

Why Trend Micro TippingPoint® ?

네트워크 보안팀

김석주 부장(anthony_kim@trendmicro.com)



NSS LABS NEXT GENERATION INTRUSION PREVENTION SYSTEM(NG IPS) GROUP TEST – 2018



- 유일하게 “Recommended”를 받은 전용 NGIPS 제조사
- Trend Micro TippingPoint는 3년 연속 “Recommended” 평가
- 다양한 환경의 Network Throughput 및 Connection에서 상위 평가
- **Only vendor to “PASS” Power Fail Open test**

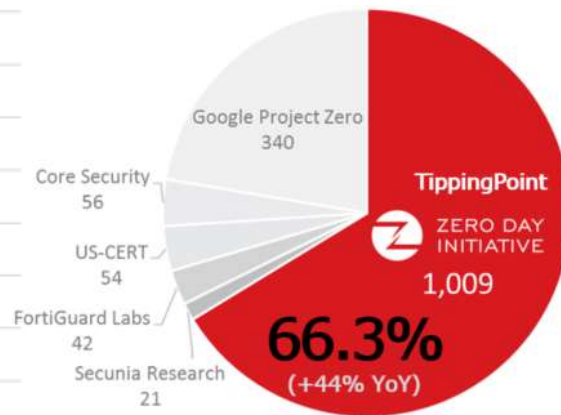
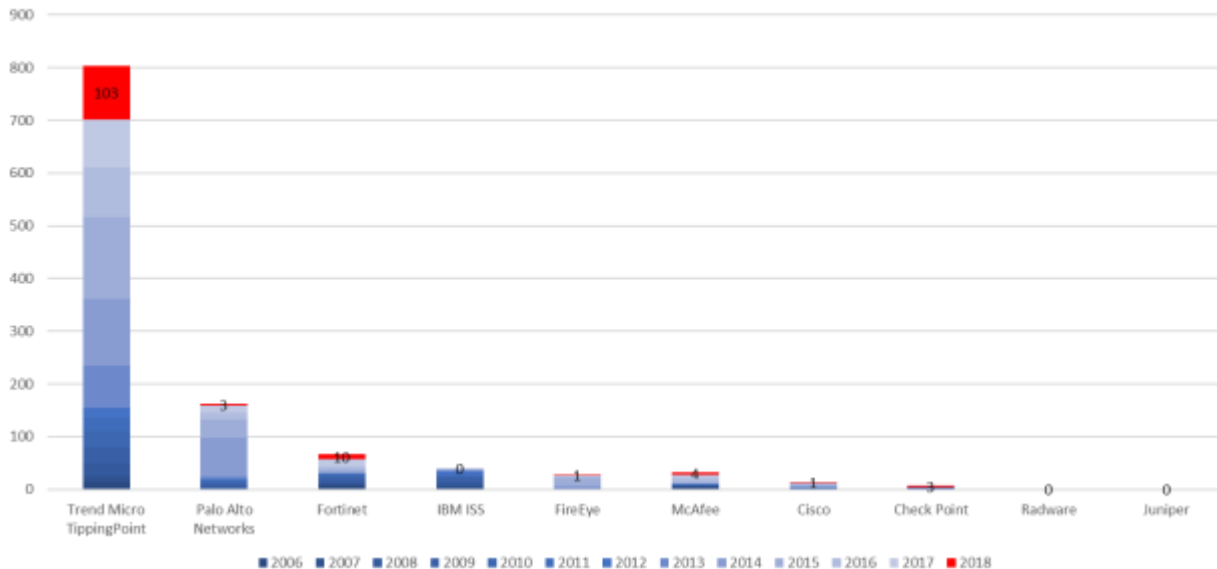
NSS LABS NGIPS GROUP TEST RESULTS

PRODUCT	NSS-TESTED THROUGHPUT		3-YEAR TCO (US\$)
Trend Micro TippingPoint 8400TX • v5.1.0.4965	31,566 Mbps		\$222,477
	Exploit Block Rate¹	Evasions Blocked	Stability and Reliability
	97%	147/147	PASS

Why TippingPoint NGIPS?

: 글로벌 최고의 취약점 리서치를 통한 선제적 보안 대응

Microsoft Vulnerability Acknowledgements 2006-Present



Source: Frost & Sullivan. Analysis of the Global Public Vulnerability Research Market 2017

*From publicly available data at <https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments> as of October 1, 2018

Why TippingPoint NGIPS?

: 글로벌 최고의 취약점 리서치를 통한 선제적 보안 대응

UPCOMING ADVISORIES

The following is a list of vulnerabilities discovered by Zero Day Initiative researchers that are set to be publicly disclosed. The affected vendor has been contacted on the specified date and while they work on a patch for these vulnerabilities. Trend Micro customers are protected from exploitation by IPS filters delivered ahead of public disclosure. Trend Micro customers are additionally protected against 0day vulnerabilities discovered by our own researchers.

UPCOMING PUBLISHED

348 advisories pending public disclosure

Search advisories

ZDI ID	AFFECTED VENDORS	SEVERITY	REPORTED	DEADLINE
ZDI-CAN-6861	Hewlett Packard Enterprise	CVSS: 8.8	2018-08-22 10 days ago	2018-12-20
ZDI-CAN-6768	Hewlett Packard Enterprise	CVSS: 8.8	2018-08-22 10 days ago	2018-12-20
ZDI-CAN-6767	Hewlett Packard Enterprise	CVSS: 8.8	2018-08-22 10 days ago	2018-12-20

PUBLISHED ADVISORIES 2018

The following is a list of all publicly disclosed vulnerabilities discovered by Zero Day Initiative researchers. While the affected vendor is working on a patch for these vulnerabilities, Trend Micro customers are protected from exploitation by security filters delivered ahead of public disclosure.

All security vulnerabilities that are assigned by the Zero Day Initiative are handled according to the ZDI Disclosure Policy. Once the affected vendor patches the vulnerability, we publish an accompanying security advisory which describes the issue, including links to the vendor's fixes.

UPCOMING PUBLISHED

Search

ZDI ID	ZDI CAN	AFFECTED VENDORS	CVE	PUBLISHED	UPDATED
ZDI-2018-001	Microsoft	Windows	CVE-2018-001	2018-01-01	2018-01-01
ZDI-2018-002	Microsoft	Windows	CVE-2018-002	2018-01-01	2018-01-01
ZDI-2018-003	Microsoft	Windows	CVE-2018-003	2018-01-01	2018-01-01

ZERO DAY INITIATIVE:

→ 발견한 보안취약점에 대한 자세한 정보는 해당 제조사에게만
공유 및 통보

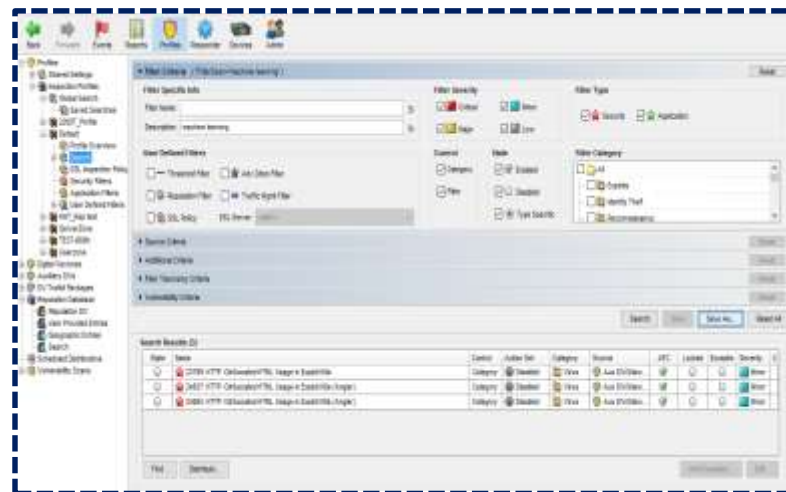
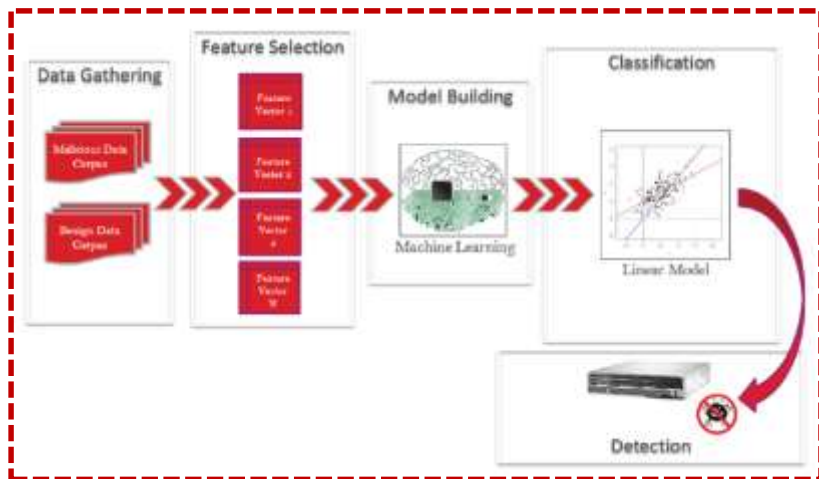
Date	Name	Control	Action Set ID	Category	Source	Severity
2018-08-22	ZDI-CAN-6861: Zero Day Initiative Vulnerability (HP)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6768: Zero Day Initiative Vulnerability (Microsoft)	Category	Block / Notify	Exploits	0day	Critical
2018-08-22	ZDI-CAN-6767: Zero Day Initiative Vulnerability (Adobe Flash)	Category	Block / Notify	Exploits	0day	Critical
2018-08-22	ZDI-CAN-6766: Zero Day Initiative Vulnerability (Adobe Reader DC)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6765: Zero Day Initiative Vulnerability (Microsoft Internet Explorer)	Category	Block / Notify	Exploits	0day	Critical
2018-08-22	ZDI-CAN-6764: Zero Day Initiative Vulnerability (Microsoft Internet Explorer)	Category	Block / Notify	Exploits	0day	Critical
2018-08-22	ZDI-CAN-6763: Zero Day Initiative Vulnerability (Microsoft Internet Explorer)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6762: Zero Day Initiative Vulnerability (Adobe Flash)	Category	Block / Notify	Exploits	0day	Critical
2018-08-22	ZDI-CAN-6761: Zero Day Initiative Vulnerability (Microsoft Internet Explorer)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6760: Zero Day Initiative Vulnerability (Microsoft Internet Explorer)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6759: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6758: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6757: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6756: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6755: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6754: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6753: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6752: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6751: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6750: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6749: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6748: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6747: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6746: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6745: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6744: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6743: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6742: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6741: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6740: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6739: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6738: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6737: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6736: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6735: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6734: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6733: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6732: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6731: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6730: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6729: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6728: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6727: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6726: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6725: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6724: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6723: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6722: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6721: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6720: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6719: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6718: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6717: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6716: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6715: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6714: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6713: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6712: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6711: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6710: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6709: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6708: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6707: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6706: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6705: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6704: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6703: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6702: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical
2018-08-22	ZDI-CAN-6701: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor)	Category	Block / Notify	Vulnerabilities	0day	Critical

- 보안 패치가 존재하지 않는 보안 취약점에 대한 공격 가시성 및 사전 방어.
- Trend Micro에서는 해당 시그니처에 "ZDI-CAN" 으로 구분해서 고객에게 제공

Why TippingPoint NGIPS?

: 머신러닝 필터 (웹트래픽 분석)

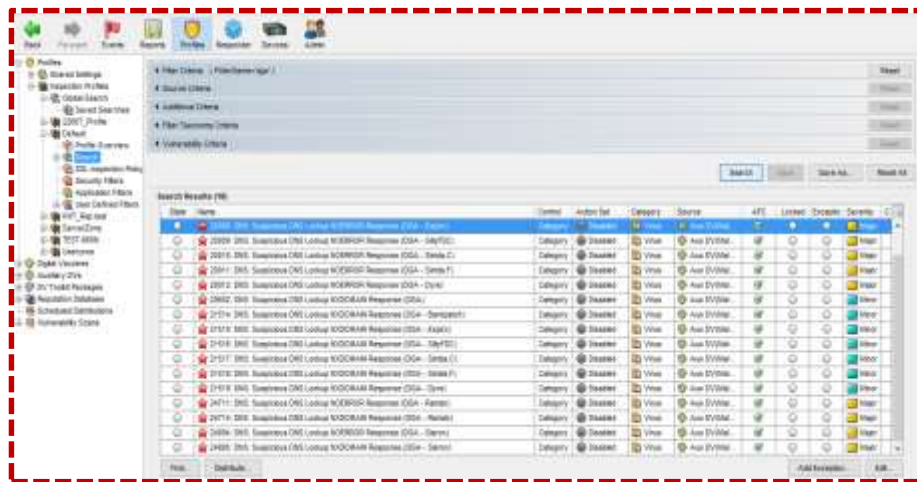
- ✓ Html and Java script contents를 분석하여 modeling 된 통계치와 비교/분석하여 탐지
- ✓ HTML안에 있는 특수 문자, space등 값을 이용하여 legitimate/illegitimate 의 modeling 생성
- ✓ 기존의 Signature방식으로 탐지되지 않는 Suspicious 웹 트래픽 탐지에 효과적이고 오탐없는 기술



Why TippingPoint NGIPS?

: 머신러닝 필터 (DGA)

- ✓ Domain Generation Algorithm : 최신 멀웨어, 랜섬웨어, Worm 확산 등에 활용됨
- ✓ Malware에 감염된 노드에서 C&C 서버에 접속을 시도할 때, hard-code 된 IP나 도메인 대신에 Domain Generation Algorithm에 의해 생성되는 도메인을 탐지
- ✓ Suspicious 및 알려지지 않은 악성 도메인 접속 시도 차단



[DGA 관련 필터]

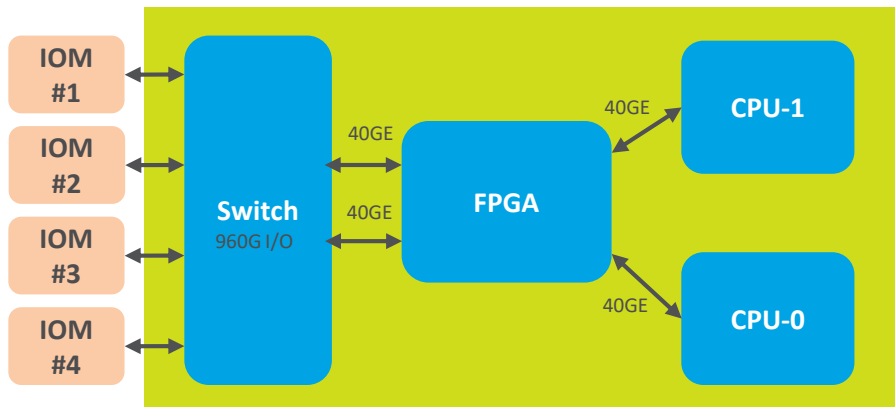
```
def generate_domain(year, month, day):  
    """Generates a domain name for the given date."""  
    domain = ""  
  
    for i in range(16):  
        year = ((year * 8 * year) >> 11) * ((year & 0xFFFFFFFF) << 17)  
        month = ((month * 4 * month) >> 15) * 16 * (month & 0xFFFFFFFF)  
        day = ((day * (day << 13)) >> 19) * ((day & 0xFFFFFFFF) << 12)  
        domain += chr(((year * month * day) % 25) + 97)  
  
    return domain
```

<Day/Month/Year을 이용 랜덤 도메인 생성 예시>

Why TippingPoint NGIPS?

: High-End IPS 설계 (FPGA Processor)

✓ 인라인 구성 IPS로서 가장 안정적인 서비스 유지와 동시에 보안 성능을 제공



NSS LABS NGIPS GROUP TEST RESULTS

Product	Exploit Block Rate ¹	NSS-Tested Throughput	3-Year TCO (US\$)
Trend Micro TippingPoint 8400TX v5.0.0.4815	99.65%	36,280 Mbps	522,477
	False Positives	Evasions Blocked	Stability and Reliability
	PASS	IS7/IS7	PASS
	Exploits Blocked	CAWS Live Exploits	Security Effectiveness
	99.36%	99.93%	99.6%

* Source : 2017 NSS Labs : NGIPS Group Test Results, Security Value Map



Why TippingPoint NGIPS?

: High-End IPS 설계 (Inspection Throughput 확장성 및 유연성)

- ✓ 운영중인 IPS H/W Model에서 서비스 Down-Time 없이 처리 트래픽 확장
- ✓ 다양한 네트워크 구간에 인터페이스 종류에 맞는 I/O 모듈을 운영중에도 설치 및 제거

TX Series	
Flexible Inspection Throughput License	3Gbps / 5Gbps / 10Gbps / 15Gbps / 20Gbps / 30Gbps / 40Gbps
Network Interface / Connectivity	I/O Module (UTP, 1G SFP, 10G SFP+, 40G QSFP+)
Onboard SSL Inspection Capacity	2Gbps (2K keys SHA256) – Optional Lic.
Stackable Inspection Throughput	Max. 120Gbps Inspection Throughput
Latency	<40 microseconds
Concurrent Sessions	120,000,000
New Connections per Second	650,000
Form Factor	8200TX-1U, 8400TX-2U
Power Supply	Dual/redundant hotswappable

Why TippingPoint NGIPS?

: 취약점 기반 구조 필터(Signature(RegEx) + Vulnerability Filter)

✓ 보안취약점 방어 기반의 보안 필터로 원천적인 보안취약점을 정확하게 방어함으로써 미탐/과탐 또는 오탐율 최소화 및 성능 극대화

TippingPoint

Competitors

예) MS12-027 취약점 공격 방어를 위해 1개의 필터로 대응

Filter Specific Info

Filter Name:

Description: ms12-027

CVE Id:

Bugtraq Id:

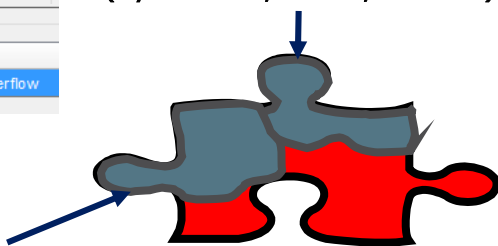
Search Results (1)

State	Name
<input checked="" type="checkbox"/>	12232: HTTP: Microsoft Windows Common Controls Buffer Overflow

예) MS12-027 취약점 공격 방어를 위해 25개의 필터로 대응

```
MS12-027 (25)
(1:13801) "FILE-IDENTIFY RTF file download request"
(1:13587) "FILE-IDENTIFY Microsoft Office Word file download request"
(1:18516) "FILE-IDENTIFY Microsoft Office Word file download request"
(1:20486) "FILE-IDENTIFY RTF file magic detected"
(1:20795) "FILE-IDENTIFY Microsoft Office Word file attachment detected"
(1:20796) "FILE-IDENTIFY Microsoft Office Word file attachment detected"
(1:21746) "FILE-IDENTIFY RTF file attachment detected"
(1:21747) "FILE-IDENTIFY RTF file attachment detected"
(1:21797) "FILE-OFFICE MSCOMCTL ActiveX control deserialization arbitrary code execution attempt"
(1:21798) "FILE-OFFICE MSCOMCTL ActiveX control deserialization arbitrary code execution attempt"
(1:21799) "FILE-OFFICE MSCOMCTL ActiveX control deserialization arbitrary code execution attempt"
(1:21800) "FILE-OFFICE MSCOMCTL ActiveX control deserialization arbitrary code execution attempt"
(1:21801) "FILE-OFFICE MSCOMCTL ActiveX control deserialization arbitrary code execution attempt"
(1:21896) "FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt"
(1:21897) "FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt"
(1:21898) "FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt"
```

Zero-Day Exploit A
(by 악성코드, 멀웨어, 공격툴...)

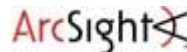
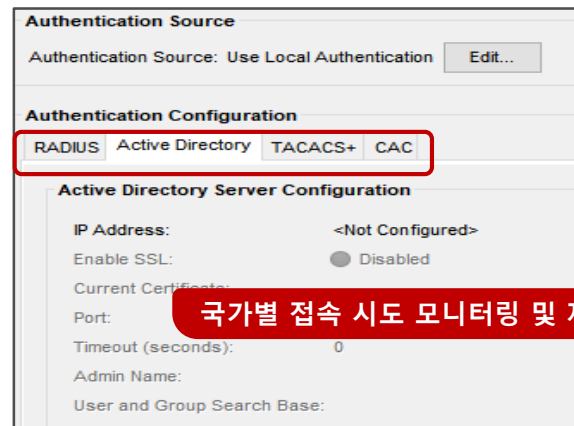
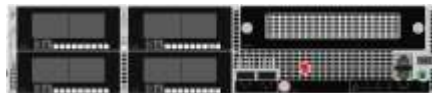
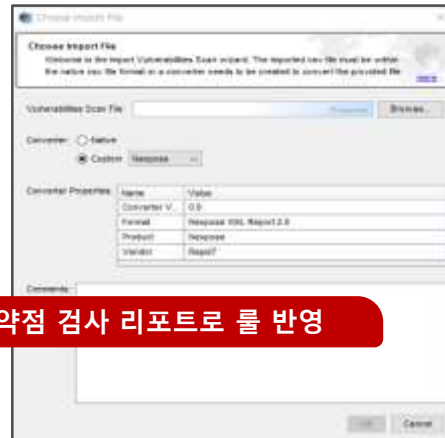
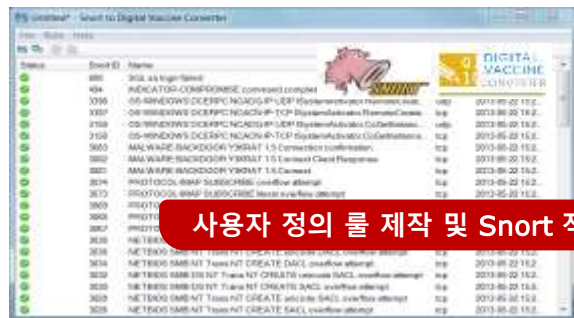


Zero-Day Exploit B
(by 악성코드, 멀웨어, 공격툴...)

Vulnerability
(보안취약점)

Why TippingPoint NGIPS?

: 사용자 환경의 보안 툴 및 시스템과 연동하여 편의성 제공



: Trend Micro APT 및 STIX Suspicious Object 연계로 보안성 극대화



차세대 IPS를 뛰어넘는 XGen™ IPS



Smart

알려진, 공개되지 않은
그리고 알려지지 않은
위협에 더 빠른 대응



Optimized

고성능으로 서비스의
안정성과 환경에
최적화한 보호



Connected

위협 인텔리전스와
중앙화된 위협 분석
개체들을 실시간 공유

감사합니다
