INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-18 13:47 UTC

Iran-Affiliated Threat Actors Pivot to ICS/OT Targeting Following Operation Epic Fury, Connectivity Restored After 47-Day Blackout

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0185
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Rockwell Automation FactoryTalk, Allen-Bradley PLCs, Unitronics PLCs, Palo Alto Networks Cortex XDR, Cortex XSIAM, Cortex Xpanse, Next-Generation Firewall
Published	2026-04-17T22:35:07+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Following the February 28, 2026 U.S.-Israel offensive Operation Epic Fury, Iranian-affiliated threat actors tracked as CL-STA-1128 (overlapping with Cyber Av3ngers and Storm-0784) have escalated targeting of operational technology infrastructure, specifically Rockwell Automation FactoryTalk software and Allen-Bradley PLCs, across energy, utilities, food processing, and financial services sectors. The restoration of Iran's domestic internet connectivity on mid-April 2026 after a 47-day blackout expands the operational pool of available threat actors and signals a likely increase in tempo. Organizations running internet-connected ICS/OT equipment in critical infrastructure sectors face immediate risk of operational disruption, physical process manipulation, and destructive attack.

Technical Analysis

CL-STA-1128, a cluster overlapping with Cyber Av3ngers and Storm-0784, has pivoted from prior Unitronics PLC targeting (documented by CISA, November 2023) to Rockwell Automation FactoryTalk software and Allen-Bradley PLCs. During Iran's domestic internet blackout (approximately March 1 to mid-April 2026), threat actors maintained operational continuity via VSAT and Starlink satellite uplinks; connectivity restoration expands the available operator pool.

Exploitation patterns are consistent with three CWEs: CWE-284 (Improper Access Control), CWE-693 (Protection Mechanism Failure), and CWE-1188 (Insecure Default Initialization), indicating authentication bypass and default credential abuse as primary initial access vectors. Palo Alto Networks Cortex XDR, XSIAM,

Xpanse, and Next-Generation Firewall management interfaces are targeting vectors for visibility impairment (T1562) and credential capture (T1078); no confirmed vulnerability in these products has been disclosed. Organizations should audit management-plane access controls and monitor for unauthorized configuration changes.

Relevant MITRE ATT&CK and ATT&CK for ICS techniques include: T0811 (Data Destruction), T0883 (Internet Accessible Device), T0816 (Device Restart/Shutdown), T0843 (Program Organization Units), T0853 (Scripting), T0866 (Exploitation of Remote Services), T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1133 (External Remote Services), T1485 (Data Destruction), T1542 (Pre-OS Boot), T1562 (Impair Defenses), T1566/T1566.002 (Phishing/Spearphishing Link), T1071.001 (Web Protocols), T1498 (Network Denial of Service), T1219 (Remote Access Software), T1583.001/T1583.003 (Acquire Infrastructure: Domains/Virtual Private Server). Techniques prefixed 'T0' are ICS-specific; 'T1' techniques are enterprise ATT&CK.

No CVE identifiers or specific patch versions were included in the source data. Rockwell Automation security advisories should be reviewed directly for current patch status. This assessment is sourced primarily from T3 vendor and industry sources; human validation of provided URLs is recommended before external publication.

Action Checklist

1. Step 1: Containment, Immediately audit network segmentation between IT and OT environments. Isolate all internet-facing Rockwell Automation FactoryTalk instances and Allen-Bradley PLCs from external network access. Verify that Palo Alto Cortex XDR, XSIAM, Xpanse, and NGFW management interfaces are not exposed to untrusted networks. Prioritize assets in energy, utilities, food processing, and financial services.
2. Step 2: Detection, Hunt for indicators consistent with T1078 (Valid Accounts) and T1133 (External Remote Services): review VPN and remote access logs for authentication from VSAT/satellite IP ranges, off-hours logins, and accounts accessing OT assets without recent prior history. Check FactoryTalk and Allen-Bradley PLC audit logs for unauthorized configuration changes, program downloads (T0843), or device restart commands (T0816). Review Palo Alto NGFW and Cortex logs for anomalous management-plane access or defense impairment events (T1562). Cross-reference login events against known Cyber Av3ngers and Storm-0784 TTPs per CISA Advisory AA23-335A (Unitronics campaign). Note: verify with CISA whether AA23-335A remains current guidance for 2026 Rockwell targeting.
3. Step 3: Eradication, Audit all Rockwell Automation FactoryTalk and Allen-Bradley PLC accounts; remove default credentials (CWE-1188) and enforce strong, unique passwords. Review Rockwell Automation security advisories at https://www.rockwellautomation.com/en-us/trust-center/security-advisories.html and prioritize any advisories related to FactoryTalk authentication, PLC access control (CWE-284, CWE-1188), or default credential vulnerabilities issued between February and April 2026. Apply patches as they become available; if no patches are available, prioritize network isolation and access control hardening. Human validation of URL recommended. Enforce access control lists to restrict PLC programming interfaces to authorized engineering workstations only (CWE-284). Review and harden Palo Alto NGFW and Cortex product configurations per current vendor hardening guides.
4. Step 4: Recovery, Validate PLC ladder logic and FactoryTalk project files for unauthorized modifications before resuming production operations. Verify that OT asset firmware and software versions match known-good baselines. Monitor for recurrence of satellite-sourced authentication attempts, lateral movement from IT to OT segments, and any T0816 (Device Restart/Shutdown) or T1485/T0811

(Destructive) activity for a minimum of 30 days post-remediation.

5. Step 5: Post-Incident, Conduct a tabletop exercise focused on ICS/OT destructive attack scenarios specific to FactoryTalk and Allen-Bradley environments. Evaluate whether current detection coverage addresses ATT&CK for ICS techniques (T0811, T0816, T0843, T0853, T0866, T0883). Review CISA Advisory AA23-335A and CISA ICS-CERT advisories for applicable compensating controls. Assess whether security tooling (Cortex, NGFW) alert thresholds adequately surface management-plane anomalies.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership, legal counsel, and relevant sector ISAC (E-ISAC for energy, Water ISAC for utilities, FS-ISAC for financial services) immediately if any Allen-Bradley PLC audit trail confirms a T0843 (Program Download) or T0816 (Device Restart/Shutdown) event from an unauthorized source, or if any FactoryTalk account creation/modification is identified within the post-April 17, 2026 window, as these conditions indicate active OT compromise with potential for physical-process impact and may trigger CIRCIA 72-hour reporting obligations for critical infrastructure owners.
Recovery Notes	Before resuming any production operations, every Allen-Bradley PLC in scope must have its current online project cryptographically compared against the last known-good backup using Studio 5000 Compare — no exceptions, as CL-STA-1128 TTPs include stealthy ladder logic modification designed to cause delayed physical process disruption consistent with T0811 (Manipulation of Control) and T0816 (Device Restart/Shutdown). Post-recovery monitoring must remain heightened for a minimum of 30 days given that Iran's internet connectivity restoration on April 17, 2026 marks the likely operational reactivation window for pre-staged access; watch specifically for satellite-ASN-sourced VPN authentications, CIP command anomalies on EtherNet/IP, and any Cortex XDR agent health degradation indicating T1562 (Impair Defenses). Coordinate with Rockwell Automation's Product Security Incident Response Team (PSIRT) if ladder logic tampering is confirmed, as firmware-level persistence mechanisms in Allen-Bradley ControlLogix and CompactLogix families may require vendor-assisted recovery procedures not available through standard Studio 5000 workflows.

Forensic Artifacts	Allen-Bradley PLC onboard audit trail (Studio 5000 / RSLogix 5000 > Controller Properties > General > Audit Trail): primary artifact for T0843 (Program Download) and T0816 (Device Restart/Shutdown) — look for 'Download,' 'Go Online,' 'Mode Change,' and 'Restart' entries with source workstation IP and timestamp in the post-April 17, 2026 window. | FactoryTalk Diagnostics log at C:\ProgramData\Rockwell Automation\Diagnostics on the FactoryTalk application server: records project open/save/download operations, user authentication events, and configuration change history — search for entries referencing accounts not in the authorized operator roster or originating from non-engineering-workstation hostnames. | VPN and remote access authentication logs filtered for source IP ASN ownership matching ViaSat (AS21928), Hughes Network Systems (AS6730), Inmarsat, or other VSAT providers: CL-STA-1128 and Cyber Av3ngers have demonstrated satellite-relay access to obscure geographic origin, making ASN-level filtering more reliable than GeoIP country-of-origin for this threat actor. | Palo Alto NGFW traffic logs (Monitor > Logs > Traffic) and system logs (Monitor > Logs > System) filtered for admin login events, configuration commits, and any traffic on CIP/EtherNet/IP ports (TCP/UDP 44818, TCP 2222) crossing the IT/OT boundary — cross-reference with Cortex XDR/XSIAM incident queue for any T1562 (Impair Defenses) alerts indicating agent policy modification or service termination coincident with the intrusion window. | SHA-256 hashes of all Allen-Bradley PLC project files (.ACD) and FactoryTalk project archives (.fta, .med) extracted from both the controller (online) and the engineering workstation backup share — a hash mismatch between online and backup copy is direct evidence of unauthorized T0843 (Program Download) and the primary indicator distinguishing confirmed OT compromise from a near-miss.

Per-Action IR Details

Step 1: Containment — Immediately audit network segmentation between IT and OT environments. Isolate all internet-facing Rockwell Automation FactoryTalk instances and Allen-Bradley PLCs from external network access. Verify that Palo Alto Cortex XDR, XSIAM, Xpanse, and NGFW management interfaces are not exposed to untrusted networks. Prioritize assets in energy, utilities, food processing, and financial services.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 12.2 (Establish and Maintain a Secure Network Architecture) — IG2/IG3 reference for OT/IT segmentation

Compensating: Without enterprise NAC or next-gen firewall licensing: use Windows Firewall with Advanced Security (netsh advfirewall) on FactoryTalk engineering workstations to block all inbound connections except from explicitly whitelisted engineering workstation IPs. On Linux-based OT gateways, apply iptables rules dropping all traffic on EtherNet/IP port 44818 and CIP port 2222 except from the authorized subnet. Physically disconnect or disable the WAN interface on any Allen-Bradley PLC that has a live internet-routable address — this is a two-person, zero-cost action. Run 'nmap -sV -p 44818,2222,102,502 ' from a jump host to identify any still-exposed PLCs.

Evidence: Before isolating, capture a full netflow or pcap snapshot from the IT/OT boundary switch or firewall to preserve evidence of active C2 or exfiltration sessions originating from or destined to VSAT/satellite IP ranges (ASN blocks commonly associated with ViaSat, Inmarsat, and Hughes Network Systems). Export Palo Alto NGFW traffic logs filtered on destination/source matching known satellite IP ranges and FactoryTalk default port 19476. Capture current ARP tables and routing tables from the OT network switches before segmentation changes alter the topology. Document all Allen-Bradley PLC IP addresses, firmware versions, and last-seen communication partners from FactoryTalk Linx or RSLinx Classic device tree before isolation.

Step 2: Detection — Hunt for indicators consistent with T1078 (Valid Accounts) and T1133 (External Remote Services): review VPN and remote access logs for authentication from VSAT/satellite IP ranges, off-hours logins, and accounts accessing OT assets without recent prior history. Check FactoryTalk and Allen-Bradley

PLC audit logs for unauthorized configuration changes, program downloads (T0843), or device restart commands (T0816). Review Palo Alto NGFW and Cortex logs for anomalous management-plane access or defense impairment events (T1562). Cross-reference login events against known Cyber Av3ngers and Storm-0784 TTPs per CISA Advisory AA23-335A (Unitronics campaign).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM: run the following PowerShell on FactoryTalk application servers to extract authentication events — 'Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4625,4648,4672) -and $_.TimeCreated -gt (Get-Date).AddDays(-30)} | Export-Csv C:\IR\auth_audit.csv'. For Allen-Bradley PLC audit trail, open Studio 5000 or RSLogix 5000, navigate to Controller Properties > General > Audit Trail and export the full log to CSV; look for 'Download' and 'Go Online' events from unexpected source workstations (T0843 artifacts). Deploy a free Sigma rule set targeting T1078/T1133 on exported Windows event logs using Chainsaw (free, open-source, binary available on GitHub): 'chainsaw hunt C:\IR\evtx_logs\ --sigma sigma_rules\ --mapping mappings\sigma-event-logs-all.yml'. For satellite IP detection without SIEM, cross-reference VPN authentication source IPs against a downloaded MaxMind GeoLite2 ASN database using a Python script querying ASN ownership for known VSAT providers.

Evidence: FactoryTalk Diagnostics log located at C:\ProgramData\Rockwell Automation\Diagnostics — export and search for 'program download,' 'controller mode change,' and 'project modified' entries timestamped after April 17, 2026 (Iran connectivity restoration date). Allen-Bradley PLC onboard audit trail (accessible via Studio 5000 > Controller Properties > General > Audit Trail): preserve raw export before any firmware reset. Windows Security Event Log on FactoryTalk server: Event ID 4624 (successful logon) and 4625 (failed logon) filtered by Logon Type 10 (RemoteInteractive) and 3 (Network) — specifically accounts not in the authorized OT operator group. VPN concentrator authentication logs filtered for source ASN blocks belonging to ViaSat (AS21928), Hughes Network Systems (AS6730), or Inmarsat — consistent with CL-STA-1128 satellite-sourced access TTPs documented in post-Unitronics campaign analysis. Palo Alto NGFW system logs for 'admin login' and 'config change' events on management plane, and Cortex XDR/XSIAM alert history for any T1562 (Impair Defenses) detections including agent tampering or policy modification events.

Step 3: Eradication — Audit all Rockwell Automation FactoryTalk and Allen-Bradley PLC accounts; remove default credentials (CWE-1188) and enforce strong, unique passwords. Apply all current Rockwell Automation security advisories available at https://www.rockwellautomation.com/en-us/trust-center/security-advisories.html (human validation of URL recommended). Enforce access control lists to restrict PLC programming interfaces to authorized engineering workstations only (CWE-284). Review and harden Palo Alto NGFW and Cortex product configurations per current vendor hardening guides.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST CM-6 (Configuration Settings), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.2 (Use Unique Passwords), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: For teams without PAM tooling: export the FactoryTalk Security user database (FactoryTalk Administration Console > User Accounts) to a spreadsheet and manually audit every account against the authorized personnel list; flag and disable any account not associated with a named current employee. On Allen-Bradley PLCs, use Studio 5000 or RSLogix 5000 to navigate to Controller Properties > Security and verify CIP Security is enabled where firmware supports it; if not, set a controller-level password and document it in an offline credential vault (KeePass is free and acceptable for a 2-person team). For CWE-284 ACL enforcement without enterprise NAC: configure Stratix switch port security or standard managed-switch MAC address filtering to ensure only the IP

addresses of authorized engineering workstations can reach PLC EtherNet/IP ports (TCP/UDP 44818). Validate Palo Alto NGFW management access is restricted to a dedicated management VLAN using the free Palo Alto Security Baseline Assessment tool or manually audit 'Device > Setup > Management > Management Interface Settings.'

Evidence: Before removing default accounts or changing credentials, capture a full export of the FactoryTalk Security user database including account creation dates, last login timestamps, and group memberships — this establishes whether any accounts were created or modified during the intrusion window post-April 17, 2026. Export Allen-Bradley PLC controller memory (using Studio 5000 'Save to File' of the current online project) to preserve any malicious ladder logic or Add-On Instructions (AOIs) that CL-STA-1128 may have injected as part of T0843 (Program Download) activity before eradication overwrites them. Capture Palo Alto NGFW running configuration ('show config running' via CLI) and Cortex XDR agent policy state before any hardening changes alter the baseline for forensic comparison.

Step 4: Recovery — Validate PLC ladder logic and FactoryTalk project files for unauthorized modifications before resuming production operations. Verify that OT asset firmware and software versions match known-good baselines. Monitor for recurrence of satellite-sourced authentication attempts, lateral movement from IT to OT segments, and any T0816 (Device Restart/Shutdown) or T1485/T0811 (Destructive) activity for a minimum of 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), NIST IR-4 (Incident Handling), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For ladder logic integrity validation without a commercial OT integrity tool: use the Studio 5000 or RSLogix 5000 'Compare' function to diff the current online PLC project against the last known-good offline backup stored in a write-protected network share or USB vault — document every discrepancy. For firmware baseline verification, run 'Get-WinEvent -LogName Application -Source "Rockwell*"' and cross-reference reported firmware strings against Rockwell's published firmware release notes for the specific Allen-Bradley PLC model. For ongoing satellite-IP monitoring without SIEM: create a scheduled PowerShell task running every 4 hours that parses VPN authentication logs and alerts (via email or Slack webhook) on any source IP resolving to VSAT ASNs — a 30-line script is sufficient. Deploy the free Claroty Community Edition or Dragos ICS Community Tools if budget allows; otherwise, passive Wireshark capture on the IT/OT boundary with a display filter for EtherNet/IP ('enip') provides continuous visibility at zero cost.

Evidence: Before restoring production, capture a cryptographic hash (SHA-256) of each Allen-Bradley PLC project file (.ACD) downloaded from the controller and compare against hashes stored in the pre-incident backup archive — any mismatch indicates residual T0843 (Program Download) tampering. For FactoryTalk project files (.fta, .med, .rsview32), run 'certutil -hashfile SHA256' on the Windows engineering workstation and log results. Capture a Wireshark pcap on the OT network segment during the first controlled production restart to establish a clean traffic baseline for CIP command sequences — this becomes the reference for T0816 (Device Restart) anomaly detection going forward. Document all firmware version strings from each Allen-Bradley PLC model in the environment using Studio 5000 'Who Active' scan and export to CSV before and after recovery to confirm no unauthorized firmware downgrades occurred.

Step 5: Post-Incident — Conduct a tabletop exercise focused on ICS/OT destructive attack scenarios specific to FactoryTalk and Allen-Bradley environments. Evaluate whether current detection coverage addresses ATT&CK for ICS techniques (T0811, T0816, T0843, T0853, T0866, T0883). Review CISA Advisory AA23-335A and CISA ICS-CERT advisories for applicable compensating controls. Assess whether security tooling (Cortex, NGFW) alert thresholds adequately surface management-plane anomalies.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-3 (Incident Response Testing), NIST IR-8 (Incident Response Plan), NIST SI-4 (System Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For tabletop without a commercial simulation platform: download the free CISA Tabletop Exercise Package (CTEP) for ICS environments from cisa.gov/resources-tools/resources/cisa-tabletop-exercises-package and adapt Scenario Module 4 (Industrial Control Systems) to insert FactoryTalk and Allen-Bradley-specific injects such as 'unauthorized program download to Line 3 PLC detected' and 'Cortex XSIAM alert suppressed — possible T1562 agent tampering.' For ATT&CK for ICS coverage gap analysis: load the free MITRE ATT&CK Navigator (web app, no install required at mitre-attack.github.io/attack-navigator) and map T0811, T0816, T0843, T0853, T0866, and T0883 against your current detection rules; unpopulated cells with no associated Sigma or YARA rule represent coverage gaps. Export the gap list as a prioritized backlog for detection engineering sprints.

Evidence: Compile a complete incident timeline from all log sources (FactoryTalk Diagnostics, Allen-Bradley PLC audit trails, VPN authentication logs, NGFW traffic logs, Cortex XDR alert history) anchored to April 17, 2026 as the earliest plausible intrusion window — this timeline is the primary artifact for the lessons-learned report required under NIST IR-8 (Incident Response Plan) and supports any CISA voluntary reporting under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Preserve all forensic artifacts (PLC project file hashes, FactoryTalk user export, pcap captures, eradication change log) in a write-protected evidence repository for a minimum of 12 months per NIST AU-11 (Audit Record Retention) to support potential law enforcement referral given the nation-state attribution to CL-STA-1128.

Detection Guidance

Focus detection on three areas: (1) Remote access anomalies, review VPN, RDP, and external remote services (T1133) logs for authentication originating from VSAT or Starlink satellite IP address blocks, particularly during off-hours; flag accounts accessing OT jump hosts or engineering workstations that have no recent access history. (2) OT asset activity, monitor FactoryTalk audit logs and Allen-Bradley PLC event logs for unauthorized program downloads, configuration changes, or device restart commands; compare against authorized change windows. Alert on any CIP (Common Industrial Protocol) traffic from non-engineering workstations. (3) Security tool impairment, monitor Palo Alto Cortex XDR and NGFW management-plane logs for unauthorized policy changes, agent uninstall attempts, or logging suppression events consistent with T1562 (Impair Defenses). Behavioral indicators consistent with this cluster include use of legitimate remote access software (T1219) to blend with normal traffic and spearphishing lures targeting OT operators (T1566.002). As specific IOCs (IP addresses, domains, file hashes) become available, they will be published by CISA and Palo Alto Unit 42. Subscribe to threat feeds at https://www.cisa.gov/ics-alerts and https://unit42.paloaltonetworks.com/ for indicator updates.

Framework Mappings

MITRE-ATTACK

- **T1485** — Data Destruction
- **T1566** — Phishing
- **T0811** — Data from Information Repositories
- **T1190** — Exploit Public-Facing Application
- **T0883** — Internet Accessible Device
- **T1071.001** — Web Protocols
- **T0816** — Device Restart/Shutdown
- **T1542** — Pre-OS Boot
- **T1566.002** — Spearphishing Link

- **T1133** — External Remote Services
- **T0843** — Program Download
- **T1078** — Valid Accounts
- **T0866** — Exploitation of Remote Services
- **T1562** — Impair Defenses
- **T1583.001** — Domains
- **T0853** — Scripting
- **T1583.003** — Virtual Private Server
- **T1498** — Network Denial of Service
- **T1219** — Remote Access Tools

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1485	Data Destruction	Impact
T1566	Phishing	Initial-Access
T0811	Data from Information Repositories	Collection
T1190	Exploit Public-Facing Application	Initial-Access
T0883	Internet Accessible Device	Initial-Access
T1071.001	Web Protocols	Command-And-Control
T0816	Device Restart/Shutdown	Inhibit-Response-Function
T1542	Pre-OS Boot	Defense-Evasion
T1566.002	Spearphishing Link	Initial-Access
T1133	External Remote Services	Persistence
T0843	Program Download	Lateral-Movement
T1078	Valid Accounts	Defense-Evasion
T0866	Exploitation of Remote Services	Initial-Access
T1562	Impair Defenses	Defense-Evasion
T1583.001	Domains	Resource-Development
T0853	Scripting	Execution
T1583.003	Virtual Private Server	Resource-Development
T1498	Network Denial of Service	Impact
T1219	Remote Access Tools	Command-And-Control

Sources

Source	URL	Tier
Unit 42	https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/	T3
	https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/	T3
	https://www.michiganfarmnews.com/iranian-affiliated-cyber-attacks-t...	T3
	https://www.csis.org/analysis/iran-conflict-heightens-cyber-threats...	T3
Rockwell Automation Security Advisories	https://www.rockwellautomation.com/en-us/trust-center/security-advi...	T3

Generated 2026-04-18 13:47 UTC by TJS Security Command Center