HIVEPRO STRATEGIC INTELLIGENCE

# The Great Convergence: Iranian Cyber & Kinetic Warfare

Feb 28 – Mar 5, 2026 marks the single most significant escalation in hybrid warfare history — kinetic strikes and digital disruption operating as a unified strategic weapon. **Swipe to understand the full threat.**

TLP: CLEAR

NATO ADMIRALTY: B2

EXECUTIVE SUMMARY

# The Numbers Behind Operation Epic Fury

In just five days, the world witnessed an unprecedented synchronization of large-scale kinetic action and cyber disruption. These are the defining metrics of the convergence event.

## ~900

### Kinetic Strikes

In the first 12 hours targeting IRGC command, missile programs, and nuclear sites

## 1-4%

### Internet Remaining

Iranian internet connectivity surviving at peak domestic blackout

## ~$80

### Crude Surge

Brent crude price spike (per barrel) following Strait of Hormuz threat escalation

STRATEGIC TIMELINE

# Kinetic–Cyber Synchronization: Day by Day

Pre-conflict reconnaissance transitioned seamlessly into coordinated offensive action. The timeline below reflects the precision of Iranian pre-positioning — and the speed of the convergence.

1

## Early Feb 2026

**Reconnaissance Phase:** Iranian-linked actors surge API and mobile app probing against Israeli and Gulf government infrastructure.

2

## Feb 26, 2026

**Final Staging:** Pre-positioning continues. Cyber indicators signal imminent operations. No kinetic action yet.

3

## Feb 28, 2026

**D-Day — Operations Epic Fury & Roaring Lion:** ~900 strikes in 12 hours. Supreme Leader Khamenei killed; confirmed by Iranian state media March 1.

4

## Mar 2, 2026

**Cyber Retaliation Escalates:** Israeli strikes eliminate MOIS Deputy Minister Panjaki (Handala Hack director). "Electronic Operations Room" established by Iranian-aligned actors.

5

## Mar 4–5, 2026

**Infrastructure Sabotage Claims:** Handala Hack, APT IRAN, Z-Pentest, and CyberAv3ngers all claim ICS/OT compromises across energy, water, and grain infrastructure.

THREAT LANDSCAPE

# The Iranian Cyber Ecosystem

Iran's cyber apparatus operates through a multi-layered structure: state-directed APTs, front companies, and hacktivist personas — providing plausible deniability while executing high-impact, strategically coordinated operations. Despite near-total domestic internet blackout, **pre-positioned distributed assets outside Iran maintained full offensive tempo.**

ADVERSARY ORDER OF BATTLE | ADMIRALTY: A1

# Iranian Cyber Actor Registry

Seven primary threat groups active Feb 28 – Mar 5, 2026. Each operates under distinct agency direction with specialized tactical roles.

| Actor | Common Aliases | Agency | Specialty | Primary Targets |
|---|---|---|---|---|
| Void Manticore | Handala Hack, Karma, Storm-0842 | MOIS | Data Theft, Wipers, Psych Ops | IT Services, Healthcare, Energy |
| Static Kitten | MuddyWater, Mango Sandstorm | MOIS | Phishing, Espionage | Telecom, Defense, Govt |
| Hazel Sandstorm | OilRig, APT34, Helix Kitten | MOIS | Credential Harvesting, Backdoors | Critical Infra, Telecom |
| Cotton Sandstorm | Emennet Pasargad, Aria Sepehr | IRGC | Influence Ops, Infostealers | Political Networks, Media, NGOs |
| Pioneer Kitten | UNC757, Lemon Sandstorm | Gov't Contractor | Edge Exploitation, Access Broker | VPN/Firewall Infra, Tech |
| CyberAv3ngers | Cyber Avengers | IRGC-CEC | ICS/OT Sabotage, PLC Targeting | Water, Power Grid, Fuel |
| Charming Kitten | APT35, Phosphorus, Mint Sandstorm | IRGC | Dissident Tracking, Spearphishing | High-profile Individuals, Academia |

**Analyst Note:** Static Kitten/MuddyWater is operationally distinct from OilRig/APT34 (Hazel Sandstorm) — both MOIS-directed but tracked separately. Pioneer Kitten's specific agency sponsorship (MOIS vs. IRGC) remains unconfirmed.

ACTOR DEEP DIVE

ADMIRALTY: A2

# Void Manticore / Handala Hack

## Leadership Decapitation

Directing Deputy Intelligence Minister Yahya Hosseini Panjaki — assessed director of Handala Hack — was eliminated in Israeli strikes on MOIS HQ, Feb 28.

## Operational Pattern

Targets IT service providers for downstream access to defense-adjacent entities. Uses **Starlink IP ranges** to bypass domestic internet disruptions. Velocity-focused and opportunistic.

## Notable Claims

Compromise of Israeli energy exploration company and Jordan's fuel systems. "RedWanted" site used to list and hunt individuals supporting Israel.

ACTOR DEEP DIVE

ADMIRALTY: A2

# Static Kitten: Operation Olalampo

Active since late January 2026, Operation Olalampo deploys an unprecedented four-malware suite. Notably, debug strings contain **emoji characters** — a low-confidence indicator of AI-assisted development by an Iranian state actor.

01

## GhostFetch

Sandbox-aware first-stage downloader — detects analysis environments before proceeding.

02

## GhostBackDoor

Advanced second-stage implant loaded directly into memory — **no disk write**, evading standard AV detection.

03

## CHAR

Rust-based backdoor with Telegram C2 (`stager_51_bot`). Unconventional coding patterns suggest possible AI-assisted development.

04

## HTTP_VIP

Native downloader deploying AnyDesk for persistent remote access to compromised systems.

**Strategic Objective:** Maintain long-term espionage footholds in telecom and government networks across MENA, increasingly exploiting public-facing servers.

ACTOR DEEP DIVE

ADMIRALTY: A1

# CyberAv3ngers: ICS/OT Sabotage Threat

## Directing Agency

IRGC Cyber Electronic Command (IRGC-CEC) — the most operationally dangerous ICS threat actor in the Iranian ecosystem.

## Primary Targets

Water treatment, energy utilities, and fuel infrastructure in the **U.S., Israel, Jordan, and Gulf states.** Specifically targets Unitronics Vision Series PLCs.

## Mar 4 Activity

Shared imagery of compromised **VeroPoint PLC interfaces** and energy monitoring dashboards — signaling persistent access and intent for physical disruption.

DESTRUCTIVE MALWARE

ADMIRALTY: C3

# Sicarii Wiper: Suspected False Flag

### ⚠️ Irrecoverable Destruction

Sicarii regenerates a new RSA key pair locally, encrypts files, then **discards the private key** — making decryption functionally impossible. Total data loss. **Recovery is not possible post-infection regardless of ransom payment.**

### False Flag Assessment

Sicarii implements geo-fencing logic checking time zones, keyboard layouts, and network adapter IP ranges that **prevents execution on Israeli systems** — combined with no confirmed technical link to any Iranian group.

**Analyst Assessment:** High-probability false flag operation. The geo-fencing logic protecting Israeli systems while the malware operates in an Iranian-attributed conflict window is a deliberate misdirection designed to invite misattribution. Attribute with extreme caution.

VULNERABILITY INTELLIGENCE | ADMIRALTY: A1

# Critical CVE Exploitation Matrix

**Defender Priority:** All six CVEs have confirmed active exploitation in this conflict window. Patch or mitigate immediately.

| Product | CVE | CVSS | Actor / Method | KEV Date |
|---|---|---|---|---|
| FortiOS, FortiProxy | CVE-2026-24858 | 9.4 | Pioneer Kitten / FortiCloud SSO Auth Bypass | Jan 27, 2026 |
| Ivanti Connect Secure | CVE-2025-0282 | 9.0 | Pioneer Kitten (initial access) / RESURGE implant **(China-nexus: UNC5221)** | Jan 8, 2025 |
| Ivanti EPMM | CVE-2026-1281 | 9.8 | Pioneer Kitten / Unauthenticated RCE | Jan 29, 2026 |
| PHP-CGI (Windows) | CVE-2024-4577 | 9.8 | MuddyWater / RCE on Web Servers | Jun 7, 2024 |
| Palo Alto Expedition | CVE-2024-5910 | 9.8 | Cotton Sandstorm / Admin Account Takeover | Nov 7, 2024 |
| Fortinet SSL VPN | CVE-2018-13379 | 9.8 | APT33 & APT34 / Path Traversal & Credential Leak | Nov 3, 2021 |

**Critical RESURGE Note:** While Pioneer Kitten (Iran) exploits CVE-2025-0282 for initial access, the advanced RESURGE persistence implant — which embeds into the Linux OS — is attributed to UNC5221, a **China-nexus** threat actor. Finding RESURGE means you are dealing with a Chinese APT that walked through the door Iran left open. Any CVE-2025-0282 compromise requires a full factory reset from a clean image; standard patching leaves implants intact.

INFRASTRUCTURE SABOTAGE

ADMIRALTY: B2

# Jordan: Multi-Vector Physical Infrastructure Attack

Claimed by APT IRAN on March 4 as alleged retaliation for drone interceptions. The attack combines agriculture degradation, economic fraud, and energy disruption in a single coordinated campaign.

## Agriculture Sabotage

Gradual temperature elevation in northern grain silos — systematically degrading wheat quality without triggering immediate alarms.

## Economic Fraud

Weighing software manipulation underreporting incoming grain weights by **10%** — a covert financial drain on national food supply chains.

## Energy Disruption

Disabling solar inverters at major farms and manipulating plant control systems to reduce electricity output across the region.

INFRASTRUCTURE SABOTAGE

ADMIRALTY: B2

# Israel: Water & Civil Alert System Targeting

## Water Pump Controls

Z-Pentest Alliance published screenshots of Hebrew-language HMI panels showing real-time flow rate and pump pressure controls — asserting capability to trigger emergency shutdowns.

## Civil Alert Attack

The "Conquerors Electronic Army" claimed synchronized attacks against Israeli civil emergency alerting systems, **timed to coincide with active missile strikes.**

**Analytic Assessment:** Targeting civil alert systems during active bombardment represents a deliberate attempt to degrade life-safety warnings to civilians. This constitutes a direct attack on the civilian population's ability to seek shelter.

INFO-OPS

ADMIRALTY: A1

# The RedAlert APK: Weaponizing Civilian Safety

## Delivery Mechanism

A malicious replica of the Israeli Home Front Command RedAlert app distributed via Hebrew-language SMS (`redalerts[.]me`) during late February kinetic strikes — targeting civilians actively seeking shelter guidance.

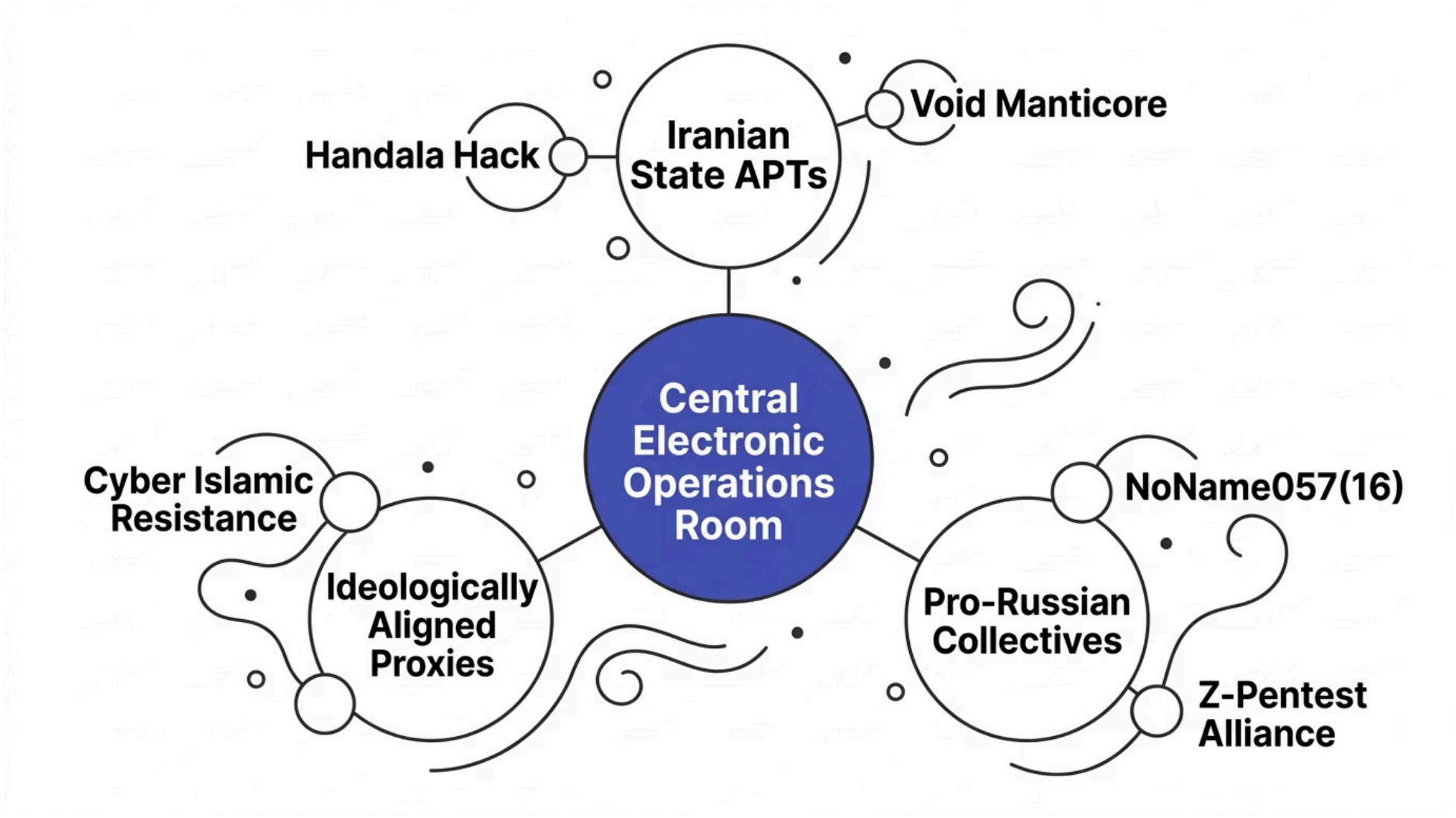
## Capabilities

Harvests **call logs, SMS messages, contacts, and account information** while presenting a fully functional alert interface — victims believe they are protected while being actively exfiltrated.

COORDINATION ARCHITECTURE

# The Electronic Operations Room

Established February 28, 2026 — an unprecedented coordination layer unifying state APTs, ideological proxies, and pro-Russian collectives into a single offensive structure.




This coordination model provides Iran strategic reach beyond its own decimated command infrastructure — proxy actors carry operational tempo while state attribution remains deniable.

INDICATORS OF COMPROMISE

TLP: CLEAR

# Network & Infrastructure Indicators

Immediately ingest the following into your SIEM, EDR, and threat intelligence platforms. All indicators confirmed active within the Feb 28 – Mar 5, 2026 conflict window.

| Type | Indicator Value | Actor / Campaign |
|---|---|---|
| C2 Domain | codefusiontech[.]org | MuddyWater (Op. Olalampo) |
| C2 Domain | connect.il-cert[.]net | Cotton Sandstorm (WezRat) |
| Phishing Domain | whatsapp-meeting.duckdns[.]org | MuddyWater overlap |
| Phishing Domain | redalerts[.]me | RedAlert APK Distribution |
| Telegram Bot C2 | stager_51_bot | MuddyWater (CHAR Backdoor) |
| IP Address | 104.28.244.115 | Pioneer Kitten (Fortinet SSO Bypass) |
| IP Address | 38.54.6.28 | Pioneer Kitten (Account Creation) |
| IP Address | 217.119.139.50 | Pioneer Kitten (FortiGate Access) |

INDICATORS OF COMPROMISE

TLP: CLEAR

# Endpoint & Malware Hash Indicators

Hash values are provided as single unbroken strings. Copy each hash exactly as displayed — do not allow line wrapping when ingesting into SIEM or EDR platforms, as hidden line breaks will cause hunt queries to fail.

| | | |
|---|---|---|
| 5087a896360f5d99fbf4eb859c824d19eb | RedAlert APK | Iranian Info-Ops |
| 6fa358387bf6c2c5e836f7927921c5 (SHA-256) | Replica | |
| `62ED16701A14CE26314F2436D9532FE606C15407` (SHA-1) | SOCKS5 Reverse Proxy | MuddyWater (Op. Olalampo) |
| `9e107d5736611b127529497e0210214c` (MD5) | WezRat Bot ID Hash | Cotton Sandstorm (WezRat) |
| `gshdoc_release_X64_GUI.exe` | GhostFetch Dropper | MuddyWater (Op. Olalampo) |
| `Updater.exe` (internally `bd.exe`) | WezRat Loader | Cotton Sandstorm (WezRat) |
| `JumpViewUi.dll` | Upload / Cookie Theft Module | Cotton Sandstorm (WezRat) |
| `STITP.dll` | Screenshot Module | Cotton Sandstorm (WezRat) |

**SOC Note — RedAlert APK Hash:** The authoritative SHA-256 for the malicious RedAlert APK replica should be sourced directly from the FBI/IC3 advisory. Add to mobile MDM blocklists and EDR immediately upon confirmation. Do not rely on the placeholder value above for operational hunting.

POST-EXPLOITATION HUNT

# Hunt These Accounts Now

Immediately detect and investigate the creation of any of the following privileged accounts — all are **confirmed indicators of post-exploitation** following Fortinet SSO or Ivanti compromise. All 10 accounts must be monitored.

- **audit**
- **backup**
- **itadmin**
- **secadmin**
- **support**
- **backupadmin**
- **remoteadmin**
- **svcadmin**
- **system**
- **account**

Any of these accounts appearing in your environment following a Fortinet or Ivanti alert constitutes confirmed breach. Escalate immediately — do not treat as routine access management.

MITIGATION FRAMEWORK

# Pillar 1: Identity & Access Hardening

01

## FortiCloud SSO Remediation

Immediately disable "Allow administrative login using FortiCloud SSO" on all Fortinet devices unless strictly required. Audit all local admin accounts for post-exploitation indicators.

02

## Ivanti Rebuild Protocol

For confirmed CVE-2025-0282 compromise: **factory reset using an external known-clean image**; apply the patch; reset all credentials including krbtgt (twice). Standard patching leaves RESURGE implants intact.

03

## Enterprise Credential Rotation

Implement immediate enterprise-wide credential rotation to neutralize actors relying on harvested initial access from prior reconnaissance phases.

MITIGATION FRAMEWORK

# Pillar 2: ICS/OT Protection

## Unitronics PLC Hardening

Change default credentials on all Unitronics Vision Series PLCs and HMIs. **Eliminate direct internet exposure using VPNs immediately.** CyberAv3ngers specifically targets these devices.

## Air-Gap & Segment

Strictly isolate OT/ICS networks from corporate IT. Deploy industrial DMZs. Any IT-OT connectivity is an attack surface in the current threat environment.

## Behavioral OT Monitoring

Hunt for **MITRE ATT&CK ICS T0813** "Impair Process Control" — anomalous changes in pump pressure, flow rates, or inverter states outside operational schedules are active attack indicators.

MITIGATION FRAMEWORK

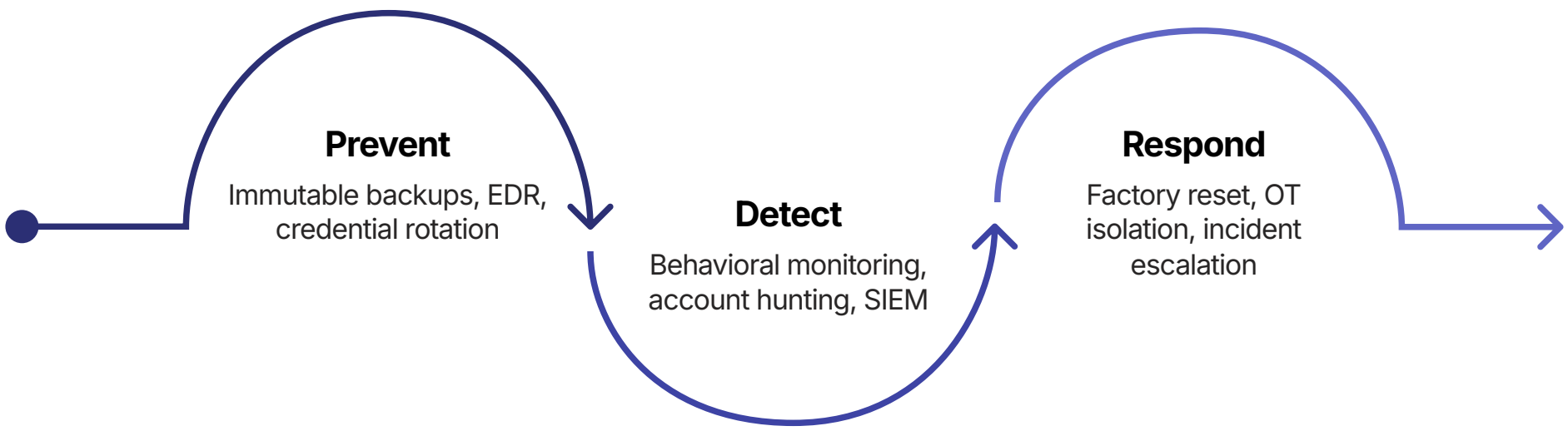
# Pillar 3: Malware Defense

## Immutable Backup Validation

Sicarii ransomware causes **irreversible data destruction** — decryption is impossible regardless of ransom payment. At minimum, one backup copy must be stored offline or in an immutable format. **Validate backup integrity now.**

## Pre-Execution Binary Blocking

Signature-based AV fails against WezRat and CHAR's polymorphic techniques. **Deploy behavioral EDR solutions** that block unknown binary execution. Memory-resident malware (GhostBackDoor) requires memory scanning capabilities.



STRATEGIC CONCLUSION

# The Convergence Is Here

The defense of the VPN edge, the hardening of global energy infrastructure, and the protection of the information environment are **the critical battlegrounds of 2026.** The Iranian cyber threat is no longer a secondary concern managed by IT departments — it demands a coordinated, multi-national response at the highest levels of organizational and government leadership.

> The actors have demonstrated they can operate through a near-total domestic internet blackout. Pre-positioning, distributed infrastructure, and proxy coordination make attribution-based defense insufficient. **Harden posture now — before the next convergence event.**

**📌 Share this report with your SOC, CISO, and national security leadership. Tag a defender who needs to see this.**