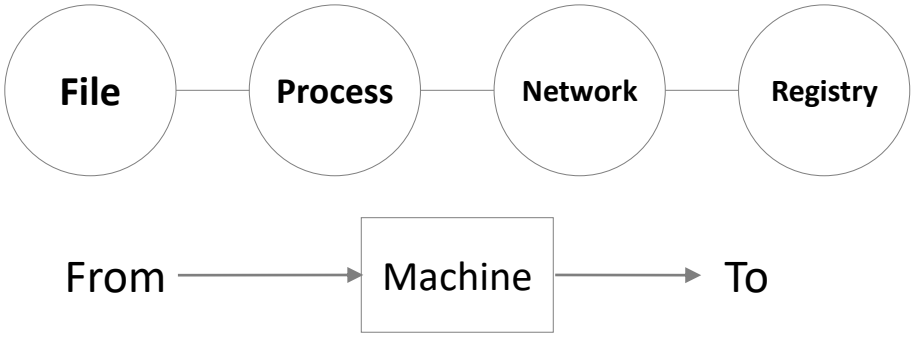
106
유럽, 중동, 아프리카

172
APAC

from ZDnet 2018.01.11 By Asha McLean

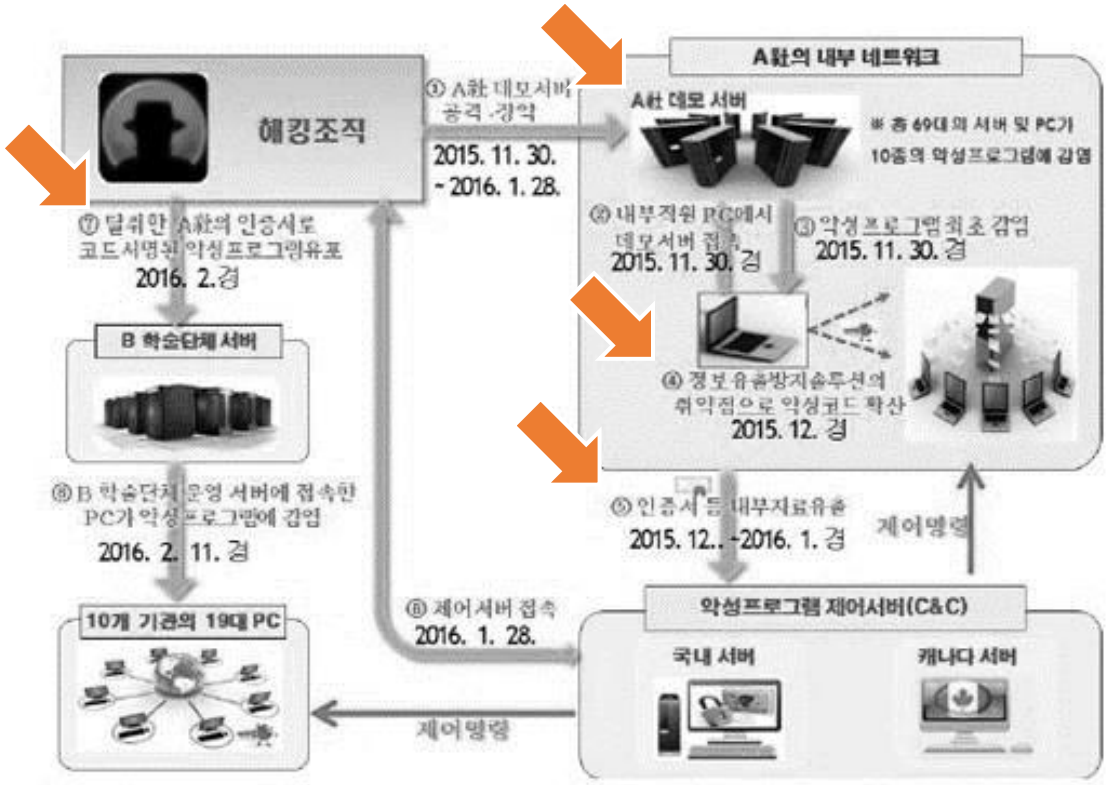
Root cause, Investigation





2. 주요 이슈 – 내부 보안 홀(Hall)

- 보안 SW를 통한 내부 감염 -



From 2016-05-31, 보안뉴스 코드서명 해킹은 북한 소행…실제 피해는 없어

1. 보안 업체의 시스템이 감염 됨
2. 보안 SW 자체 취약성
3. 신뢰 SW 경로로 내부 침입 가능

(ex-우리 회사 PC는 그 파일 없어?)

2. 주요 이슈 – 내부 보안 홀(Hall)

혹시 내부에 감염 호스트가 있지 않을까요?

없다고 어떻게(무엇을 보고) 확신을 하실 수 있나요?

2. 주요 이슈 – 내부 보안 홀(Hall)

- Coverage MAP (Before) -

	사전 차단 (Prevention)	사후 탐지 (Detection)	
North – South	○	○	?
	접근제어 리스트, 시그니처, 휴리스틱, 임계값 화이트리스트	(제한적인) 탐지 시나리오, 평판 정보, Sandbox	?
	N-Firewall, IPS, Virus-wall, 백신, DDoS, WAF…	IDS, SIEM, Sandbox 기반 IDPS…	?
East – West	○	○	?
	접근제어 리스트	(제한적인) 탐지 시나리오	?
	N-Firewall (망 보호), H-Firewall	SIEM	?

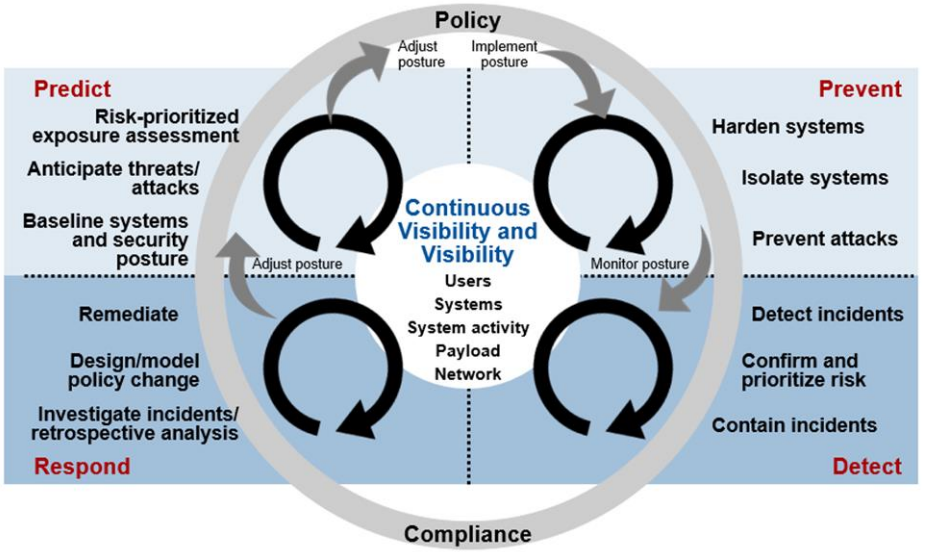
3. 보안 동향

Prevention에서 Detection으로...

최근의 보안은 '**빠른 탐지와 빠른 대응**'에 맞춰져 이뤄지고 있다. 이는 '**공격은 이미 당했다**'는 전제 하에 이를 **최대한 빠른 시간 안에 발견**해내고 **해결**하는 것을 기본 골자로 한다는 것이다.

From 2017.09.19 보안뉴스-각광받는 기술 오케스트레이션, 자동화와 어떻게 다른가?
/ 글 : 다리오 포르테(Dario Forte), DFLabs

능동형 보안 아키텍처의 구성
(Advanced Security Architecture)



VECTRA

Goodus
Breathing Life into Technology

1. Vectra社 Cognito - 개요

인공지능 기반 APT 대응 솔루션

인공지능 기반 탐지모델

- 벤더의 머신러닝(지도학습), 딥러닝 – 탐지모델로 **악성행위** 탐지
- 로컬 사이트에서 머신러닝(비지도학습) – 탐지모델 **비정상행위** 탐지

사이버 킬 체인 기반

- 기존 보안 솔루션을 침투 또는 우회하는 위협 **탐지, 대응**
- **C&C접속, 봇넷행위, 내부정찰, 내부확산, 정보유출 행위 구분**

내부 네트워크 가시성

- 내부 간 트래픽 감시
- 암호화 트래픽 감시
- 내부 호스트 **악성행위 가시성** 확보

실시간 자동 상관분석

- 위협 빈도, 양, 기간, 최근성 등
- **우선순위 실시간 스코어링**
- **관제 Tier-1 수준**의 분석, 요약

1. Vectra社 Cognito - 제품개요

제품 영역 – Network IDPS(Intrusion Detection Prevention System)

Market Definition/Description

The network IDPS market is composed of **stand-alone physical and/or virtual appliances that inspect network traffic**, either on-premises or in virtualized/public cloud environments. They are often located in the network to inspect traffic that has passed through perimeter security devices, such as firewalls, secure web gateways and secure email gateways. While detection only (i.e., intrusion detection system [IDS]) is still often used, a large number of appliances are still deployed in line to allow for blocking capabilities. They provide detection via several methods — for example, signatures, protocol anomaly detection, **various methods of analytics, behavioral monitoring and heuristics, advanced threat defense (ATD) integration, and threat intelligence (TI)** to uncover unwanted and/or malicious traffic and report or take action on it.

Stand-alone IDPSs are most often deployed for the following reasons:

- When separation of duties means that some networking functions (firewalls) are managed by a different team managing security (i.e., IDPS)
- **Behind the firewall as an additional layer of defense to inspect north-south traffic**
- Behind an application delivery controller (load balancer) to inspect traffic allowed
- When best-of-breed detection efficacy is required
- **As an IDPS on the internal network in line to provide protection/detection for internal assets**
- **As an IDS monitoring the internal network for lateral movement of threats and other compliance mandates**
- When high IDPS throughput and low-latency performance are required
- **To provide network security separation (segmentation) on parts of the internal network where it's easier to deploy IDPS than technology like firewalls**
- **To provide additional visibility and detection capabilities in the public or private cloud**
- **For network-based intrusion and threat detection using additional methods like advanced analytics (such as user and entity behavior analytics [UEBA]) to detect threats that have bypassed other controls**

2. Vectra社 Cognito – 인공지능 기술

Traditional Programming

- 주어진 연산식으로 결과를 구함 -

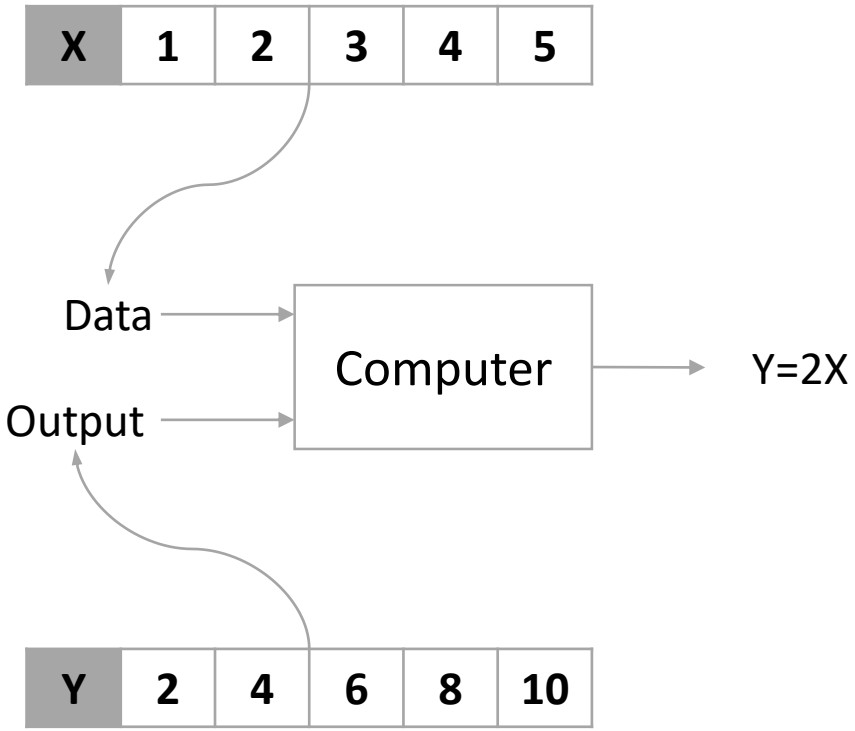
Machine Learning

- 예측 하기 위해 연산식을 구함 -

2. Vectra社 Cognito – 인공지능 기술

Traditional Programming

Machine Learning

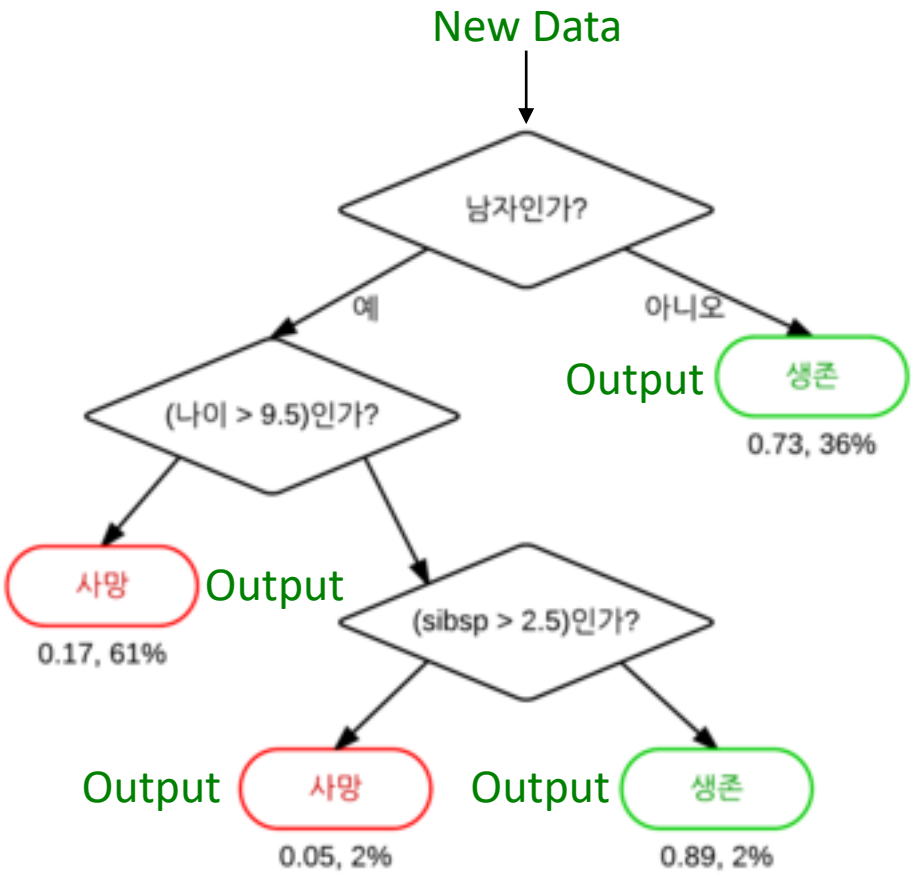


2. Vectra社 Cognito – 인공지능 기술

Decision Tree - 함수

```
digraph Tree {
node [shape=box] ;
0 [label="X[1] <= 0.5₩ngini = 0.473₩nsamples = 891₩nvalue = [549, 342]"] ;
1 [label="X[2] <= 6.5₩ngini = 0.3064₩nsamples = 577₩nvalue = [468, 109]"] ;
0 -> 1 [labeldistance=2.5, labelangle=45, headlabel="True"] ;
2 [label="X[0] <= 2.5₩ngini = 0.4444₩nsamples = 24₩nvalue = [8, 16]"] ;
1 -> 2 ;
3 [label="gini = 0.0₩nsamples = 10₩nvalue = [0, 10]"] ;
2 -> 3 ;
4 [label="X[3] <= 20.825₩ngini = 0.4898₩nsamples = 14₩nvalue = [8, 6]"] ;
2 -> 4 ;
5 [label="gini = 0.0₩nsamples = 5₩nvalue = [0, 5]"] ;
4 -> 5 ;
6 [label="X[3] <= 31.3312₩ngini = 0.1975₩nsamples = 9₩nvalue = [8, 1]"] ;
4 -> 6 ;
7 [label="gini = 0.0₩nsamples = 5₩nvalue = [5, 0]"] ;
6 -> 7 ;
8 [label="X[2] <= 2.5₩ngini = 0.375₩nsamples = 4₩nvalue = [3, 1]"] ;
6 -> 8 ;
9 [label="gini = 0.0₩nsamples = 3₩nvalue = [3, 0]"] ;
8 -> 9 ;
10 [label="gini = 0.0₩nsamples = 1₩nvalue = [0, 1]"] ;
8 -> 10 ;
11 [label="X[0] <= 1.5₩ngini = 0.2798₩nsamples = 553₩nvalue = [460, 93]"] ;
1 -> 11 ;
12 [label="X[3] <= 26.1437₩ngini = 0.4599₩nsamples = 120₩nvalue = [77, 43]"] ;
11 -> 12 ;
13 [label="gini = 0.0₩nsamples = 10₩nvalue = [10, 0]"] ;
12 -> 13 ;
14 [label="X[2] <= 53.0₩ngini = 0.4762₩nsamples = 110₩nvalue = [67, 43]"] ;
12 -> 14 ;
15 [label="X[3] <= 27.1354₩ngini = 0.4949₩nsamples = 89₩nvalue = [49, 40]"] ;
14 -> 15 ;
16 [label="X[3] <= 26.4688₩ngini = 0.2604₩nsamples = 13₩nvalue = [2, 11]"] ;
```

Decision Tree - 도식화

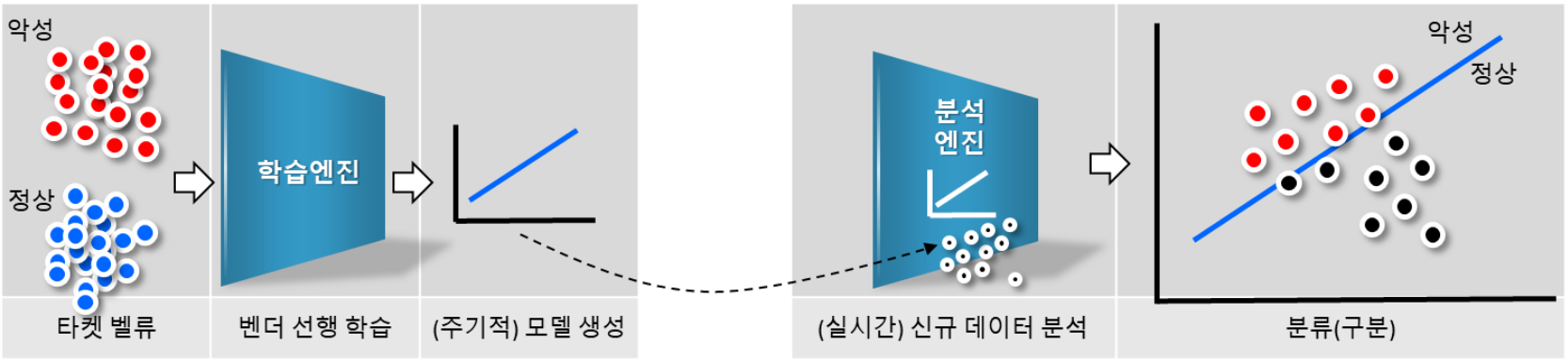


- 예측 모델-

2. Vectra社 Cognito – 인공지능 기술

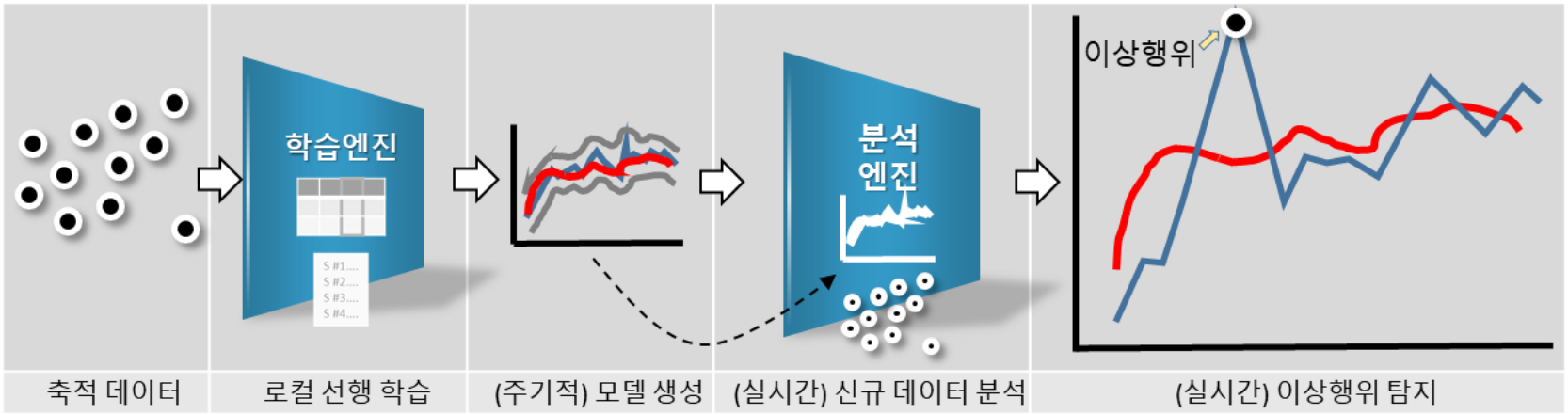
지도 학습 (Global Learning)

글로벌 러닝 – 분류(Classification)



비지도 학습 (Local Learning)

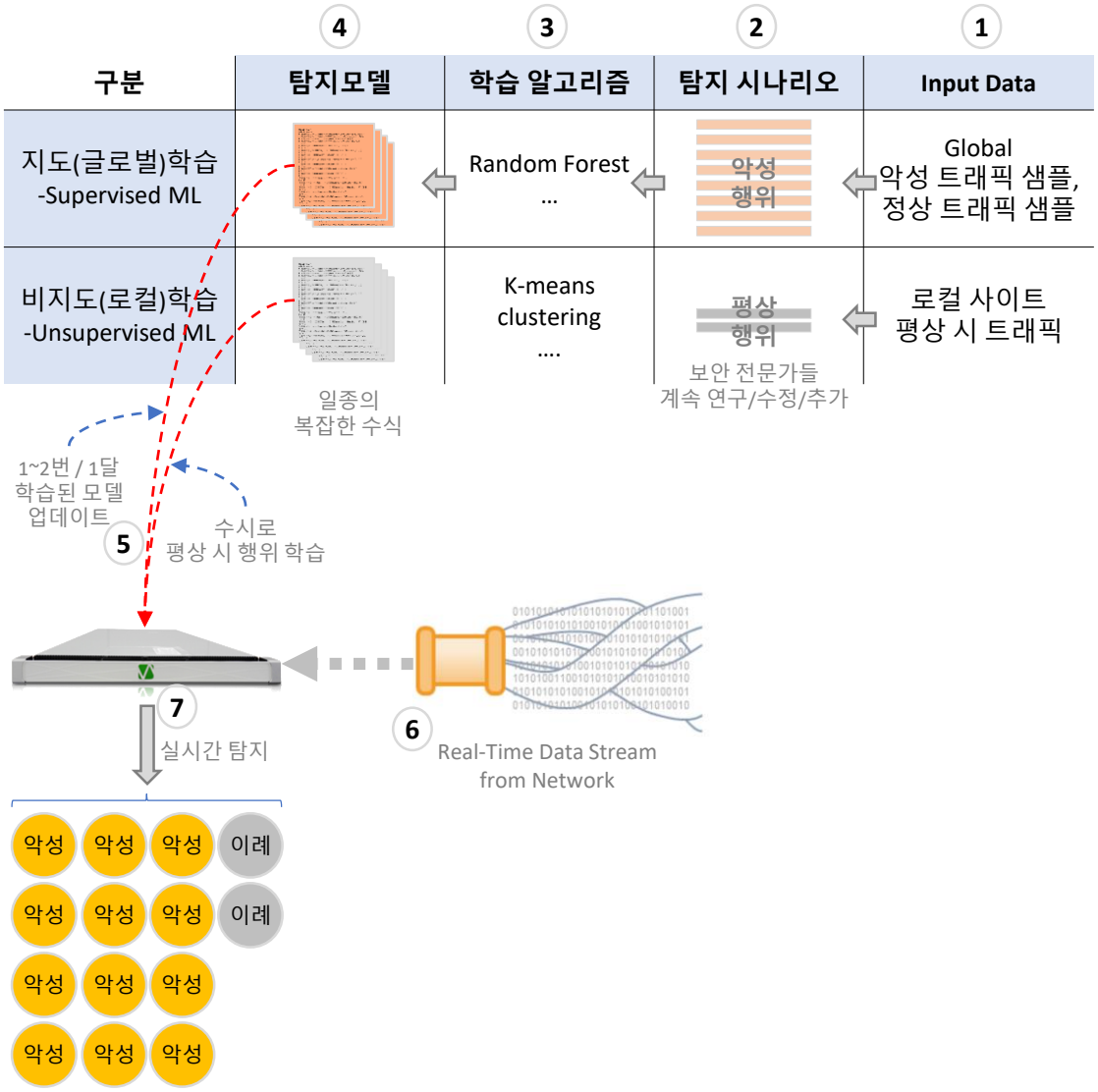
로컬 러닝 – 베이스라이닝 (Baselining)



2. Vectra社 Cognito – 인공지능 기술

지도 학습 (Global Learning)	(개발사에서) 분류, 구분	악성인 것을 알려줌	업무에 필요?
비지도 학습 (Local Learning)	(고객사에서) 집단 혹은 개별의 특성, 프로파일링	이례적인 것을 알려줌 튀는 행위인 것을 알려줌	악성인가? (해당 지식 필요) 업무에 필요한가?

2. Vectra社 Cognito – 인공지능 기술



① Input Data

학습용 data는 악성을 구분하기 위해 global data와 이례적인 것을 탐지하기 위한 고객 로컬 사이트 평상 data를 사용

② 탐지시나리오

C&C접속, Botnet 행위, 악성코드 확산, 정보유출과 같은 악성 행위 위주의 시나리오와 서버접속 행위, 외부 전송 행위 등 모니터링할 만한 평상행위 시나리오로 구분 ※Vectra는 악성 행위 위주의 시나리오가 더 많음

③ 학습 알고리즘

구분, 분류 중심의 지도학습 알고리즘과 특성화, 베이스라이닝 중심의 비지도학습 알고리즘 사용 ※딥러닝 알고리즘도 사용

④ 탐지 모델

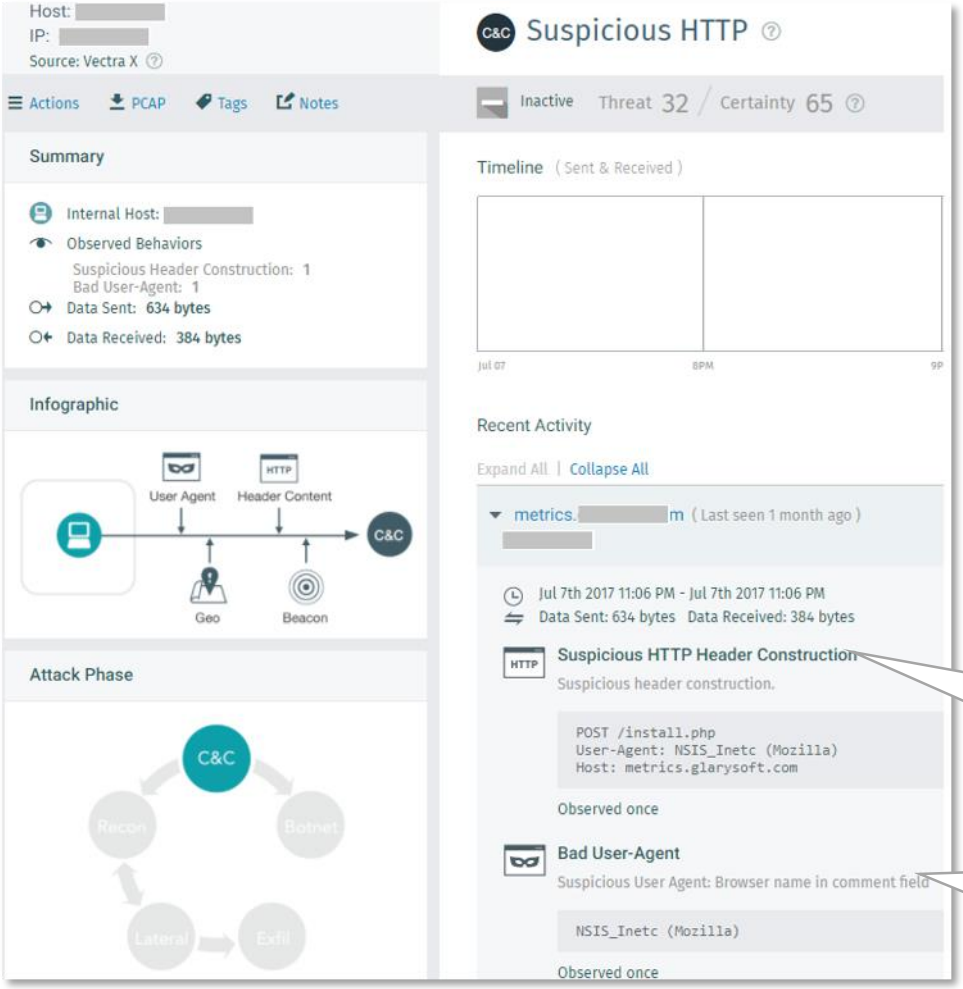
Packet header와 payload 전체를 보며 접속 빈도수, data volume, 접속 시도 지속성, 응답(성공)률 등 다양한 요소들을 탐지하는 복잡한 조건 및 수식

⑤⑥⑦

탐지모델 update는 글로벌 러닝(벤더러닝)은 1달에 1~2번 업데이트 되며 로컬학습은 평상시 행위를 학습하므로 수시로 업데이트 작업을 수행한다. 해당 탐지모델들로 실시간 트래픽에서 악성과 이례적인 것을 탐지한다.

2. Vectra社 Cognito – 인공지능 기술

글로벌 러닝 탐지모델 사례 in Vectra Cognito ➔ 악성행위를 탐지 (1)



C&C Suspicious HTTP

(1) 글로벌 러닝으로 C&C 접속 트래픽에서 각각의 속성별로 멀웨어의 특징을 지속적으로 학습함

(2) HTTP user agent, HTTP header, Beaconing, 서버의 위치 4가지 요소에서 나타나는 **멀웨어의 특징**들이 발견되는 경우 Threat과 Certainty가 자동 분석되어 관리 및 표출됨

(3) Suspicious HTTP의 스코어링

① Threat 점수는 C&C 서버를 찾고 접속하려는 비코닝 (Beaconing) 행위가 key, 4가지 요소가 발견되면 될수록 점수 상향 조정

② Certainty 점수는 HTTP agent와 HTTP heade가 key, 여러 개의 C&C 접속 행위가 많을 수록 점수 상향 조정

HTTP 헤더 구조(presence, absence, order)가 의심스러움

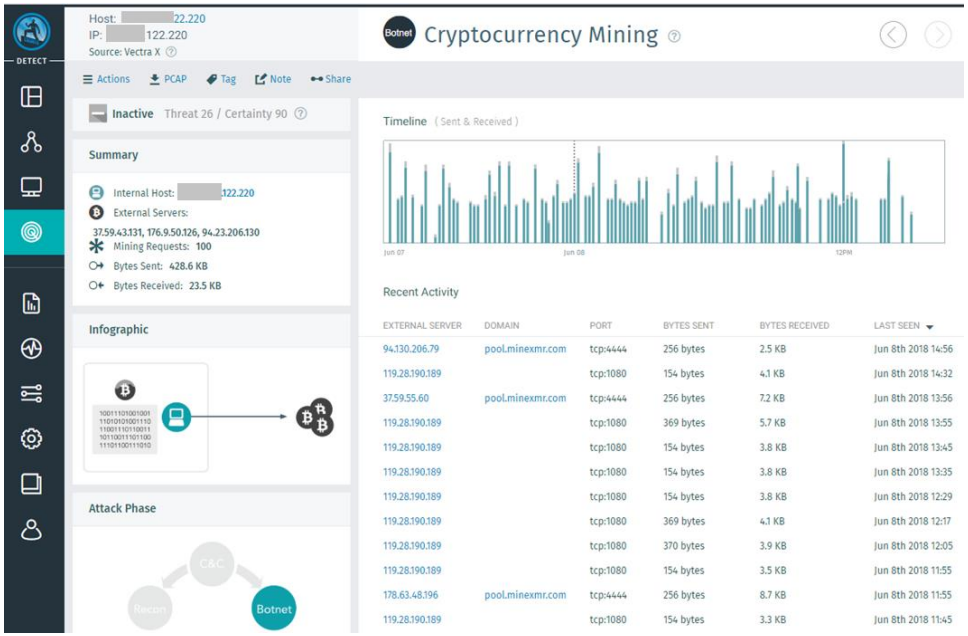
Comment Field에 User agent Browser name이 기입되어 의심스러움

VECTRA

Goodus
Breathing Life into Technology

2. Vectra社 Cognito – 인공지능 기술

글로벌 러닝 탐지모델 사례 in Vectra Cognito ➔ 악성행위를 탐지 (2)



[지도학습에 의해 정의된 탐지모델로 탐지된 "가상화폐 채굴 " 봇넷 행위]

Bot Cryptocurrency Mining

✓ 마이닝 프로토콜을 구별하는 탐지모델을 글로벌러닝에 의해서 정의 한 후 실시간 탐지한 결과

✓ 만약 이를 비지도학습(이례적인 것)에 의해서 탐지한다면

- 이례적인 포트 4444/tcp 사용
- 한 밤중에 인터넷 접속을 한 특이한 행동
- 이례적인 URL 접속

등의 이례적인 사항들을 뽑아내어 제공할 것입니다. (관리자는 제공된 결과로 추가 분석 필요)

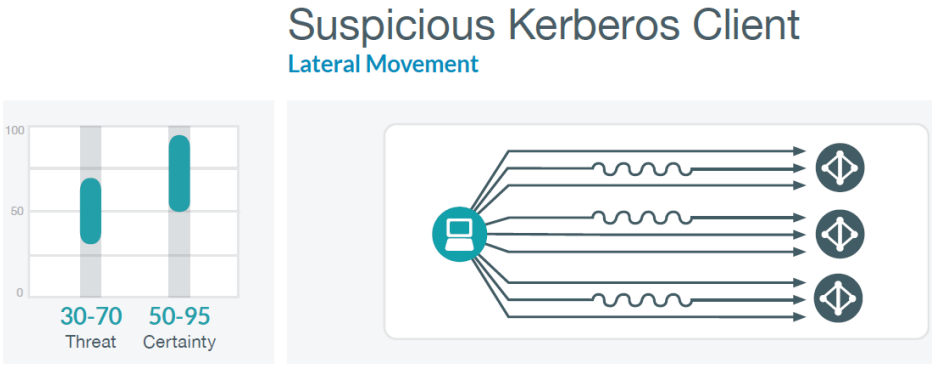
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"QQx64","pass":"x","agent":"XMRig/2.5.2 (Windows NT 6.0; Win64; x64) libuv/1.19.2 gcc/7.3.0"}}
{"id":1,"jsonrpc":"2.0","result":{"id":"1c922965-d4ec-48db-9625-7e8bce687669","job":{"blob":"0707dda8e3d805e1f4e28b8a3b3945c5552d245b286ceb24bc6e98303b649bd125eae5166c3f76000000154f75eb699a4e40af90727d5cc8275a7f87b30772a5a683a8cadcea6eda5437f30f","job_id":"5868150","target":"cf8b0000","coin":"XMR","variant":-1},"extensions":["nicehash"],"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":{"blob":"070799a9e3d805e1f4e28b8a3b3945c5552d245b286ceb24bc6e98303b649bd125eae5166c3f7600000015f4a0b486805232d3872a75664b246e56f83a5c97ec367318b32a2ef8897f53bb0f","job_id":"5869150","target":"cf8b0000","coin":"XMR","variant":-1}}
{"jsonrpc":"2.0","method":"job","params":{"blob":"0707d5a9e3d805e1f4e28b8a3b3945c5552d245b286ceb24bc6e98303b649bd125eae5166c3f7600000001549def6a690533b31c1de8c778e4e3bf52eb1eb7c43f81fb748896003c89429cf0f","job_id":"5870150","target":"cf8b0000","coin":"XMR","variant":-1}}
{"jsonrpc":"2.0","method":"job","params":{"blob":"070791aae3d805e1f4e28b8a3b3945c5552d245b286ceb24bc6e98303b649bd125eae5166c3f76000000155df9f02a8b2212092813a10200f0a70d11e899659fa3eff6ece113ecb989edd60f","job_id":"5871150","target":"cf8b0000","coin":"XMR","variant":-1}}
{"jsonrpc":"2.0","method":"job","params":{"blob":"0707cdaae3d805e1f4e28b8a3b3945c5552d245b286ceb24bc6e98303b649bd125eae5166c3f7600000015d0e541a1889a0a9c5d

VECTRA

Goodus
Breathing Life into Technology

2. Vectra社 Cognito – 인공지능 기술

로컬 러닝 탐지모델 사례 in Vectra Cognito ➔ 이례적인 행위를 탐지 (1)

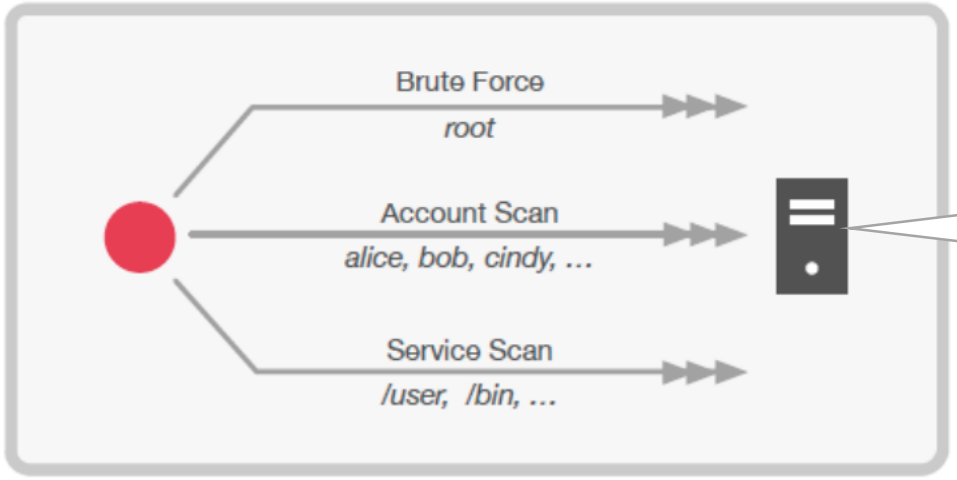


Lateral Suspicious Kerberos Client

(1)로컬 러닝으로 학습된 베이스라인과 비교하여 이례적인 Kerberos 접속 행위를 탐지한다.

①Threat 점수는 접속 횟수의 편차(Deviation)와 접속 유형의 강도(Strength), 이례적인 접속 서버 IP, 이례적인 로그인 접속 수 또는 서비스 조회 수

②Certainty 점수는 베이스라인으로부터 편차의 강도



감염 된 PC에서 계정 탈취를 위한 행위, 계정 탈취 후의 일련의 행위를 탐지

2. Vectra社 Cognito – 인공지능 기술

로컬 러닝 탐지모델 사례 in Vectra Cognito ➔ 이례적인 행위를 탐지 (2)

[비지도학습에 의해 정의된 탐지모델로 탐지된 "의심스러운 관리자 " 행위]

Lateral Suspicious Admin

- ✓ 관리용 프로토콜은 RDP(터미널 접속), SSH, Telnet 등 존재
- ✓ Vectra Cognito는 평소에 접속하는 관리자 접속 세션을 학습(기억)하고 있음
- ✓ 왼쪽 사례는 어떤 사용자가 172.19.53.21로 접속해왔던 키보드 타입이 있었는데 어느 날 평소에 보이지 않았던 keyboard와 다른 타입의 값이 보였고 이런 현상은 정상적인 터미널접속 프로그램이 아닌 임의의 프로그램(악성프로그램)이 사용자 모르게 접속한 행위로 보일 수 있다는 것을 알려주는 사례
  - 2017.08.25 ~ 2017.09.08 기간 동안 학습한 키보드 레이아웃 값 : Unknown – 3758162962
  - 2017.09.21 15:28에 접속했을 때 이례적인 키보드 레이아웃 값 : encrypted keyboard - 0

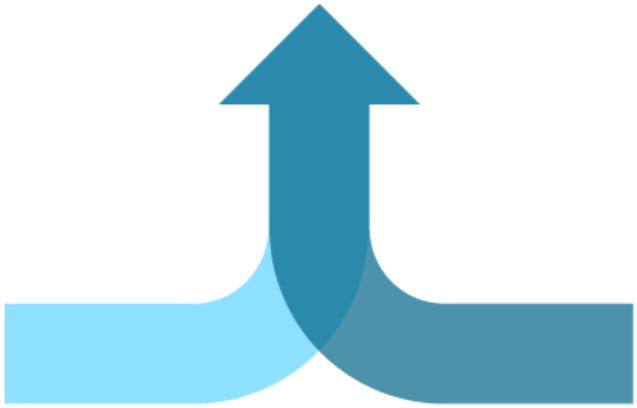
터미널 접속 관련 packet payload가 인코딩되어있기 때문에 서버 접속 후 행위가 악성인지 아닌지 어렵습니다. Vectra cognito는 이런 경우 Packet의 payload의 보이는(visible) 영역 또는 packet들의 조합을 보고 평상시 행위를 학습(기억)하고 있다가 이례적인 것을 탐지하여 악성 행위를 탐지

2. Vectra社 Cognito – 인공지능 기술

Attacker behaviors: unifying data science & security research

Attacker Behavior models

- 공격자가 반드시 해야만 하는 것들을 탐지(High-fidelity)
- No-Signature : 알려진 공격과 알려지지 않은 공격 탐지



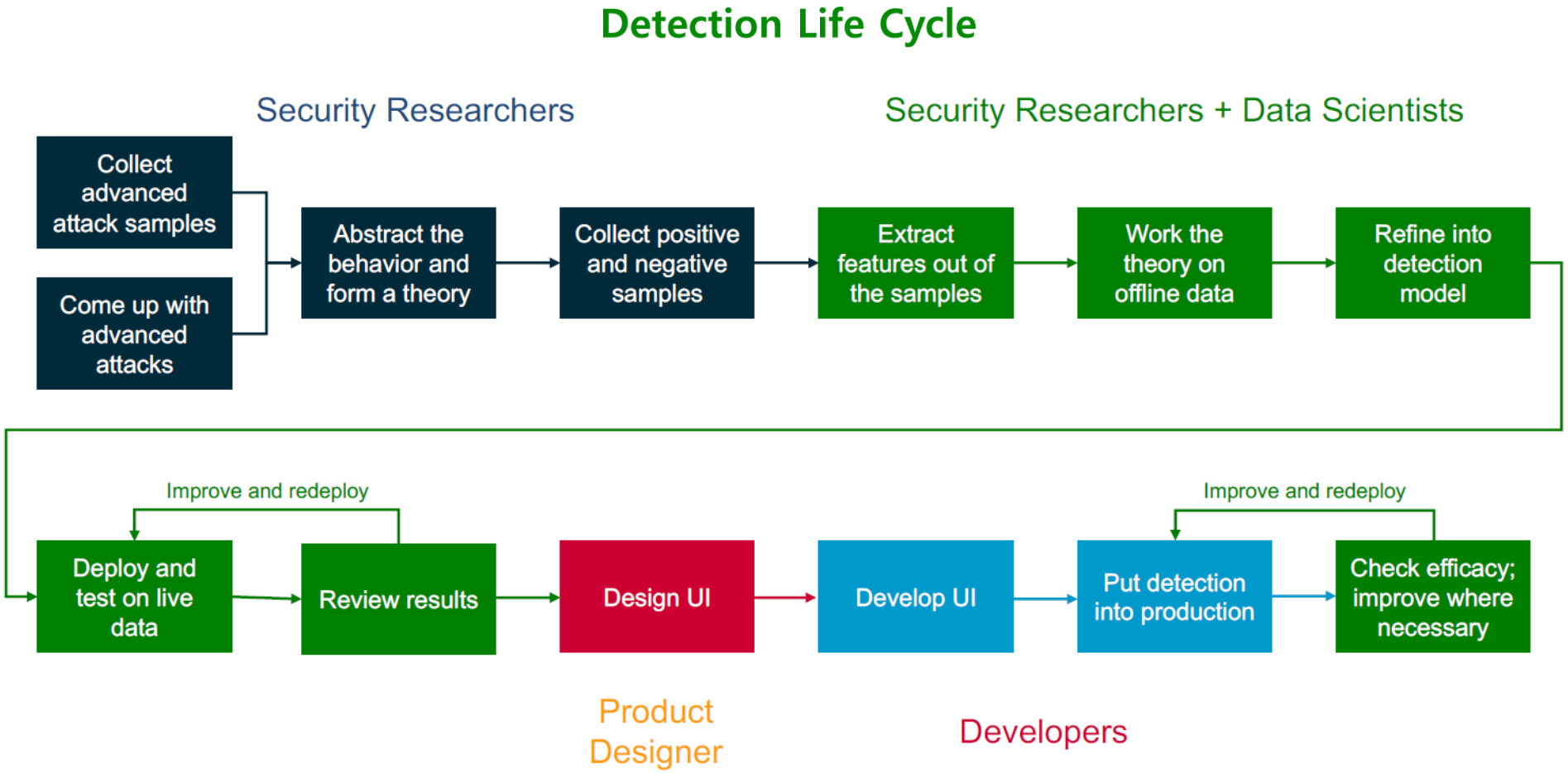
Security Research

- 기본적인 공격자 행동을 식별, 우선 순위 지정 및 특성화
- 모델 검증

Data Science

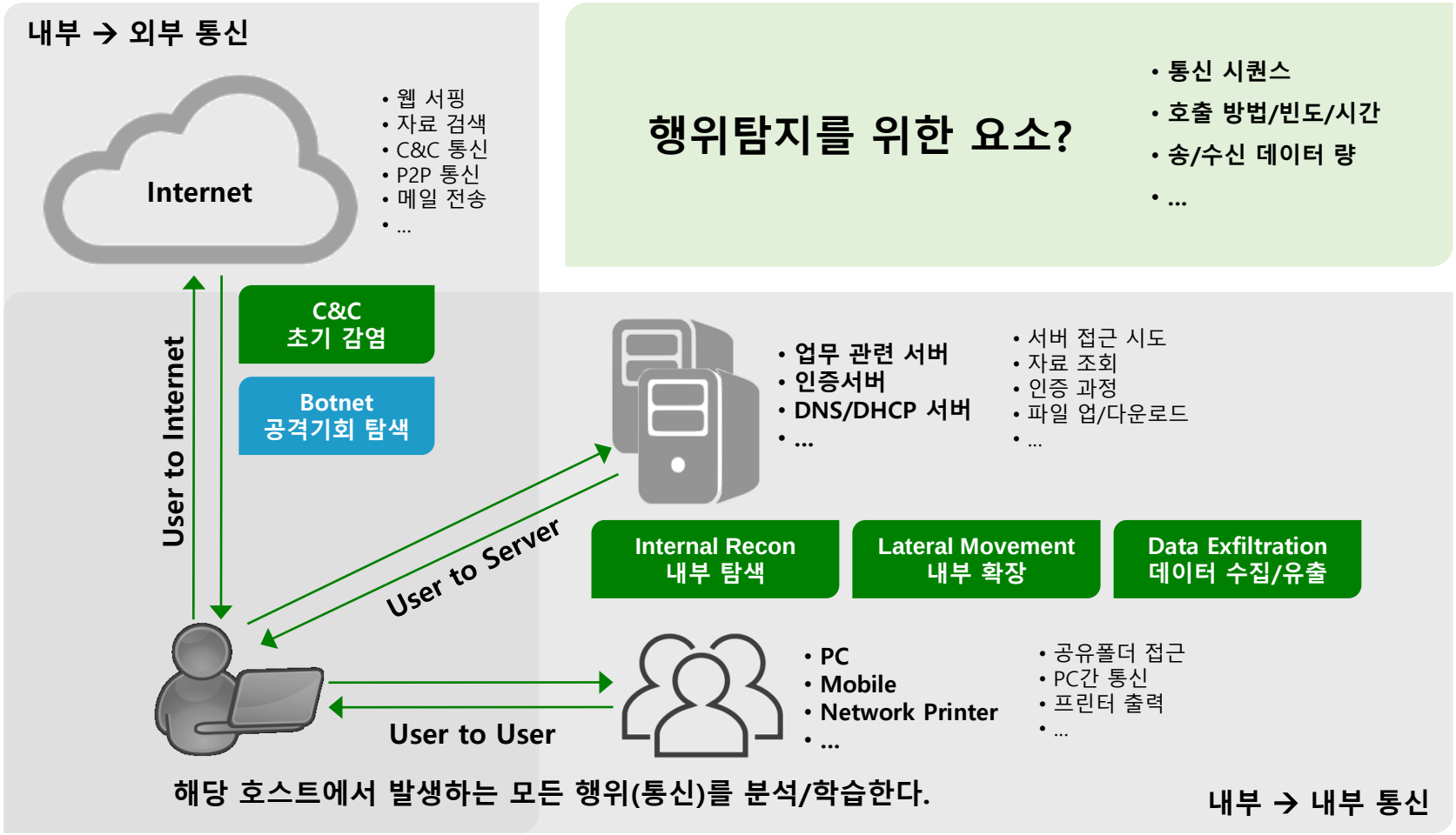
- 행동을 식별하기위한 최선의 방법 결정
- 모델 개발 및 조정

2. Vectra社 Cognito – 인공지능 기술



3. Vectra社 Cognito - Cyber Kill Chain

탐지 방법

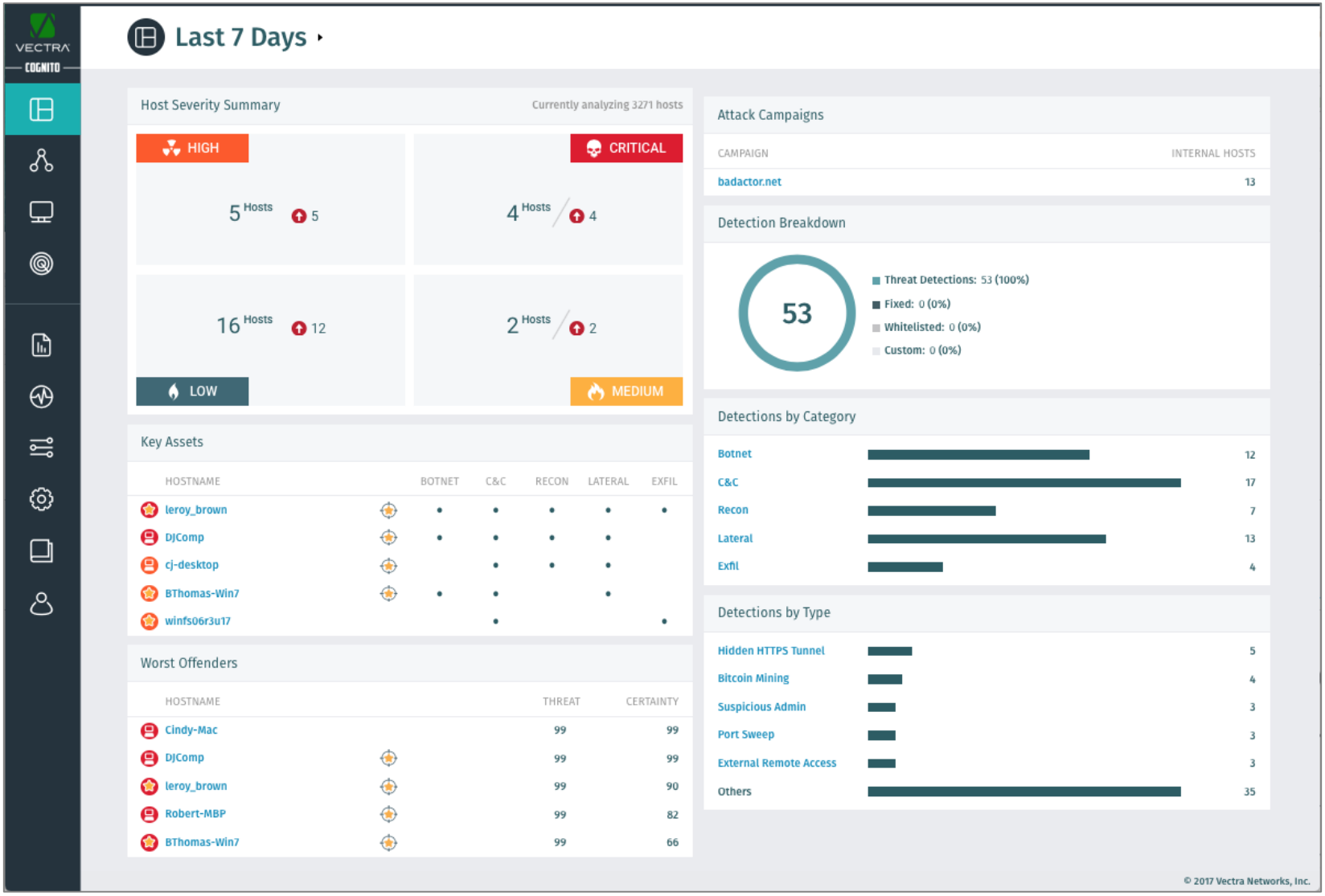


Cyber Kill-Chain ! + 행위(Behaviors)기반 탐지 !

VECTRA

Goodus
Breathing Life into Technology

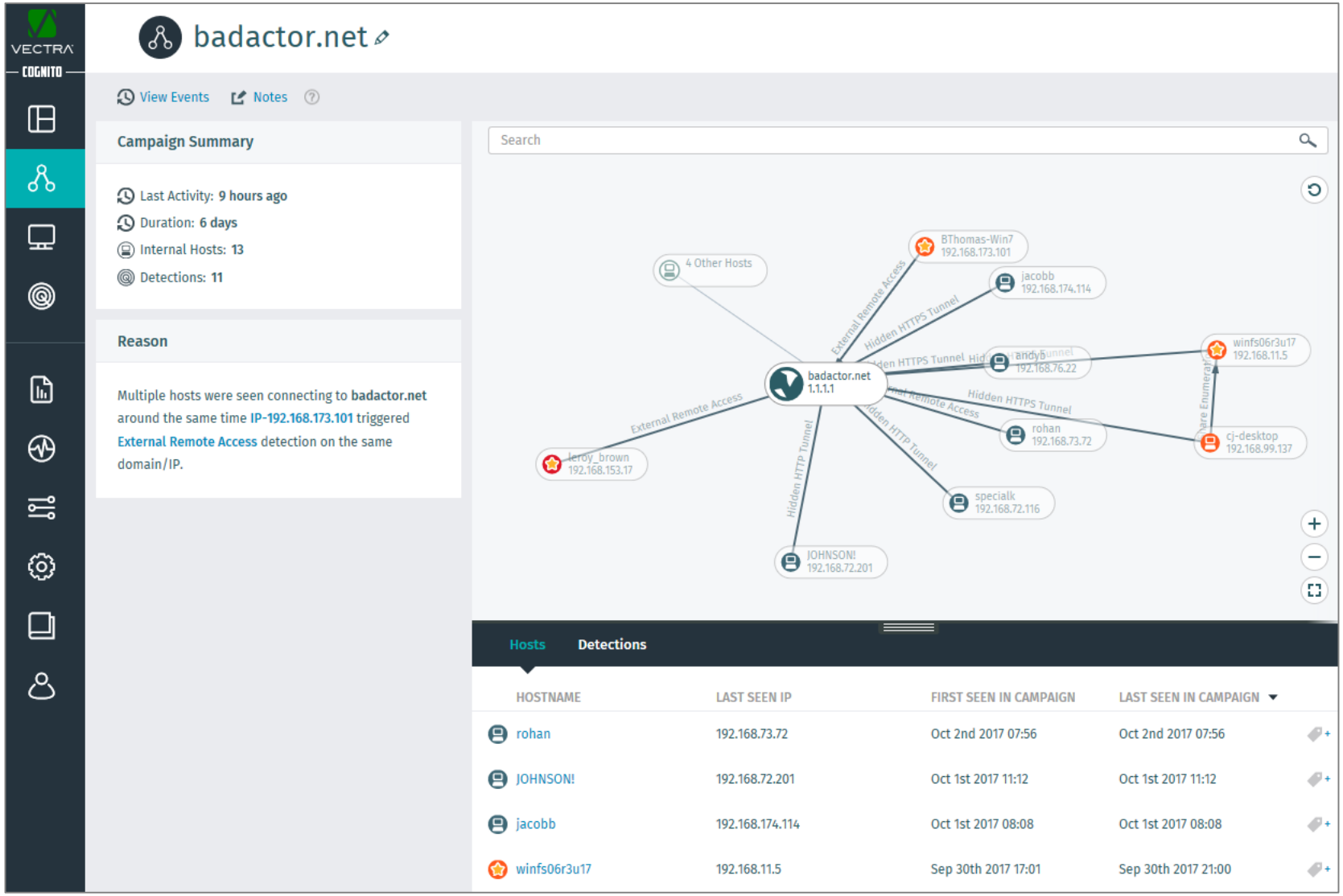
4. Vectra社 Cognito – 내부 가시성



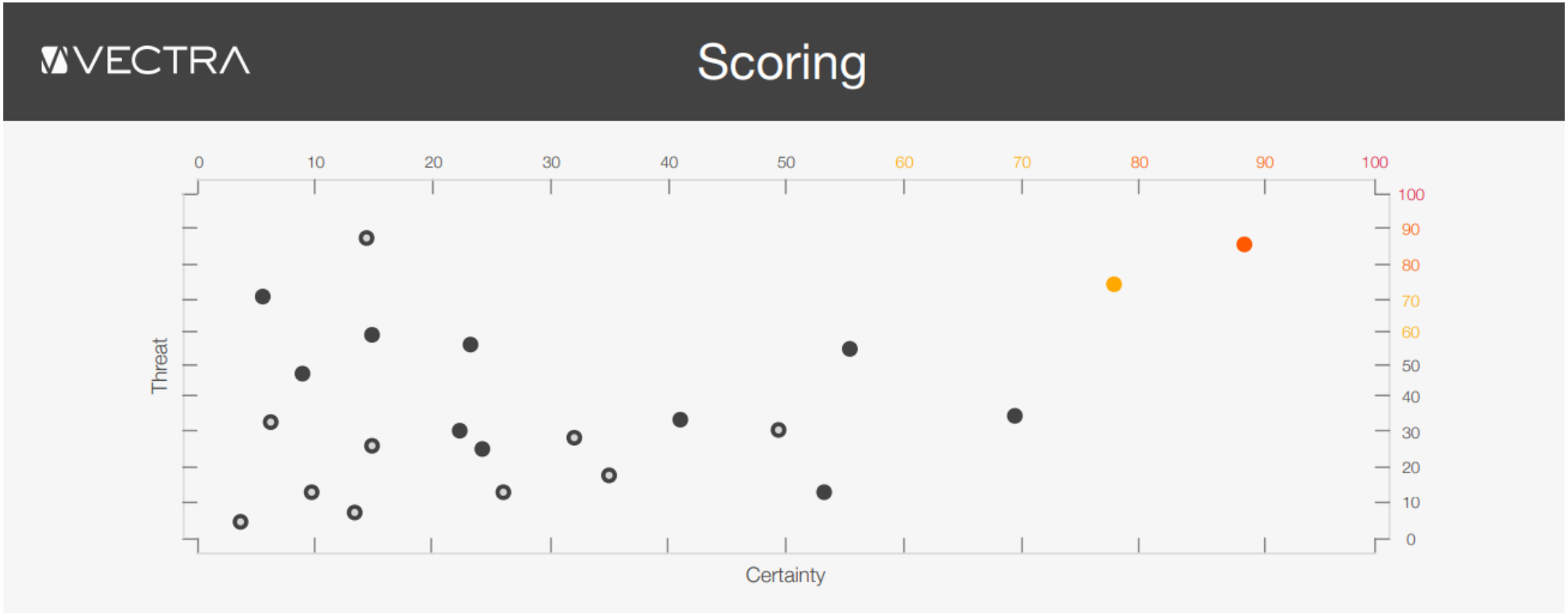
VECTRA

Goodus
Breathing Life into Technology

4. Vectra社 Cognito – 내부 가시성



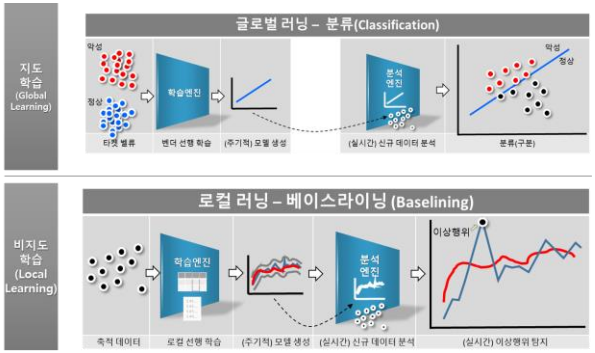
5. Vectra社 Cognito – 실시간 자동 상관분석



- 관리자의 숫자적인 정의 값을 수정/관리할 필요 없음 (중요 호스트 지정 및 예외 처리로 대신)
- 2차원 메트릭스 구성으로 가장 먼저 처리해야 할 것과 나중에 처리할 것을 구분
- 위협 발생의 반복성과 위협들의 조합으로 활동이 없으면 점수는 0으로 감소하여 기본 UI에서 보이지 않음

→ 관리자 공수(workload)가 준다.
(탐지 모델의 튜닝 공수)

6. Vectra社 Cognito - 특장점

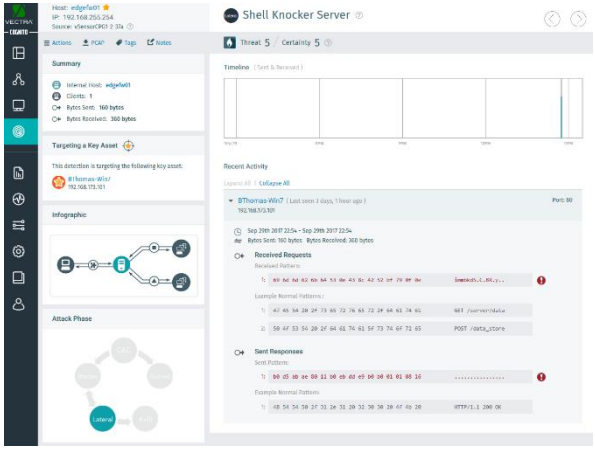


→ 글로벌러닝 (악성 구별)

→ 로컬러닝 (튀는 것)

→ 과탐이 적다

→ 분석 시간이 줄어든다

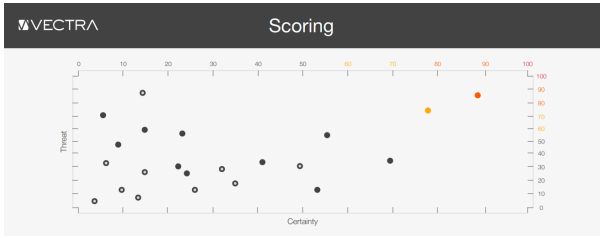


→ 1차 정리, 요약된 분석 화면

→ 관련 정보가 한 눈에

→ 분석 시간이 줄어든다

→ 비전문가도 사용하고 분석할 수 있다



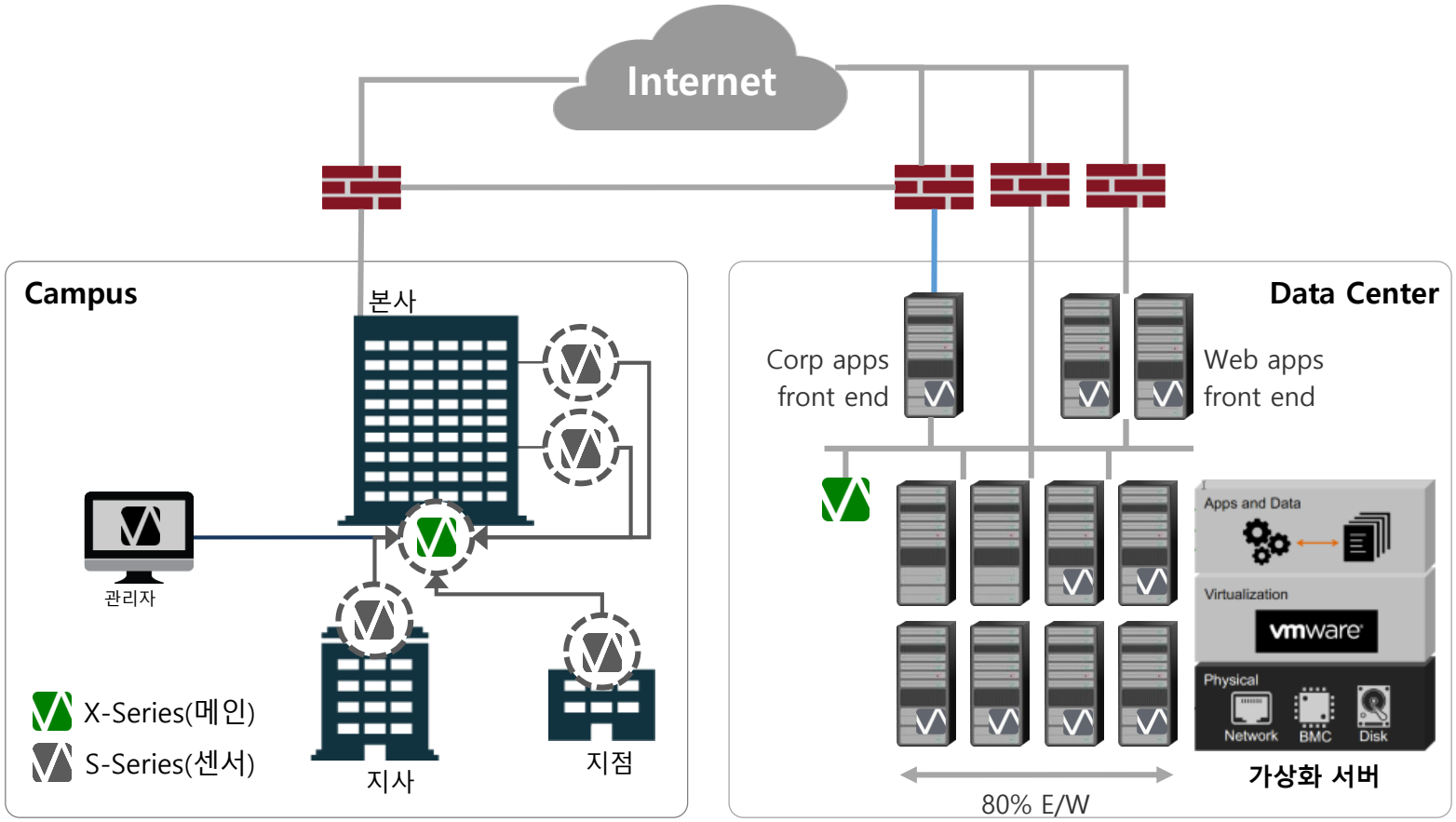
→ 자동 실시간 상관분석에 따른 점수 관리

→ 탐지모델 튜닝 X

→ 관리자 공수(workload)가 준다

8. Vectra社 Cognito – 장비구성

구성방안



기업 전체 및 가상화 네트워크 지원

메인 백본 스위치가 위치하는 곳에 Vectra 메인장비(X-Series)를 설치하고, 본사의 주요 내부 트래픽을 수집 할 수 있는 곳 및 지사, 지점 등의 주요 위치에 센서(S-series)를 설치하여 메인 장비 및 센서에서 수집된 네트워크 트래픽을 메인 장비에서 통합 분석합니다.

9. Vectra社 Cognito – 결론

기술적 타당성

백신, IPS, Sandbox 기반 APT 대응장비 등이 있어도 여전히 침해사고는 계속 일어났습니다. 사고 발견 또한 늦습니다. 그 이유는 시그니처방식, 네트워크 인입구간의 편중보안, 샌드박스 탐지방식의 맹신등에 있습니다. 지능형위협공격은 100% 막을 수 없습니다. 그리고 특정 공격단계만 보아서도 안됩니다. **하이브리드 머신러닝 기반과 통합 인털리전스 기술을 제공하는 벡트라는 기존 탐지 방식을 보완할 수 있고 기존 솔루션과도 훌륭하게 연동이 가능합니다. 벡트라는 이미 세계적으로 유수의 고객이 사용중에 있어 기술적 우수성이 입증된 기술과 솔루션을 제시합니다.**

관리, 투자 타당성

벡트라는 화려한 UI나 분석 전문가를 위한 상세한 포렌식로그 부분에는 약합니다. 하지만, 부족한 보안전문가 인력, 신속한 조치가 필요한 경우에 최적화된 솔루션입니다. 더구나 **내부 보안에 상대적으로 취약한 부분과 조직 내에 이미 감염되어 있는 호스트들을 파악하는 문제는 이제 현실로 다가오는 필수적인 보안조치입니다. 벡트라의 기술과 보안 커버리지 영역은 이때까지의 그 어느 솔루션과도 중복되지 않으며 독창적이고 입증된 솔루션입니다. 보안의 보호 대상은 내부에 있습니다. 상대적으로 보안의 사각지대였던 내부 보안의 중요성을 인식하시고 투자에 주저함이 없기를 바랍니다.**

Ⅰ. 제안 개요

Ⅱ. 제품 소개

Ⅲ. 첨부자료

1. 도입사례

기존보안 인프라

- **팔로알토** NGFW, **시스코 소스파이어** IPS, HP **아크사이트** SIEM **외**

요구사항

- **비정상 트래픽 및 공격 징후를 자동 탐지**
- **선제대응 환경 구축**
- **침투한 공격자의 내부 네트워크 활동을 탐지하여 네트워크 가시성 확보.**

도입효과

- **서버에서 "Automated Replication"공격과 내부 데이터를 수집하고 있는 여러 호스트를 탐지**
- **서버에서 IPS가 탐지하지 못한 악성 도메인 "Suspect Domain"을 접속하는 행위 탐지**

Microsoft

1. 도입사례

- 경계 보안 방어를 위한 F/W, IPS/IDS 와 엔드포인트 보호를 위한 안티 바이러스 솔루션 외

- 경계선 방어 단계와 사후 분석 단계의 Security Gap을 최소화
- 내부 네트워크 내에서 활동중인 위협을 탐지하는데 소요되는 시간 단축
- 타겟 공격 및 관련된 위협으로 인한 피해 최소화

- 기존의 수동적이거나 시간 소모적인 위협 관리 작업 완전히 자동화,
- 실시간 위협을 식별, 위협 우선순위를 제공으로 조치와 관련된 의사결정 시간 단축
- 인력 추가 투입 없이 전문 보안 분석가 업무 자동 수행

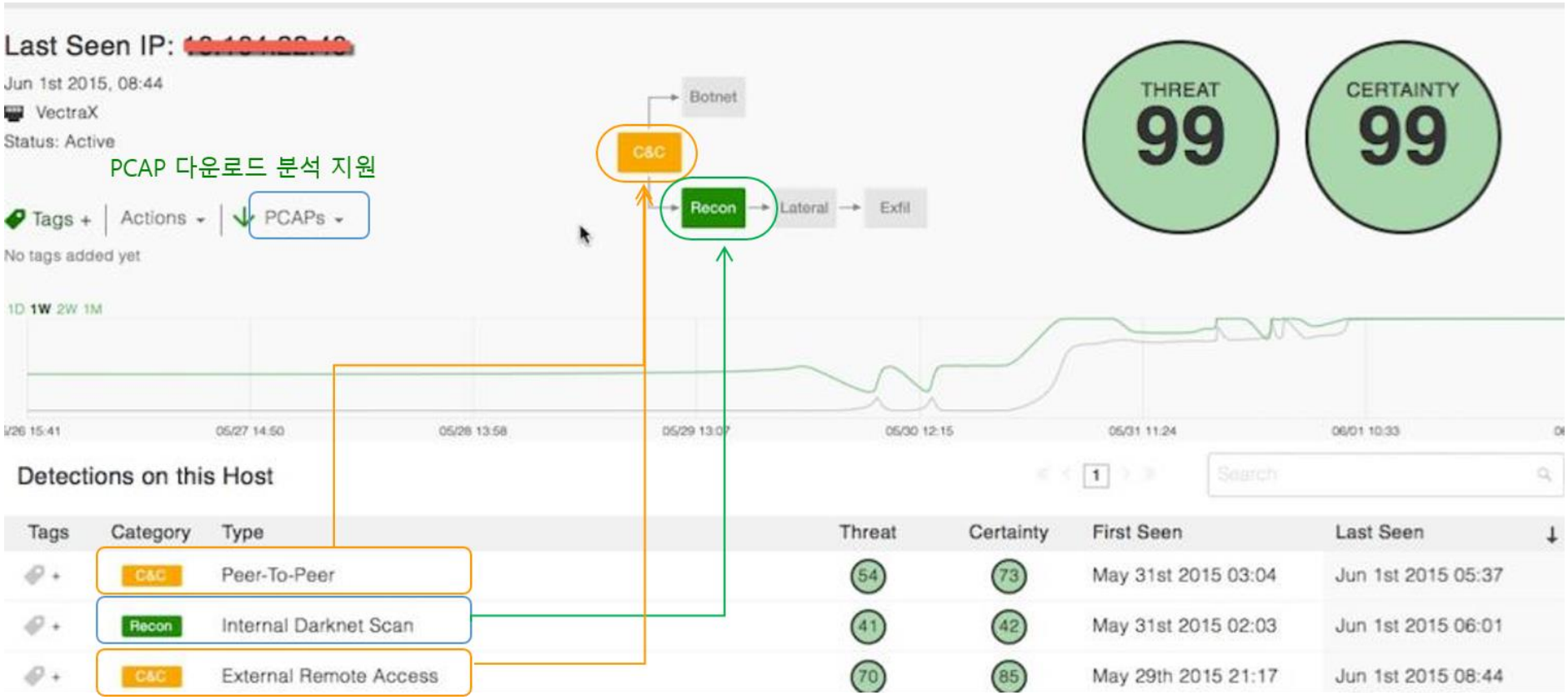
Jackson HEALTH SYSTEM
통합 의료 정보 서비스 제공

VECTRA

Goodus
Breathing Life into Technology

3. 탐지 사례 (내부 스캐닝, 원격접속)

내부 침투 후 원격접속으로 감염된 호스트에 접속하여 내부 호스트 또는 네트워크를 분석하는 전체 스캔, 그리고 탐지하기 어려운 P2P 통신 또는 암호 통신으로 데이터를 외부로 유출하는 공격 탐지

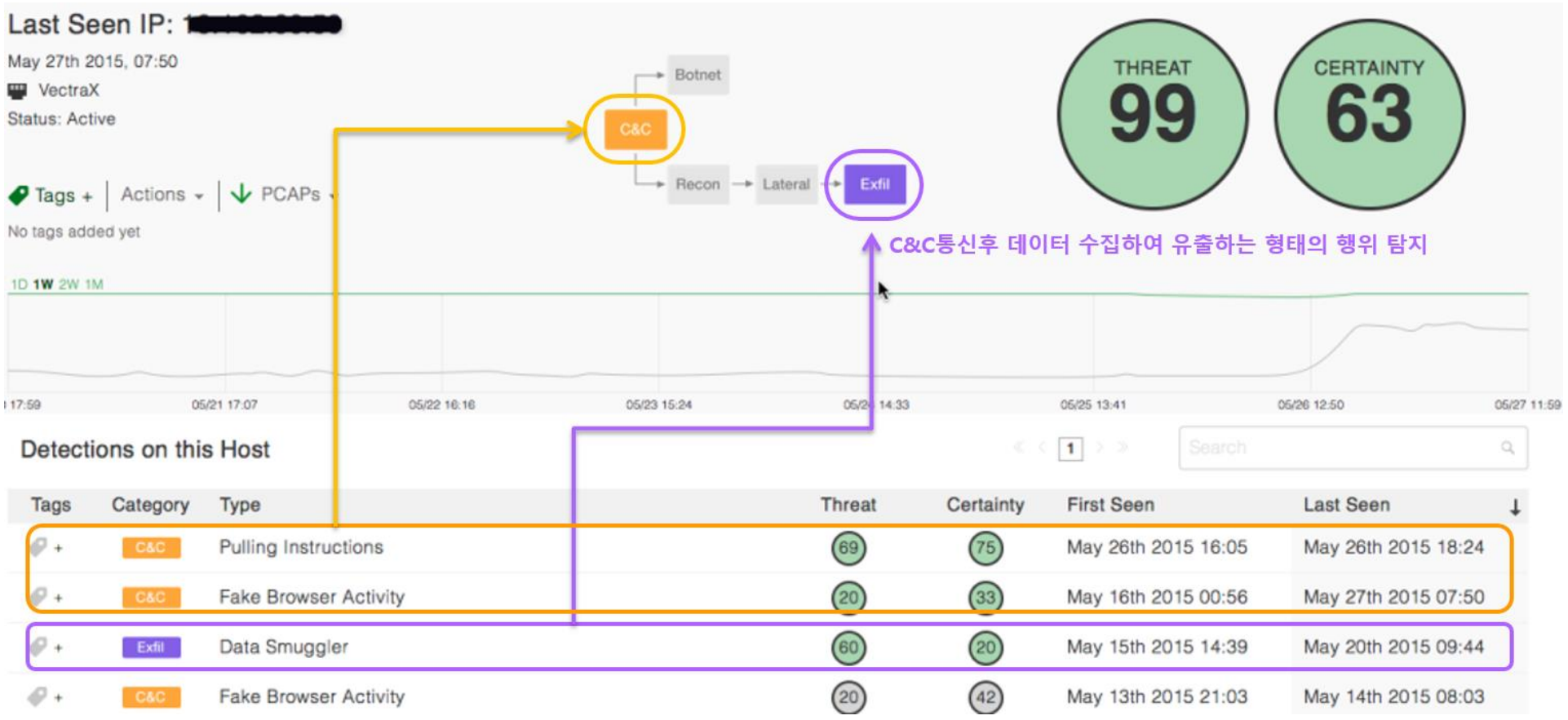


VECTRA

Goodus
Breathing Life into Technology

3. 탐지 사례 (데이터 유출)

내부에 침투된 호스트에서 데이터가 외부로 전송되는 데이터 유출 탐지.

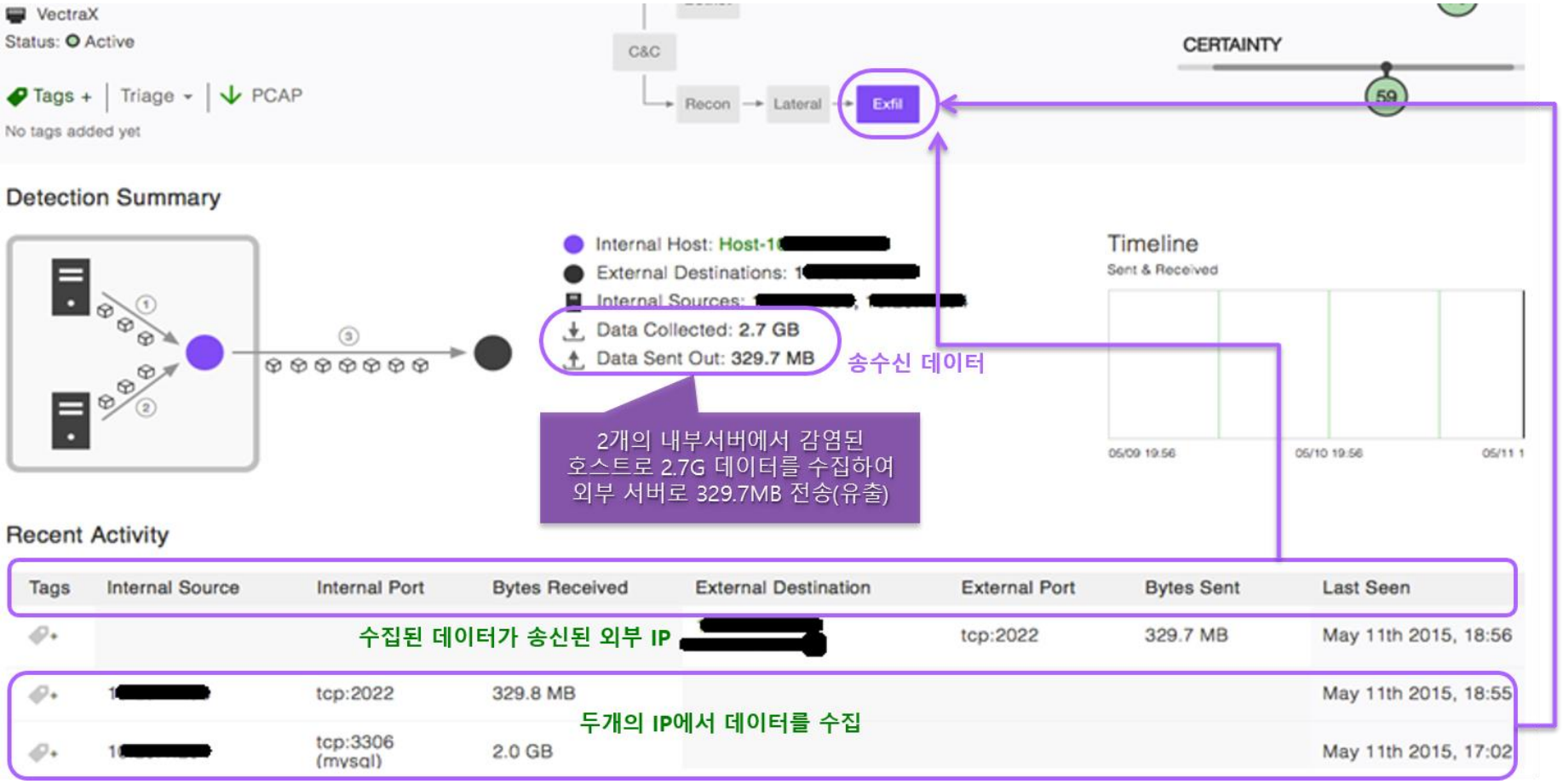


VECTRA

Goodus
Breathing Life into Technology

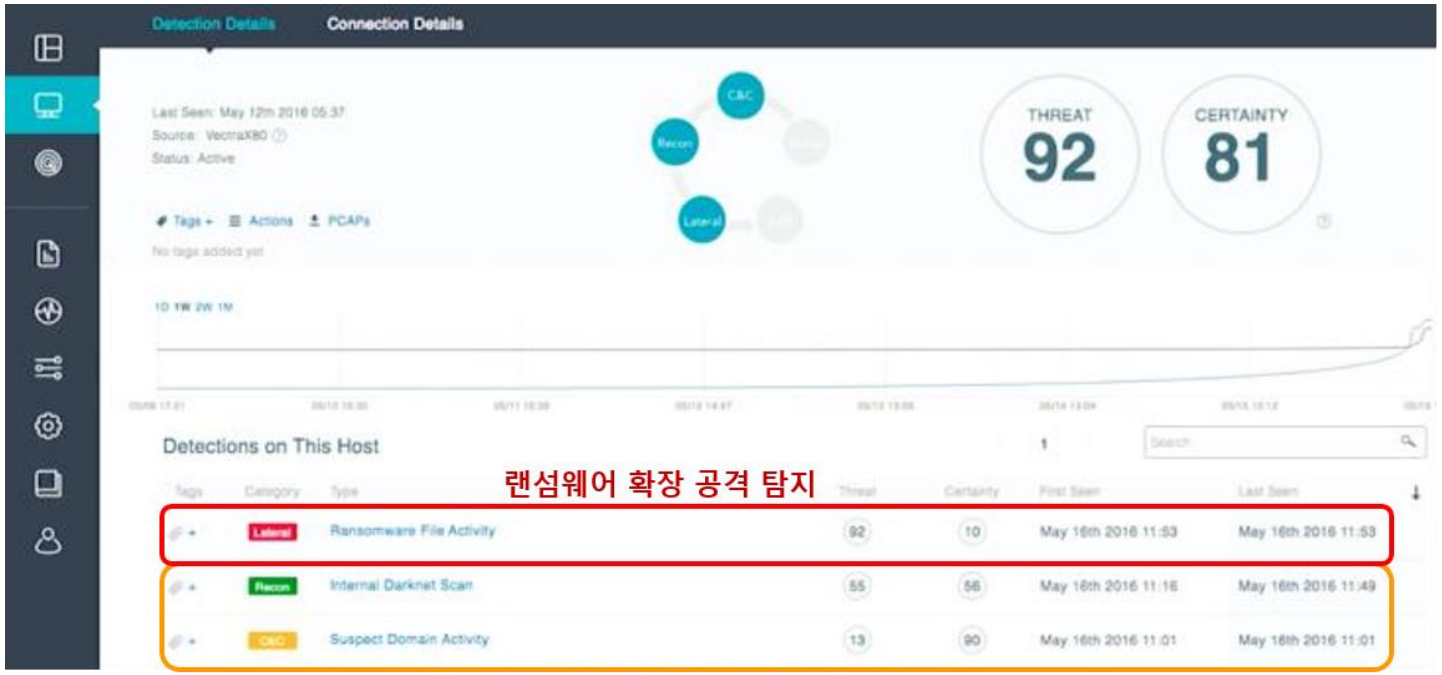
3. 탐지 사례 (데이터 유출)

내부 두개의 호스트에서 수집된 데이터의 외부 유출을 탐지하였고 상세 내역 제공.



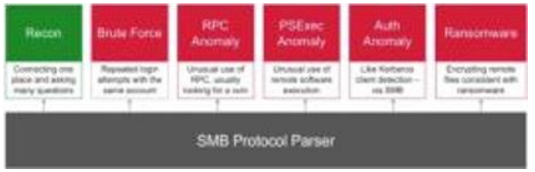
3. 탐지 사례 (랜섬웨어)

랜섬웨어도 다른 초기감염 => 감염 호스트 데이터암호화 => 확장 공격 (공유폴더 검색 및 접속 시도 등)의 형태로 진행됨으로 감염된 호스트를 통해 내부 네트워크 공유 폴더 등의 자료가 암호화 되기 전에 탐지



랜섬웨어 행위

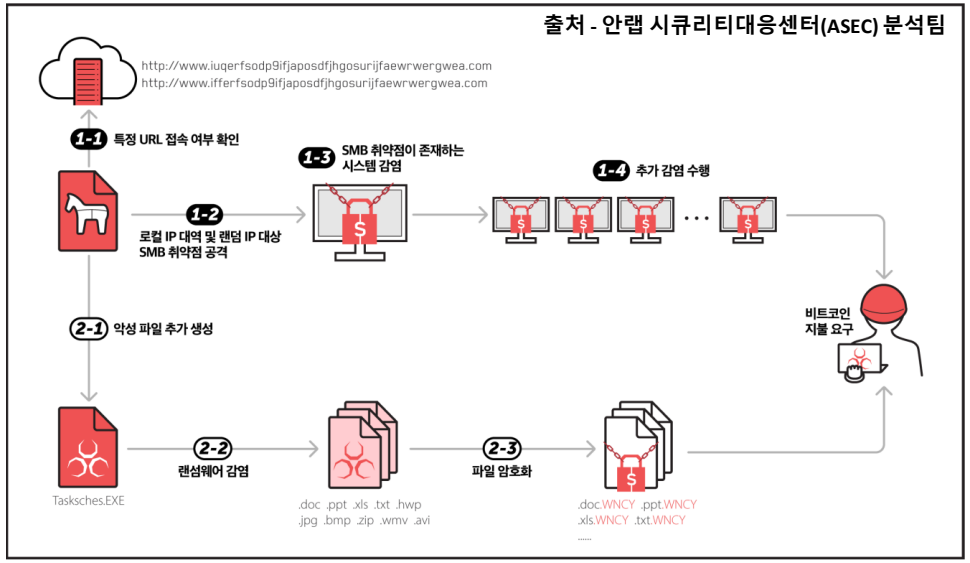
프로토콜 및 행위 분석



VECTRA

Goodus
Breathing Life into Technology

3. 탐지 사례 (랜섬웨어-워너크라이)

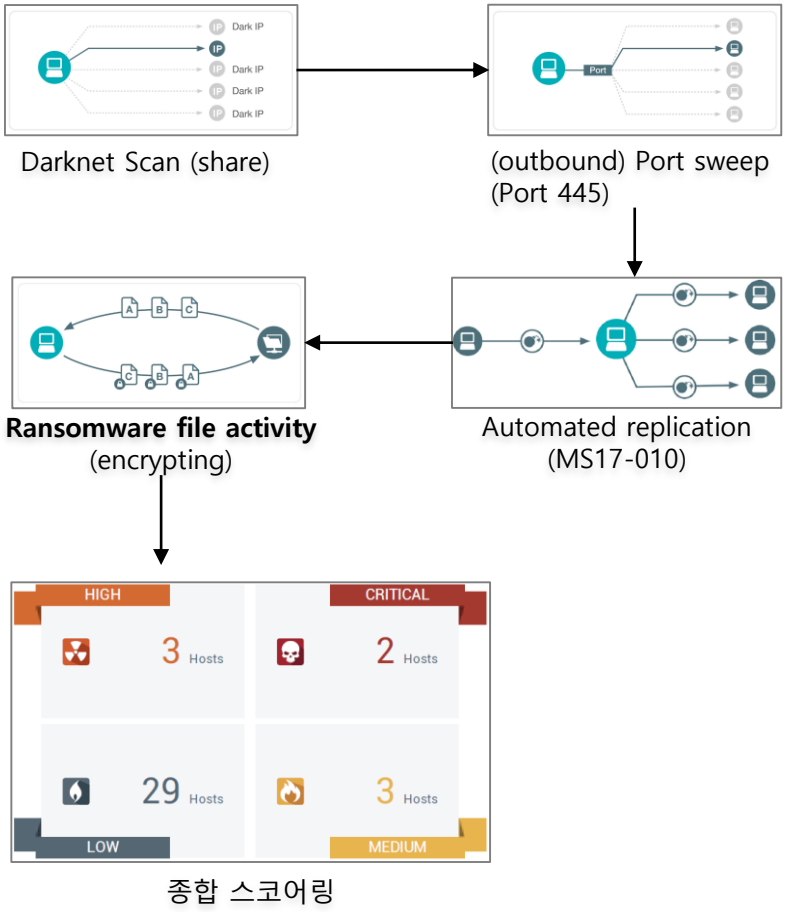


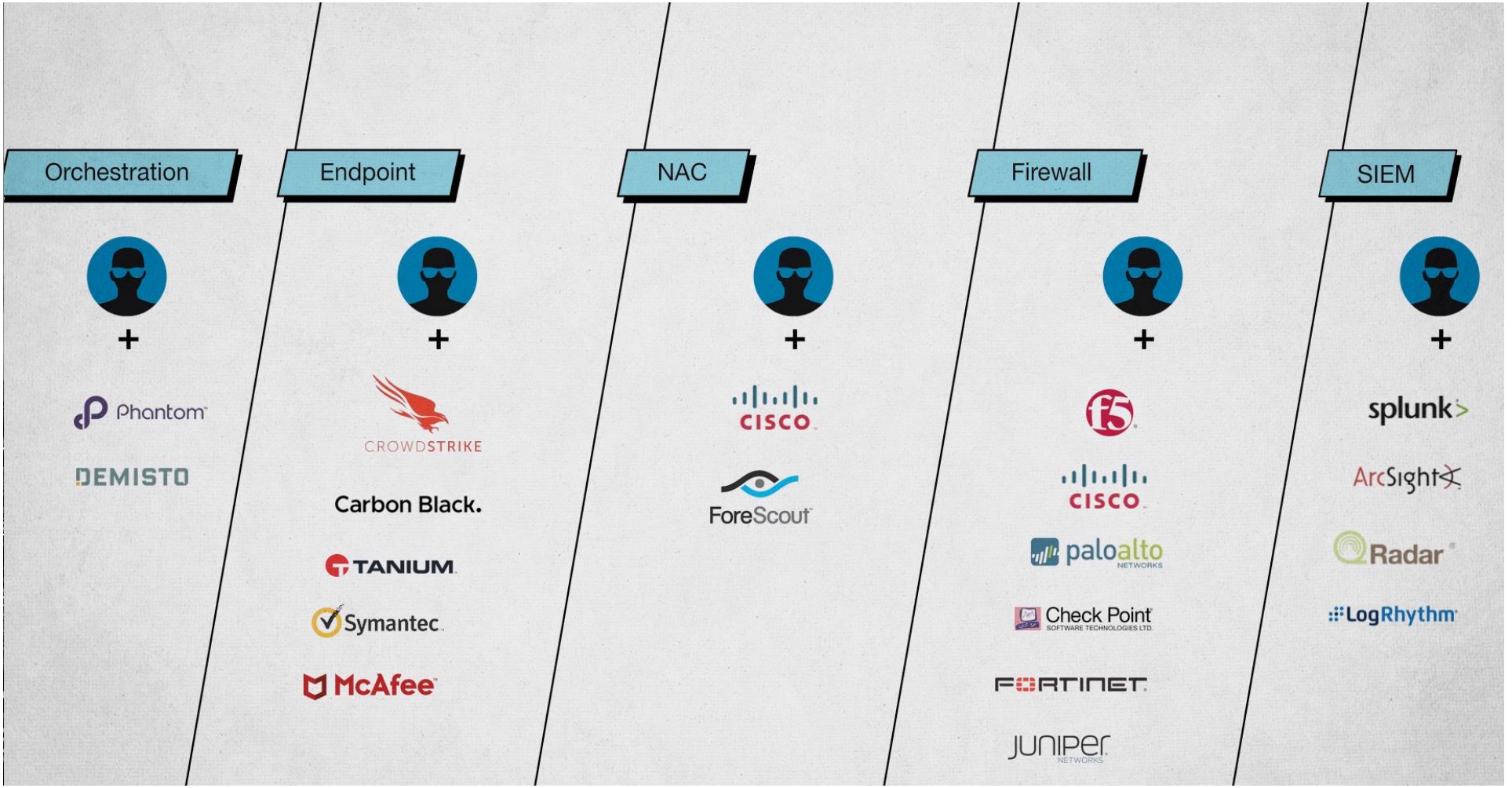
1-1 감염 – 특정 URL 접속

- http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

감염된 PC 환경이 가상이 아닌 실제인지 확인하는 **과정을 위해 접속에 실패할 경우에만 다음 동작을 수행**

1-2,3,4 측면 전파 (Lateral Movement) –SMB 취약점 이용 전파




Orchestration
+
Phantom
DEMISTO
Endpoint
+
CROWDSTRIKE
Carbon Black.
TANIUM
Symantec
McAfee
NAC
+
CISCO
ForeScout
Firewall
+
f5
CISCO
paloalto NETWORKS
Check Point SOFTWARE TECHNOLOGIES LTD.
FORTINET
JUNIPER NETWORKS
SIEM
+
splunk>
ArcSight
Radar
LogRhythm

DEMO, Q&A