글로벌 보안 위협 동향
2017년 4분기 분석 결과

배준호 이사 (이메일: jbae@fortinet.com)
시스템 엔지니어링팀 매니저, 포티넷 코리아

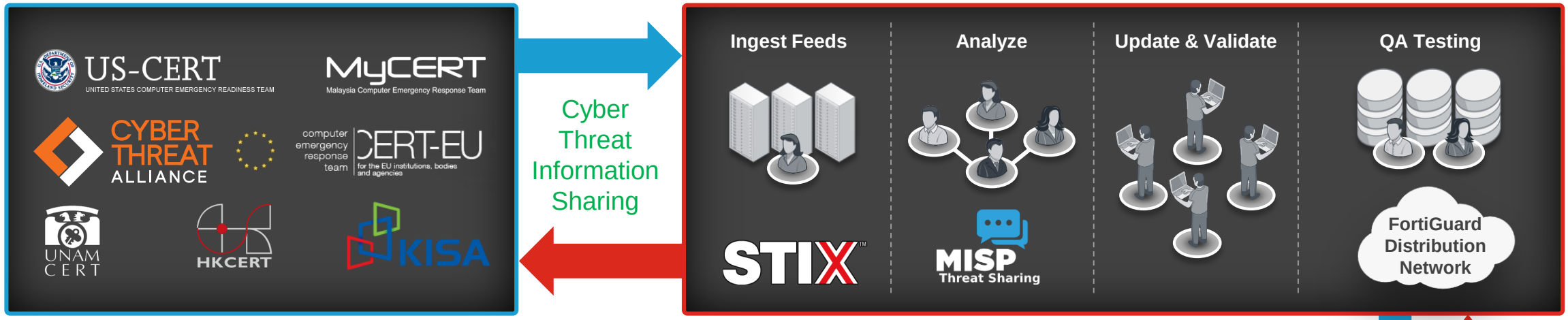
2018년 4월 11일


FORTINET
THREAT
동향 보고서
2016년 4분기
FORTINET
글로벌 보안 위협
동향 보고서
2017년 1분기
FORTINET
글로벌
보안 위협
동향 보고서
2017년 2분기
FORTINET
글로벌
보안 위협
동향 보고서
2017년 3분기
FORTINET
글로벌
보안 위협
동향 보고서
2017년 4분기

분석 보고서 발행 주체는 포티넷 위협 분석 대응 센터인 포티가드 AI (FortiGuard AI)

Industry Leading Patented Security Technology

사이버 위협 정보 공유와 머신 러닝 분석 기법을 적용한 포티가드 AI (FortiGuard AI)



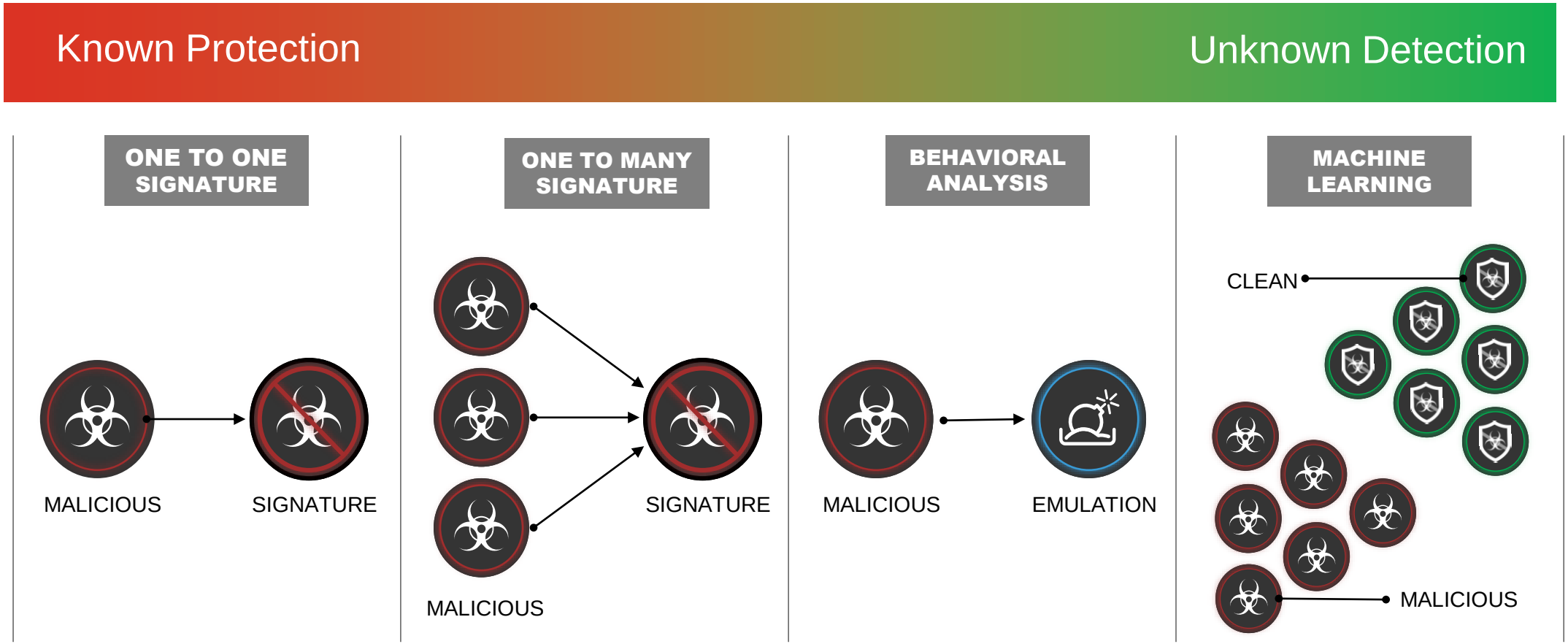
FortiGuard AI Labs

글로벌 보안 위협 정보 공유 시스템

국내 KISA와 협업

악성 코드 탐지 기술 진화

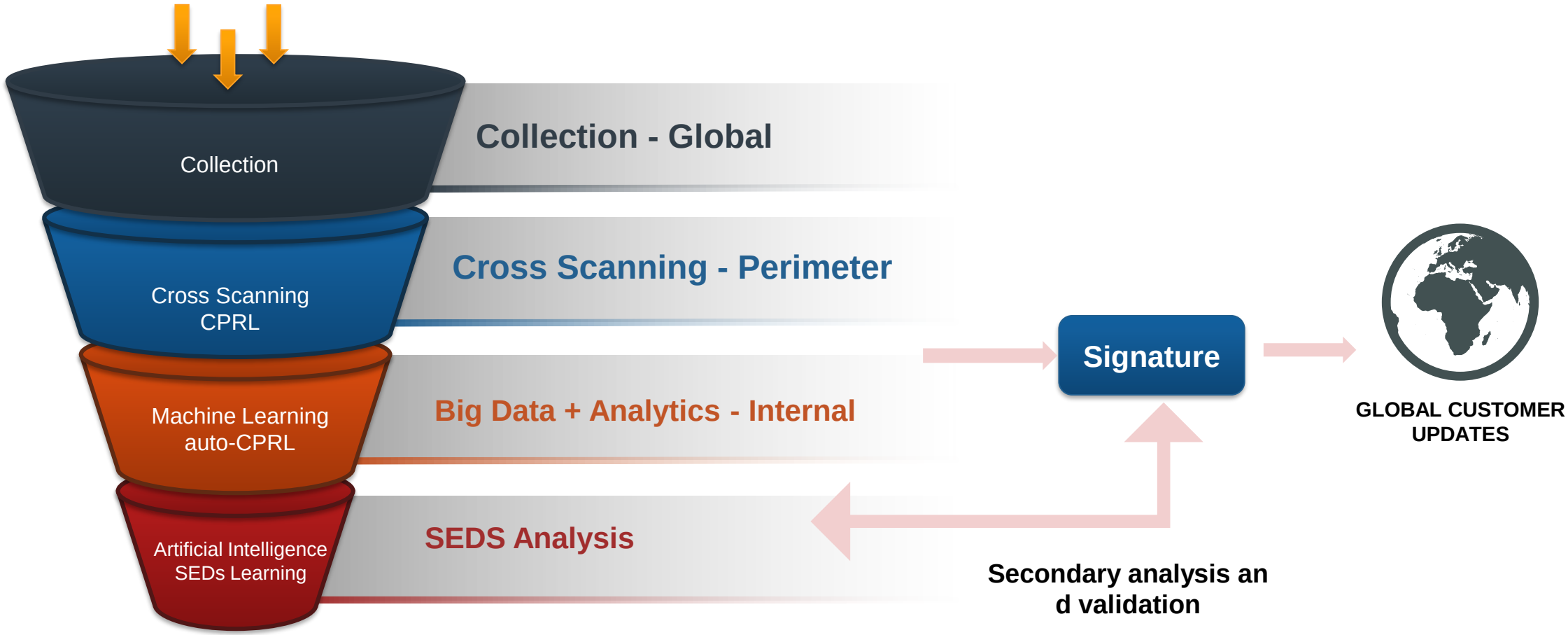
알려진 (Known) 공격 탐지부터 알려지지 않은 (Unknown) 공격 탐지까지



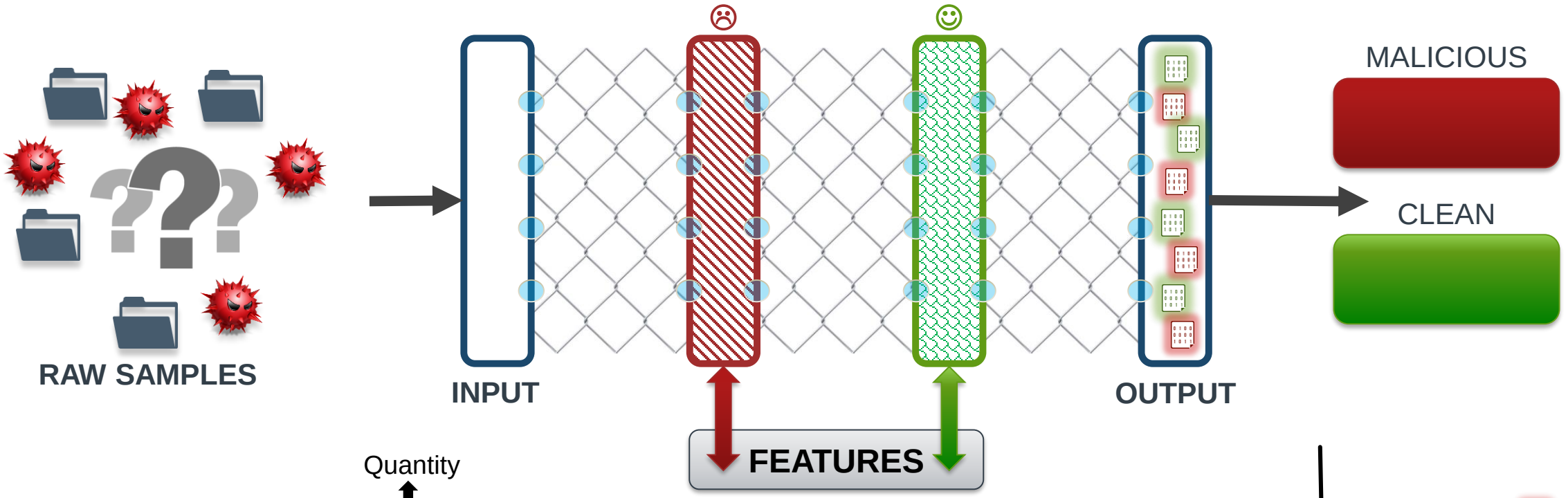
포티가드 AI 아키텍처

머신 러닝과 인공 지능 적용

- Augmenting pattern recognition and automatic signature creation technology
- Continued learning and feature improvement – higher accuracy of the system

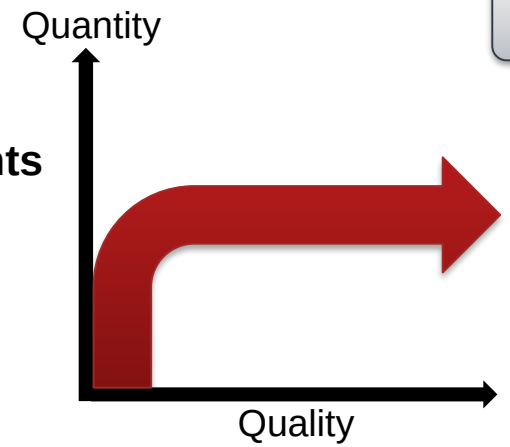


포티가드 AI 동작 구조와 결과

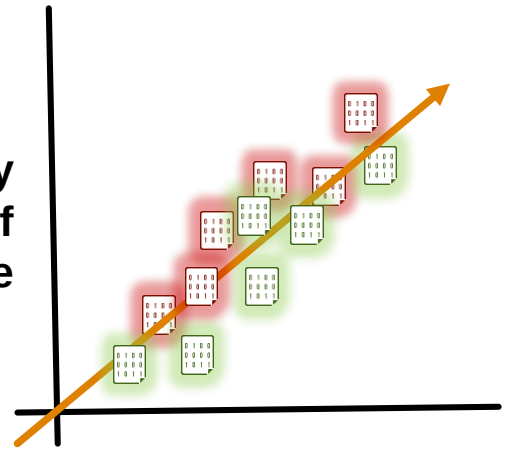


Feature Set Improvements

- Quality
- Stabilized Number
- Weighting Confidence

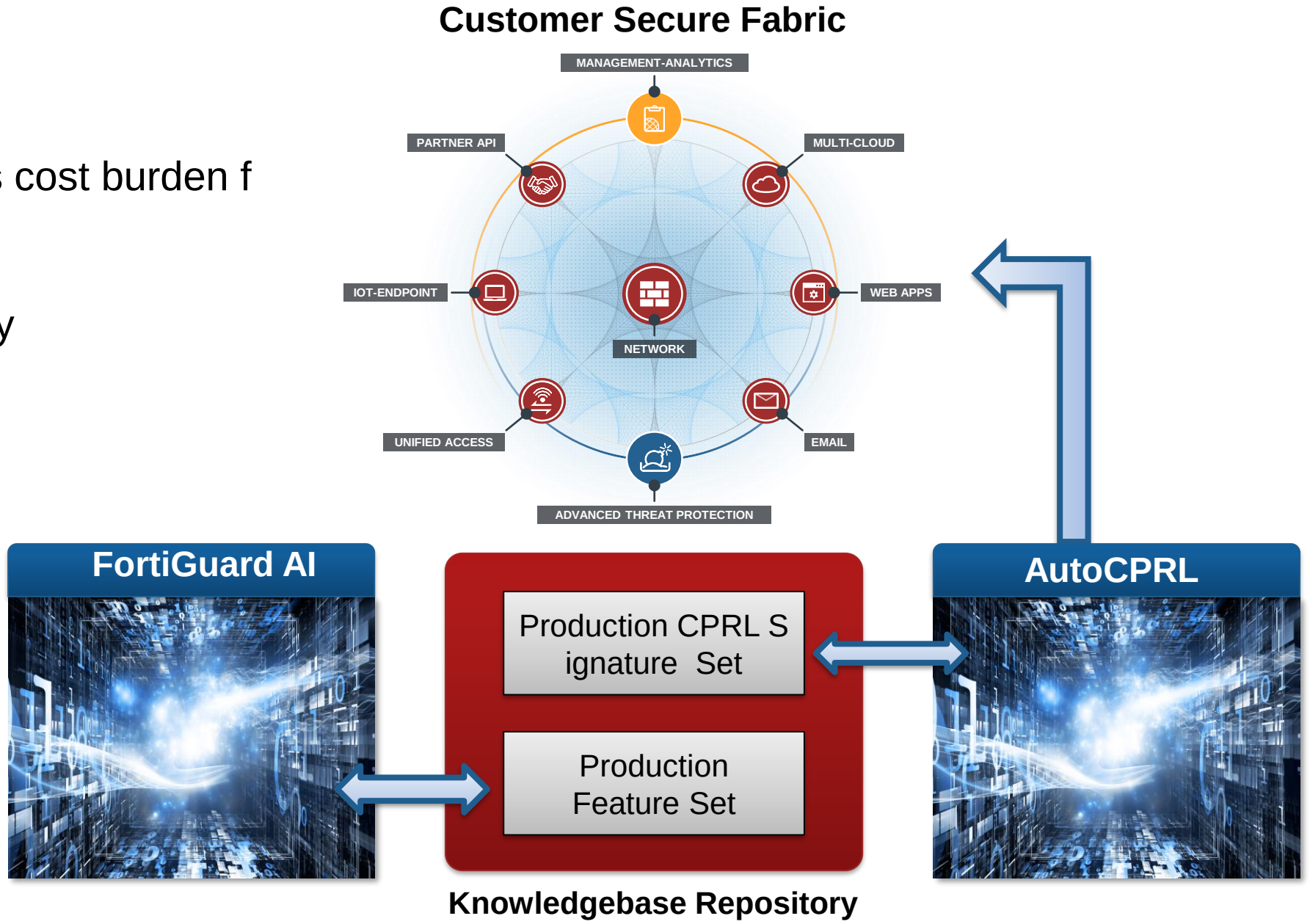


Continued Accuracy to a High Degree of Confidence



산출물

- Significantly increases cost burden f or cybercriminals
- Unsurpassed accuracy
- Proven and validated
- Extremely adaptive



출처 및 척도

이 보고서에서 밝히는 여러 가지 정보는 상용 서비스 시설에 포티넷이 구축한 방대한 네트워크 기기/센서 제품군에서 얻어서 포티가드 랩(FortiGuard Labs)에서 취합한 내용입니다. 여기에는 2017년 10월 1일부터 12월 31일까지 세계 각지에서 활발하게 움직이는 상용 서비스 시설에서 관찰된 수십억 개의 위협 이벤트와 사건 사고 등이 포함됩니다. 독립적 조사 결과에 따르면[1], 포티넷의 보안 장치 점유율이 가장 크기 때문에 업계에서 가장 대규모로 위협 데이터 샘플 추출이 가능합니다. 데이터는 모두 익명 처리하며 샘플에 표시된 단체에는 신원을 식별할 수 있는 정보를 전혀 포함하지 않습니다.

여러분도 쉽게 상상하실 수 있으시겠지만, 이러한 정보는 다양한 관점에서 사이버 위협 동향을 살펴볼 수 있는 훌륭한 시각을 제공합니다. 이 보고서에서는 그와 같은 동향의 중심에서 서로 보완적인 관계에 있는 주요 분야 세 가지, 즉 애플리케이션 익스플로잇, 악성 소프트웨어(멀웨어), 봇넷을 중점적으로 다루겠습니다.

익스플로잇
이 보고서에서 설명하는 애플리케이션 익스플로잇은 주로 네트워크 IPS를 통해 수집하였습니다. 이 데이터세트에서 취약한 시스템을 파악하기 위한 공격자 정찰(reconnaissance) 활동과 그러한 취약점을 악용하려는 시도를 살펴볼 수 있습니다.

멀웨어
이 보고서에서 설명하는 멀웨어 샘플은 경계 기기, 샌드박스 또는 엔드포인트 등에서 수집하였습니다. 이 데이터세트는 대체로 공격을 대상 시스템에 성공적으로 설치하는 단계가 아닌, 공격의 무기화나 전달 단계를 나타냅니다.

봇넷
이 보고서에서 설명한 봇넷 활동은 네트워크 기기를 통해 수집하였습니다. 이 데이터세트는 침입을 받은 내부 시스템과 악성 외부 호스트 사이를 오가는 C2(Command & Control, C&C) 트래픽을 의미합니다.

당사에서는 이와 같은 다양한 위협 동향의 측면 외에 데이터의 의미를 설명하고 해석하는 데 세 가지 척도를 사용합니다. 이 보고서에서 규모, 출현율 및 강도라는 용어를 자주 접하게 될 것입니다. 이러한 용어는 항상 본문에서 제시한 정의를 준수하여 사용합니다.

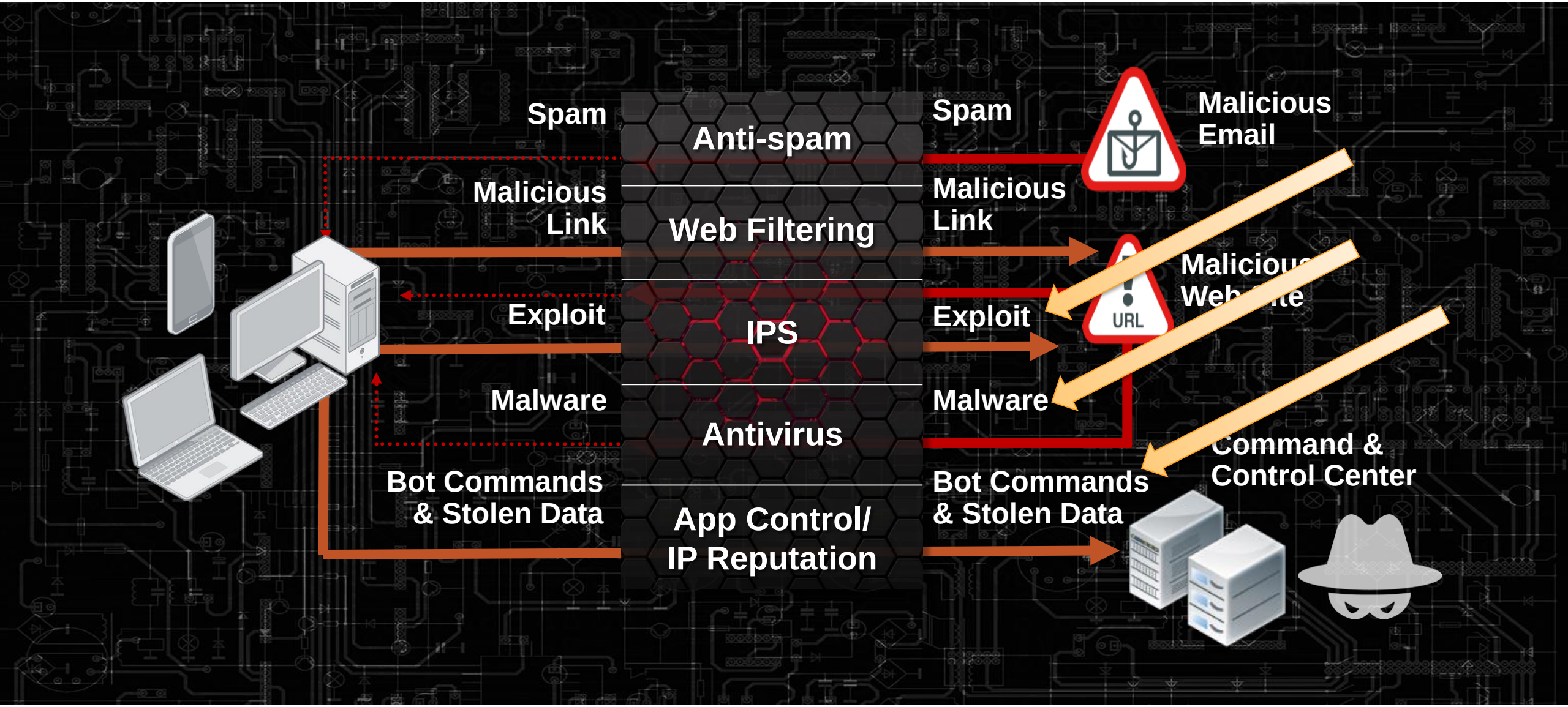
이 보고서에 포함된 수치에는 수많은 위협이 포함되어 있습니다. 몇 가지 위협에 대해서는 간략한 설명을 제공하지만, 분명 독자 여러분은 더 자세한 정보를 원할 것입니다. 이 보고서를 읽으면서 필요할 경우 포티가드 랩(FortiGuard Labs) 백과 사전을 참조하십시오.

규모	전반적인 빈도 또는 비율의 척도입니다. 위협 이벤트로 관찰된 총 횟수 또는 백분율을 나타냅니다.
출현율	여러 그룹에 걸친 분포도 또는 침투성입니다. 위협 이벤트를 적어도 한 번 이상 발견하여 신고한 조직의 백분율[2]을 나타냅니다.
강도	일간 규모 또는 빈도를 말합니다. 조직 한 곳에서 한 가지 위협 이벤트가 관찰되는 일일 평균 횟수를 말합니다.

[1] 출처: IDC 전 세계 보안 어플라이언스 추적기, 2017년 4월(연간 단위 출고량 기준)

[2] 당사는 위협 활동을 신고한 조직에서만 출현율을 측정할 수 있기 때문입니다. 어떤 봇넷의 출현율이 50%에 달하더라도 전 세계 기업 절반에 영향을 미친 것으로 해석할 수 없습니다. 봇넷 데이터 세트에 있는 기업 중 절반이 해당 봇넷을 목격했다는 의미합니다. 일반적으로 분모는 수만 개의 기업으로 구성됩니다.

익스플로잇, 멀웨어, 봇넷 동작 단계 이해



요약 1: 익스플로잇 동향 (Exploit Trends)

Unique Exploit Detections

5,988

Exploits Seen per Firm (avg)

274

Firms who saw Severe Exploits

72%

Recorded Exploits of WIFI Camera Devices

33%

익스플로잇 증가 의미 ?

- **알려진 취약점을 가진 시스템 탐지 활동의 증가**

요약 2: 멀웨어, 봇넷 동향

Malware

- 17,671 unique variants ↗
- 3,317 different families ↗
- 22% detected ransomware →
- 14% reported mobile malware ↘

Botnet

- 513 daily botnet communications per firm ↓
- 259 unique botnets detected ↗
- 1.9 active botnets per firm →
- 3.3% of firms saw >10 botnets ↗

요약 3: 제로 데이 리서치 (Zero Day Research)

12 zero days
ANNOUNCED
in 1Q 2018

185 zero days
DISCOVERED
2017

38 zero days
DISCOVERED
in 4Q 2017

527 zero days
DISCOVERED
since 2006

http://fortiguard.com/zeroday

* Fortinet follows responsible disclosure policies

4분기 동향 보고서 내용을 살펴 보겠습니다.

주요 토픽과 트렌드 하이라이트 & 권고 사항 1

Botnets

Firms typically have one or two different botnets active at any given time – some 10 or more!	Firms need to eradicate the underlying issues causing infections – find and fix root cause

Mobile Malware

Mobile is increasingly becoming a target – Q4 saw 14% firms reporting	Ensure mobile devices have appropriate security controls in place and are being monitored

IOT Exploits on the Rise

Exploit activity against IOT devices (like WiFi cameras) quadrupled in Q4	Identify ALL devices connected to your n/w. Segment IOT devices into secured n/w zones with customized policies

Ransomware

22% of firms detected some type of ransomware in Q4	Minimize impact by ensuring you have a good offline backup. Define pay or not-pay policies and process ahead of time

주요 토픽과 트렌드 하이라이트 & 권고 사항 2

Cryptojacking

Sharp increase in cryptomining malware – systems infected so they can be leveraged to mine cryptocurrencies

→ Regularly review system processes running on computers to find/kill culprits

Steganography

Top reported exploit in December used steganography to conceal hidden information with graphics file – distributes ransomware

→ Utilize a data sanitation service – like Content Disarm and Reconstruction that removes active content from files in real-time

P2P Proxy Target

Firms with high utilization of P2P and proxy apps have up to 9x higher rates of botnets and malware

→ Firms need to review policies, update software inventory, and scan for rogue applications

Vulnerability Swarm

37% of firms STILL seeing exploits targeting Apache Struts vulnerability – Attackers smell blood and swam.

→ Utilize a security audit service that can identify vulnerabilities and configuration weaknesses and help implement best practices


FORTINET