Qualys®

Enterprise TruRisk™ Platform

확장된 기업 네트워크 전반에서 비즈니스 리스크 줄이는 방법

De-risk your business across the extended enterprise

Qualys®

You can't **manage** what you can't **measure**.
You can't **measure** what you can't **see**.
You can't **secure** what you can't **manage**.

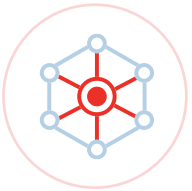
Qualys.

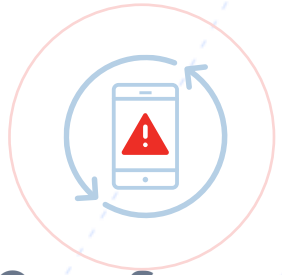
IT Assets

Digital Certificates

SaaS Apps

Servers



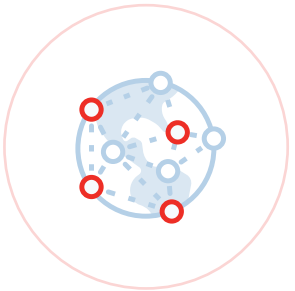


Open Source Software

Databases

공격 표면은 끊임없이 진화하고 있습니다

IP Cameras



Endpoints

Cloud Assets

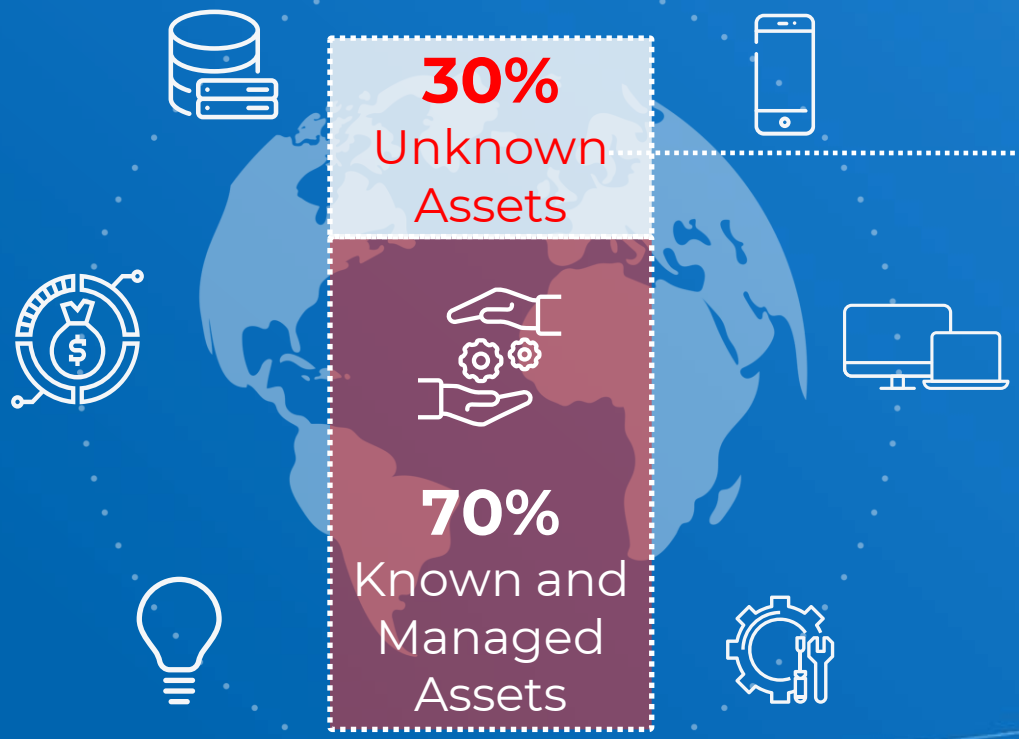
Cloud Apps

First-party Apps

Qualys.

관리되지 않는 자산의 영향

당신이 모르는 자산, 공격자는 알고 있습니다.



- **오직 9%** 의 회사만이 **공격표면의 100%를 적극적으로 모니터링 하고 있다고 믿고 있습니다.**
- **43%** 의 회사가 **자산 감지를 위해서 80시간 이상을 소비하고 있습니다.**
- **69%** 의 회사가 **"미관리 자산"을 목표로 하는 공격을 경험하고 있습니다.**

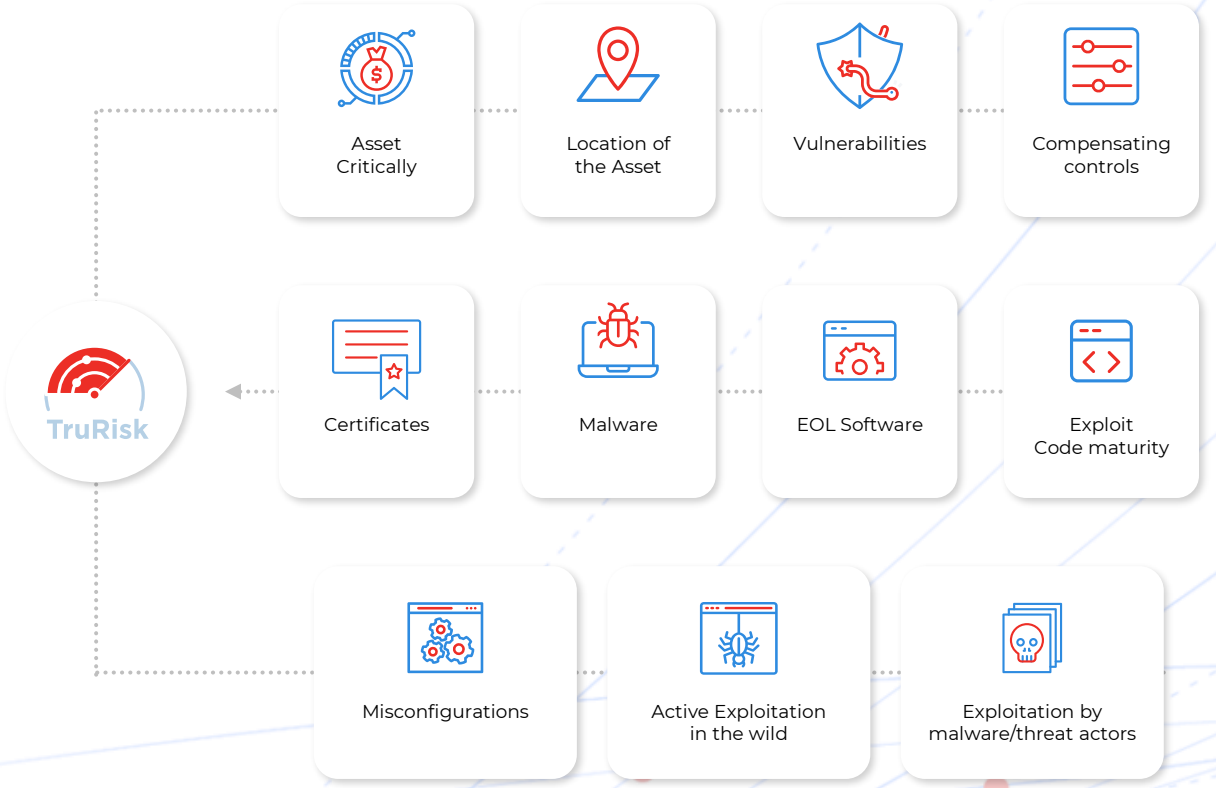
Qualys.

실질적일 리스크 관리

다양한 보안 위협 항목 기반 위협지표 구성

리스크 기반 우선관리 필요

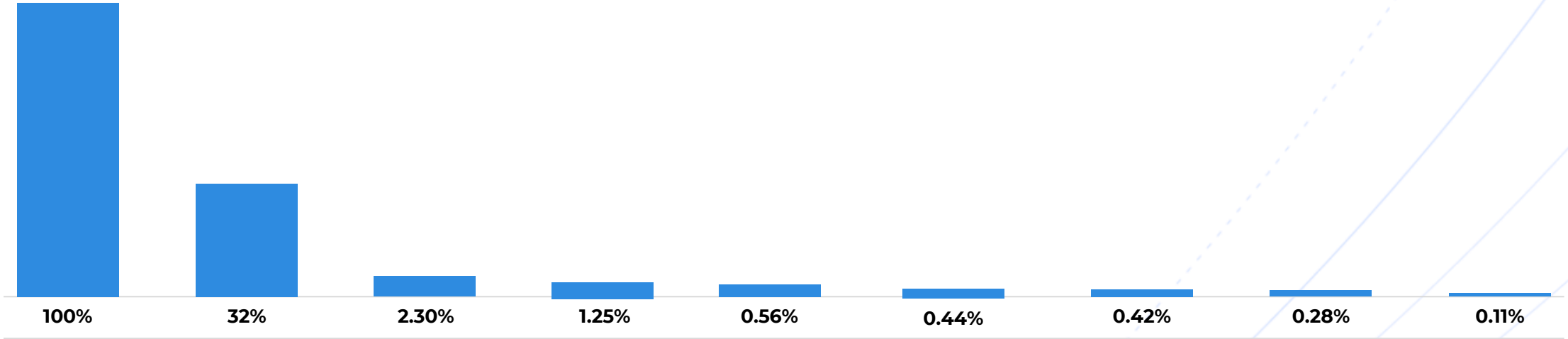
익스플로잇 위험, 가능성 또는 증거 및
비즈니스 영향을 기반으로 우선 순위 지정



Qualys.

리스크를 측정하는 여러 방법

리스크 를 어떻게 정확하게 측정 하시나요?



244,655	78,093	5,615	3,068	1,381	1,082	1017	697	270
Universe of All Known Vulnerabilities	Vulnerabilities with Exploit Available	Vulnerabilities with Weaponized Exploit Code	EPSS > 0.9	Exploited by Malware	CISA KEV	Exploited by Threat Actors	Named Vulnerabilities (Log4Shell, Heartbleed)	Exploited by Ransomware

Updated: Apr 9, 2024

Qualys.

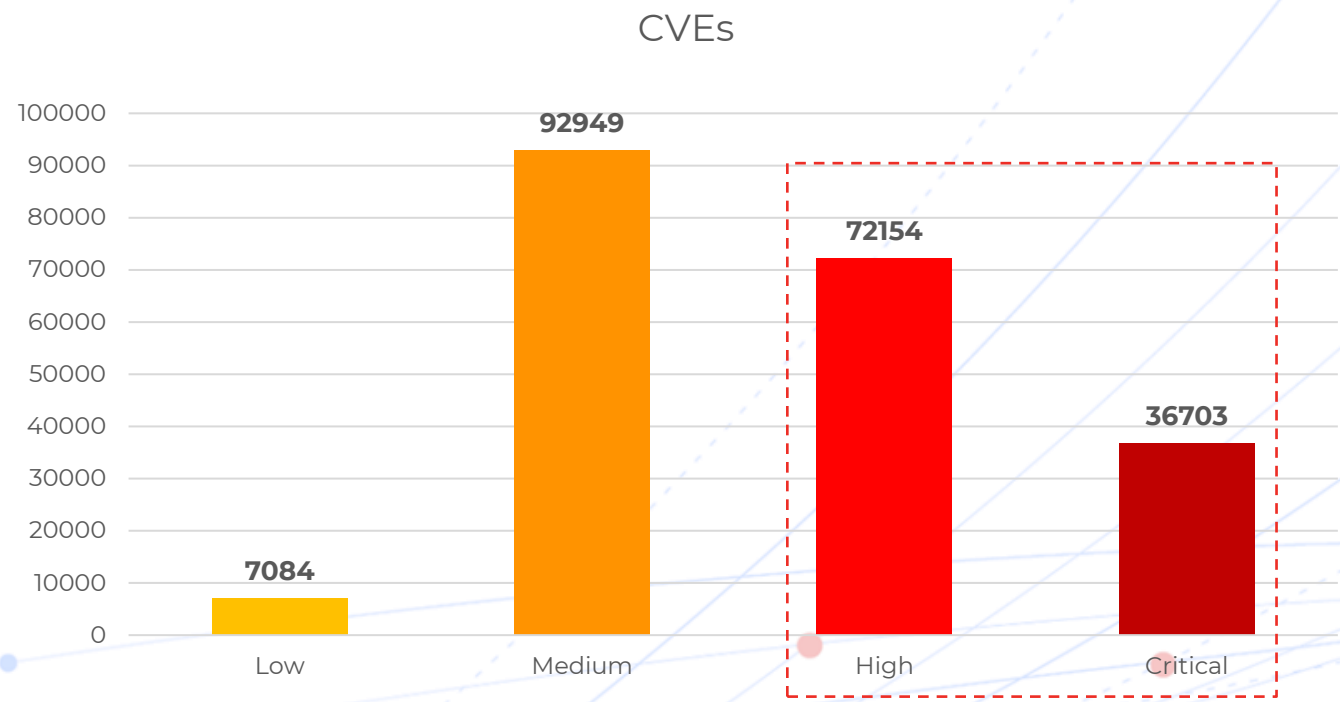
CVSS를 통한 리스크 측정

가장 중요한 것에 집중

52%

Too **many** vulnerabilities (105k+) **are rated high or critical by CVSS**

Common Vulnerability Scoring System (CVSS)



Qualys.

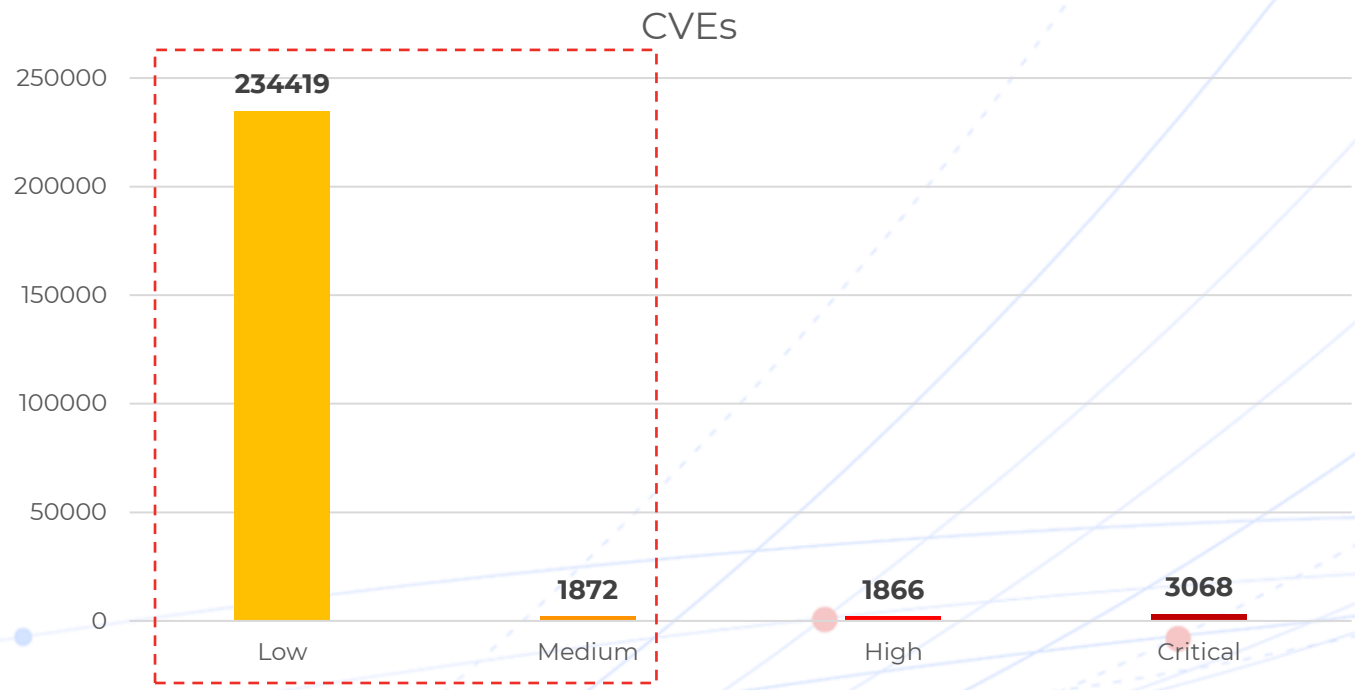
Measuring by EPSS

양이 아닌 리스크를 줄이는데 집중

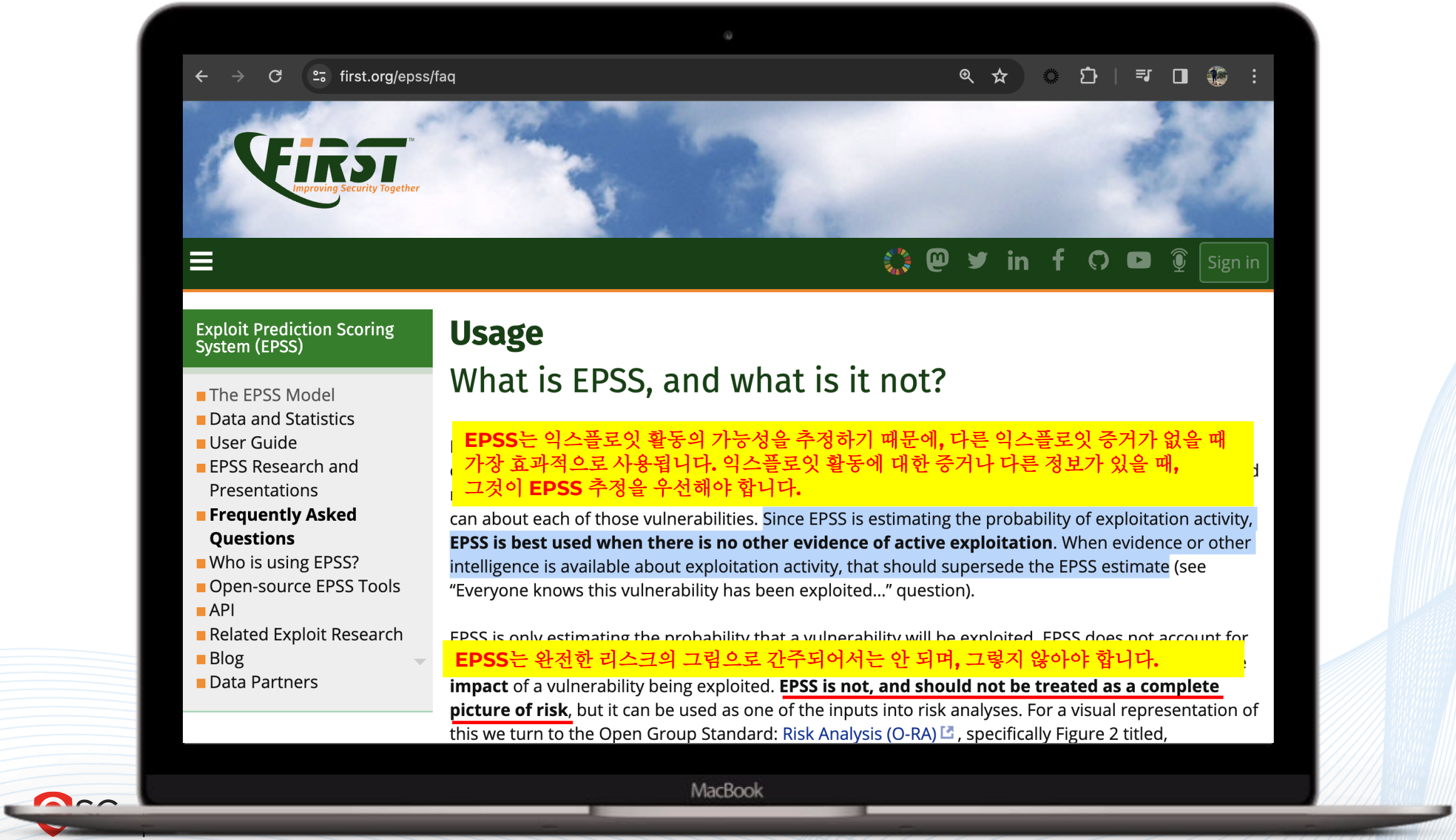
98%

Too **many** vulnerabilities (234K) **are rated low or medium by EPSS**

Exploit Prediction Scoring System (EPSS)



Qualys.


first.org/epss/faq
FIRST
Improving Security Together
Sign in
Exploit Prediction Scoring System (EPSS)
The EPSS Model
Data and Statistics
User Guide
EPSS Research and Presentations
Frequently Asked Questions
Who is using EPSS?
Open-source EPSS Tools
API
Related Exploit Research
Blog
Data Partners
Usage
What is EPSS, and what is it not?
EPSS는 익스플로잇 활동의 가능성을 추정하기 때문에, 다른 익스플로잇 증거가 없을 때 가장 효과적으로 사용됩니다. 익스플로잇 활동에 대한 증거나 다른 정보가 있을 때, 그것이 EPSS 추정을 우선해야 합니다.
can about each of those vulnerabilities. Since EPSS is estimating the probability of exploitation activity, EPSS is best used when there is no other evidence of active exploitation. When evidence or other intelligence is available about exploitation activity, that should supersede the EPSS estimate (see "Everyone knows this vulnerability has been exploited..." question).
EPSS is only estimating the probability that a vulnerability will be exploited. EPSS does not account for
EPSS는 완전한 리스크의 그림으로 간주되어서는 안 되며, 그렇지 않아야 합니다.
impact of a vulnerability being exploited. EPSS is not, and should not be treated as a complete picture of risk, but it can be used as one of the inputs into risk analyses. For a visual representation of this we turn to the Open Group Standard: Risk Analysis (O-RA), specifically Figure 2 titled,
MacBook

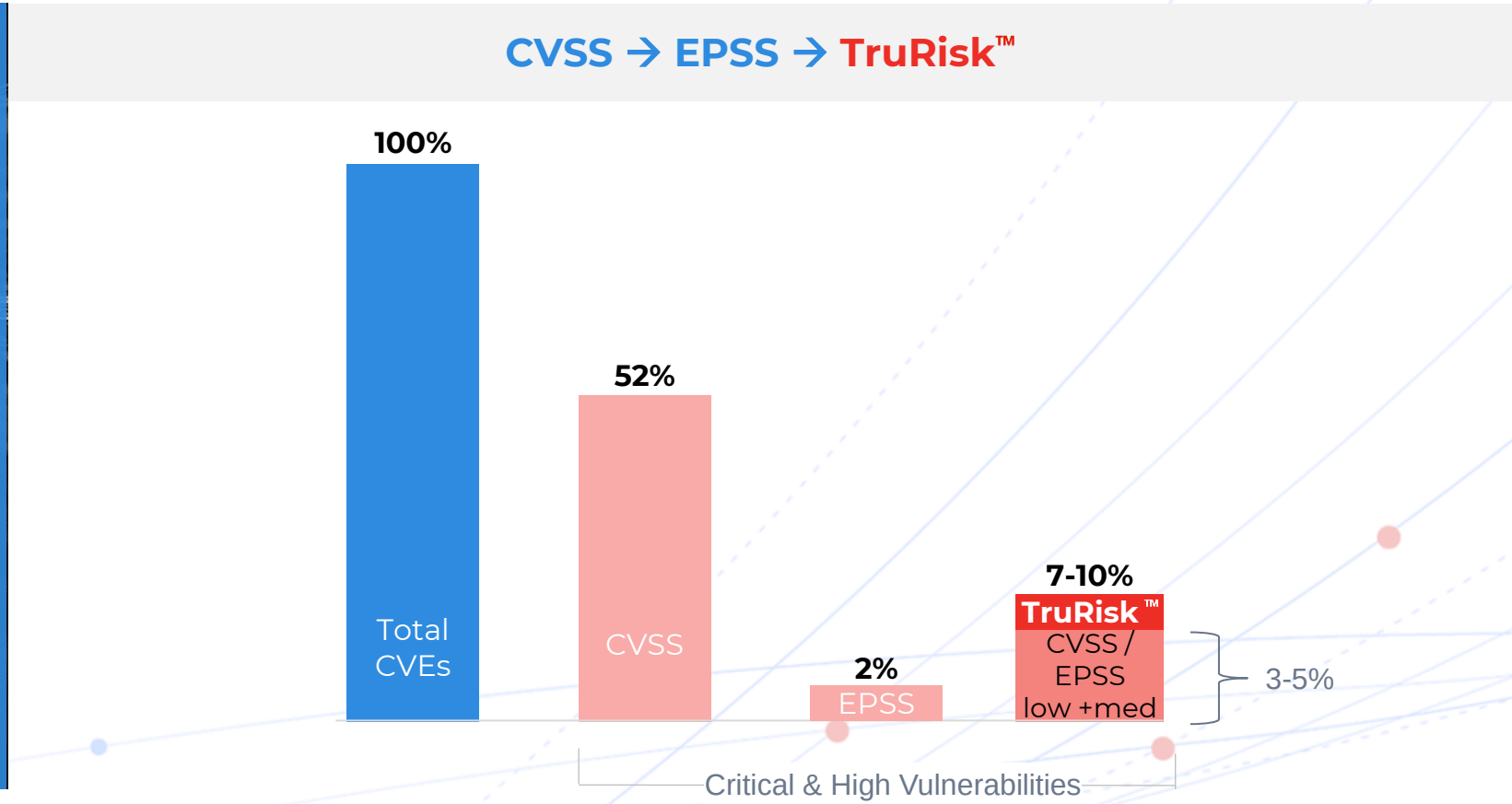
실질적인 위협 우선관리 TruRisk™

Cut 52% to **<10% with TruRisk™**

CVSS
Too Many

EPSS
Too Few

TruRisk™
Just Right!



Qualys.

중간 점수 CVSS, 심각한 점수 EPSS, 낮은 점수 TruRisk™

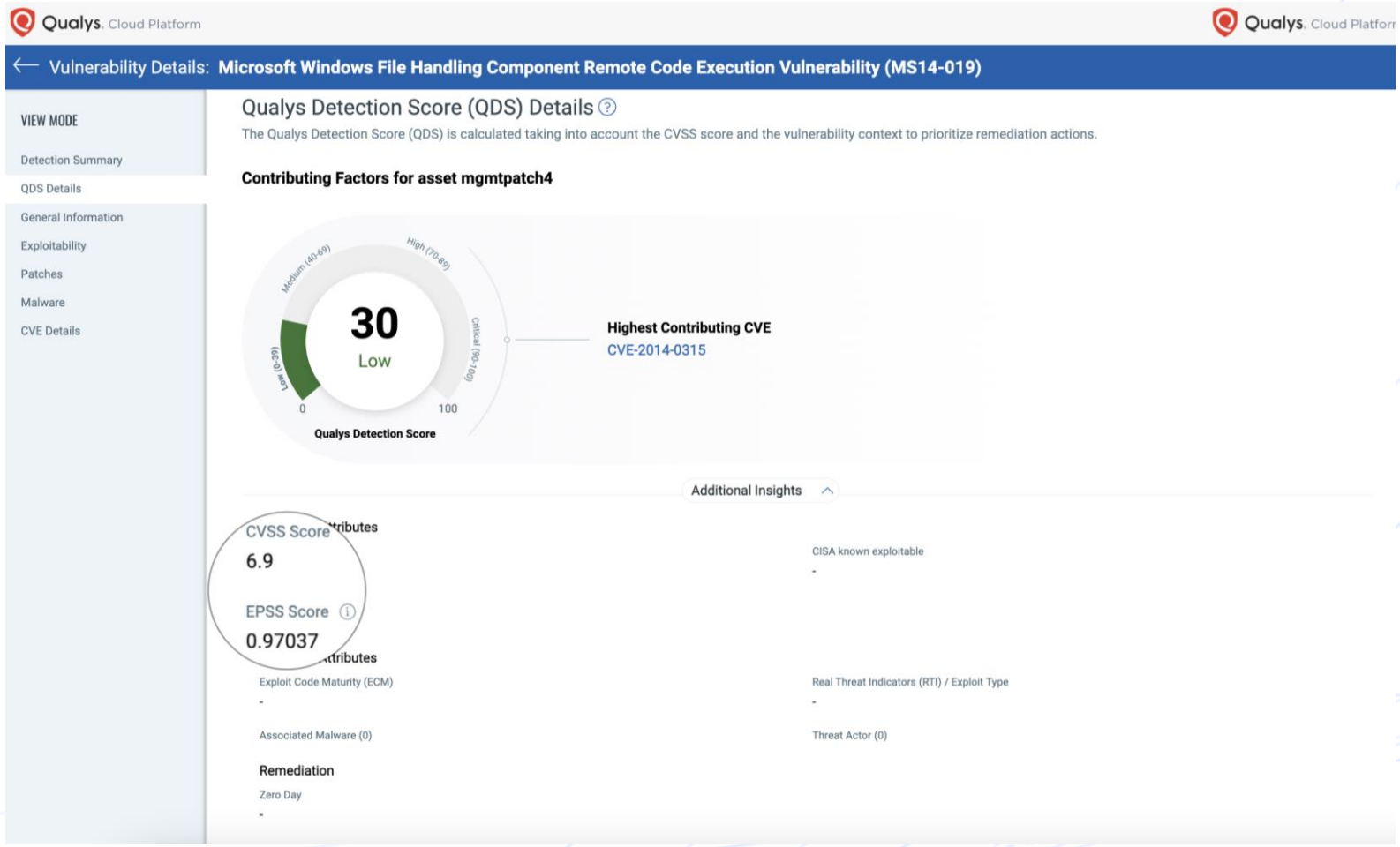
Microsoft Windows File Handling Component RCE (MS14-019)

CVSS 6.9

EPSS 0.97037

No Evidence of Exploitation

No Exploits available



692M Vulnerabilities incorrectly prioritized by CVSS & EPSS

Source: Qualys Cloud Platform

낮은 점수 CVSS, 낮은 점수 EPSS, 심각한 점수 TruRisk™

VMware Tools Authentication Bypass Vulnerability (VMSA-2023-0013)

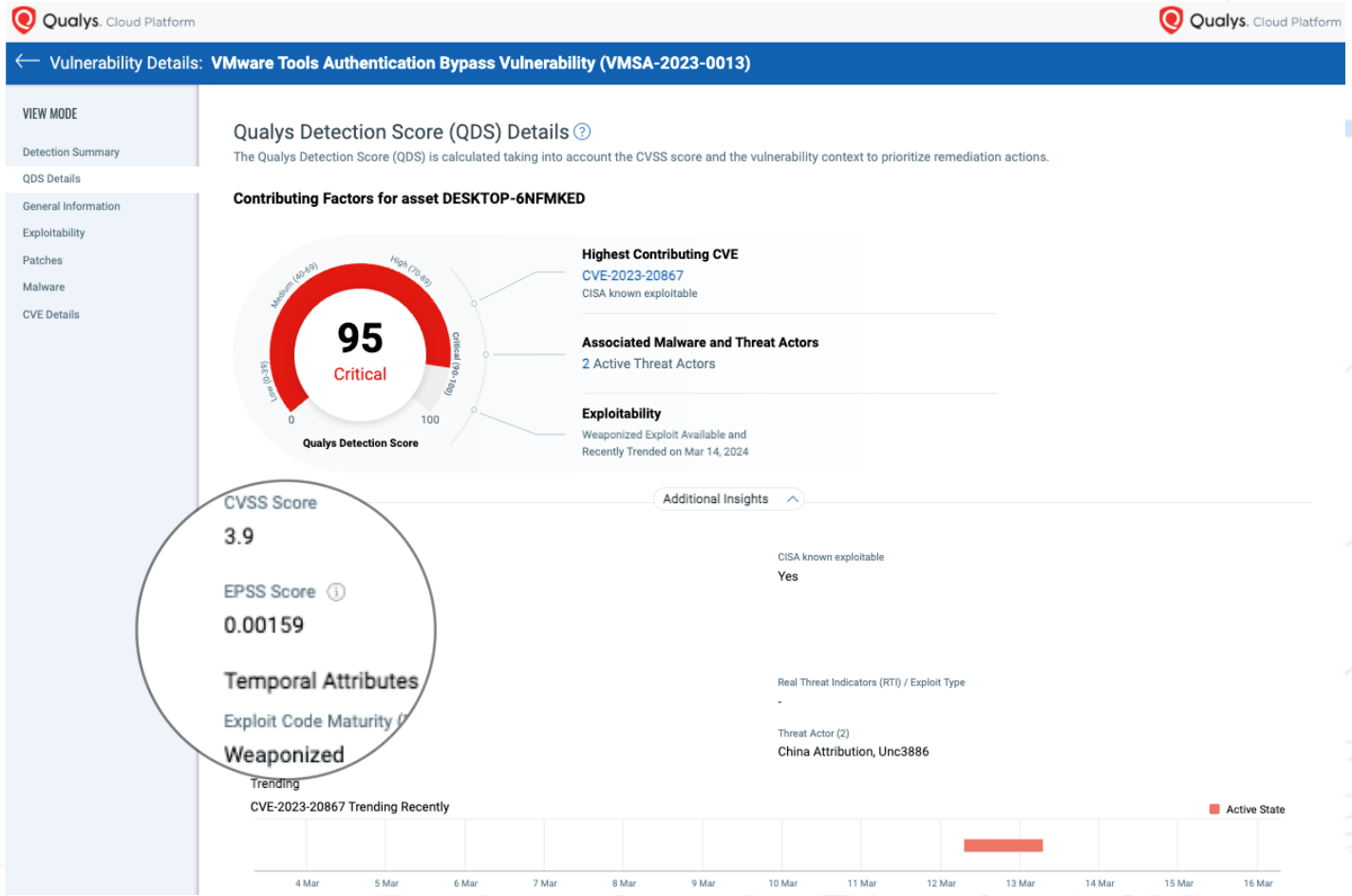
CVSS 3.9

EPSS 0.00159

CISA KEV

Weaponized PoC

Exploited by 2 Threat Actors & Trending

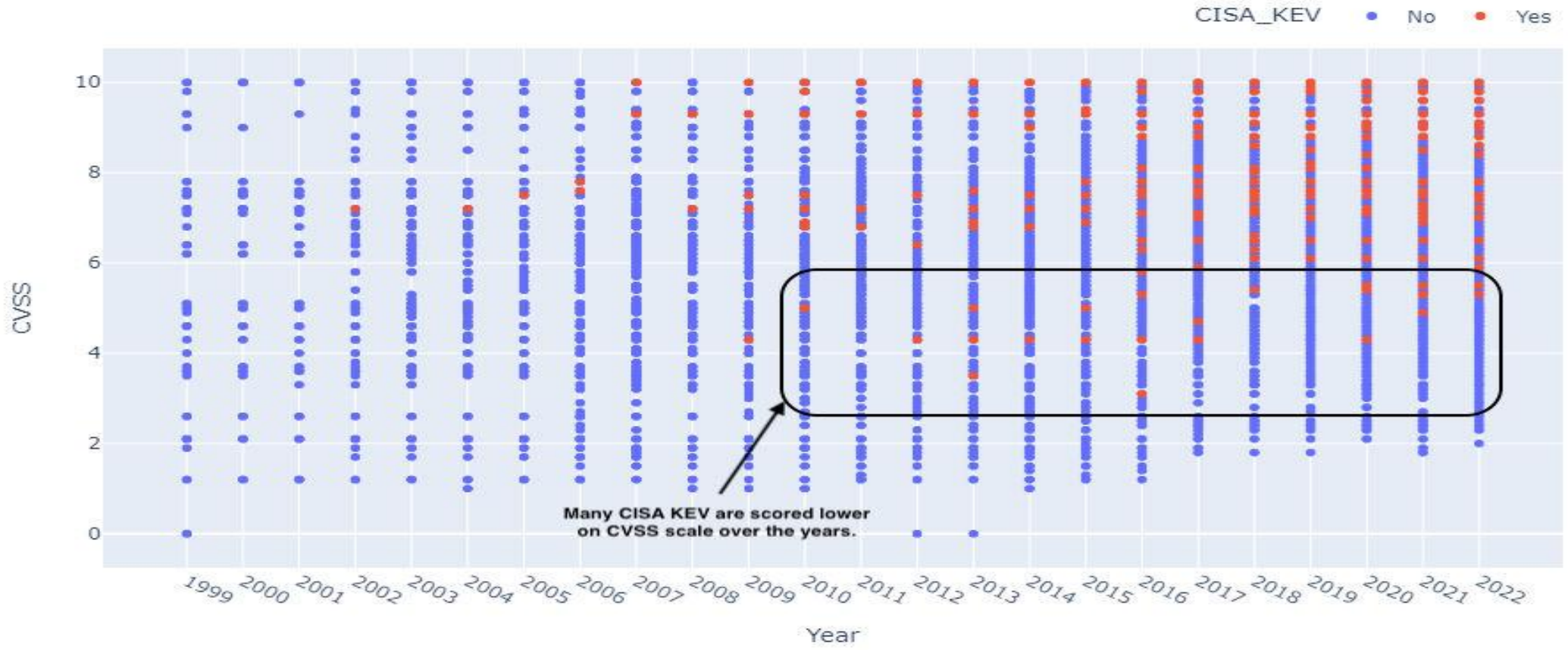


87M Vulnerabilities not prioritized by CVSS & EPSS

Source: Qualys Cloud Platform

CVSS vs CISA KEV

1999년부터 공개된 **CVE** 취약점 중**, CVSS Score 4**점 미만에서도 실제 침해사고 발생**. 2002**년 등 과거에 공개된 취약점 사용

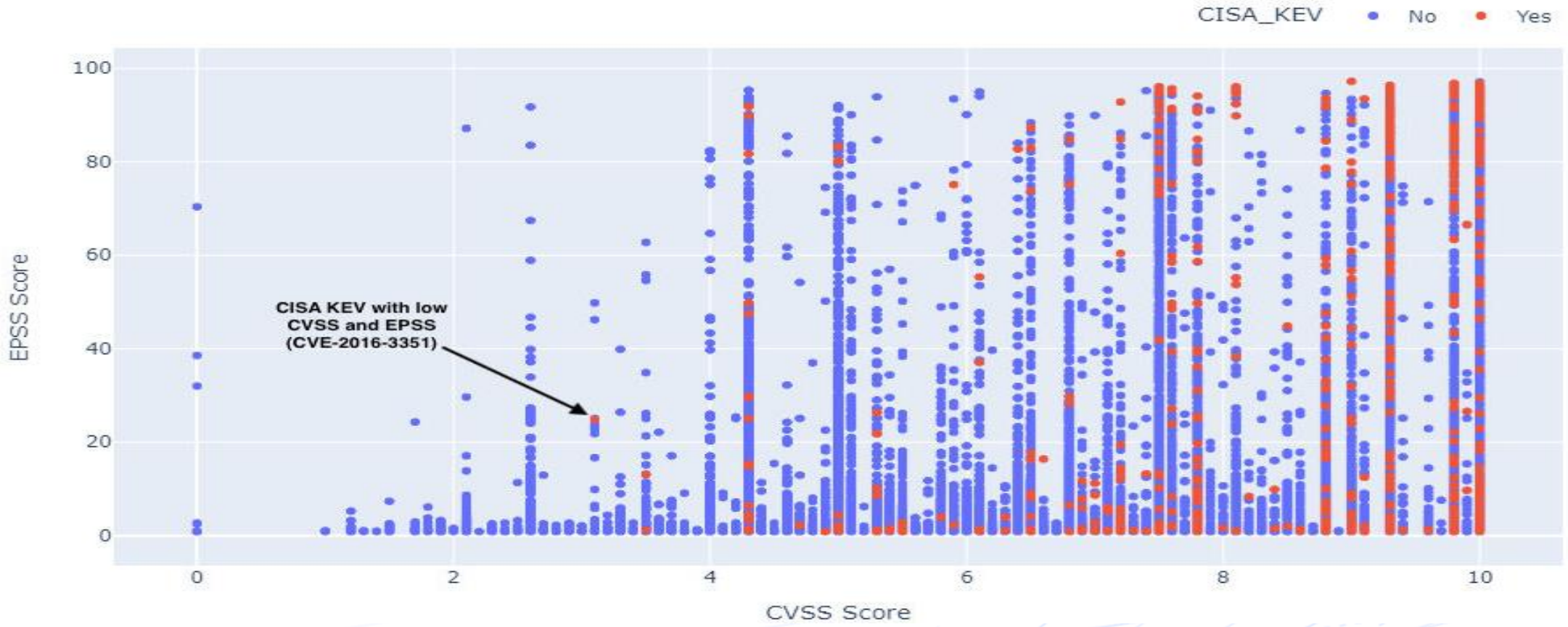


Qualys.

출처: Qualys

CVSS vs EPSS vs CISA KEV

EPSS Score 또한, **1 ~ 100%** 사이의 다양한 구간에서 침해사고 발생

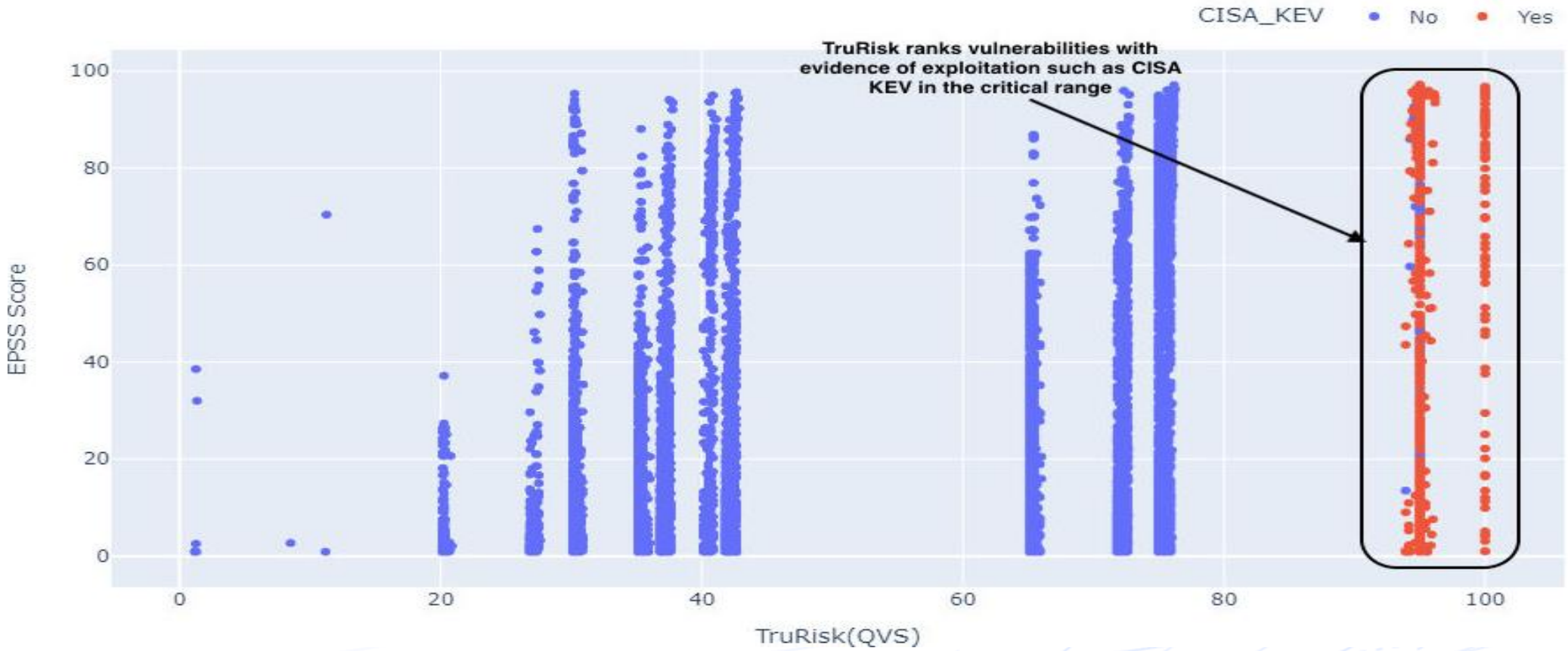


Qualys.

출처: Qualys

EPSS vs CISA KEV vs QDS

Qualys QDS Score의 경우, **90**점 이상에서 **CISA_KEV** 및 **EPSS Score** 전반에 걸쳐 침해사고 발생된 **CVE**취약점 제공



Qualys.

출처: Qualys

TruRisk™ 기반 리스크 측정

사이버 리스크 측정

Qualys TruRisk를 통해 취약점, 자산 및 자산 그룹 전반에 걸쳐 위험을 정량화하여 조직이 위험 노출을 능동적으로 줄이고 시간에 따라 위험 감소를 추적할 수 있도록 도와줍니다.

실질적인 리스크 기반 우선관리

Prioritize based on context from the **4-E**s:

1. **Exposure (노출)**
2. **Exploitation (악용)**
3. **Evidence (근거)**
4. **Enterprise Context (비지니스 영향)**

최고수준의 위협 인텔리전스 포함

25개 이상의 위협 출처에서 수집한 20만 개 이상의 취약점에 대한 통찰력을 활용하여 **Qualys Cloud Threat DB**로 **최고 수준의 위협 인텔리전스**를 얻으세요.

Qualys.

MITRE ATT&CK 매트릭 기반 우선관리

공격자 중심 관리

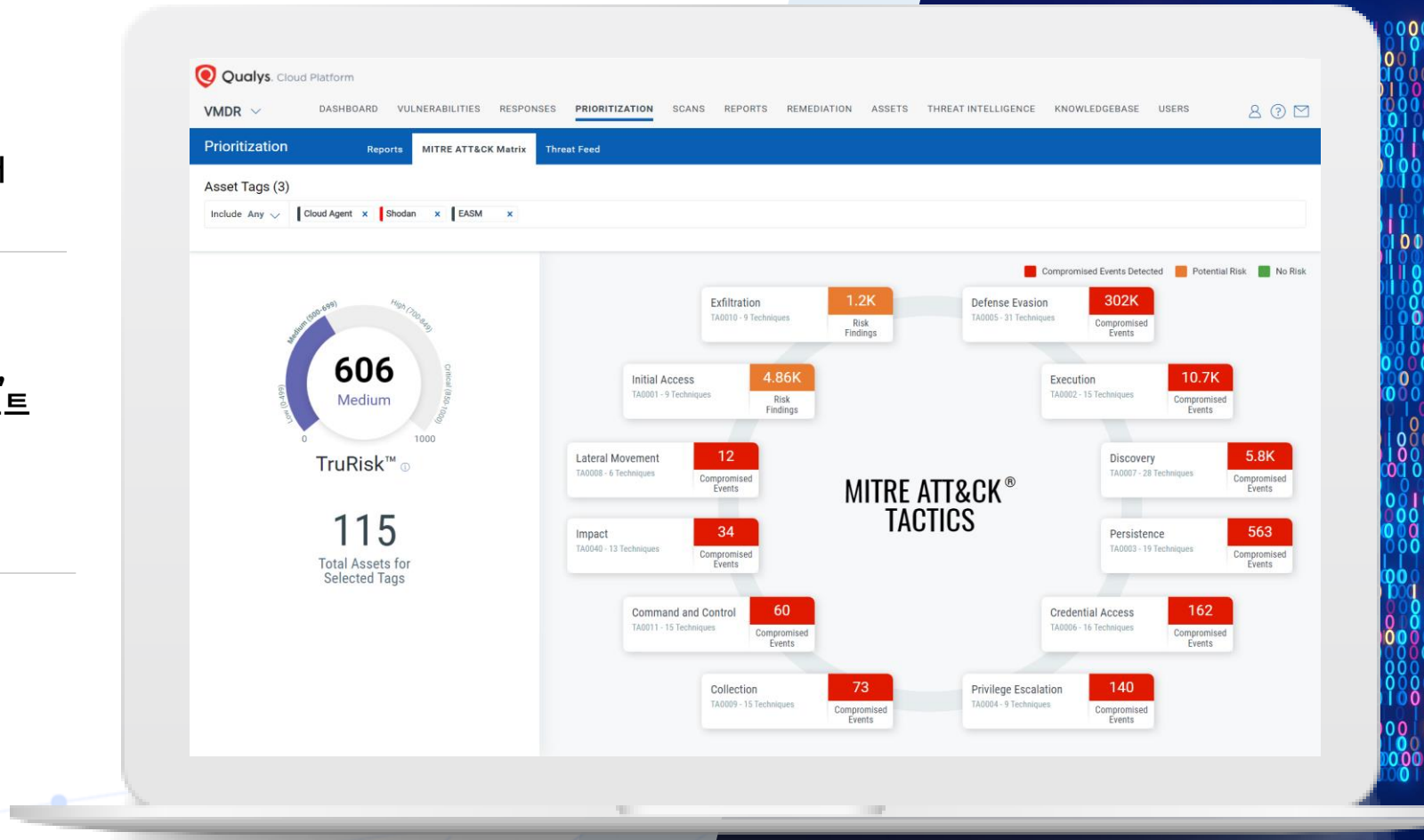
공격자의 관점에서 상위 ATT&CK 전술과 기법을 살펴보고, 위험을 줄이기 위해 위협 정보 기반 방어 관리

전반적인 ATT&CK 관리

CVE 취약점, CCE 잘못된 구성, EDR의 악성 행위, 자산 세부정보(예: 외부 노출 자산 식별 및 RDP 포트 세부정보)에 대한 통합 ATT&CK 관리

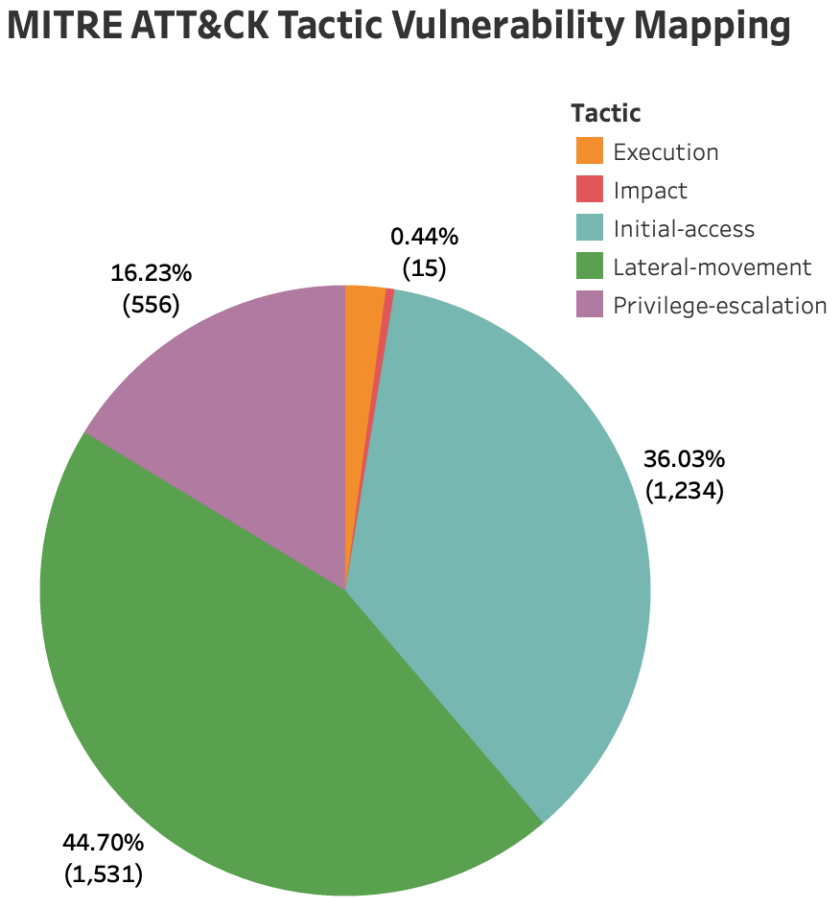
공격 경로 제거

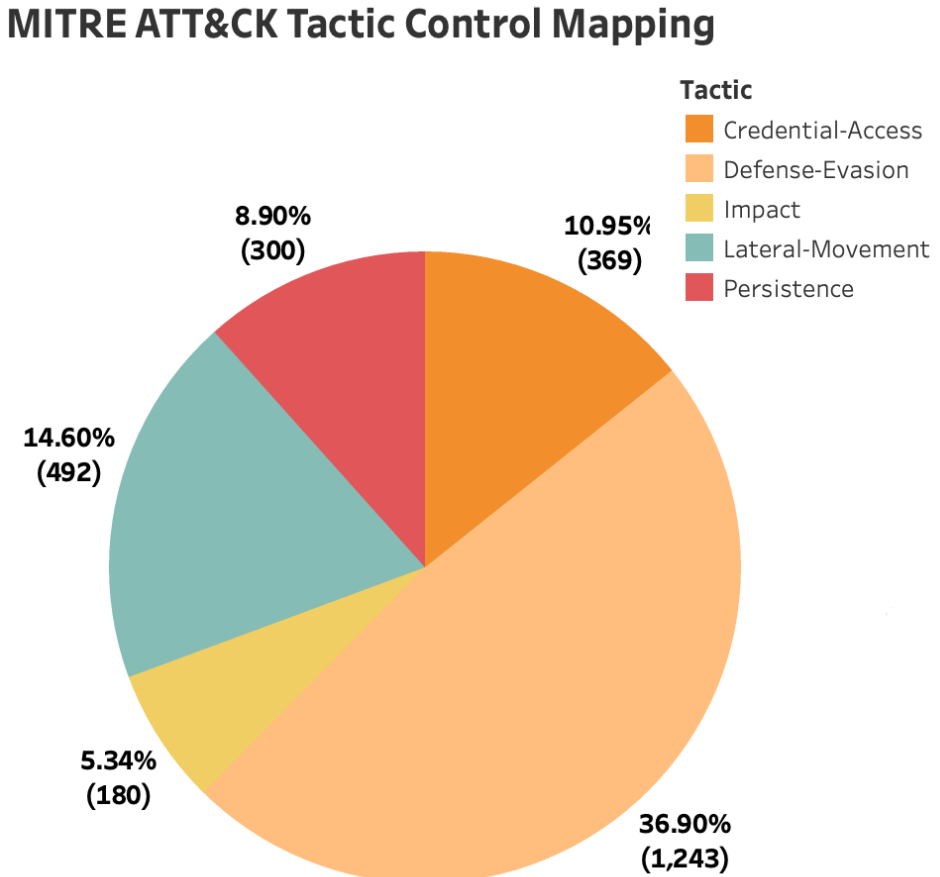
MITRE ATT&CK 통찰력을 활용하여 공격 경로를 식별, 우선 순위 지정, 제거하고 통합 패치 관리를 통해 능동적으로 킬 체인을 관리



Qualys.

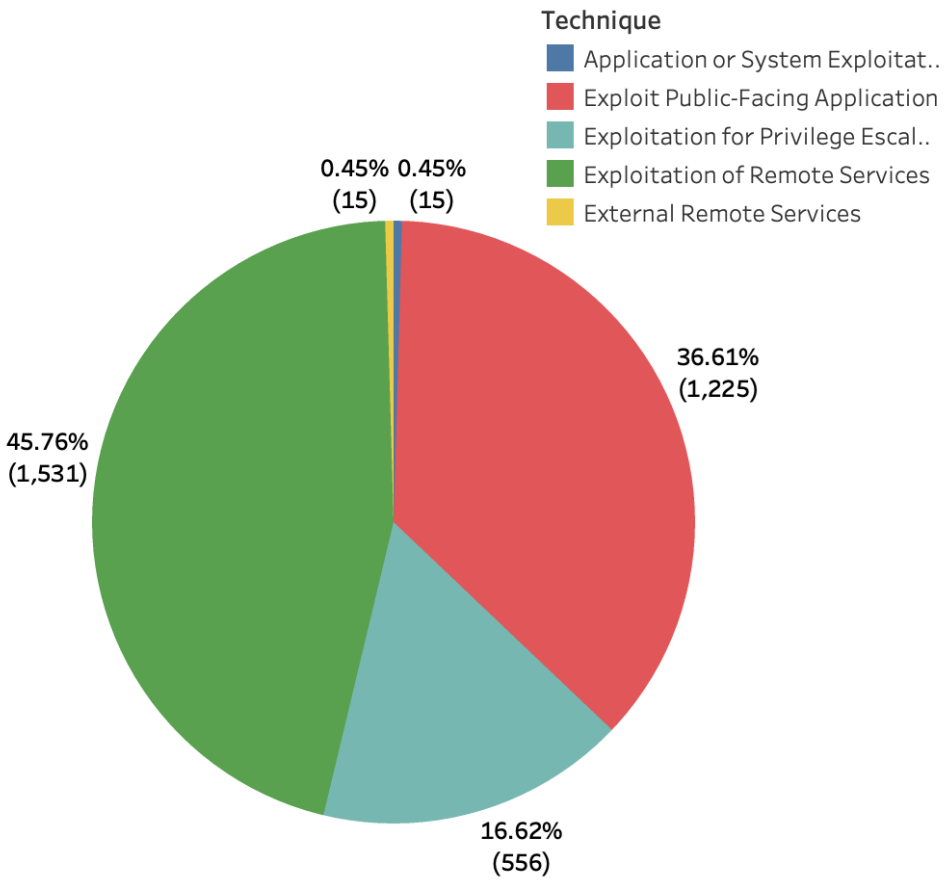
Top ATT&CK Tactics



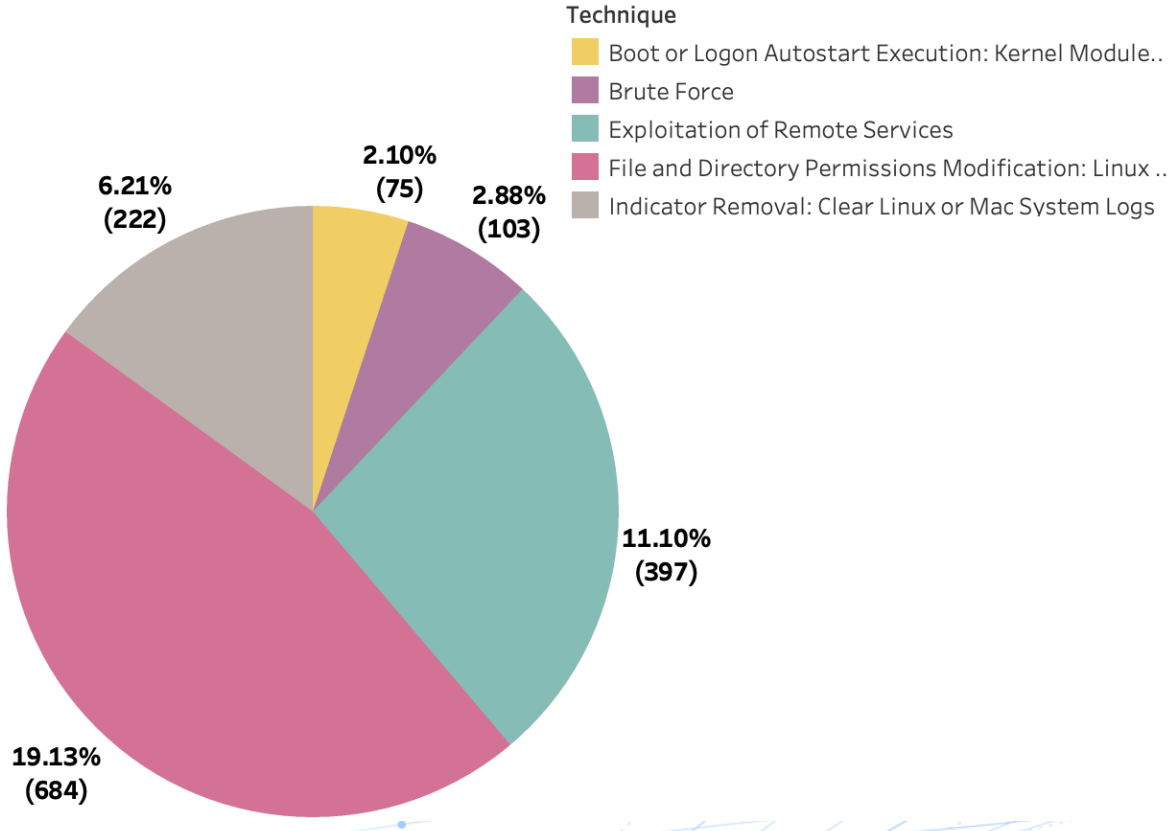


Top ATT&CK Techniques

MITRE ATT&CK Technique Vulnerability Mapping



MITRE ATT&CK Technique Control Mapping



비지니스 리스크 줄이기

내부 / 외부 비인가 및 미관리 자산에 대한 가시성 확보

OS 및 소프트웨어의 EoL/EoS 가시성 확보

실제 위협기반 취약점 우선 관리

취약점과 연계된 신속한 패치 및 조치 수행 관리


Qualys®