# A Risk-Based Defense of the Threat Landscape With Qualys VMDR

**Mehul Revankar**
VP, VMDR
Qualys

**Raphael Silva**
Cyber Risks Leader
Banco Pan

Qualys®

# Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

## De-risk your business.

# Organizations Lack Visibility

How Can You **Measure** the Unknown?

## Attack Surface is Expanding and Unknown

Attack Surface also encompasses first & third-party software, EoL/EoS software, open-source vulnerabilities. The list keeps growing.

IT/WORKSTATIONS/SERVERS | IOT | EXTERNAL DEVICES

**37%** Unknown external assets

**69%** Orgs experienced attack from unknown assets

**56** No. of vulnerable open-source packages per asset

**41%** **OSS Vulnerabilities exploitable with Exploit available on each asset**

Qualys.

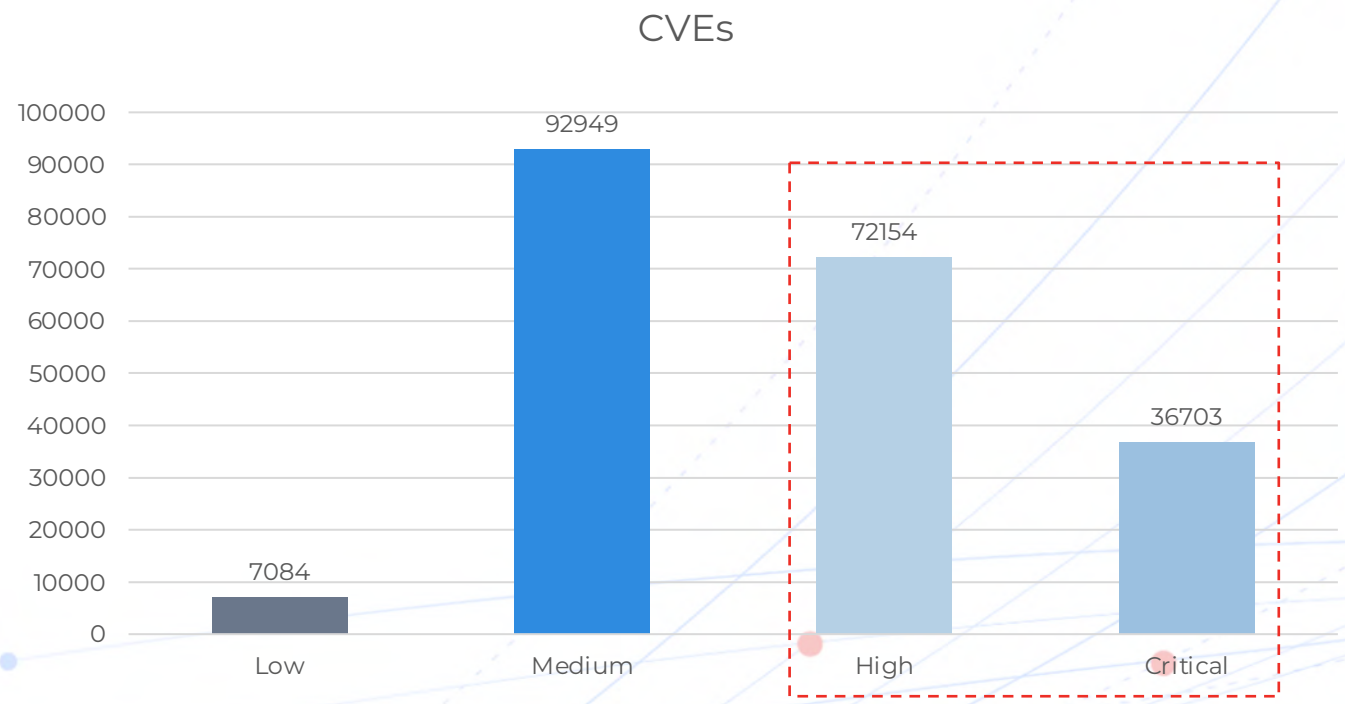
# Too Many Critical' Vulns

How Do You **Communicate** What Is High Risk?

**52%**

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

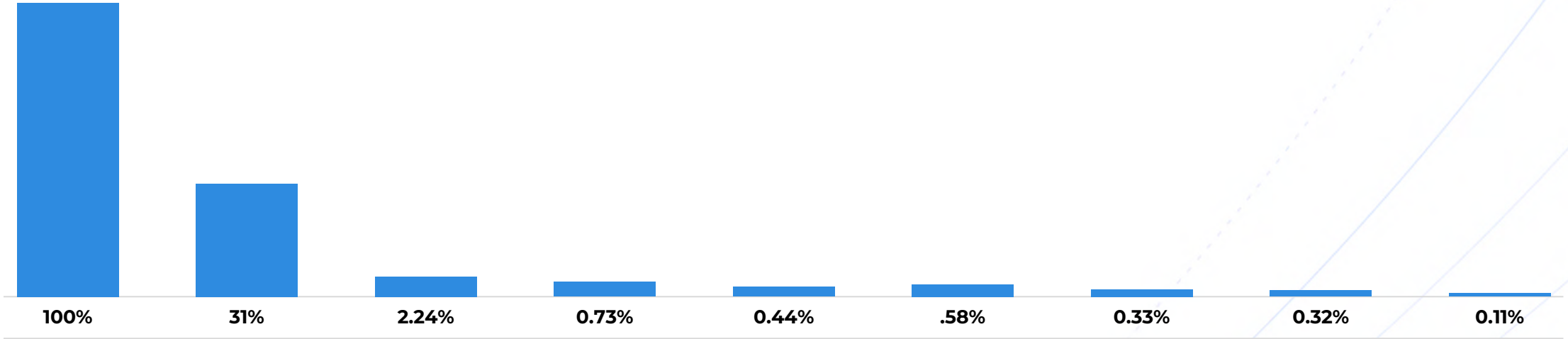
**Common Vulnerability Scoring System (CVSS)**




Qualys.

# So Many Vulnerabilities to Choose From

## Which Risks Should You **Eliminate**?




| 228,562 | 71,647 | 5,136 | 1,667 | 1,012 | 1,345 | 758 | 747 | 270 |
|---|---|---|---|---|---|---|---|---|
| Universe of All Known Vulnerabilities | Vulnerabilities with Exploit Available | Vulnerabilities with Weaponized Exploit Code | EPSS > 0.9 | CISA KEV | Exploited by Malware | Named Vulnerabilities (Log4Shell, Heartbleed) | Exploited by Threat Actors | Exploited by Ransomware |

Updated: 10/03/2023

Qualys.

# Fast Weaponization

Risk eliminated slower than weaponization?

## Attackers have a 11-day advantage

On average, weaponized vulnerabilities are patched within 30.6 days yet **only patched an average of 57.7% of the time**. These same vulnerabilities are weaponized by attackers in 19.5 days on average.

**19.5 Days**
Time to Weaponize

11.1 Days
Exploitation Opportunities

**30.6 Days**
Mean Time to Remediate

57.7% Remediated Vulnerabilities

Qualys.

# The Result?

Qualys.

# Undesired Outcomes

## Endless Cycle of Failed Results

Organizations **don't have accurate inventory, stale CMDB**, leading to a breach

Security Teams **focus on remediating inconsequential vulnerabilities**, which **don't reduce risk**

**IT Teams miss SLA's** for high-risk vulnerabilities

Security & IT Teams **waste countless hours communicating risk through spreadsheets, reports & manual processes**

Failures expose organization to unnecessary risk

Qualys.

# The Solution

Qualys.

# Manage & Reduce Risk Effectively

## Continuously Measure Cyber Risk

**01**

### Measure Known & Unknown Risks

Get complete visibility across your organization and know the unknown

**02**

### Communicate Cyber Risk

Prioritize based on risk of exploitation, and communicate risk across vulnerabilities, assets and groups of assets

**03**

### Eliminate Risk

Patch any device anywhere, leverage multiple avenues from remediation to mitigation and block attack paths to eliminate risk

Qualys.

# Measure Unknown Risk with CSAM/EASM

## Know the Unknown

### Discover All Assets

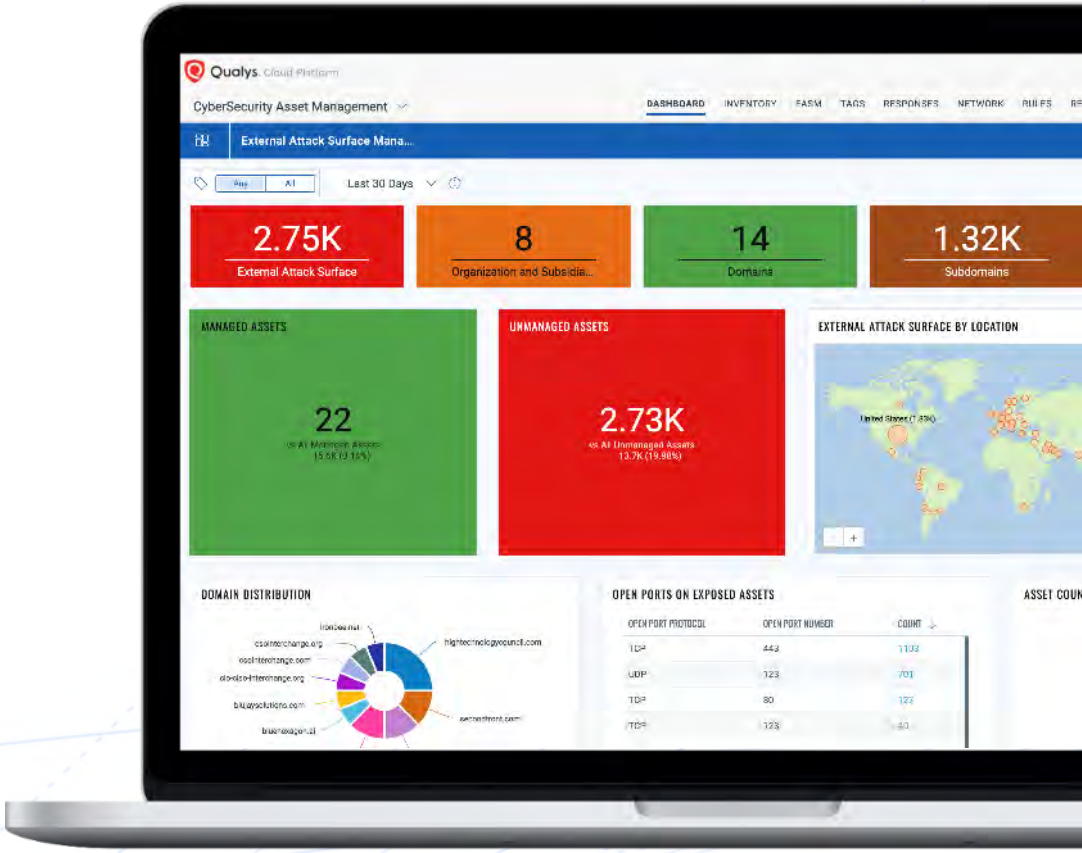
Get **inside-out and outside-in** visibility of all assets and get an attackers view of the network

### Get Complete Asset Context & Visibility

Add business context, Tags, **Identify crown Jewels**, enhance visibility by seamlessly integrating with CMDB's, Third Party & ITSM solutions

### Identify Security Gaps

Detect EOL/EOS Software, Unauthorized software, missing business critical software (EDR), inventory **open-source software, packages & libraries**




Qualys.

# Measure Risk with VMDR & TruRisk

## Measure CyberRisk

**Quantify risk across vulnerabilities, assets, and groups of assets** helping organizations proactively reduce risk exposure and track risk reduction over time with Qualys TruRisk

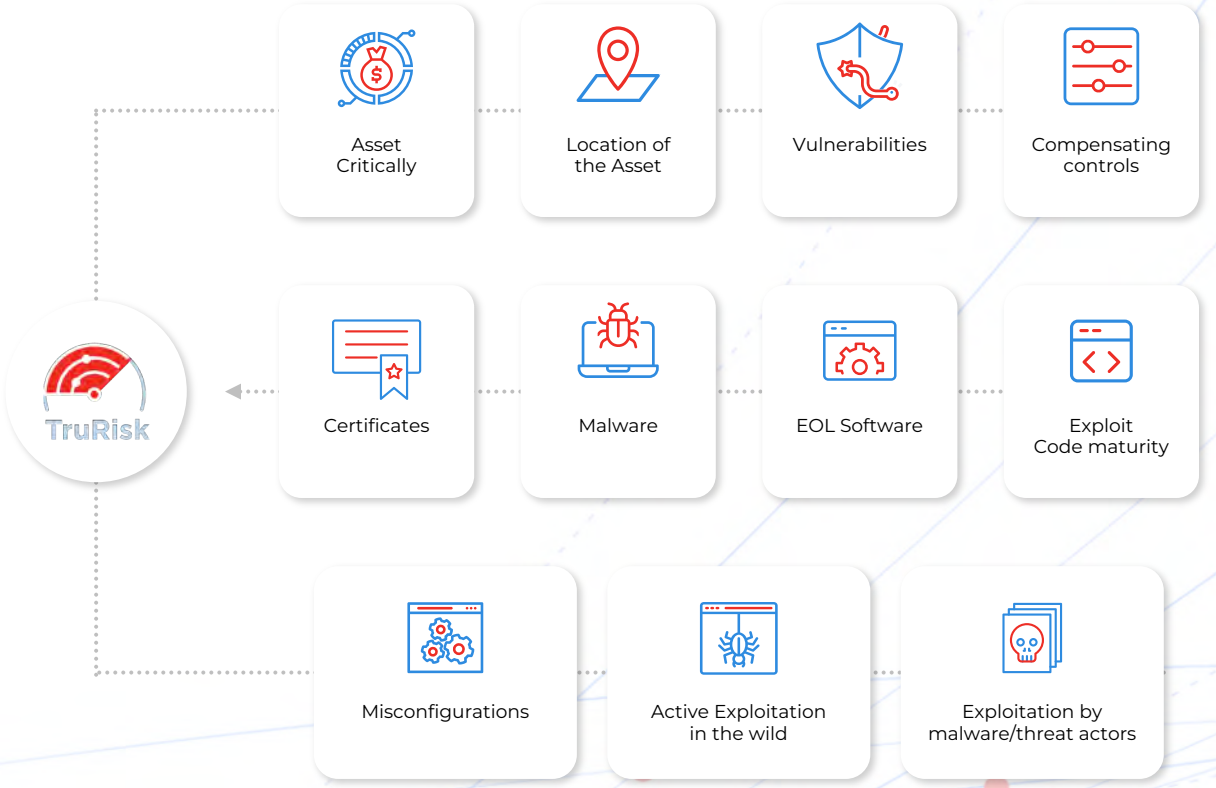


Qualys.

# Measure Risk with VMDR & TruRisk

## Prioritize Based On Risk

Prioritize based on **risk of exploitation, likelihood of exploitation or evidence of exploitation** & business impact




Qualys.

# Low/Medium CVSS High TruRisk

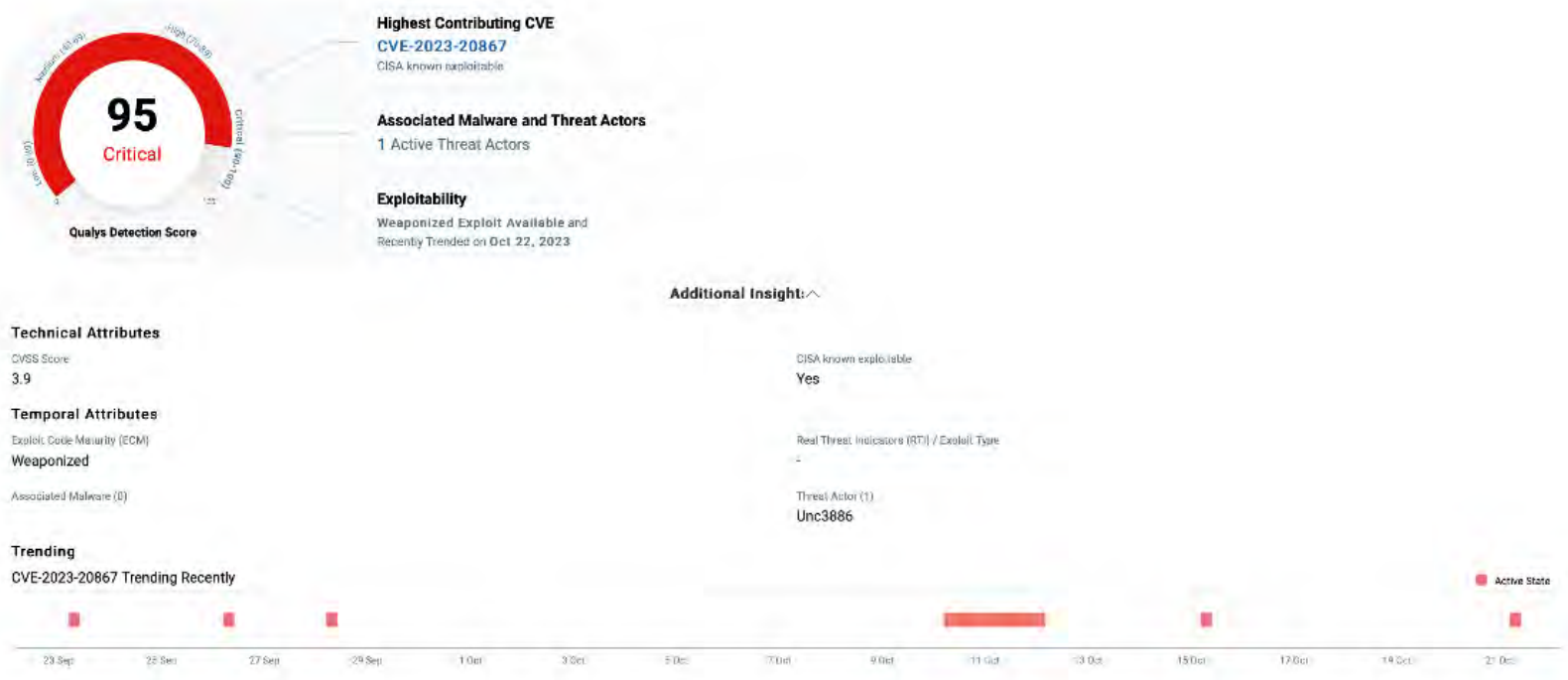
VMware Tools Authentication Bypass Vulnerability (VMSA-2023-0013)

CVSS 3.9

CISA KEV

Weaponized PoC

Exploited by Threat Actor & Trending




87M

Qualys.

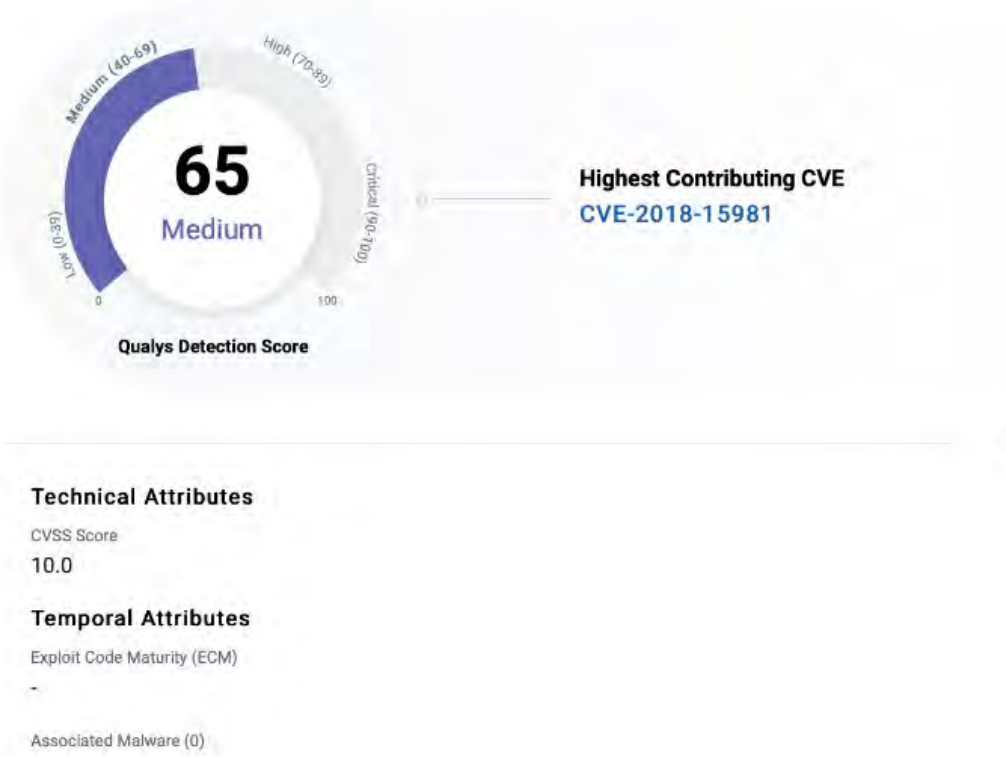
# Low/Medium TruRisk High CVSS

Adobe Security Update for Flash Player (APSB18-44)

CVSS 10.0

No evidence of exploitation

No Exploits available

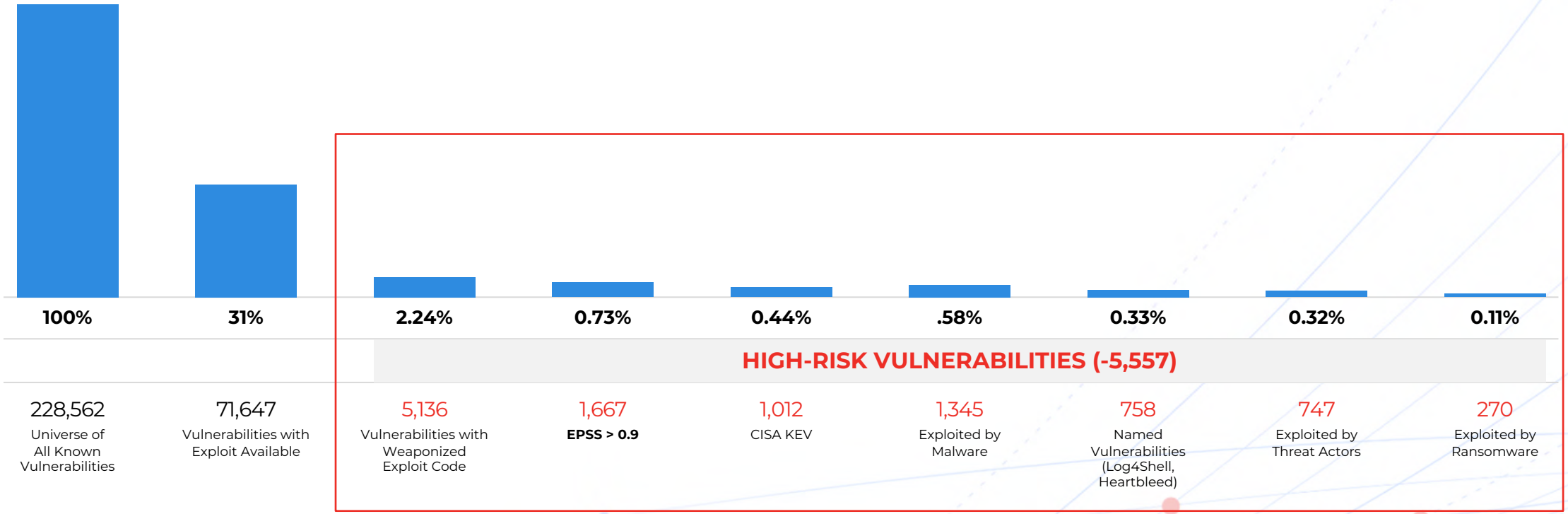



692M

Qualys.

# Never Miss a Beat

## TruRisk Correctly Prioritizes All High-Risk Vulnerabilities




Updated: 10/03/2023

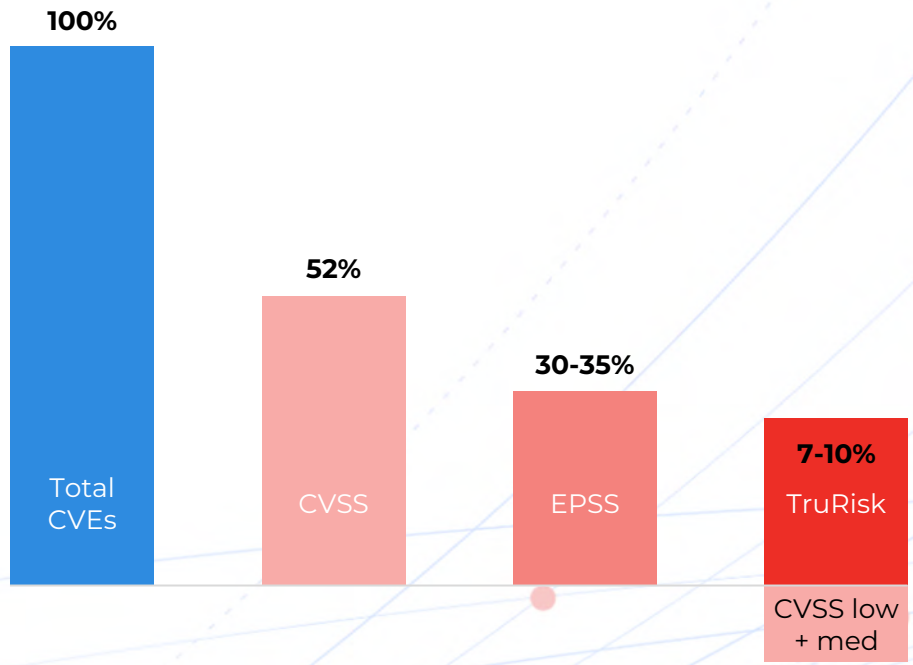
Qualys.

# Industry Leading Prioritization with TruRisk

Up to **85%**
fewer vulnerabilities

**~80%**
less ‘Ransomware’ vulnerabilities

## CVSS -> EPSS to TruRisk




Qualys.

# Measure Risk with VMDR & TruRisk

## Measure CyberRisk

**Quantify risk across vulnerabilities, assets, and groups of assets** helping organizations proactively reduce risk exposure and track risk reduction over time with Qualys TruRisk

## Prioritize Based On Risk

Prioritize based on **risk of exploitation, likelihood of exploitation or evidence of exploitation** & business impact & **Mitre ATT&CK context**

## Best-In-Class Threat Intelligence Included

Leverage insights from over 200k vulnerabilities sourced from over **25+ threat sources** to get best in class threat intelligence with the Qualys Cloud Threat DB


Qualys.

# Best-In-Class Research & Threat Intelligence

**Two** Pwnie Award Wins

**12+** Pwnie Award Nominations

**120+** Strong Research Team


**25+ Sources**

Qualys.

# Desired Outcomes (Accurate Inventory)

Build Up on Successes from One Step to the Next

**98%** Accurate CMDB

**55.5% Reduction** in TruRisk Score (600 -> 267) across **37K assets**

**92%** Reduction in MTTR (90 Days -> 7 Days)

**20% Reduction** in Cyber Insurance Premium

CINTAS®

Qualys.

# Communicate Risk with TruRisk

Know Your Risk Posture from Every Angle

01

## Measure Cyber Risk

**Quantify risk across vulnerabilities, assets, and groups of assets** helping organizations proactively reduce risk exposure and track risk reduction over time with Qualys TruRisk

02

## Communicate Cyber Risk

Communicate risk across different teams, business units and geographic locations by leveraging dashboards, reports and ITSM tools

03

## Eliminate Risk

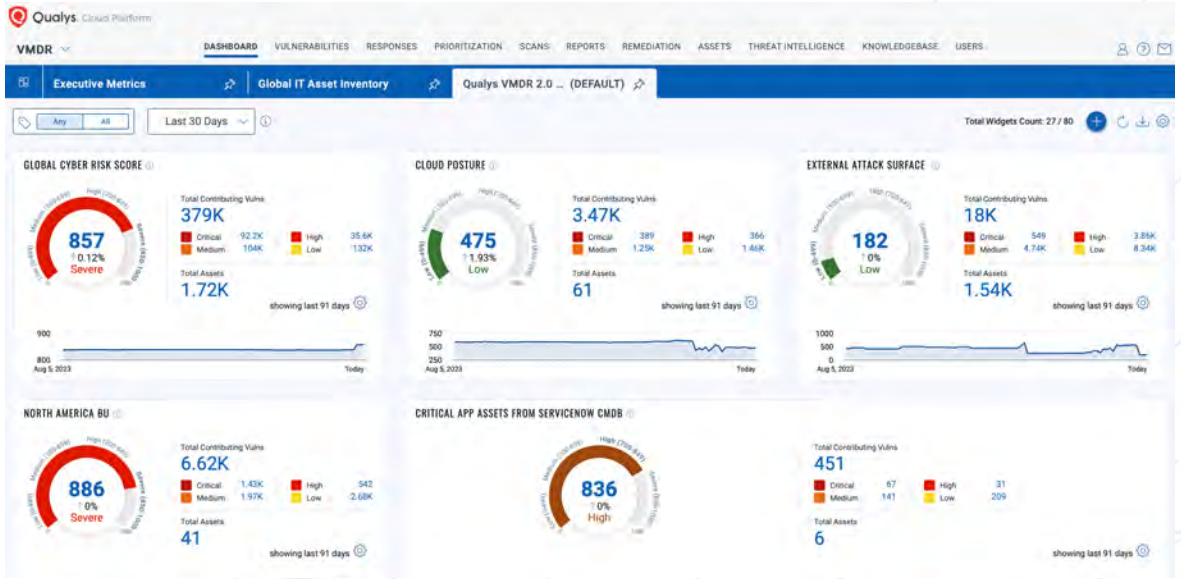
Patch any device anywhere, leverage multiple avenues from remediation to mitigation and block attack paths to eliminate risk


Qualys.

# Communicate Risk with VMDR

## Use Unified Dashboards To Communicate Risk

Create intuitive, customized **persona-based dashboards,** and share them across the organization from C-Level execs to practitioners




Qualys.

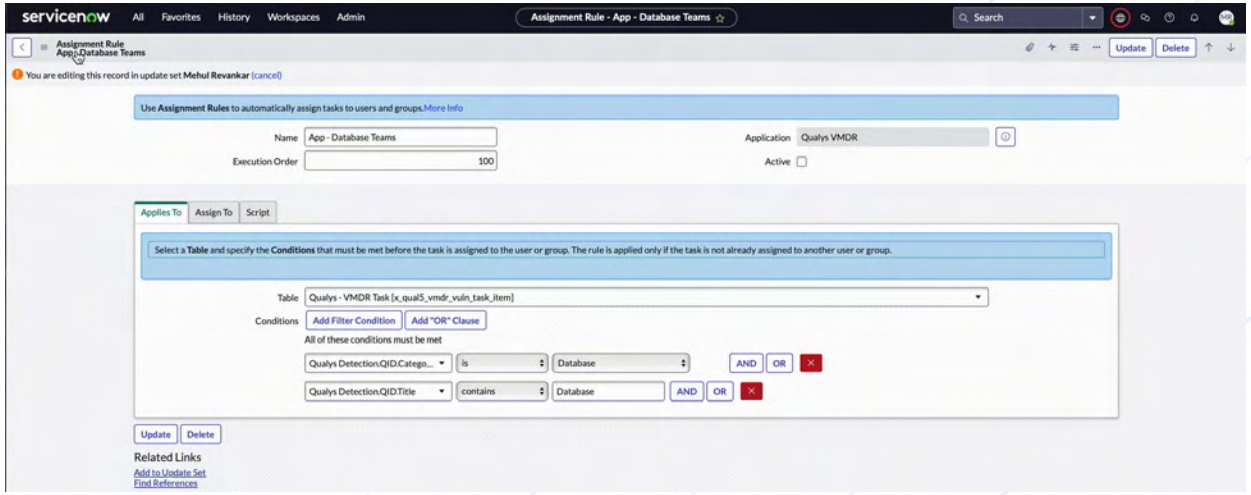
# Communicate Risk with VMDR

## Use Unified Dashboards To Communicate Risk

Create intuitive, customized **persona-based dashboards,** and share them across the organization from C-Level execs to practitioners

## Integrate with ITSM Solutions

Create Workflow Tickets, assign tasks to rightful owners, and close them out upon remediation




Qualys.

# Communicate Risk with VMDR

## Use Unified Dashboards To Communicate Risk

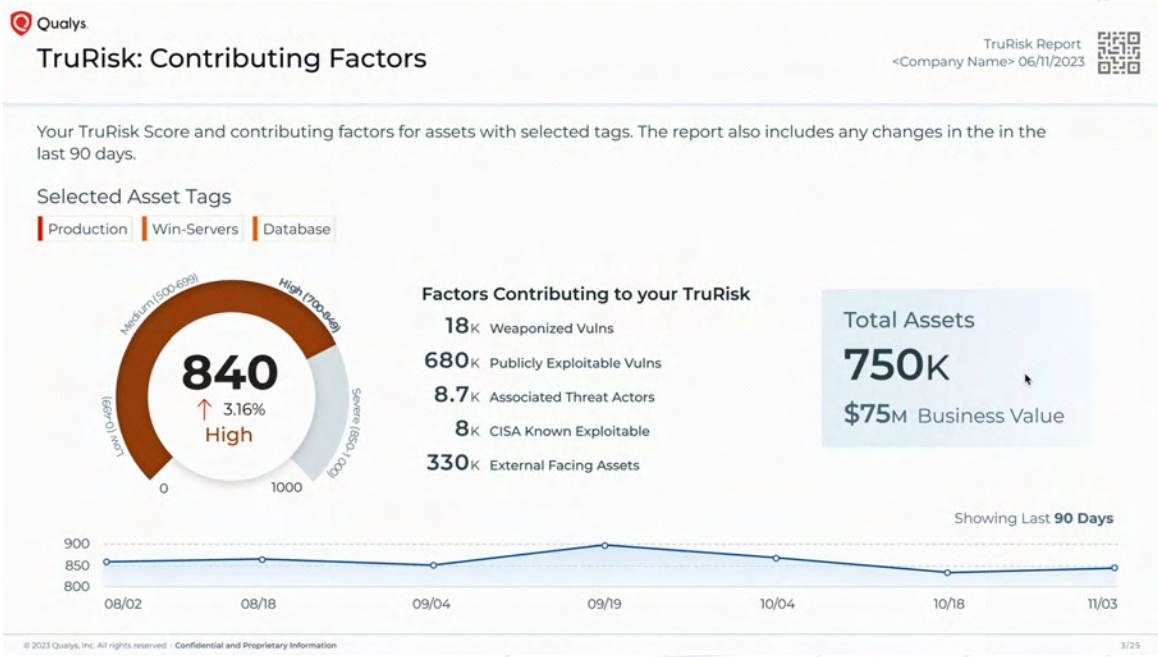
Create intuitive, customized **persona-based dashboards,** and share them across the organization from C-Level execs to practitioners

## Integrate with ITSM Solutions

Create Workflow Tickets, assign tasks to rightful owners, and close them out upon remediation

## Leverage TruRisk Report

Share the State of the Union with executives to understand the latest trends and landscape of risk for your organization, and implement prescriptive actions to mitigate risk




Qualys.

# Desired Outcomes (Effective Prioritization)

Build Up on Successes from One Step to the Next

- **Prioritization Based on Risk (QDS >80)**
  Fewer vulnerabilities reduced more risk
- **70% real risk reduction** in just days
- **75% Fewer Resources Required** for vulnerability management
- **Saved countless hours in manual effort** by automatically creating tickets in ServiceNow, assigning them to rightful owners and remediate them upon approval, and close tickets


Qualys.

# Eliminate Risk with TruRisk

## Ingesting the Best Intelligence Anywhere

01

### Measure Cyber Risk

**Quantify risk across vulnerabilities, assets, and groups of assets** helping organizations proactively reduce risk exposure and track risk reduction over time with Qualys TruRisk

02

### Communicate Cyber Risk

Communicate risk across different teams, business units and geographic locations by leveraging dashboards, reports and ITSM tools

03

### Eliminate Risk

Patch any device anywhere, leverage multiple avenues from remediation to mitigation and block attack paths to eliminate risk

**Qualys Patch Management**

Qualys.

# Eliminate Risk with Qualys Patch Management

### Patch Any Device, Anywhere

Patch all major Windows, Linux & Mac OS'es, 3rd Party Apps. Run scripts to fix misconfigs, run custom remediation

### Automated Risk Based Remediation

Precisely identify patches to remediate vulnerabilities, and automatically remediate low impact, high risk vulnerabilities with zero touch automated patching

### Eliminate Attack Paths with MITRE ATT&CK Context

Leverage MITRE ATT&CK Insights to identify attack pathways to exploitation and eliminate the risk (for e.g. lateral movement)

### Track Remediation End To End

Integrate with ITSM solutions to automatically create tickets, deploy patches upon approval drastically improving MTTR

**Qualys Patch Management**

Qualys.

# Desired Outcomes (Risk Elimination)

Build Up on Successes from One Step to the Next

**~70%** **Vulnerability debt due to 3rd party software**

**3M** Patches deployed in 6 months (SCCM 1.2M in 2 yrs, reactively)

**~94%** of vulnerabilities closed w/ Integrated Patching. Patch/sec teams to concentrate on critical remaining

**In 2022**

**44,803**
patches from Microsoft, 10K+ from third parties

**10K+**
from third parties

VLC:
**105**
(2007-2022)


Adobe:
**1530**
(2004-2023)

Chrome:
**2647**
(2008-2023)

iTunes:
**613**
(2005-2023)

Firefox:
**2131**
(2003-2023)

Qualys.

# ...this is why **Qualys VMDR is #1 Solution**

Qualys.

# Recognized Leader in Risk-Based Vulnerability Management





Qualys.

# Demo

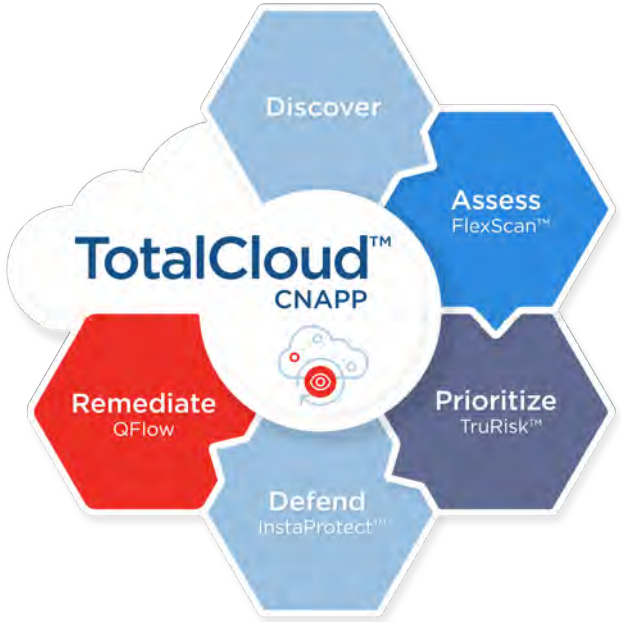
Qualys.

# ...but there's more to managing risk

Qualys.

# Extend Vulnerability Management to the Cloud

Secure Every Attack Surface. Reduce More Risk




## Cloud & Container Security with TotalCloud

Securing the modern cloud & container ecosystem **requires a new approach, with flexibility to scan through multiple methods & licensing for ephemeral assets**. And go beyond vulnerability mgmt. to cloud security posture management**.**

## Learn more at:

**2:20 – 3:00 PM**

**Elevating Cloud Security from Config Assessment to Measuring, Prioritizing and Reducing Your Risk in Cloud with Qualys TotalCloud**

**Parag Bajaria, VP, Product Management, Qualys**
**Terry Barber, Manager, Security Operations, American Express Global Business Travel**

Qualys.

# Active Directory Risks

## Secure Every Attack Surface. Reduce More Risk


### Active Directory (AD) Security

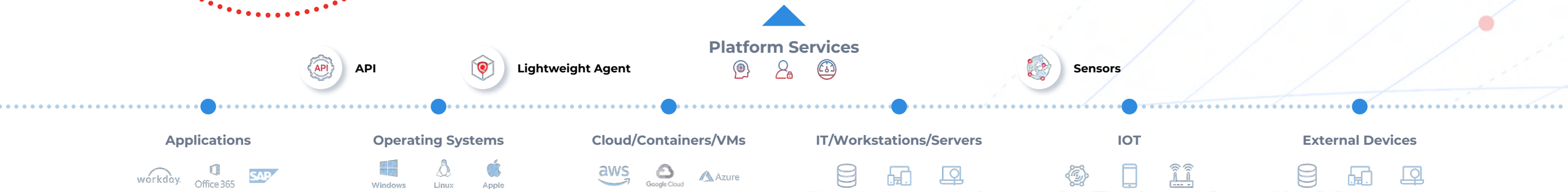
(AD) serves as the backbone of IT infrastructure in many organizations, and the **risk of Active Directory attacks is on the rise.** To manage cyber risk effectively, securing AD is crucial for protecting organizations from breaches and unauthorized access.

## Learn more at:

**4:00 – 4:20 PM – Track 1**

**Manage and Reduce the Active Directory Attack Surface**

**Lavish Jhamb, Senior Product Manager, Qualys**




Qualys.

# Risk From Supply Chain

## More Attack Surfaces. More Risk

### First-Party Risk

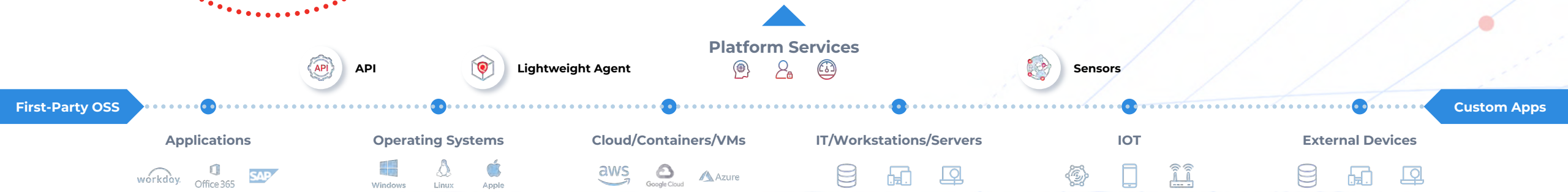
**Hidden risks from Open-source software**, and First Party software continue to rise. Silo'd tools, lack of visibility make the problem even worse.

## Learn more at:

**3:00 – 3:30 PM**

**Assess, Prioritize and Remediate the Technology Supply Chain Risks with Qualys Platform**

Eran Livne, Sr. Director, Product Management, Qualys
Corey Amsler, Director, Cybersecurity,
General Electric Vernova




Qualys.

# Customer Presentation


Qualys.

BANCO PAN

Leading Brazil in Payroll Loans

## Ibovespa: BPAN4

**Company Founded:**
1969

**Headquarters:**
São Paulo, Brazil

**Company Size:**
~3,000 Employees

**Company Scope:**
National

**Products:** Credit cards, payroll loans, vehicle financing, real estate services and digital banking.

Qualys.

# Raphael Ferreira

Cyber Risks Leader, Banco PAN

3 years with Banco PAN

10 years of experience in cybersecurity, with focus on penetration testing, vulnerability management and analysis, third-party risk management and cyber risk analysis

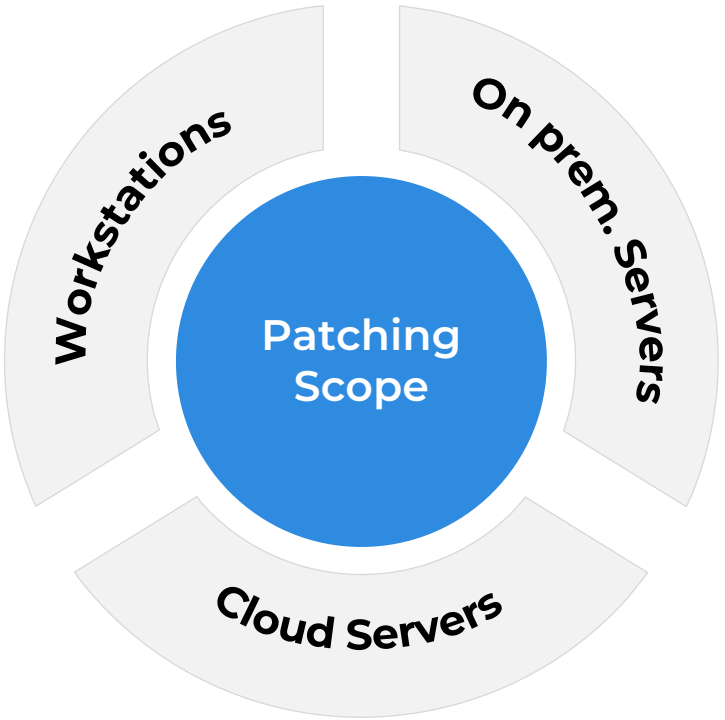
MBA in Information Technology Management from the University of Computer Science and Administration in São Paulo, Brazil

Qualys.

# Problem

Qualys.

# More than 80k vulnerabilities, Most of Them with SLA Expired




**Use Case:** Fixing vulns required manual, labor-intensive approach

- Manual processes and systems
- Lack of team with expertise in vulnerability remediation
- Executive reporting with bad indicators
- The previous tool did not support Linux

Qualys.

# Solution

Qualys.

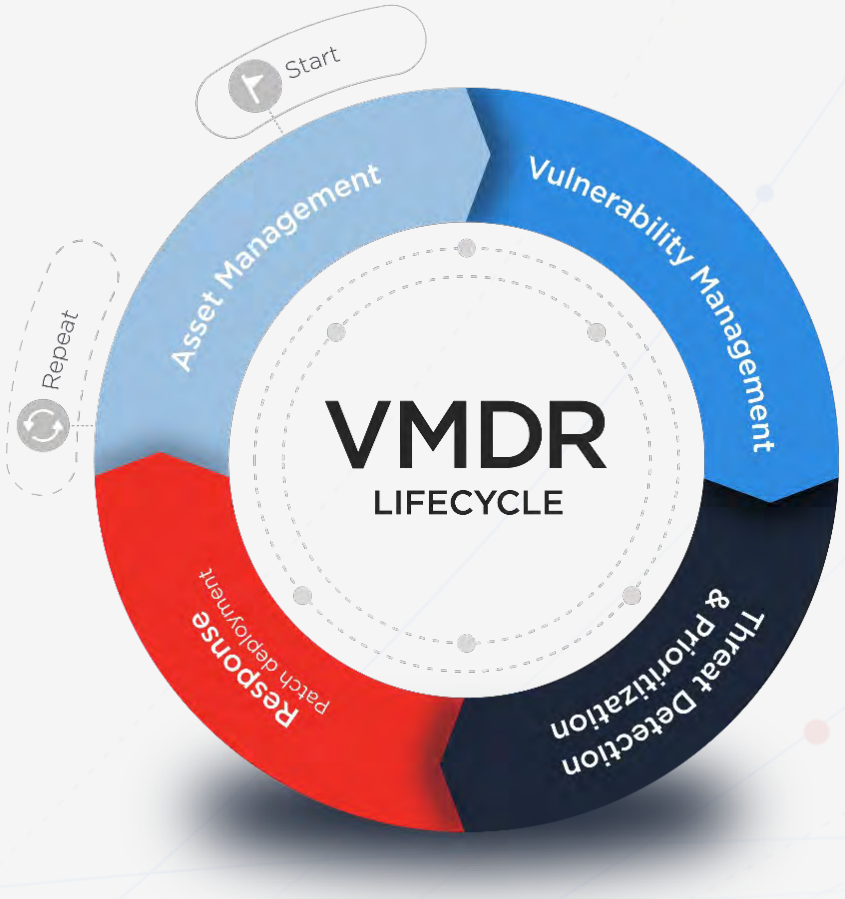
# Leveraged Qualys TruRisk Platform to Reduce Risk

- **Transitioned to Risk Based Approach** instead of trying to fix every vulnerability

- **Tracked Every Prioritized vulnerability for remediation end to end** from Discovery to Prioritization to Remediation with ServiceNow & Qualys Patch Management

- Created Tickets, assigned them to rightful asset or application owners. **Defined SLA's for remediation**. Tracked progress with ServiceNow Dashboards

- **Automatically deployed patches** for remediation with Qualys Patch Management upon approval

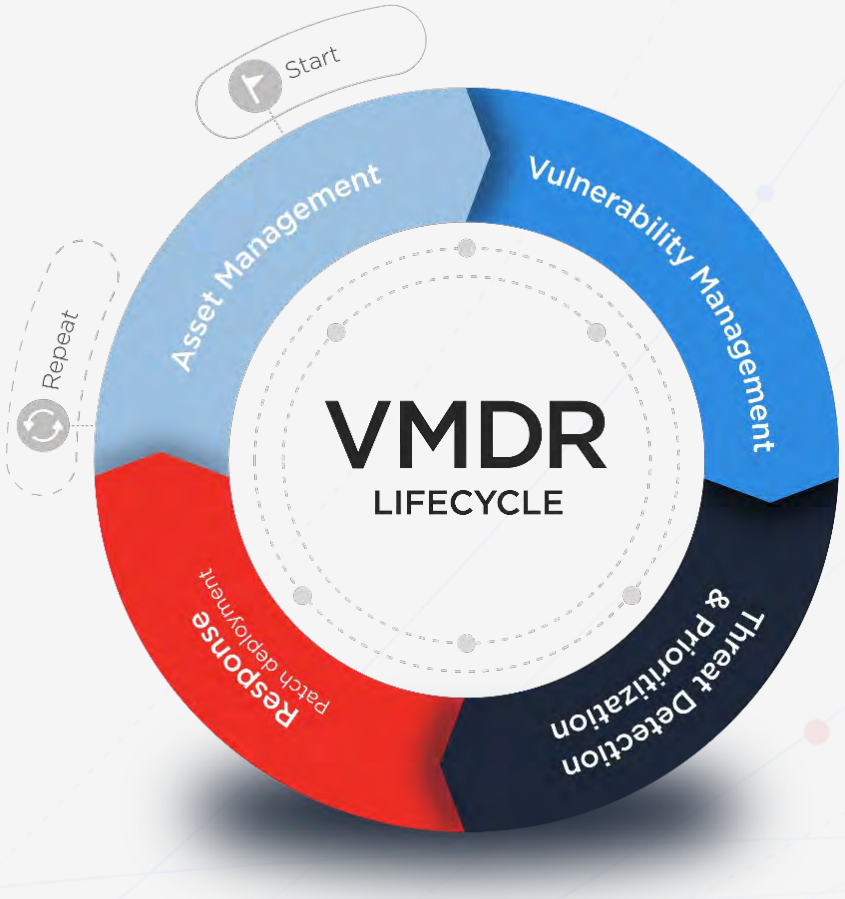



Qualys.

# VMDR + ServiceNow ITSM + Patch Management

## A Path to Vulnerability Management Nirvana

- Overall, **70% drop in high and critical vulnerabilities** in 30 days
- **75% (4 to 1) drop in number of analysts** required to manage vulnerabilities across different teams
- **95% decrease** on Workstations related vulnerabilities & **51% decrease** in vulnerabilities within On Prem servers
- Accuracy of **96% on CMDB,** after adding previously unmatched CIs



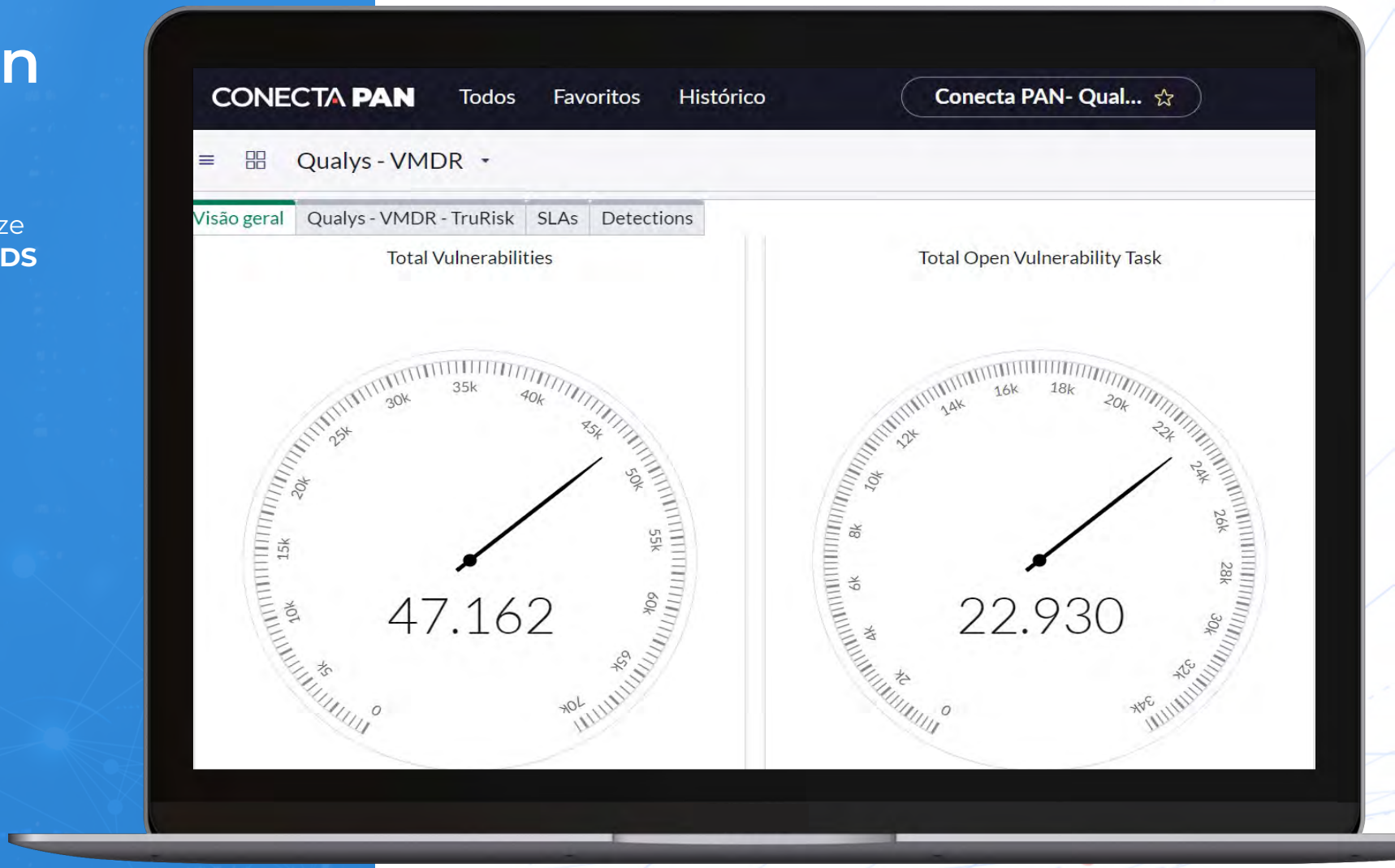

Qualys.

# Proof of Concept

Qualys.

# Qualys Integration with ServiceNow

We used **Qualys TruRisk** to prioritize vulnerabilities based on risk with **QDS (Qualys Detection Score) > 80**

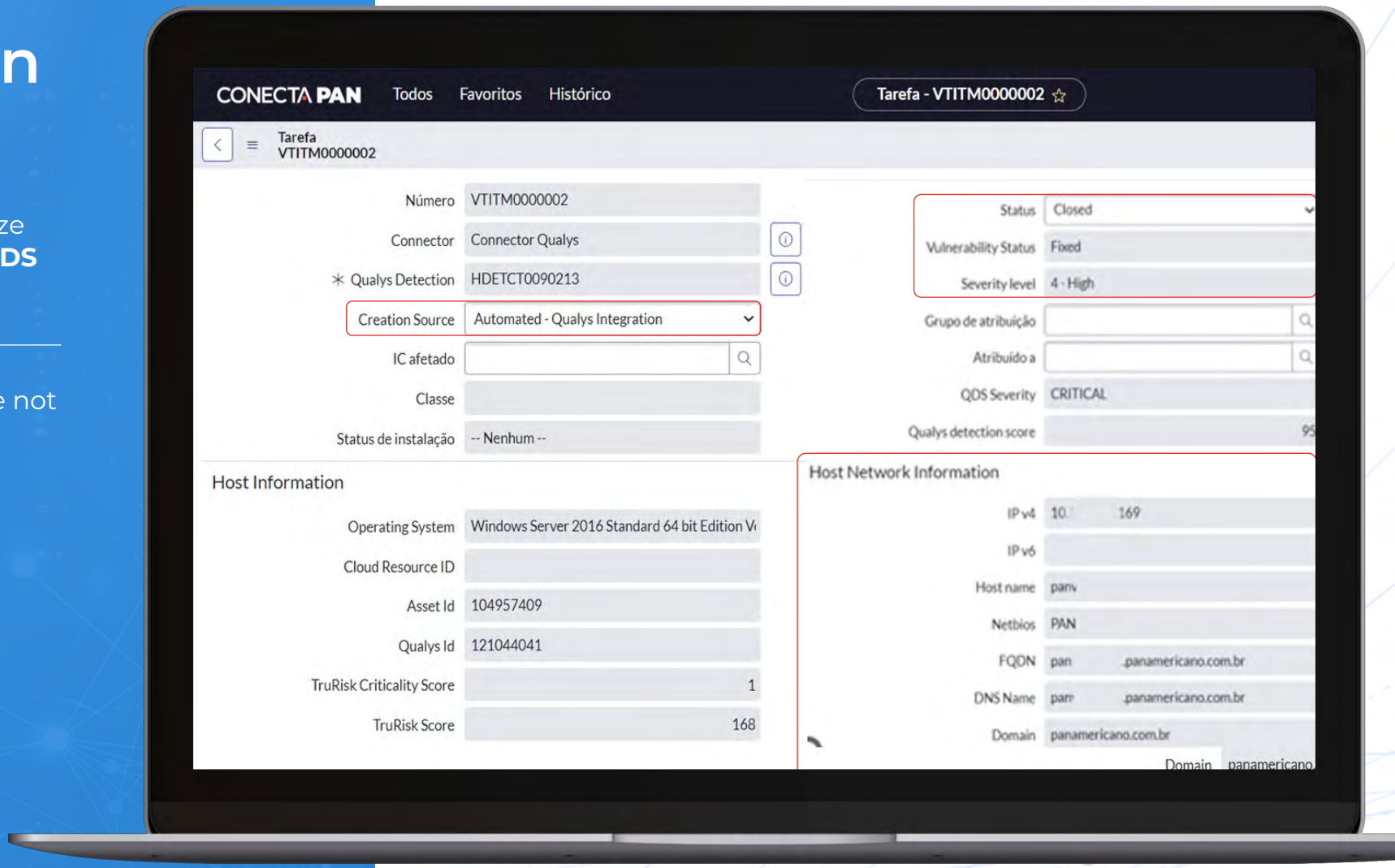



Qualys.

# Qualys Integration with ServiceNow

- We used **Qualys TruRisk** to prioritize vulnerabilities based on risk with **QDS (Qualys Detection Score) > 80**

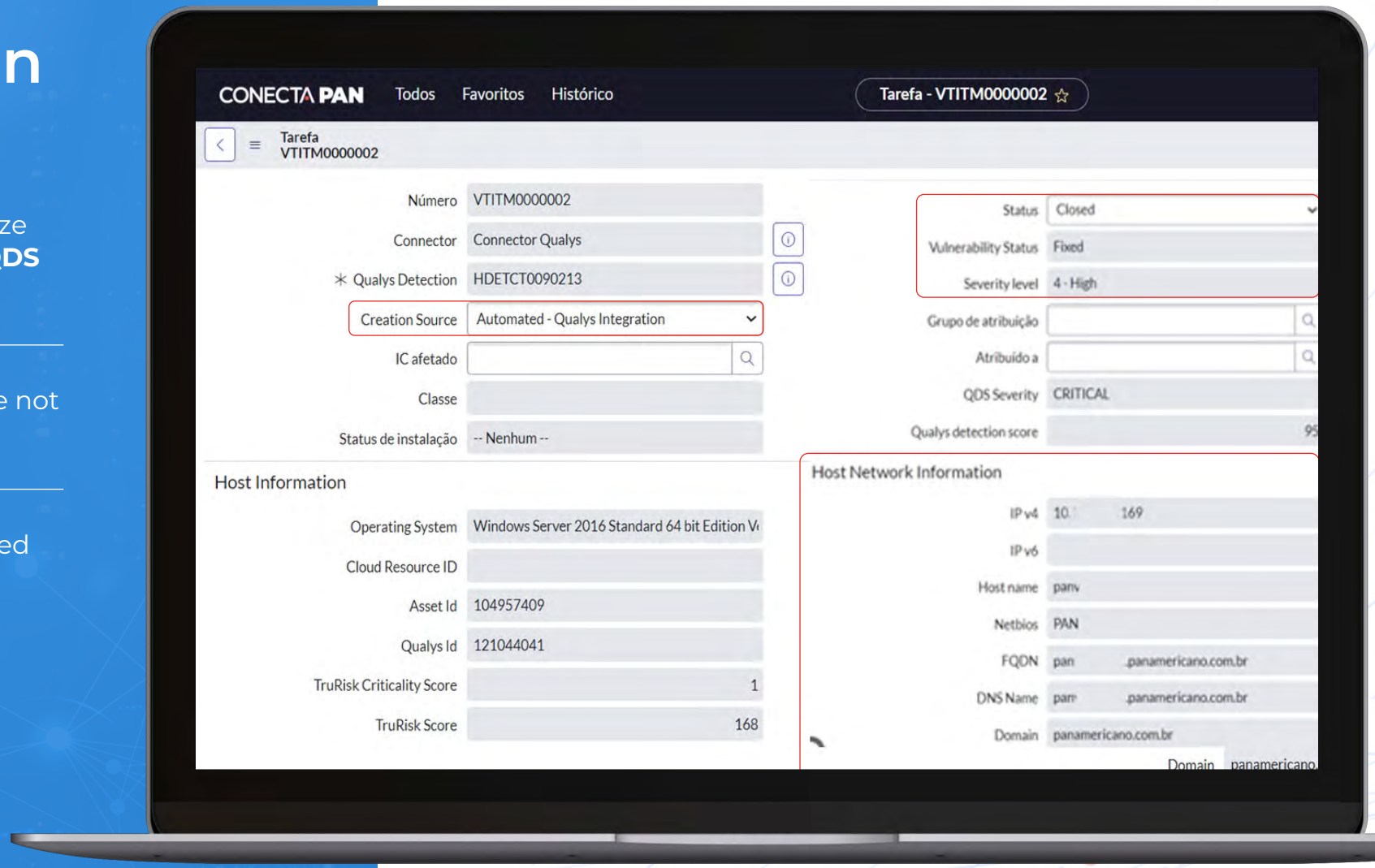
- Identified multiple assets that were not updated in ServiceNow CMDB




Qualys

# Qualys Integration with ServiceNow

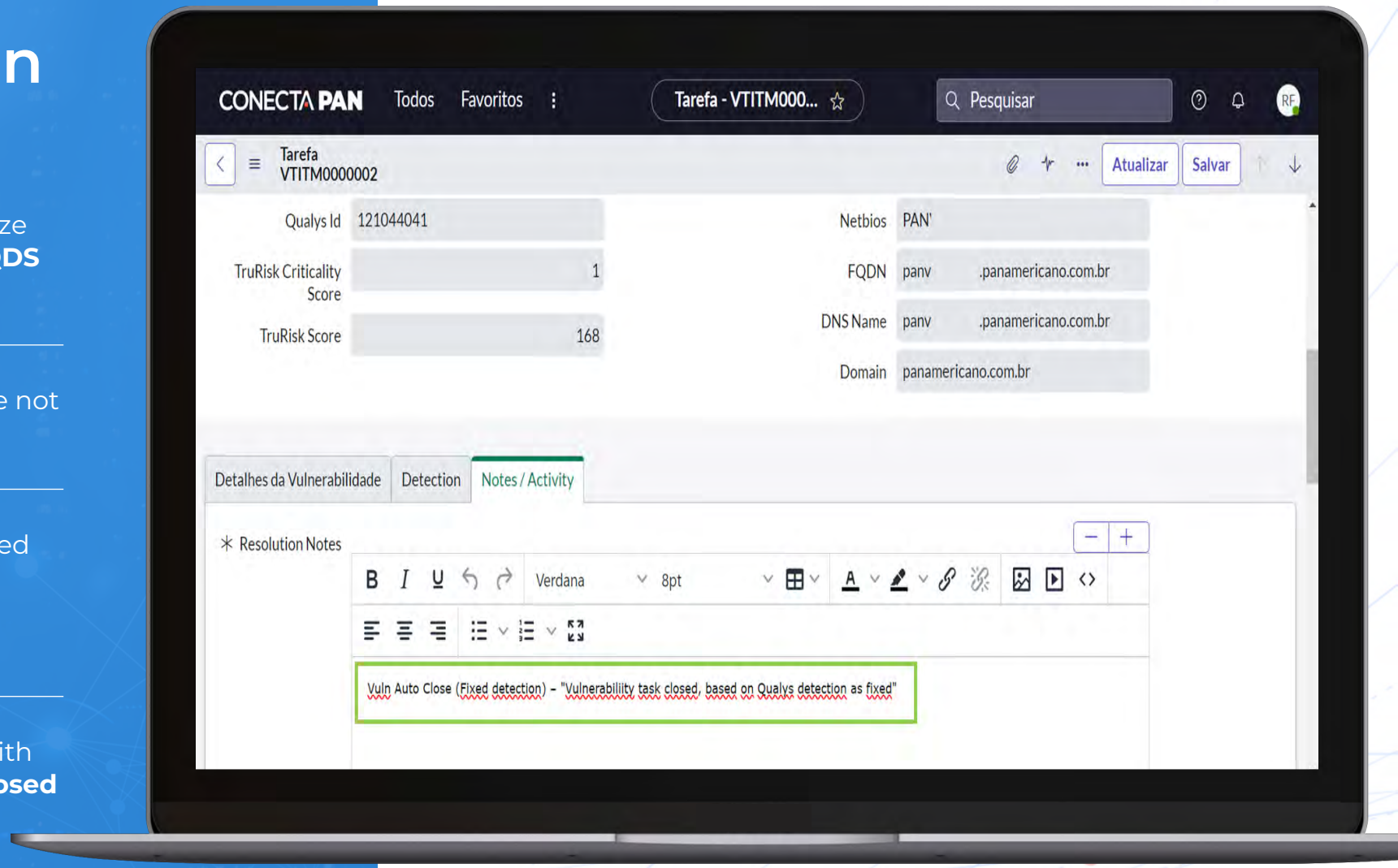
- We used **Qualys TruRisk** to prioritize vulnerabilities based on risk with **QDS (Qualys Detection Score) > 80**
- Identified multiple assets that were not updated in ServiceNow CMDB
- For all imported assets also imported **vulnerability information and managed its lifecycle** end to end in ServiceNow




Qualys

# Qualys Integration with ServiceNow

- We used **Qualys TruRisk** to prioritize vulnerabilities based on risk with **QDS (Qualys Detection Score) > 80**
- Identified multiple assets that were not updated in ServiceNow CMDB
- For all imported assets also imported **vulnerability information and managed its lifecycle** end to end in ServiceNow
- Automatically deployed patches with Qualys Patch Management and **closed the ticket status** on **ServiceNow**




Qualys

# Business Outcome

Qualys.

# Key Outcomes

## VMDR + SNOW integration + Patch Management, a game changer

### Vulnerability Reduction

70% of reduction considering all critical & high severity vulnerabilities.

### MTTR Reduction

Reducing 54% of the time spent to fix vulnerabilities on servers and 68% less time to remediate workstation vulnerabilities.

### Time Saving (Employee hours)

Patch Management replaced the need of an additional analyst solely focused on vulnerability fixing in each infrastructure team.

Qualys.

# Our Main Gains

## VMDR + PM + SNOW integration helped with success

### Accurate CMDB

We identified hundreds of assets that were not on CMDB and added these assets with owner, exposure and other relevant information.

### Fast track of main issues on ITSM tool

Since we imported just confirmed vulnerabilities with QDS greater than 80, we focused the vulnerability remediation processes on the relevant issues that have potential to compromise the bank.

### Increased cyber maturity of the entire company.

Considering the vulnerability management and remediation process that is now automated, information security team protects the main data of the company and can use our internal resources in a smarter way.

Qualys.


SC 23


SC 23