TREND MICRO

Security
TRENDS 2018

Security TRENDS 2018

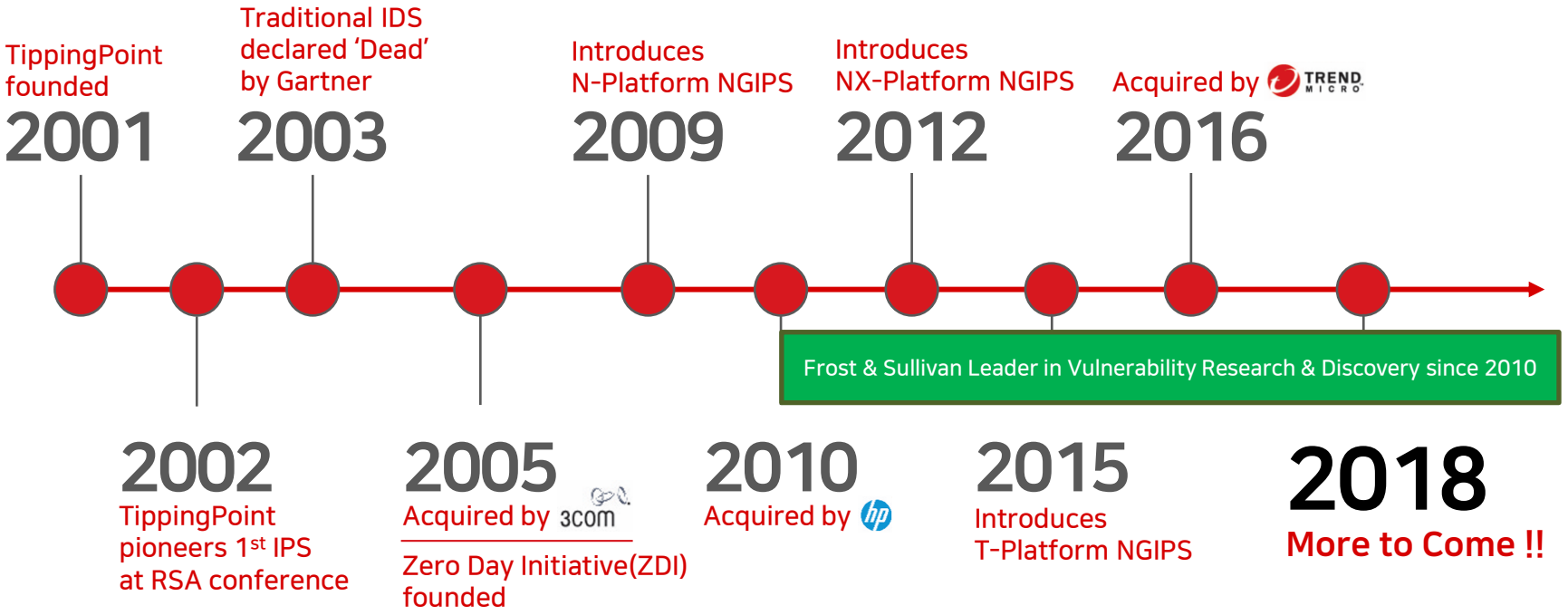
한국트렌드마이크로
김정수 이사

TREND MICRO | Security TRENDS 2018

TippingPoint is Back !!

하이브리드 데이터센터 보호를 위한 최상의 보안취약점 대응 전략

TippingPoint 의 역사...



지연 시간이 없는 고성능의 네트워크 인프라

클라우드 데이터센터

물리/가상화 데이터센터

지방 및 해외 지점/사업장

스마트팩토리

재고 관리 시스템

의료 기기

공조설비 시스템

차량 관제 시스템

경계가 없는 기업 네트워크의 확장

어디에서든 접속 가능한 IoT/IIoT 환경 확산

* IIoT(Industrial Internet of Thing) : 산업용 사물인터넷


디지털 트랜스포메이션
VS
Connected 보안취약점 대응

보안취약점 패치되면 뭐하나…여전히 취약한 버전을 사용하는데

특정 리포팅 솔루션, 지난 5·6월 패치됐지만 여전히 취약 버전 사용

(보안뉴스, 2017-10-24)

보안취약점 제보의 불법 vs 공익 논쟁, 또 다시 불붙다

정보통신망법상 불법 행위 vs 국가기관 보안성 위한 공익 활동
외국처럼 버그바운티 상시 운영해 보안성 높이자는 의견도 나와

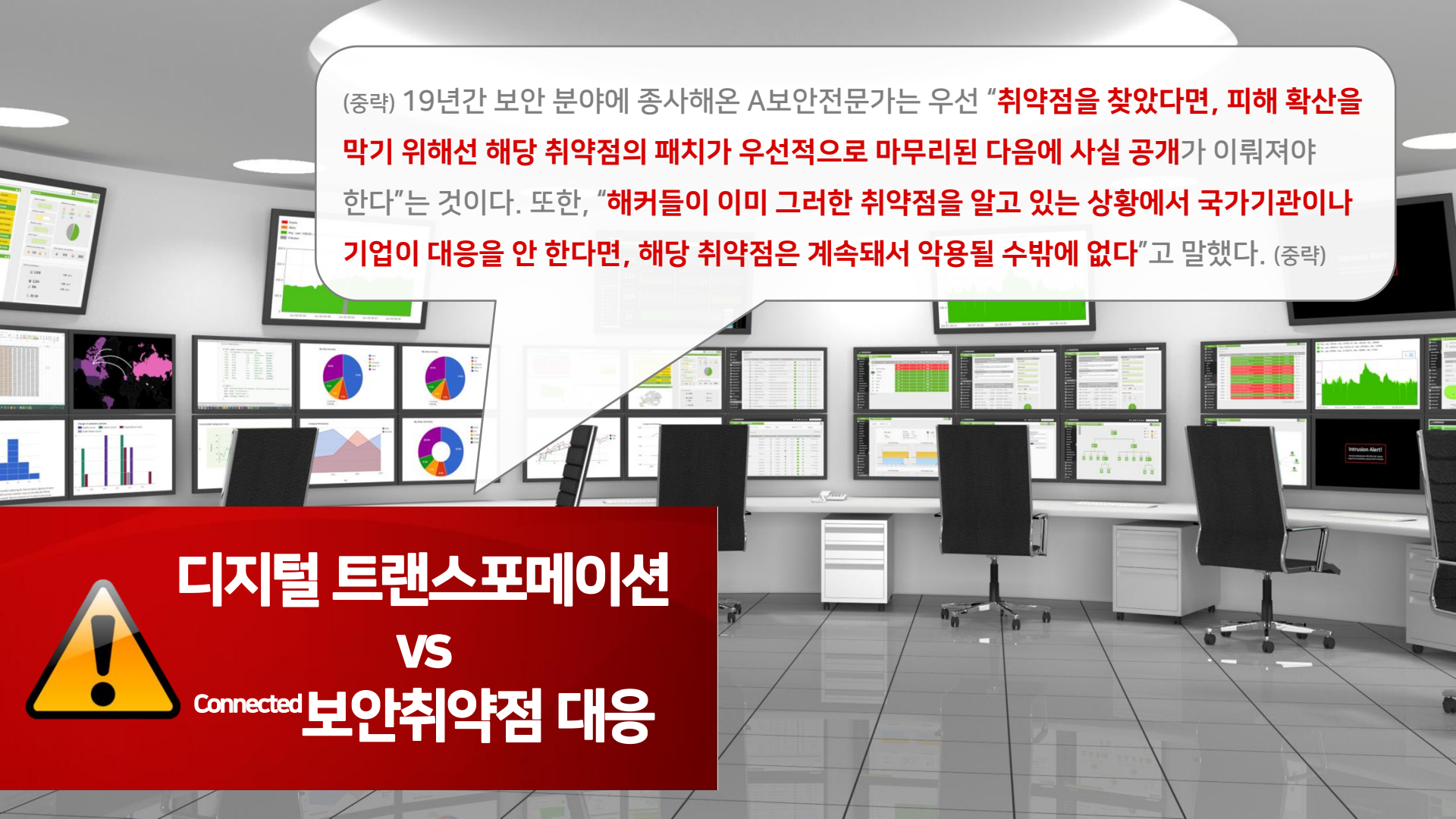
(보안뉴스, 2018-04-01)

보안에 좋다는 취약점 패치, ICS에서는 잘 안 통하는데

* ICS(Industrial Control Systems) : 산업 제어 시스템

보안취약점 발견하고 패치하는 것, 보안 위생 수준 향상시켜
ICS는 패치 위해 가동 멈추기 힘들고, 기기들도 매우 오래돼

(보안뉴스, 2017-06-22)

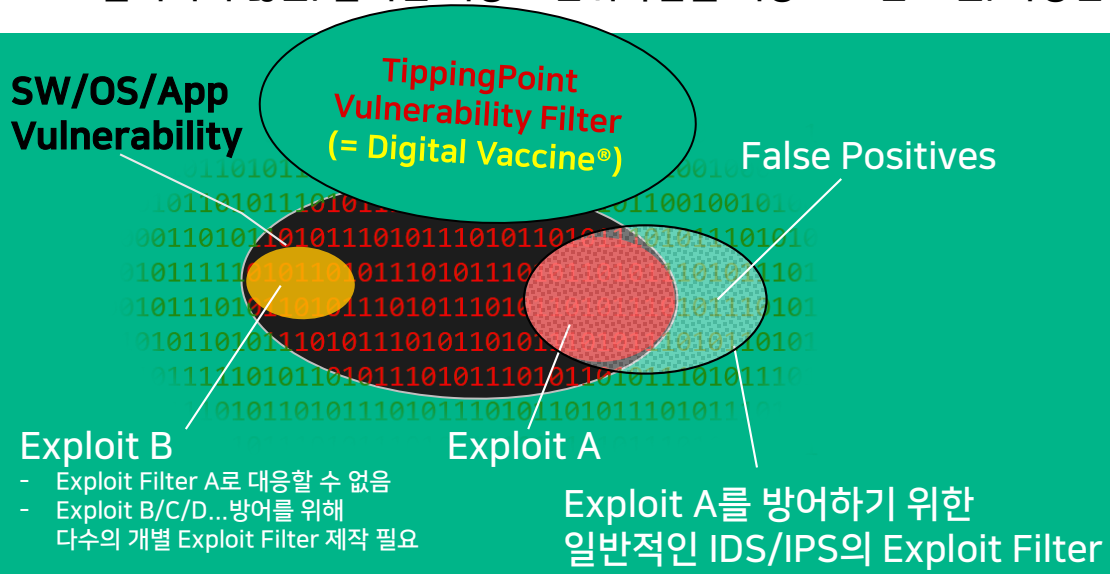

(중략) 19년간 보안 분야에 종사해온 A보안전문가는 우선 "취약점을 찾았다면, 피해 확산을 막기 위해선 해당 취약점의 패치가 우선적으로 마무리된 다음에 사실 공개가 이뤄져야 한다"는 것이다. 또한, "해커들이 이미 그러한 취약점을 알고 있는 상황에서 국가기관이나 기업이 대응을 안 한다면, 해당 취약점은 계속돼서 악용될 수밖에 없다"고 말했다. (중략)
디지털 트랜스포메이션
VS
Connected 보안취약점 대응

TippingPoint 는
보안취약점 을 어떻게 대응하고 있는가?

보안취약점 방어 기반의 필터 : Vulnerability Filter

TREND MICRO | Security TRENDS 2018

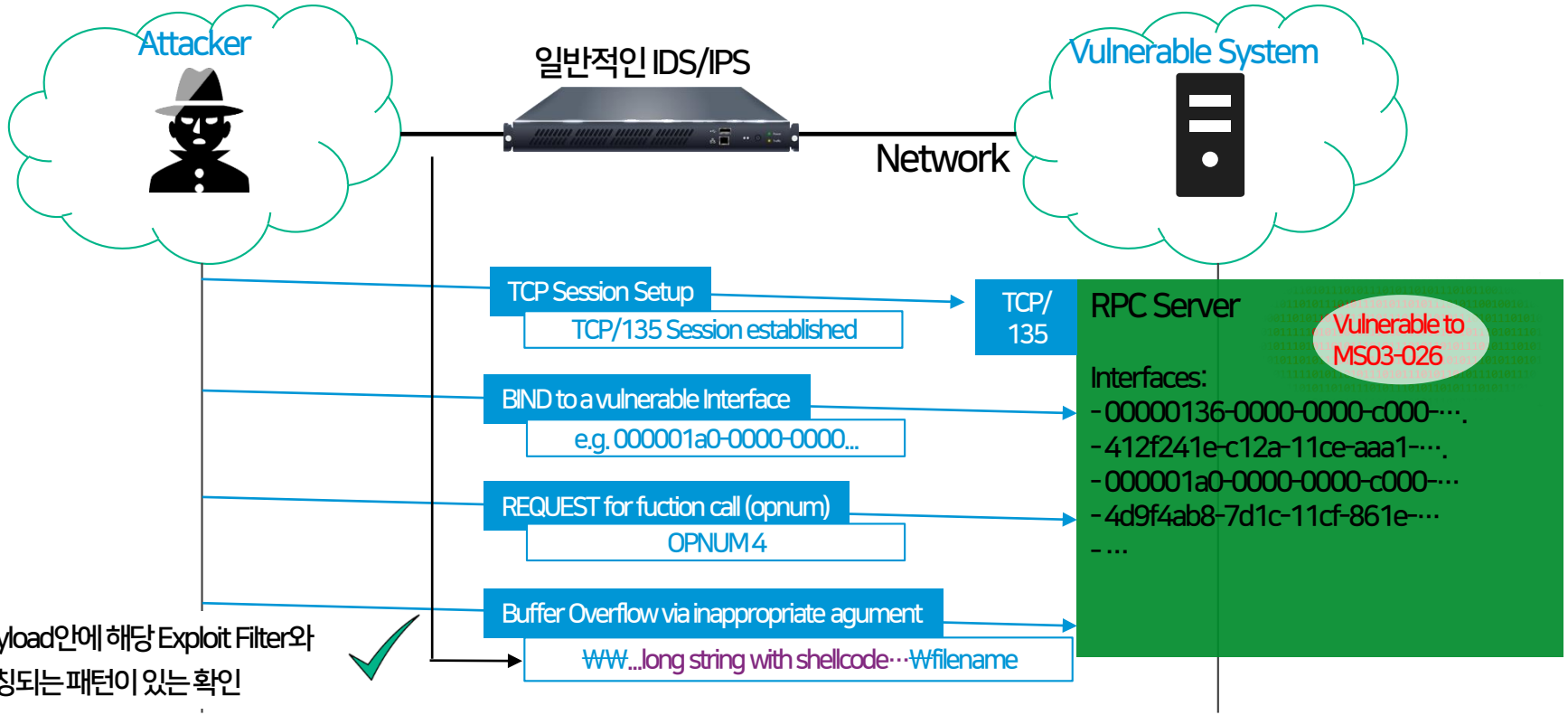
- 2004년 보안업계 최초로 Vulnerability Filter 소개
- 알려지지 않은/알려진 해당 보안취약점을 대상으로 한 모든/다양한 공격 요소를 대응 가능



Term	Definition
Vulnerability	**SW/OS/App의 태생적인 보안 결함**
Exploit	해당 보안취약점(Vulnerability)을 활용한/활용키 위한 다양한 공격 방식 : 악성코드, 멀웨어, 공격툴 등등
Exploit Filter	• 손쉽게 제작할 수 있으나 특정 Exploit 만 대응할 수 있고, 변종 Exploit 대응시, 다수의 개별 필터 제작 필요 • 성능상의 이유로 최대한 "일반적인 " 보안 필터로 제작 및 배포, 이에 따른 오탐/미탐/과탐 문제 발생
Vulnerability Filter	**해당 보안취약점(Vulnerability)을 활용한/활용키 위한 다양한 Exploit를 대응 가능한 보안취약점 방어 기반의 필터**

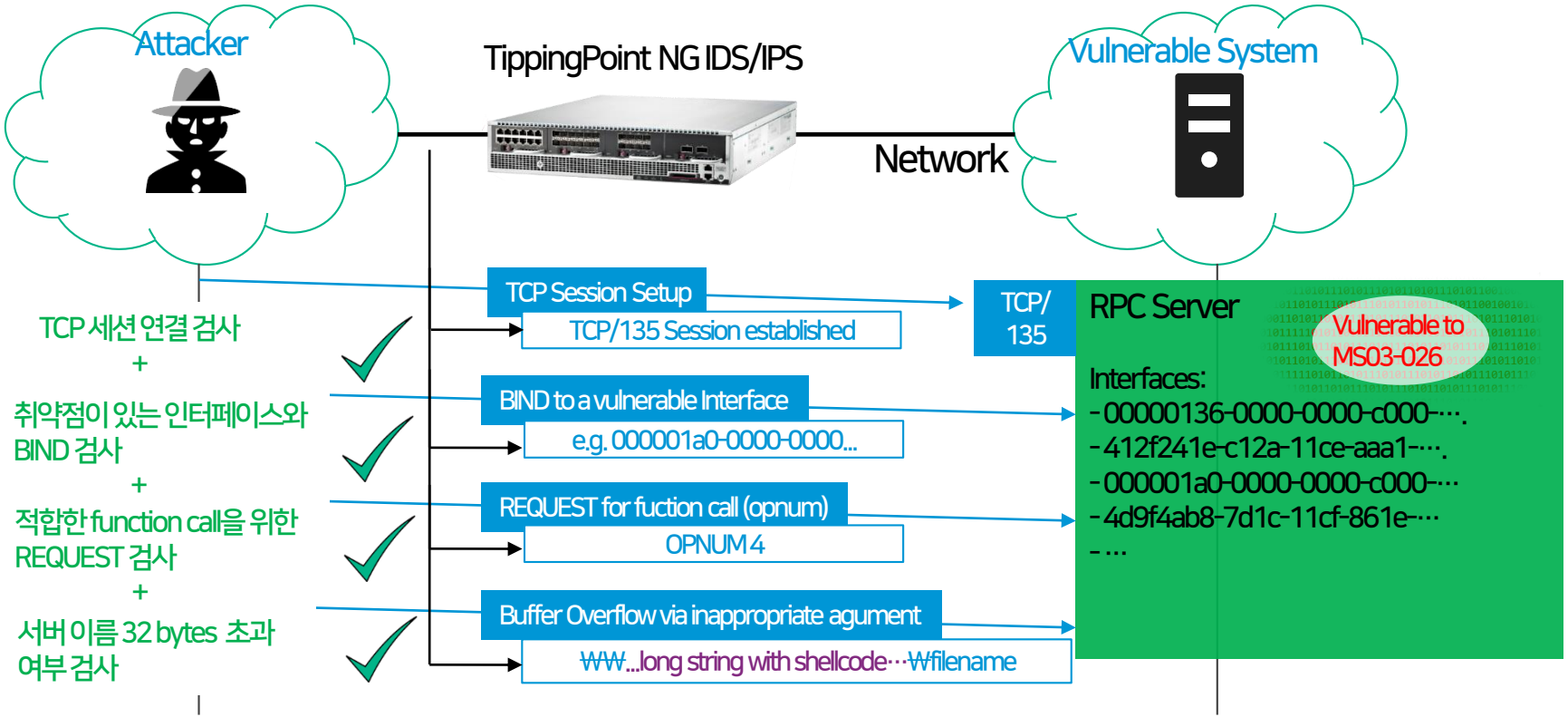
개별/변종/다수의 Exploit 방어보다
원천적인 보안취약점(Vulnerability) 방어가 중요!

일반적인 IDS/IPS의 Exploit Filter 대응 방식



단순 패턴 매칭 방식의 Exploit Filter = 오탐/미탐/과탐 요인

TippingPoint 보안취약점 방어 기반 필터 대응 방식



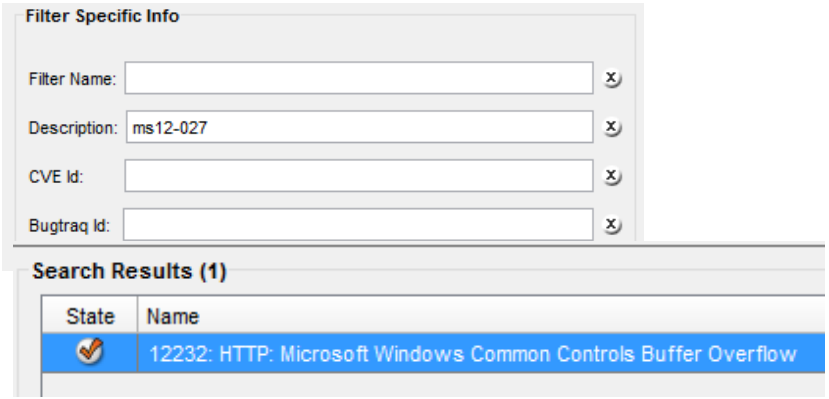
보안취약점 방어 기반 필터를 활용하여 "모든 공격 요소를 검사",
원천적인 보안취약점을 정확하게 방어함으로써 오탐/미탐/과탐 최소화

TippingPoint 보안취약점 방어 기반 필터 vs 일반적인 IDS/IPS의 Exploit Filter (예시)

TREND MICRO | Security TRENDS 2018

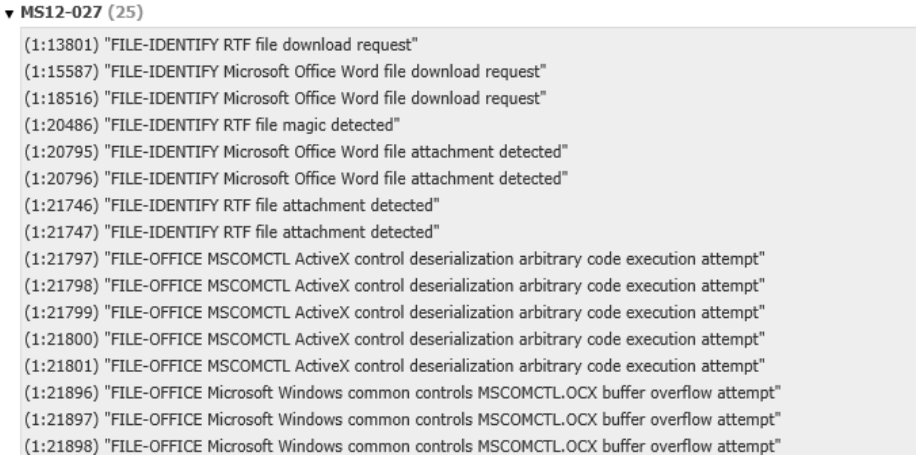
[TippingPoint]

MS12-027 보안취약점을 방어하기 위해
총 13,000개 이상의 필터 중 "1개의 필터"로 대응!!



[타사 IDS/IPS]

동일한 MS12-027 보안취약점을 방어하기 위해
총 27,000개 이상의 필터 중 "25개의 필터" 필요
(변종 Exploit 대응을 위해서는 추가적인 필터 적용 필요)



Rethink SecOps for IDS/IPS !! :
NG IDPS 도입시, 보안 운영 효율성 부문도 적극 검토 요구됨

TippingPoint 업계 최고의 버그 바운티(Bug Bounty) 프로그램 운영

- 2005년 시작된 "**보안취약점 신고/제보 보상 프로그램**"으로, 보안취약점 발견/연구에 있어서 **특정 벤더 제품에 국한되어 있지 않는 유일한 Bug Bounty 프로그램**
- 동종 IDS/IPS업계에서 **가장 큰 규모의 모범적인 Bug Bounty 로 성장**
- 80여 개국의 3,000명이 넘는 인원이 내/외부 보안연구원 및 화이트 해커로 활동
- 신규 보안취약점 발견/연구 및 신고/제보 보상을 위해 매년 수십억원의 지속적인 투자 유지

신고/제보된 보안취약점의 자세한 정보는 패치가 나오기 전까지는
"신고/제보자 – TippingPoint ZDI – 보안취약점이 발견된 제조사" 만 공유

보안패치 출시 전에 관련 보안취약점을 즉각적으로 간편하게 방어할 수 있는

네트워크상의 가상 패치 (Network Virtual Patch)

It is TippingPoint DNA!! : Faster Protection Against Unknown Threats

TippingPoint NG IDPS는 해당 보안취약점을 방어할 수 있는 Digital Vaccine®을 업데이트!!

TippingPoint 운영 고객사는 해당 보안취약점 패치 출시 전부터 즉각적인 방어 시작!

일반 IDS/IPS업체 필터 제작 시작

발견된 보안취약점 ZDI 신고/제보

ZDI는 관련 제조사에 해당 보안취약점 정보 공유 및 패치를 개발토록 권고

(데드라인 4개월 / 모바일 관련 취약점의 경우, 데드라인 1개월)

관련 제조사의 회신을 받음

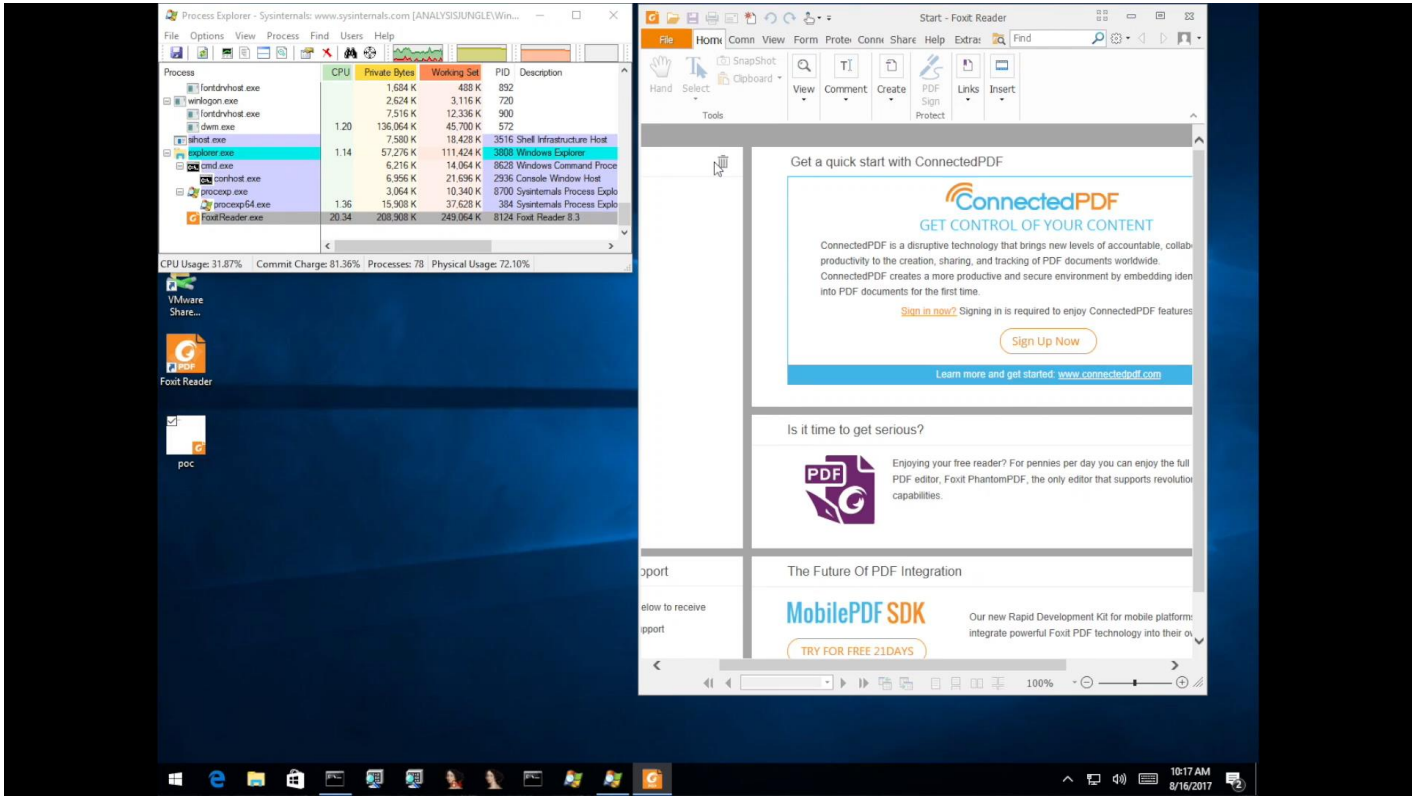
(패치 개발 가능 여부 및 데드라인 내의 패치 개발 스케줄)

데드라인 내에 관련 제조사의 보안취약점 패치 개발

(패치 개발이 미진한 부분은 추가 패치 개발로 보완)

ZDI 혹은 관련 제조사에서 해당 보안취약점 정보 공개

2017년 Foxit PDF Reader 보안취약점 발견 사례



보안패치 출시 유무와 무관하게 관련 보안취약점을 즉각적으로 간편하게 방어할 수 있는

네트워크상의 가상 패치 (Network Virtual Patch)

TREND MICRO | Security TRENDS 2018

<2017년 Foxit PDF Reader 보안취약점 발견/대응 사례>

2017년 6월 22일

발견된 보안취약점 ZDI 신고/제보

2017년 6월 22일

TippingPoint NG IDPS는 해당 보안취약점을 방어할 수 있는 Digital Vaccine®을 업데이트!!

Filter Name : ZDI-CAN-451

2017년 7월 20일

ZDI는 관련 제조사에 해당 보안취약점 정보 공유 및 패치를 개발토록 권고

(데드라인 4개월 / 모바일 관련 취약점의 경우, 데드라인 1개월)

2017년 8월 17일

Foxit으로부터 패치하지 못하겠다는 회신을 받음

2017년 8월 26일

ZDI에서 관련 보안취약점 정보(CVE2017-10951) 대외 공개

TippingPoint 운영 고객사는 해당 보안취약점 패치 출시 전부터 즉각적인 방어 [illegible]

결국, 보안패치 개발하여 릴리즈

실시간 보안취약점 발견을 위한 화이트 해커 콘테스트 개최

- 2007년부터 매년 개최 (상반기/2일간/수억원의 상금)
- 각종 웹브라우저, 엔터프라이즈 애플리케이션, 가상화솔루션, 운영체제 등에 대한 보안취약점을 실시간으로 발견 및 해킹

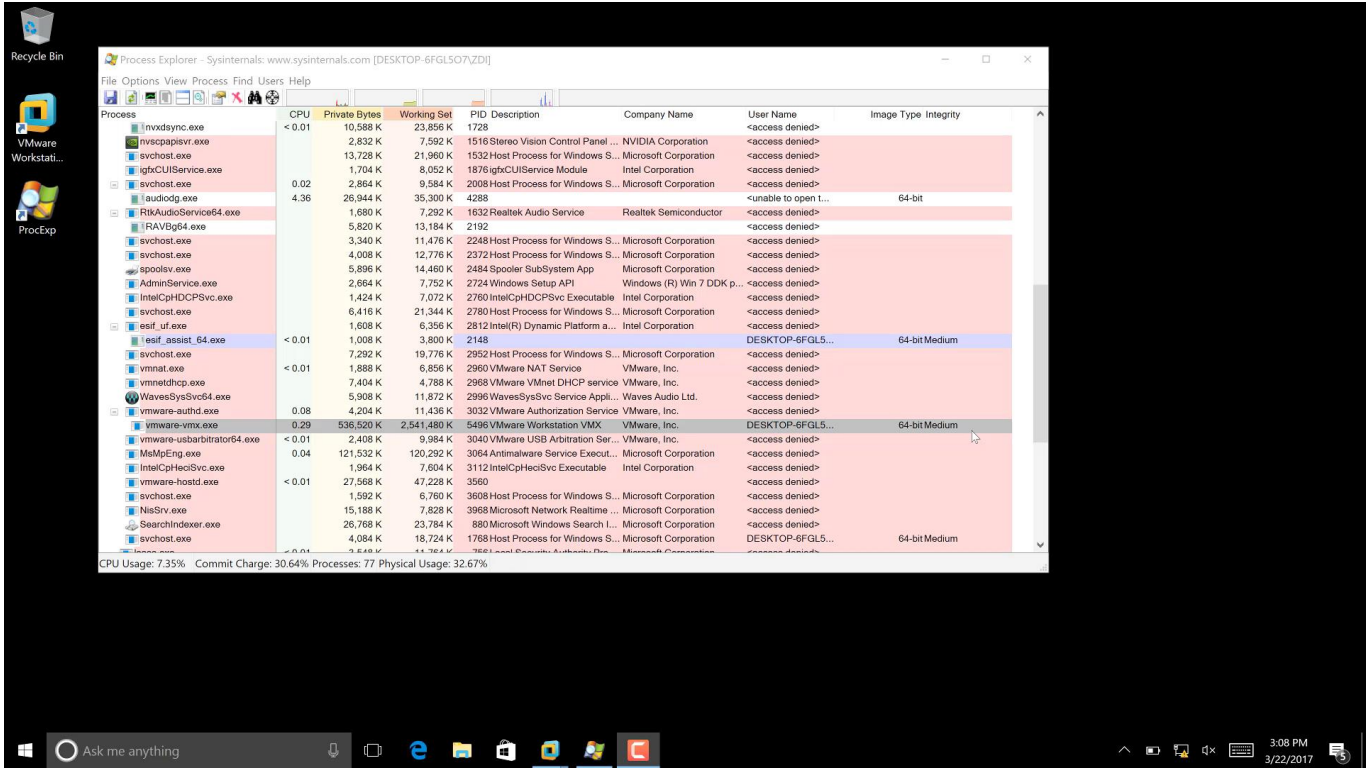
- 2017년 : Vmware Escape 공격 사례 발견
- 2018년 : 미출시 MS Windows도 포함

- 2012년부터 매년 개최 (상반기/2일간/수억원의 상금)
- 각종 "모바일 플랫폼"에 대한 보안취약점을 실시간으로 발견 및 해킹

- 11개의 서로 다른 Bug를 사용(Pwn2Own 역사상 가장 긴 Exploit Chain)하여 삼성 갤럭시 S8상에서 코드 실행 사례 발견

실시간 보안취약점 발견을 위한 화이트 해커 콘테스트 개최

< 2017년 Pwn2Own에서 발견된 Vmware Escape 공격 사례 >



Pwn2Own을 통해 발견된 보안취약점은 TippingPoint 고객이 즉각적으로 방어할 수 있도록 Digital Vaccine으로 탑재

ZDI-18-151	ZDI-CAN-5345	Apple	CVE-2017-7172	2018-02-07	2018-02-07
(Pwn2Own) Apple Safari UIProcess Out-Of-Bounds Access Privilege Escalation Vulnerability					
ZDI-18-150	ZDI-CAN-5344	Apple	CVE-2017-7160	2018-02-07	2018-02-07
(Pwn2Own) Apple Safari FTL JIT Integer Overflow Remote Code Execution Vulnerability					
ZDI-18-149	ZDI-CAN-5343	Apple	CVE-2017-7162	2018-02-07	2018-02-07
(Pwn2Own) Apple iOS backboardd Double Free Privilege Escalation Vulnerability					
ZDI-18-148	ZDI-CAN-5342	Apple	CVE-2017-13866	2018-02-07	2018-02-07
(Pwn2Own) Apple Safari DFG JIT Type Confusion Remote Code Execution Vulnerability					
ZDI-18-147	ZDI-CAN-5341	Apple	CVE-2017-7171	2018-02-07	2018-02-07
(Pwn2Own) Apple iOS backboardd Untrusted Pointer Dereference Privilege Escalation Vulnerability					
ZDI-18-146	ZDI-CAN-5340	Apple	CVE-2017-13870	2018-02-07	2018-02-07
(Pwn2Own) Apple Safari MutationObserver Use-After-Free Remote Code Execution Vulnerability					

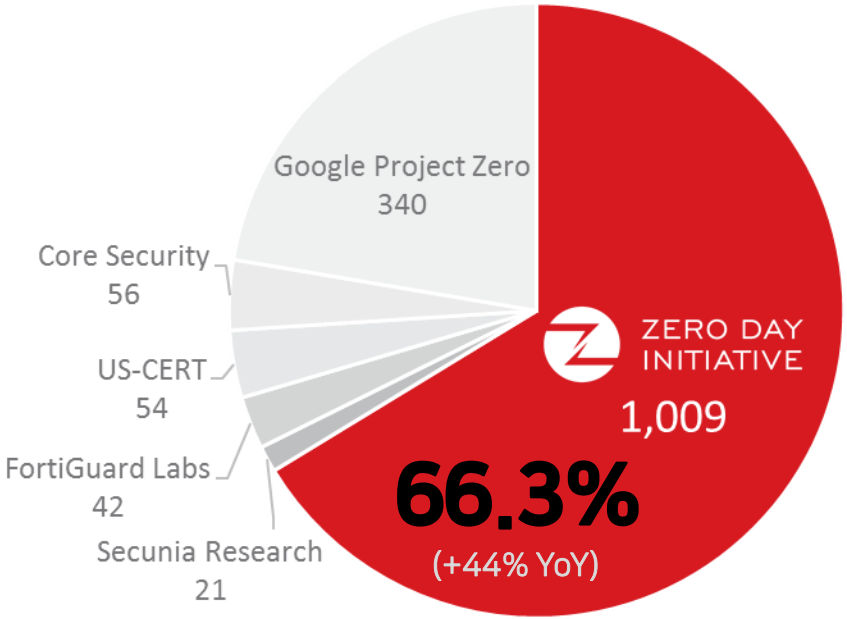
TippingPoint Zero Day Initiative 에서 발견하여 부여한 2017년 CVE

TREND MICRO

Security TRENDS 2018

CVE-2017-3289, CVE-2016-0165, CVE-2016-2123, CVE-2016-6814, CVE-2016-8204, CVE-2016-8205, CVE-2016-8206, CVE-2016-8207, CVE-2016-8211, CVE-2016-8341, CVE-2016-8341, CVE-2016-8519, CVE-2017-0011, CVE-2017-0015, CVE-20170018, CVE-2017-0032, CVE-2017-0047, CVE-2017-0067, CVE-2017-0094, CVE-2017-0155, CVE-2017-0158, CVE-2017-0226, CVE-2017-0228, CVE-2017-0233, CVE-2017-0234, CVE-2017-0236, CVE-2017-0238, CVE-2017-0240, CVE-2017-0240, CVE2017-0250, CVE-2017-0266, CVE-2017-0285, CVE-2017-0285, CVE-2017-0291, CVE-2017-0291, CVE-2017-0291, CVE-2017-0292, CVE-2017-0293, CVE-2017-0296, CVE-2017-10940, CVE-2017-10941, CVE-2017-10942, CVE-2017-10943, CVE-201710944, CVE-2017-10945, CVE-2017-10946, CVE-2017-10947, CVE-2017-10948, CVE-2017-10949, CVE-2017-10950, CVE-2017-10951, CVE-2017-10952, CVE-2017-10953, CVE-2017-10954, CVE-2017-10955, CVE-2017-11209, CVE-2017-11210, CVE2017-11211, CVE-2017-11212, CVE-2017-11214, CVE-2017-11216, CVE-2017-11216, CVE-2017-11217, CVE-2017-11218, CVE-2017-11219, CVE-2017-11223, CVE-2017-11224, CVE-2017-11227, CVE-2017-11228, CVE-2017-11230, CVE-2017-11231, CVE-2017-11231, CVE-2017-11232, CVE-2017-11233, CVE-2017-11234, CVE-2017-11235, CVE-2017-11236, CVE-2017-11237, CVE-2017-11238, CVE-2017-11239, CVE-2017-11239, CVE-2017-11241, CVE-2017-11242, CVE-2017-11242, CVE-201711243, CVE-2017-11244, CVE-2017-11244, CVE-2017-11245, CVE-2017-11246, CVE-2017-11248, CVE-2017-11249, CVE-2017-11251, CVE-2017-11252, CVE-2017-11255, CVE-2017-11256, CVE-2017-11256, CVE-2017-11257, CVE-2017-11258, CVE2017-11259, CVE-2017-11259, CVE-2017-11260, CVE-2017-11261, CVE-2017-11261, CVE-2017-11265, CVE-2017-11267, CVE-2017-11268, CVE-2017-11269, CVE-2017-11270, CVE-2017-11271, CVE-2017-11274, CVE-2017-11382, CVE-2017-11383, CVE-2017-11384, CVE-2017-11385, CVE-2017-11386, CVE-2017-11387, CVE-2017-11388, CVE-2017-11388, CVE-2017-11389, CVE-2017-11390, CVE-2017-11391, CVE-2017-11392, CVE-2017-11393, CVE-2017-11394, CVE-2017-11762, CVE-201711779, CVE-2017-11781, CVE-2017-11790, CVE-2017-11794, CVE-2017-11800, CVE-2017-11812, CVE-2017-12263, CVE-2017-12487, CVE-2017-12488, CVE-2017-12489, CVE-2017-12490, CVE-2017-12491, CVE-2017-12492, CVE-2017-12493, CVE2017-12494, CVE-2017-12495, CVE-2017-12496, CVE-2017-12497, CVE-2017-12498, CVE-2017-12499, CVE-2017-12500, CVE-2017-12501, CVE-2017-12502, CVE-2017-12503, CVE-2017-12504, CVE-2017-12505, CVE-2017-12506, CVE-2017-12507, CVE-2017-12508, CVE-2017-12509, CVE-2017-12510, CVE-2017-12511, CVE-2017-12512, CVE-2017-12513, CVE-2017-12514, CVE-2017-12515, CVE-2017-12516, CVE-2017-12517, CVE-2017-12518, CVE-2017-12519, CVE-2017-12520, CVE-201712521, CVE-2017-12522, CVE-2017-12523, CVE-2017-12524, CVE-2017-12525, CVE-2017-12526, CVE-2017-12554, CVE-2017-12556, CVE-2017-12557, CVE-2017-12558, CVE-2017-12559, CVE-2017-12560, CVE-2017-12561, CVE-2017-12694, CVE2017-12705, CVE-2017-12707, CVE-2017-12710, CVE-2017-12713, CVE-2017-13982, CVE-2017-13983, CVE-2017-13984, CVE-2017-13985, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-201714078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-201714078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14078, CVE-2017-14079, CVE-2017-14079, CVE-2017-14079, CVE-2017-14079, CVE-2017-14080, CVE-2017-14081, CVE-2017-14081, CVE-2017-14088, CVE2017-14088, CVE-2017-14350, CVE-2017-2354, CVE-2017-2430, CVE-2017-2432, CVE-2017-2454, CVE-2017-2462, CVE-2017-2463, CVE-2017-2481, CVE-2017-2491, CVE-2017-2506, CVE-2017-2525, CVE-2017-2526, CVE-2017-2530, CVE-2017-2533, CVE-2017-2534, CVE-2017-6977, CVE-2017-2535, CVE-2017-2536, CVE-2017-2537, CVE-2017-2538, CVE-2017-2539, CVE-2017-2540, CVE-2017-2541, CVE-2017-2542, CVE-2017-2543, CVE-2017-2544, CVE-2017-2545, CVE-2017-2546, CVE-20172547, CVE-2017-2548, CVE-2017-2939, CVE-2017-2941, CVE-2017-2946, CVE-2017-2946, CVE-2017-2949, CVE-2017-2949, CVE-2017-2949, CVE-2017-2949, CVE-2017-2949, CVE-2017-2949, CVE-2017-2949, CVE-2017-2949, CVE-2017-2949, CVE2017-2949, CVE-2017-2949, CVE-2017-2949, CVE-2017-2949, CVE-2017-2949, CVE-2017-2949, CVE-2017-2949, CVE-2017-2950, CVE-2017-2951, CVE-2017-2959, CVE-2017-2960, CVE-2017-2961, CVE-2017-2962, CVE-2017-2963, CVE-2017-2964, CVE-2017-2965, CVE-2017-2966, CVE-2017-2967, CVE-2017-2970, CVE-2017-2974, CVE-2017-2975, CVE-2017-2976, CVE-2017-2977, CVE-2017-2978, CVE-2017-2979, CVE-2017-2981, CVE-2017-2994, CVE-2017-2994, CVE-2017-2995, CVE-20173001, CVE-2017-3001, CVE-2017-3001, CVE-2017-3001, CVE-2017-3001, CVE-2017-3009, CVE-2017-3019, CVE-2017-3020, CVE-2017-3021, CVE-2017-3022, CVE-2017-3023, CVE-2017-3028, CVE-2017-3029, CVE-2017-3031, CVE2017-3031, CVE-2017-3032, CVE-2017-3033, CVE-2017-3034, CVE-2017-3035, CVE-2017-3036, CVE-2017-3040, CVE-2017-3042, CVE-2017-3042, CVE-2017-3042, CVE-2017-3042, CVE-2017-3043, CVE-2017-3044, CVE-2017-3045, CVE-2017-3046, CVE-2017-3047, CVE-2017-3048, CVE-2017-3049, CVE-2017-3050, CVE-2017-3051, CVE-2017-3052, CVE-2017-3053, CVE-2017-3055, CVE-2017-3056, CVE-2017-3057, CVE-2017-3058, CVE-2017-3059, CVE-2017-3060, CVE-2017-3060, CVE-20173062, CVE-2017-3063, CVE-2017-3075, CVE-2017-3080, CVE-2017-3082, CVE-2017-3083, CVE-2017-3084, CVE-2017-3085, CVE-2017-3091, CVE-2017-3100, CVE-2017-3113, CVE-2017-3115, CVE-2017-3120, CVE-2017-3121, CVE-2017-3121, CVE2017-3121, CVE-2017-3122, CVE-2017-3122, CVE-2017-3122, CVE-2017-3123, CVE-2017-3124, CVE-2017-3230, CVE-2017-3248, CVE-2017-3272, CVE-2017-4902, CVE-2017-4902, CVE-2017-4903, CVE-2017-4904, CVE-2017-4905, CVE-2017-4908, CVE-2017-4910, CVE-2017-4911, CVE-2017-4911, CVE-2017-4911, CVE-2017-4911, CVE-2017-4911, CVE-2017-4924, CVE-2017-4997, CVE-2017-5053, CVE-2017-5059, CVE-2017-5154, CVE-2017-5152, CVE-2017-5177, CVE-2017-5428, CVE-20175448, CVE-2017-5789, CVE-2017-5790, CVE-2017-5791, CVE-2017-5792, CVE-2017-5793, CVE-2017-5794, CVE-2017-5795, CVE-2017-5797, CVE-2017-5804, CVE-2017-5805, CVE-2017-5806, CVE-2017-5810, CVE-2017-5811, CVE-2017-5812, CVE2017-5816, CVE-2017-5817, CVE-2017-5818, CVE-2017-5819, CVE-2017-5820, CVE-2017-5821, CVE-2017-5822, CVE-2017-5823, CVE-2017-6020, CVE-2017-6023, CVE-2017-6621, CVE-2017-6622, CVE-2017-6635, CVE-2017-6636, CVE-2017-6637, CVE-2017-6669, CVE-2017-6669, CVE-2017-6669, CVE-2017-6983, CVE-2017-6990, CVE-2017-6991, CVE-2017-7000, CVE-2017-7001, CVE-2017-7002, CVE-2017-7052, CVE-2017-7053, CVE-2017-7071, CVE-2017-7091, CVE-2017-7092, CVE-20177093, CVE-2017-7095, CVE-2017-7111, CVE-2017-7184, CVE-2017-7929, CVE-2017-8002, CVE-2017-8002, CVE-2017-8002, CVE-2017-8003, CVE-2017-8007, CVE-2017-8011, CVE-2017-8012, CVE-2017-8013, CVE-2017-8015, CVE-2017-8453, CVE2017-8454, CVE-2017-8455, CVE-2017-8460, CVE-2017-8465, CVE-2017-8465, CVE-2017-8466, CVE-2017-8467, CVE-2017-8468, CVE-2017-8486, CVE-2017-8496, CVE-2017-8503, CVE-2017-8532, CVE-2017-8547, CVE-2017-8553, CVE-2017-8575, CVE-2017-8576, CVE-2017-8577, CVE-2017-8578, CVE-2017-8579, CVE-2017-8580, CVE-2017-8590, CVE-2017-8598, CVE-2017-8601, CVE-2017-8601, CVE-2017-8601, CVE-2017-8624, CVE-2017-8631, CVE-2017-8633, CVE-2017-8641, CVE-20178653, CVE-2017-8661, CVE-2017-8676, CVE-2017-8689, CVE-2017-8692, CVE-2017-8717, CVE-2017-8718, CVE-2017-8720, CVE-2017-8728, CVE-2017-8737, CVE-2017-8738, CVE-2017-8738, CVE-2017-8743, CVE-2017-8744, CVE-2017-8750, CVE2017-8944, CVE-2017-8947, CVE-2017-8954, CVE-2017-8955, CVE-2017-8956, CVE-2017-8957, CVE-2017-8994, CVE-2017-8994, CVE-2017-9634, CVE-2017-9634, CVE-2017-9636, CVE-2017-9636, CVE-2017-9636, CVE-2017-9636, CVE-2017-9636, CVE-2017-9638, CVE-2017-9638, CVE-2017-9638, CVE-2017-9638, CVE-2017-9638, CVE-2017-9639, CVE-2017-9659, CVE-2017-9659, CVE-2017-9660, CVE-2017-9662 ……

TippingPoint with Market-leading Vulnerability Research



Source: Frost & Sullivan. Analysis of the Global Public Vulnerability Research Market 2017 (February 2018)

Microsoft

Adobe

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

- ICS(산업제어시스템) 보안취약점을 가장 많이 발견!
- Adobe/MS 보안취약점을 가장 많이 발견!

ZERO DAY INITIATIVE

LEADER in
Global Vulnerability Research and Discovery
SINCE 2007

FROST & SULLIVAN


TippingPoint

TippingPoint 8200TX

TippingPoint 8400TX

TippingPoint 8200TX

1U Form Factor

+40Gbps Inspection Throughput

120,000,000 Concurrent Session

<40µs Latency

On-box SSL

Pay as you grow

120 Gbps

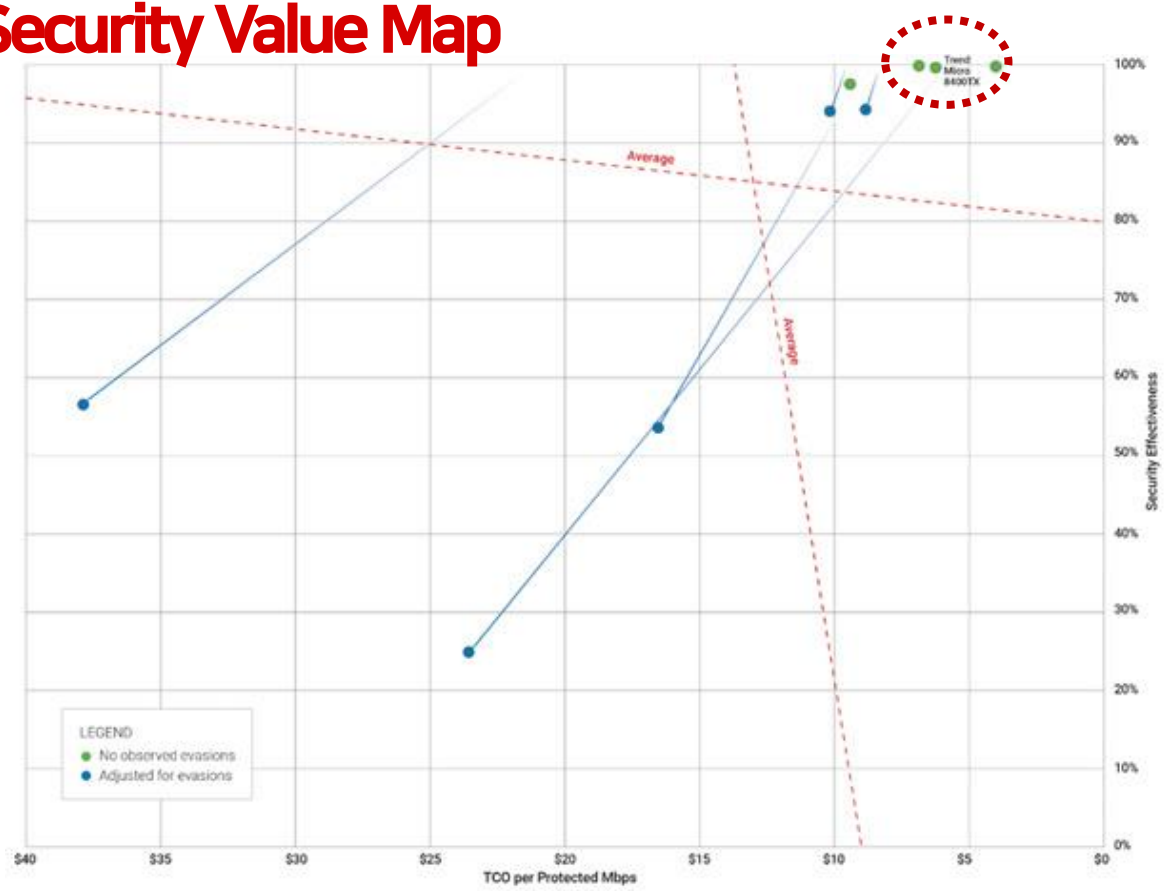
80 Gbps

3~40 Gbps

SSL Throughput also can be scalable from 2Gbps to 10Gbps

2017 NSS Labs : NGIPS Group Test Results

Security Value Map



TREND MICRO | Security TRENDS 2018

NSS LABS RECOMMENDED

Trend Micro™ TippingPoint®

RECOMMENDED

99.6% Security Effectiveness

NSS Labs 2017 NGIPS Group Test

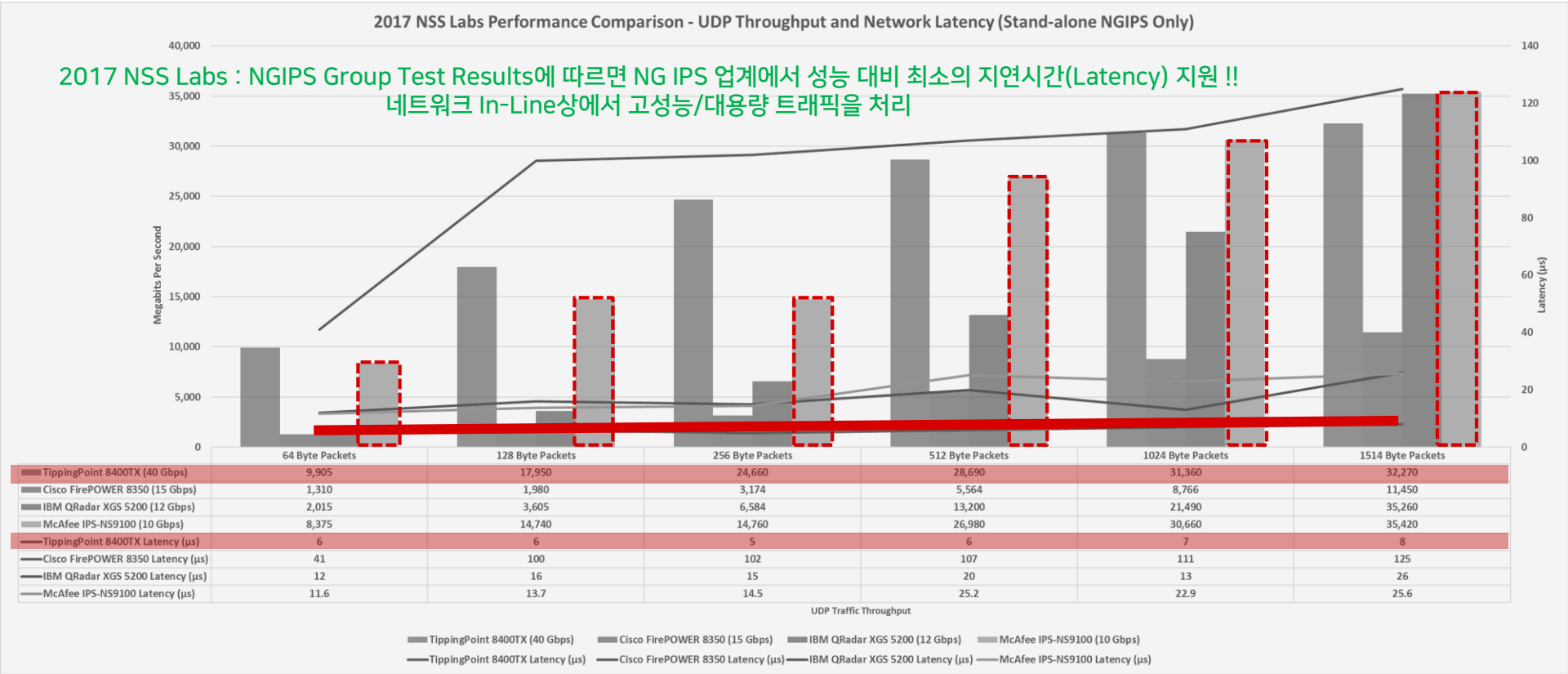
TREND MICRO TIPPINGPOINT RECOMMENDED DATA CENTER IPS

NSS LABS RECOMMENDED

NSS LABS 2018 DCIPS GROUP TEST

2017 NSS Labs : NGIPS Group Test Results
Latency & Performance

TREND MICRO | Security TRENDS 2018



	64 Byte Packets	128 Byte Packets	256 Byte Packets	512 Byte Packets	1024 Byte Packets	1514 Byte Packets
TippingPoint 8400TX (40 Gbps)	9,905	17,950	24,660	28,690	31,360	32,270
Cisco FirePOWER 8350 (15 Gbps)	1,310	1,980	3,174	5,564	8,766	11,450
IBM QRadar XGS 5200 (12 Gbps)	2,015	3,605	6,584	13,200	21,490	35,260
McAfee IPS-NS9100 (10 Gbps)	8,375	14,740	14,760	26,980	30,660	35,420
TippingPoint 8400TX Latency (µs)	6	6	5	6	7	8
Cisco FirePOWER 8350 Latency (µs)	41	100	102	107	111	125
IBM QRadar XGS 5200 Latency (µs)	12	16	15	20	13	26
McAfee IPS-NS9100 Latency (µs)	11.6	13.7	14.5	25.2	22.9	25.6

* Source : 2017 NSS Labs : NGIPS Group Test Results, Latency & Performance

TippingPoint
XGen IDPS

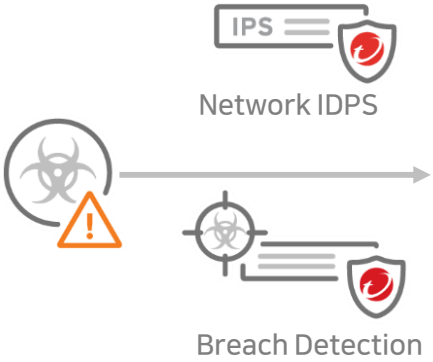
TREND MICRO | Security TRENDS 2018

Next-Gen IDPS

- Detection of Known & Unknown Vulnerabilities
- Context-aware Traffic Inspection
- IP/DNS & URL Reputation
- Encrypted Traffic Inspection
- Geo/Location Filtering
- Active Directory Integration
- Comprehensive Network Traffic Visualization
- Third Party Integration

XGen IDPS

- **Machine Learning**
- **DGA(Domain Generation Algorithms) Defense**
- **High-Performance Malware Filter Package**
  - Bot Activity
  - Data Exfiltration
  - Ransomware
  - Mobile
  - Command & Control
  - Phone Home
- **Detection/Remediation of UNDISCLOSED Vulnerabilities**
- **Automated Sandbox Analysis**
- **Lateral Movement Detection**

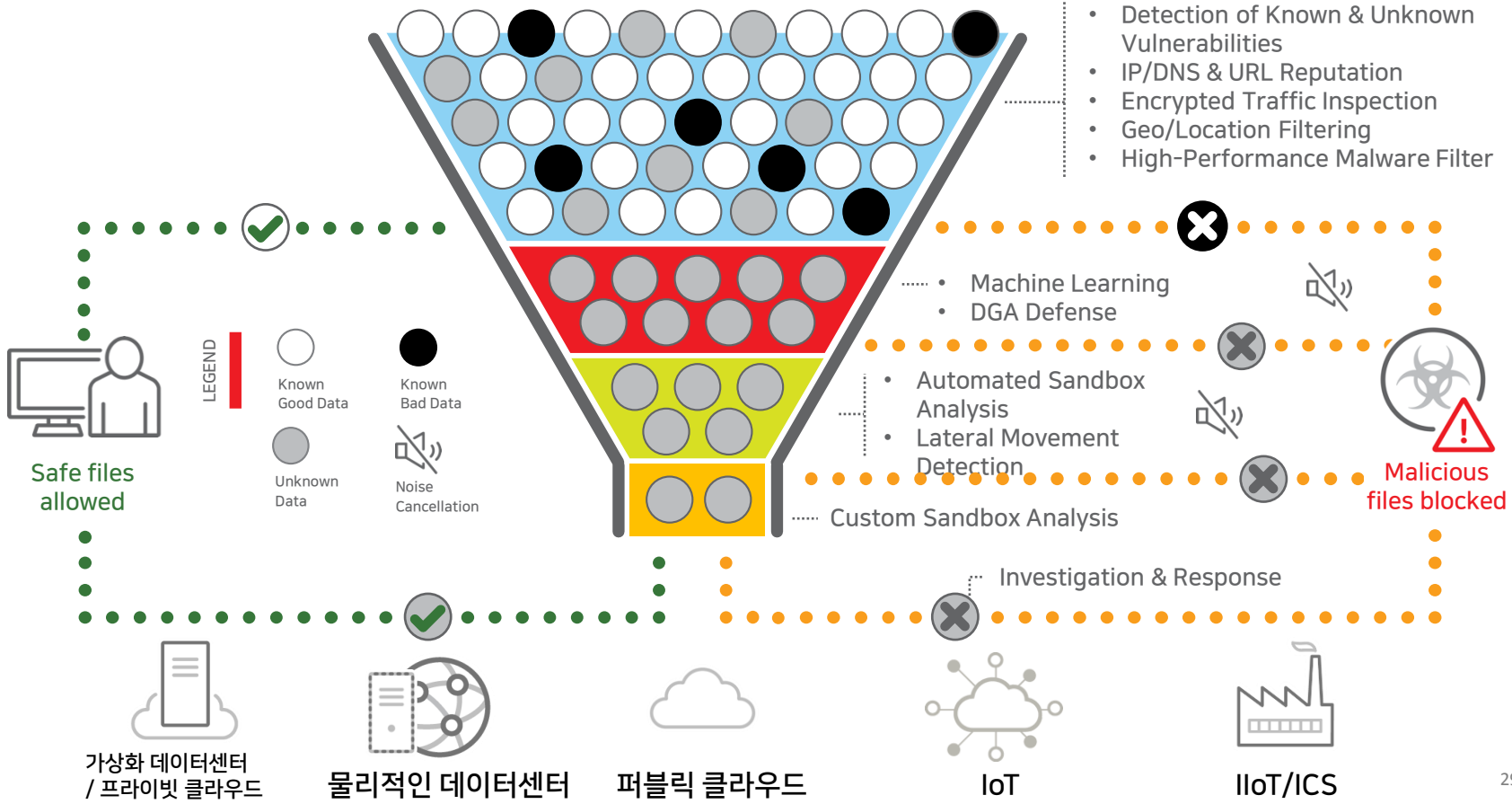



Server Workloads


Endpoints

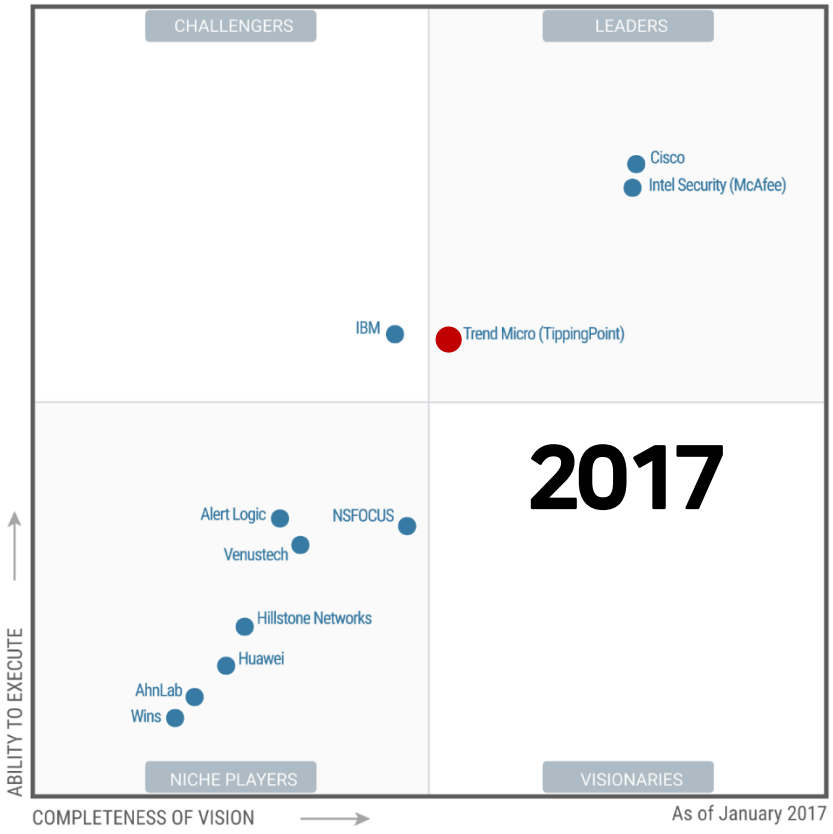
하이브리드 데이터센터 보호를 위한
TippingPoint XGen IDPS의 보안취약점 대응 전략

TREND MICRO | Security TRENDS 2018



2018 Gartner MQ for IDPS

* Source : 2017 & 2018 Gartner Magic Quadrant for Intrusion Detection and Prevention Systems




TippingPoint Returns.
Slimmer, Stronger
and Smarter

TREND MICRO

Security
TRENDS 2018

THANK YOU

한국트렌드마이크로
김정수 이사