Let’s Talk Endpoint Monitoring

IBM QRadar Endpoint Content Extension

Colin Carle
QRadar Offering Manager

Amy Seo
Security Content Developer

Nigel Sood
Security Content Developer

Rory Bray
Security Architect

Gladys Koskas
QRadar Security Content Specialist

Augustine Chife
Security Content Developer

Will Leonard
Security Content Developer

Jonathan Pechta
QRadar Support

Krista Paget
Security Content Developer

Mololuwa Josiah
Security Content Developer

IBM **Security**

13 August 2020

Legal notes and disclaimer

U.S. Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to up this information. THIS document is distributed "AS IS" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice. Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM’s products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

Other company, product, or service names may be trademarks or service marks of others. A current list of IBM trademarks is available at “Copyright and trademark information” www.ibm.com/legal/copytrade.shtml

Agenda

Announcements	**04**
About the Endpoint Monitoring Content Ext	**05**
Configuration for Windows Endpoint Monitoring	**06**
Configuration for Linux Endpoint Monitoring	**07**
Demo Scenario 1: Windows	**09**
Demo Scenario 2: Linux	**15**
Q&A	**21**
Common Questions	**22**
Enhancements and Support	**27**
Reference information	**30**

Announcements

Threat Content Pack 1.2.0

- This update introduces a new AQL function to detect Homograph attacks from events or flows. Read more about homograph attacks here: https://en.wikipedia.org/wiki/IDN_homograph_attack
- Added two new rules for DNS Queries:
  - Suspicious DNS Query Length
  - Suspicious program initiating DNS Query
- Download: https://exchange.xforce.ibmcloud.com/hub/extension/IBMQRadar:IBMContentPackageInternalThreat

QRadar Security Analytics Self Monitoring 1.1.0

This content pack assists with monitoring changes in QRadar.

- This update includes new custom property extractions for Offense Closed Comment, Offense Closed Reason, and Offense IDs.
- New rule for 'unusally high or low offenses' detected.
- New Saved Searches: Number of Offenses Created, QRadar Audit : Offenses Closed Reason, QRadar Audit : Top Offenses Closed Reason
- New report for closed offenses

How do you differentiate between normal and suspicious activity?

Bad actors make use of

- Account creation, permissions management, and other management tasks using PowerShell are all part of legitimate workflows
- Bad actors make use of the same activity, and it can be difficult to disambiguate between normal and malicious activity
- Detecting suspicious activity requires complex logic to avoid creating additional work for the analyst

Normal

- Privilege modification
- File Downloads
- Script Execution
- Hidden file creation

Suspicious

- Communication with suspicious URL / IP
- Disable security tools
- Process masquerading
- Application shimming

Source: insert data source citation

IBM **Security QRadar** Endpoint Content Extension

Endpoint Content Extension

- Monitor and secure endpoints in your security deployment
- Optimized for Windows and Linux log sources types
- Recommended configurations for Windows and Linux

Key capabilities

- 25 Building Blocks
- New and updated custom event properties for Windows and Linux
- 19 Custom Rules
- 16 Reference sets
- MITRE ATT&CK® Coverage with the Use Case Manager

Benefits

- Logic provided in the building blocks will save you time and effort
- Tunable reference sets that are flexible for your deployment
- Lightweight content management
- Meaningful detections, to reduce false positives.
- Built in guidance and recommendations

Configuration for Windows Endpoint Monitoring

You must configure your Windows endpoints to monitor security events with Sysmon, add the SwiftonSecurity Sysmon configuration, tune Sysmon event IDs 1 and 7 in the XML file, and install Sysmon as an administrator.

Audit monitoring

- Security Events
- Sysmon
- Powershell Auditing

Dependencies

- IBM QRadar Custom Properties for Microsoft Windows
- Windows Security Event Log DSM

Required downloads

- Sysmon: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- Sysmon configuration from SwiftonSecurity: https://github.com/SwiftOnSecurity/sysmon-config

Configuration

- Enable audit process tracking (on success events) in the Local Security Policy.
- Enable Powershell auditing options ‘Script Block Logging’.
- Increase the maximum payload size in QRadar.

Configuration for Linux Endpoint Monitoring

You must configure your Linux endpoints with updated rules in auditd. It is recommended to backup your auditd rules before you modify Linux endpoints.

Auditd monitoring

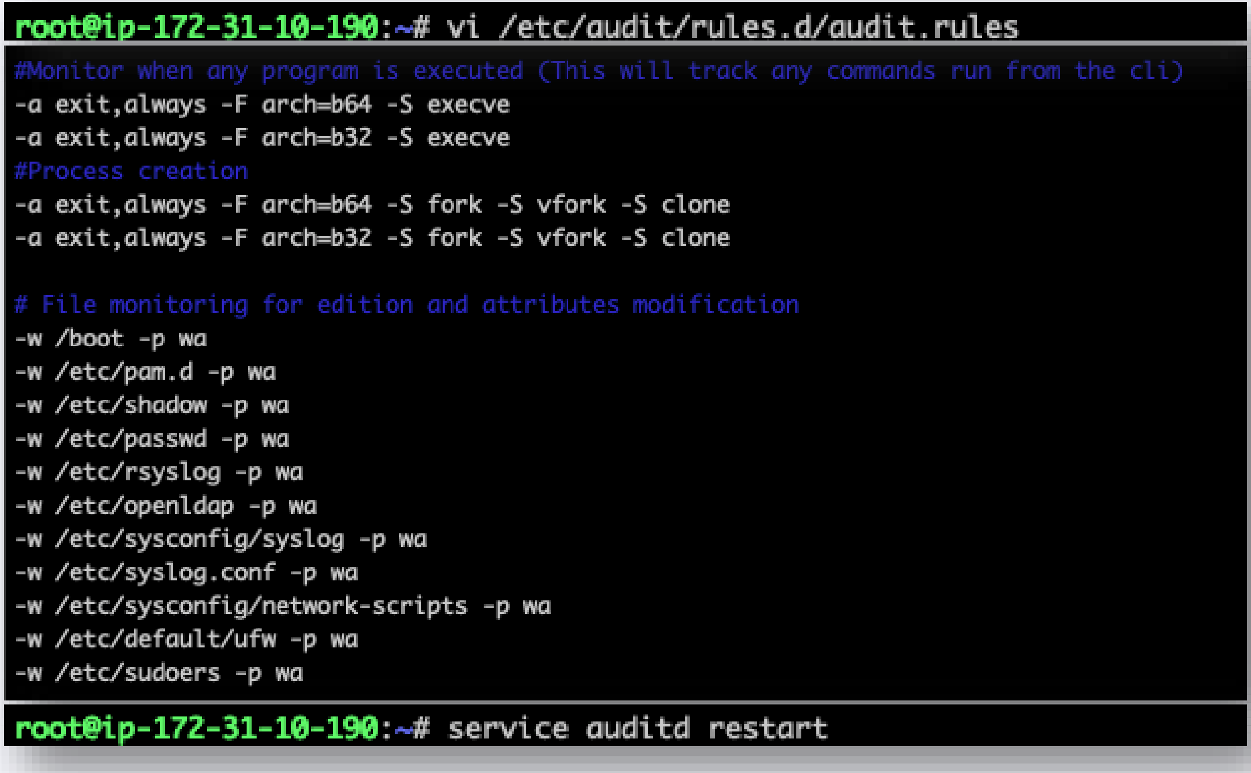
- Process execution
- Process creation
- File monitoring

Note: You must restart auditd to load any rule changes. For example:

```
service auditd restart
```

Dependencies

- [IBM QRadar Custom Properties for Linux]
- Linux OS DSM



```
root@ip-172-31-10-190:~# vi /etc/audit/rules.d/audit.rules
#Monitor when any program is executed (This will track any commands run from the cli)
-a exit,always -F arch=b64 -S execve
-a exit,always -F arch=b32 -S execve
#Process creation
-a exit,always -F arch=b64 -S fork -S vfork -S clone
-a exit,always -F arch=b32 -S fork -S vfork -S clone

# File monitoring for edition and attributes modification
-w /boot -p wa
-w /etc/pam.d -p wa
-w /etc/shadow -p wa
-w /etc/passwd -p wa
-w /etc/rsyslog -p wa
-w /etc/openldap -p wa
-w /etc/sysconfig/syslog -p wa
-w /etc/syslog.conf -p wa
-w /etc/sysconfig/network-scripts -p wa
-w /etc/default/ufw -p wa
-w /etc/sudoers -p wa
root@ip-172-31-10-190:~# service auditd restart
```

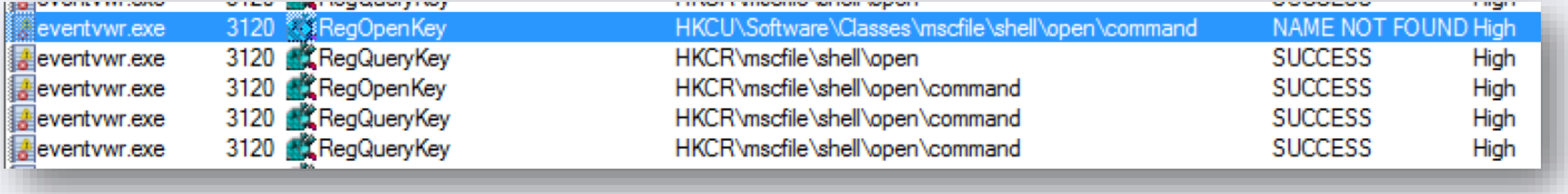
IBM QRadar Endpoint Content Extension

Demo 1: Windows detection example

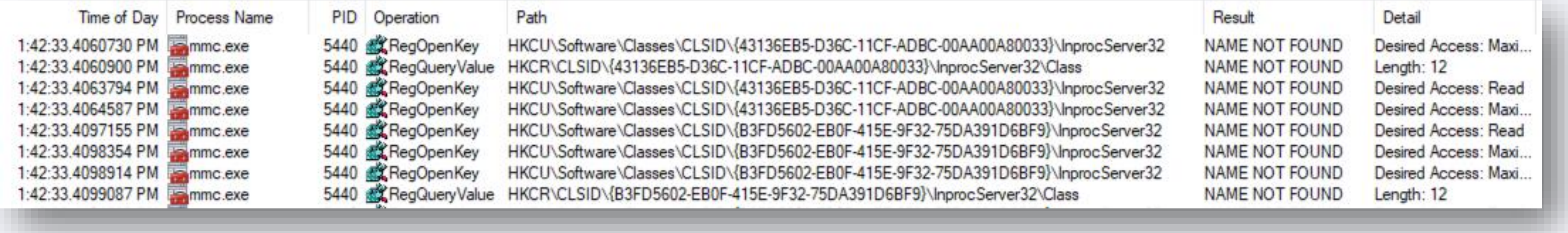
Scenario 1

An attacker connects to a Windows environment, modifies registry entries to redirect a legitimate program to a PowerShell environment, and proceeds to a group discovery.

Target an elevated process to tamper with



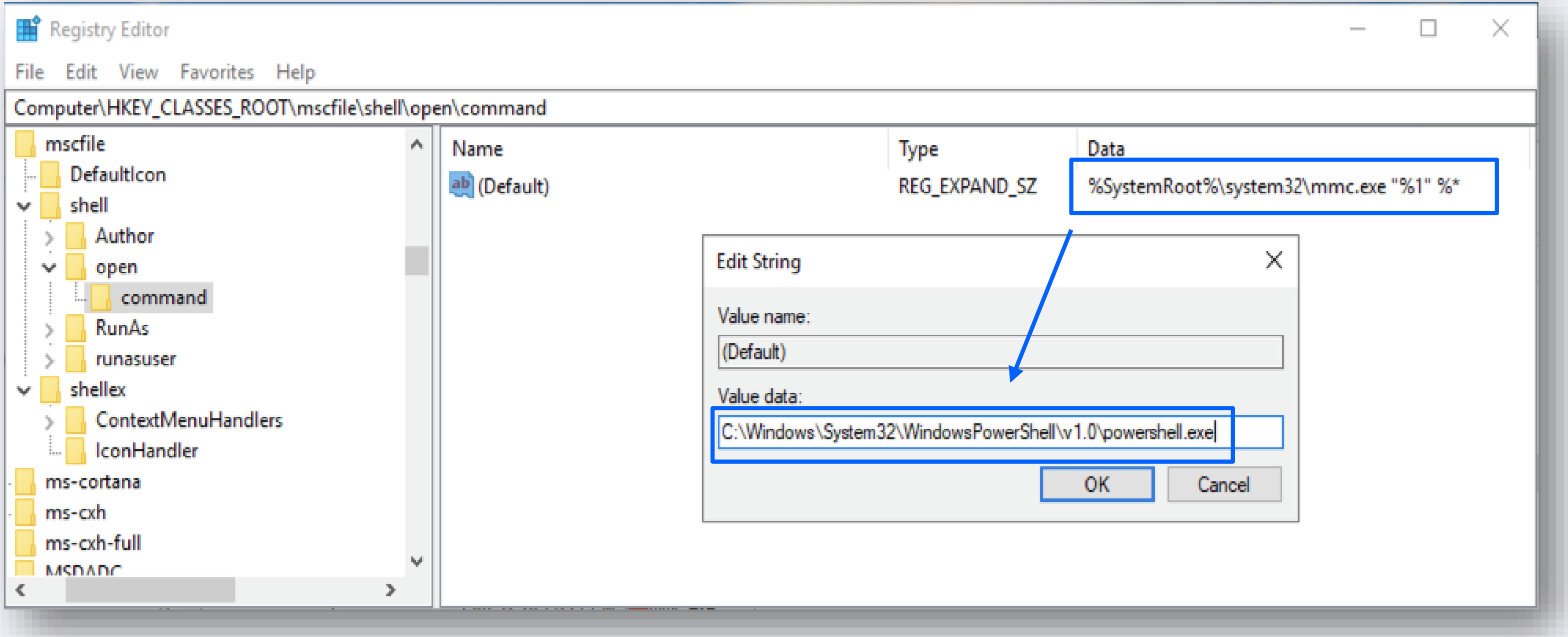
eventvwr.exe	3120	RegOpenKey	HKCU\Software\Classes\mscfile\shell\open\command	NAME NOT FOUND	High
eventvwr.exe	3120	RegQueryKey	HKCR\mscfile\shell\open	SUCCESS	High
eventvwr.exe	3120	RegOpenKey	HKCR\mscfile\shell\open\command	SUCCESS	High
eventvwr.exe	3120	RegQueryKey	HKCR\mscfile\shell\open\command	SUCCESS	High
eventvwr.exe	3120	RegQueryKey	HKCR\mscfile\shell\open\command	SUCCESS	High



Time of Day	Process Name	PID	Operation	Path	Result	Detail
1:42:33.4060730 PM	mmc.exe	5440	RegOpenKey	HKCU\Software\Classes\CLSID\{43136EB5-D36C-11CF-ADBC-00AA00A80033}\InprocServer32	NAME NOT FOUND	Desired Access: Maxi...
1:42:33.4060900 PM	mmc.exe	5440	RegQueryValue	HKCR\CLSID\{43136EB5-D36C-11CF-ADBC-00AA00A80033}\InprocServer32\Class	NAME NOT FOUND	Length: 12
1:42:33.4063794 PM	mmc.exe	5440	RegOpenKey	HKCU\Software\Classes\CLSID\{43136EB5-D36C-11CF-ADBC-00AA00A80033}\InprocServer32	NAME NOT FOUND	Desired Access: Read
1:42:33.4064587 PM	mmc.exe	5440	RegOpenKey	HKCU\Software\Classes\CLSID\{43136EB5-D36C-11CF-ADBC-00AA00A80033}\InprocServer32	NAME NOT FOUND	Desired Access: Maxi...
1:42:33.4097155 PM	mmc.exe	5440	RegOpenKey	HKCU\Software\Classes\CLSID\{B3FD5602-EB0F-415E-9F32-75DA391D6BF9}\InprocServer32	NAME NOT FOUND	Desired Access: Read
1:42:33.4098354 PM	mmc.exe	5440	RegOpenKey	HKCU\Software\Classes\CLSID\{B3FD5602-EB0F-415E-9F32-75DA391D6BF9}\InprocServer32	NAME NOT FOUND	Desired Access: Maxi...
1:42:33.4098914 PM	mmc.exe	5440	RegOpenKey	HKCU\Software\Classes\CLSID\{B3FD5602-EB0F-415E-9F32-75DA391D6BF9}\InprocServer32	NAME NOT FOUND	Desired Access: Maxi...
1:42:33.4099087 PM	mmc.exe	5440	RegQueryValue	HKCR\CLSID\{B3FD5602-EB0F-415E-9F32-75DA391D6BF9}\InprocServer32\Class	NAME NOT FOUND	Length: 12

- Enumerate possible candidates using SysInternals Process Monitor
- Find a high integrity process

Fileless user account control (UAC) bypass



Computer\HKEY_CLASSES_ROOT\mscfile\shell\open\command

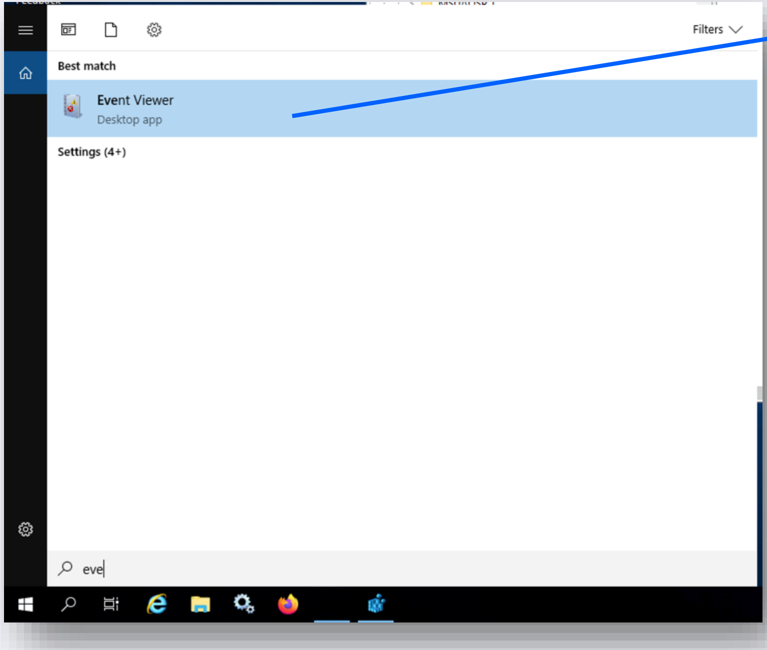
Name	Type	Data
(Default)	REG_EXPAND_SZ	%SystemRoot%\system32\mmc.exe "%1" %*

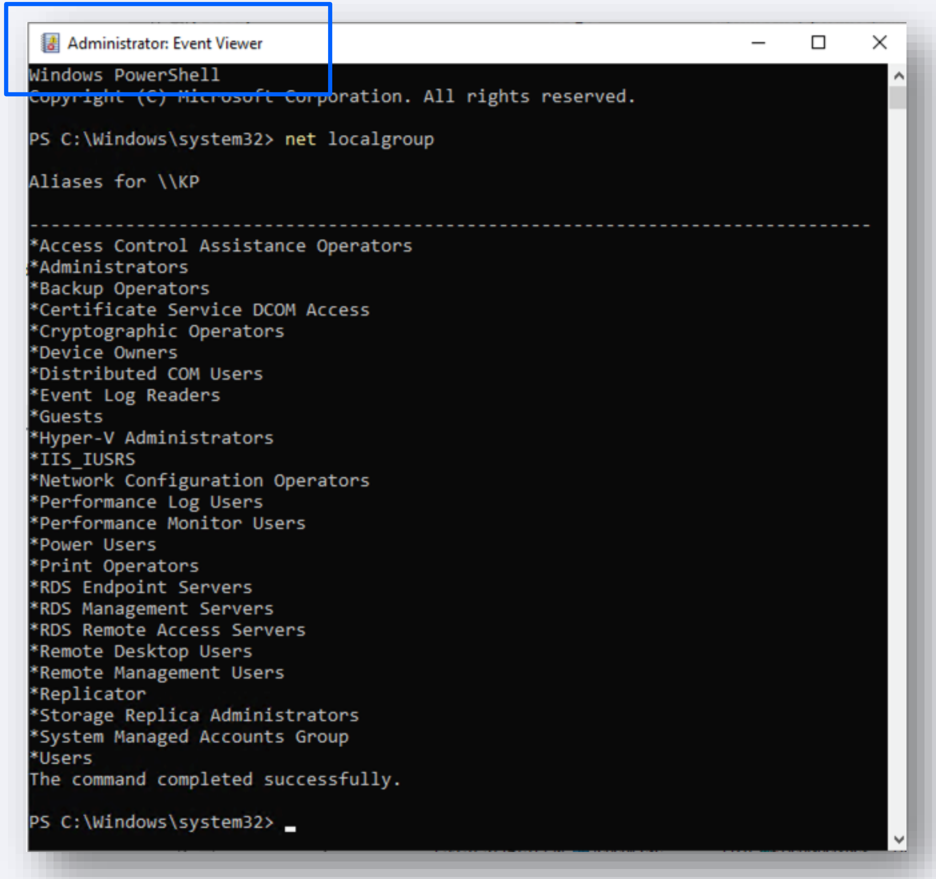
Value name: (Default)

Value data: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

- Microsoft Management Console (mmc.exe) loads Microsoft Console files (.msc)
- Replace the executable with PowerShell

Execute PowerShell script or command

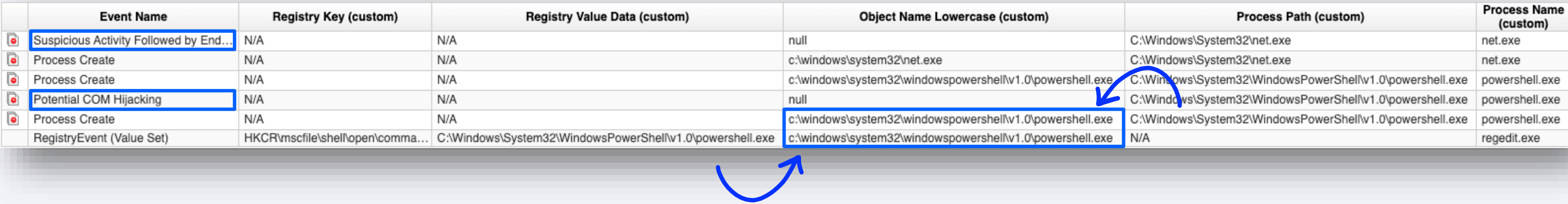




```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> net localgroup

Aliases for \\KP

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Print Operators
*RDS Endpoint Servers
*RDS Management Servers
*RDS Remote Access Servers
*Remote Desktop Users
*Remote Management Users
*Replicator
*Storage Replica Administrators
*System Managed Accounts Group
*Users
The command completed successfully.

PS C:\Windows\system32> _
```

- PowerShell will be loaded instead of Event Viewer
- Attacker can execute malicious or discovery commands

Component Object Model (COM) Hijacking



Event Name	Registry Key (custom)	Registry Value Data (custom)	Object Name Lowercase (custom)	Process Path (custom)	Process Name (custom)
Suspicious Activity Followed by End...	N/A	N/A	null	C:\Windows\System32\net.exe	net.exe
Process Create	N/A	N/A	c:\windows\system32\net.exe	C:\Windows\System32\net.exe	net.exe
Process Create	N/A	N/A	c:\windows\system32\windowspowershell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe
Potential COM Hijacking	N/A	N/A	null	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe
Process Create	N/A	N/A	c:\windows\system32\windowspowershell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe
RegistryEvent (Value Set)	HKCR\mscfile\shell\open\comma...	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	c:\windows\system32\windowspowershell\v1.0\powershell.exe	N/A	regedit.exe

Detection in QRadar:

1. Behavior through process path
   - registry modification
   - process creation
2. Specific registries
   - ddeexec
   - InprocServer32
   - clsid for .exe drop target

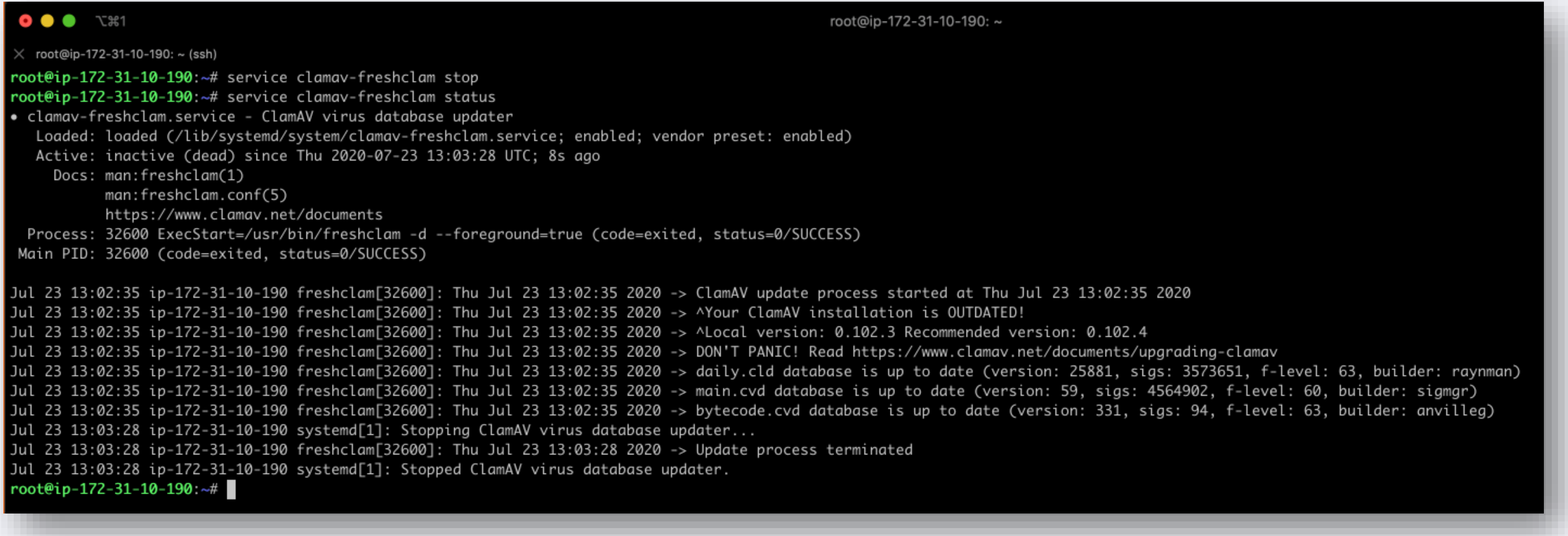
IBM QRadar Endpoint Content Extension

Demo 2: Linux detection example

Scenario 2

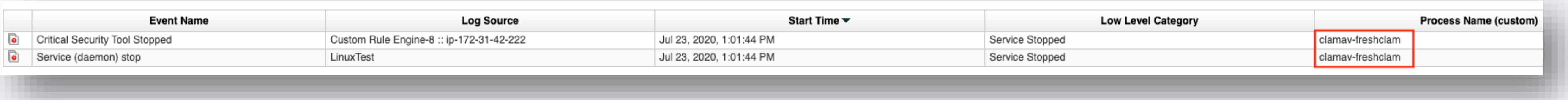
An attacker connects to a Linux environment, disables the antivirus, and creates a hidden space to drop a virtual bomb on the system.

Disable anti-virus



```
root@ip-172-31-10-190:~# service clamav-freshclam stop
root@ip-172-31-10-190:~# service clamav-freshclam status
• clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Thu 2020-07-23 13:03:28 UTC; 8s ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://www.clamav.net/documents
  Process: 32600 ExecStart=/usr/bin/freshclam -d --foreground=true (code=exited, status=0/SUCCESS)
 Main PID: 32600 (code=exited, status=0/SUCCESS)

Jul 23 13:02:35 ip-172-31-10-190 freshclam[32600]: Thu Jul 23 13:02:35 2020 -> ClamAV update process started at Thu Jul 23 13:02:35 2020
Jul 23 13:02:35 ip-172-31-10-190 freshclam[32600]: Thu Jul 23 13:02:35 2020 -> ^Your ClamAV installation is OUTDATED!
Jul 23 13:02:35 ip-172-31-10-190 freshclam[32600]: Thu Jul 23 13:02:35 2020 -> ^Local version: 0.102.3 Recommended version: 0.102.4
Jul 23 13:02:35 ip-172-31-10-190 freshclam[32600]: Thu Jul 23 13:02:35 2020 -> DON'T PANIC! Read https://www.clamav.net/documents/upgrading-clamav
Jul 23 13:02:35 ip-172-31-10-190 freshclam[32600]: Thu Jul 23 13:02:35 2020 -> daily.cld database is up to date (version: 25881, sigs: 3573651, f-level: 63, builder: raynman)
Jul 23 13:02:35 ip-172-31-10-190 freshclam[32600]: Thu Jul 23 13:02:35 2020 -> main.cvd database is up to date (version: 59, sigs: 4564902, f-level: 60, builder: sigmgr)
Jul 23 13:02:35 ip-172-31-10-190 freshclam[32600]: Thu Jul 23 13:02:35 2020 -> bytecode.cvd database is up to date (version: 331, sigs: 94, f-level: 63, builder: anvilleg)
Jul 23 13:03:28 ip-172-31-10-190 systemd[1]: Stopping ClamAV virus database updater...
Jul 23 13:03:28 ip-172-31-10-190 freshclam[32600]: Thu Jul 23 13:03:28 2020 -> Update process terminated
Jul 23 13:03:28 ip-172-31-10-190 systemd[1]: Stopped ClamAV virus database updater.
root@ip-172-31-10-190:~# 
```

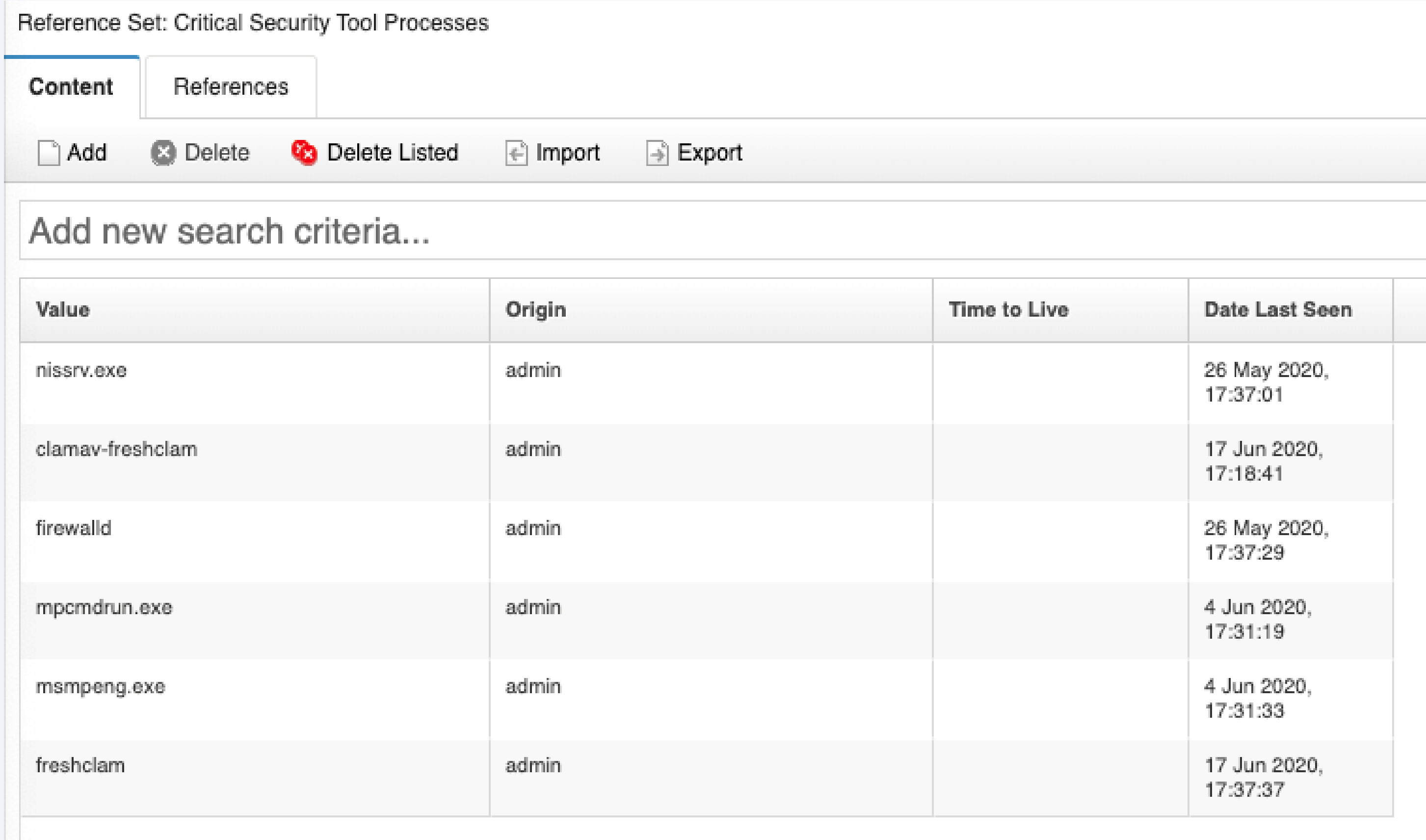
- QRadar detected clamav-freshclam was stopped



	Event Name	Log Source	Start Time ▼	Low Level Category	Process Name (custom)
	Critical Security Tool Stopped	Custom Rule Engine-8 :: ip-172-31-42-222	Jul 23, 2020, 1:01:44 PM	Service Stopped	clamav-freshclam
	Service (daemon) stop	LinuxTest	Jul 23, 2020, 1:01:44 PM	Service Stopped	clamav-freshclam

IBM **Security**

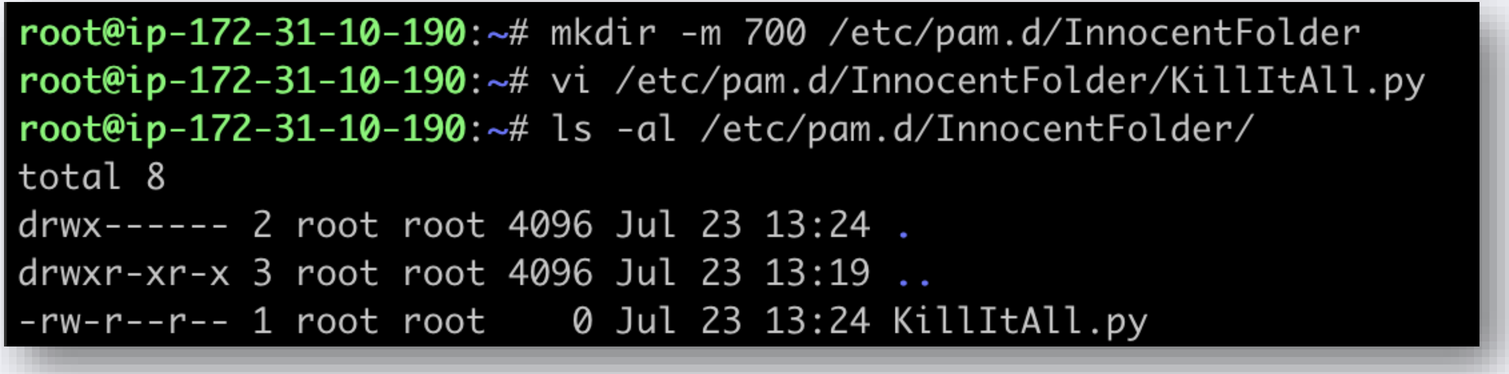
Monitor additional critical security tools



Reference Set: Critical Security Tool Processes

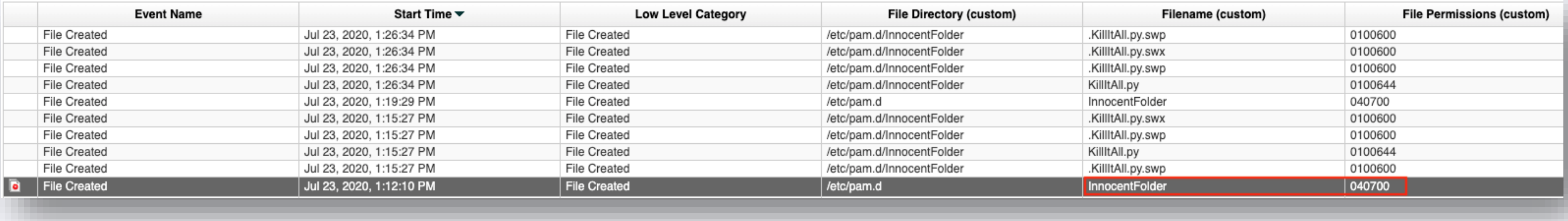
Value	Origin	Time to Live	Date Last Seen
nissrv.exe	admin		26 May 2020, 17:37:01
clamav-freshclam	admin		17 Jun 2020, 17:18:41
firewalld	admin		26 May 2020, 17:37:29
mpcmdrun.exe	admin		4 Jun 2020, 17:31:19
msmpeng.exe	admin		4 Jun 2020, 17:31:33
freshclam	admin		17 Jun 2020, 17:37:37

Create a folder with restrictive rights and drop malicious script



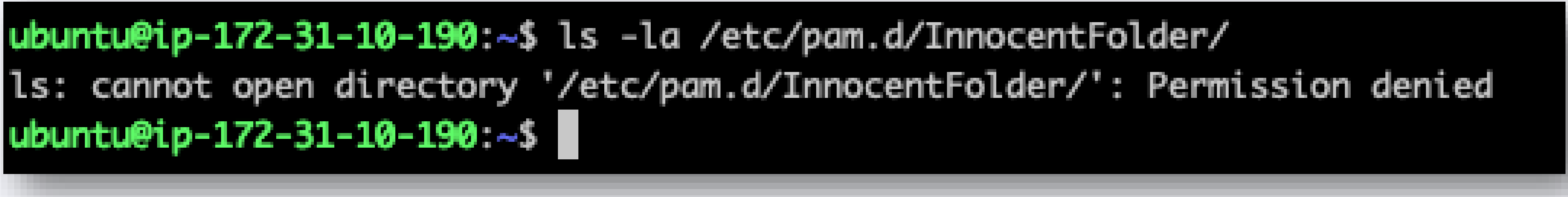
```
root@ip-172-31-10-190:~# mkdir -m 700 /etc/pam.d/InnocentFolder
root@ip-172-31-10-190:~# vi /etc/pam.d/InnocentFolder/KillItAll.py
root@ip-172-31-10-190:~# ls -al /etc/pam.d/InnocentFolder/
total 8
drwx------ 2 root root 4096 Jul 23 13:24 .
drwxr-xr-x 3 root root 4096 Jul 23 13:19 ..
-rw-r--r-- 1 root root    0 Jul 23 13:24 KillItAll.py
```

- QRadar detected creation of hidden folder which is a normal activity by itself but not after antivirus is disabled



	Event Name	Start Time ▾	Low Level Category	File Directory (custom)	Filename (custom)	File Permissions (custom)
	File Created	Jul 23, 2020, 1:26:34 PM	File Created	/etc/pam.d/InnocentFolder	.KillItAll.py.swp	0100600
	File Created	Jul 23, 2020, 1:26:34 PM	File Created	/etc/pam.d/InnocentFolder	.KillItAll.py.swx	0100600
	File Created	Jul 23, 2020, 1:26:34 PM	File Created	/etc/pam.d/InnocentFolder	.KillItAll.py.swp	0100600
	File Created	Jul 23, 2020, 1:26:34 PM	File Created	/etc/pam.d/InnocentFolder	KillItAll.py	0100644
	File Created	Jul 23, 2020, 1:19:29 PM	File Created	/etc/pam.d	InnocentFolder	040700
	File Created	Jul 23, 2020, 1:15:27 PM	File Created	/etc/pam.d/InnocentFolder	.KillItAll.py.swx	0100600
	File Created	Jul 23, 2020, 1:15:27 PM	File Created	/etc/pam.d/InnocentFolder	.KillItAll.py.swp	0100600
	File Created	Jul 23, 2020, 1:15:27 PM	File Created	/etc/pam.d/InnocentFolder	KillItAll.py	0100644
	File Created	Jul 23, 2020, 1:15:27 PM	File Created	/etc/pam.d/InnocentFolder	.KillItAll.py.swp	0100600
	File Created	Jul 23, 2020, 1:12:10 PM	File Created	/etc/pam.d	InnocentFolder	040700

Another user failed to view contents of the hidden directory



```
ubuntu@ip-172-31-10-190:~$ ls -la /etc/pam.d/InnocentFolder/
ls: cannot open directory '/etc/pam.d/InnocentFolder/': Permission denied
ubuntu@ip-172-31-10-190:~$ 
```

IBM QRadar Endpoint Content Extension

Q&A

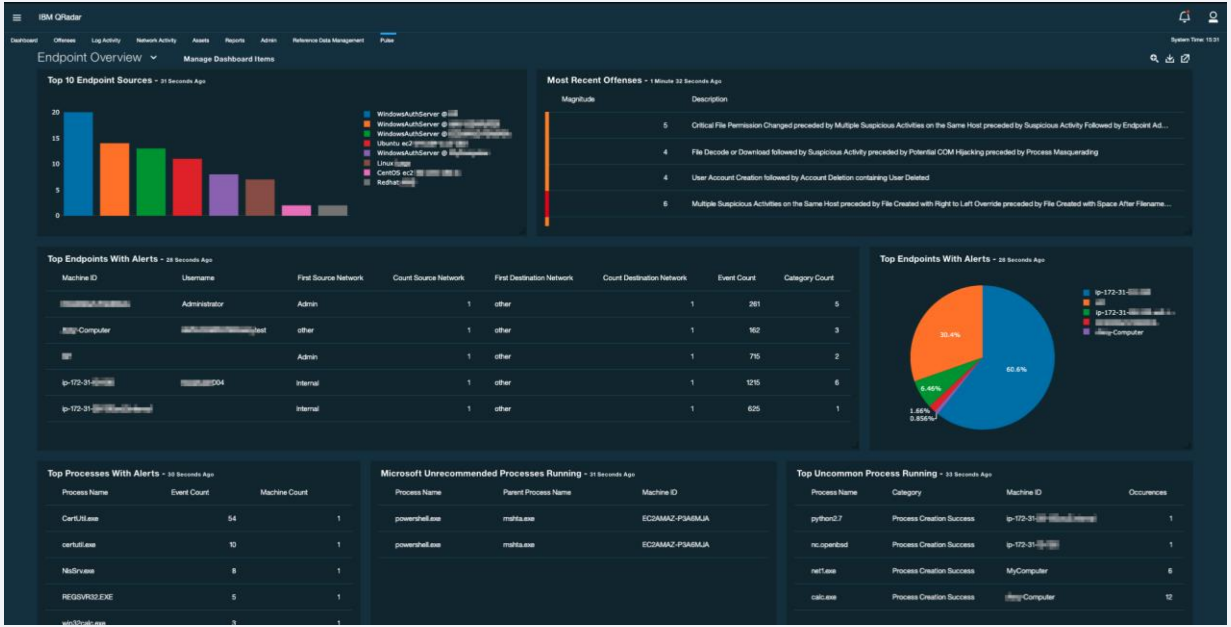
Use the **+Add Question** button to ask the panelists a question.

Common Questions

1. **Does the Endpoint Monitoring Content Extension include a Pulse dashboard?**
   Yes!

Endpoint Overview

- Top Endpoint Sources
- Most Recent Offenses
- Top Endpoints with Alerts
- Top Processes with Alerts
- Microsoft Unrecommended Processes Running
- Top Uncommon Processes Running



Top 10 Endpoint Sources - 31 Seconds Ago

Most Recent Offenses - 1 Minute 32 Seconds Ago

Magnitude	Description
5	Critical File Permission Changed preceded by Multiple Suspicious Activities on the Same Host preceded by Suspicious Activity Followed by Endpoint Ad...
4	File Decode or Download followed by Suspicious Activity preceded by Potential COM Hijacking preceded by Process Masquerading
4	User Account Creation followed by Account Deletion containing User Deleted
6	Multiple Suspicious Activities on the Same Host preceded by File Created with Right to Left Override preceded by File Created with Space After Filename...

Top Endpoints With Alerts - 28 Seconds Ago

Machine ID	Username	First Source Network	Count Source Network	First Destination Network	Count Destination Network	Event Count	Category Count
[redacted]	Administrator	Admin	1	other	1	261	5
[redacted]-Computer	[redacted]test	other	1	other	1	162	3
[redacted]		Admin	1	other	1	715	2
ip-172-31-[redacted]	[redacted]D04	Internal	1	other	1	1215	6
ip-172-31-[redacted]		Internal	1	other	1	625	1

Top Endpoints With Alerts - 28 Seconds Ago

Top Processes With Alerts - 30 Seconds Ago

Process Name	Event Count	Machine Count
CertUtil.exe	54	1
certutil.exe	10	1
NisSrv.exe	8	1
REGSVR32.EXE	5	1
win32calc.exe	3	1

Microsoft Unrecommended Processes Running - 31 Seconds Ago

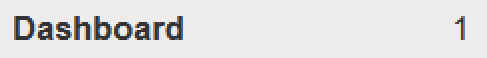
Process Name	Parent Process Name	Machine ID
powershell.exe	mshta.exe	EC2AMAZ-P3A6MJA
powershell.exe	mshta.exe	EC2AMAZ-P3A6MJA

Top Uncommon Process Running - 33 Seconds Ago

Process Name	Category	Machine ID	Occurences
python2.7	Process Creation Success	ip-172-31-[redacted]	1
nc.openbsd	Process Creation Success	ip-172-31-[redacted]	1
net1.exe	Process Creation Success	MyComputer	6
calc.exe	Process Creation Success	[redacted]-Computer	12

Common Questions (continued)

2. **Do all content extensions include dashboards?**
   No, there are some older content extensions that do not include Pulse dashboards. The contents list on the X-Force App Exchange identifies if an extension contains a dashboard.



Dashboard	1

3. **If I reinstall QRadar, do I need to reinstall my content extensions?**
   Rules, custom properties, searches, and other packaged information are included in the nightly configuration backup on the QRadar Console. When you restore your QRadar Console’s configuration backup, the content is available for use.

4. **What happens when I uninstall a content extension?**
   It depends on your QRadar version. As of QRadar 7.3.3 and later, all content is removed, including reference sets added by the content extension. In QRadar 7.3.2, rules and custom properties added by content extensions are removed during uninstall.

5. **Can I download older content extensions?**
   No, older content extensions are replaced on the IBM X-Force App Exchange. Users can download the latest available version.

6. **We use QRadar on Cloud, are content extensions available?**
   Yes, all content extensions can be installed on QRadar on Cloud.

Common Questions (continued)

7. **What content extensions are installed by default in QRadar?**
   In QRadar 7.4.1 more custom properties are available by default, but no extensions are installed by default.

8. **Are there any content extensions that are considered 'must have'?**
   There are currently ~70 content extensions available for QRadar.
   - Baseline Maintenance (merged into software updates)
   - IBM Security Threat Content
   - IBM QRadar Security Analytics Self Monitoring
   - IBM QRadar Custom Properties for Linux
   - IBM QRadar Custom Properties for Windows

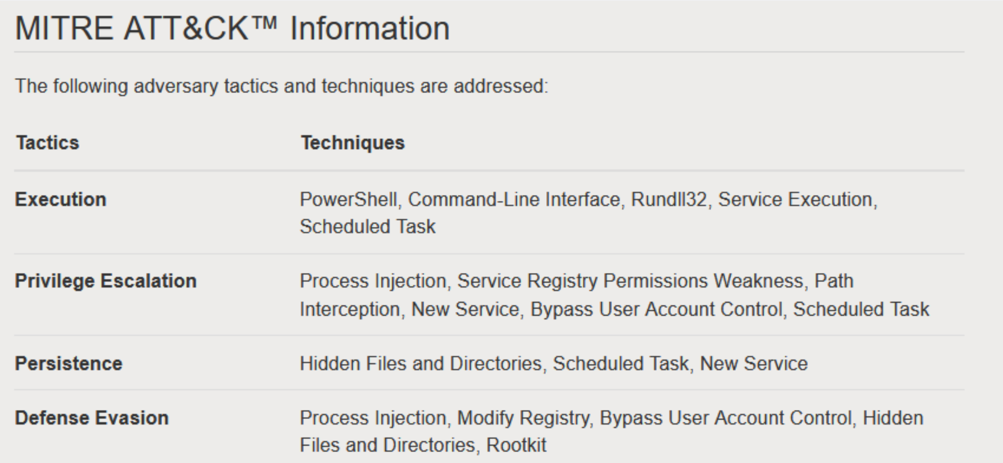
   Depending on event sources:
   - Amazon AWS Content Extension
   - Custom Properties for Microsoft Exchange
   - Microsoft Azure

9. **Can I edit a rule, search, or other content added by an extension?**
   Yes, all content added by extensions can be modified. When rules are added, they are owned by SYSTEM, when users modify a rule, it creates a copy under their username. Administrators should be careful when modifying custom properties to understand the impact to other users and performance.

Common Questions (continued)

10. **We use the Mitre ATT&CK framework, can I view content by tactics?**
Yes, the X-Force App Exchange was updated to include Mitre ATT&CK mapping information. This information is also made available in the QRadar Use Case Manager application for users to understand rule coverage and where they might have gaps.

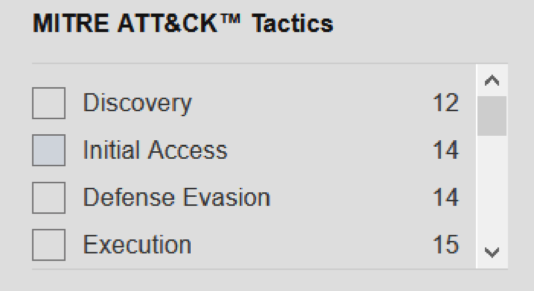
The Use Case Manager app is a default application installed with your QRadar 7.4.1 software update.



MITRE ATT&CK™ Information

The following adversary tactics and techniques are addressed:

Tactics	Techniques
Execution	PowerShell, Command-Line Interface, Rundll32, Service Execution, Scheduled Task
Privilege Escalation	Process Injection, Service Registry Permissions Weakness, Path Interception, New Service, Bypass User Account Control, Scheduled Task
Persistence	Hidden Files and Directories, Scheduled Task, New Service
Defense Evasion	Process Injection, Modify Registry, Bypass User Account Control, Hidden Files and Directories, Rootkit



MITRE ATT&CK™ Tactics

□	Discovery	12
□	Initial Access	14
□	Defense Evasion	14
□	Execution	15

Common Questions (continued)

11. **When updating a content extension to a newer version, I was prompted to ‘Overwrite’ or ‘Keep existing data’. What do I select?**

    The 'Overwrite' option basically means that all content items in the extension will be imported. Anything marked 'ADD' in the preview is net new to the system, so will be simply added. Anything marked 'REPLACE" is already present on the system, and will be swapped out for the new version of the content bundled in the extension.

    For any other content types (saved searches, report templates, custom properties, etc), if you know you've modified any IBM-provided ones, and you see those same items listed in an extension preview, marked as REPLACE, you need to be aware that if you choose the 'Overwrite' option, you will lose those customizations. Support often recommends that users create a copy of those items before proceeding, or just choose the 'Keep existing data' option to preserve your modifications.

IBM QRadar Endpoint Content Extension

Enhancements and Support

Submitting enhancements

Requests for enhancements (RFEs) allow users to submit features to QRadar Offering teams and product owners for review.

Procedure

1. To submit an enhancement: http://ibm.biz/qradarrfesubmit
2. Component = Content Packs
3. Fill out each section
4. Enable public or keep private
5. Enabled voting (if public)

What to include in every RFE

- A description of the request
- Your security use case
- Impact on your business and deliverables

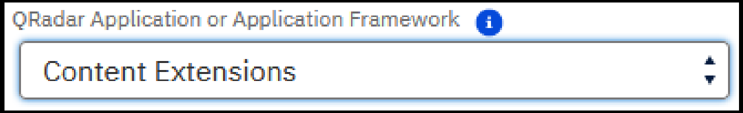
What to include for content requests

- Description of collection gap or rules
- Event logs and product versions
- Information for expected functionality or results
- Case number if you have an open case with QRadar Support

Getting help

Content extensions are fully supported by the QRadar team. Users or admins can open cases related to extensions.

1. To submit a case: https://www.ibm.com/mysupport
2. Select QRadar SIEM.
3. Select your account.
4. Under **QRadar Application or Application Framework**, select **Content Extensions**.



QRadar Application or Application Framework

Content Extensions

What to include in your case

- A description of the issue
- Version of the content extension
- The text from the rule or a screen capture
- The payload from the event that triggered the rule
- If performance related, include logs from the QRadar appliance

IBM QRadar Endpoint Content Extension

Reference Information

Endpoint Monitoring: Building Blocks

BB:BehaviorDefinition

- Admin Privileges Added (Unix)
- Admin Privileges Added (Windows)
- Admin Privileges Removed (Windows)
- Component Object Model Hijacking
- Component Object Model Hijacking Rules
- Critical Security Tool Process Information
- Download Utilities in Events
- Group or Account Discovery
- Hidden File or Folder Created
- Password Policy Discovery (Unix)
- Password Policy Discovery (Windows)
- PowerShell File Download Activity
- Process Killed
- Regular Endpoint Administration
- Run as Superuser or Another User (Unix)
- Run as Superuser or Another User (Windows)
- Suspicious Endpoint Activities
- User Account Added (Unix)
- User Account Added (Windows)
- User Account Deleted (Unix)
- User Account Deleted (Windows)

BB:CategoryDefinition

- File Decode by a Utility
- File Permission Changed
- Files with Sensitive Permissions

BB:DeviceDefinition

- Operating System

Endpoint Monitoring: Rules

- Communication with a Potential Hostile Host
- Communication with a Potential Hostile IP Address
- Credential Dumping Activities Discovered
- Critical File Permission Changed (Unix)
- Critical Security Tool Killed (Unix)
- Critical Security Tool Stopped
- Detection of Malicious IOC
- File Created with Space After Filename
- File Created with Right to Left Override
- File Decode or Download followed by Suspicious Activity
- Potential Component Object Model (COM) Hijacking
- Potential DLL Hijacking
- Potential Malicious Application Shimming
- Process Masquerading (Unix)
- Process Masquerading (Windows)
- Programming Environment Spawned by a Suspicious Process
- Recommended Blocked Process is Running
- Suspicious Activity Followed by Endpoint Administration Task
- User Account Creation followed by Account Deletion

Endpoint Monitoring: Reference Sets

- Default Process Name and Process Directories
- Anonymizer IPs
- Botnet C&C IPs
- Botnet IPs
- Critical Security Tool Processes
- Malicious URLs
- Malware Hashes MD5
- Malware Hashes SHA
- Malware IPs
- Malware URLs
- Phishing IPs
- Phishing URLs
- Recommended Blocked Processes
- Sensitive Process Names
- Shims Allowlist
- Pulse_imports

Endpoint Monitoring: Custom Properties

Name	**Optimized**
Application	Yes
Architecture	Yes
Audit ID	Yes
Call Type	Yes
Command Arguments	Yes
Encoded File Directory	Yes
Encoded Filename	Yes
File Directory	Yes
File Extension	Yes
File Permissions	Yes
Filename	Yes
Group Name	Yes
Machine ID	Yes
MD5 Hash	No

Name	**Optimized**
Parent Process Name	Yes
Process CommandLine	Yes
Process Name	Yes
Process Path	Yes
Record Number	No
Registry Key	Yes
Registry Value Data	Yes
Rule Name	Yes
SHA256 Hash	Yes
Target User Name	Yes
Token Elevation Type	Yes
UrlHost	Yes
User ID	Yes

Endpoint Monitoring: MITRE ATT&CK™ Information

Tactic	Techniques
Command and Control	(No techniques selected)
Credential Access	Credential Dumping, Credentials in Registry, Account Manipulation
Discovery	Query Registry, Password Policy Discovery, Permission Groups Discovery, Account Discovery
Defense Evasion	Modify Registry, File and Directory Permissions Modification, Disabling Security Tools, Obfuscated Files or Information, Space after Filename, Deobfuscate/Decode Files or Information, Component Object Model Hijacking, DLL Search Order Hijacking, Masquerading, Rundll32, Regsvr32, Mshta, BITS Jobs, Hidden Files and Directories, Bypass User Account Control
Privilege Escalation	Service Registry Permissions Weakness, DLL Search Order Hijacking, Application Shimming, Valid Accounts, Bypass User Account Control
Collection	Data from Local System
Persistence	Component Object Model Hijacking, DLL Search Order Hijacking, Application Shimming, Account Manipulation, Create Account, Hidden Files and Directories
Execution	Rundll32, Regsvr32, Mshta, PowerShell, Command-Line Interface

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM