INTRUVENT

COMPREHENSIVE THREAT HUNTING GUIDE

FAD Team: Hacktivist OT/ICS Targeting Detection

Detecting internet-exposed ICS/SCADA devices, hacktivist-style OT intrusions, SQL injection campaigns, and Telegram-coordinated data leak operations

Version 1.0
Published March 18, 2026
Threat Actor FAD Team / Fatimion Cyber Team (IRGC proxy)
Classification TLP:CLEAR
Total Hunt Time 5 Hours
Target Sectors Critical Infrastructure, Water, Agriculture, Energy, Government

Intruvent Technologies
INT-THG-2026-FADTEAM-OT-v1.0

Table of Contents

Overview

Executive Summary 3
MITRE ATT&CK Mapping 4

Hunt Modules

Module 1: Internet-Exposed ICS/SCADA Device Discovery 5
Module 2: Default/Weak Credential Detection on OT Systems 6
Module 3: HMI/SCADA Unauthorized Access Detection 7
Module 4: PLC Logic and Setpoint Modification Detection 8
Module 5: OT Network Anomalous Traffic Patterns 9
Module 6: SQL Injection Campaign Detection 10
Module 7: Web Application Defacement Detection 11
Module 8: VNC/RDP Unauthorized Access to OT Workstations 12
Module 9: DDoS and Volumetric Attack Detection 13
Module 10: Data Exfiltration and Leak Infrastructure Detection 14

Appendices

Appendix A: OT Monitoring Infrastructure Requirements 15
Appendix B: References 16

1 Executive Summary

AT A GLANCE

THREAT ACTOR FAD Team / Fatimion Cyber Team (IRGC proxy)	PRIMARY OBJECTIVE OT/ICS disruption, data exfiltration, psychological operations
ACTIVE SINCE August 2023 (Telegram); escalated March 2026	TARGET SECTORS Critical Infrastructure, Water, Agriculture, Energy, Government
KEY DIFFERENTIATOR Hacktivist-militia hybrid targeting OT/ICS via internet exposure	PRIMARY TECHNIQUES SQL injection, DDoS, SCADA/PLC access via default credentials, data leaks

FAD Team (Fatimion Cyber Team) is an IRGC-aligned hacktivist group that has claimed unauthorized access to SCADA/PLC systems across multiple countries, conducted global SQL injection campaigns, and launched coordinated DDoS and data leak operations. The group operates within the Cyber Islamic Resistance coalition and the Electronic Operations Room, a coordination body formed on February 28, 2026, following the commencement of Operation Epic Fury.

This guide focuses on detecting hacktivist-style OT/ICS targeting. Iranian-aligned groups (including CyberAv3ngers and FAD Team) primarily target internet-exposed OT devices using default credentials, Shodan/Censys scanning, and opportunistic exploitation. Unlike sophisticated APT operations that involve prolonged dwell time, hacktivist OT attacks are typically fast, shallow, and optimized for maximum media attention.

This guide provides **10 hunt modules** designed for organizations with OT/ICS infrastructure, water/wastewater utilities, agricultural control systems, and energy facilities. Modules include both IT-side detection (network monitoring, log analysis) and OT-side detection (process historian, PLC monitoring) approaches. Not all organizations will have the OT monitoring infrastructure described; alternative detection approaches using network-level indicators are included where applicable. Total estimated hunt time: **5 hours**.

Threat Overview

FAD Team represents a category of threat actor that sits between low-sophistication hacktivists and state-directed APT groups. The group has claimed SCADA/PLC access in Israel and other countries, published screenshots of what appeared to be HMI dashboards on Telegram, and was categorized by Palo Alto Unit 42 among groups focused on "wiper malware and permanent data destruction."

The group's OT targeting pattern mirrors CyberAv3ngers (IRGC-CEC), which exploited internet-exposed Unitronics PLCs using default credentials (password: 1111) via TCP port 20256. CyberAv3ngers compromised at least 75 devices in a 2023 campaign, including 34 in the US wastewater sector, leading to CISA Advisory AA23-335A and US Treasury sanctions against six IRGC-CEC officials.

Hunt modules in this guide address the most likely attack paths: internet-exposed ICS devices, default credentials, unauthorized HMI access, SQL injection against web applications, and DDoS attacks against public-facing services. Organizations operating water treatment, agricultural irrigation, or energy generation/distribution systems are at elevated risk.

KEY CHARACTERISTICS

- IRGC-aligned proxy hacktivist
- SCADA/PLC access claims (multiple countries)
- Global SQL injection campaigns
- DDoS against government/media targets
- Telegram-coordinated operations
- Data exfiltration and public leaks
- Electronic Operations Room member
- Targets internet-exposed OT devices
- Wiper malware capability (assessed)
- Shared exploit exchange with 60+ groups

2 MITRE ATT&CK Mapping

The following techniques are assessed based on FAD Team's claimed activities and the broader Iranian hacktivist OT targeting pattern (including CyberAv3ngers). Techniques marked [ASSESSED] are analytical judgments; techniques marked [CONFIRMED] are verified through independent reporting.

`T1190` CONFIRMED
Exploit Public-Facing Application
SQL injection campaigns against web applications; exploitation of internet-exposed SCADA/HMI web interfaces

`T1078 [ASSESSED]`
Valid Accounts / Default Credentials
Access to OT systems via default or weak credentials on internet-exposed devices (CyberAv3ngers pattern: Unitronics default password "1111")

`T1498` CONFIRMED
Network Denial of Service
DDoS attacks against Kuwait government, Bahrain News Agency, Qatar Gasco, and Qatar Radio

`T1491.002` CONFIRMED
External Defacement
Website defacement campaigns against government and media targets

`T1213` CONFIRMED
Data from Information Repositories
Database exfiltration via SQL injection; 23,553 records from ATV Kuwait app

`T1567` CONFIRMED
Exfiltration Over Web Service
Stolen data published via Telegram channels for maximum psychological impact

`T0883 [ASSESSED] (ICS)`
Internet Accessible Device
Targeting internet-exposed PLCs, HMIs, and SCADA systems via Shodan/Censys scanning

`T0831 [ASSESSED] (ICS)`
Manipulation of Control
Claimed PLC parameter modification; depth of actual control access not independently verified

`T0886 [ASSESSED] (ICS)`
Remote Services
Unauthorized access to SCADA systems via exposed web interfaces and remote access protocols

`T1595.002 [ASSESSED]`
Vulnerability Scanning
Scanning for internet-exposed ICS devices via search engines (Shodan, Censys, FOFA)

`T1583.006` CONFIRMED
Web Services (Telegram)
Telegram as primary coordination, C2, and data publication platform

`T1485 [ASSESSED]`
Data Destruction
Unit 42 categorized FAD Team among groups focused on wiper malware; no samples published

3 Hunt Modules

OT Monitoring Infrastructure Note
Several modules in this guide reference OT-specific monitoring capabilities (process historian queries, PLC event logs, OT network traffic analysis). Not all organizations will have these capabilities deployed. Where applicable, each module includes alternative detection approaches using IT-side network monitoring, firewall logs, and endpoint telemetry. Organizations without dedicated OT monitoring should prioritize Modules 1, 2, 6, 7, 8, 9, and 10, which rely primarily on IT-side telemetry.

1 Internet-Exposed ICS/SCADA Device Discovery

Duration: 30 min Priority: CRITICAL

Objective: Identify any ICS/SCADA/HMI devices in your environment that are directly accessible from the internet, the primary attack vector for hacktivist OT targeting.

Background

FAD Team and CyberAv3ngers target internet-exposed OT devices. CyberAv3ngers compromised 75+ Unitronics PLCs in 2023 by scanning Shodan for devices exposed on TCP port 20256 with default credentials. CISA Advisory AA23-335A confirmed this as the primary attack vector. FAD Team has claimed similar SCADA/PLC access across multiple countries. The single most impactful defensive action is eliminating internet exposure of OT devices.

Hunt Procedure: External Exposure Scan (IT-Side)

INVESTIGATION AID

SHODAN / CENSYS QUERY

```
# Search Shodan for your organization's OT devices exposed to internet
# Replace YOUR_ORG_IP_RANGE with your public IP ranges
# Source: CISA AA23-335A recommended scan approach

# Shodan queries for common OT protocols:
shodan search "port:502 net:YOUR_ORG_IP_RANGE"     # Modbus
shodan search "port:102 net:YOUR_ORG_IP_RANGE"     # S7comm (Siemens)
shodan search "port:44818 net:YOUR_ORG_IP_RANGE"   # EtherNet/IP
shodan search "port:47808 net:YOUR_ORG_IP_RANGE"   # BACnet
shodan search "port:20000 net:YOUR_ORG_IP_RANGE"   # DNP3
shodan search "port:20256 net:YOUR_ORG_IP_RANGE"   # Unitronics PCOM
shodan search "port:1911 net:YOUR_ORG_IP_RANGE"    # Niagara Fox
shodan search "port:9600 net:YOUR_ORG_IP_RANGE"    # OMRON FINS

# Also check for exposed HMI web interfaces:
shodan search "http.title:\"HMI\" net:YOUR_ORG_IP_RANGE"
shodan search "http.title:\"SCADA\" net:YOUR_ORG_IP_RANGE"
shodan search "http.title:\"Unitronics\" net:YOUR_ORG_IP_RANGE"
```

Hunt Procedure: Firewall Rule Audit for OT Protocols

INVESTIGATION AID

KQL (AZURE FIREWALL / NETWORK LOGS)

```
// Detect inbound connections to common OT protocol ports from external IPs
// Any match indicates potential internet exposure of OT devices
AzureNetworkAnalytics_CL
| where Direction_s == "Inbound"
| where DestPort_d in (502, 102, 44818, 47808, 20000, 20256, 1911, 9600, 4840)
| where SrcIP_s !startswith "10." and SrcIP_s !startswith "172.16."
    and SrcIP_s !startswith "192.168."
| project TimeGenerated, SrcIP_s, DestIP_s, DestPort_d,
    Protocol_s, Action_s
| sort by TimeGenerated desc
```

☐ Run external Shodan/Censys scans against all organizational public IP ranges for OT protocols
☐ Audit perimeter firewall rules for any inbound rules permitting traffic to OT protocol ports (502, 102, 44818, 47808, 20000, 20256)
☐ Verify that no HMI web interfaces are accessible from the internet (check for HTTP/HTTPS on non-standard ports)
☐ If any internet-exposed OT devices are found, initiate emergency remediation (firewall block, VPN requirement)

Any Internet-Exposed OT Device Is Critical
If this module identifies any internet-exposed ICS/SCADA device, treat it as an immediate security incident. CyberAv3ngers compromised 75+ PLCs through this exact attack vector. Remove internet exposure immediately, then investigate for signs of unauthorized access.

2 Default/Weak Credential Detection on OT Systems

Duration: 30 min Priority: CRITICAL

Objective: Identify OT devices and systems still configured with default, factory-set, or weak credentials that Iranian-aligned hacktivists exploit for initial access.

Background

CyberAv3ngers exploited Unitronics Vision Series PLCs using the factory default password "1111" on TCP port 20256 (CISA AA23-335A). This is the single most common initial access vector for hacktivist OT targeting. Many ICS/SCADA devices ship with well-known default credentials that operators never change. FAD Team's claimed SCADA/PLC access likely follows the same pattern of targeting default-credential devices found via internet scanning.

Known Default Credentials (OT Devices)

Vendor / Product	Default Credential	Port	Source
Unitronics Vision Series PLC	Password: `1111`	TCP 20256	CISA AA23-335A
Siemens S7-300/400	No authentication by default	TCP 102	ICS-CERT
Allen-Bradley / Rockwell	No authentication on older firmware	TCP 44818	Rockwell Advisory
Schneider Electric Modicon	Various defaults per model	TCP 502	Schneider Security Bulletin
Hikvision IP Cameras	`admin / 12345` (legacy)	TCP 80/443	CVE-2017-7921

Hunt Procedure: Authentication Failure Analysis on OT Segments

DETECTION ONLY

KQL (MICROSOFT SENTINEL / LOG ANALYTICS)

```
// Detect authentication attempts to OT network segments from external sources
// Requires network segmentation and logging at IT/OT boundary
Syslog
| where Facility == "auth" or Facility == "authpriv"
| where SeverityLevel in ("err", "warning", "crit")
| where Computer has_any ("scada", "hmi", "plc", "rtu", "ot-")
| summarize FailedAttempts = count(),
    SourceIPs = make_set(HostIP, 20)
    by Computer, bin(TimeGenerated, 15m)
| where FailedAttempts > 5
| sort by FailedAttempts desc
```

☐ Audit all PLC, HMI, and RTU devices for default or factory credentials
☐ Verify Unitronics devices are not using default password "1111" (CISA AA23-335A)
☐ Check Hikvision cameras for default admin/12345 credentials and unpatched firmware
☐ Implement account lockout or alerting for repeated failed authentications to OT devices
☐ Document all OT device credentials in a secure password management system

3 HMI/SCADA Unauthorized Access Detection

Duration: 30 min Priority: CRITICAL

Objective: Detect unauthorized access to HMI web interfaces and SCADA consoles, the type of access FAD Team has claimed and published screenshots of on Telegram.

Background

FAD Team published screenshots on Telegram showing what appeared to be HMI (Human Machine Interface) dashboards from SCADA systems in Israel and other countries. These screenshots could represent monitoring-only access to exposed HMI web portals or full operational control. Detecting unauthorized access to HMI interfaces is critical because even monitoring-only access provides an attacker with reconnaissance data about facility operations, and many HMI web interfaces do not separate read and write access.

Hunt Procedure: HMI Web Interface Access from External IPs

DETECTION ONLY

KQL (WEB APPLICATION FIREWALL / IIS LOGS)

```
// Detect access to HMI web interfaces from non-internal IP addresses
// Adjust URL patterns to match your HMI vendor's web paths
W3CIISLog
| where csUriStem has_any (
    "/hmi", "/scada", "/webvisu", "/awp",
    "/portal", "/monitor", "/dashboard",
    "/cgi-bin/ViewerFrame", "/unitronics")
| where cIP !startswith "10." and cIP !startswith "172.16."
    and cIP !startswith "192.168."
| project TimeGenerated, cIP, csUriStem, csMethod,
    scStatus, csUserAgent, sSiteName
| sort by TimeGenerated desc
```

Hunt Procedure: Anomalous Access Times to OT Systems

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect logins to OT workstations outside normal operating hours
// Many OT environments have predictable access patterns
SecurityEvent
| where Computer has_any ("scada", "hmi", "ot-", "plc-ws")
| where EventID in (4624, 4625)   // Logon success and failure
| where hourofday(TimeGenerated) !between (6 .. 18)  // Outside business hours
| project TimeGenerated, Computer, Account, LogonType,
    IpAddress, EventID
| sort by TimeGenerated desc
```

☐ Review all HTTP/HTTPS access logs for HMI web interfaces; identify any external IP access
☐ Establish baseline of authorized HMI users and access times
☐ Check for VNC (port 5900-5999) or RDP (port 3389) connections to OT workstations from unexpected sources
☐ If HMI screenshots have appeared on Telegram channels, immediately audit access logs for the corresponding time period

4 PLC Logic and Setpoint Modification Detection

Duration: 35 min Priority: CRITICAL

Objective: Detect unauthorized modifications to PLC ladder logic, setpoints, or operational parameters that could indicate physical process manipulation.

Background

FAD Team claimed "manipulation of control" of PLC systems. CyberAv3ngers developed custom ladder logic files to download to compromised Unitronics PLCs (CISA AA23-335A). PLC logic modifications represent the highest-impact OT attack because they can alter physical processes (water treatment chemical dosing, pump speeds, valve states) with potential safety consequences. Detection requires either OT-specific monitoring or network-level analysis of industrial protocol traffic.

Hunt Procedure: PLC Program Download Detection (Network Level)

DETECTION ONLY

SURICATA / ZEEK / OT NETWORK MONITOR

```
# Detect Modbus function codes associated with PLC programming
# Function code 0x10 (Write Multiple Registers) in large quantities
# Function code 0x0F (Write Multiple Coils) in large quantities
# These are normal in small volumes during maintenance windows
# Alert on these outside maintenance windows or from unexpected IPs

# Suricata rule example:
alert modbus any any -> $OT_NETWORK any (
    msg:"MODBUS Write Multiple Registers - Potential PLC Reprogramming";
    modbus: function 16;
    threshold: type threshold, track by_src, count 50, seconds 60;
    sid:3001001; rev:1;)

# For Unitronics PCOM protocol (TCP 20256):
alert tcp any any -> $OT_NETWORK 20256 (
    msg:"PCOM Traffic to Unitronics PLC - Potential Unauthorized Access";
    flow:to_server,established;
    sid:3001002; rev:1;)
```

Alternative: IT-Side Detection (No OT Monitoring)

DETECTION ONLY

KQL (NETWORK FLOW LOGS)

```
// For organizations without OT protocol monitoring:
// Detect traffic to PLC programming ports from unexpected sources
AzureNetworkAnalytics_CL
| where DestPort_d in (502, 102, 44818, 20256)  // OT protocol ports
| where SrcIP_s !in (AUTHORIZED_ENGINEERING_WORKSTATIONS)
| project TimeGenerated, SrcIP_s, DestIP_s, DestPort_d,
    BytesSent_d, BytesReceived_d
| sort by TimeGenerated desc
```

☐ Verify that PLC program backups exist for all critical PLCs and are stored offline
☐ Compare current PLC logic against known-good backups (hash comparison where possible)
☐ Review process historian data for unexpected setpoint changes in the past 90 days
☐ Confirm that PLC programming ports (Modbus 502, S7comm 102, EtherNet/IP 44818) are only accessible from authorized engineering workstations

Safety-Critical: PLC Logic Verification
If PLC logic modifications are detected, do NOT immediately revert without consulting process engineers. Reverting corrupted or modified PLC logic without understanding the current process state could cause physical safety hazards. Isolate the PLC from the network first, then coordinate with operations staff for safe recovery.

5 OT Network Anomalous Traffic Patterns

Duration: 30 min Priority: HIGH

Objective: Detect anomalous network traffic patterns within OT segments that could indicate reconnaissance, lateral movement, or unauthorized control actions.

Background

OT networks are characteristically predictable. The same devices communicate with the same peers using the same protocols at regular intervals. Any deviation from this baseline is potentially significant. Hacktivist actors conducting reconnaissance within an OT network will generate traffic patterns that differ from normal operations: new source/destination pairs, unusual protocols, scanning activity, or connections to internet-facing services from OT segments.

Hunt Procedure: New Communication Pairs in OT Segments

DETECTION ONLY

KQL (NETWORK FLOW LOGS / OT NETWORK MONITOR)

```
// Identify new source-destination pairs in OT network segments
// Compare recent connections against a 30-day baseline
let OT_Subnet = "10.10.0.0/16";  // Replace with your OT subnet
let BaselinePeriod = ago(30d);
let RecentPeriod = ago(24h);
let Baseline = AzureNetworkAnalytics_CL
    | where TimeGenerated between (BaselinePeriod .. ago(24h))
    | where SrcIP_s startswith "10.10."
    | distinct SrcIP_s, DestIP_s, DestPort_d;
AzureNetworkAnalytics_CL
| where TimeGenerated > RecentPeriod
| where SrcIP_s startswith "10.10."
| distinct SrcIP_s, DestIP_s, DestPort_d
| join kind=leftanti Baseline on SrcIP_s, DestIP_s, DestPort_d
```

Hunt Procedure: Outbound Internet Connections from OT Segments

DETECTION ONLY

KQL (FIREWALL LOGS)

```
// OT devices should rarely initiate outbound internet connections
// Any outbound connection from OT segments may indicate compromise
AzureNetworkAnalytics_CL
| where Direction_s == "Outbound"
| where SrcIP_s startswith "10.10."  // Replace with OT subnet
| where DestIP_s !startswith "10." and DestIP_s !startswith "172.16."
    and DestIP_s !startswith "192.168."
| project TimeGenerated, SrcIP_s, DestIP_s, DestPort_d,
    Protocol_s, BytesSent_d
| sort by TimeGenerated desc
```

☐ Establish and document a baseline of normal OT network communication patterns
☐ Verify that OT networks are segmented from IT networks with monitored firewall boundaries
☐ Investigate any outbound internet connections originating from OT network segments
☐ Check for scanning activity (sequential IP or port access) within OT segments

6 SQL Injection Campaign Detection

Duration: 30 min Priority: HIGH

Objective: Detect SQL injection attacks against public-facing web applications, FAD Team's most technically verified attack capability.

Background

FAD Team has conducted sustained global SQL injection campaigns targeting military, education, and government web applications (Cyberwarzone, Unit 42). The March 2026 Kuwait offensive included database exfiltration of 23,553 user records from the ATV Kuwait application. SQL injection remains the group's most reliably documented technical capability. Organizations with public-facing web applications containing database backends are at risk.

Hunt Procedure: WAF SQL Injection Alert Analysis

DETECTION ONLY

KQL (AZURE WAF / APPLICATION GATEWAY)

```
// Analyze WAF logs for SQL injection attempts
// Focus on attempts that bypassed WAF or returned 200 OK
AzureDiagnostics
| where ResourceType == "APPLICATIONGATEWAYS"
| where action_s == "Matched" or action_s == "Blocked"
| where ruleGroup_s == "REQUEST-942-APPLICATION-ATTACK-SQLI"
| summarize AttemptCount = count(),
    DistinctPaths = dcount(requestUri_s),
    SuccessCount = countif(httpStatus_d == 200)
    by clientIP_s, bin(TimeGenerated, 1h)
| where AttemptCount > 10
| sort by AttemptCount desc
```

Hunt Procedure: Database Error Exposure in Web Logs

DETECTION ONLY

KQL (IIS / APACHE LOGS)

```
// Detect SQL error messages in web server responses
// These indicate either successful SQLi probing or misconfigured error handling
W3CIISLog
| where scStatus == 500
| where csUriQuery has_any (
    "UNION", "SELECT", "INSERT", "UPDATE", "DELETE",
    "DROP", "OR%201=1", "OR+1=1", "' OR '",
    "CONCAT", "GROUP_CONCAT", "INFORMATION_SCHEMA",
    "SLEEP(", "WAITFOR", "BENCHMARK(")
| project TimeGenerated, cIP, csUriStem, csUriQuery,
    scStatus, csUserAgent
| sort by TimeGenerated desc
```

Hunt Procedure: Mass Data Exfiltration from Databases

DETECTION ONLY

KQL (SQL SERVER AUDIT LOGS)

```
// Detect unusually large result sets or bulk data access
// FAD Team exfiltrated 23,553+ records from ATV Kuwait
AzureDiagnostics
| where ResourceType == "SERVERS/DATABASES"
| where Category == "SQLSecurityAuditEvents"
| where action_name_s has_any ("SELECT", "BATCH")
| where affected_rows_d > 1000
| project TimeGenerated, server_principal_name_s,
    database_name_s, action_name_s, affected_rows_d,
    client_ip_s, statement_s
| sort by affected_rows_d desc
```

☐ Review WAF logs for SQL injection attempts in the past 30 days; investigate any that returned HTTP 200
☐ Verify that database error messages are not exposed in web application responses
☐ Audit database access logs for bulk SELECT operations from web application service accounts
☐ Confirm parameterized queries are used in all database-facing web applications (prevent SQLi at source)

7 Web Application Defacement Detection

Duration: 25 min Priority: HIGH

Objective: Detect website defacement, a core hacktivist tactic used by FAD Team and the Cyber Islamic Resistance coalition.

Background

Website defacement is a primary tactic across the Iranian hacktivist ecosystem. FAD Team conducts defacement operations against government and media targets for psychological impact and propaganda purposes. Defacement often accompanies SQL injection (the attacker gains write access to the web application) or exploits CMS vulnerabilities. Detection relies on web content integrity monitoring.

Hunt Procedure: Web Content Integrity Monitoring

DETECTION ONLY

KQL (FILE INTEGRITY MONITORING)

```
// Detect modifications to web content files (HTML, JS, CSS, images)
// in web server document roots
DeviceFileEvents
| where ActionType in ("FileModified", "FileCreated")
| where FolderPath has_any ("inetpub\\wwwroot", "var/www/html",
    "htdocs", "public_html")
| where FileName endswith_any (".html", ".htm", ".php", ".asp",
    ".aspx", ".js", ".css", ".jpg", ".png", ".gif")
| where InitiatingProcessFileName !in~ ("w3wp.exe", "httpd",
    "nginx", "deploy.exe")  // Exclude known deployment processes
| project Timestamp, DeviceName, FileName, FolderPath,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

Hunt Procedure: Hacktivist Defacement Signature Detection

DETECTION ONLY

KQL (WEB APPLICATION LOGS)

```
// Detect POST requests that may upload defacement content
// Focus on file upload endpoints and CMS admin panels
W3CIISLog
| where csMethod == "POST"
| where csUriStem has_any ("/upload", "/admin", "/wp-admin",
    "/administrator", "/filemanager", "/editor")
| where cIP !startswith "10." and cIP !startswith "192.168."
| where scStatus in (200, 201, 302)
| project TimeGenerated, cIP, csUriStem, scStatus,
    csUserAgent, scBytes
| sort by TimeGenerated desc
```

☐ Implement file integrity monitoring (FIM) on all public-facing web server document roots
☐ Establish automated hash comparison of homepage and key pages against known-good versions
☐ Monitor for unauthorized CMS admin panel access from external IPs
☐ Configure alerts for any file creation or modification in web roots outside deployment windows

8 VNC/RDP Unauthorized Access to OT Workstations

Duration: 25 min Priority: HIGH

Objective: Detect unauthorized remote desktop access (VNC, RDP) to OT engineering workstations and HMI stations that could enable SCADA/PLC manipulation.

Background

OT engineering workstations with VNC or RDP access represent a bridge between IT and OT networks. An attacker who gains remote desktop access to an engineering workstation can directly interact with SCADA software, modify PLC programs, and change process parameters. Iranian hacktivist groups have historically targeted exposed VNC/RDP services. The CyberAv3ngers Unitronics campaign leveraged direct protocol access, but broader OT access often comes through compromised engineering workstations.

Hunt Procedure: External VNC/RDP Connections to OT Assets

DETECTION ONLY

KQL (NETWORK FLOW LOGS)

```
// Detect VNC and RDP connections from external sources to OT workstations
AzureNetworkAnalytics_CL
| where DestPort_d in (3389, 5900, 5901, 5902, 5903)
| where DestIP_s startswith "10.10."  // Replace with OT subnet
| where SrcIP_s !startswith "10." and SrcIP_s !startswith "172.16."
    and SrcIP_s !startswith "192.168."
| project TimeGenerated, SrcIP_s, DestIP_s, DestPort_d,
    BytesSent_d, BytesReceived_d
| sort by TimeGenerated desc
```

Hunt Procedure: RDP Logon to OT Workstations

DETECTION ONLY

KQL (WINDOWS SECURITY EVENTS)

```
// Detect RDP logons (Type 10) to OT-designated workstations
SecurityEvent
| where EventID == 4624
| where LogonType == 10  // RemoteInteractive (RDP)
| where Computer has_any ("ew-", "eng-", "scada-", "hmi-", "ot-")
| project TimeGenerated, Computer, Account, IpAddress,
    LogonType, WorkstationName
| sort by TimeGenerated desc
```

☐ Audit all VNC and RDP services running on OT network segments
☐ Verify that remote access to OT workstations requires VPN + MFA (no direct internet exposure)
☐ Review RDP logon events (Event ID 4624, Type 10) on engineering workstations for the past 90 days
☐ Confirm that VNC services on OT workstations use strong passwords and are not exposed to the internet

9 DDoS and Volumetric Attack Detection

Duration: 25 min Priority: HIGH

Objective: Detect DDoS attacks targeting public-facing services, a confirmed and frequent FAD Team tactic with 149+ attacks documented across 16 countries.

Background

Between February 28 and March 2, 2026, the Cyber Islamic Resistance coalition (including FAD Team) conducted 149 hacktivist-driven DDoS attacks targeting 110 organizations across 16 countries (Rescana). Kuwait accounted for 28% of targets, Israel 27.1%, and Jordan 21.5%. FAD Team's March 5 Kuwait offensive included DDoS against government portals, the military website, and the Ministry of Health. DDoS attacks serve dual purposes: service disruption and distraction while other operations (data exfiltration, defacement) proceed.

Hunt Procedure: HTTP Flood Pattern Detection

DETECTION ONLY

KQL (AZURE WAF / CDN LOGS)

```
// Detect HTTP flood DDoS patterns against public-facing services
AzureDiagnostics
| where ResourceType == "APPLICATIONGATEWAYS"
| summarize RequestCount = count(),
    DistinctIPs = dcount(clientIP_s),
    AvgResponseTime = avg(timeTaken_d)
    by bin(TimeGenerated, 5m), host_s
| where RequestCount > 10000
| sort by RequestCount desc
```

Hunt Procedure: Concurrent DDoS and Data Exfiltration Detection

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Check if DDoS activity coincides with other suspicious activity
// Hacktivists often use DDoS as a distraction during data theft
let DDoSPeriods = AzureDiagnostics
    | where TimeGenerated > ago(24h)
    | where ResourceType == "APPLICATIONGATEWAYS"
    | summarize RequestCount = count() by bin(TimeGenerated, 5m), Resource
    | where RequestCount > 10000
    | project DDoSTime = TimeGenerated, Resource;
SecurityEvent
| where TimeGenerated > ago(24h)
| where EventID in (4624, 4625)
| where IpAddress !startswith "10." and IpAddress !startswith "192.168." and IpAddress !startswith "172.16."
| extend BinnedTime = bin(TimeGenerated, 5m)
| join kind=inner DDoSPeriods on $left.BinnedTime == $right.DDoSTime
| summarize LoginAttempts = count(),
    DistinctAccounts = dcount(TargetUserName),
    Accounts = make_set(TargetUserName, 10)
    by IpAddress, Resource, BinnedTime
| sort by LoginAttempts desc
```

☐ Verify DDoS protection is active on all public-facing services (CDN, WAF, cloud DDoS mitigation)
☐ Review traffic patterns for the past 30 days for volumetric spikes
☐ During any DDoS event, simultaneously check for data exfiltration, SQLi, or defacement activity
☐ Verify that government and media portals have dedicated DDoS mitigation

10 Data Exfiltration and Leak Infrastructure Detection

Duration: 30 min Priority: HIGH

Objective: Detect data exfiltration from organizational systems and monitor for leaked data appearing on Telegram channels and paste sites.

Background

FAD Team publishes stolen data on Telegram for maximum psychological impact. The March 2026 Kuwait offensive included publication of 23,553 user records in three PDF files (names, emails, passwords, phone numbers). The group announced plans to continue publishing databases. Data exfiltration typically follows SQL injection or direct database access. Detection requires monitoring both outbound data flows and external publication channels.

Hunt Procedure: Anomalous Outbound Data Volume

DETECTION ONLY

KQL (NETWORK FLOW LOGS)

```
// Detect unusually large outbound data transfers from web/database servers
AzureNetworkAnalytics_CL
| where Direction_s == "Outbound"
| where SrcIP_s in (WEB_SERVER_IPS, DATABASE_SERVER_IPS)
| summarize TotalBytesSent = sum(BytesSent_d)
    by SrcIP_s, DestIP_s, bin(TimeGenerated, 1h)
| where TotalBytesSent > 100000000  // 100 MB threshold
| sort by TotalBytesSent desc
```

Hunt Procedure: Telegram API Communication Detection

INVESTIGATION AID

KQL (PROXY / FIREWALL LOGS)

```
// Detect direct communication with Telegram API from servers
// Legitimate Telegram use from desktops is expected;
// Telegram API calls from servers may indicate automated exfiltration
CommonSecurityLog
| where RequestURL has_any (
    "api.telegram.org",
    "t.me",
    "telegram.org/bot")
| where SourceIP in (SERVER_IP_LIST)  // Replace with server IPs
| project TimeGenerated, SourceIP, RequestURL, RequestMethod,
    SentBytes, ReceivedBytes
| sort by TimeGenerated desc
```

External Monitoring Recommendations

In addition to internal detection, organizations should:

- Monitor known Iranian hacktivist Telegram channels for organizational data mentions
- Subscribe to threat intelligence feeds that track paste sites (Pastebin, Ghostbin, Rentry) for leaked credentials
- Set up Google Alerts for organizational domain names combined with "hack," "breach," "leak," or "data"
- Engage a digital risk protection service to monitor Telegram, dark web forums, and paste sites for organizational data

☐ Review outbound data transfer logs from database and web servers for the past 30 days
☐ Check for Telegram API communication from server infrastructure (not expected in most environments)
☐ Verify data loss prevention (DLP) rules are configured for PII patterns (SSN, credit card, email lists)
☐ Search Telegram and paste sites for any organizational data that may have already been leaked

A Appendix A: OT Monitoring Infrastructure Requirements

Minimum OT Monitoring Capabilities

The hunt modules in this guide reference various monitoring capabilities. The table below maps each module to the required monitoring infrastructure and provides alternative approaches for organizations without dedicated OT monitoring.

Module	Primary Detection	Required Infrastructure	Alternative (No OT Monitoring)
1. Internet-Exposed ICS	External scanning (Shodan/Censys)	Public IP range inventory	Shodan search is accessible to all organizations
2. Default Credentials	OT device audit	OT asset inventory	Manual audit of known OT devices; vendor documentation review
3. HMI Unauthorized Access	Web/application logs	HMI web server logging	Firewall logs for traffic to HMI ports from external IPs
4. PLC Logic Modification	OT network protocol monitoring	OT IDS (Claroty, Nozomi, Dragos)	Firewall logs for traffic to OT protocol ports; manual PLC backup comparison
5. OT Traffic Anomalies	Network flow analysis	OT network TAP + flow exporter	IT/OT boundary firewall logs; NetFlow from OT switches
6. SQL Injection	WAF and web server logs	WAF (Azure, AWS, Cloudflare)	IIS/Apache access logs; database audit logs
7. Defacement	File integrity monitoring	FIM agent on web servers	Periodic manual comparison of web content hashes
8. VNC/RDP to OT	Network flow + Windows event logs	Windows event forwarding from OT workstations	Firewall logs for RDP/VNC ports to OT subnets
9. DDoS Detection	CDN/WAF analytics	DDoS mitigation service	ISP-level traffic analysis; web server response time monitoring
10. Data Exfiltration	Network flow + DLP	DLP solution + proxy logs	Firewall outbound traffic analysis; Telegram channel monitoring

Recommended OT Monitoring Platforms
For organizations seeking to implement dedicated OT network monitoring, the following platforms provide passive network detection and asset discovery for industrial environments: Claroty (clarotyxdome.com), Nozomi Networks (nozominetworks.com), Dragos Platform (dragos.com), and Microsoft Defender for IoT (formerly CyberX). These platforms can detect anomalous OT protocol traffic, unauthorized PLC programming, and new device discovery without impacting process operations.

B Appendix B: References

Government Advisories

[1] **CISA** - "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities" (Advisory AA23-335A, November 2023)
cisa.gov

[2] **CISA** - "Iranian Cyber Actors May Target Vulnerable [Critical Infrastructure]" (June 2025)
ic3.gov

[3] **MITRE ATT&CK** - "CyberAv3ngers, Soldiers of Solomon, Group G1027"
attack.mitre.org

[4] **WaterISAC / Gate15** - "Joint Advisory: Middle East Conflict and Critical Infrastructure" (March 2026)
waterisac.org

Vendor Threat Intelligence (Primary)

[5] **Palo Alto Unit 42** - "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran" (March 2026)
unit42.paloaltonetworks.com

[6] **Cyberwarzone** - "Fatimion Cyber Team: Inside the Iran-Linked Hacking Group Waging Cyber War Across the Middle East" (March 6, 2026)
cyberwarzone.com

[7] **Claroty Team82** - "Inside a New OT/IoT Cyberweapon: IOCONTROL" (December 2024)
claroty.com

[8] **The Washington Institute** - "Profile: Fatemiyoun Electronic Squad"
washingtoninstitute.org

[9] **SecurityScorecard** - "From The Depths of the Shadows: IRGC and Hacker Collectives Of The 12-Day War" (August 2025)
securityscorecard.com

[10] **Flashpoint** - "Escalation in the Middle East: Tracking Operation Epic Fury" (March 2026)
flashpoint.io

[11] **CloudSEK** - "A Threat Actor Landscape Assessment of ICS/OT Targeting in the 2026 Iran-US Conflict" (March 2026)
cloudsek.com

Secondary Sources

[12] **Rescana** - "Global Surge: 149 Hacktivist DDoS Attacks Target SCADA and Critical Infrastructure Across 16 Countries" (March 2026)
rescana.com

[13] **CSIS** - "Beyond Hacktivism: Iran's Coordinated Cyber Threat Landscape" (March 2026)
csis.org

[14] **Dark Reading** - "Pro-Iranian Actors Launch Barrage of Cyberattacks" (March 2026)
darkreading.com

[15] **Hackmanac** - FAD Team Kuwait ATV breach claim confirmation (March 2026)
x.com/H4ckmanac

[16] **Intruvent Technologies** - "Iran Conflict Geopolitical Situation Report v1.3" (INT-GSR-2026-IRANCONFLICT-v1.3, March 2026)

NEED HELP IMPLEMENTING THESE DETECTIONS?

Our threat hunting team can deploy, tune, and operationalize these detection rules in your environment.

- ✓ Detection rule deployment and tuning
- ✓ Managed threat hunting operations
- ✓ Incident response retainer

Contact Our Team

or

Automate continuous detection with BRACE, our sector-specific threat intelligence platform. See BRACE plans →