INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-03 13:21 UTC

AI-Accelerated Exploit Timelines Are Dismantling the Patch Window, Security Programs Must Restructure Now

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0106
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Enterprise vulnerability management programs broadly; CrowdStrike Falcon Platform referenced as defensive platform
Discovery Source	Rss:T1 Threatintel

Executive Summary

Frontier AI models are compressing the time from vulnerability disclosure to active exploitation toward near-real-time, according to CrowdStrike's 2026 Global Threat Report, which documents an 89% year-over-year increase in AI-enabled adversary attacks and a 42% increase in zero-days exploited before public disclosure. The fastest observed lateral movement breakout time fell to 27 seconds, a pace that renders traditional periodic-scanning and severity-backlog vulnerability management programs structurally obsolete. Organizations that do not shift to continuous exposure validation and exploitability-driven prioritization are operating with a response posture built for a threat tempo that no longer exists.

Technical Analysis

CrowdStrike's 2026 Global Threat Report identifies a structural inflection point in the vulnerability exploitation lifecycle: frontier AI (advanced large language models with autonomous agent capabilities) is collapsing the window between disclosure and weaponization to the point where it can no longer serve as a meaningful defensive buffer. The 89% year-over-year increase in AI-enabled adversary activity, combined with a 42% rise in zero-days exploited before public disclosure, means that for a growing category of vulnerabilities, the traditional patch window simply does not open. The 27-second lateral movement breakout time is the sharpest illustration of the operational tempo shift. At that speed, detection-and-response workflows predicated on human-reviewed alert queues, weekly scan cycles, and severity-sorted remediation backlogs cannot interrupt an intrusion before meaningful damage occurs.

The MITRE ATT&CK techniques associated with this threat pattern span the full attack lifecycle and map to the report's findings. Initial access is achieved through exploitation of public-facing applications (T1190), valid accounts (T1078), and brute force (T1110). Reconnaissance using active scanning (T1595) and network service discovery (T1046) precedes lateral movement. Credential access techniques including OS credential dumping (T1003) and account discovery (T1087) accelerate the breakout timeline. Exploitation of remote services (T1210) and client-side vulnerabilities (T1203) extend reach. Privilege escalation (T1068) and the use of alternate authentication material (T1550) sustain access. These are not novel techniques; what AI enables is their chaining and execution at machine speed, with adaptive decision-making between stages.

The CWE-level weaknesses implicated, missing authentication (CWE-306), improper access control (CWE-284), improper authentication (CWE-287), and improper privilege management (CWE-269), point to the structural gaps AI-accelerated exploitation is designed to find and chain. Attackers do not need novel techniques when foundational access control failures remain unaddressed at scale.

The report's defensive recommendation is a shift from periodic, severity-based vulnerability management to continuous exposure validation and exploitability-driven prioritization. This means integrating real-time exploitability signals (active exploitation evidence, proof-of-concept availability, attacker tooling indicators) rather than relying on CVSS base scores, which measure theoretical severity rather than operational exploitation probability. Exposure validation must be continuous because the threat side is operating continuously.

Note on source quality: The primary sources for this story are CrowdStrike blog and resource materials (Tier 3), which represent vendor-published analysis rather than independent peer-reviewed research. The statistical claims (89% increase, 42% zero-day increase, 27-second breakout time) are drawn from CrowdStrike's proprietary telemetry and have not been independently corroborated by third-party sources in the materials provided. Two source URLs reference specific AI product integrations (Claude Mythos and GPT-5.4-Cyber) that could not be independently verified against Anthropic or OpenAI official disclosures; those claims have been excluded from this analysis as unverified. The strategic directional finding, that AI is compressing exploit timelines, is consistent with publicly available analysis from CISA and MITRE, lending credibility to the general thesis even where specific metrics depend on vendor-sourced data.

Action Checklist

1. Step 1: Assess exposure, audit your current vulnerability management program's scan frequency, prioritization methodology, and mean time to remediation; determine whether your program is built around periodic cycles or continuous validation, and identify the gap between those two states
2. Step 2: Review controls, verify that foundational access control weaknesses are addressed at scale: enforce MFA across all authentication paths (CWE-287, T1078, T1110), audit privilege assignments and enforce least privilege (CWE-269, T1068), confirm authentication requirements on all externally exposed services (CWE-306, T1190), and validate network segmentation to limit lateral movement at the 27-second breakout tempo
3. Step 3: Update threat model, incorporate AI-accelerated exploit timelines as a permanent operational condition in your threat register; revise assumptions about the disclosure-to-exploitation window for all critical and high-severity vulnerabilities, and treat pre-disclosure zero-day exploitation as a baseline probability rather than an edge case
4. Step 4: Communicate findings, brief leadership on the specific structural gap: if your program remediates critical vulnerabilities on a weekly or monthly cycle, and exploitation is occurring in hours or minutes, quantify that gap explicitly; attach it to the 89% AI-enabled attack increase from CrowdStrike's

report to provide external validation

5. Step 5: Monitor developments, review CrowdStrike's full 2026 Global Threat Report when published if not yet available; monitor CISA Known Exploited Vulnerabilities catalog for exploitation velocity trends; and watch for follow-on research from MITRE, SANS, and independent threat intelligence providers that corroborates or refines the timeline compression finding

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and executive leadership immediately if CISA adds any CVE affecting your externally exposed services to the KEV catalog with a due-date window shorter than your current MTTR, if CrowdStrike Falcon or your monitoring platform detects T1190 or T1078 exploitation attempts against unpatched assets, or if your program gap analysis reveals critical vulnerabilities with MTTR exceeding 7 days against an environment with confirmed external exposure — any of these conditions indicates the structural gap described in the CrowdStrike 2026 GTR is actively exploitable in your environment.
Recovery Notes	After implementing continuous validation and access control hardening, verify that MFA enrollment is at 100% for all externally exposed and privileged authentication paths before declaring recovery — partial MFA deployment leaves CWE-287 and CWE-306 exposure intact against AI-accelerated T1078 and T1190 campaigns. Monitor CISA KEV additions daily for a minimum of 90 days post-restructuring to validate that your new MTTR SLAs are being met against real-world exploitation tempo, and retain MTTR metrics monthly to demonstrate measurable gap closure. Conduct a tabletop exercise simulating a 27-second lateral movement breakout scenario within 60 days to validate that your revised segmentation and detection controls perform as expected under the CrowdStrike-documented tempo.
Forensic Artifacts	CISA KEV JSON delta logs (timestamped daily pulls) correlated against your asset inventory — directly evidences the disclosure-to-exploitation compression affecting your specific CVE population and provides the quantitative basis for MTTR gap analysis | Vulnerability scanner MTTR export (Nessus, OpenVAS, or equivalent) showing discovery date vs. remediation date per CVE severity band — establishes the organizational baseline against which AI-accelerated exploitation windows (hours vs. weeks) are measured | Windows Security Event Log Event IDs 4625 (Failed Logon), 4648 (Explicit Credential Use), 4688 (Process Creation), and 4769 (Kerberos Service Ticket) — captures T1110 brute force, T1078 valid account abuse, and T1068 privilege escalation activity consistent with AI-generated exploit payloads operating at 27-second lateral movement tempo | Active Directory privilege group membership snapshots (exported via Get-ADGroupMember) and authentication policy configuration exports — baselines the least-privilege and MFA enforcement state that CWE-287, CWE-269, and CWE-306 weaknesses undermine, providing before/after evidence for remediation verification | Network flow logs or Zeek connection logs from east-west segments (specifically SMB port 445, RDP port 3389, WMI port 135 and dynamic RPC) — captures lateral movement candidates consistent with the 27-second breakout tempo documented in CrowdStrike 2026 GTR, tying AI-accelerated attack velocity to observable network behavior in your environment

Per-Action IR Details

Step 1: Assess exposure — audit your current vulnerability management program's scan frequency, prioritization methodology, and mean time to remediation; determine whether your program is built around

periodic cycles or continuous validation, and identify the gap between those two states

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability, policies, and detection readiness before adverse events occur

Controls: NIST SI-2 (Flaw Remediation) — identify, report, and correct system flaws with tested remediation timelines, NIST RA-3 (Risk Assessment) — assess likelihood and impact of threats including AI-accelerated exploitation timelines, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — documented process with frequency, prioritization, and MTTR metrics, CIS 7.2 (Establish and Maintain a Remediation Process) — risk-based remediation strategy with defined SLAs for critical and high findings

Compensating: Export your current vulnerability scanner output (Nessus Essentials, OpenVAS, or Trivy for containers) to CSV and calculate actual MTTR per severity band using a simple spreadsheet: sort by discovery date vs. close date, group by CVSS tier. For continuous validation without a commercial platform, deploy a weekly cron-scheduled OpenVAS scan with delta reporting piped to a local log file: `openvas-cli -u admin -w pass --xml-output /var/log/vuln-delta-$(date +%F).xml`. Compare consecutive runs with `diff` to surface newly introduced findings within 7 days rather than your next quarterly cycle.

Evidence: Before restructuring the program, snapshot the current state as a baseline artifact: export the full vulnerability backlog with discovery timestamps and current status from your scanner, capture your patch deployment logs from WSUS, SCCM, or Ansible to compute actual MTTR per CVE, and document scan schedule configuration files (e.g., Nessus policy XML, OpenVAS task definitions) to establish the periodic-vs-continuous gap that CrowdStrike's 27-second breakout tempo exposes.

Step 2: Review controls — verify that foundational access control weaknesses are addressed at scale: enforce MFA across all authentication paths (CWE-287, T1078, T1110), audit privilege assignments and enforce least privilege (CWE-269, T1068), confirm authentication requirements on all externally exposed services (CWE-306, T1190), and validate network segmentation to limit lateral movement at the 27-second breakout tempo

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Hardening and access control validation to reduce attack surface before exploitation occurs, directly addressing the lateral movement tempo documented in CrowdStrike 2026 GTR

Controls: NIST AC-2 (Account Management) — maintain accounts inventory and enforce authorization requirements across all authentication paths, NIST AC-6 (Least Privilege) — restrict access rights for users, groups, and processes to minimum necessary, NIST IA-2 (Identification and Authentication — Organizational Users) — uniquely identify and authenticate users, including MFA enforcement, NIST SC-7 (Boundary Protection) — implement managed interfaces and network segmentation to contain lateral movement, NIST SI-4 (System Monitoring) — monitor for unauthorized access attempts consistent with T1078 (Valid Accounts) and T1110 (Brute Force), CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce MFA on all externally exposed services to counter CWE-306 and T1190, CIS 6.4 (Require MFA for Remote Network Access) — MFA required for all remote access paths targeted by T1078, CIS 6.5 (Require MFA for Administrative Access) — MFA on all admin accounts to raise the cost of T1068 privilege escalation, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — limit blast radius of T1068 exploitation to dedicated admin tiers, CIS 4.4 (Implement and Manage a Firewall on Servers) — host-based firewall enforcement to constrain lateral movement at 27-second breakout tempo

Compensating: For MFA without enterprise IAM: deploy Authelia (open source) as a reverse proxy authentication layer in front of externally exposed services, or enable TOTP on SSH via libpam-google-authenticator. Audit privilege assignments with: `net localgroup administrators` (Windows) or `getent group sudo wheel` (Linux) piped to a text file for manual review. For network segmentation validation without an NDR platform, run `nmap -sn 10.0.0.0/8 --exclude ` from each VLAN to confirm east-west reach is limited, and deploy Zeek (open source) on a network tap to log lateral movement candidates — specifically SMB (T1021.002) and WMI (T1047) sessions that would appear in a 27-second breakout chain.

Evidence: Capture Windows Security Event Log Event ID 4625 (Failed Logon) and 4648 (Explicit Credential Logon) to identify T1110 brute force and T1078 valid account abuse patterns pre-enforcement; export Active Directory group membership snapshots (`Get-ADGroupMember -Identity 'Domain Admins' -Recursive | Export-CSV`) to baseline

privilege scope before least-privilege enforcement; and collect firewall rule exports and network topology diagrams to document current segmentation state against the lateral movement path a 27-second breakout would traverse (prioritizing SMB 445, RDP 3389, and WMI 135/dynamic ports between tiers).

Step 3: Update threat model — incorporate AI-accelerated exploit timelines as a permanent operational condition in your threat register; revise assumptions about the disclosure-to-exploitation window for all critical and high-severity vulnerabilities, and treat pre-disclosure zero-day exploitation as a baseline probability rather than an edge case

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Maintaining current threat intelligence and updating detection/response assumptions as part of ongoing IR readiness, aligned with CSF GV and ID functions

Controls: NIST RA-3 (Risk Assessment) — assess likelihood of threats including AI-accelerated pre-disclosure exploitation as documented in CrowdStrike 2026 GTR, NIST SI-5 (Security Alerts, Advisories, and Directives) — receive and act on threat intelligence from CISA, CrowdStrike, and MITRE on an ongoing basis, NIST IR-8 (Incident Response Plan) — update IR plan to reflect revised exploitation window assumptions for critical/high CVEs, NIST PM-16 (Threat Awareness Program) — maintain current threat awareness program incorporating CTI on AI-enabled adversary techniques, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — update documented process to reflect compressed disclosure-to-exploitation windows, replacing periodic assumptions with continuous-validation SLAs

Compensating: Maintain a local threat register in a shared spreadsheet or Markdown wiki with a dedicated column for 'assumed exploitation window' per CVE severity tier — update the critical/high rows to reflect hours rather than days based on CrowdStrike 2026 GTR findings. Subscribe to CISA KEV RSS feed (`https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json`) and poll it daily via a cron job that diffs the JSON against your asset inventory: `curl -s https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json | jq '.vulnerabilities[].cveID' > /tmp/kev-today.txt && diff /tmp/kev-yesterday.txt /tmp/kev-today.txt`. For zero-day baseline probability, integrate MITRE ATT&CK Navigator layers for T1190 (Exploit Public-Facing Application) and T1068 (Exploitation for Privilege Escalation) into your threat register to map coverage gaps against techniques AI-generated exploits most commonly operationalize.

Evidence: Pull historical CISA KEV entries with `dueDate` vs. `dateAdded` delta to quantify the actual disclosure-to-known-exploitation window for your existing asset CVE population — this produces the organization-specific data that validates or refines the CrowdStrike 89% AI-enabled attack increase figure for your threat register; also archive the CrowdStrike 2026 GTR summary and any MITRE or SANS follow-on publications as evidentiary sources supporting the model revision, timestamped in your threat register for audit trail purposes under NIST IR-8 (Incident Response Plan) documentation requirements.

Step 4: Communicate findings — brief leadership on the specific structural gap: if your program remediates critical vulnerabilities on a weekly or monthly cycle, and exploitation is occurring in hours or minutes, quantify that gap explicitly; attach it to the 89% AI-enabled attack increase from CrowdStrike's report to provide external validation

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned, program improvement communication, and updating organizational policies based on threat intelligence findings; also maps to CSF GV function for governance and leadership communication

Controls: NIST IR-4 (Incident Handling) — implement incident handling capability improvements and communicate capability gaps to leadership, NIST IR-6 (Incident Reporting) — report incident-relevant findings and structural program gaps to organizational leadership within defined timeframes, NIST IR-8 (Incident Response Plan) — update IR plan based on post-incident findings and communicate changes to relevant stakeholders, NIST PM-9 (Risk Management Strategy) — integrate AI-accelerated exploitation timeline findings into organizational risk management strategy and leadership briefings, CIS 7.2 (Establish and Maintain a Remediation Process) — document and communicate the risk-based remediation gap between current MTTR and AI-compressed exploitation windows

Compensating: Build a one-page gap quantification document using only open data: (1) your MTTR from Step 1 scanner export, (2) CISA KEV average time-to-exploitation pulled from the KEV JSON delta analysis, and (3) the CrowdStrike 2026 GTR 89% figure as external validation. Present a simple table: Severity | Your MTTR | Industry Exploitation Tempo | Gap (hours). This requires no tooling beyond a spreadsheet and is defensible to a board audience. Store the briefing document with version control (Git or dated filename convention) to satisfy NIST IR-8 (Incident Response Plan) documentation requirements.

Evidence: Retain the MTTR baseline data computed in Step 1, the threat model revision artifacts from Step 3, and the CISA KEV delta analysis as supporting evidence for the leadership briefing — these constitute the organizational record under NIST AU-11 (Audit Record Retention) that justifies program restructuring investment and provides a defensible paper trail if a breach occurs during the gap period; document the briefing date, attendees, and decisions made as a formal record in your incident response program documentation.

Step 5: Monitor developments — track the CrowdStrike 2026 Global Threat Report release for the full published dataset; monitor CISA Known Exploited Vulnerabilities catalog for exploitation velocity trends; and watch for follow-on research from MITRE, SANS, and independent threat intelligence providers that corroborates or refines the timeline compression finding

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Continuous monitoring of threat intelligence sources to detect emerging exploitation trends and refine detection capability, aligned with CSF DE.AE-07 (CTI integration into adverse event analysis)

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — receive system security alerts and advisories from CISA, MITRE, and CrowdStrike on an ongoing basis, NIST IR-5 (Incident Monitoring) — track and document exploitation velocity trends as part of ongoing incident monitoring program, NIST SI-4 (System Monitoring) — monitor for adversary use of AI-accelerated techniques including T1190 (Exploit Public-Facing Application) and T1078 (Valid Accounts) at compressed tempos, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate CISA KEV velocity data into vulnerability prioritization process with monthly or more frequent review cycles, CIS 8.2 (Collect Audit Logs) — ensure logging is enabled and retained across enterprise assets to support detection of exploitation attempts consistent with AI-accelerated attack patterns

Compensating: Automate CISA KEV monitoring with a daily cron job that diffs the KEV JSON against your asset inventory and sends an email alert for matches: `python3 kev_checker.py --inventory assets.csv --kev https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json --mailto soc@yourorg`. For MITRE and SANS follow-on research, configure an RSS aggregator (FreshRSS, self-hosted) to track MITRE ATT&CK blog, SANS Internet Storm Center, and relevant threat intel feeds. Deploy a Sigma rule pointing at your Windows Event Log or syslog for T1190 and T1078 indicators — the Sigma community rules repository (github.com/SigmaHQ/sigma) contains detection rules for both techniques that a 2-person team can load into any SIEM or run manually with Chainsaw (`chainsaw hunt /path/to/evtx --sigma sigma/rules/ --mapping mappings/sigma-event-logs-all.yml`) against exported EVTX files.

Evidence: Maintain a timestamped intelligence log (flat file or wiki page) recording each KEV addition relevant to your asset inventory, each CrowdStrike GTR update, and each MITRE or SANS publication that refines the AI exploitation timeline finding — this log serves as the evidentiary basis under NIST AU-6 (Audit Record Review, Analysis, and Reporting) for future program adjustments and demonstrates due diligence if exploitation occurs; specifically track the delta between CVE NVD publication date and CISA KEV addition date for each entry affecting your environment, as this metric directly quantifies the disclosure-to-exploitation compression the CrowdStrike 2026 GTR documents.

Detection Guidance

Detection in a compressed-timeline environment requires shifting from reactive alert triage to proactive behavioral baselining across the attack chain described in the report.

For initial access detection, monitor authentication logs for brute force patterns (T1110) and anomalous valid account usage (T1078), specifically, accounts authenticating from new geographies, devices, or at unusual

times without prior behavioral history. Web application and VPN access logs should be reviewed for scanning patterns consistent with T1595 active reconnaissance preceding exploitation attempts.

For lateral movement at speed, the 27-second breakout time means automated detection is mandatory. Hunt for rapid sequential authentication events across multiple internal hosts from a single source identity within short time windows. EDR telemetry should flag process execution chains consistent with credential dumping (T1003) followed immediately by remote service exploitation (T1210) or pass-the-hash/ticket activity (T1550).

For privilege escalation (T1068), alert on privilege change events outside of approved change windows and on process tokens acquiring elevated rights without corresponding IT workflow records.

For network discovery (T1046), internal network scans originating from non-scanner endpoints are a high-confidence indicator of post-compromise reconnaissance; baseline your authorized scanner IPs and alert on deviations.

Policy gap audit: Review whether your vulnerability prioritization workflow incorporates real-time exploitability signals (CISA KEV additions, active exploitation confirmations) or relies solely on CVSS base scores. CVSS scores do not reflect exploitation probability or active attacker interest; programs that triage solely by score will systematically deprioritize vulnerabilities that are actively exploited at lower base scores.

Log sources to prioritize: authentication logs (Active Directory, IdP, VPN), EDR process execution telemetry, network flow data for east-west movement, and vulnerability scanner output correlated against CISA KEV and threat intelligence feeds for exploitability status.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to CrowdStrike 2026 Global Threat Report for published indicators`	The CrowdStrike 2026 Global Threat Report references AI-enabled adversary tooling and campaign activity; specific IOC values (hashes, C2 infrastructure, payload signatures) are expected in the full report but were not available in the source materials provided for this analysis	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1087** — Account Discovery
- **T1003** — OS Credential Dumping
- **T1046** — Network Service Discovery
- **T1595** — Active Scanning
- **T1210** — Exploitation of Remote Services
- **T1203** — Exploitation for Client Execution
- **T1068** — Exploitation for Privilege Escalation

- **T1190** — Exploit Public-Facing Application
- **T1110** — Brute Force
- **T1550** — Use Alternate Authentication Material

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-7** — Unsuccessful Logon Attempts
- **AC-3** — Access Enforcement
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1087	Account Discovery	Discovery
T1003	OS Credential Dumping	Credential-Access
T1046	Network Service Discovery	Discovery
T1595	Active Scanning	Reconnaissance
T1210	Exploitation of Remote Services	Lateral-Movement
T1203	Exploitation for Client Execution	Execution
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1190	Exploit Public-Facing Application	Initial-Access
T1110	Brute Force	Credential-Access
T1550	Use Alternate Authentication Material	Defense-Evasion

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/frontier-ai-collapses-exploi...	T3
Mythos Is a Wake-Up Call: Five Steps to Prepare for Frontier AI	https://www.crowdstrike.com/en-us/resources/crowdcasts/mythos-is-a-...	T3
Frontier AI for Defenders: CrowdStrike and OpenAI TAC	https://www.crowdstrike.com/en-us/blog/frontier-ai-for-defenders-cr...	T3

Source	URL	Tier
CrowdStrike Integrates GPT-5.4-Cyber into Falcon Platform - LinkedIn	https://www.linkedin.com/posts/getaigovernence_falcon-aiagents-aise...	T3
Anthropic and OpenAI unveil Claude Mythos and GPT-5.4-Cyber	https://www.orangecyberdefense.com/be/blog/innovation/anthropic-and...	T3

Generated 2026-05-03 13:21 UTC by TJS Security Command Center