

Threat attack simulation certificate

System compromise 2025 — Windows — CrowdStrike Falcon EDR · Simulation S1

A

GLOBAL GRADE
23 events executed

MTTD

<1 min

first alert after execution

MTTR

1 min

reaction on alerted events

DURATION

37 min

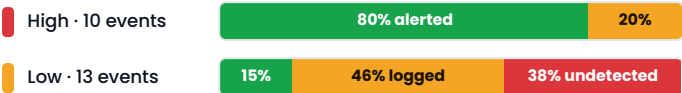
2026/02/18 07:10 → 07:47 UTC

MTTD and MTTR are computed on events with the Alerted status, and only where detection and reaction timestamps have been provided.

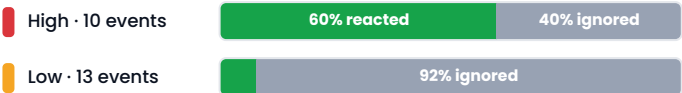
>_ Detection & reaction performance



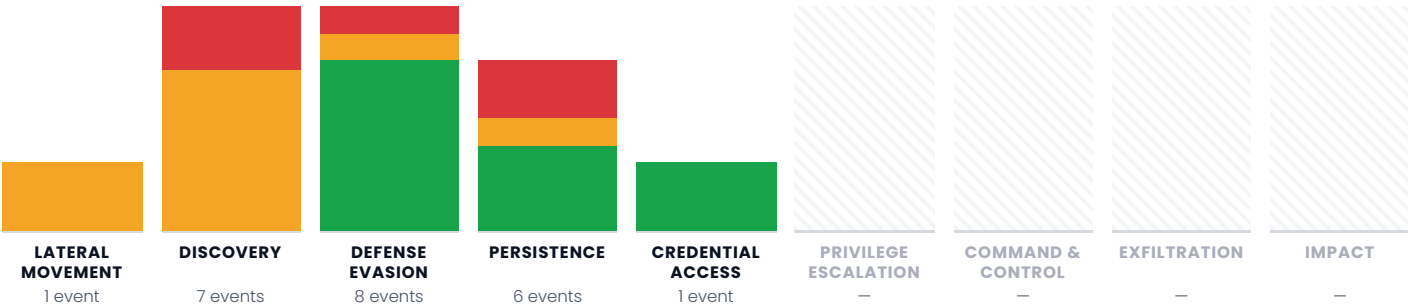
>_ DETECTION PER SEVERITY



>_ REACTION PER SEVERITY



>_ Detection compliance based on MITRE ATT&CK



>_ MITRE ATT&CK coverage — 5 tactics, 23 events

1
LATERAL MOVEMENT
T1021.006

7
DISCOVERY
T1087.001 · T1124 · T1033 · T1012 · T1518.001 · T1615 · T1497.001

8
DEFENSE EVASION
T1564.001 · T1112 · T1562.001 · T1562.002 · T1562.004 · T1548.002 · T1070.001

6
PERSISTENCE
T1547.004 · T1547.005 · T1037.001 · T1546.009 · T1546.013

1
CREDENTIAL ACCESS
T1003.001

>_ Simulation details

Scenario	System compromise 2025 — Windows — powershell [WMI]
Events executed	23
Execution window	2026/02/18 07:10:08 → 07:47:24 UTC
Duration	00:37:16
Target type	Industrial infra
Perimeter	#DEMO# windows-dc / Azure (domain admin) [with EDR]

>_ Reference

Company	Erium-demo
Campaign	System compromise 2025 Windows — CrowdStrike Falcon EDR
Simulation ID	S1. 583acdcc-6c65-45ba-bc18-c820603eeb97
Delivered on	2026/08/25 03:14 UTC
Issued by	Arnaud Le Men

N°	EVENT	MITRE TACTIC	EXECUTION	DETECTION
001	 Session Creation: WMI Password Authentication	Lateral Movement	Executed	Logged
002	 Account Discovery: Local Account (WMI/Powershell)	Discovery	Executed	Logged
003	 System Time Discovery (WMI/Powershell)	Discovery	Executed	Undetected
004	 System Owner Discovery (WMI/Powershell)	Discovery	Executed	Logged
005	 Query Registry: AlwaysInstallElevated Key (WMI/Powershell)	Discovery	Executed	Logged
006	 Security Software Discovery: Firewall (WinRM/Powershell)	Discovery	Executed	Undetected
007	 Group Policy Discovery (WMI/Powershell)	Discovery	Executed	Logged
008	 Virtualization/Sandbox Evasion: System Checks (WMI/Powershell)	Discovery	Executed	Logged
009	 Hide Artifacts: Hide Folder (WMI/Powershell)	Defense Evasion	Executed	Undetected
010	 Modify Registry: Disable LSA Protection (WMI/Powershell)	Defense Evasion	Executed	Alerted
011	 Modify Registry: Enable Restricted Admin (WMI/Powershell)	Defense Evasion	Executed	Alerted
012	 Impair Defenses: Enable Remote Desktop (WMI/Powershell)	Defense Evasion	Executed	Alerted
013	 Impair Defenses: Disable System Firewall (WMI/Powershell)	Defense Evasion	Executed	Alerted
014	 System Binary Proxy Execution: Disable User Account Control (WMI/Powershell)	Defense Evasion	Executed	Alerted
015	 Persistence: Winlogon Helper Shell (WMI/Powershell)	Persistence	Executed	Alerted
016	 Boot or Logon Autostart Execution: Security Support Provider (WMI/Powershell)	Persistence	Executed	Alerted
017	 Persistence: Registry UserInitMprLogonScript Persistence (WMI/Powershell)	Persistence	Executed	Undetected
018	 Persistence: Registry Winlogon Helper Userinit (WMI/Powershell)	Persistence	Executed	Alerted
019	 Event Triggered Execution: AppCert DLLs (WMI/Powershell)	Persistence	Executed	Logged
020	 Event Triggered Execution: PowerShell Profile (WMI/Powershell)	Persistence	Executed	Undetected
021	 OS Credential Dumping: LSASS Memory via comsvcs (WMI/Powershell)	Credential Access	Executed	Alerted
022	 Impair Defenses: Disable CommandLine Auditing (WMI/Powershell)	Defense Evasion	Executed	Logged
023	 Indicator Removal: Clear Windows Event Logs (WMI/Powershell)	Defense Evasion	Executed	Alerted

 Alerted — the control raised an alert

 Logged — traced without alerting

 Undetected — no trace found

 High severity event

 Low severity event