



Qualys Multi-Vector EDR Holiday Season Playbook

November 16, 2021

Table of Contents

Qualys Multi-Vector EDR Holiday Season Playbook	1
Introduction to Qualys Multi-Vector EDR Holiday Protection.....	3
<i>What I Get with Holiday EDR Enabled</i>	<i>3</i>
<i>Let's Get Started</i>	<i>4</i>
Step 1 - Enable your Cloud Agents for EDR	4
Step 2 - Enable EDR and Malware Protection in Configuration Profile	5
Step 3 - Verify that EDR with Anti-Malware is activated.....	6
Step 4 - Configure Rule-Based Alerts for Events	7
Step 5 - View Events and Detections.....	8
<i>Hunting Use Cases</i>	<i>9</i>
Threat Actor Tactic and Hunting Approach – “Suspicious Use of SVCHOST”:	9
Monitor Active Network Connections.....	9
Powershell Execution Policy Bypass	10

Introduction to Qualys Multi-Vector EDR Holiday Protection

As we enter the holiday season, malicious actors aim to strike while we try to relax and take time off. They view holidays as attractive timeframes in which to target victims, while defenses are less monitored. It's a head start for attackers as they feel less pressure of being detected while probing victim organizations and looking for an ideal vector to exploit. In Alert ([AA21-243A](#)), the FBI and CISA have issued a joint advisory warning about an increase in the number of attacks coinciding with weekends and holidays. Holidays such as Mother's Day, Memorial weekend, and the 4th of July of 2021 saw a record number of attacks from groups like the DarkSide and ReEvil ransomware groups.

To stay safe, one of the top suggestions is to implement a tool like Qualys Multi-Vector Endpoint Detection and Response (EDR) that can monitor your device files, processes, mutex, network, registry, etc., from a behavioral analytics standpoint. Qualys correlates multi-vector threat sources from several points of view: host telemetry, vulnerabilities, and exploits, misconfigurations, file integrity violation, certificate issues, missing patches, network traffic, threat intel feeds, user context, file-less, and ransomware attacks. Qualys leverages our single cloud-based capabilities to protect against APT, zero-days, and known/unknown ransomware.

As an existing Qualys customer, getting this protection is as easy as activating the already deployed Qualys Cloud Agents for Multi-Vector EDR with Anti-malware to detect and prevent zero-day and ransomware-related attacks. The Qualys agent has inbuilt malware detection and blocking capabilities that can be turned on within a matter of minutes via our 60-day free EDR to discover and block any malware lurking in your system.

View video: [Introducing Qualys Multi-Vector EDR](#)

Refer to [Qualys Documentation](#) and [Qualys Videos](#) to set up and configure Qualys capabilities, as required.

What I Get with Holiday EDR Enabled

Now that the Holiday EDR is enabled, you can start detecting and blocking malware. As you already have VMEDR capabilities, with holiday EDR you can additionally:

Protect your assets against the latest advanced malware

EDR utilizes a myriad of detection technologies to protect and detect malware throughout the entire attack lifecycle, including anti-malware engine, threat intelligence feeds, correlation rules, memory exploit protection, malicious network protection, anti-phishing protection, and MITRE ATT&CK tactics and techniques

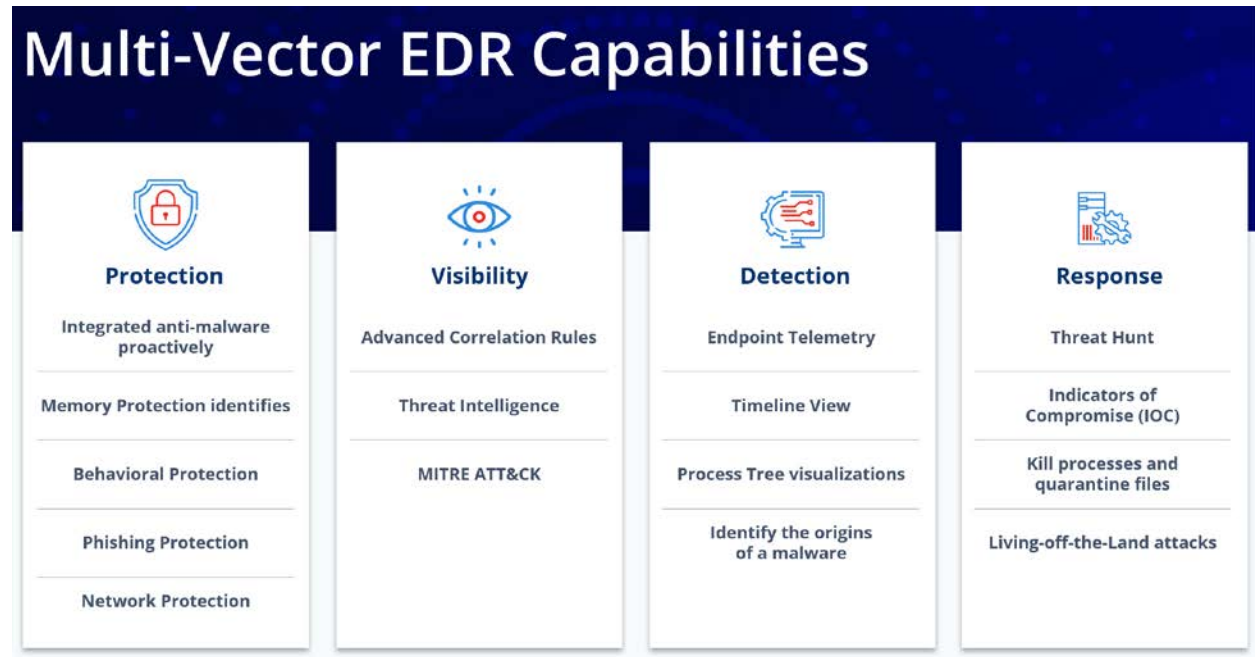
Hunt and Detect unknown malware and suspicious activities

EDR collects endpoint telemetry from your devices to identify attack-related behavior and provides visibility and context to how malware appeared on the device

Save Time and money

EDR is built natively on the Qualys Cloud Platform, sharing priorities, visibility, and intelligence with other products (such as Cybersecurity Asset Management, Vulnerability Management, Policy Compliance, File Integrity Monitoring, Patch Management, etc.), providing you with a single agent, single pane of glass, and single Management Console

Multi-Protection Technologies



Let's Get Started

As an existing Qualys user, you already have all the components in place to quickly get started. Just follow these simple steps to get started.

Before you start, refer following documentation for hardware, software recommendation, and detailed steps

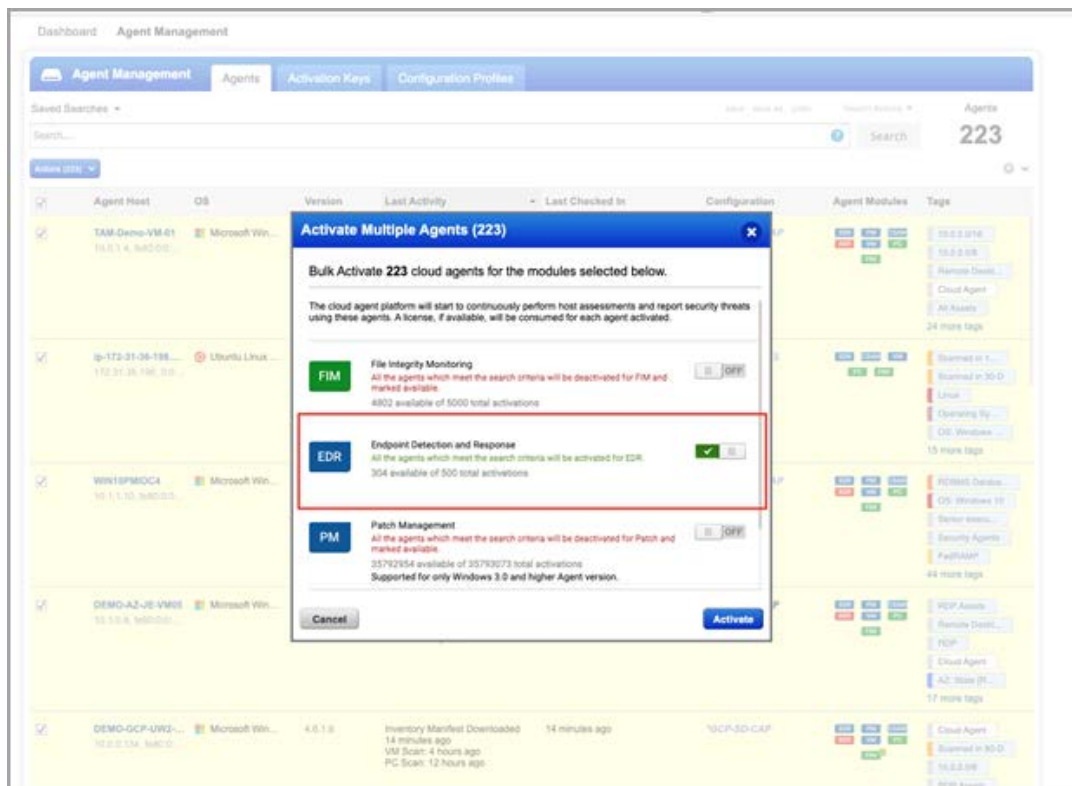
[EDR Onboarding Guide](#) | [EDR Getting Started Guide](#) | [EDR Online Help](#)

Step 1 - Enable your Cloud Agents for EDR

You need a Cloud Agent that has been activated for EDR on each asset that you want to monitor for suspicious activity. You can either:

- Select the existing activation key and upgrade the associated agents for EDR.
- Install new Cloud Agent and activate the agent for EDR.

For detailed steps, refer to: [Configure Cloud Agents for EDR](#)

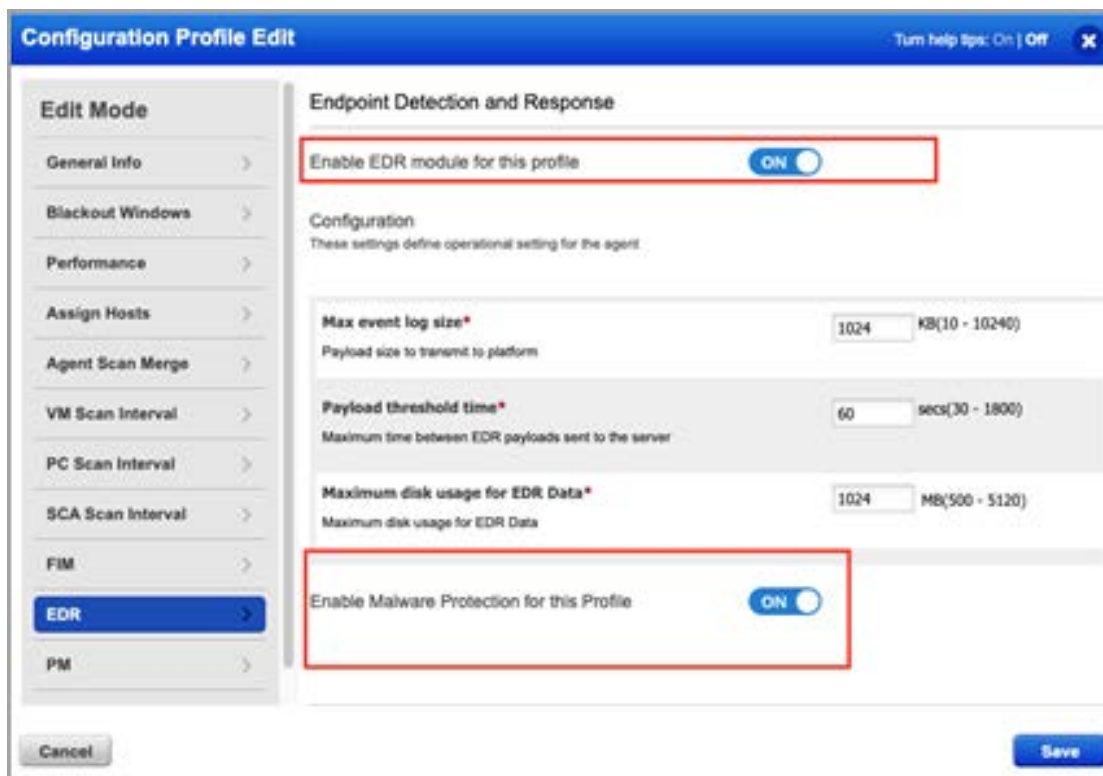


Step 2 - Enable EDR and Malware Protection in Configuration Profile

Navigate to the Cloud Agent > Agents tab and identify the agent that has EDR enabled on it.

Toggle Enable EDR module for this profile to On. This is required for EDR data collection. Toggle the Enable Malware Protection for this Profile to On for anti-malware activation.

For detailed steps, refer to: [Enable EDR module](#) | [Enable Malware Protection](#)

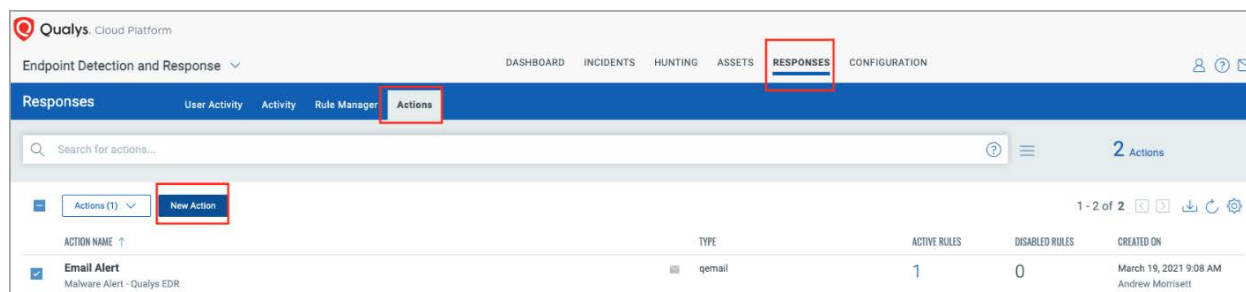


Step 3 - Verify that EDR with Anti-Malware is activated

Navigate to the Assets tab in the EDR module, and in the AV status column, verify that the number of assets matches your assigned agent profile selection. Also, view the AV status of the agent. The status changes to Installed as the Malware Protection enables for each agent.

Endpoint Detection and Response							
DASHBOARD INCIDENTS HUNTING ASSETS RESPONSES CONFIGURATION							
Assets							
Assets Active Threats By Host							
<div>196 Total Assets</div> <div> TAGS: Cloud Agent 196, 123-cdj-test-asse... 196, OS: Windows 8.1 ... 196, All Assets 196, Operating System... 188, 45 more </div> <div> OPERATING SYSTEM: Microsoft Windo... 11, Amazon Linux 2 10, Microsoft Windo... 10, Ubuntu Linux 18... 10, Microsoft Windo... 9, 45 more </div>							
NAME	OPERATING SYSTEM	AGENT VERSION	LAST CHECKED IN	CREATED ON	AV STATUS	LAST LOGGED IN USER	TAGS
ip-192-168-0-38.ec2.internal 172.17.0.1, fe80:0:0:4de:29ff:fec2:b99e...	Ubuntu Linux 18.04.6	4.6.0.56	Nov 04, 2021	Sep 18, 2019	-	reboot	Scanned in 90-D 26 more
ip-192-168-0-242.ec2.internal fe80:0:0:45f9:5ff:fe6:8e55, 192.168.0...	CentOS Linux 7.6.1810	4.6.0.56	Nov 04, 2021	Jul 09, 2019	-	reboot	123-cdj-test-asse... 31 more
ip-192-168-0-185.ec2.internal 192.168.0.185, fe80:0:0:496:b1ff:feaf:b...	Amazon Linux 2	4.6.0.56	Nov 04, 2021	Jul 09, 2019	-	reboot	Operating System... 15 more
ip-172-31-41-105.us-east-2.comp... fe80:0:0:83f9:df1:fe4a:73ec, 172.31.41...	Amazon Linux 2	4.6.0.56	Nov 04, 2021	May 12, 2021	-	reboot	Type: Servers 32 more
ip-172-31-37-33.us-east-2.comp... fe80:0:0:884:59ff:fe82:a3b0, 172.31.37...	Red Hat Enterprise Linux Server 7.7	4.6.0.56	Nov 04, 2021	Feb 13, 2020	-	ec2-user	OS: UNIX/Linux... 32 more
ip-172-31-36-198.us-east-2.comp... 172.17.0.1, 172.31.36.198, fe80:0:0:8d...	Ubuntu Linux 18.04.5	4.6.0.56	Nov 04, 2021	Feb 04, 2021	-	reboot	172.16.0.0/12 19 more
ip-172-31-33-250.us-east-2.comp... fe80:0:0:87a:x3ff:fe6b:fae6, 172.31.33...	Amazon Linux 2	4.6.0.56	Nov 04, 2021	May 12, 2021	-	reboot	123-cdj-test-asse... 33 more
ip-172-31-20-135.us-west-1.comp... 172.17.0.1, fe80:0:0:49:aff:fe62:90c9, 1...	Ubuntu Linux 18.04.5	4.6.0.56	Nov 04, 2021	Oct 01, 2020	-	reboot	All Assets 20 more
ip-172-31-16-173.us-west-2.comp... 172.17.0.1, fe80:0:0:df1:fe4c:7bb5, 172.31.16...	Amazon Linux 2	4.6.0.56	Nov 04, 2021	May 03, 2021	-	ec2-user	Scanned in 30-D 28 more
ip-172-31-12-193.us-east-2.comp... 52.15.141.175, 172.31.12.193	Ubuntu Linux 18.04.5	4.6.0.56	Nov 04, 2021	Jan 19, 2021	-	reboot	Scanned in 90-D 14 more
ip-172-31-10-40.us-west-2.comp...	Amazon Linux 2	4.6.0.56	Nov 04, 2021	May 03, 2021	-	ec2-user	Cloud Agent

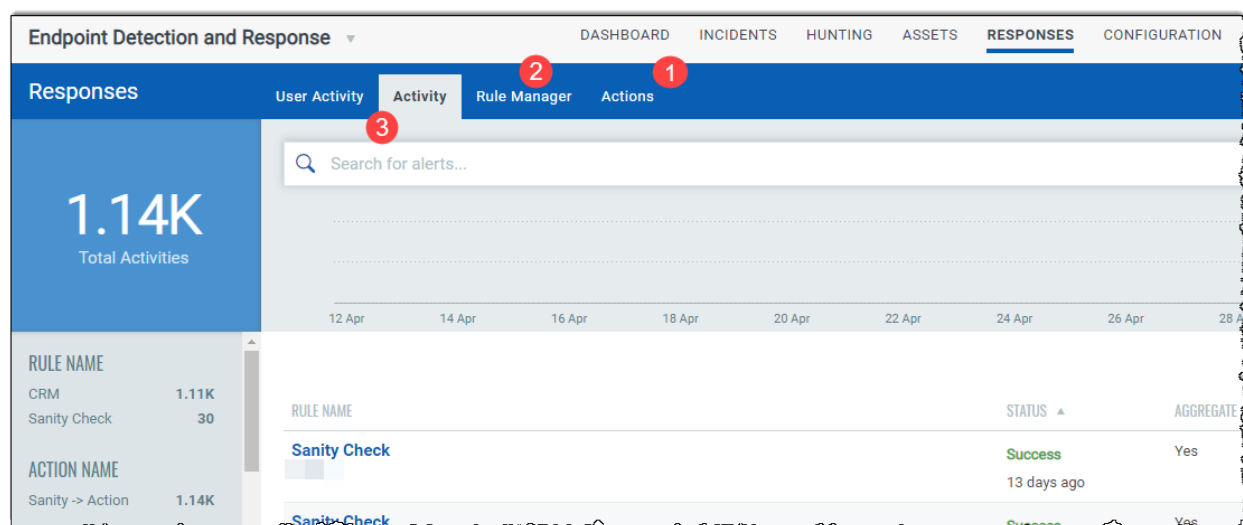
Navigate to the Configuration tab and set up your Anti-Malware profile. The default profile is applied if you do not edit it. Review and edit various functionality options, including an exclusion section.



Step 4 - Configure Rule-Based Alerts for Events

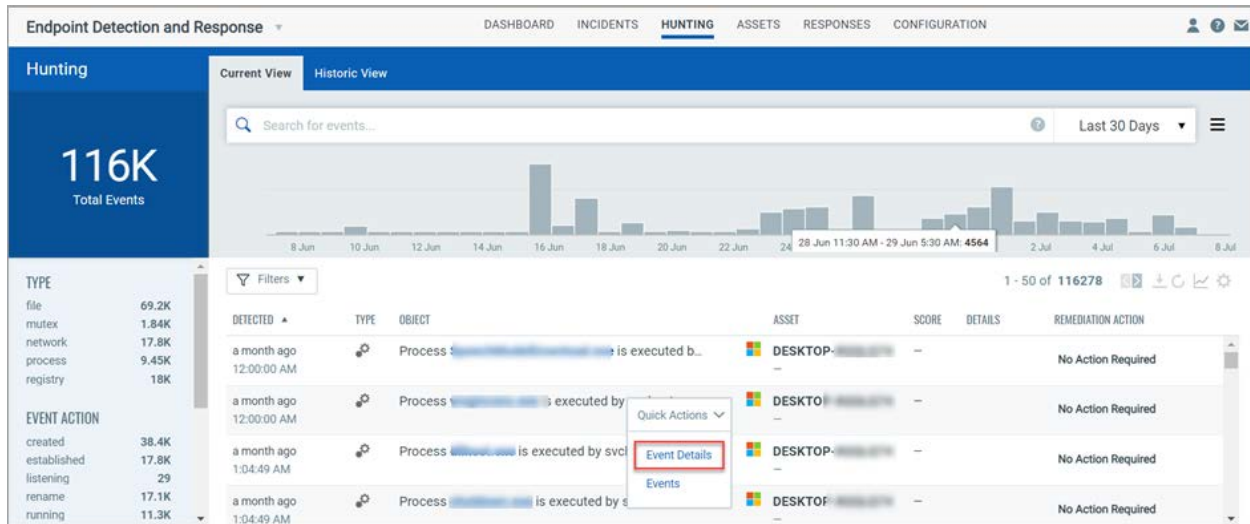
You can configure EDR to monitor events for conditions specified in a rule and send you alerts if events matching the condition are detected. For EDR to send alerts, you need to first configure a rule action to specify the action taken when events matching a condition is detected. EDR will use the rule action settings to send you the alerts. Finally, create a rule to specify the conditions for triggering the rule and select rule actions for sending the alert when a rule is triggered.

For detailed steps, refer to: [Configure rule-based alerts for events](#)



Step 5 - View Events and Detections

All detections and events are listed in the Hunting tab. You can view details of each event and perform remediation actions (Quarantine File/ Delete File/ Kill Process) on File, Mutex, Network, and Process events. Refer to [View Event Details](#)



Hunting Use Cases

The Hunting tab in Qualys Multi-Vector EDR is a single search box to query your entire environment for devices file, process, mutex, network, registry status. All of these can also be configured to be an alert.

We have provided a few threat hunting queries to get you started in understanding your environment. Also, refer to [Hunting Tutorial](#)

Threat Actor Tactic and Hunting Approach – “Suspicious Use of SVCHOST”:

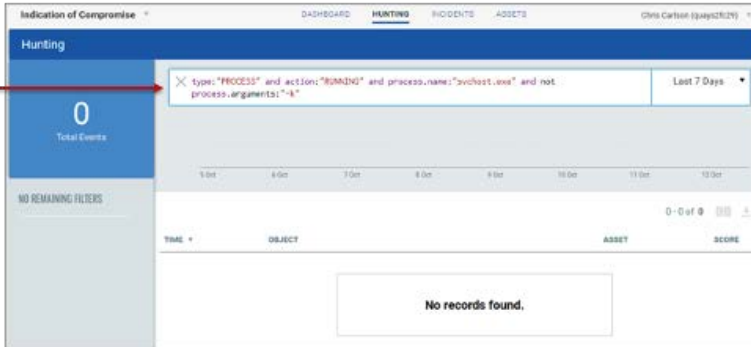
Service Host (“svchost.exe”) is a system process that hosts multiple Windows services.

Normal usage is to use the “-k” argument to define the service (via DLL) to instantiate, e.g., “svchost.exe -k imgsvc”. This will display the service name that is loaded by svchost.

Threat actors try to evade detection by injecting malware directly into svchost.exe instead of calling their code directly, thus there is no “-k” argument.

Hunting approach: svchost.exe running without “-k” argument is suspicious.

Search Logic:
Find all running svchost.exe processes that do not have “-k” as an argument.

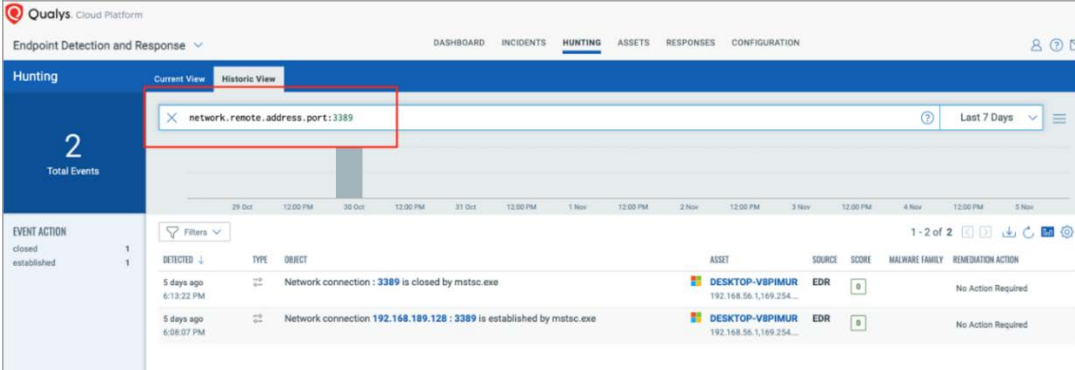


The screenshot shows the Qualys Hunting interface. A search query is entered: "type:'PROCESS' and action:'RUNNING' and process.name:'svchost.exe' and not process.arguments:'-k'". The interface shows 0 total events and a message "No records found.".

Monitor Active Network Connections

The two most prevalent initial access vectors for Ransomware are phishing and brute forcing unsecured remote desktop protocol (RDP) endpoints. You can search both current and historical views for what sort of RDP connections have occurred on your devices.

Hunting approach: network.remote.address.port:3389



The screenshot shows the Qualys Hunting interface with a search query: "network.remote.address.port:3389". The interface shows 2 total events. The results table is as follows:

DETECTED	TYPE	OBJECT	ASSET	SOURCE	SCORE	MALWARE FAMILY	REMEDIATION ACTION
5 days ago 6:12:22 PM	Network connection	3389 is closed by mtask.exe	DESKTOP-VSPIMUR	EDR	0		No Action Required
5 days ago 6:08:07 PM	Network connection	192.168.189.128 : 3389 is established by mtask.exe	DESKTOP-VSPIMUR	EDR	0		No Action Required

Powershell Execution Policy Bypass

Since attackers utilize Powershell to execute malicious code, it is crucial to monitor its usage across your organization. There has been a dramatic rise in the abuse of Powershell as it is on every Windows device, can call the Windows API, avoid detection by Anti-virus, run commands without writing to the disk, and is whitelisted in many organizations. There are many ways to bypass execution policies preventing Powershell from running, and this is the activity we are looking for in this search.

Hunting approach: type:PROCESS and process.name:powershell.exe and process.arguments:"ExecutionPolicy Bypass"

