Qualys CISA Shields Up Guidance Playbook

March 30, 2022

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Qualys CISA Shields Up Guidance Playbook

Since the CISA launched Shields Up, the Qualys team has analyzed how customers can strengthen their security posture and meet CISA's recommendations.
Recognizing the heightened threats to the global digital world, the Qualys Security and Engineering teams have rigorously and vigilantly worked on vulnerability management solutions that mitigate this amplified threat environment's potential and baneful risks. We have implemented additional security, monitoring, and governance measures involving our senior leadership and are committed to ensuring that the Qualys Cloud Platform remains available and secure to support the enterprises we serve worldwide.

Read more about understanding and mitigating Cyber threats in our blogs:
Ukrainian Targets Hit by HermeticWiper, New Datawiper Malware

Russia-Ukraine Crisis: How to Strengthen Your Security Posture to Protect against Cyber Attack, based on CISA Guidelines

Refer Qualys blogs to know more about strengthening your defenses consistent with CISA Shields Up guidelines and Qualys Documentation to set up and configure Qualys apps.

Let's Get Started

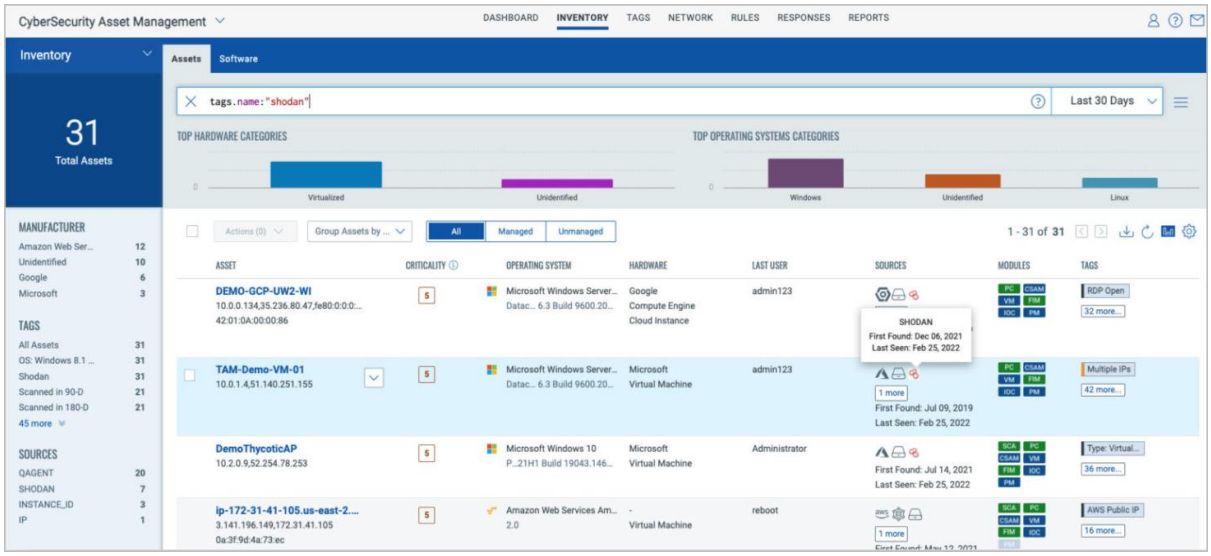
Based on the high-level guidelines introduced by CISA concerning data security and governance measures, Qualys recommends the following concrete steps to be practiced safeguarding critical assets and networks.

According to CISA's Shields Up guidelines, there are four measures to strengthen security posture:
Step 1: Know Your Shodan/Internet Exposed Assets Automatically
Step 2: Detect, Prioritize, and Remediate CISA's Catalog of Known Exploited Vulnerabilities
Step 3: Protect Your Cloud Services and Office 365 Environment
Step 4: Continuously Detect a Potential Intrusion

Step 1: Know Your Shodan/Internet Exposed Assets Automatically

Discover and protect your external facing assets

Qualys Cybersecurity Asset Management (CSAM) revolutionized asset management for security teams. With Qualys CSAM, organizations can detect security gaps like unauthorized or EOL software and respond with appropriate actions to mitigate risk, thus reducing the 'threat debt.'



Step 1.1 - Deploy and Setup Cloud Agent

You can start developing your inventory by installing cloud agents. Navigate to the Home page and click the Download Cloud Agent button from the Discovery and Inventory tab. Refer to the following documentation to get started with Cloud Agent.

Install Qualys Cloud Agents | Cloud Agent Getting Started Guide | Cloud Agent Onboarding Videos

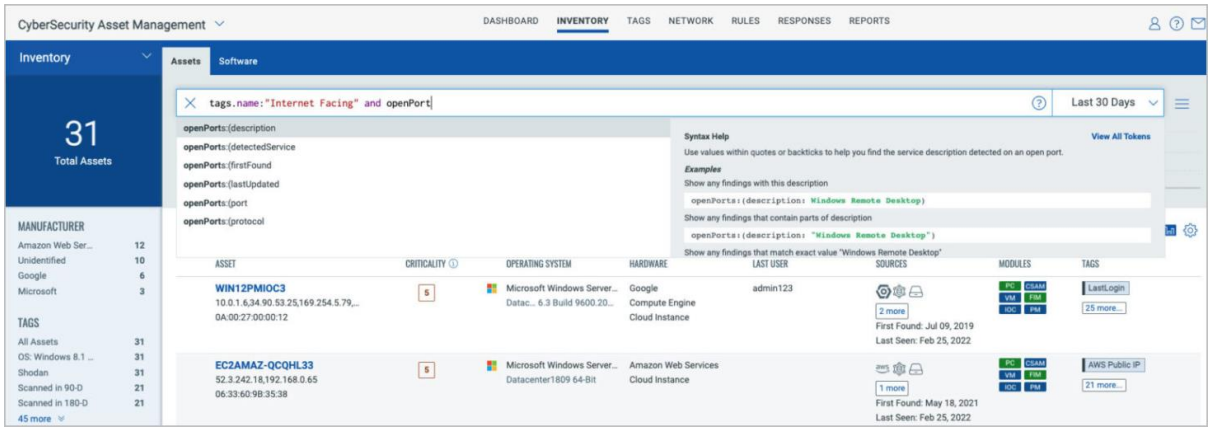
Step 1.2 - Detect at-risk Assets & Applications

CSAM enriches your asset inventory with in-context, relevant information to help you detect at-risk assets and applications. Please use the following QQL to import assets from Shodan to your inventory.

Query: tags:(name: “shodan”)

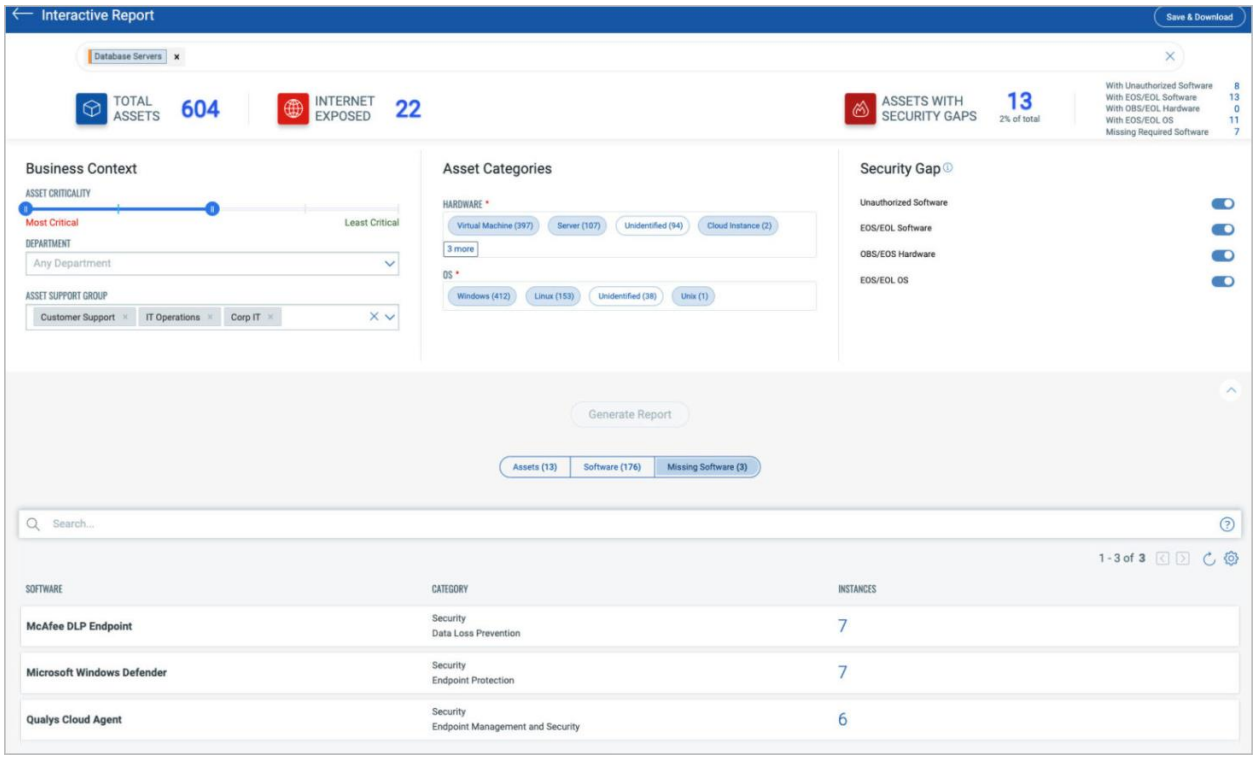
Detect and disable all non-essential ports and protocols, especially on internet exposed assets

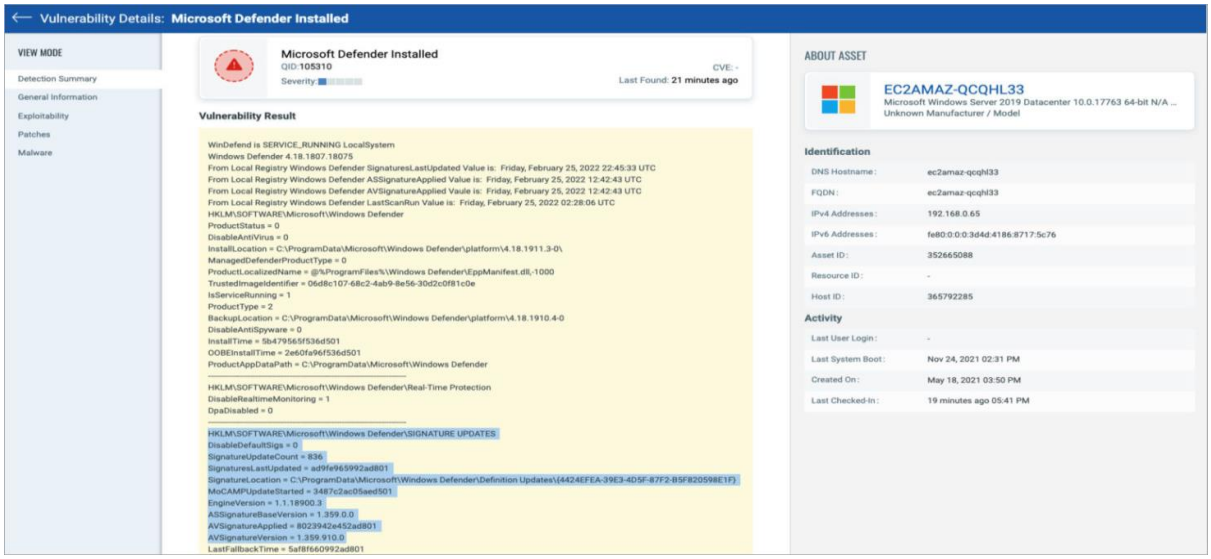
Qualys CSAM supports extensive query language that renders valuable insights to act responsibly towards remediation (for example, Windows Remote Desktop). This aids IT teams in detecting and disabling any non-essential ports and protocols, particularly on web-exposed assets that may be running a remote-control service.



Ensure all systems are protected with up-to-date antivirus/anti-malware software

Identify assets in your inventory that are lacking antivirus or have out-of-date signatures. CSAM allows you to define software rules and required software can be assigned to a particular set of assets or environment. For example, antivirus and a data loss protection agent should be installed on all database servers.



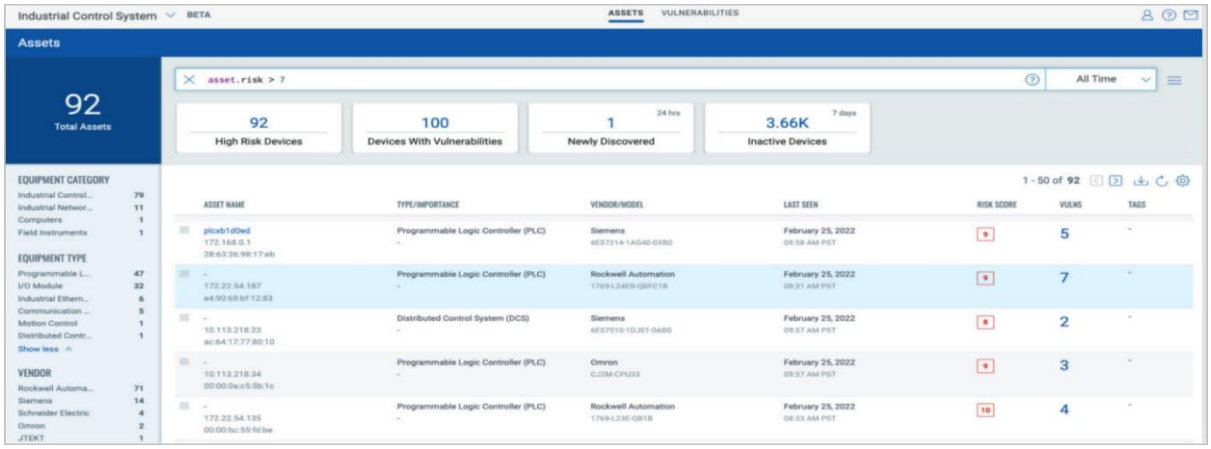


Qualys Multi-Vector EDR with Integrated Anti-Malware is enabled wherever the Qualys Cloud Agent is installed for immediate threat protection from devices missing antivirus or anti-malware.
In addition to essential anti-malware protection, Multi-Vector EDR automatically discovers and classifies all IT assets, including endpoints using multiple Qualys sensors. It identifies malicious activity that usually bypasses traditional antivirus such as Living-off-the-Land attacks and MITRE ATT&CK tactics and techniques.

Refer to the following documentation to get started with CSAM.
CSAM Videos | CSAM Getting Started Guide | CSAM Online Help

Monitor Industrial Control Systems and Operational Technology

The acceleration of Digital transformation has enabled systems like Industrial Control Systems (ICS) and Network segmentation to connect with corporate networks like Industrial IoT platforms and device platforms.
With Qualys Industrial Control Security (ICS), you can gain complete insight into your critical infrastructure, network connections, and vulnerabilities. ICS is currently beta. Reach out to your Technical Account Manager for more information.



Step 2 - Detect, Prioritize and Remediate CISA's Catalog of Known Exploited Vulnerabilities

Qualys Researcher analyzed all the 300+ CVEs from CISA known exploited vulnerabilities and mapped them to the Qualys QIDs. In VMDR, a new "CISA Exploited" RTI is added to assist customers in creating vulnerability reports that focus on CISA exploited vulnerabilities.

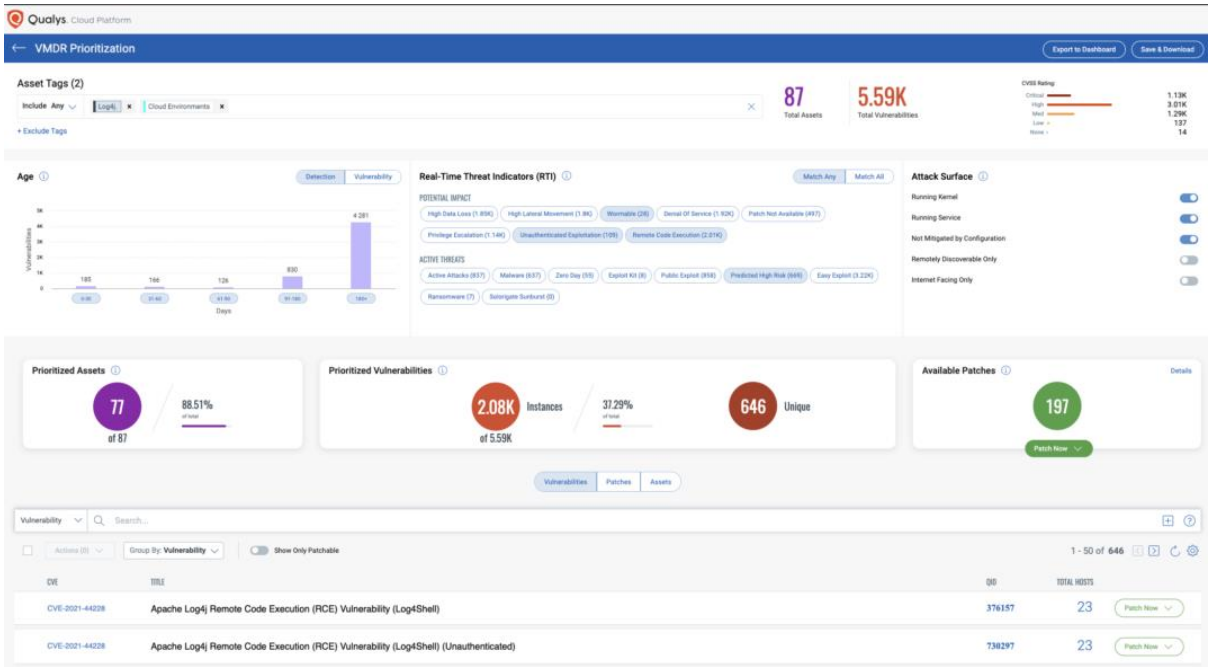
Step 2.1 Detect the vulnerability

Using VMDR, the vulnerabilities can be prioritized using the following real-time threat indicators (RTIs):

- Predicted_High_Risk
- Wormable
- Remote_Code_Eecution
- Unauthenticated_Exploitation
- CISA Exploited

Step 2.2 Generate Prioritization Report

Navigate to the VMDR > Prioritization tab and select all the necessary asset tags. Then choose the CISA Exploited RTI and generate the report.



Refer to the following docs to get started with VMDR
VMDR Onboarding Videos | VMDR Getting Started Guide | VMDR Online Help

Remediate CISA recommended catalog of exploited vulnerabilities

Qualys Patch Management links "CISA Exploited" vulnerabilities found in the environment with the necessary patches for remediation, allowing users to obtain fixes without having to go through the VPN.

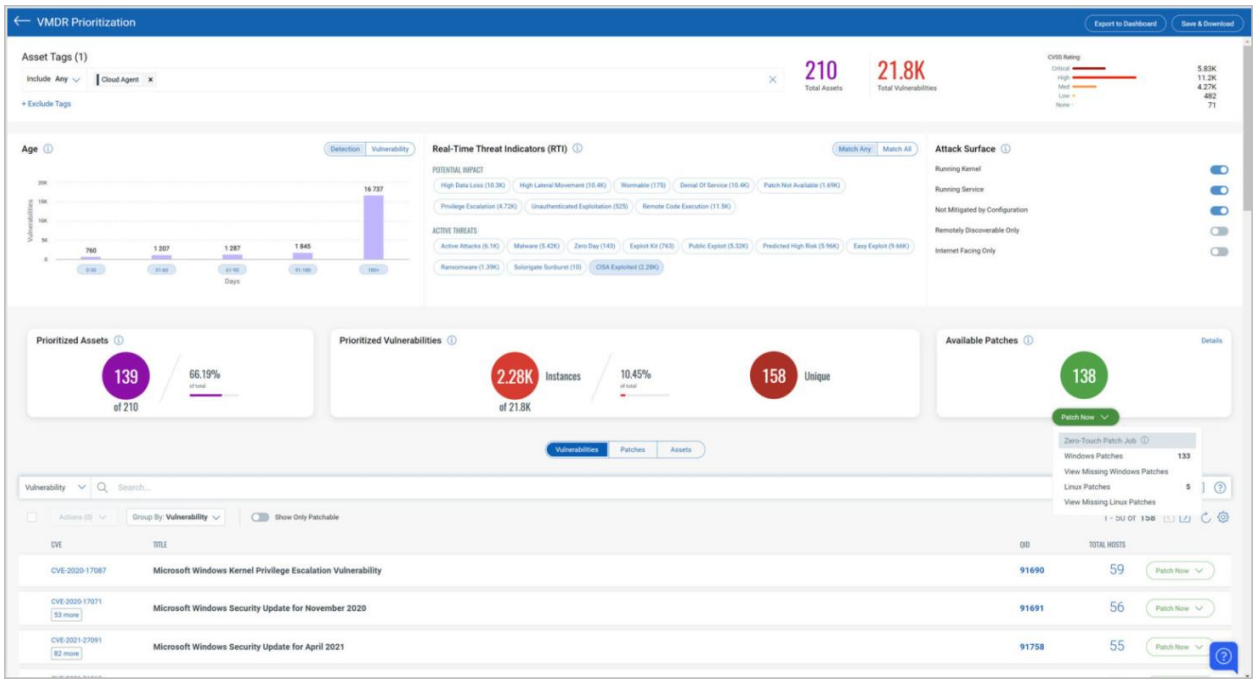
Step 2.1 – Create Patch Jobs

Patch jobs may be created using either the Patch Management app or your VMDR prioritization report.

Navigate to Patch Management > Jobs and create a Deployment Job. Follow the wizard to create and deploy the job. Refer to Deploying Patch Jobs on Assets.

Step 2.2– Use VMDR to create Patch Jobs

Select the vulnerabilities you want to fix in the VMDR Prioritization Report and add them to a new job. Qualys will automatically map all the identified vulnerabilities to the patches that remediate those vulnerabilities.



Refer to the following resources to get started with Patch Management

Deploying Patch Jobs on Assets | Patch Management Getting Started Guide | Patch Management Videos

Step 3: Protect Your Cloud Services and Office 365

As noted by CISA, the leading attack vector for breaches are misconfiguration of cloud services and SaaS applications like Office 365.

Detect and Remediate Public Cloud Infrastructure Misconfigurations

Protect your public cloud infrastructure by securing the following on priority:

- IAM: Ensure all users are MFA enabled and rotate all access keys older than 30 days. Verify that all service accounts are valid (i.e., in use) and have the minimum privilege.
- Audit Logs: Turn on access logging for all cloud management events and for critical services (e.g., S3, RDS, etc.)
- Public-facing assets: Validate that the firewall rules for public-facing assets allow only the needed ports.

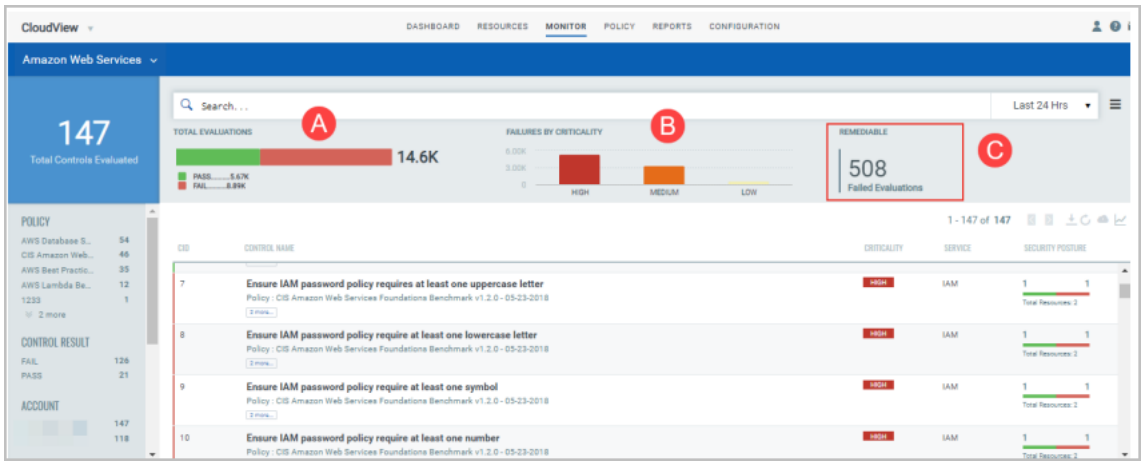
Step 3.1. Configure Connectors for Remediation

Configuring connections for remediation consists of two steps: enabling remediation and assigning write access to the connector.
From the Configuration > Cloud Provider tab, select a connector. Then from the Quick Actions menu, select Enable, to enable the connector.

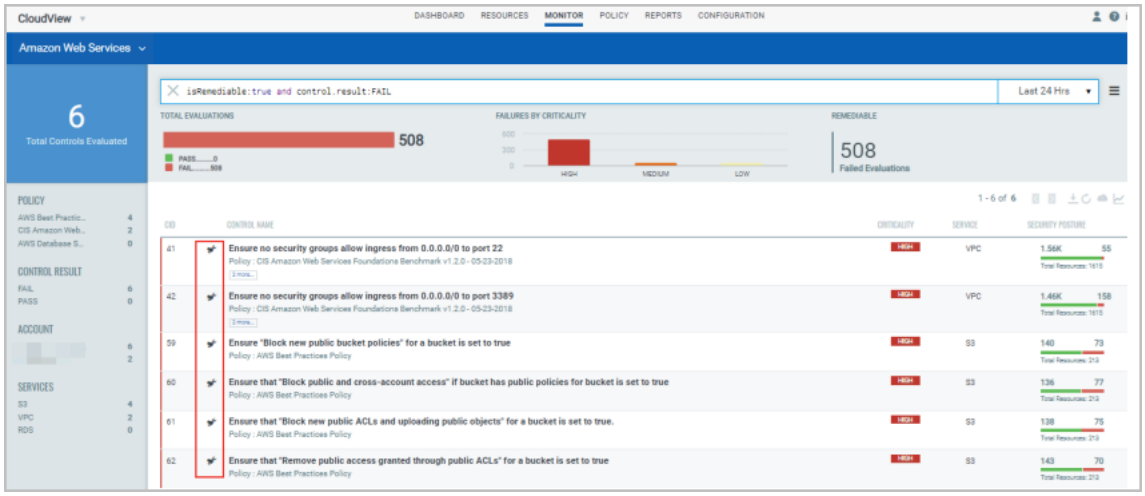
The detailed steps for each cloud provider:
Configure Remediation for New Connectors: AWS
Configure Remediation: Microsoft Azure
Configure Remediation: GCP

Step 3.2. Remediating Cloud Resources

The Cloud posture subtab enlists the available controls for remediation and the count of failed evaluations that could be remediated. With remediation enabled, you can filter out controls with failed evaluations that can be remediated.
In CloudView, navigate to the Monitor > Cloud Posture tab. Select a cloud provider and you can enter your query in the search box.

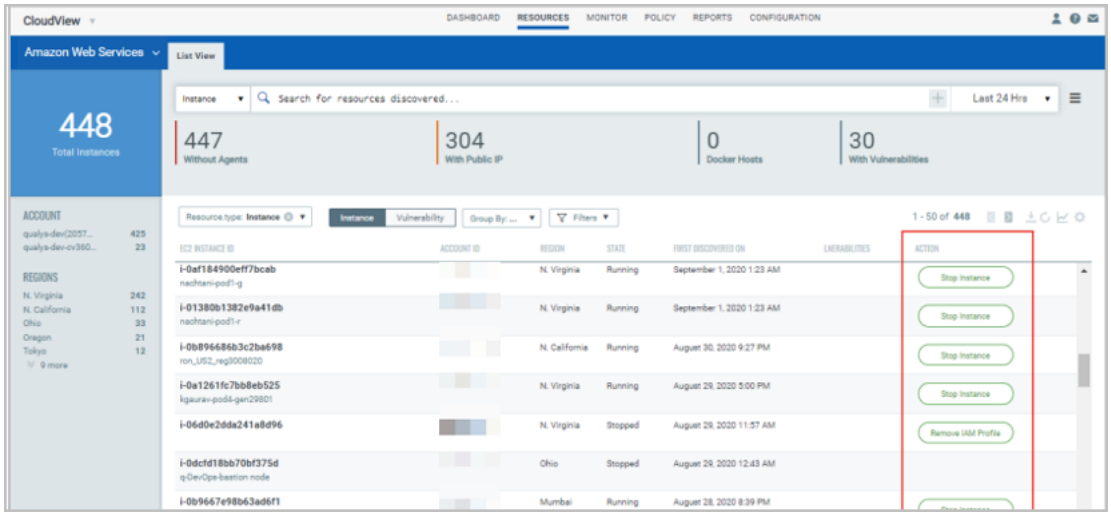


The “ ” icon indicates that these controls are available for remediation. Click on one of the controls to proceed with Remediation.



Step 3.3. Actions for Cloud Resources

The Resources tab offers you with actions that you can execute on instances to quickly fix unknown behaviour of an instance or vulnerability on an instance.
In CloudView, navigate to the Monitor > Cloud Posture tab. Select a cloud provider and you can enter your query in the search box.



Refer to the following resources to get started with CloudView
CloudView Online Help | CloudView Getting Started Guide | CloudView videos

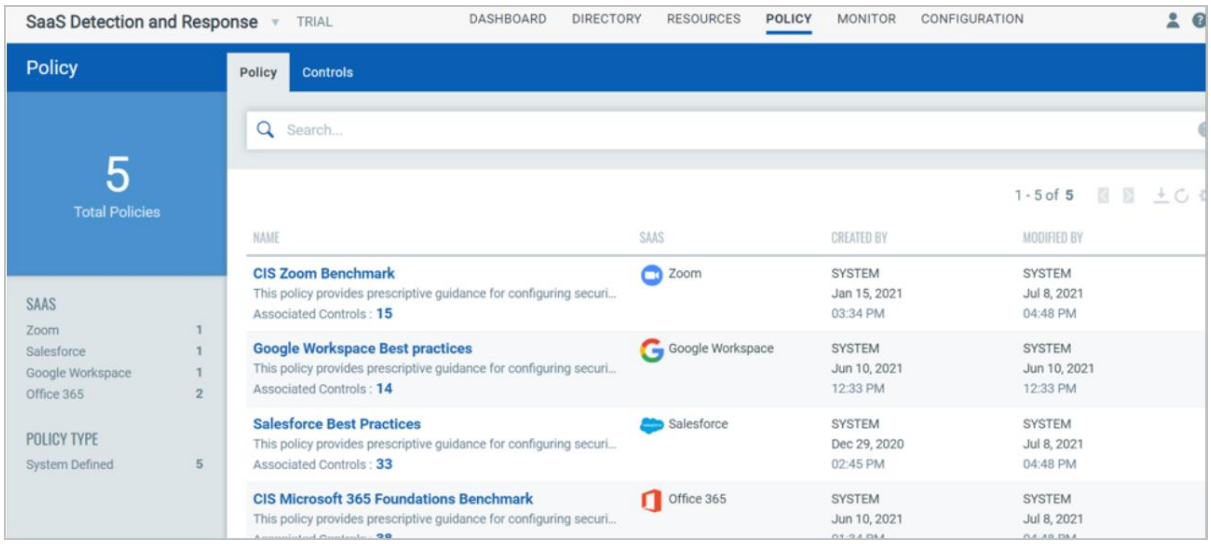
Protect your Office 365 and Other SaaS Services

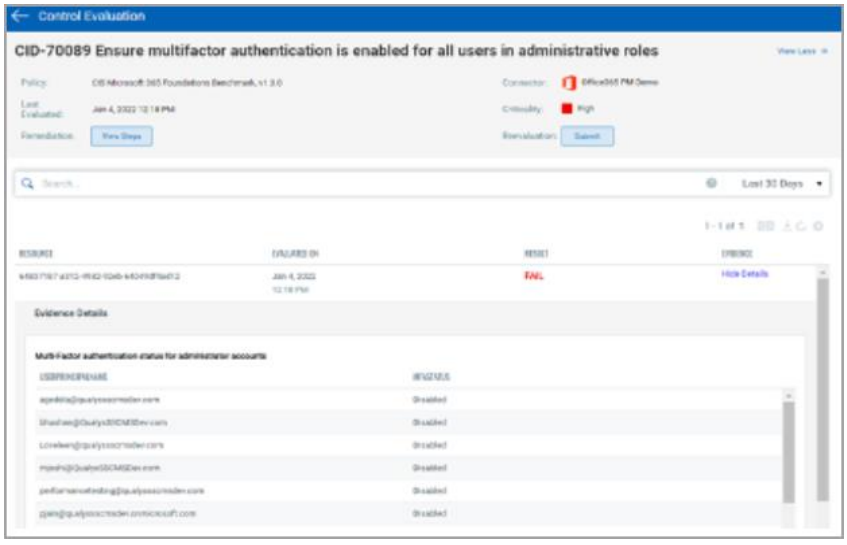
Qualys SaaSDR allows for continuous security posture evaluation of Office 365 via the CIS (Center for Internet Security) (Center for Internet Security) certified Office policy and automatic security configuration assessment for Zoom, Salesforce, and Google Workspace.

Step 3.1 Enable policy for connector

You can also enable/disable the policy by following the navigation steps-

- Click on the policy to open it in the View Mode.
- Navigate to the Connectors tab.
- Select a connector and from the Actions menu, enable or disable the policy for this connector.

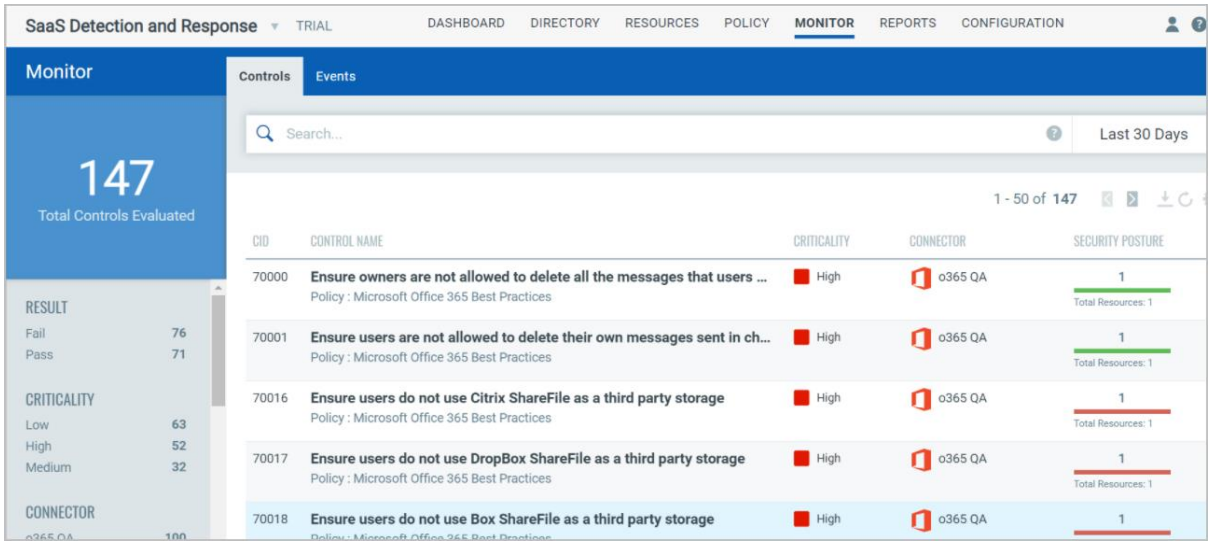




Once a policy is enabled for a connector, you can view your compliance posture in the Monitor tab.

Step 3.2 Monitor Compliance Posture

You can also monitor compliance posture for each connector from the Monitor tab.



From the Security Posture column, you can drill down to view details of each control and their pass or fail status.

Refer to the following resources to get started with SaaSDR

SaaSDR Online Help | SaaSDR Getting Started Guide

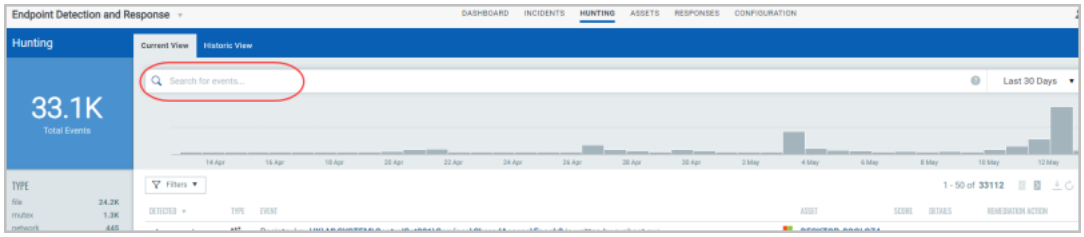
Step 4: Continuously Detect any Potential Threats and Attacks

With Qualys Multi-Vector EDR, customers can detect Indicators of Compromise (IOC) and MITRE ATT&CK Tactics & Techniques provided by CISA and respond quickly to mitigate the risk.

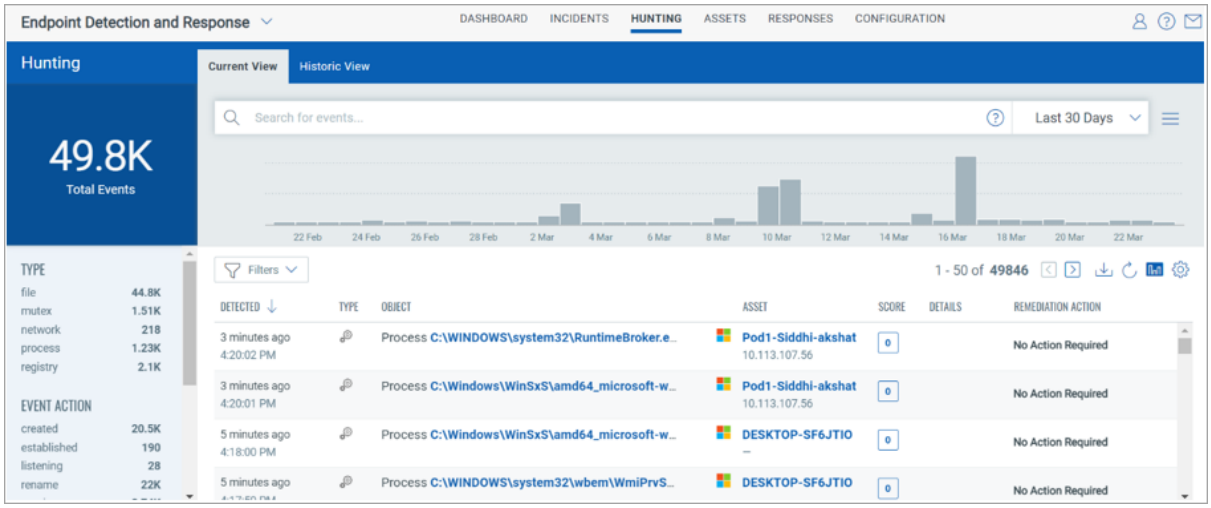
With EDR's searching and filtering capabilities you can quickly find all about your incidents, events and assets all in one place. Anomalous endpoint behavior is detected and identified as MITRE ATT&CK Tactics and Techniques.

How to detect threats

Navigate to Hunting tab > Current View sub tab lists all the events that are active on the assets. In current View, you'll notice Search box where you will enter search query. Your matches will appear in the list.

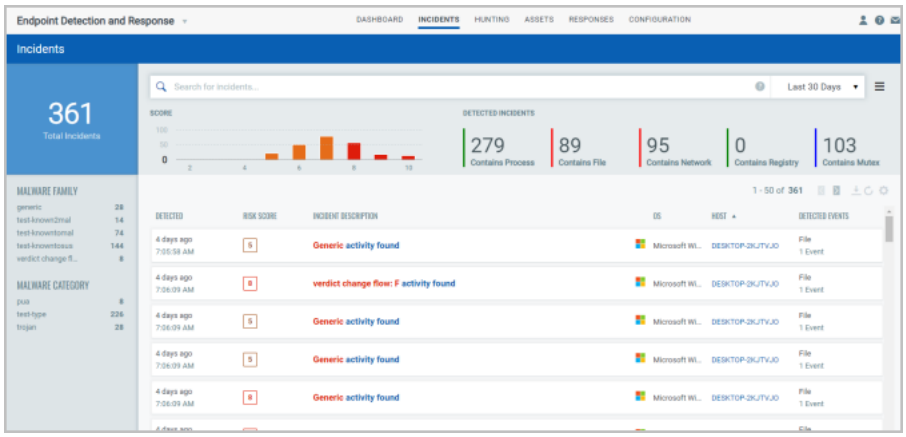


Once you have your search results, you can download your results and easily manage events or incidents.

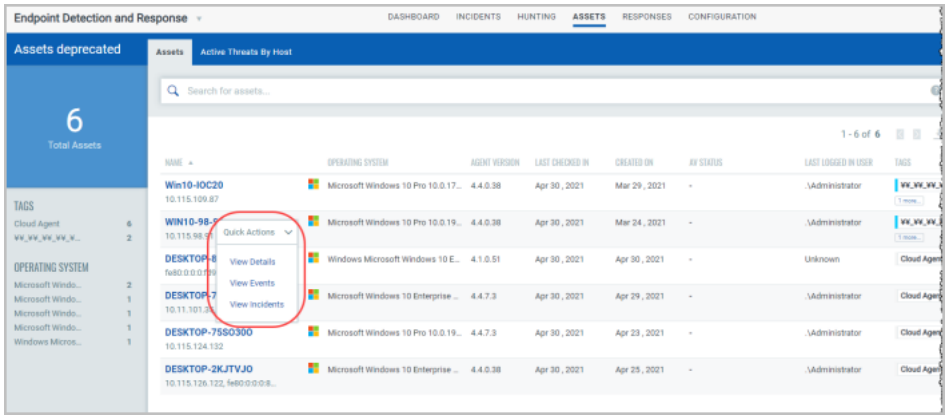


Investigate threats

Investigate incidents for active threats by Malware name and malware family name. Here all the incidents detected on an asset are listed here.

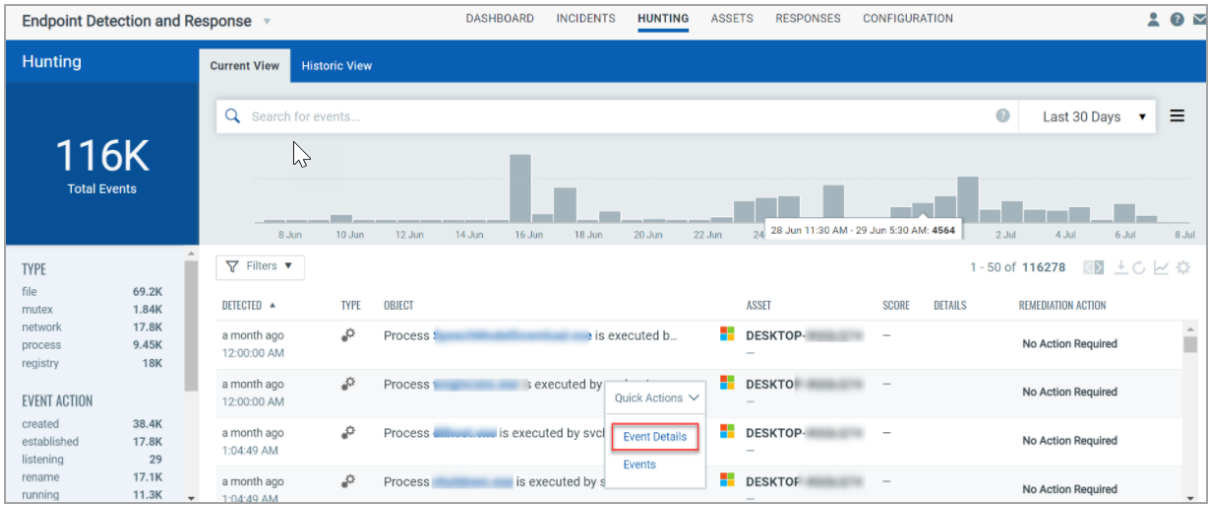


Using Quick action menu, you will get up to date information about Asset Details, Event Details, and Incident details.



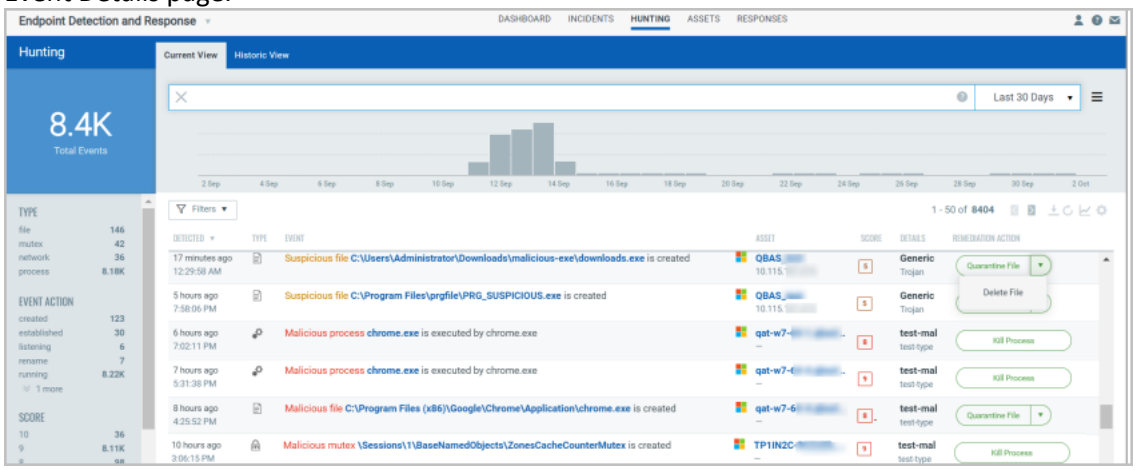
Event Details

Events registered on the agents are analysed, and appropriate ATT&CK tactics and techniques are applied on the Event Details page.

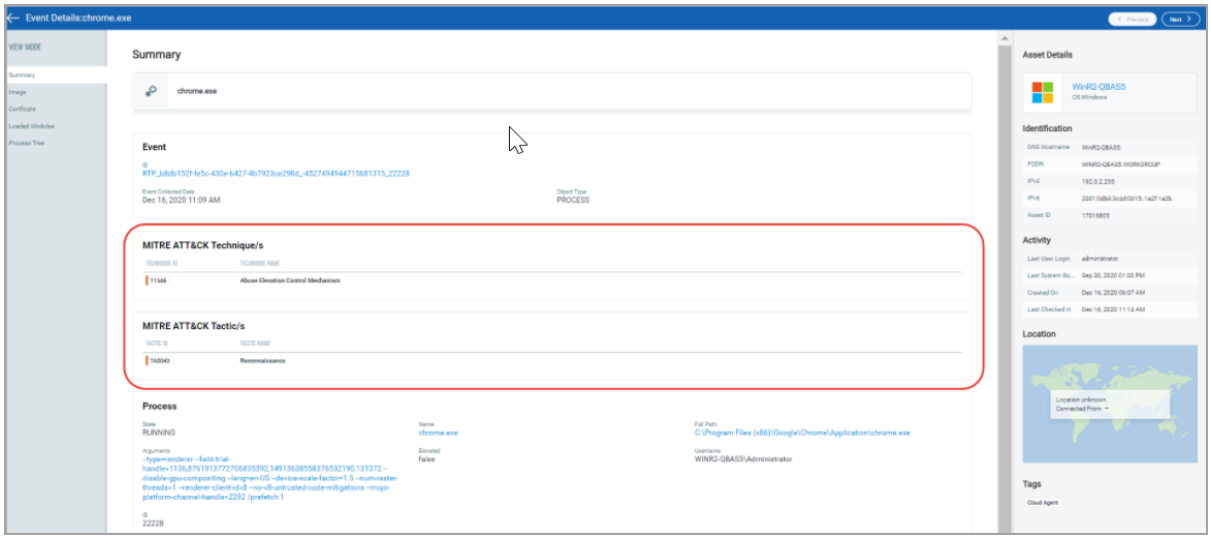


Remediation

You can remediate malicious events detected on the assets from the Hunting tab and the Events Details page. The remediation options are available in the Remediation Action column. Remediation actions can be performed for File, Process, Network, and Mutex events from the Hunting and the Event Details page.



After the malicious behavior is detected on the endpoint, with the help of EDR the events are evaluated in context with MITRE ATT&CK**.**



Refer to the EDR blog for more information:
Log4Shell Exploit Detection and Response with Qualys Multi-Vector EDR

Refer to the following docs to get started with EDR
EDR Onboarding Videos | EDR Getting Started Guide | EDR Online Help