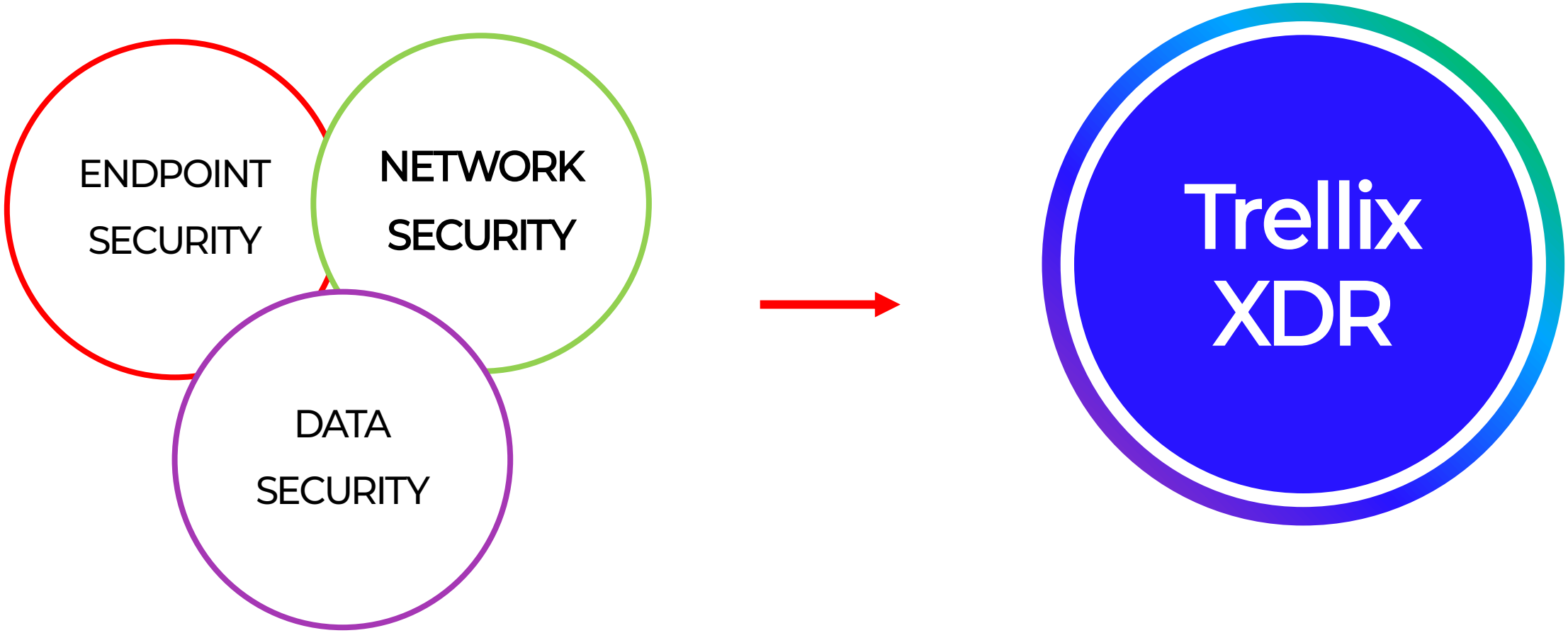
Trellix

Network Security

네트워크 위협 방어 NX 플랫폼 소개

Trellix Korea

Trellix Product 포트폴리오

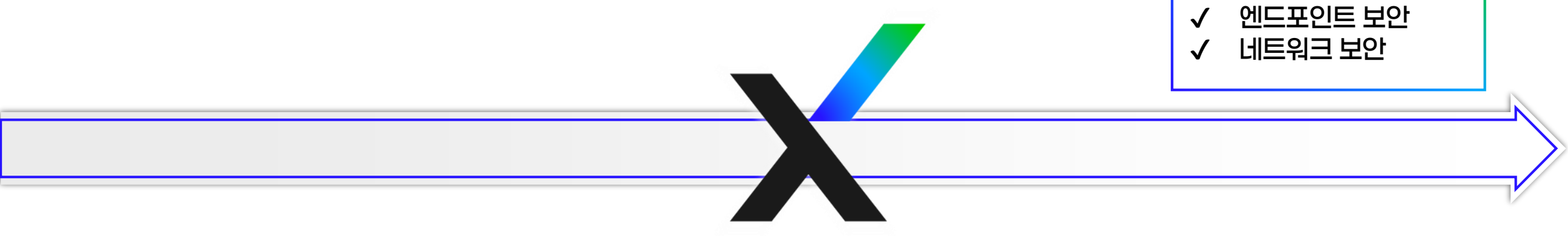


Trellix

Who Is Trellix?

XDR

- ✓ 데이터 보안
- ✓ 엔드포인트 보안
- ✓ 네트워크 보안



35

Years of **experience** backing up our security products

4,000

Trellix employees in 185 countries providing **24/7/365 service**

27,000+

Customers supported globally

250+

Global Advanced **Threat Intelligence** Researchers

80

Customers in the **Fortune 100**

Trellix

Trellix Market Leadership

✓ 2023년 로드맵 확장을 위해 **2022년 1,000명 이상 고용**

✓ Trellix는 모든 지역의 고객에게 서비스를 제공하는 **300개 이상의 전문 서비스 팀**을 보유하고 있습니다

✓ Trellix는 모든 지역에 걸쳐 15개 이상의 사무실을 보유하고 있으며 70개 이상의 국가에서 **40,000개 이상의 고객**을 지원합니다.

✓ Trellix는 TrustRadius **이메일 보안 시장 에서 (9.2/10)의 점수를 받았습니다 . 81%**의 고객이 Gartner Peer Insights 이메일 보안 시장에서 Trellix를 추천합니다.

✓ Trellix는 TrustRadius **네트워크 보안 시장 에서 (8.6/10)의 점수를 받았습니다 . 고객의 100%**가 Gartner Peer Insights 침입 탐지 및 예방 시스템(IDPS) 시장에서 Trellix를 추천합니다.

✓ Trellix는 엔드포인트 보호 플랫폼(EPP), 엔드포인트 탐지 및 대응(EDR), 네트워크 보안, 이메일 보안, 데이터 손실 방지(DLP) 및 클라우드 워크로드 보호 플랫폼(CWPP) 전반에 걸쳐 **가장 많은 리뷰를 집계한 XDR 공급업체**입니다.

출처 : https://www.trellix.com/blogs/xdr/a-fresh-perspective-to-assess-trellix-market-leadership/

Trellix

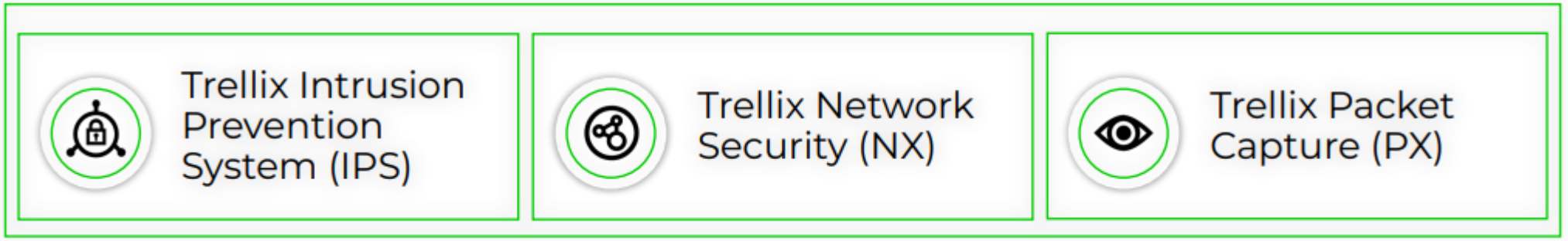
Trellix 국내 레퍼런스 | Trellix Korea

국내 Network APT 솔루션 주요 레퍼런스

- 국내 450 개 이상의 고객사에서 Trellix APT Network Security (NX,EX,HX)제품을 사용하고 있으며, 레퍼런스를 통해 충분히 검증된 솔루션을 제공합니다.

Trellix NDR: 네트워크 전체 킬체인 탐지

체계적인 Network 보안 포트폴리오



위치/용도	• 서버/데이터센터 • 대용량 트래픽 탐지	• PC / 사용자 단말기 • WEB, SMB 트래픽	• 포렌식 가시성 • 컴플라이언스
트래픽	100Gbps (200Gbps 확장)	20Gbps	40Gbps
주요 기능	**Deep packet Inspection:** Exploit protection/Virtual patching, advanced malware engines, DoS/DDoS, Deep file inspection, C&C, reputation, L7 visibility	**Advanced Threat Detection:** Lateral movement, Web infections, callbacks, beaconing, data exfiltration, IPS, L7 visibility	**Full packet capture:** Lossless packet capture, Session decoder, indexing and fast search.
제로데이 탐지	IVX 연동(VX)	On Box / IVX 클러스터	IVX 연동(AX)
배포/구성	Physical, Virtual, Public and Private Cloud, Integration with AWS Load Balancer.		

Trellix

사용자 망 /서비스 망 보안 강화 제안

서비스 망에 구축된 IPS와 Office망에 구축된 NX간에 탐지된 정보 공유

IVX(Intelligent Virtual eXecution) : 알려지 위협과 알려지지 않은 위협을 정확히 찾아내는 샌드박스

공격 체류 시간 단축: 트래픽 인입 시 지속적으로 콘텐츠를 검사하고 탐지를 수행.

알려지지 않은 제로데이 위협 식별: 정적, 동적, URL 및 행동 분석을 포함한 다양한 분석 기술.

SOC 헌팅 보완: 신뢰도 높은 경고를 통해 분석가는 중요한 위협에 집중할 수 있습니다.

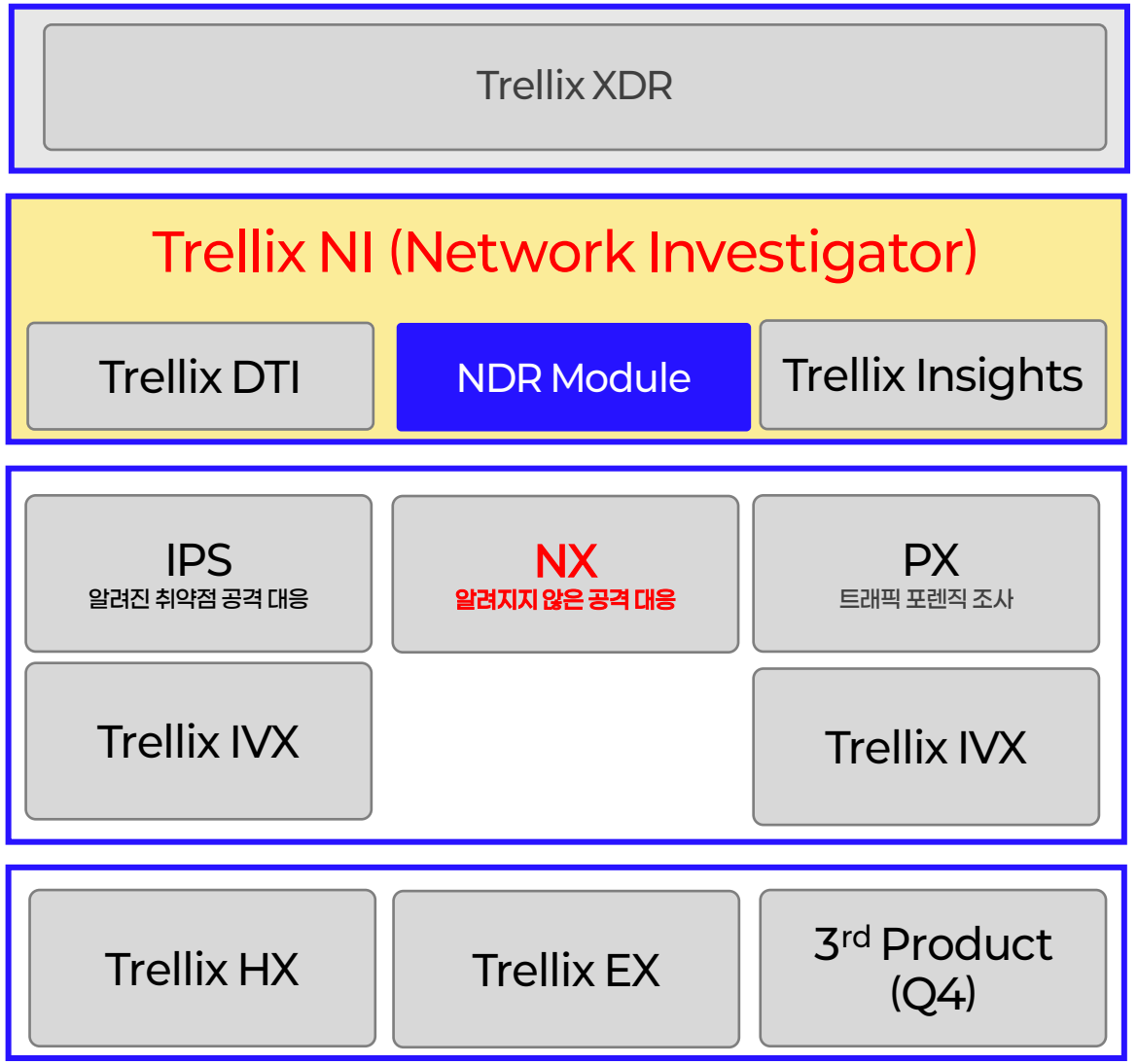
알려지지 않은 익스플로잇과 악성코드를 식별하여 Kill Chain 감염 및 피해를 방지합니다.

Trellix

대규모 네트워크 보호 범위 확장

네트워크 **전체 영역에 대한 커버리지** 제품으로 강화된 단일 플랫폼을 제공

- ✓ 사용자망/서비스망 등 강력한 보안이 적용되지 못하는 곳까지 커버리지(저성능 자산)
- ✓ 강력한 위협 인텔리전스와 연동을 통한 지속적인 업데이트
- ✓ 포렌직 조사 기능을 통한 상세 분석 제공



Trellix

Trellix NDR : 네트워크 보호 범위 확장

Protection, detection, forensic & hunting

알려지지 않은 공격 탐지
"Signature-less detection"
안전한 환경에서 의심되는 악성코드 실행

행동 분석
의심스러운 패턴을 공개
기계 학습은 알려진 나쁜 행동과 유사한 특성을 식별

시그니쳐 기반 탐지
"Find known bad"
대규모 고속 분석

트래픽 포렌직 분석
경계 보호가 실패한 경우의 가시성

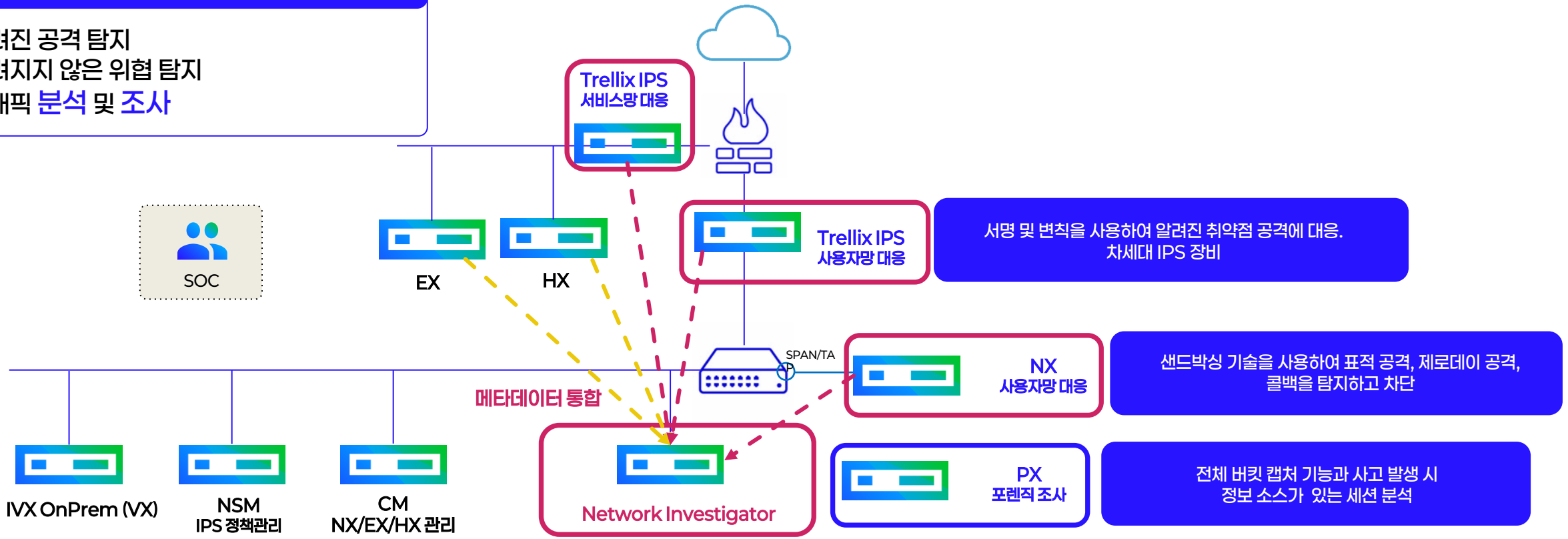
Trellix

Trellix NDR을 이용한 위협 분석/조사/추적

NX/EX/HX를 사용하는 고객사일 경우, NDR을 통한 이벤트 상세 분석/조사/추적 및 포렌직 수행

NDR에 필요한 탐지 기술

- 알려진 공격 탐지
- 알려지지 않은 위협 탐지
- 트래픽 분석 및 조사



Trellix

즉시 활용 가능한 인텔리전스

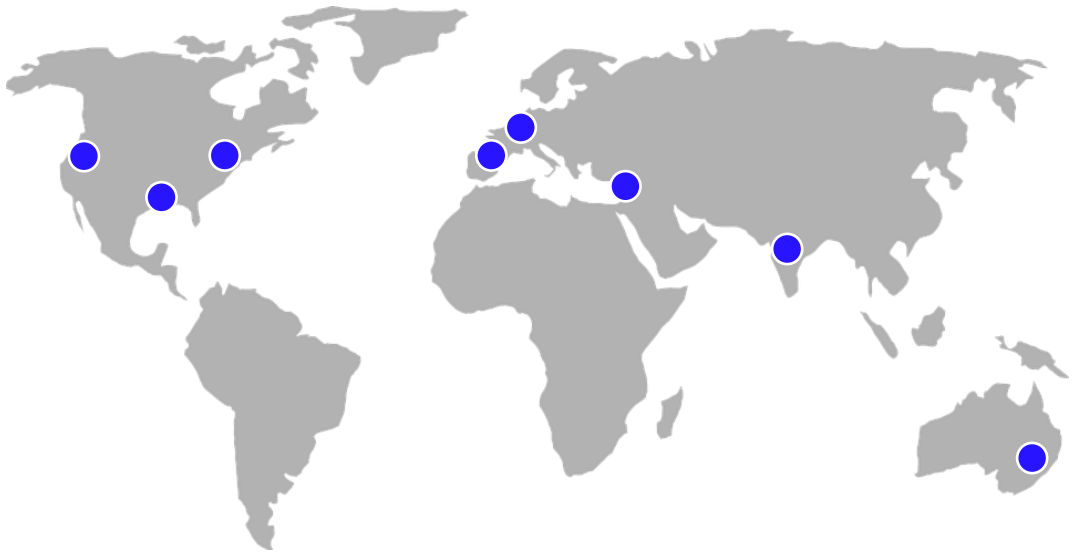
- ✓ 기존 FireEye 와 McAfee 제품의 결합으로 글로벌 **약 10억 개의 실시간 센서**를 통해 강력한 인텔리전스를 제공합니다.
- ✓ GTI를 기반으로 ATLAS, INTaaS, Insight 등의 다양한 플랫폼으로 제품에 **실시간 분석 정보 제공**.
- ✓ 기존 맥아피 제품의 35년 간 축적된 악성코드 분석 데이터 기반과 FireEye 의 APT 의 기술력으로 만들어낸 **압도적 인텔리전스 제공**

Trellix 솔루션이 제공하는 GTI(Global Threat Intelligence)는 전세계 고객사에 설치된 10억개 이상의 Trellix 센서, 가상머신의 수집 데이터, 보안컨설팅(MDR), 다크웹 첩보 수집을 통해 제공

Trellix

Trellix Global Threat Intelligence

+ FireEye DTI 통합 완료 (2023.09)



+50
TI Analysts

+200
researchers

- 멀티 시간대에 위치하여 연중 무휴 24시간 서비스 제공
- 원격 및 현장에서 분석가 지원
- 러시아어, 중국어, 베트남어, 프랑스어, 독일어, 스페인어, 포르투갈어, 히브리어, 아랍어, 네덜란드어를 구사하는 원어민 분석가
- 분석가로부터 취약점및 악성코드 연구까지 다양한 기술 제공
- 국가 CERTS, IC 기관, LE 기관, 국방 및 상업조직에 이르는 다양한 고객층 보유
- 인텔리전스부터 제품까지 데이터 기반 연구
- 전 세계적으로 10억 개 이상의 센서를 통한 SIGINT 정보

*SIGINT (Signal Intelligence) : 제품을 통해 업데이트 되는 인텔리전스 정보

NX 제품 소개

Trellix NX 주요 기능

MVX
가상머신 검사

YARA / AV-SUIT
Byte 레벨의 룰 및 시그니처 기반 검사

Embeded URL
문서 내 URL 검사

IPS for APT
네트워크 행동 패턴 검사

SMARTVISION
내부확산 탐지

Evidence Collector
로그 전송

RiskWare
악성과 유사한 코드 검사

Malware Guard
머신 러닝

Layer 7 Meta Data Exporter
메타데이터 제공

Trellix

Multi-Flow (Session based) 분석 방식

1 FireEye Hardened Hypervisor

- 내장되어 있는 Custom hypervisor
- 일반 가상화 솔루션의 디자인과 다르게 위협 분석을 위해 디자인됨

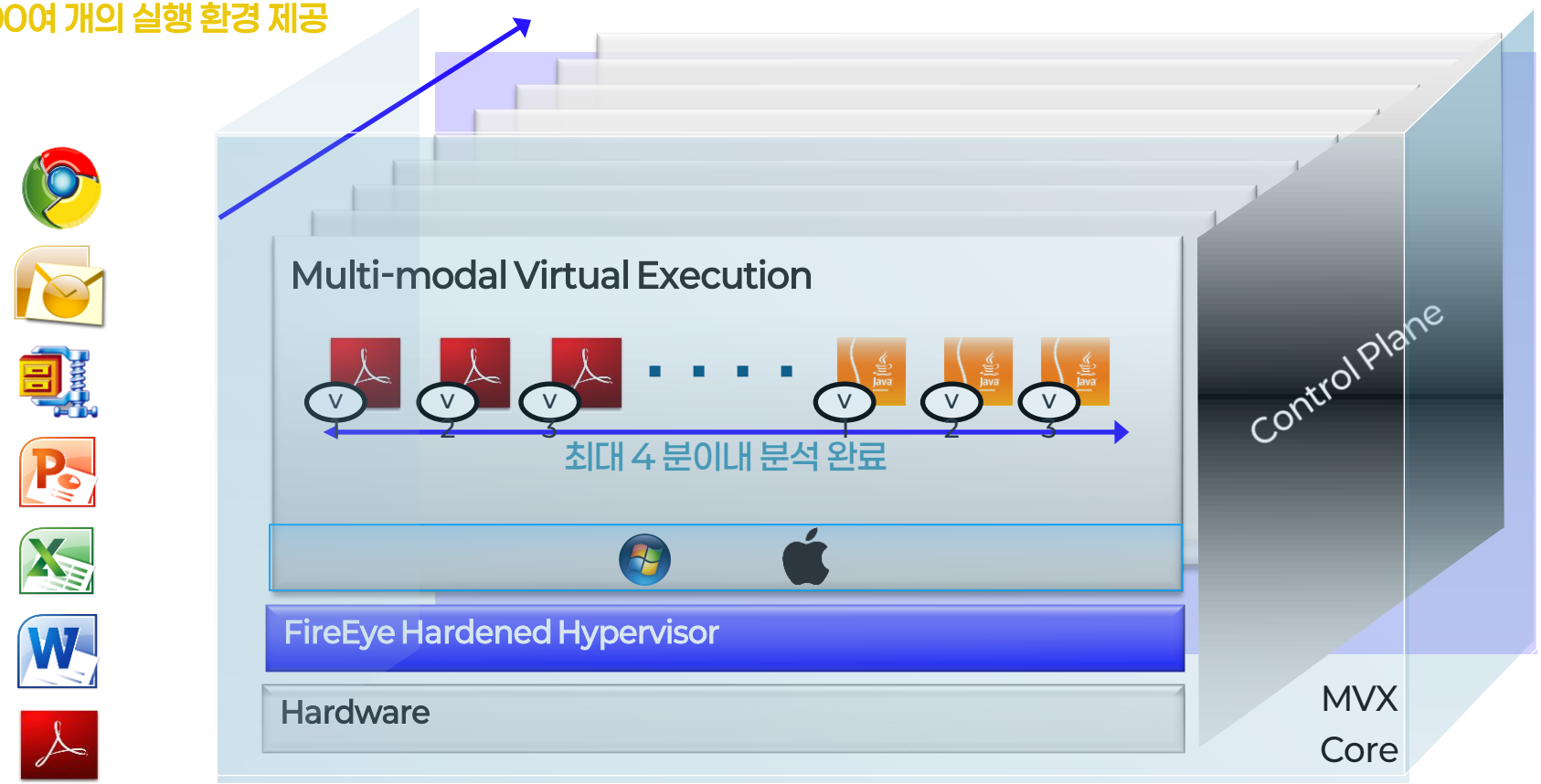
2 Multi-modal Virtual Execution

- 다양한 OS
- 다양한 서비스팩
- 다양한 어플리케이션
- 다양한 파일 타입

3 Threat Protection at Scale

- 200여개의 실행환경 제공
- Multi-stage analysis

200여 개의 실행 환경 제공



- WinXP
- Win7 32bit/64bit
- Win10 64bit

- OSX 10.11.3
- OSX 10.8.2

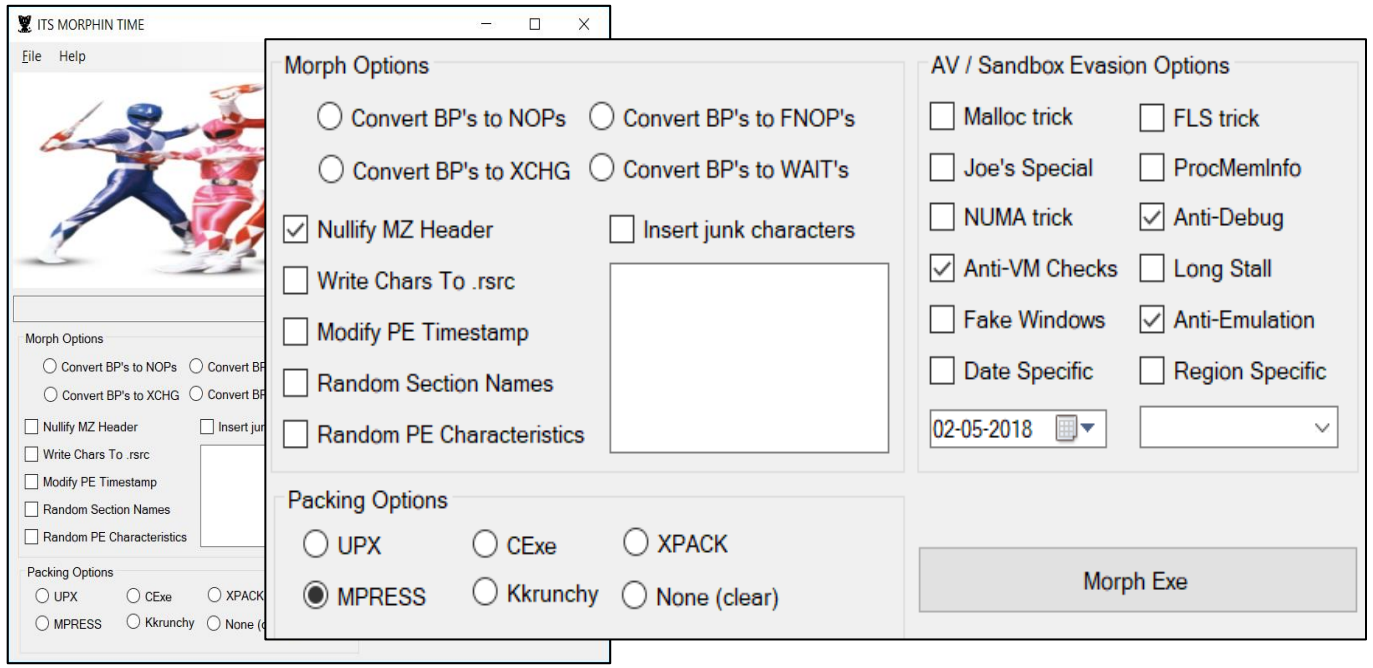
- CentOS 7.2

Trellix

가상머신 회피 기법 사용

가상 머신 환경인지 검증하는 단계 삽입

- 공격자도 상용 가상 머신 환경(VMWare, Virtual Box)를 쉽게 구할 수 있으며, 가상 머신 환경인 경우 악성 행위를 하지 않음.



[백신/샌드박스 우회 툴]

Source: http://www.gironsec.com

< Figure0. 메인 함수 >

프로그램에서는 제일 먼저 가상환경을 탐지해낸다. 3가지 방법으로 탐지를 시도해내고 있으며 탐지 될 경우, 종료한다. 이로 인해 행위 분석으로는 결과가 나오지않을 수 있다.

```
char VMDetect()
{
  unsigned __int32 v0; // eax@1

  v0 = __indword(0x5658u);
  return 0;
}
```

```
char VMDetect2()
{
  char result; // al@1

  result = 1;
  __asm { vpcext  7, 0Bh }
  return result;
}
```

< Figure1. 가상 환경 탐지 함수 >

- VMDetect
  ->0x5658 포트에서 값을 읽어서 "VMXh" 일 경우, 탐지해낸다. 대표적으로 Vmware을 이용할 경우 탐지된다.
- VMDetect2
  ->VirtualPC에서 읽을 수 없는 명령어를 실행해 Try~Catch로 탐지한다. 대표적으로 VirualBox을 이용할 경우 탐지된다.
- VMDetect3
  ->SbieDll.dll의 존재 유무로 탐지해낸다. 이 라이브러리는 샌드박스 라이브러리로 일반적인 PC에서는 로드되지 않는다.

[Erebus 랜섬웨어(나야야 사건)]

Trellix

APT 위협 탐지 극대화를 위한 컨텍스트 기반 탐지/차단

- 익스플로잇(Exploit)과 악성코드 배포를 위해 다양한 우회 기법과 멀티 플로우 기반 공격

초기침투 및 거점 확보

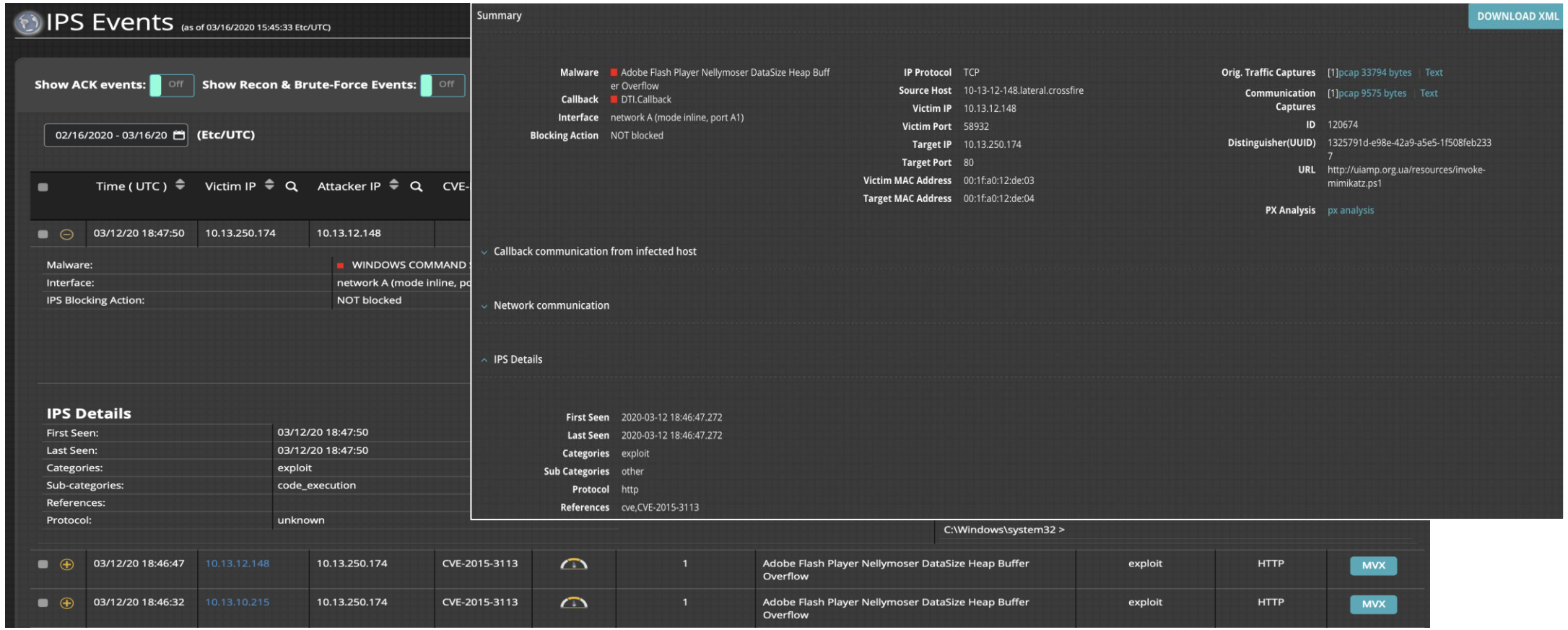
자체 기술력 MVX 동적 분석 기술 - Multi Layered, Multi-Vector, Multi-Flow 공격 대응 엔진

- FUME(FireEye Unified Multiflow) 엔진
  - 멀티플로우 탐지기능과 파일 탐지기능의 효과적인 벨런싱을 통해 최근 Exploit KIT과 같은 멀티 공격 기법에 대해 상호연관(correlation) 기법을 통해 탐지 엔진
- 탐지 성능 개선된 IPS/IDS 모듈 제공
  - OS, Application 취약점에 대한 알려진 공격 위협 탐지, MVX 엔진 검증
  - 기본 제공 기능으로, 추가적인 IPS 라이선스 구입 필요 없음
  - 최대 5,000 개의 사용자 IPS 룰 지원
- Windows, Mac OS, CentOS 등 멀티 OS 환경 지원
  - APT탐지만을 위해 특화된 가상 머신
  - 알려진/알려지지 않은 Exploit 탐지
  - 파일 기반이 아닌 Multi Flow 기반 탐지
  - 장비 당 최대 192개의 가상 머신
  - Revert Time 3초 이내(경쟁사 수분 걸림)

Trellix

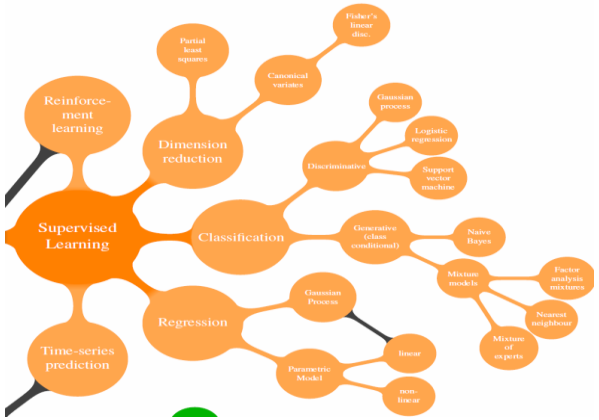
IPS for APT

- Client Side : Exploit Kit/Shell Code, Information Leakage, Cross Domain, Code Execution 등
- Server Side : Code Execution, Cmd Injection, SQL Injection, XSS, CSRF, Application DoS, Exploit/Shellcode Detection 등
- Mobile Side : Android C&C / RAT Detection
- APT Side : More than 20+ File types, VM based detection



Trellix

APT 위협 탐지 극대화를 위한 지도형 머신러닝



머신러닝(Malware Guard) 기반의 탐지 결과 참조.

- 알려지지 않은 악성코드 변종에 대한 탐지 및 차단
- FireEye의 타의 추종을 불허하는 악성 프로그램에 대한 모델링은 실제 침해현장으로부터 수집
- 랜섬웨어 방어에 대단히 효과적.

머신러닝엔진은 각 센서에서 수집된 일 백 만건 이상의 케이스들을 FireEye 머신러닝 플랫폼을 통해 중앙 학습된 정보를 기반으로 정책을 NX 장비로 내려주며 주기적으로 업데이트 됨.

Malware	Backdoor.Win.CYBERGATE
VXE Callback	Backdoor.Win.CYBERGATE
Application Type	Windows Explorer
File Type	exe
Builtin AV	Win.Trojan.Llac-7
Yara Rule	FE_Backdoor_Win32_CYBERGATE_1 FE_Evasion_DBGDetect_Files FE_VM_Evasion_IOPorts
Malware Guard	fe_ml_heuristic
FUME	Exploit.MultiFlowPayload_udfa

Malicious behaviour observed

Malware Guard fe_ml_heuristic

2020 Mar. US Navy Award & Cyber Security Excellence

AMERICAN CYBER AWARDS Winner 2020

AI ATAC

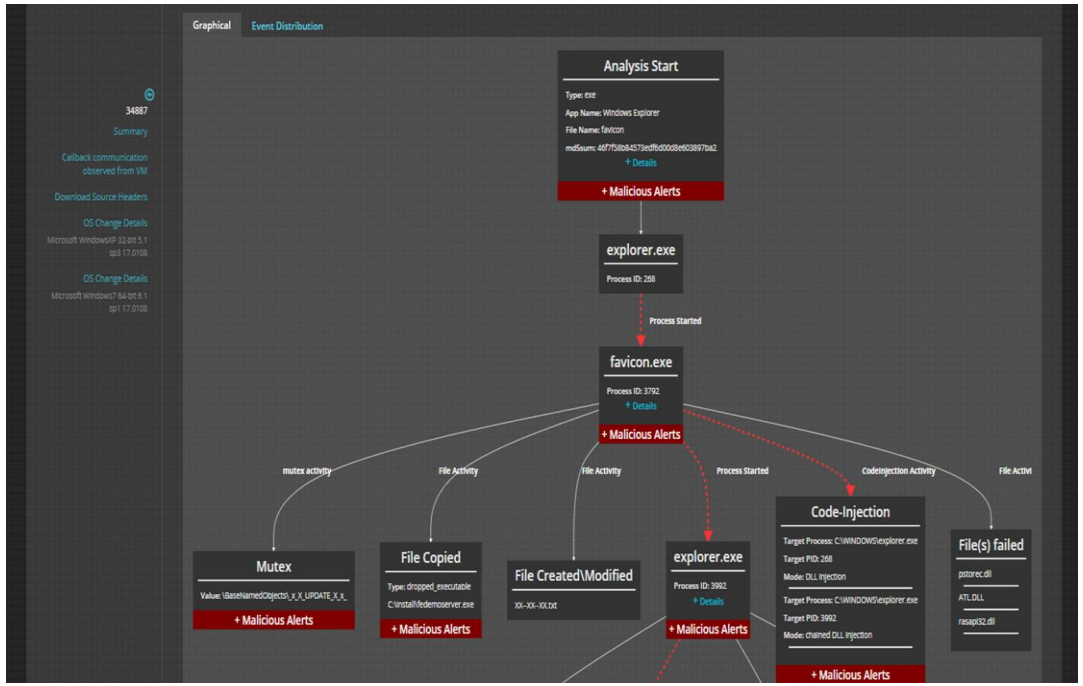
Government Innovation Awards WINNER 2020

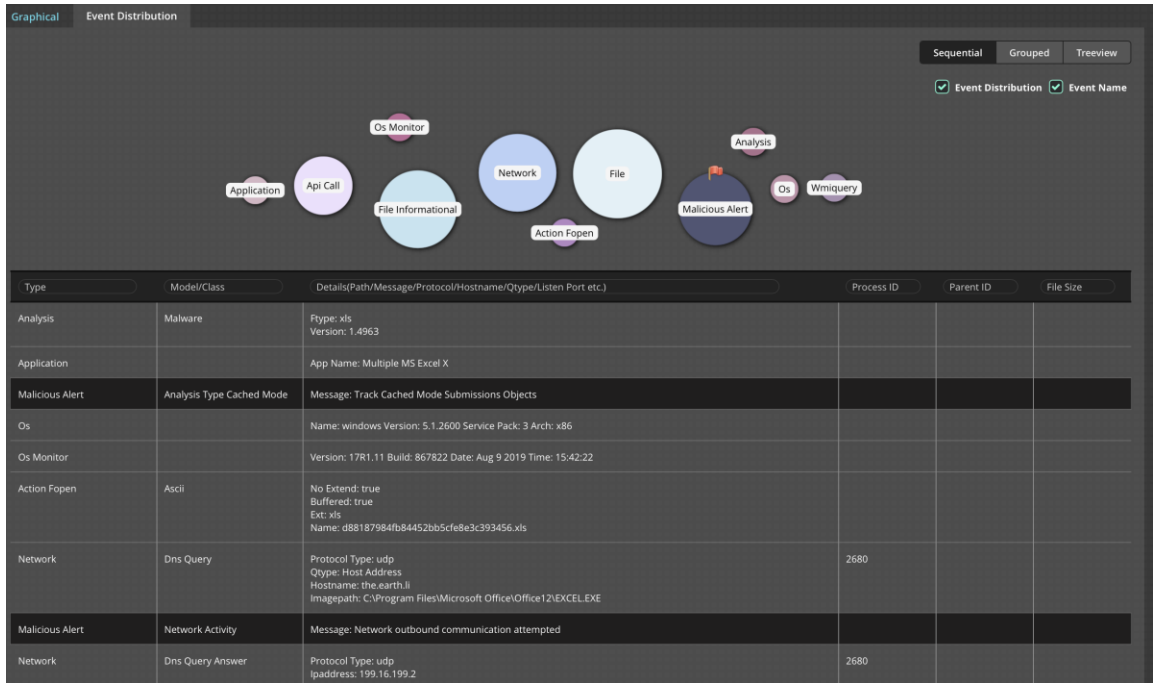
https://news.naver.com/main/read.nhn?mode=LS2D&mid=shm&sid1=105&sid2=732&oid=030&aid=0002872195

Trellix

APT 위협 탐지 및 선제 대응을 위한 행위 기반 도식화된 플로우 제공

- NX 전용 엔진인 MVX 가상머신을 통해 OS의 변경되는 모든 행위를 통해 알려진/알려지지 않은 기법/파일 탐지
  이를 도식화된 그림으로 제공함으로써 악성코드에 대한 이해 및 정오탐 Evidence 기반 이해 제공
  하나의 이벤트로 부터 파생되는 여러가지 Indicator들의 가시성을 확보하여, APT Life Cycle의 Kill-Chain 접점 추가 확인 및 대응





Trellix

문서내 URL 검사 제공 (Unified-FAUDE)

Doc/pdf 문서내에 URL에 대한 정적 분석 제공

Summary

DOWNLOAD XML

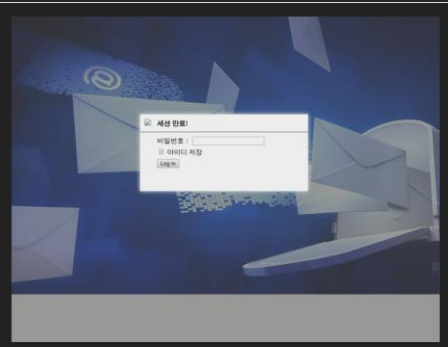
Infection	Local.Infection	**IP Protocol**	TCP	**Communication Captures**	[1]pcap 16613 bytes | Text
Interface	network A (mode inline, port A1)	**Source Host**	10-12-10-173.victim.crossfire	**ID**	134347
Blocking Action	NOT blocked	**Victim IP**	10.12.10.173	**Distinguisher(UUID)**	e46f964b-d4ad-49a6-91fc-dbedc21fcf1c
		Victim Port	51071	**URL**	http://uiamp.org.ua/activity/player.swf
		Target IP	10.12.250.38	**URL Screenshot**	URL SCREENSHOT
		Target Port	80	**PX Analysis**	px analysis
		Victim MAC Address	00:1f:a0:12:de:1a		
		Target MAC Address	00:1f:a0:12:de:17		

Attempted infection communication

Intelligence Summary

URL Screenshot Preview

URL:
https://byte-92980trwfg-191-qksxb-dot-hi8-o76-67f.appspot.com/rsync/?email=
Target Brand:
["Unknown"]
Screenshot:

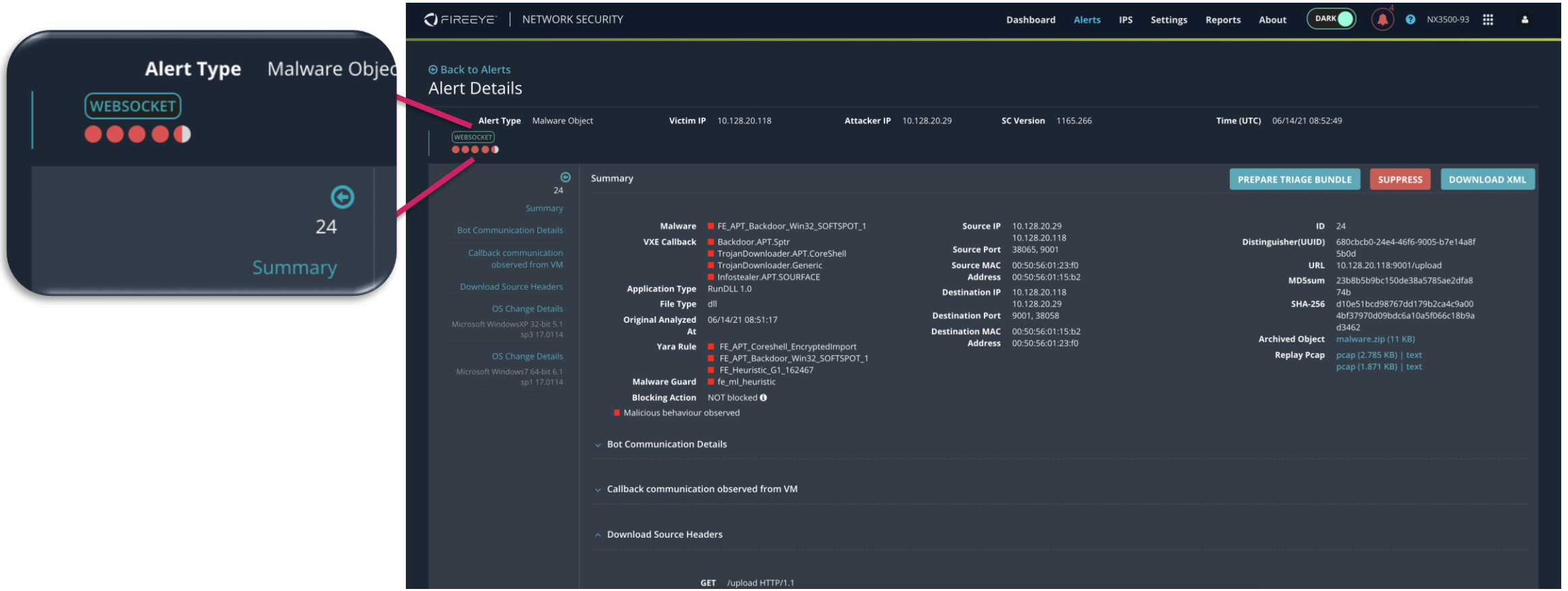


```
sc-fattire-7400 (config) # analysis url policy adv-url-defense enable
Feature already enabled.
sc-fattire-7400 (config) #
sc-fattire-7400 (config) #
sc-fattire-7400 (config) # show analysis url-policy
    TypoSquatting:                  yes
    URL phishing whitelist policy:  yes
    URL phishing blacklist policy:  yes
    Advanced URL Defense:           yes
```


Trellix

Web Socket 통신 분석

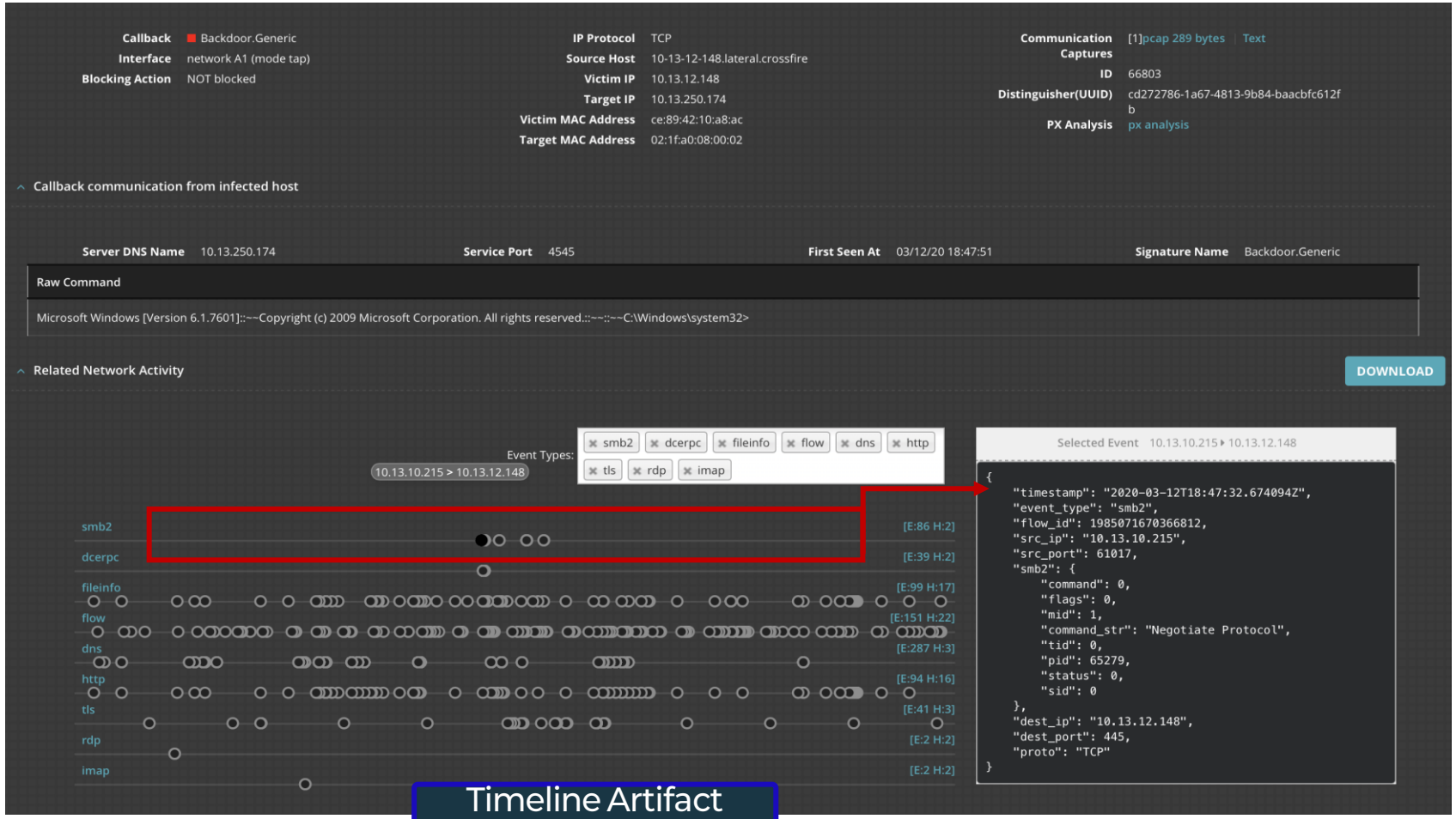
Web Socket 통신을 통한 악성파일 분석



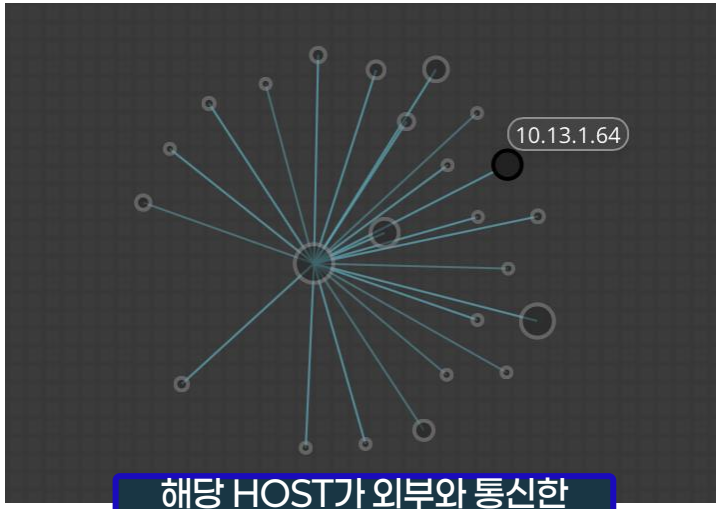
Trellix

APT 위협 탐지 극대화를 위한 포렌식 데이터 제공

- NX에서 탐지 되는 이벤트에 대해서, 해당 이벤트를 기점으로 하여서 +-5분간의 L7 정보 기반의 타임라인을 제공.
- 이를 통해서, 3rd party 네트워크 포렌식이나 SIEM 장비의 연동 없이도 이벤트가 발생한 상황에서의 현황을 파악 가능함.



Timeline Artifact 제공

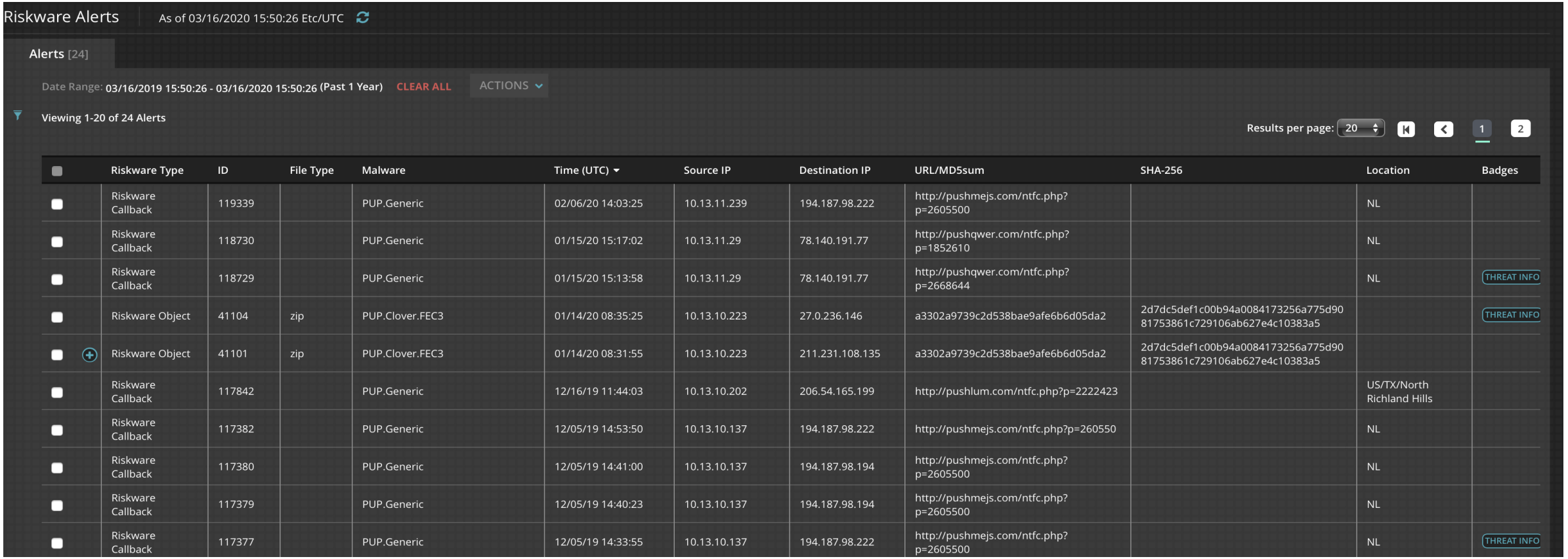


해당 HOST가 외부와 통신한 IP 정보 확인

Trellix

Riskware 기능

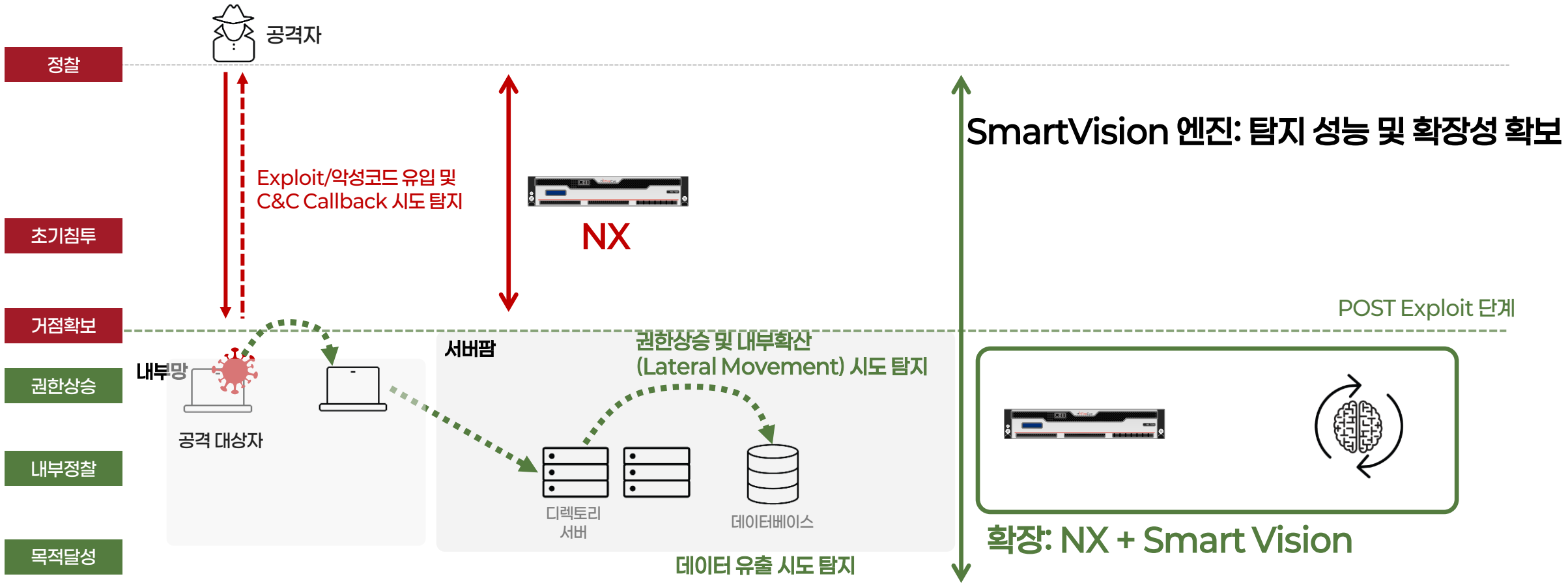
- PUP/Adware에 대한 전용 탐지 엔진 장착
- 이를 통해서, 이벤트의 우선 순위를 사용자가 직관적으로 파악 가능하도록 함
- 악성으로 판단되는 기준에 미치지 못하더라도 일정 수준의 행위가 파악되는 의심 파일에 대해 탐지



Riskware Type	ID	File Type	Malware	Time (UTC)	Source IP	Destination IP	URL/MD5sum	SHA-256	Location	Badges
Riskware Callback	119339		PUP.Generic	02/06/20 14:03:25	10.13.11.239	194.187.98.222	http://pushmejs.com/ntfc.php?p=2605500		NL	
Riskware Callback	118730		PUP.Generic	01/15/20 15:17:02	10.13.11.29	78.140.191.77	http://pushqwer.com/ntfc.php?p=1852610		NL	
Riskware Callback	118729		PUP.Generic	01/15/20 15:13:58	10.13.11.29	78.140.191.77	http://pushqwer.com/ntfc.php?p=2668644		NL	THREAT INFO
Riskware Object	41104	zip	PUP.Clover.FEC3	01/14/20 08:35:25	10.13.10.223	27.0.236.146	a3302a9739c2d538bae9afe6b6d05da2	2d7dc5def1c00b94a0084173256a775d9081753861c729106ab627e4c10383a5		THREAT INFO
Riskware Object	41101	zip	PUP.Clover.FEC3	01/14/20 08:31:55	10.13.10.223	211.231.108.135	a3302a9739c2d538bae9afe6b6d05da2	2d7dc5def1c00b94a0084173256a775d9081753861c729106ab627e4c10383a5		
Riskware Callback	117842		PUP.Generic	12/16/19 11:44:03	10.13.10.202	206.54.165.199	http://pushlum.com/ntfc.php?p=2222423		US/TX/North Richland Hills	
Riskware Callback	117382		PUP.Generic	12/05/19 14:53:50	10.13.10.137	194.187.98.222	http://pushmejs.com/ntfc.php?p=260550		NL	
Riskware Callback	117380		PUP.Generic	12/05/19 14:41:00	10.13.10.137	194.187.98.194	http://pushmejs.com/ntfc.php?p=2605500		NL	
Riskware Callback	117379		PUP.Generic	12/05/19 14:40:23	10.13.10.137	194.187.98.194	http://pushmejs.com/ntfc.php?p=2605500		NL	
Riskware Callback	117377		PUP.Generic	12/05/19 14:33:55	10.13.10.137	194.187.98.222	http://pushmejs.com/ntfc.php?p=2605500		NL	THREAT INFO

Trellix

APT 대응을 위한 상관 관계 분석 엔진



Trellix

APT 위협 탐지 극대화를 위한 컨텍스트 기반 탐지/차단

- SmartVision 엔진 - Full Attack Life Cycle 기반 지능형 APT 공격 대응 위한 고급 상관관계 분석 엔진

권한상승 및 내부확산 과정 이후

SmartVision 엔진 상관 관계 분석 – Attack Life Cycle 기준 대응을 위한 NX 새로운 영역으로 진화

ID	NAME	TYPE	TIME	SENSOR	SOURCE IP	DESTINATION IP	SEVERITY	SC Version
831	SMB PSEXEC [Output] Over SMBv2	PsExec Activity	03/12/18 14:12:47	nx10v-rubicon	192.168.99.101	192.168.99.77	6	684.326
832	Sysinternals PsExec Activity Over SMBv2 TCP Port 445	PsExec Activity	03/12/18 14:12:47	nx10v-rubicon	192.168.99.101	192.168.99.77	6	684.326
830	SAMR Service Remote User Enumeration Over SMBv2 TCP Port 445	User Enumeration Attempt	03/12/18 14:12:44	nx10v-rubicon	192.168.99.199	192.168.99.77	2	684.326
827	Mimikatz Activity Detected	Mimikatz Activity	03/12/18 14:07:36	nx10v-rubicon	192.168.99.199	192.168.99.100	9	684.326
826	SVCCTL Remote Service Launch Over SMBv1 TCP Port 445	Remote Service Launch	03/12/18 14:07:33	nx10v-rubicon	192.168.99.199	192.168.99.77	2	684.326
825	SRVSVC Service Remote Share Enumeration Over SMBv1 TCP Port 445	Share Enumeration	03/12/18 14:07:33	nx10v-rubicon	192.168.99.199	192.168.99.77	2	684.326
828	SMB PSEXEC [Output] Over SMBv2	PsExec Activity	03/12/18 14:07:31	nx10v-rubicon	192.168.99.101	192.168.99.77	6	684.326
829	Sysinternals PsExec Activity Over SMBv2 TCP Port 445	PsExec Activity	03/12/18 14:07:31	nx10v-rubicon	192.168.99.101	192.168.99.77	6	684.326

120+ 이상의 네트워크 기반의 상관관계 룰

- Remote Task Schedule via AT Service
- Remote Service Launch via SVCCTL(Service Control Manager) SMB
- Windows WMI Remote Shell Launch

… 생략 …

- SMB Connection To C$ Hidden Share
- SMB EXE File Write To C$ share
- DLL upload SMB
- Remote PSEXECSVC Binary Transfer SMB

… 생략 …

Trellix

통합 운영 | 효율적인 관리 및 대응을 위한 사용자 중심 분석 및 대응 자동화

네트워크/이메일/엔드포인트 통합 운영

Trellix

NX H/W Spec

구분	NX4600	NX5600	NX6600	NX8600
성능	최대 1 Gbps (센서 모드 2 Gbps)	최대 2.5 Gbps (센서 모드 5 Gbps)	최대 5 Gbps (센서 모드 10 Gbps)	최대 10 Gbps (센서 모드 20 Gbps)
폼 팩터	2U Rack-Mount	2U Rack-Mount	2U Rack-Mount	2U Rack-Mount
크기 (W x D x H)	19 in x 26 in x 3.5 in	19 in x 26 in x 3.5 in	19 in x 26 in x 3.5 in	19 in x 26 in x 3.5 in
랙 마운트	2RU, fits 19-inch Rack	2RU, fits 19-inch Rack	2RU, fits 19-inch Rack	2RU, fits 19-inch Rack
네트워크 모니터링 포트	(4) 1G RJ45 bypass (4) 1G/10G SFP+ (4) 10G SFP+	(4) 1G/10 RJ45 bypass (4) 1G/10G SFP+ (4) 10G SFP+	(2) 40G QSFP+ (4) 10G SFP+ (2) 1G/10G SFP+ (4) 1G/10G RJ45 bypass	(2) 40G QSFP+ (4) 10G SFP+ (2) 1G/10G SFP+ (4) 1G/10G RJ45 bypass (2) 100G QSFP28
네트워크 모드	인라인 모니터, Fail-Open, Fail Close 또는 TAP/SPAN	인라인 모니터, Fail-Open, Fail Close 또는 TAP/SPAN	인라인 모니터, Fail-Open, Fail Close 또는 TAP/SPAN	인라인 모니터, Fail-Open, Fail Close 또는 TAP/SPAN
IPMI 포트	100/1GbaseT	100/1GbaseT	100/1GbaseT	100/1GbaseT
메모리	128 GB (8x16 GB)	128 GB (8x16 GB)	128 GB (8x16 GB)	128 GB (8x16 GB)
디스크	(2) 4TB HDD, RAID 1, 3.5, FRU	(2) 4TB HDD, RAID 1, 3.5, FRU	(2) 4TB HDD, RAID 1, 3.5, FRU	(2) 4TB HDD, RAID 1, 3.5, FRU
전원	(1+1), FRU, 920W 110-240V	(1+1), FRU, 1000W/1200W 110-240V	(1+1), FRU, 1000W/1200W 110-240V	(1+1), FRU, 1000W/1200W 110-240V
최대 파워 소비량	552 W	852 W	928 W	1100 W

Trellix


Trellix