



# How Well Do You Know Your VMDR

## Know the Hidden Gems of VMDR



**Kevin O'Keefe**

Lead Security Solution Architect

# 1. What do you use to prioritize your risk remediation program?

**CVSS**

**QDS**

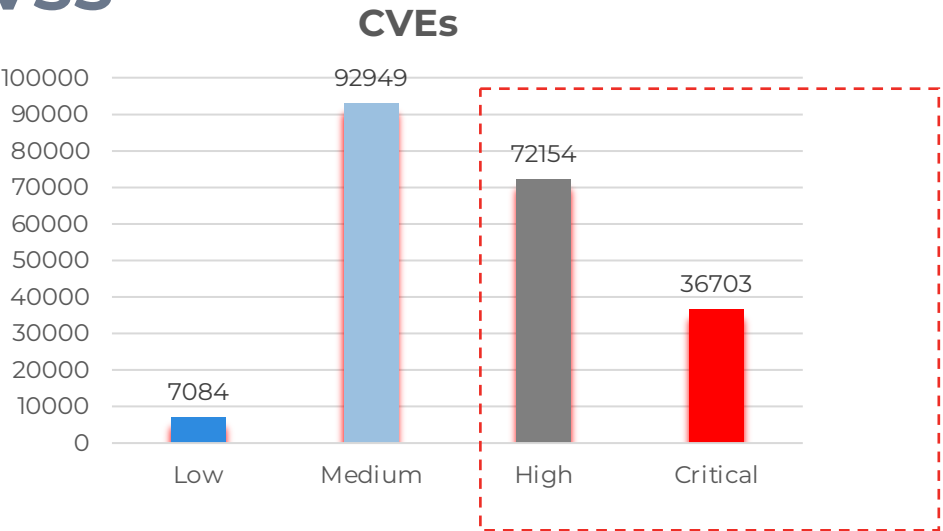
**Qualys Severity**

# Too Many Vulns Have Been Deemed ‘Critical’

## CVSS Lacks Threat Context

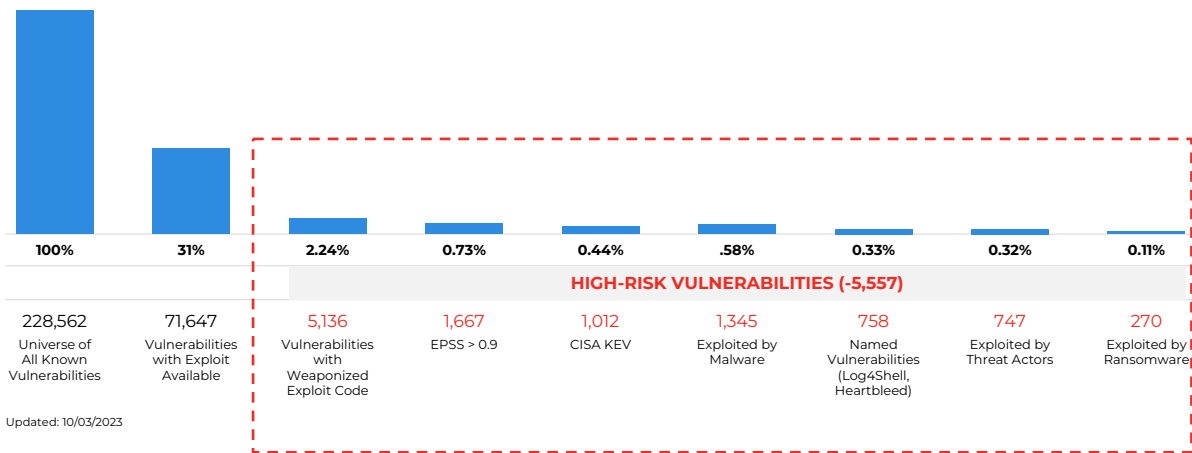
52%

Too many vulnerabilities **are rated high or critical by CVSS**

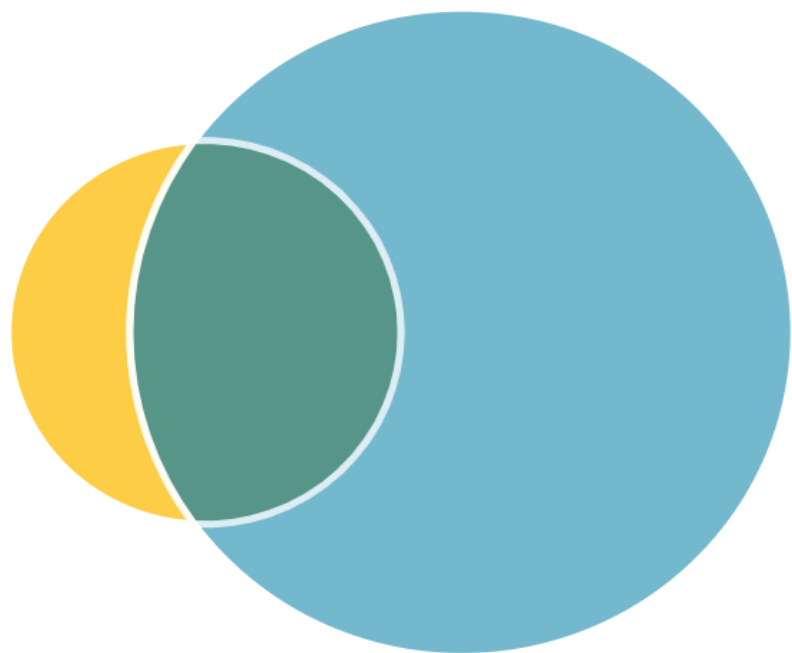


<5%

of vulnerabilities cause over **80% of risk**




# Real World Examples



QDS and CVSS Overlap

**502532**

 Qualys Detection Score

**744255**

 CVSS 3.1

**2123754**

## 2. How often do you rotate your certificates?

**90 Days**

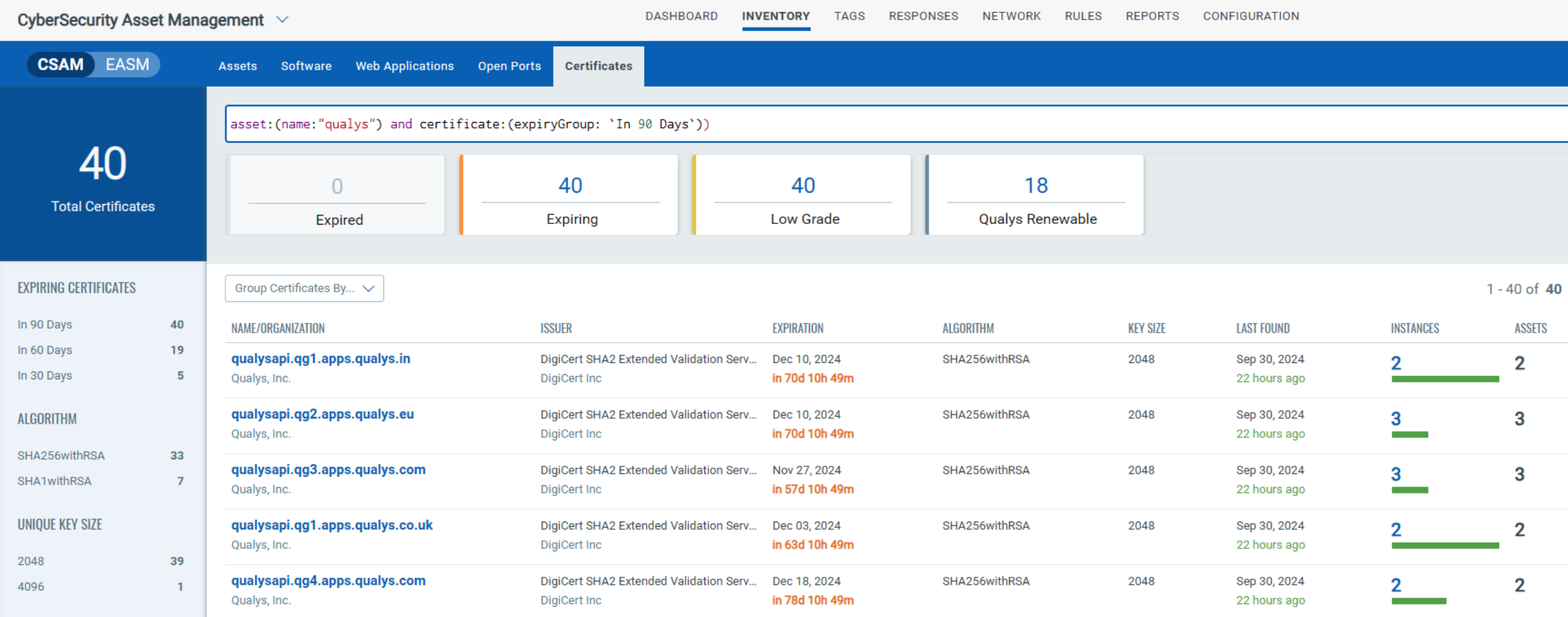
**Yearly**

**30 Days**

# Current Solution



# Certificate Management



# 3. Container, Cloud or Both?

**Cloud**

**Both**

**Containers**



# Cloud Inventory

← Asset Details: ip-172-31-0-45.eu-west-2.compute.internal

## INVENTORY

Asset Summary  
System Information  
Network Information  
Open Ports  
Installed Software  
Traffic Summary  
Business Information  
EC2 Information

## SECURITY

Vulnerabilities  
VMDB Prioritization  
EDR  
Certificates  
Secure Access Control

## COMPLIANCE

File Integrity Monitoring  
Policy Compliance

## SOURCES

Summary  
Passive Sensor  
Agent Summary  
Alert Notification

## EC2 Information

### General

Reservation ID :	r-0f54c42961d4a6ff9
Instance ID :	i-0e8258f50a903cc4f
Instance Type :	t2.medium
Created Date :	Apr 23, 2021 03:53 PM
State :	RUNNING
Spot Instance :	No
Image (AMI) ID :	ami-0cbe2951c7cd54704
Account ID :	636123215182

### EC2 Instance Tags

OS :	ubuntu2016
Purpose :	canned Demo resource - Do not delete without approval from PM
Email :	cloud-sa@qualys.com
aws:cloudformation:stack-id :	arn:aws:cloudformation:eu-west-2:636123215182:stack/test/71109dd0-a2dc-11e9-b1cb-02eeda323ec6
Department :	Product Management
aws:cloudformation:stack-name :	test
aws:cloudformation:logical-id :	MyUbuntuMachine

### Network

VPC ID :	vpc-02db160d9c0078402
DNS (Private) :	ip-172-31-0-45.eu-west-2.compute.internal
DNS (Public) :	ec2-3-8-77-85.eu-west-2.compute.amazonaws.com
Local Hostname :	ip-172-31-0-45.eu-west-2.compute.internal
MAC Address :	06:6e:e0:80:9c:5c
IP Address (Private) :	172.31.0.45
IP Address (Public) :	3.8.77.85
Group ID :	sg-08c18de643bc1ed1f
Group Name :	demo-aws-ew2-linuxsg

### Location

Region :	eu-west-2
Availability Zone :	eu-west-2a
Zone :	VPC
Subnet ID :	subnet-0fb748977ae07ce88

DE-RISK YOUR BUSINESS



# Container Inventory

36

Hosts missing Sensor

Download Sensor

1 - 47 of 47



HOST NAME	CRITICALITY ⓘ	OPERATING SYSTEM	IMAGES	CONTAINERS
<b>10.115.76.113</b> 10.115.76.113, fe80:0:0:0:b06e:f623:eabb:8bb	4	Ubuntu Linux 18.04.6	7	2
<b>10.115.76.183</b> 172.17.0.1, 10.115.76.183	4	CentOS Linux 7.6.1810	8	10
<b>10.115.67.46</b> 172.17.0.1, 192.168.122.1, 10.115.67.46	5	CentOS Linux 7.9.2009	19	28
<b>comkubernetsn</b> fe80:0:0:0:868:1fff:fe38:e8e2, fe80:0:0:0:cc3f:5eff:feb...	4	CentOS Linux 7.8.2003	12	7

# 4. Which policy guidelines do you use?

**CIS**

**None**

**NIST**

# Real World Examples

← Compliance Control

policy: "CIS Benchmark for Microsoft Windows 11 Enterprise, v1.0.0 [Automated and Manual, All Profiles] v.2.0"



1 - 50 of 1068



CID ↓	STATEMENT	INSTANCE	POLICY	POSTURE	CATEGORY	CRITICALITY
22349	<b>Status of the 'Restrict Driver Installation to Administrators' setting.</b> Last Evaluated:6 hours ago 04:41 AM	os	CIS Benchmark for Micros...	Pass	OS Security Settings	MEDIUM
22349	<b>Status of the 'Restrict Driver Installation to Administrators' setting.</b> Last Evaluated:6 hours ago 04:40 AM	os	CIS Benchmark for Micros...	Pass	OS Security Settings	MEDIUM
22344	<b>Status of the 'DoH Policy' setting.</b> Last Evaluated:6 hours ago 04:41 AM	os	CIS Benchmark for Micros...	Fail	OS Security Settings	SERIOUS
22344	<b>Status of the 'DoH Policy' setting.</b> Last Evaluated:6 hours ago 04:40 AM	os	CIS Benchmark for Micros...	Fail	OS Security Settings	SERIOUS
22185	<b>Ensure 'Enable news and interests on the taskbar' is set to 'Disabled'</b> Last Evaluated:6 hours ago 04:41 AM	os	CIS Benchmark for Micros...	Fail	OS Security Settings	SERIOUS

# Real World Examples

Control Status by Policies

View Controls (1285)

POLICY NAME	LAST EVALUATED DATE	LAST SCAN DATE	BREAK DOWN BY STATUS
ALL - CIS Benchmark for Ubuntu Linux	Jun 8, 2023	Jun 8, 2023	<div></div>
CIS Benchmark for Docker 1.13.0, v1.0.0 [Scored and Not Scored, Level 1 and Leve...	Jun 8, 2023	Jun 8, 2023	<div></div>
PCD_CIS Benchmark for Docker 1.13.0, v1.0.0 [Scored and Not Scored, Level 1 an...	Jun 8, 2023	Jun 8, 2023	<div></div>

# 5. Subscription Health Dashboard

**Yes**

**No**

# Real World Examples

← Dashboard Templates

subscription


×

All (11)

VMDR (11)

SHOWING RESULTS FOR "SUBSCRIPTION"

Qualys Subscription Health




Tracking for proper deployments, asset merging, and data correlation best practices in...

Created By: Qualys

Use template

Patch Tuesday | 2018




Annual Patch Tuesday Dashboard leveraging data in your Qualys Vulnerability...

Created By: Qualys

View Blog

Use template

Patch Tuesday | 2021




Annual Patch Tuesday Dashboard leveraging data in your Qualys Vulnerability...

Created By: Qualys

View Blog

Use template

Patch Tuesday | 2022



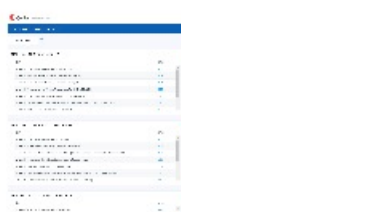
Annual Patch Tuesday Dashboard leveraging data in your Qualys Vulnerability...

Created By: Qualys

View Blog

Use template

Patch Tuesday | 2023




Annual Patch Tuesday Dashboard leveraging data in your Qualys Vulnerability...

Created By: Qualys

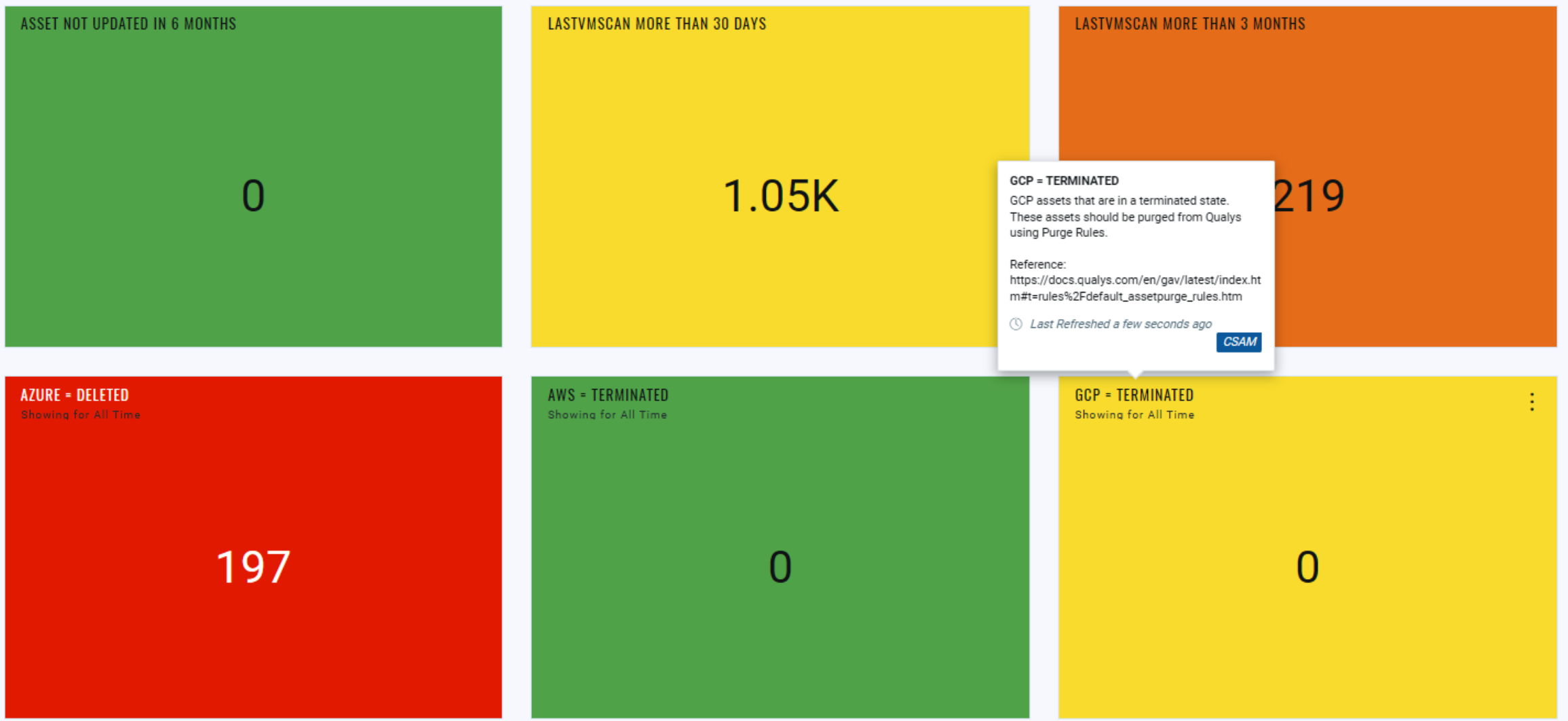
View Blog

Use template

DE-RISK YOUR BUSINESS

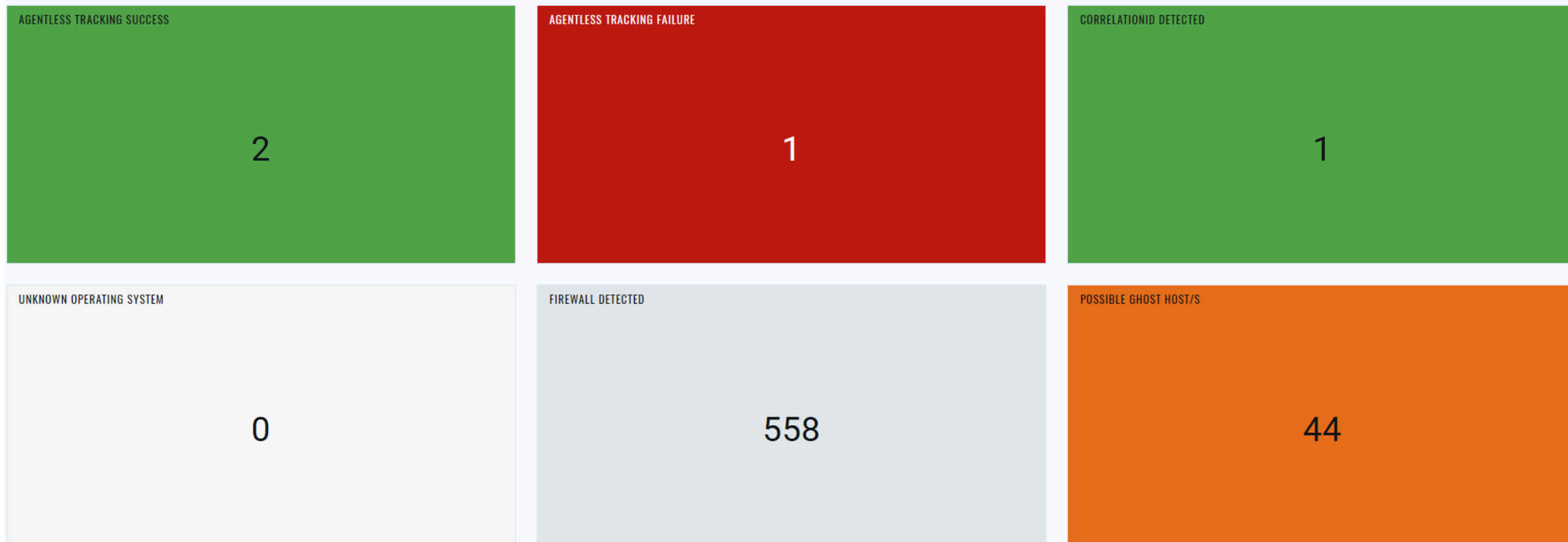


# Real World Examples





# Real World Examples



# Qualys Scorecard



<https://www.qualys.com/vmdr-scorecard/>

# Qualys Scorecard



<https://www.qualys.com/vmdr-scorecard/>



Qualys®