Guide

KEEP CALM AND PRIORITIZE

Top 5 Requirements for Prioritizing Vulnerability Remediation

Qualys

Overview

IT departments are overwhelmed by the abundance of vulnerabilities that continue to grow at a rapid pace every day. They struggle to identify the most critical threats they must address right away at any given point to protect their organizations from a compromise.

Attempting to eradicate 100 percent of vulnerabilities sequentially, by treating them all as equally important, is impractical, myopic and dangerous.

SOME VULNERABILITIES REPRESENT A MINOR RISK, WHILE OTHERS MUST BE ADDRESSED IMMEDIATELY

Ignoring serious vulnerabilities for extended periods of time while you tend to trivial ones is like deciding to paint a house whose roof you know is in danger of collapsing. Moreover, the damage potential of vulnerabilities fluctuates constantly. For example, a vulnerability considered unimportant for months can suddenly become critical if an exploit kit for it becomes widely available.

Consequently, organizations that fail to properly prioritize vulnerability remediation open themselves up to devastating cyber attacks. They risk sustaining extensive damage to their operations, financial standing, brand image, corporate reputation and customer and partner relationships.

5 Key Elements for Successfully Prioritizing Vulnerability Remediation

- A comprehensive and continuously updated view of all your IT assets
- Knowledge of the constant stream of vulnerability disclosures
- The ability to correlate external threat information with your vulnerability gaps
- Dashboard tools to visualize your threat landscape
- Precise assessments of your organization's threat scenarios

1

A COMPREHENSIVE AND CONTINUOUSLY UPDATED VIEW OF ALL YOUR IT ASSETS

A comprehensive, continuously updated view of all your IT assets, whether they are on premises or in the cloud, and permanently or intermittently attached to your network

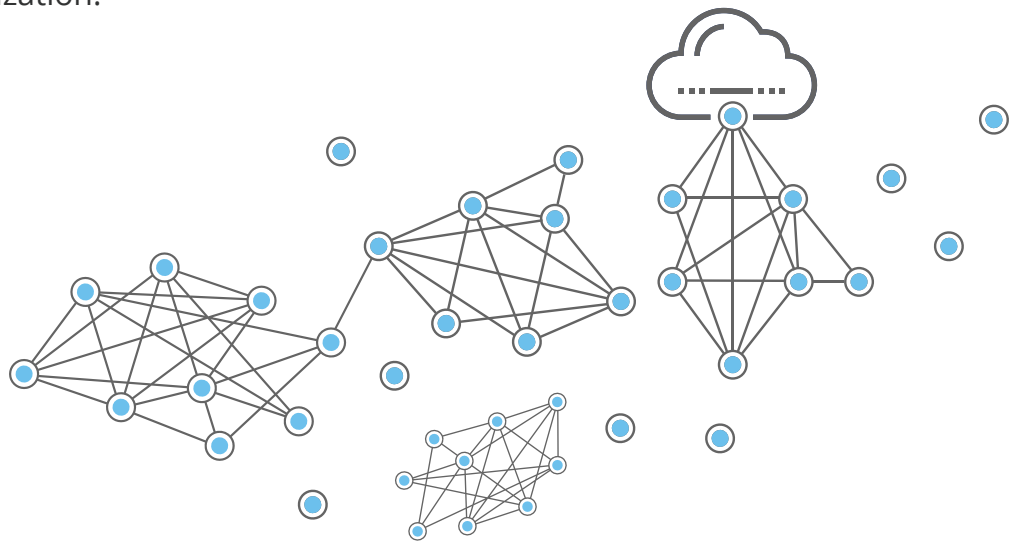
When attempting to prioritize vulnerability remediation, it's what you don't know that derails your efforts. At the most basic level, this means being aware of all the hardware and software in your organization, from high-end systems to mobile apps.

There can be no "phantom" servers, PCs, smartphones, tablets, printers, applications, middleware and the like lurking in your network without your knowledge. You must have a complete, unobstructed view of your IT environment at all times, and be instantly aware of its changes.

AN INVISIBLE IT ASSET CAN'T BE ANALYZED FOR VULNERABILITIES, SO IT'S A TICKING TIME BOMB WAITING TO BE DETONATED BY AN ATTACKER.

In addition to having a complete list of your IT assets, you need granular, detailed access to the components of each one. You must also understand how extensively each asset is interconnected with and dependent of other systems. Finally, it's critical to know what is the role of each asset in your overall IT environment and how valuable and important it is to your organization.

This contextual knowledge and detailed data form the foundation upon which you can then begin the process of prioritizing vulnerability remediation. Absent this underlying information structure, your attempts to assess vulnerability risks will be ill-informed and ultimately erratic and ineffective.



2

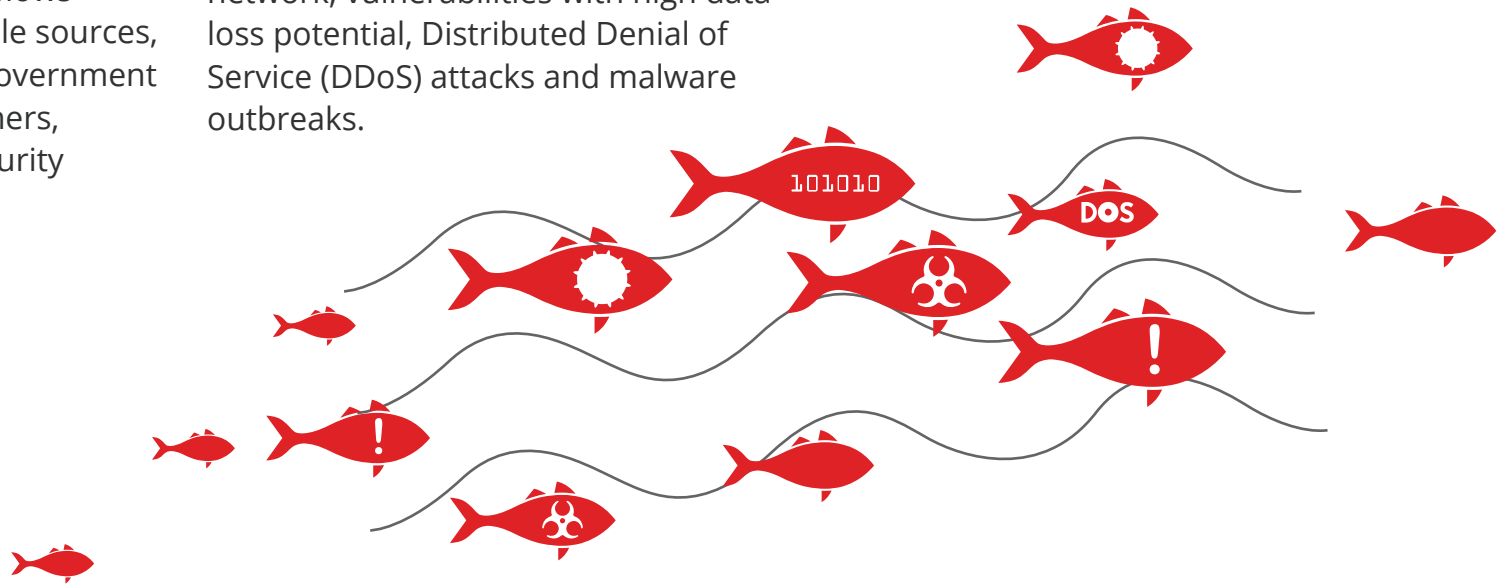
KNOWLEDGE OF THE CONSTANT STREAM OF VULNERABILITY DISCLOSURES

Knowledge of the constant stream of infosec vulnerability disclosures

Just like you must have a clear and deep knowledge of your organization's IT assets, **YOU ALSO NEED TO PLUG INTO THE FIREHOSE OF EXTERNAL VULNERABILITY DISCLOSURES, SO YOU'RE AWARE OF THE LATEST THREATS OUT IN THE WILD.**

This disclosure information flows uninterruptedly from multiple sources, including industry groups, government agencies, academic researchers, technology analysts and security vendors.

For example, you must be aware of "zero day" vulnerabilities being actively exploited, publicly available exploit code, actively attacked vulnerabilities, "lateral movement" vulnerabilities that let hackers use a compromised system to attack other machines on the same network, vulnerabilities with high data loss potential, Distributed Denial of Service (DDoS) attacks and malware outbreaks.



3

THE ABILITY TO CORRELATE EXTERNAL THREAT INFORMATION WITH YOUR VULNERABILITY GAPS

The ability to correlate external threat information with the vulnerability gaps that exist in your IT environment

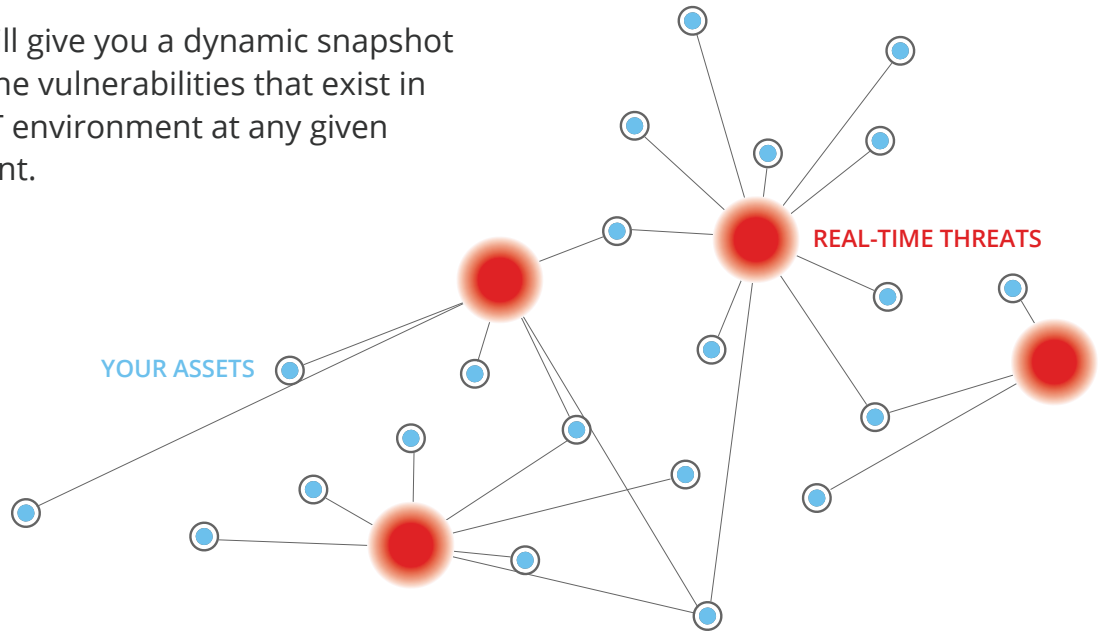
Lets say you have a comprehensive, detailed view of your IT asset landscape. And you're also up to date on the universe of thousands upon thousands of disclosed vulnerabilities. Congratulations, but you're far from done. Now you must connect the dots. And to do so manually is an arduous task.

YOU NEED TO MESH BOTH SETS OF INTERNAL AND EXTERNAL DATA – YOUR IT ASSET INFORMATION AND DISCLOSED VULNERABILITIES – AND CORRELATE THEM.

And you need to be doing this continuously, so you're alerted whenever there is a match.

You also must be able to proactively conduct specific searches, combining multiple variables, to find assets that may be potentially at risk.

This will give you a dynamic snapshot of all the vulnerabilities that exist in your IT environment at any given moment.



4

DASHBOARD TOOLS TO VISUALIZE YOUR THREAT LANDSCAPE

Dashboards, control panels, graphing and reporting tools to visualize your threat landscape in a holistic, consolidated way

Once you have correlated your internal and external threat data and identified impacted IT assets, you must be able to drill down on the data, mine it for patterns, slice and dice it, aggregate it in custom reports and represent it graphically.

THIS MULTIDIMENSIONAL AND ITERATIVE ANALYSIS OF THE DATA WILL ALLOW YOU TO EXTRACT INSIGHTS AND GAIN AN AWARENESS OF YOUR SECURITY POSTURE THAT YOU OTHERWISE WOULDN'T HAVE ACCESS TO.

You should be able to measure your progress and remediation efforts with real-time trend analysis and generate scan and patch reports for your stakeholders. After all, the goal is not just to identify vulnerabilities and assets, but rather to prioritize which ones you are going to remediate first.

5

PRECISE ASSESSMENTS OF YOUR ORGANIZATION'S THREAT SCENARIOS

Precise assessments of how critical certain threat scenarios are in your organization's specific context, to accurately detect risk

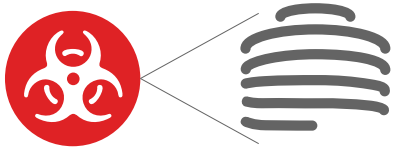
Finally, you're now ready to factor in various criteria for assessing how critical certain threat scenarios are in your organization's specific context using actionable intelligence.

After all, every IT environment is different.

THE GOAL: To be able to prioritize your vulnerability remediation tasks in a continual, contextual, automated and precise process.

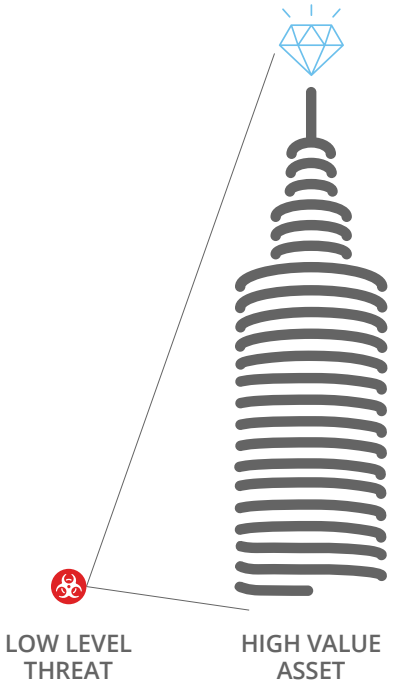
SCENARIO A:

Lets say there's a vulnerable database software that is being savagely exploited in the wild, causing chaos in many companies. And you happen to have one instance of it. However, in your environment this database is only present in a system of marginal importance that is isolated from the rest of your infrastructure. You determine that if that asset were compromised, the risk to your organization would be trivial.



SCENARIO B:

Likewise, you may encounter the opposite scenario, in which a vulnerability that isn't attracting much attention in the industry may be a critical one for your organization.



Qualys **ThreatPROTECT**

Overwhelmed by vulnerabilities?

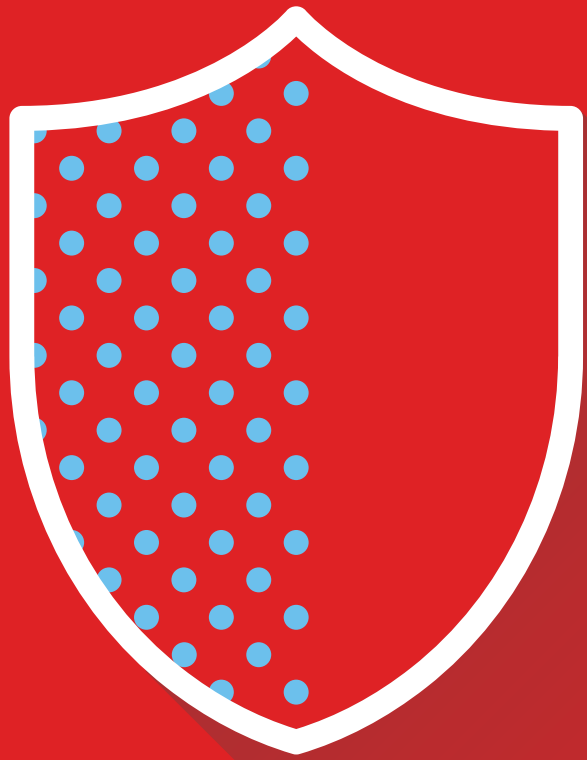
Qualys ThreatPROTECT lets you take full control of evolving threats, so you know which vulnerabilities to remediate first.

New vulnerabilities are disclosed every day, amounting to thousands per year. Qualys ThreatPROTECT correlates active threat intelligence information with your vulnerability data, allowing you to pinpoint the IT assets that are at greatest risk within your organization.

With ThreatPROTECT, you get a holistic, contextual and continually updated “at a glance” view of your threat exposure. The latest addition to the Qualys Cloud Platform, ThreatPROTECT eliminates guesswork and flags for you which vulnerabilities you must tackle now.

ThreatPROTECT features a highly customizable dashboard with a variety of report templates and graph-creation capabilities. It also has a powerful search engine, and a live threat intelligence feed.

ThreatPROTECT fine-tunes your IT department’s vision and guides it with actionable intelligence through the process of closing security holes in a precise, strategic manner.

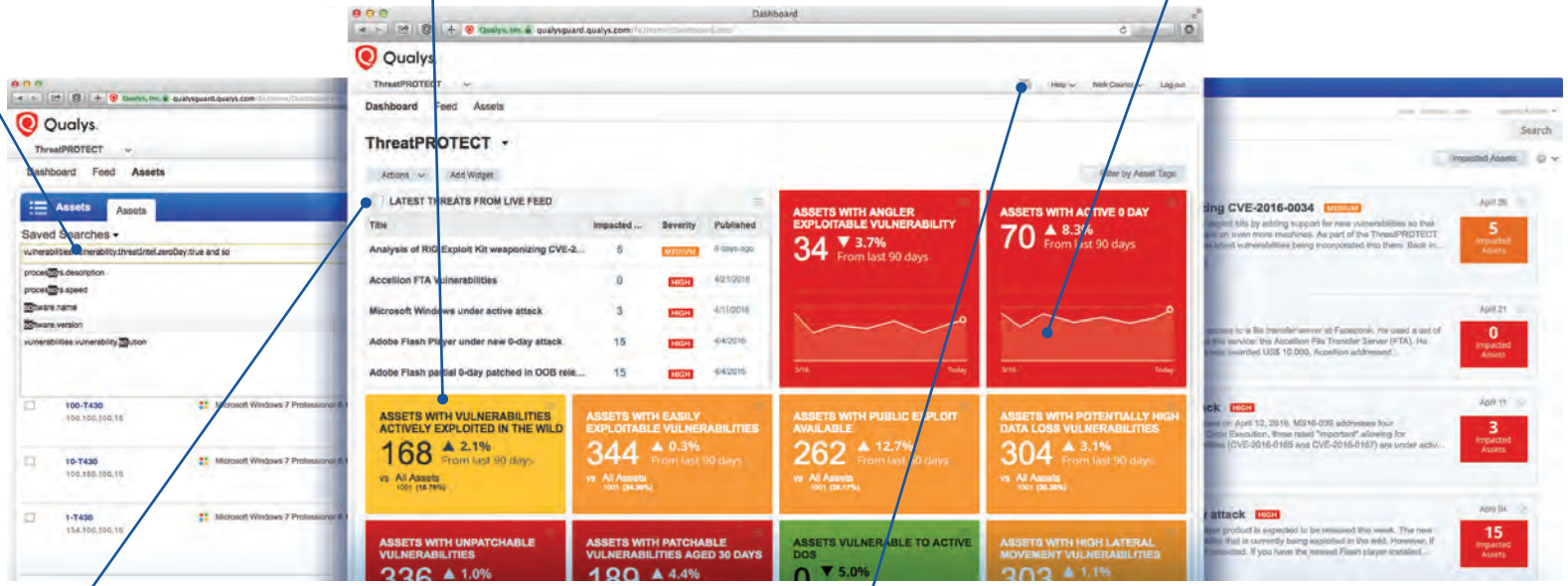


Qualys **ThreatPROTECT**

Identify vulnerable systems with Google-like search.

Quickly see how your systems are exposed to active threats such as zero-days, actively attacked vulnerabilities, and many more.

Measure your progress and remediation efforts with real-time trend analysis.



Includes a Live Threat Intelligence Feed where Qualys security engineers continuously validate and rate new threats from internal and external sources.

Get alerted when new active threats surface in your environment, and when your user-defined thresholds are met.

For a 14 day trial, visit **qualys.com/ThreatPROTECT**

Qualys.