Enterprise Endpoint Compromise Analysis

By: Ritvik Indupuri
Date: 10/20/2025

1. Executive Summary

An investigation was conducted into a multi-stage intrusion that began with a successful MFA fatigue attack leveraging compromised srogers credentials. The adversary established an initial foothold on workstation TOT-TAPIR-DT using wmiexec.py-style execution to create a persistent local user and perform internal reconnaissance. The threat actor then moved laterally to the domain controller FUTURE-DC using noisy, psexec.py-like techniques and executed commands to download additional tooling. The complete attack path was reconstructed with high fidelity by correlating Falcon EDR telemetry with targeted LogScale queries that filtered investigative noise.

2. Investigation & Evidence Highlights

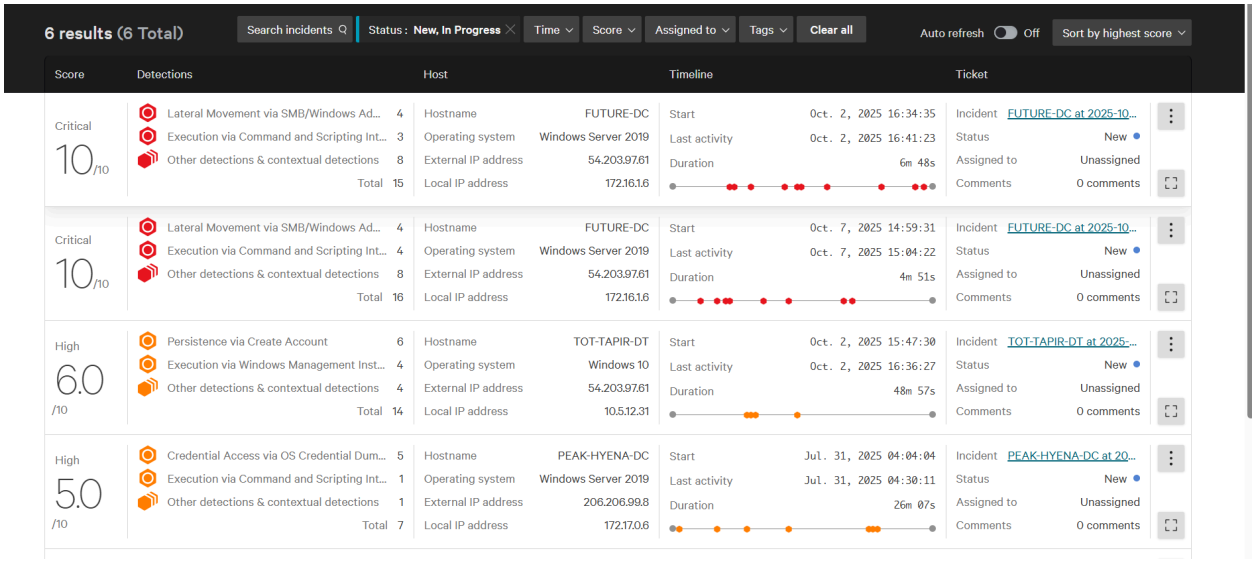

Figure 1: Global Incident Dashboard

The primary incident dashboard provides an immediate overview of the attack's breadth, displaying multiple high-severity incidents across the environment, including critical-level lateral movement alerts on FUTURE-DC and the initial persistence on TOT-TAPIR-DT.

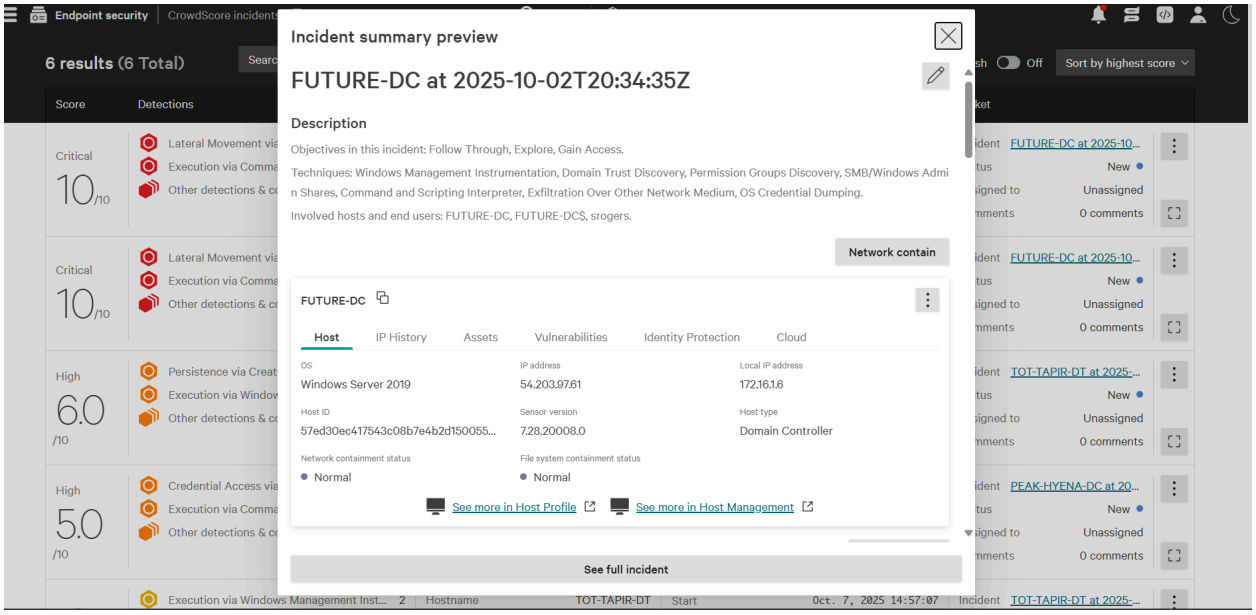

Figure 2: Incident Summary Preview for FUTURE-DC

Pivoting to a critical alert on the domain controller, the incident summary for FUTURE-DC details the attack objectives ("Follow Through, Explore, Gain Access") and the MITRE ATT&CK® techniques involved, such as WMI, SMB, and Credential Dumping.

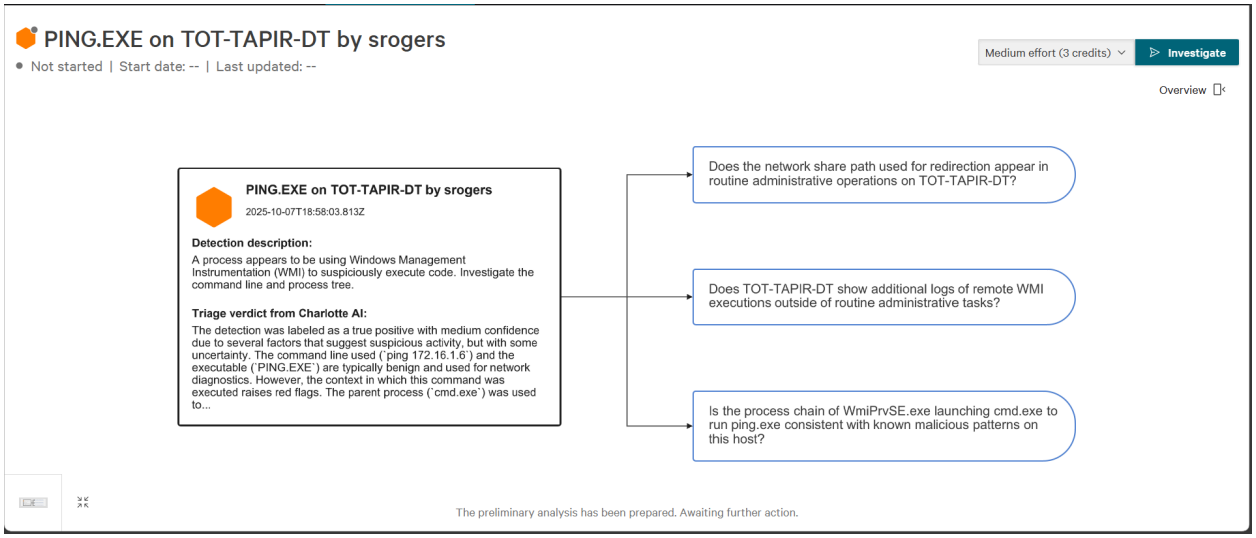

Figure 3: Charlotte AI Triage of Initial Execution (TOT-TAPIR-DT)

The initial suspicious activity on TOT-TAPIR-DT is detailed in a Charlotte AI triage card. It correctly identifies the anomalous execution of PING.EXE via a WMI process, rating it a true positive and confirming the use of wmiexec-style remote execution.

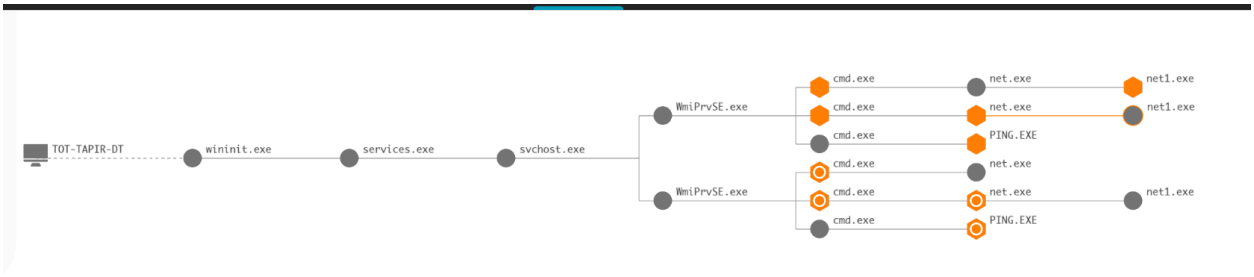

Figure 4: Process Graph of WMI Execution Flow (TOT-TAPIR-DT)

This process graph provides definitive visual evidence of the execution chain on TOT-TAPIR-DT. It clearly shows WmiPrvSE.exe executing multiple cmd.exe instances for net.exe (persistence) and ping.exe (discovery) commands.

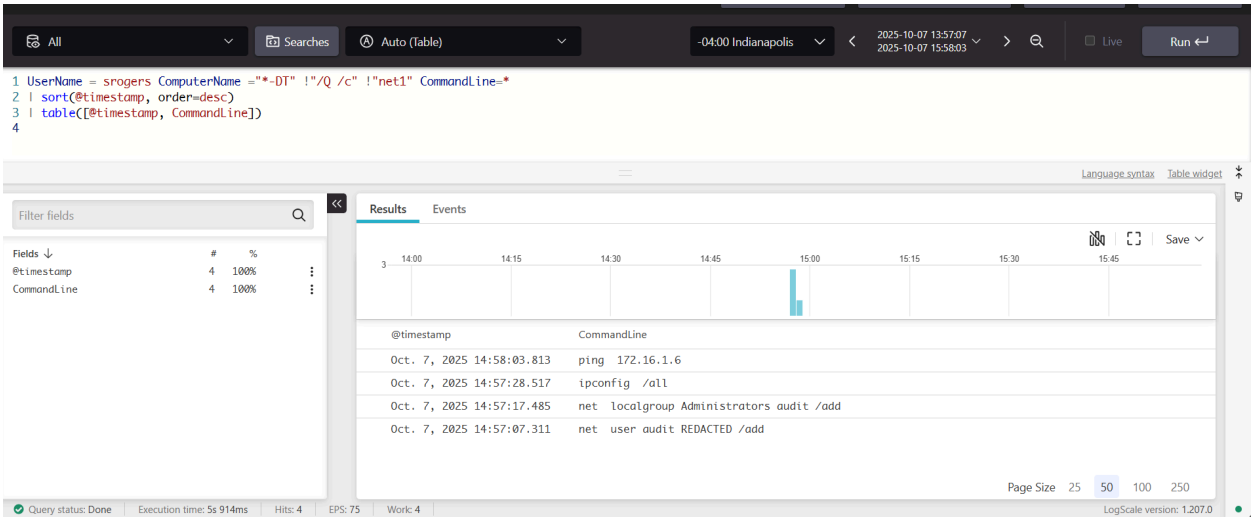

Figure 5: LogScale Query - Persistence & Recon (TOT-TAPIR-DT)

A LogScale query confirms the adversary's command line history on the initial host. The query below provides direct evidence of local account creation (net user audit), privilege escalation (net localgroup), and network discovery (ipconfig /all, ping).

```
UserName = srogers ComputerName ="*-DT" !"/Q /c" !"net1" CommandLine=*
| sort(@timestamp, order=desc)
| table([@timestamp, CommandLine])
```

Figure 6: LogScale Query used for Persistence & Recon (TOT-TAPIR-DT)

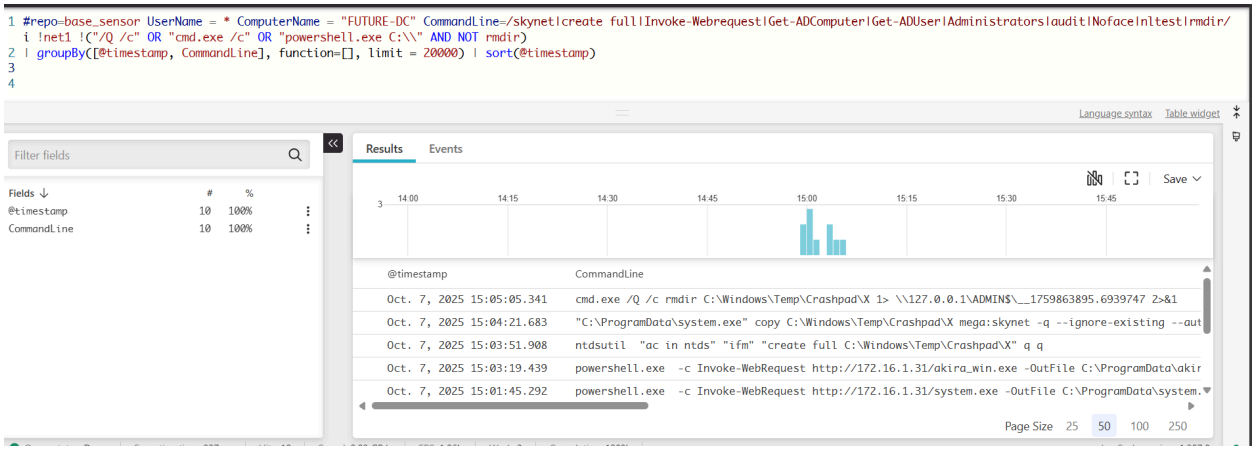

Figure 6: LogScale Query - Actions on Objective (FUTURE-DC)

A second, more complex query filters out psexec and wmiexec noise on the domain controller to reveal the adversary's follow-on actions. The results show the use of powershell.exe with Invoke-WebRequest to download additional tooling and ntdsutil for potential credential dumping.

```
#repo=base_sensor UserName = * ComputerName = "FUTURE-DC"
CommandLine=/skynet|create
full|Invoke-Webrequest|Get-ADComputer|Get-ADUser|Administrators|audit|
Noface|nltest|rmdir/i
!net1 !("/Q /c" OR "cmd.exe /c" OR "powershell.exe C:\\" AND NOT
rmdir)
| groupBy([@timestamp, CommandLine], function=[], limit = 20000)
| sort(@timestamp)
```

3. Analytical Summary & MITRE ATT&CK® Mapping

Tactic	Technique & ID	Host	Evidence
Execution	Windows Management Instrumentation (T1047)	TOT-TAPIR-DT	WmiPrvSE.exe spawning cmd.exe for remote execution. (Figure 3, Figure 4)
Persistence	Create Account: Local Account (T1136.001)	TOT-TAPIR-DT	net user audit /add command confirmed in LogScale. (Figure 5)
Privilege Escalation	Valid Accounts: Local Accounts (T1078.001)	TOT-TAPIR-DT	net localgroup Administrators audit /add command. (Figure 5)
Discovery	System Information Discovery (T1082)	TOT-TAPIR-DT	ipconfig /all for network configuration details. (ure 5)
Discovery	Network Service Discovery (T1046)	TOT-TAPIR-DT	ping command used to identify the Domain Controller. (Figure 4, Figure 5)
Lateral Movement	Service Execution (T1569.002)	FUTURE-DC	Noisy service creation consistent with psexec.py tooling. (Figure 1, Figure 2)
Command & Control	Ingress Tool Transfer (T1105)	FUTURE-DC	Invoke-WebRequest used to download additional tooling. (Figure 6)

4. Conclusion

This analysis provides a definitive reconstruction of the adversary's modus operandi, from initial access via MFA fatigue to lateral movement with Impacket tooling. The investigation successfully correlated noisy EDR telemetry with targeted LogScale queries to validate the full attack chain, confirming the adversary's lifecycle from compromise on a workstation to actions-on-objective on a domain controller. The findings confirm the platform's ability to provide the comprehensive visibility required to trace and stop a sophisticated breach.
