Marek Skalický, CISM, CRISC
Managing Director for CEE and Turkey

Everything visible. Everything secure.

- ICT Asset & Posture Visibility
- High Data Accuracy
- Full Scale Data Collection
- Continuity and Immediacy
- Transparent-Orchestration

1+ trillion
Security Events

3+ billion
IP Scans/Audits a Year

On Premise & Virtualized

Endpoints & Mobile

Public & Private Clouds

Qualys.

Qualys Security Cloud Platform

Architecture

Integrated Suite of Applications

CA | AI | VM | CM | TP | FIM | PC | PCI | SAQ | IOC | WAS | WAF

Analytics and Reporting Engines

kafka | ceph | elastic | cassandra | redis | Flink | Microservices

Distributed Sensors

Hardware | Virtual | Cloud | Agent | Passive | API

Qualys.

Qualys Sensors

Scalable, self-updating & centrally managed

Physical

Legacy data centers

Corporate infrastructure

Continuous security and compliance scanning

Virtual

Private cloud infrastructure

Virtualized Infrastructure

Continuous security and compliance scanning

Cloud/Container

Commercial IaaS & PaaS clouds

Pre-certified in market place

Fully automated with API orchestration

Continuous security and compliance scanning

Cloud Agents

Light weight, multi-platform

On premise, elastic cloud & endpoints

Real-time data collection

Continuous evaluation on platform for security and compliance

Passive

Passively sniff on network

Real-time device discovery & identification

Identification of APT network traffic

Extract malware files from network for analysis

API

Integration with Threat Intel feeds

CMDB Integration

Log connectors

ServiceDesk and Ticketing Integrations

Agentless + Agent Based + Passive

Qualys.

Qualys Cloud Agent Platform

Lightweight agent (3 MB) for on premise servers, dynamic cloud environments and mobile endpoints

Secure scalable architecture for millions of devices Centrally managed, self updating

Architecture for IoT device security and compliance with SDK

Qualys Integrated Cloud Apps

ASSET MANAGEMENT

AI — Asset Inventory
Maintain full, instant visibility of all your global IT assets

SYN — CMDB Sync
Synchronize asset information from Qualys into ServiceNow CMDB

CI — Cloud Inventory
Inventory of all your cloud assets across AWS, Azure, GCP and others

CRI — Certificate Inventory
Inventory of TLS/SSL digital certificates on a global scale

IT SECURITY

VM — Vulnerability Management
Continuously detect and protect against attacks, anytime, anywhere

TP — Threat Protection
Pinpoint your most critical threats and prioritize patching

IOC — Indication of Compromise
Continuously monitor endpoints to detect suspicious activity

CRA — Certificate Assessment
Assess all your digital certificates for TLS/SSL vulnerabilities

CM — Continuous Monitoring
Alerts you in real time about network irregularities

CS — Container Security
Discover, track, and continuously protect containers

PM — Patch Management (Beta in Sept)
Select, manage, and deploy patches to remediate vulnerabilities

COMPLIANCE MONITORING

PC — Policy Compliance
Assess security configurations of IT systems throughout network

PCI — PCI Compliance
Automate, simplify and attain PCI compliance quickly

FIM — File Integrity Monitoring
Log and track file changes across global IT systems

CSA — Cloud Security Assessment
Get full visibility and control across all public cloud instances

SCA — Security Configuration Assessment
Automate configuration assessment of global IT assets

SAQ — Security Assessment Questionnaire
Minimize the risk of doing business with vendors and other third parties

WEB APPLICATION SECURITY

WAS — Web Application Scanning
Secure web applications with end-to-end protection

WAF — Web Application Firewall
Block attacks and virtually patch web application vulnerabilities

Qualys.

Qualys Global IT Asset Inventory

Source of truth for IT assets

Discover all assets in global, hybrid infrastructure

Asset information is normalized and categorized for hardware and software

Enriched with metadata and indexed for 2-second visibility

Qualys.

Inventory

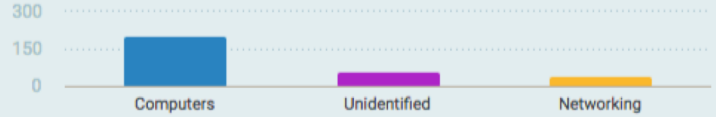
Assets | Software

275
Total Assets

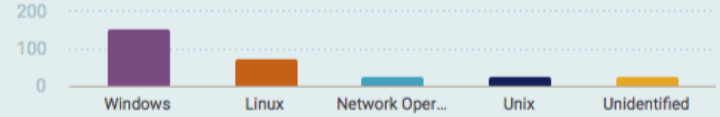
Search for assets

Last 30 Days ▼

TOP HARDWARE CATEGORIES



TOP OPERATING SYSTEMS CATEGORIES



MANUFACTURER

Dell	67
Lenovo	56
Unidentified	47
IBM	41
HP	36
Cisco Systems	22
Juniper Networks	4
Apple	2

Show less

TAGS

Cloud Agent	239
AGENT_TARGETS	58
fullscan-iplist	35
pod 11 agents	25
All CISCO devices	19

Group Assets by... ▼

1 - 50 of **275**

ASSET	OPERATING SYSTEM	HARDWARE	LAST USER	INVENTORY	TAGS
itam-qrhel6sp-62-140	Red Hat Enterprise Linux 6 Server 6.0	Unidentified	root	Source: QAGENT Updated: Apr 13 2018	Cloud Agent 1 more...
itam-2k12r2dp	Microsoft Windows Server 2012 R2 Datacenter 6.3	VMware, Inc. VMware V...	administrator	Source: QAGENT Updated: Apr 13 2018	Cloud Agent 1 more...
itam-mssql2016	Microsoft Windows Server 2016 Standard 10.0	VMware, Inc. VMware V...	.\Administrator	Source: QAGENT Updated: Apr 13 2018	ITAM 1 more...
itam-centos66	The CentOS Project CentOS 6 6.6	Unidentified	root	Source: QAGENT Updated: Apr 13 2018	ITAM 1 more...
zgs-33213.com	Canonical Ubuntu Precise Pangolin	VMware, Inc. VMware V...		Source: QAGENT	Cloud Agent

Qualys Passive Network Discovery

Eliminate blind spots. Identify and profile devices as soon as they connect to the network.

Continuously augment inventory with additional details, in near-real time.

Extends discovery, for sensitive systems that may not be suited for active probing or agent.

Continuously discover and profile every device with network activity

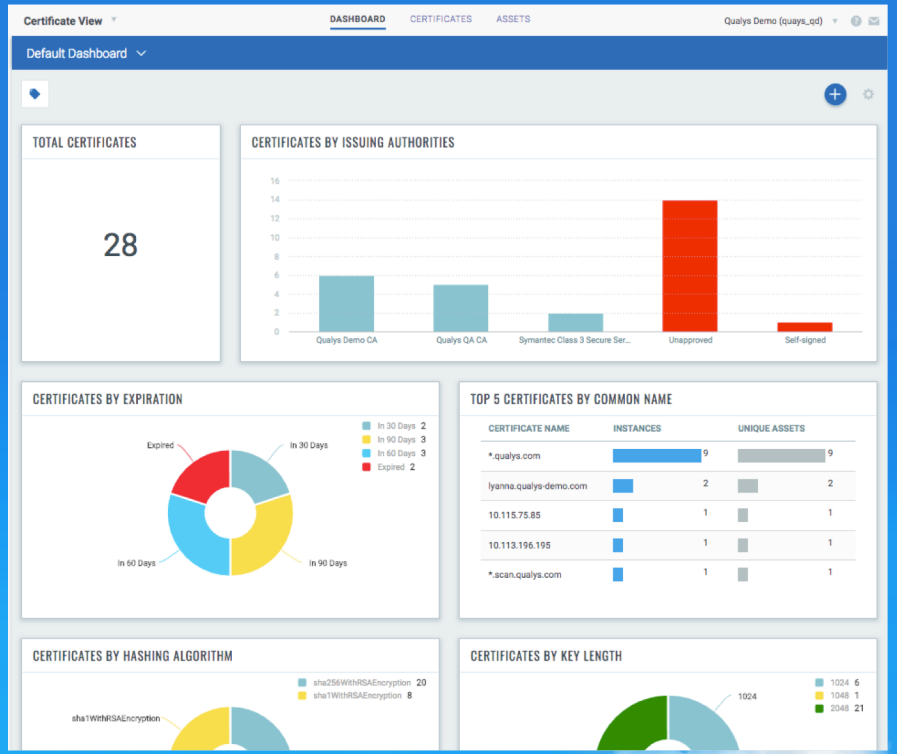
Qualys Certificate View

Discover, inventory, monitor certificates

Discover, inventory, monitor host configurations & vulnerabilities

Vulnerability analysis & grading (host/port/service/certificate)

Coverage across both on-premise and cloud environments

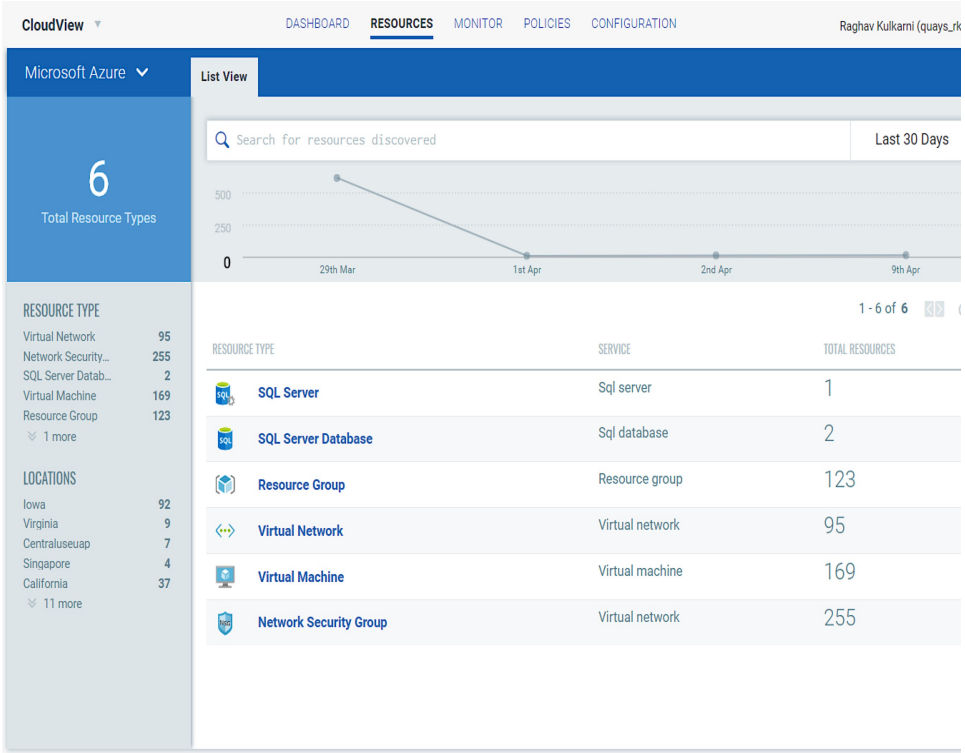


Qualys.

Qualys CloudView

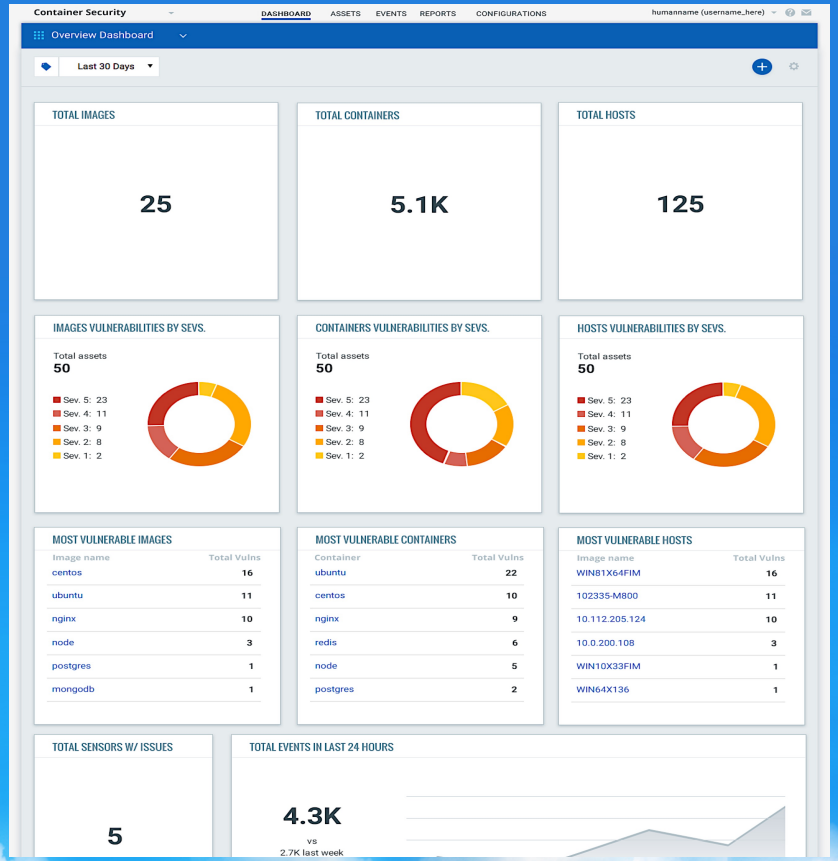
Cloud Inventory + Cloud Security Assessment = CloudView

Unparalleled Visibility and Continuous Security Monitoring across public cloud infrastructure



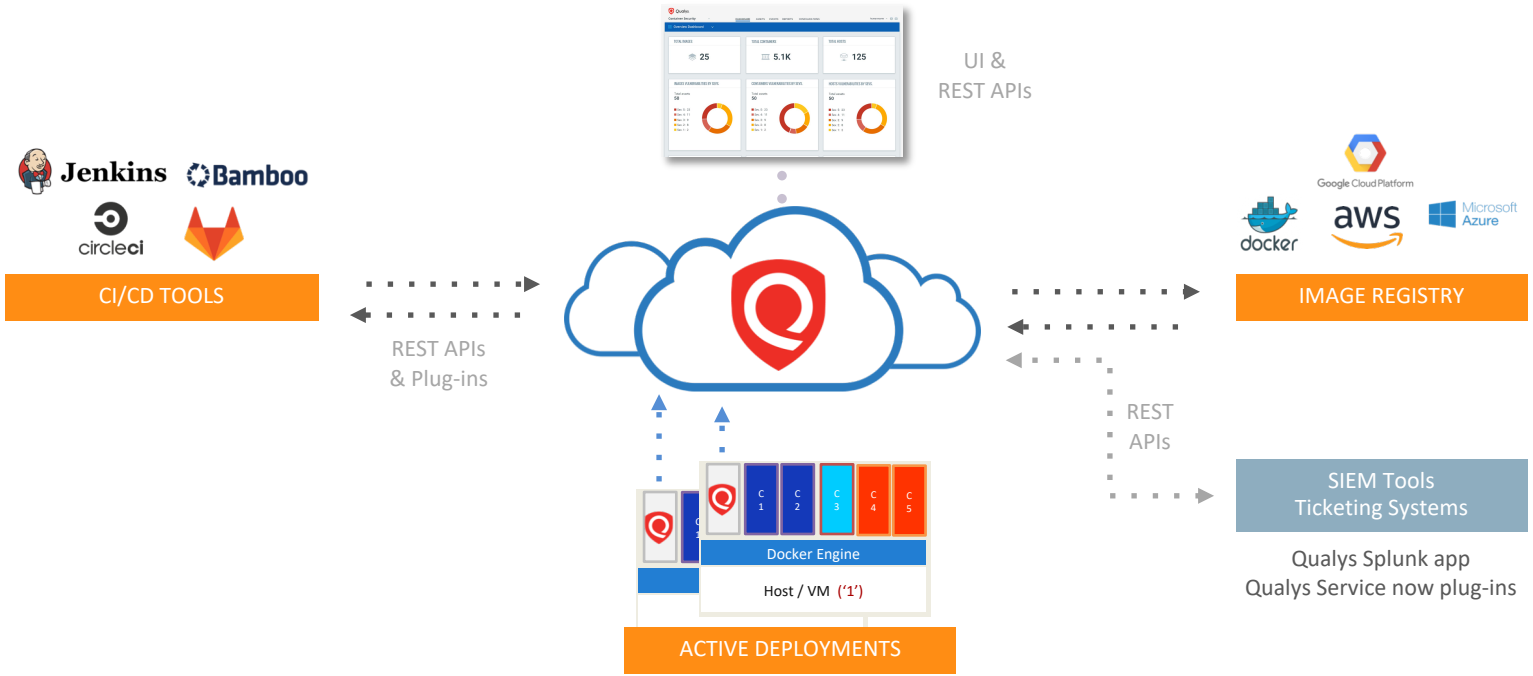
Qualys Container Security

- Container Discovery and Inventory
- CI/CD pipeline Integration with Jenkins
- Assess Container Images
- Monitor running containers
- Block vulnerable images from being promoted
- Track drift of containers from images



Qualys Container Security

Functional Overview



Qualys.

Qualys Web Application Security

Large-scale dynamic scanning (DAST)

Detection of OWASP TOP10 Vulns

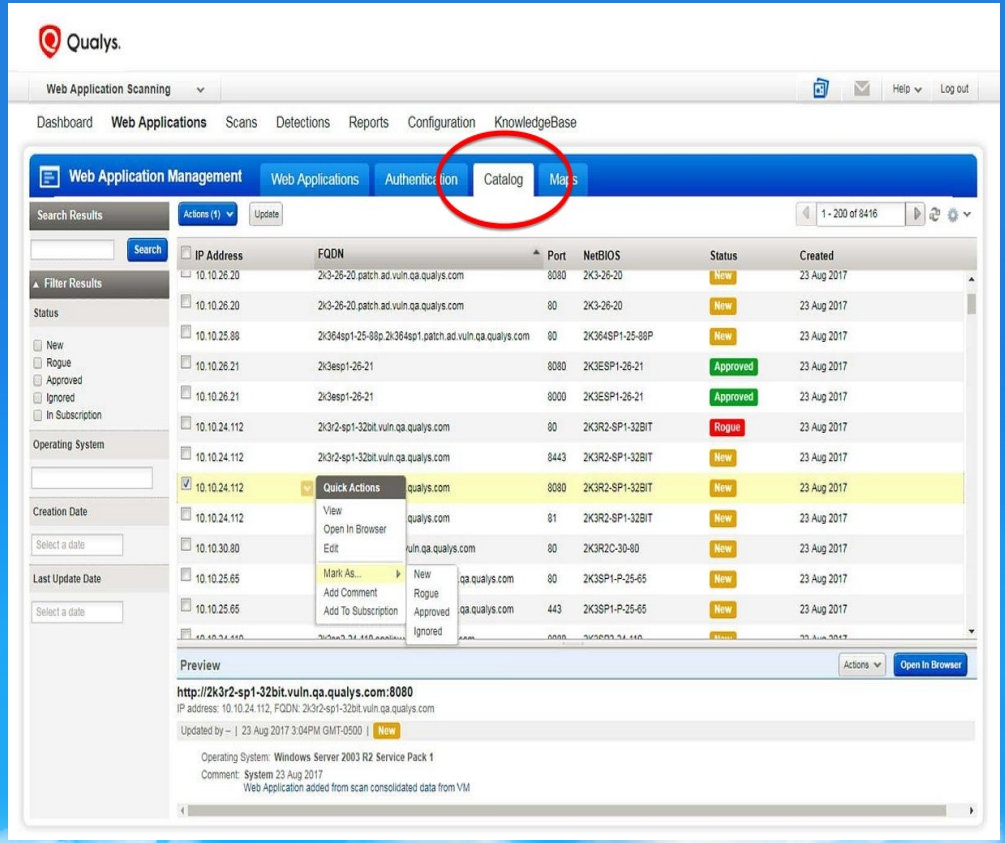
Public-facing and Internal apps scanned

Automated Web App Catalog

Sophisticated scheduling capabilities

Authentication for deep scanning

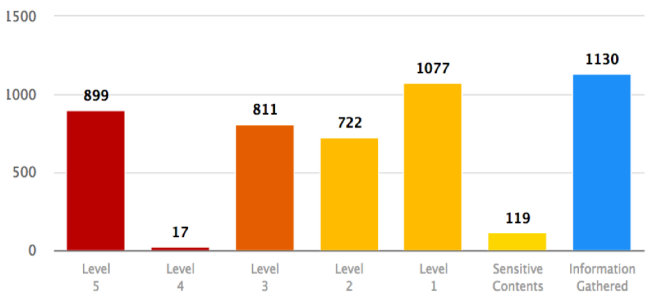
Malware Detection for public websites



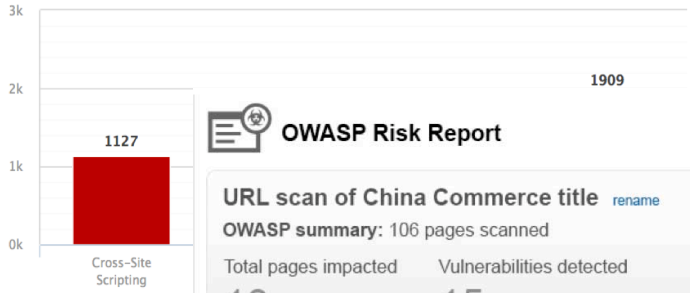
Summary

Security Risk	Web Applications	Vulnerabilities
HIGH	87	3526

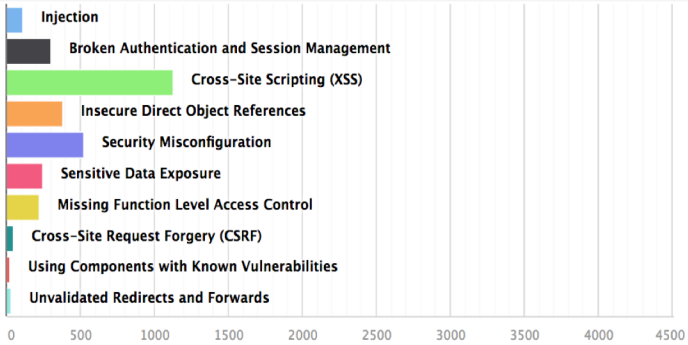
Findings by Severity



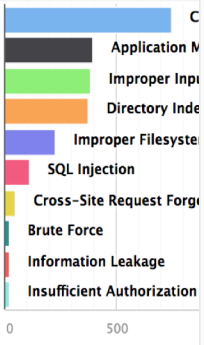
Vulnerabilities by Group



OWASP Top 10 2013 Vulnerabilities



WASC Top 10 Vulnerabilities



OWASP Risk Report

URL scan of China Commerce title rename

OWASP summary: 106 pages scanned

http://www.

December 25, 20

DNS Hostname:

NetBIOS Hostname: VS-W

Operating System: Wi

Total pages impacted	Vulnerabilities detected
10	15

Risk percentage by scanned pages

106 Pages scanned

Impacted pages: 10 (9.33%)

Vulnerability by severity level

15 Vulnerabilities

Level 5: 6 (40.40%)

Level 4: 3 (22.33%)

Level 3: 2 (14.25%)

Level 2: 3 (13.33%)

Level 1: 1 (10.33%)

Categories

A-1 Injection — 4 Pages | 12 Vulns

Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusteddata is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.

A-2 Cross-Site Scripting (XSS) — 6 Pages | 3 Vulns

XSS flaws occur whenever an application takes untrusteddata and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Category A-2: Cross-Site Scripting (XSS)

4 Impacted pages

http://www.mwtest.info/malware-demos-named/Killbits/Killbits.htm

QID: 10577 View details

Microsoft October 2010 Security Update: 16 bulletins, 49 vulnerabilitie

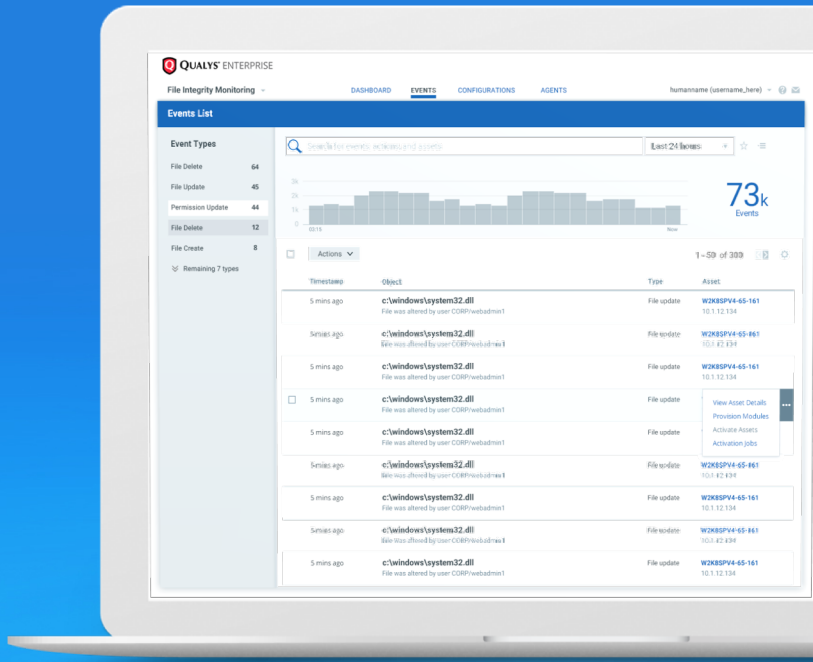
QID: 10906 View details

PHPBB2 ViewTopic.PHP Cross Site Scripting Vulnerability

http://www.mwtest.info/malware-demos-named/MS07-004/MS07-004

Qualys File Integrity Monitoring

- Real-time detection
- Built on the Qualys Cloud Agent
- Easy to install, configure and manage
- No expensive infrastructure to deploy



Qualys.

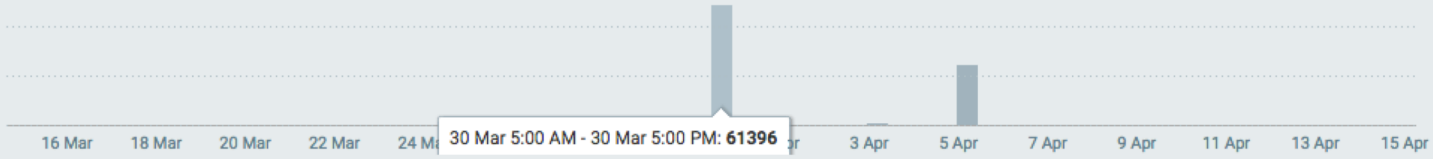
Events

All Events | Event Review | Ignored

98.7K
Total Events

profile.name:"Windows Agent"

Last 30 Days



EVENT ACTION

Delete	31.5K
Attributes	23.3K
Create	22.0K
Content	15.8K
Rename	4.63K
1 more	

USER

NT AUTHORITY\...	93.1K
MSEDGEWIN10\I...	3.59K
NT AUTHORITY\...	1.98K
NT AUTHORITY\...	36
MSEDGEWIN10\...	4

PROCESS

Sychost Exe 40.8K

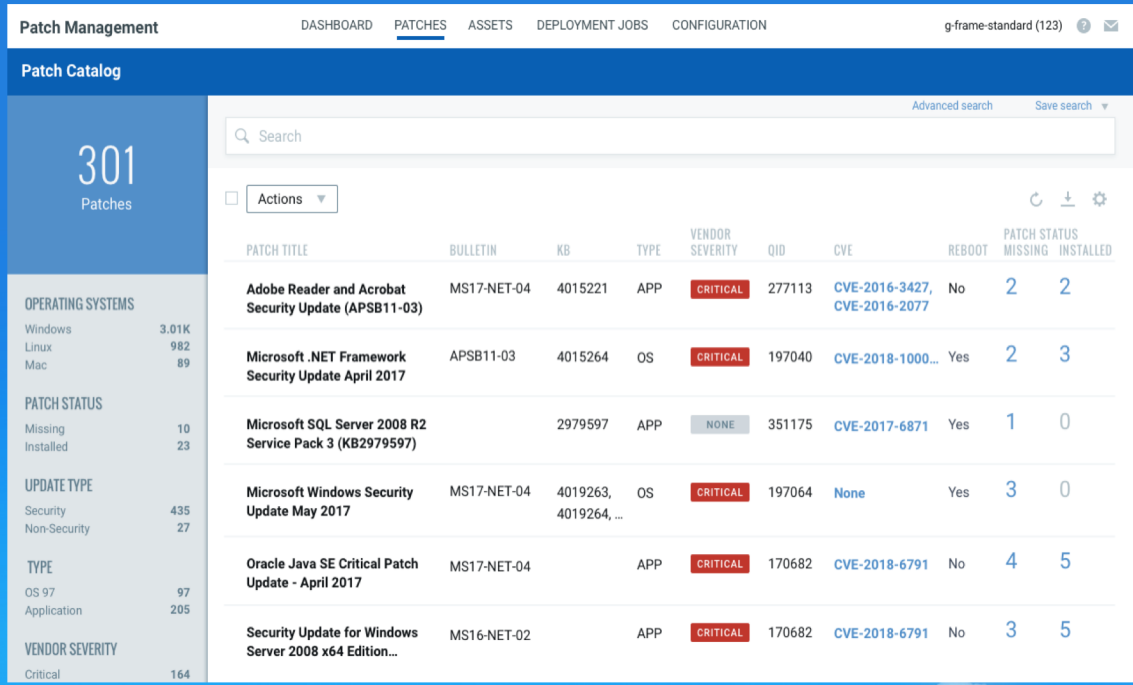
Actions (0)

1 - 50 of **98749**

TIME	TARGET	ACTION	ACTOR	HOST	SEVERITY
9 days ago 11:13:46 PM	**sentinel.tmp** \Device\HarddiskVolume1\ProgramData\Qualys\Qual...	Delete	NT AUTHOR...	**MSEDGEWIN10** fe80:0:0:0:c42a:e...	
9 days ago 11:13:46 PM	**165721.qeb** \Device\HarddiskVolume1\ProgramData\Qualys\Qual...	Content	NT AUTHOR...	**MSEDGEWIN10** fe80:0:0:0:c42a:e...	
9 days ago 11:13:46 PM	**sentinel.tmp** \Device\HarddiskVolume1\ProgramData\Qualys\Qual...	Create	NT AUTHOR...	**MSEDGEWIN10** fe80:0:0:0:c42a:e...	
9 days ago 11:13:46 PM	**164445.qeb** \Device\HarddiskVolume1\ProgramData\Qualys\Qual...	Delete	NT AUTHOR...	**MSEDGEWIN10** fe80:0:0:0:c42a:e...	
9 days ago 11:13:46 PM	**165721.qeb** \Device\HarddiskVolume1\ProgramData\Qualys\Qual...	Create	NT AUTHOR...	**MSEDGEWIN10** fe80:0:0:0:c42a:e...	

Qualys Patch Management

- Discover missing patches on assets
- Correlate with vulnerabilities
- Prioritize with Threat Protection
- Create Patching Policies / Profiles
- Deploy patches to Windows, Mac, and Linux OS in one platform - anywhere



Qualys.

Qualys Mobile Security Platform

1Mobility company Acquisition

Cloud Agents on iOS, Android & Windows Mobile

EMM (Enterprise Mobility Management)

Realtime Asset Inventory

AV, VM, PC & Threat detection

Policy enforcement

Beta Q1 2019

Qualys

New UX Transformation

Intuitive Easy Navigation with least steps.

Focused Interactive Workflows with feedback.

Mobile device accessibility built-in.

Desktop

Mobile

Thank You

mskalicky@qualys.com