INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-07 19:04 UTC

CrowdStrike Extends Managed Threat Hunting to Microsoft Defender Environments Amid 82% Malware-Free Intrusion Rate

SECURITY ANALYSIS | MEDIUM | CVSS 5.0

SCC Item ID	SCC-STY-2026-0115
Type	Security Analysis
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	CrowdStrike Falcon OverWatch for Defender; Microsoft Defender (enterprise deployments)
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike launched Falcon OverWatch for Defender on May 5, 2026, bringing human-led managed threat hunting to enterprises running Microsoft Defender as their primary endpoint platform. The launch is a direct response to a documented shift in adversary tradecraft: CrowdStrike's 2026 Global Threat Report found that 82% of intrusions in 2025 required no malware, instead relying on stolen credentials, legitimate system tools, and living-off-the-land techniques that automated detection consistently misses. For security leaders, this signals that endpoint protection platforms alone, regardless of vendor, are no longer sufficient against modern intrusion tradecraft, and that human expertise in the detection loop is increasingly a baseline expectation rather than a premium add-on.

Technical Analysis

The 82% malware-free intrusion statistic from CrowdStrike's 2026 Global Threat Report is not a marketing number, it reflects a sustained, measurable shift in how threat actors operate. Techniques like credential abuse (T1078), process injection (T1055), living-off-the-land binaries via the command line (T1059), lateral movement over legitimate remote services (T1021), and defense evasion through masquerading (T1036) and security tool impairment (T1562) do not produce the artifact signatures that behavioral engines are trained to flag. Threat actors tracked in CrowdStrike Falcon OverWatch intelligence have been associated with these identity- and tool-based intrusion patterns. Falcon OverWatch for Defender is designed to address the detection gap these techniques create. The service overlays CrowdStrike's human threat hunting team on top of Defender telemetry, allowing organizations standardized on Microsoft's endpoint stack to receive continuous expert analysis without replacing their agent. The architectural model is significant: rather than forcing a full EDR migration to access

managed hunting, the service meets organizations where their endpoint investment already sits. This reflects a broader industry recognition that the managed detection and response market is expanding beyond single-vendor ecosystems. The practical implication for security operations teams is that the question is no longer which EDR produces the best alert, it is whether any team has the human capacity and adversary context to act on weak behavioral signals before dwell time becomes damage.

Action Checklist

1. Step 1: Assess exposure, determine whether your organization runs Microsoft Defender as its primary endpoint protection platform, particularly across enterprise workloads where Falcon OverWatch for Defender would apply
2. Step 2: Review controls, audit your current detection coverage for malware-free intrusion techniques: credential-based access (T1078), LOLBIN abuse (T1059), lateral movement via remote services (T1021), and defense evasion (T1562, T1036); confirm whether your SIEM or EDR generates actionable alerts for these patterns or relies primarily on signature and malware detection
3. Step 3: Update threat model, incorporate the 82% malware-free intrusion rate as a baseline assumption in your threat model; map known malware-free intrusion TTPs against your environment using MITRE ATT&CK and assess whether existing detections cover these techniques
4. Step 4: Communicate findings, brief leadership on the gap between automated endpoint detection and identity- and tool-based intrusion tradecraft; frame managed hunting as a compensating control for environments where SOC analyst capacity or adversary context is limited
5. Step 5: Monitor developments, track CrowdStrike's Falcon OverWatch for Defender service documentation and the 2026 Global Threat Report for published indicators, hunting hypotheses, and technique-specific guidance relevant to Defender-standardized deployments

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent if queries against Windows Security Event Log, Sysmon, or Defender for Endpoint Advanced Hunting reveal active anomalous credential use (Event ID 4648, 4768/4769 off-hours or from non-standard hosts), LOLBIN process chains (certutil, mshta, or regsvr32 spawned by unexpected parent processes), or Defender tamper protection disable events (Event ID 5001/5007) — any of which indicates a malware-free intrusion consistent with SPIDER-cluster tradecraft may already be in progress rather than a prospective risk.
Recovery Notes	Because this threat class produces no malware artifacts, recovery validation must focus on identity and configuration integrity rather than malware removal: reset credentials for any accounts flagged during the detection gap audit, rotate Kerberos TGT (krbtgt account double-reset per Microsoft guidance) if lateral movement via pass-the-ticket cannot be ruled out, and restore Defender tamper protection and behavioral monitoring settings to baseline (verified against the registry snapshot captured in Step 1). Monitor Windows Security Event IDs 4624, 4648, 4768, and 4769 for 30 days post-remediation for recurrence of anomalous credential patterns, and validate that any new Sigma or Defender custom detection rules deployed as compensating controls are generating expected telemetry in your test environment before declaring recovery complete.

Forensic Artifacts	Windows Security Event Log — Event IDs 4624 (successful logon), 4648 (explicit credential logon), 4768/4769 (Kerberos TGT/service ticket requests): primary telemetry for T1078 credential-based access and pass-the-ticket lateral movement used by SPIDER-cluster adversaries operating without malware | Sysmon Event ID 1 (Process Create with full command line) filtered on known LOLBIN executables (wmic.exe, certutil.exe, mshta.exe, regsvr32.exe, cscript.exe, wscript.exe): direct forensic evidence of T1059 and T1036 abuse chains that malware-free intrusions rely on and that Defender signature detection cannot catch | Microsoft-Windows-Windows Defender/Operational Event Log — Event ID 5001 (real-time protection disabled) and Event ID 5007 (configuration changed): forensic evidence of T1562.001 defense evasion against Defender, a prerequisite step for SPIDER-cluster credential-based intrusions in Defender-standardized environments | PowerShell Operational Event Log — Event ID 4104 (Script Block Logging): captures obfuscated and de-obfuscated PowerShell payloads used in T1059.001 execution; absence of this log or gaps in the timeline are themselves forensic indicators of log tampering or logging misconfiguration exploited during the intrusion | Defender for Endpoint Advanced Hunting DeviceLogonEvents and DeviceProcessEvents tables (if MDE Plan 2 licensed): the most complete forensic source for reconstructing malware-free intrusion timelines in Defender environments, specifically correlating credential reuse events to subsequent LOLBIN process execution and remote service lateral movement (T1021) within the same adversary session

Per-Action IR Details

Step 1: Assess exposure — determine whether your organization runs Microsoft Defender as its primary endpoint protection platform, particularly across enterprise workloads where Falcon OverWatch for Defender would apply

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establish IR capability and assess environment posture before incidents occur

Controls: NIST IR-4 (Incident Handling) — ensure handling capability covers identity- and tool-based intrusion, not only malware events, NIST IR-8 (Incident Response Plan) — IR plan must account for detection gaps specific to Defender-only environments lacking behavioral hunting coverage, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — inventory must identify which enterprise workloads are protected solely by Microsoft Defender versus augmented EDR, CIS 2.2 (Ensure Authorized Software is Currently Supported) — confirm Defender is fully licensed for enterprise features (Defender for Endpoint Plan 2) that enable behavioral telemetry required for LOLBIN and credential-abuse detection

Compensating: Run the following PowerShell one-liner on a domain controller or via MECM/Intune query to enumerate endpoints reporting Defender as their active AV engine and confirm Plan tier: `Get-MpComputerStatus | Select-Object -Property AMProductVersion, AMServiceEnabled, BehaviorMonitorEnabled, RealTimeProtectionEnabled`. Export results to CSV and cross-reference against your asset inventory to identify workloads with BehaviorMonitorEnabled=False, which are blind to LOLBIN chains. For cloud-joined devices, use `az security atp setting show` (Azure CLI) to confirm Defender for Endpoint integration status.

Evidence: Before assessing coverage gaps, capture the current Defender configuration baseline: export `HKLM\SOFTWARE\Microsoft\Windows Defender\Features` registry hive to document tamper protection and behavioral monitoring state; pull `Microsoft-Windows-Windows Defender/Operational` event log (Event ID 5007 = configuration change, Event ID 5001 = real-time protection disabled) to establish whether Defender settings have been modified prior to your audit — a precursor indicator of defense evasion (T1562.001) by an adversary already present.

Step 2: Review controls — audit your current detection coverage for malware-free intrusion techniques: credential-based access (T1078), LOLBIN abuse (T1059), lateral movement via remote services (T1021), and defense evasion (T1562, T1036); confirm whether your SIEM or EDR generates actionable alerts for these patterns or relies primarily on signature and malware detection

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Validate detection tooling and logging infrastructure against known adversary tradecraft before incidents occur

Controls: NIST SI-4 (System Monitoring) — monitoring must extend beyond malware signatures to cover credential misuse, LOLBIN execution chains, and remote service lateral movement characteristic of the 82% malware-free intrusion pattern, NIST AU-2 (Event Logging) — event logging configuration must capture process creation with full command lines, PowerShell script block logging, and WMI activity to detect T1059 and T1021 abuse, NIST AU-12 (Audit Record Generation) — confirm Defender for Endpoint or Sysmon is generating process lineage records sufficient to reconstruct LOLBIN execution chains (e.g., wmic.exe, certutil.exe, mshta.exe spawned by Office or browser processes), CIS 8.2 (Collect Audit Logs) — audit logs must be collected from Windows Security, PowerShell, and Sysmon sources to cover the credential-based and living-off-the-land techniques documented in CrowdStrike's 2026 Global Threat Report, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — detection gap assessment is a formal input to vulnerability and risk management; document LOLBIN and credential-abuse detection gaps as control deficiencies

Compensating: Deploy Sysmon with SwiftOnSecurity's config (https://github.com/SwiftOnSecurity/sysmon-config) to generate Event ID 1 (Process Create with command line), Event ID 3 (Network Connect), and Event ID 10 (Process Access — credential theft via LSASS). Load the Sigma rule set for LOLBIN detection (specifically rules tagged `attack.execution.t1059` and `attack.defense_evasion.t1562`) into a free ELK stack or Graylog instance. To test T1078 coverage, run `Get-WinEvent -LogName Security -FilterXPath "*[System[EventID=4624] and EventData[Data[@Name='LogonType']='3']]"` to confirm network logon events are being captured — the primary telemetry source for credential-based lateral movement.

Evidence: Capture the following before remediating gaps: (1) PowerShell `Get-WinEvent -LogName 'Microsoft-Windows-PowerShell/Operational'` for Event ID 4104 (Script Block Logging) to baseline current PowerShell visibility; (2) check whether `HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging` is enabled — absence means T1059.001 activity is invisible; (3) pull Defender for Endpoint's DeviceProcessEvents table (if MDE Advanced Hunting is licensed) filtered on InitiatingProcessFileName in ('wmic.exe','certutil.exe','mshta.exe','regsvr32.exe') to identify any pre-existing LOLBIN execution that automated alerts missed.

Step 3: Update threat model — incorporate the 82% malware-free intrusion rate as a baseline assumption in your threat model; map CORDIAL SPIDER, SNARKY SPIDER, and COOKIE SPIDER TTPs against your environment using MITRE ATT&CK and assess whether existing detections cover their known techniques

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: Integrate cyber threat intelligence into event analysis and maintain situational awareness of adversary tradecraft relevant to the environment

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — CrowdStrike's 2026 Global Threat Report and Falcon OverWatch for Defender launch documentation constitute authoritative threat advisories that must be formally ingested and acted upon, NIST RA-3 (Risk Assessment) — threat model update incorporating CORDIAL SPIDER, SNARKY SPIDER, and COOKIE SPIDER TTP profiles constitutes a formal risk assessment activity; document residual risk where detections do not cover known techniques, NIST IR-4 (Incident Handling) — incident handling capability must be updated to include hunting hypotheses derived from SPIDER-cluster TTPs, not only reactive alert triage, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — threat model refresh is a required input to the vulnerability management process, particularly for technique-based gaps not captured by CVE scoring

Compensating: Use MITRE ATT&CK Navigator (free, browser-based at https://mitre-attack.github.io/attack-navigator/) to build a layer for each SPIDER adversary cluster. For COOKIE SPIDER (known for credential harvesting and phishing-to-persistence chains), prioritize T1078 (Valid Accounts), T1566 (Phishing), and T1547 (Boot/Logon Autostart). For CORDIAL SPIDER and SNARKY SPIDER, cross-reference any published CrowdStrike or third-party reporting against the ATT&CK technique matrix and color-code coverage gaps red. Export the gap list and convert to a Sigma rule backlog — each uncovered technique becomes a rule request. This is achievable by a 2-person team in a half-day sprint using only open-source tooling.

Evidence: Prior to threat model finalization, pull the following hunt data to validate whether SPIDER-cluster activity is already present: (1) Windows Security Event ID 4648 (Logon with explicit credentials) — a primary indicator of T1078

credential reuse; (2) Event ID 4768/4769 (Kerberos TGT/Service ticket requests) filtered for anomalous service accounts or off-hours requests indicative of pass-the-ticket lateral movement; (3) Defender for Endpoint DeviceLogonEvents filtered on LogonType='Network' with IsLocalAdmin=True — a high-fidelity indicator of credential-based privileged access without malware; (4) check for persistence artifacts in `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and scheduled tasks under `C:\Windows\System32\Tasks` for entries created by LOLBIN processes, consistent with SPIDER-cluster post-exploitation patterns.

Step 4: Communicate findings — brief leadership on the gap between automated endpoint detection and identity- and tool-based intrusion tradecraft; frame managed hunting as a compensating control for environments where SOC analyst capacity or adversary context is limited

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establish organizational support, resource allocation, and communication channels for IR capability before incidents occur

Controls: NIST IR-8 (Incident Response Plan) — IR plan must document the detection gap between signature-based Defender alerting and the behavior-based hunting required to catch malware-free intrusions; leadership briefing validates organizational acceptance of residual risk or authorizes compensating controls, NIST IR-6 (Incident Reporting) — reporting structures must include upward communication of systemic detection capability gaps, not only active incident status, NIST CA-7 (Continuous Monitoring) — continuous monitoring strategy must be updated to reflect that 82% of intrusions will not generate traditional malware alerts; leadership must authorize monitoring scope expansion to include identity telemetry and LOLBIN behavioral analytics, CIS 7.2 (Establish and Maintain a Remediation Process) — the detection gap identified in Steps 1-3 must enter a formal risk-based remediation process with documented ownership, timeline, and leadership sign-off

Compensating: Prepare a one-page executive brief using the following quantified framing: 'CrowdStrike's 2026 Global Threat Report documents that 82% of observed intrusions used no malware — meaning our current Defender signature-based detection would generate zero alerts for the majority of active adversary campaigns. Managed threat hunting adds a human analytical layer that correlates credential reuse (Event ID 4624/4648), LOLBIN execution chains (Sysmon Event ID 1), and lateral movement (Event ID 4771/4776) into adversary narratives that automated rules cannot construct.' Attach the ATT&CK Navigator gap layer from Step 3 as a visual aid. No budget for managed hunting? Document the decision and residual risk in writing with a named owner — this creates the audit trail required by NIST IR-8 and satisfies GRC obligations without requiring immediate spend.

Evidence: Before the leadership briefing, compile quantitative evidence from your own environment to ground the discussion: run a 30-day query against your SIEM or Defender for Endpoint Advanced Hunting for alerts tagged only as behavioral (no malware hash) versus signature-based — the ratio directly mirrors the 82% finding and makes the gap concrete rather than theoretical. If no SIEM exists, pull `Get-WinEvent -LogName Security | Where-Object {$_.Id -in 4624,4648,4768,4769} | Group-Object Id | Select-Object Name, Count` to show the volume of credential-event telemetry currently uncorrelated by any hunting capability.

Step 5: Monitor developments — track CrowdStrike's Falcon OverWatch for Defender service documentation and the 2026 Global Threat Report for published indicators, hunting hypotheses, and technique-specific guidance relevant to Defender-standardized deployments

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Use lessons learned and threat intelligence to improve detection capabilities and update IR procedures continuously

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — establish a formal process to ingest CrowdStrike threat intelligence publications, CISA advisories referencing SPIDER-cluster activity, and Falcon OverWatch for Defender release notes as authoritative external threat feeds, NIST IR-4 (Incident Handling) — IR playbooks for credential-based intrusion and LOLBIN abuse must be versioned and updated as CrowdStrike publishes new SPIDER-cluster technique profiles and Defender-specific hunting hypotheses, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — hunting hypotheses derived from new threat intelligence must be operationalized as recurring log review procedures or Sigma rules, not filed as static documents, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — threat intelligence monitoring feeds directly into the vulnerability management process by surfacing new technique-based detection gaps before they are exploited

Compensating: Subscribe to the following free intelligence streams to track SPIDER-cluster activity and Defender-specific hunting guidance without a paid TIP: (1) CISA Known Exploited Vulnerabilities catalog RSS feed for any LOLBIN or credential-abuse techniques receiving emergency directives; (2) MITRE ATT&CK TAXII feed (`https://cti-taxii.mitre.org/taxii/`) consumable by free OpenCTI or MISP instances to receive structured TTP updates for SPIDER-cluster group objects as CrowdStrike and partners publish them; (3) Sigma HQ GitHub repository (`https://github.com/SigmaHQ/sigma`) — watch for new rules tagged `attack.credential_access`, `attack.defense_evasion`, and `attack.lateral_movement` that operationalize emerging SPIDER TTPs into Defender-compatible detection logic. Assign one analyst to a weekly 30-minute review cycle and log findings in a shared ticketing system.

Evidence: As part of ongoing monitoring, maintain a running artifact collection task: (1) archive CrowdStrike 2026 Global Threat Report IOCs (domain patterns, user-agent strings, named pipe patterns used by SPIDER clusters) into your local MISP or a flat YARA rule file for Defender custom indicators; (2) track Defender for Endpoint custom detection rule version history in your change management system — each new hunting hypothesis from OverWatch documentation should produce a versioned custom detection rule update; (3) log Event ID 5007 (Defender configuration change) on all endpoints to detect any tampering with behavioral monitoring settings between intelligence review cycles, consistent with T1562.001 defense evasion used by malware-free adversaries to blind Defender before credential-based lateral movement.

Detection Guidance

Given the MITRE techniques associated with this story, hunting focus should concentrate on identity and tooling abuse rather than malware artifacts. Key areas: review authentication logs for anomalous credential use patterns consistent with T1078 (valid accounts), including off-hours access, unfamiliar source IPs, and service account activity outside normal baselines. Monitor process creation logs for T1059 interpreter chains (PowerShell, cmd, WMI, cscript) spawned from unusual parent processes or with encoded command lines. Audit remote service activity (T1021) for lateral movement signatures, RDP, SMB, and WinRM sessions initiated from workstations rather than jump hosts. Check for T1055 process injection indicators: unexpected cross-process memory writes, suspicious thread creation in high-value processes. Review security tool logs for T1562 impairment attempts, registry modifications to Defender exclusions, service stop commands targeting security agents, or audit log clearing. Credential access attempts (T1003, T1110) should be correlated across endpoint and identity logs: LSASS access, brute-force patterns against Active Directory, and password spray signatures. Masquerading (T1036) hunts should flag binaries executing from non-standard paths or with names mimicking legitimate system tools. For teams running Defender, Microsoft Defender for Identity and Sentinel can supplement endpoint telemetry with identity and network context for several of these techniques.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to CrowdStrike 2026 Global Threat Report and Falcon OverWatch for Defender launch materials for published indicators`	CORDIAL SPIDER, SNARKY SPIDER, and COOKIE SPIDER technique-specific indicators associated with credential abuse, LOLBIN execution, and defense evasion; actual IOC values not published in available source material	LOW

Framework Mappings

MITRE-ATTACK

- **T1110** — Brute Force
- **T1055** — Process Injection
- **T1078** — Valid Accounts
- **T1548** — Abuse Elevation Control Mechanism
- **T1059** — Command and Scripting Interpreter
- **T1021** — Remote Services
- **T1036** — Masquerading
- **T1562** — Impair Defenses
- **T1003** — OS Credential Dumping

NIST-800-53R5

- **AC-7** — Unsuccessful Logon Attempts
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **CM-6** — Configuration Settings
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **AU-9** — Protection of Audit Information

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1110	Brute Force	Credential-Access
T1055	Process Injection	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1059	Command and Scripting Interpreter	Execution
T1021	Remote Services	Lateral-Movement
T1036	Masquerading	Defense-Evasion
T1562	Impair Defenses	Defense-Evasion
T1003	OS Credential Dumping	Credential-Access

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/crowdstrike-launches-falcon-...	T3
	https://www.investing.com/news/company-news/crowdstrike-launches-th...	T3
	https://itbrief.asia/story/crowdstrike-widens-quiltworks-launches-d...	T3
	https://smestreet.in/technology/crowdstrike-falcon-overwatch-for-de...	T3
CrowdStrike Falcon OverWatch for Defender Extends Managed ...	https://ir.crowdstrike.com/news-releases/news-release-details/crowd...	T3

Generated 2026-05-07 19:04 UTC by TJS Security Command Center