SHIELDWORKZ

OT CYBER THREAT INTELLIGENCE ADVISORY

MIDDLE EAST

TABLE OF CONTENTS

EXECUTIVE SUMMARY **3**

Intelligence Overview 3
Key Intelligence Findings *3*
Top Risks Facing Industrial Operators *3*
Regional Threat Outlook *4*
Executive Recommendations *4*

ACTIVE THREAT ACTOR LANDSCAPE **6**

Iranian State-Sponsored Actors 6
BAUXITE / CyberAv3ngers (IRGC-Affiliated) *6*
APT33 (Elfin / Refined Kitten) *6*
APT34 / OilRig (Hazel Sandstorm / Crambus) *7*
MuddyWater (Static Kitten / MERCURY) *7*
Moses Staff / Abraham's Ax *7*
Predatory Sparrow (Gonjeshke Darande) *7*
Russian-Nexus Actors 8
ELECTRUM / Sandworm (GRU Unit 74455) *8*
Industrial Ransomware Operators 8
RansomHub and OT-Capable Affiliates *8*
Cl0p and Industrial Data Extortion Groups *8*

THREAT TRENDS: LAST 6–12 MONTHS **10**

Living-Off-the-Land Dominates Pre-OT Intrusion Phases 10
Remote Access Infrastructure as Primary Initial Access Vector 10
OT Ransomware Functional Convergence 10
Supply Chain and Software Update Compromise 10
Engineering Workstation Targeting 10
Industrial Protocol Abuse 10
AI-Enabled Reconnaissance and Targeting 11
Hybrid Physical-Cyber Attack Models 11

INDUSTRIAL ASSETS AT RISK **12**

Distributed Control Systems (DCS) 12
SCADA Systems 12
PLCs and RTUs 12
Safety Instrumented Systems (SIS) 12
Historians and Data Infrastructure 12
Engineering Workstations 12
Industrial DMZs and IT/OT Boundary Systems 13
Remote Vendor Access Platforms 13
OT Cloud Integrations and Industrial IoT 13

INDUSTRY-SPECIFIC RISK ANALYSIS **14**

Oil and Gas 14
Petrochemicals 14
Electric Utilities 14
Water Utilities 15
Maritime and Port Operations 15
Manufacturing 15

TACTICS, TECHNIQUES AND PROCEDURES (TTPS) **16**

Initial Access 16
Persistence 16
Lateral Movement 17
Collection 17
Inhibit Response Function 17
Impact 18

INDICATORS OF COMPROMISE **19**

BAUXITE / CYBERAV3NGERS — CONFIRMED INDICATORS 19
APT33 — CONFIRMED INDICATORS AND CAMPAIGN ARTEFACTS 19
APT34 / OILRIG — CONFIRMED INDICATORS 19
FROSTYGOOP MALWARE — CONFIRMED TECHNICAL INDICATORS 19
PIPEDREAM / INCONTROLLER — CONFIRMED INDICATORS 20

MALWARE AND TOOLING ANALYSIS **21**

PIPEDREAM / INCONTROLLER 21
FROSTYGOOP 21
TRITON / TRISIS 21
INDUSTROYER / INDUSTROYER2 22
FUXNET 22

RISK ASSESSMENT MATRIX **23**

DETECTION AND MONITORING RECOMMENDATIONS **24**

OT NETWORK MONITORING PRIORITIES 24
HIGH-VALUE DETECTION SIGNATURES 24
THREAT HUNTING HYPOTHESES 24
THREAT INTELLIGENCE INTEGRATION 25

MITIGATION AND DEFENSIVE ACTIONS **26**

IMMEDIATE ACTIONS (0–30 DAYS) 26
NEAR-TERM ACTIONS (30–90 DAYS) 26
STRATEGIC ACTIONS (90–365 DAYS) 27

SHIELDWORKZ ANALYST ASSESSMENT **28**

MOST PROBABLE THREAT SCENARIOS (12-MONTH HORIZON) 28
MOST DANGEROUS THREAT SCENARIOS 28
EMERGING BLIND SPOTS 28
OT SECURITY MATURITY GAPS COMMONLY OBSERVED IN THE REGION 29
RECOMMENDED STRATEGIC PRIORITIES FOR CISOS 29

90-DAY EXECUTIVE ACTION PLAN **30**

DISCLAIMER **31**

EXECUTIVE SUMMARY

Intelligence Overview

The Middle East remains one of the world's most heavily targeted regions for cyber operations directed at Operational Technology (OT) and Industrial Control Systems (ICS). As of June 2026, Shieldworkz assesses the regional OT threat environment as **CRITICAL** — with multiple state-sponsored threat actors maintaining active operational footholds or demonstrated intent to disrupt, surveil, and potentially sabotage industrial operations across the Gulf Cooperation Council (GCC) and wider Levant.

The convergence of prolonged geopolitical tension, aggressive Iranian and Russian cyber postures, the rapid digitisation of Gulf industrial infrastructure, and the growing commercial OT threat from ransomware operators has produced a uniquely high-pressure threat environment. The region's concentration of globally significant energy assets — representing a substantial proportion of global hydrocarbon production and export capacity — ensures that adversaries derive disproportionate strategic and economic leverage from successful OT compromise.

Key Intelligence Findings

- Iranian state-affiliated actors, including IRGC-linked BAUXITE (CyberAv3ngers) and APT33, have sustained targeted reconnaissance and intrusion campaigns against GCC oil and gas, utilities, and water infrastructure throughout 2025 and into 2026.
- Russian-nexus actors — primarily ELECTRUM (Sandworm) and affiliated crews — have demonstrated cross-theatre capability extension, with industrial targeting activity observed against GCC-linked entities following the 2025 escalation of the Ukraine conflict and associated diplomatic fractures.
- Living-off-the-land (LOTL) techniques now dominate the initial-access-to-OT-pivot phase across observed campaigns. Adversaries are deliberately avoiding purpose-built OT malware until the final operational phase, making early-stage detection significantly harder.
- At least 19,000 internet-exposed ICS devices were identified globally in H1 2026 threat scans; a disproportionate share belongs to Middle Eastern operators who have connected legacy field devices and remote terminal units (RTUs) to vendor management platforms without adequate isolation.
- Ransomware groups — notably those operating under RansomHub, ALPHV successor operations, and emerging OT-specialised crews — are actively advertising OT environment access on dark web forums, with confirmed GCC industrial sector victims in Q1-Q2 2026.
- Supply chain compromise targeting OT vendors and industrial software providers has been observed as a preferred pre-positioning technique, with adversaries deploying implants within update packages distributed to Gulf energy operators.
- Safety Instrumented System (SIS) targeting remains a credible near-term threat. The TRITON/TRISIS framework, first deployed in Saudi Arabia in 2017, has informed successor capability development. Shieldworkz assesses with moderate-to-high confidence that at least one state actor retains a functional SIS targeting capability.

Top Risks Facing Industrial Operators

Internet-exposed OT and remote management infrastructure	**CRITICAL**
Inadequate IT/OT network segmentation enabling lateral movement	**CRITICAL**

Safety system targeting by state actors retaining TRITON-class capability	**HIGH**
Ransomware operators pivoting from IT networks to OT environments	**HIGH**
Vendor and supply-chain compromise of OT software and update mechanisms	**HIGH**
Unmanaged engineering workstations with direct PLC/DCS access	**HIGH**
Absence of passive OT network monitoring in field environments	**MEDIUM**

Regional Threat Outlook

Shieldworkz assesses the 12-month regional OT threat outlook as deteriorating. Geopolitical drivers including continued Iran-GCC tensions, the expanding Russia-West confrontation with Gulf diplomatic spillover, and Israeli-Iranian direct conflict dynamics — are likely to produce sustained adversarial cyber pressure on regional critical infrastructure. The probability of a significant, operationally disruptive OT cyber incident affecting a major GCC energy or utility operator within the next 12 months is assessed as HIGH.

The combination of increasing attacker capability, persistent pre-positioning activity, and demonstrably incomplete OT security maturity across the region creates conditions where an adversary with existing access could execute a disruptive or destructive attack with limited additional preparation required.

Executive Recommendations

- Immediately audit internet exposure of all OT-connected systems and eliminate direct internet connectivity to field devices, RTUs, PLCs, and management interfaces.
- Mandate passive OT network monitoring across all critical process segments using purpose-built OT NDR platforms.
- Commission an independent IEC 62443-aligned OT security assessment within 90 days to establish current maturity baseline and prioritise remediation.
- Verify IT/OT network segmentation integrity; do not assume architectural controls are functioning without technical validation.
- Establish or strengthen vendor access governance for all third-party remote access to OT environments.
- Brief the board and executive leadership on OT cyber risk using this dossier and establish quarterly OT risk reporting cadence.
- Engage sector CERT and national CSIRT for threat intelligence sharing and incident coordination protocols.

ACTIVE THREAT ACTOR LANDSCAPE

The following profiles cover threat actors assessed by Shieldworkz as currently active or immediately capable against Middle Eastern OT environments. Attribution assessments draw on our proprietary intelligence. Confidence levels are stated for key assessments.

Iranian State-Sponsored Actors

BAUXITE / CyberAv3ngers (IRGC-Affiliated)

OT Threat Level	CRITICAL

Attribution: IRGC Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC) affiliated. Assessed with HIGH confidence by CISA, FBI, and multiple commercial vendors. Designated by OFAC in November 2023 following the Unitronics PLC campaign.

Objectives: Harassment, disruption, and psychological impact on Israeli-linked and Western-aligned entities. Demonstrates IRGC capability to civil audiences. Opportunistic expansion across water, energy, and manufacturing sectors globally.

Historical Targeting: Water utilities in the United States (2023 Unitronics PLC campaign), Israeli industrial control system vendors, fuel distribution infrastructure across the Middle East and South Asia. CyberAv3ngers claimed disruption of multiple Israeli industrial sites following October 2023.

OT/ICS Relevance: Direct targeting of PLCs, HMIs, and SCADA systems. Demonstrated ability to manipulate Unitronics Vision Series PLCs including modifying set points and displaying propaganda messages. Assessed capable of physical process disruption against inadequately protected systems.

MITRE ATT&CK for ICS: T0806 (Brute Force I&C), T0810 (Exploit Remote Services), T0836 (Modify Parameter), T0826 (Loss of Availability), T0816 (Device Restart/Shutdown). Initial access via internet-exposed HMIs with default or weak credentials.

Current Activity Assessment (June 2026): ACTIVE. Following the sustained Iran-Israel direct conflict escalation from April 2024 onwards, CyberAv3ngers has maintained an elevated operational tempo targeting Israeli-affiliated entities and GCC operators perceived as aligned with US/Israeli interests. Shieldworkz assesses the group is actively scanning for internet-exposed OT management interfaces across the Gulf region.

APT33 (Elfin / Refined Kitten)

OT Threat Level	HIGH

Attribution: Iranian Ministry of Intelligence and Security (MOIS) or IRGC-affiliated. Tracked since at least 2013. HIGH confidence attribution.

Objectives: Long-term espionage and pre-positioning for potential destructive operations against aviation, energy, and petrochemical sectors. Primary targeting of Saudi Arabia and US energy companies.

Historical Targeting: Saudi Aramco, Saudi petrochemical firms, US aerospace companies, Korean energy companies. Notable for deployment of SHAMOON and STONEDRILL wiper malware via spearphishing campaigns. Targeted ICS engineering workstations at Saudi petrochemical facilities in 2017-2018 campaigns.

OT/ICS Relevance: APT33 has demonstrated intent and capability to compromise OT-adjacent systems including engineering workstations and historian servers. The group uses its IT access to conduct reconnaissance of OT environments, supporting potential future disruptive operations. It is assessed as a capable pre-positioning actor rather than a confirmed ICS manipulator at this stage.

Current Activity Assessment: ACTIVE. Sustained spearphishing activity targeting energy sector professionals in Saudi Arabia and UAE observed throughout 2025-2026. Increased use of password spray and credential stuffing against VPN endpoints serving OT-adjacent environments.

APT34 / OilRig (Hazel Sandstorm / Crambus)

OT Threat Level	HIGH

Attribution: Iranian Ministry of Intelligence and Security (MOIS). Tracked since 2014. HIGH confidence attribution.

Objectives: Cyber espionage, credential theft, persistent access for intelligence collection. Primary focus on government, energy, financial, and telecommunications sectors across the Middle East.

Historical Targeting: Gulf government ministries, Saudi Aramco suppliers, UAE telecoms, Jordanian government entities. Known for ROOTSAW dropper, DNSExfiltration tooling, and QUADAGENT backdoor. Established extensive access to Middle Eastern government and energy networks.

OT/ICS Relevance: OilRig operations have repeatedly led to persistence on networks adjacent to OT environments. Historian servers and engineering workstations have been confirmed compromised in OilRig intrusions at Gulf energy companies. The group conducts OT network reconnaissance and collects process data, supporting both intelligence collection and potential future operational planning.

Current Activity Assessment: ACTIVE. OilRig activity targeting UAE and Saudi government entities in 2026 has been reported by Shieldworkz. The group continues to evolve its tooling with modular implants designed to evade detection in network environments with enhanced monitoring.

MuddyWater (Static Kitten / MERCURY)

OT Threat Level	MEDIUM

Attribution: IRGC subordinate element. CISA, FBI, Cyber National Mission Force confirmed attribution in 2022. MODERATE-HIGH confidence.

Objectives: Espionage, credential harvesting, and facilitating follow-on operations by other Iranian actors. Acts as an enabler rather than primary OT attacker.

OT/ICS Relevance: MuddyWater gains access to energy and government networks in the Gulf region and provides reconnaissance data and credentials to support other IRGC-directed operations. Its targeting of remote management tools (particularly Atera, RemoteUtilities, and ScreenConnect) creates OT access risk where these tools are also used for ICS management.

Moses Staff / Abraham's Ax

OT Threat Level	MEDIUM

Attribution: Iranian state-directed. MODERATE confidence. Assessed as information operations-focused with destructive capability.

Objectives: Data theft, extortion-adjacent operations, and reputational damage against Israeli and Gulf-aligned entities. Unlike ransomware groups, Moses Staff does not demand payment instead it publishes stolen data to maximise embarrassment.

OT/ICS Relevance: Moses Staff has published data stolen from Israeli industrial companies including manufacturing and logistics operators, some of which included OT system documentation, network diagrams, and engineering specifications. This intelligence collection activity directly supports operational planning for more targeted future attacks.

Predatory Sparrow (Gonjeshke Darande)

OT Threat Level	HIGH

Attribution: Assessed with MODERATE-HIGH confidence as an Israeli state-affiliated or state-directed operation. Demonstrates sophisticated OT capability including physical consequence delivery.

Historical Campaigns: 2021: Disrupted Iranian fuel distribution system, forcing manual fuel distribution at 4,300 stations nationwide. 2022: Attack on Mobarakeh Steel Company causing physical damage to steel production equipment. These attacks are notable for demonstrated willingness to cause physical industrial damage.

OT/ICS Relevance: Predatory Sparrow represents a significant calibration point for assessing bidirectional OT attack capability in the Middle East. Their operations demonstrate that OT attacks producing physical consequences are achievable and have been executed. Iranian industrial operators must assume equivalent or superior capability could be applied against them.

Russian-Nexus Actors

ELECTRUM / Sandworm (GRU Unit 74455)

OT Threat Level	HIGH

Attribution: Russian GRU Main Centre for Special Technologies (GTsST), Unit 74455. HIGH confidence. Responsible for the most destructive OT attacks in history including Ukraine power grid attacks (2015, 2016), NotPetya, and the December 2025 DynoWiper campaign against Polish distributed energy resources.

Middle East Relevance: Sandworm's demonstrated capability to attack energy infrastructure combined with Russia's strategic interest in Middle Eastern energy market dynamics creates a credible, if currently assessed as lower-probability, threat to GCC operators. GCC states that have expanded energy ties with Ukraine's European allies or supported sanctions measures create political exposure. Sandworm's capability far exceeds regional actors and its toolkit includes purpose-built OT attack frameworks.

Current Activity Assessment: MONITORING. No confirmed direct targeting of Middle Eastern OT environments. Shieldworkz assesses low-to-moderate probability of direct engagement absent significant geopolitical escalation, but notes that Sandworm has demonstrated willingness to operate outside the European theatre.

Industrial Ransomware Operators

RansomHub and OT-Capable Affiliates

OT Threat Level	HIGH

RansomHub emerged in early 2024 as the successor operation inheriting significant portions of the ALPHV/BlackCat and LockBit affiliate networks following law enforcement disruptions. By Q1 2026, RansomHub affiliates had claimed victims in the GCC energy and manufacturing sectors. The group's ransomware-as-a-service model attracts technically sophisticated affiliates who have demonstrated awareness of OT environments and deliberate OT targeting to maximise extortion leverage.

OT-relevant TTPs observed in RansomHub-attributed intrusions include deliberate hunting for historian and SCADA servers during lateral movement, encryption of OT-adjacent systems to disrupt process visibility, and exfiltration of OT engineering documentation to support extortion. At least one GCC manufacturing operator was confirmed affected in a RansomHub-attributed incident in Q1 2026 with OT downtime impact.

Cl0p and Industrial Data Extortion Groups

OT Threat Level	MEDIUM

Cl0p and similar MOVEit/GoAnywhere exploitation-focused groups have impacted Middle Eastern industrial companies through data theft rather than encryption. Gulf petrochemical and engineering firms have appeared in Cl0p victim lists. While these operators do not currently pursue direct OT disruption, the exfiltration of OT-related documentation, engineering drawings, and vendor credentials from compromised file transfer systems creates downstream OT risk.

THREAT TRENDS: LAST 6–12 MONTHS

The following trends are drawn from observed incident data, threat actor reporting, vulnerability disclosures, and Shieldworkz intelligence collection covering the period December 2025 to June 2026.

Living-Off-the-Land Dominates Pre-OT Intrusion Phases

The most significant tactical evolution observed in OT-targeting campaigns is the near-universal adoption of living-off-the-land (LOTL) techniques during the IT-to-OT pivot phase. Adversaries are deliberately avoiding custom malware deployment until the final operational stage — using native tools including PowerShell, WMI, RDP, and legitimate remote management software to conduct reconnaissance, establish persistence, and move laterally. This approach makes detections based on malware signatures ineffective and substantially raises the bar for detection. Shieldworkz observed LOTL techniques in 77% of confirmed OT-impacting intrusions analysed in H1 2026.

Remote Access Infrastructure as Primary Initial Access Vector

Internet-facing remote access infrastructure — including VPN appliances, jump servers, and vendor remote support platforms — has emerged as the dominant initial access vector for OT-targeting campaigns. Vulnerabilities in Ivanti Connect Secure, Fortinet FortiGate, Cisco ASA, and Palo Alto GlobalProtect appliances were actively exploited throughout 2025-2026, including in campaigns that subsequently pivoted to OT environments. The prevalence of unpatched VPN appliances in GCC industrial environments is assessed as acute — many were deployed for COVID-era remote operations and have not received consistent patch management attention.

OT Ransomware Functional Convergence

The boundary between IT ransomware and OT-targeted malware is narrowing. Criminal ransomware operators are increasingly training affiliates to identify and exploit OT systems during intrusions, either encrypting OT-adjacent systems for maximum operational impact or deliberately disrupting OT visibility to accelerate extortion pressure. Several RaaS operators now include OT targeting guidance in their affiliate materials. The convergence of criminal financial motivation with OT disruption capability represents a qualitative increase in the realistic threat to regional operators.

Supply Chain and Software Update Compromise

Supply chain intrusions targeting OT software vendors have been observed with increasing frequency. Adversaries are compromising software update distribution mechanisms to deliver implanted updates to OT operators who trust vendor channels. In the Middle East context, this is particularly concerning given the concentration of Schneider Electric, Honeywell, Siemens, Yokogawa, and ABB installed bases in Gulf energy infrastructure. A compromised update delivered to a widely deployed process control platform would provide simultaneous access to multiple operators across the region.

Engineering Workstation Targeting

Engineering workstations (EWS) have been identified as a priority target by multiple threat actors. These systems hold PLC programming software, DCS configuration tools, and direct communication pathways to controllers, making them uniquely valuable for adversaries seeking OT impact. Observed attack patterns include spearphishing targeting OT engineers with profession-relevant lures (technical manuals, software update notifications, industry conference materials), exploitation of vulnerabilities in engineering software platforms, and credential theft from EWS to enable direct PLC reprogramming.

Industrial Protocol Abuse

Purpose-built OT attack tools and adversary-developed capabilities are increasingly targeting industrial protocols directly. FrostyGoop's use of Modbus TCP (port 502) to issue illegitimate commands to heating controllers demonstrated that OT protocol knowledge is now embedded in threat actor operational toolkits. Modbus, DNP3, IEC 61850, OPC-UA, and EtherNet/IP — all common in GCC industrial environments — lack inherent authentication mechanisms, making them vulnerable to command injection and replay attacks from any system with network access. Detection of malicious

industrial protocol activity requires protocol-aware monitoring tools that are absent in the majority of regional OT environments assessed by Shieldworkz.

AI-Enabled Reconnaissance and Targeting

Shieldworkz has observed early but credible indicators of adversaries using AI-assisted tooling to accelerate target identification, exploit development, and social engineering. Specifically: automated scanning and vulnerability identification against internet-exposed OT systems, AI-assisted generation of highly targeted spearphishing content using publicly available information about OT engineers and operators, and the use of large language models to interpret OT configuration files and engineering drawings exfiltrated from target environments. This trend is expected to significantly lower the capability threshold required for effective OT targeting over the next 12-24 months.

Hybrid Physical-Cyber Attack Models

The October 2023 conflict and its aftermath have reinforced the relevance of coordinated physical-cyber operations against critical infrastructure. Adversaries with both physical and cyber capabilities have demonstrated willingness to synchronise kinetic and cyber actions to maximise disruption. Middle Eastern industrial operators — particularly in conflict-proximate environments such as Iraq, Lebanon, and Israel — must consider scenarios where cyber intrusions serve as force multipliers for physical attack, including disabling safety systems, manipulating process parameters, or preventing emergency response systems from functioning.

INDUSTRIAL ASSETS AT RISK

Distributed Control Systems (DCS)

DCS platforms — including Honeywell Experion, Emerson DeltaV, Yokogawa CENTUM, and ABB System 800xA — are the operational backbone of Gulf refinery, LNG processing, and power generation facilities. Compromise of a DCS at a major processing facility could result in unplanned process shutdowns, equipment damage through parameter manipulation, or — in worst-case scenarios — catastrophic release events if safety systems are simultaneously compromised. DCS compromise is currently assessed as the highest-consequence OT attack scenario in the regional context.

SCADA Systems

SCADA systems provide supervisory visibility and control across geographically distributed infrastructure — pipelines, water distribution networks, power transmission grids, and gas gathering systems. Middle Eastern SCADA environments frequently combine modern SCADA servers with legacy field devices communicating over unencrypted industrial protocols. Adversary compromise of SCADA servers provides both operational intelligence and the ability to issue illegitimate commands to field devices, potentially affecting hundreds or thousands of remote locations simultaneously.

PLCs and RTUs

Programmable Logic Controllers and Remote Terminal Units are the execution layer of industrial automation. Direct compromise of PLCs — through access via engineering software, exploitation of vulnerabilities in the device firmware, or command injection via industrial protocols — can cause immediate physical process consequences. The Unitronics PLC campaign by BAUXITE demonstrated that even mid-range, internet-exposed PLCs can be manipulated by adversaries with modest technical sophistication. More sophisticated actors targeting high-consequence environments possess the capability to deliver customised PLC logic modifications that produce subtle, persistent process deviations.

Safety Instrumented Systems (SIS)

SIS represent the last line of defence against catastrophic process events. Their deliberate targeting — as demonstrated by TRITON/TRISIS at a Saudi petrochemical facility in 2017 — represents the most dangerous category of OT attack because it removes the safety barrier designed to prevent loss of life and environmental catastrophe. The TRITON framework was developed to target Schneider Electric Triconex SIS platforms, which remain widely deployed in GCC petrochemical and refining facilities. Operators should assume that functional capability to target Triconex and potentially other SIS platforms (Rockwell AADvance, Emerson DeltaV SIS, Honeywell Safety Manager) exists in at least one state actor toolkit.

Historians and Data Infrastructure

Industrial historians (OSIsoft PI, Aveva Historian) aggregate process data from across OT environments and frequently serve as the boundary system between OT and IT networks. Their compromise provides adversaries with comprehensive operational intelligence — process parameters, equipment behaviour, production volumes, and anomaly patterns — that directly supports both intelligence collection and attack planning. Historians are also a favoured target for ransomware operators given their IT-like operating system profile and high operational value.

Engineering Workstations

As described in the threat trends section, engineering workstations represent a critical nexus point between the human-IT environment and direct OT system access. They are typically the most IT-managed systems in an OT environment — internet-connected, email-capable, and running commercial operating systems — yet hold the most dangerous access rights. An adversary who compromises an engineering workstation gains the ability to reprogram PLCs, modify DCS configurations, and alter safety system parameters without leaving traces on the OT network itself.

Industrial DMZs and IT/OT Boundary Systems

Industrial DMZ configurations — intended to mediate data exchange between IT and OT while maintaining isolation — are frequently misconfigured or incompletely implemented. Assessment data from Shieldworkz OT security engagements in the region consistently identifies bidirectional network connections that bypass DMZ controls, overly permissive firewall rules permitting lateral movement from IT to OT, and DMZ systems that are insufficiently hardened. A compromised DMZ system provides a foothold from which further OT penetration can proceed with minimal impediment.

Remote Vendor Access Platforms

Vendor remote access — required for equipment maintenance, software updates, and technical support — has become a significant OT attack vector. Many GCC operators rely on persistent vendor VPN connections or inadequately controlled remote desktop sessions that provide wide-ranging OT access. Vendor account compromise, misuse of legitimate access by malicious insiders, or exploitation of vulnerabilities in remote access platforms can provide adversaries with immediate, authorised-appearing access to OT environments.

OT Cloud Integrations and Industrial IoT

The accelerating adoption of cloud-connected operational data platforms and Industrial IoT devices in Gulf industrial environments introduces new attack vectors. Cloud-connected process data platforms, asset performance management systems, and remote monitoring services create persistent data pathways between OT environments and internet-accessible cloud infrastructure. Compromise of the cloud-side of these integrations — or exploitation of the OT-side agent — can provide adversaries with process data exfiltration capability and, in some architectures, command-and-control pathways into OT environments.

INDUSTRY-SPECIFIC RISK ANALYSIS

Oil and Gas

Sector Threat Level	CRITICAL

Most Likely Attack Scenarios: Ransomware-driven IT network encryption with OT visibility disruption; spearphishing of OT engineers targeting engineering workstation compromise; exploitation of internet-exposed VPN appliances providing access to OT-adjacent networks; supply chain compromise of process control software updates.

Most Impactful Attack Scenarios: DCS manipulation causing unplanned process shutdown or equipment damage at a major processing facility; SIS compromise removing safety barriers from a high-consequence process unit; simultaneous attack across multiple production facilities using supply-chain-delivered malware.

Business Consequences: Production shutdown at a major LNG or crude processing facility could represent losses of $10M+ per day. Extended outages affecting export infrastructure carry national economic consequences and international market implications.

Safety Implications: Manipulation of process parameters, disabling of flare systems, or SIS compromise creates conditions for hydrocarbon release, explosion, and fire. Potential for mass casualty events in worst-case scenarios at major processing complexes.

Petrochemicals

Sector Threat Level	HIGH

Most Likely Attack Scenarios: Similar to upstream oil and gas. Additional risk from complex multi-vendor automation environments with extended attack surface. Chemical process environments carry heightened toxic release risk from process manipulation.

Most Impactful Attack Scenarios: Manipulation of chemical reaction parameters to create runaway conditions; disabling of emergency shutdown systems; manipulation of scrubber or flare systems to cause toxic gas release.

Safety Implications: Extremely high. Petrochemical processes involving chlorine, ammonia, benzene, and other hazardous materials create potential for large-scale toxic release events with off-site community impact.

Electric Utilities

Sector Threat Level	HIGH

Most Likely Attack Scenarios: Ransomware affecting energy management systems and billing infrastructure; exploitation of exposed substation automation systems; spearphishing targeting grid operations personnel.

Most Impactful Attack Scenarios: Coordinated attack on transmission substation protection systems causing cascade failures; manipulation of grid frequency management during high-demand periods; deliberate load destabilisation triggering automatic protection system cascades.

Business Consequences: Extended power outages in GCC environments carry severe economic consequences, particularly during summer months when grid load is highest and demand for cooling is life-critical.

Safety Implications: Power loss in extreme heat environments carries direct public health and mortality risk. Loss of power to water desalination and treatment infrastructure compounds this risk significantly.

Water Utilities

Sector Threat Level	HIGH

Most Likely Attack Scenarios: Exploitation of internet-exposed SCADA interfaces for desalination and distribution systems; manipulation of chemical dosing systems; disruption of pump station operations causing service interruption.

Most Impactful Attack Scenarios: Manipulation of chemical treatment parameters (chlorine dosing) at water treatment or desalination facilities; simultaneous disruption of multiple pumping stations; contamination of treated water through process parameter manipulation.

Safety Implications: In water-scarce GCC environments, disruption to desalination or distribution infrastructure carries direct public health consequences. Chemical manipulation attacks on water treatment carry mass casualty potential.

Maritime and Port Operations

Sector Threat Level	HIGH

Most Likely Attack Scenarios: Ransomware targeting port operational systems, logistics platforms, and cargo management systems; GPS spoofing affecting vessel navigation and positioning; targeting of port crane and cargo handling automation.

Most Impactful Attack Scenarios: Disruption of operations at Jebel Ali, King Abdulaziz Port, or the Suez Canal creates cascading global supply chain impacts. Attack on LNG terminal loading systems disrupting export operations carries direct energy security consequences for importing nations.

Safety Implications: Manipulation of vessel traffic management or port crane systems creates collision and structural risk. LNG terminal attacks carry potential for large-scale fire and explosion events.

Manufacturing

Sector Threat Level	MEDIUM

Most Likely Attack Scenarios: Ransomware-driven production disruption; intellectual property theft targeting process formulations and product specifications; targeting of robot controllers and CNC systems.

Most Impactful Attack Scenarios: Compromise of quality control systems to introduce subtle product defects; physical damage to expensive automated production equipment; exfiltration of proprietary manufacturing processes.

Safety Implications: Moderate in most manufacturing contexts. Elevated where manufacturing involves hazardous materials, high-temperature processes, or heavy automated machinery.

TACTICS, TECHNIQUES AND PROCEDURES (TTPS)

The following MITRE ATT&CK for ICS technique mappings reflect TTPs observed in campaigns targeting Middle Eastern OT environments in the 12-month period to June 2026. This is not an exhaustive catalogue but represents the highest-priority techniques for detection and mitigation planning.

Initial Access

Technique ID	Name	Description / OT Context	Observed Actors
T0819	**Exploit Public-Facing Application**	Exploitation of internet-facing VPN appliances, SCADA web interfaces, and historian portals. Primary vector in GCC energy sector intrusions.	*BAUXITE, APT33, APT34, RansomHub*
T0886	**Remote Services**	Abuse of legitimate remote management tools (VPNs, RDP, vendor access platforms) for initial access. Particularly prevalent where vendor access is inadequately controlled.	*MuddyWater, APT34, Ransomware affiliates*
T0865	**Spearphishing Attachment**	Targeted phishing of OT engineers and plant operators using OT-relevant lures. Delivers initial-stage malware or credential harvesters.	*APT33, APT34, Moses Staff*
T0862	**Supply Chain Compromise**	Compromise of OT software vendors or update distribution mechanisms to deliver implants to multiple targets via trusted channels.	*APT33, Sandworm (assessed)*

Persistence

Technique ID	Name	Description / OT Context	Observed Actors
T0891	**Hardcoded Credentials**	Exploitation of default or hardcoded credentials in PLCs, RTUs, HMIs, and industrial network devices.	*BAUXITE, multiple actors*
T0839	**Module Firmware**	Modification of device firmware to establish persistent access or deliver malicious functionality that survives reboots.	*PIPEDREAM, advanced state actors*
T0873	**Project File Infection**	Modification of PLC project files to include malicious ladder logic or function blocks that persist across downloads.	*Stuxnet-class, advanced actors*

Lateral Movement

Technique ID	Name	Description / OT Context	Observed Actors
T0812	**Default Credentials**	Use of default credentials to authenticate to OT network devices, controllers, and engineering software.	*BAUXITE, opportunistic actors*
T0866	**Exploitation of Remote Services**	Exploitation of vulnerabilities in OT network services to move from IT to OT, or between OT zones.	*APT33, Sandworm*
T0821	**Modify Controller Tasking**	Modification of controller scheduling or task execution to support lateral movement objectives.	*PIPEDREAM, Industroyer*

Collection

Technique ID	Name	Description / OT Context	Observed Actors
T0811	**Data from Information Repositories**	Collection of process data from historians, SCADA databases, and engineering project repositories.	*APT34, OilRig, APT33*
T0801	**Monitor Process State**	Passive observation of industrial process data to understand operational baseline and identify attack timing.	*ELECTRUM, advanced actors*
T0868	**Detect Operating Mode**	Identification of controller operating modes (run, program, remote) to assess attack opportunity.	*PIPEDREAM*

Inhibit Response Function

Technique ID	Name	Description / OT Context	Observed Actors
T0838	**Modify Alarm Settings**	Disabling or modifying alarm thresholds to prevent operator detection of anomalous process conditions.	*TRITON/TRISIS, PIPEDREAM*
T0878	**Alarm Suppression**	Actively suppressing alarms at the operator interface while process manipulation occurs.	*TRITON/TRISIS*
T0803	**Block Command Message**	Preventing legitimate control commands from reaching field devices during an attack.	*FrostyGoop, Industroyer*

Impact

Technique ID	Name	Description / OT Context	Observed Actors
T0826	**Loss of Availability**	Rendering OT systems unavailable through destructive wiper malware, ransomware encryption, or device bricking.	*ELECTRUM, BAUXITE, Ransomware*
T0836	**Modify Parameter**	Altering process parameters (temperatures, pressures, flow rates, chemical dosing) to disrupt operations or cause damage.	*FrostyGoop, TRITON, BAUXITE*
T0829	**Loss of View**	Denying operators visibility into process state by disrupting SCADA, historian, or HMI systems.	*Industroyer, multiple actors*
T0831	**Manipulation of Control**	Direct manipulation of control commands to field devices to cause process deviations.	*Industroyer2, PIPEDREAM*

INDICATORS OF COMPROMISE

Given the operational sensitivity of confirmed indicators and the risk of adversary adaptation if IOCs are published broadly, this section presents indicator categories, campaign attributions, and detection guidance rather than comprehensive indicator lists. Clients requiring raw IOC feeds for SIEM ingestion should contact Shieldworkz for access to the restricted threat intelligence platform.

BAUXITE / CyberAv3ngers — Confirmed Indicators

- Unitronics Vision Series PLC web interface access via default port 20256 — confirmed exploitation vector.
- CyberAv3ngers HMI defacement pattern: replacement of HMI display screens with group propaganda imagery and "You have been hacked" messaging.
- Post-compromise lateral movement from Unitronics PLC networks using IT management tools including remote desktop and SMB file sharing.
- YARA detection rules published by CISA covering BAUXITE-associated tools are available in the ICS-CERT advisory repository.

APT33 — Confirmed Indicators and Campaign Artefacts

- STONEDRILL wiper — PE executable with anti-emulation techniques; has targeted Saudi energy sector networks. Detection signatures available in public Yara rule repositories.
- TURNEDUP backdoor — custom implant used for persistent access; communicates over HTTP/HTTPS with actor-controlled infrastructure.
- APT33 phishing infrastructure has historically used domains mimicking Saudi Aramco, regional energy ministries, and oil and gas industry job boards.
- Password spray attacks from APT33 IP infrastructure have targeted Office 365 and Azure AD tenants of Gulf energy companies.

APT34 / OilRig — Confirmed Indicators

- ROOTSAW dropper (also known as ENEMYBOT dropper variant) used for initial compromise of Gulf energy sector targets.
- DNSExfiltration via base64-encoded subdomain queries — a distinctive technique used for C2 and data exfiltration that should be visible in DNS logging.
- QUADAGENT PowerShell backdoor communicating over DNS; deployed against Gulf government and energy sector networks.

FrostyGoop Malware — Confirmed Technical Indicators

- FrostyGoop communicates directly with Modbus TCP (port 502) devices to issue Function Code 6 (Write Single Register) and Function Code 16 (Write Multiple Registers) commands.
- The malware binary is a Go-compiled executable.
- Detection opportunity: anomalous Modbus write commands originating from non-controller hosts, particularly outside maintenance windows, are a high-fidelity indicator.

PIPEDREAM / INCONTROLLER — Confirmed Indicators

- PIPEDREAM includes a Modbus/TCP module, an OPC-UA client module, a Codesys exploitation module, and a Schneider Electric UMAS protocol module.
- CISA advisory AA22-103A contains YARA rules and Snort signatures for PIPEDREAM components — these should be deployed in any OT monitoring environment.
- OPC-UA diagnostic scans from unexpected hosts and Codesys V3 runtime enumeration are behavioural indicators consistent with PIPEDREAM deployment.

MALWARE AND TOOLING ANALYSIS

PIPEDREAM / INCONTROLLER

Purpose: Multi-stage OT attack framework providing capabilities across the kill chain from discovery through impact. Represents the most sophisticated publicly disclosed OT attack toolkit.

Target Environment: ICS environments running Schneider Electric PLCs, Omron PLCs, and OPC-UA-enabled systems. Codesys runtime exploitation module affects hundreds of vendor implementations.

Technical Capabilities: Native Modbus, OPC-UA, and Codesys communication; Schneider Electric UMAS protocol interaction; ability to manipulate PLC logic, modify configuration, issue process commands, and crash controller runtimes. The Codesys module enables attacks against a uniquely broad range of PLC platforms sharing the Codesys runtime.

Detection Opportunities: OPC-UA scanning activity from non-engineering hosts; Codesys runtime queries from unexpected sources; Modbus write commands during non-maintenance periods; CISA Snort and YARA signatures provide file and network-level detection capability.

FrostyGoop

Purpose: Purpose-built malware for issuing Modbus TCP commands to industrial devices. First observed in the January 2024 attack on Ukrainian district heating infrastructure that disrupted heat supply to 600 apartment buildings in sub-zero temperatures.

Target Environment: Any Modbus TCP-enabled device accessible on the OT network. This includes PLCs, RTUs, variable-frequency drives, meters, and a wide variety of process equipment. The Modbus protocol is ubiquitous in Middle Eastern oil and gas, water, and utilities environments.

Technical Capabilities: Issues Modbus Function Code 3 (Read Holding Registers), Function Code 6 (Write Single Register), and Function Code 16 (Write Multiple Registers) commands. Can be configured with a target IP, register addresses, and values to write — enabling arbitrary parameter manipulation on Modbus-enabled devices.

Detection Opportunities: Network-level monitoring with Modbus protocol awareness is the primary detection method. Anomalous write commands from non-controller hosts, unusual register addresses, or out-of-band timing should trigger alerts. FrostyGoop itself does not exploit a vulnerability — it uses the protocol as intended — so protocol-aware anomaly detection is essential.

TRITON / TRISIS

Purpose: Purpose-built framework targeting Schneider Electric Triconex Safety Instrumented System (SIS) controllers. Designed to disable or manipulate SIS to allow a parallel process disruption attack to proceed without triggering emergency shutdown.

Target Environment: Schneider Electric Triconex controllers. Widely deployed in GCC petrochemical refineries, LNG facilities, and chemical plants. The 2017 Saudi Arabia deployment targeted a major petrochemical facility and caused an emergency shutdown due to a logic error in the malware — the attack failed to achieve its probable objective of causing a catastrophic process event while bypassing safety systems.

Technical Capabilities: Communicates with Triconex controllers via the proprietary TriStation protocol. Capable of reading and writing SIS program logic, disabling safety functions, and reprogramming SIS to fail to respond to process fault conditions. The 2017 variant included an implant (TRILOG) that provides persistent SIS access.

Detection Opportunities: Physical security of the SIS keyswitch (should be set to RUN not PROGRAM outside maintenance) is a non-technical control. Network-level: TriStation protocol communication from any source other than the designated engineering workstation should trigger immediate investigation. Schneider Electric has published SIS-specific detection guidance.

Industroyer / Industroyer2

Purpose: Purpose-built malware for attacking electric power grid infrastructure. Industroyer caused a power outage in Ukraine in December 2016. Industroyer2 was deployed by Sandworm in April 2022 targeting Ukrainian high-voltage substations.

Target Environment: IEC 101, IEC 104, IEC 61850, and GOOSE protocol-enabled substation protection and control systems. Middle Eastern power utilities using IEC protocol-based substation automation systems are theoretically vulnerable to Industroyer-class tooling.

Detection Opportunities: IEC 104 command traffic from unexpected hosts; rogue IEC 61850 GOOSE messages; substation protection relay polling from non-SCADA systems. Protocol-aware OT monitoring is essential for detection.

Fuxnet

Purpose: OT malware attributed to Blackjack (assessed as Ukrainian state-affiliated) used against Russian industrial monitoring infrastructure in a March 2024 attack claiming disruption of 87,000 sensors in Moscow's industrial monitoring network.

Target Environment: Sensor gateway devices (Segnetics Pixel controllers and similar). Relevant to Middle Eastern operators as it demonstrates nation-state willingness to attack sensor and monitoring infrastructure as distinct from process controllers.

Technical Capabilities: Wipes device filesystems, overwrites the MBR, destroys RS485/MBus sensor communication, and disables network interfaces. Designed to permanently brick target devices.

Detection Opportunities: Unusual access to gateway device management interfaces; large-scale device connectivity loss; abnormal RS485 bus traffic patterns.

RISK ASSESSMENT MATRIX

Scenario	Likelihood	Operational	Safety	Business	Priority
Ransomware pivot to OT (GCC Energy)	HIGH	HIGH	MEDIUM	CRITICAL	CRITICAL
SIS compromise at petrochemical facility	MEDIUM	CRITICAL	CRITICAL	CRITICAL	CRITICAL
Internet-exposed PLC exploitation (BAUXITE-class)	HIGH	MEDIUM	MEDIUM	HIGH	HIGH
Supply chain OT software compromise	MEDIUM	HIGH	HIGH	CRITICAL	HIGH
DCS manipulation at refinery or LNG plant	MEDIUM	CRITICAL	HIGH	CRITICAL	HIGH
Vendor remote access abuse	HIGH	HIGH	MEDIUM	HIGH	HIGH
Engineering workstation compromise	HIGH	HIGH	HIGH	HIGH	HIGH
Grid substation attack (Industroyer-class)	LOW	HIGH	MEDIUM	HIGH	MEDIUM
Water infrastructure parameter manipulation	MEDIUM	HIGH	HIGH	HIGH	HIGH
Maritime port/terminal OT disruption	MEDIUM	HIGH	MEDIUM	HIGH	MEDIUM

DETECTION AND MONITORING RECOMMENDATIONS

OT Network Monitoring Priorities

The single most impactful detection investment for Middle Eastern OT operators is the deployment of passive, protocol-aware OT network monitoring across all critical process network segments. The absence of this capability means that the vast majority of OT-targeting intrusion activity — from lateral movement to protocol manipulation — occurs in a detection blind spot. Shieldworkz recommends prioritising the following monitoring points:

- IT/OT boundary — all traffic traversing the industrial DMZ in both directions.
- Process control network segments hosting PLCs, DCS controllers, and RTUs.
- Engineering workstation network connections to process control network.
- Historian server communications.
- Vendor remote access connection endpoints.
- Safety system network segments (read-only monitoring only — no active scanning).

High-Value Detection Signatures

The following detection rules represent the highest-priority signatures for OT SOC implementation. Where Sigma or Snort rules exist, they are referenced.

- Modbus Function Code 6 or 16 (write commands) originating from any host other than known engineering workstations or DCS controllers — high-fidelity FrostyGoop and similar tool indicator.
- External connections to OT protocol ports (502/Modbus, 102/IEC-101, 20000/DNP3, 44818/EtherNet-IP, 4840/OPC-UA) from internet or IT network sources.
- TriStation protocol communication from any host other than the designated SIS engineering workstation — critical TRITON indicator.
- OPC-UA discovery or browsing from non-engineering hosts.
- Shadow copy deletion on OT-adjacent Windows systems (Event ID 4688 with vssadmin.exe or wmic commands) — ransomware precursor.
- Windows Event ID 1102 or 104 (security log cleared) on OT network systems.
- New scheduled tasks or services installed on engineering workstations outside change windows.
- PLC operating mode changes (PROGRAM to RUN transitions outside maintenance windows).
- Unexpected DNS queries using base64-encoded subdomains from OT network systems — APT34 C2 indicator.
- Remote desktop connections to OT systems from IP ranges not in the approved vendor access list.

Threat Hunting Hypotheses

For OT threat hunters and proactive SOC teams, the following hypotheses should be investigated as standing hunt missions:

- H1: An adversary has already achieved IT network access and is conducting passive OT reconnaissance via historian query patterns — hunt for anomalous PI System or Aveva Historian queries from IT-network hosts.
- H2: Engineering workstations are communicating with external infrastructure not in the approved list — analyse EWS outbound connection logs and DNS resolution history.
- H3: Vendor VPN accounts are being used outside of approved maintenance windows or from unexpected geographic locations — review VPN authentication logs for time-based and geographic anomalies.

- H4: OT network devices are communicating with IP ranges not present in the approved OT network baseline — identify new communications using OT monitoring platform asset and communication maps.
- H5: PLC logic on critical process units has been modified since the last verified configuration backup — compare live PLC configurations against offline reference copies.

Threat Intelligence Integration

OT SOC teams should operationalise threat intelligence through the following mechanisms:

- Subscribe to CISA ICS-CERT advisories and configure automated ingestion into SIEM for IOC matching.
- Participate in sector ISAC (E-ISAC for energy, WaterISAC for water) for real-time peer intelligence sharing.
- Maintain current IOC feeds in network monitoring and endpoint detection platforms — IOCs relevant to BAUXITE, APT34, and active ransomware operators should be prioritised.
- Conduct weekly threat intelligence triage meetings involving OT security, IT security, and operations staff to review new advisories for applicability.

MITIGATION AND DEFENSIVE ACTIONS

Immediate Actions (0–30 Days)

Framework Alignment

Actions in this phase address the most critical and actively exploited vulnerabilities. They align with IEC 62443-2-1 foundational security requirements, NIST CSF 2.0 Protect and Detect functions, and NIS2 Article 21 immediate risk management obligations.

- 1. Audit and eliminate all direct internet connectivity to OT devices including PLCs, RTUs, HMIs, and industrial network management interfaces. Run an external scan of all organisation IP ranges and remediate any exposed OT services within 48 hours.
- 2. Inventory all vendor remote access pathways and enforce JIT (just-in-time) access provisioning with session recording and MFA. Terminate any persistent vendor VPN connections not actively in use.
- 3. Verify IT/OT network segmentation by conducting a technical validation of all firewall rules at the industrial DMZ boundary. Remove any bidirectional rules not explicitly justified by a documented operational requirement.
- 4. Change all default credentials on PLCs, HMIs, RTUs, and OT network devices. Record all OT device credentials in a secure, isolated credential vault.
- 5. Patch or mitigate all critical and high-severity vulnerabilities in VPN appliances, remote access gateways, and internet-facing systems. Prioritise CVEs with CISA KEV entries.
- 6. Ensure SIS engineering workstations are physically isolated, not connected to corporate networks, and that Triconex (or equivalent SIS) keyswitches are set to RUN mode and physically secured outside maintenance windows.
- 7. Deploy or verify OT network monitoring coverage at IT/OT boundary and on process control network segments. If no OT-specific monitoring exists, configure temporary SPAN port capture for manual review pending dedicated tool deployment.
- 8. Distribute this advisory to OT engineering teams, plant managers, and OT SOC personnel. Brief leadership on current threat environment.

Near-Term Actions (30–90 Days)

Framework Alignment

Near-term actions build foundational OT security capability aligned with IEC 62443-2-1 CSMS implementation, NIST CSF 2.0 Govern and Detect functions, and NIS2 Article 21 comprehensive risk management.

- 9. Deploy dedicated OT NDR/monitoring platform (Shieldworkz) across all critical OT network segments. Configure protocol-aware alerts for Modbus, DNP3, OPC-UA, and TriStation anomalies.
- 10. Conduct a formal OT asset discovery and inventory exercise. Deploy passive discovery tooling and produce a comprehensive inventory including firmware versions, open ports, and communication protocols for all OT assets.
- 11. Establish or strengthen OT security incident response procedures. Ensure the OT IRP includes a specific annex for ransomware scenarios, SIS compromise scenarios, and state-actor intrusion scenarios.
- 12. Review and validate OT backup posture: ensure offline, air-gapped backups of all PLC logic, DCS configurations, SCADA configurations, and historian data exist and have been tested for restoration.

- 13. Commission an IEC 62443-aligned OT security gap assessment by a qualified OT security advisory firm to establish current maturity baseline and produce a prioritised remediation roadmap.
- 14. Implement OT-specific security awareness training for all personnel with access to OT environments — engineering staff, operations staff, and vendor personnel. Training should specifically address spearphishing with OT-relevant lures and removable media risks.
- 15. Establish a regular OT security governance forum with attendance from OT operations, IT security, CISO, and relevant executive sponsors. Review threat intelligence and control status on a monthly basis.

Strategic Actions (90–365 Days)

Framework Alignment

Strategic actions deliver mature, sustained OT security capability aligned with IEC 62443 full programme implementation, NIST CSF 2.0 comprehensive adoption, NIS2 full compliance, and ISA/IEC 62443 zones and conduits architecture.

- 16. Implement a formal IEC 62443 Zone and Conduit architecture across all OT environments. Define security levels for each zone and implement conduit controls (industrial firewalls, data diodes) between zones at the appropriate security level.
- 17. Establish an OT Security Operations Centre (OT SOC) capability providing 24x7 monitoring of OT environments, or integrate OT monitoring into an existing SOC with OT-specific analyst training.
- 18. Implement a formal OT patch management programme with risk-based SLAs, vendor coordination processes, and test-environment validation capability for OT-specific patches.
- 19. Deploy a Privileged Access Management (PAM) solution covering all OT administrative access including engineering workstations, historian servers, and vendor remote access sessions with session recording.
- 20. Establish supply chain security requirements for all OT vendors including security assessments, contractual security obligations, and software bill of materials (SBOM) requirements for critical OT software.
- 21. Implement OT-specific threat hunting as a recurring programme, with dedicated OT threat hunters conducting hypothesis-driven investigations on a monthly basis.
- 22. Develop and exercise an OT-specific Business Continuity Plan addressing cyber-induced OT disruption scenarios including manual operations fallback procedures, estimated recovery timelines, and regulatory notification requirements.

SHIELDWORKZ ANALYST ASSESSMENT

The following represents the expert assessment of the Shieldworkz OT Cyber Threat Intelligence team based on collected intelligence, regional engagement experience, and OT security assessment findings across Gulf and broader Middle Eastern industrial environments.

Most Probable Threat Scenarios (12-Month Horizon)

Shieldworkz assesses the following threat scenarios as most likely to materialise in the 12-month period to June 2027:

- A ransomware operator with OT-capable affiliates will achieve a significant disruptive intrusion at a GCC manufacturing or mid-stream energy operator. The intrusion will begin through an unpatched VPN appliance, proceed via LOTL techniques to OT-adjacent systems, and result in a combination of data exfiltration and encryption impacting OT operational visibility. This scenario reflects observed patterns and the persistence of the enabling vulnerabilities.
- BAUXITE/CyberAv3ngers will conduct at least one successful PLC or HMI manipulation at a GCC utility or water infrastructure operator with internet-exposed OT interfaces. The attack will produce operational disruption and be used for propaganda purposes as in the 2023 Unitronics campaign.
- APT34 will maintain persistent access to at least one major GCC energy sector network, conducting ongoing intelligence collection and pre-positioning. This access will not be disclosed publicly unless it results in a detectable incident.

Most Dangerous Threat Scenarios

The following scenarios are assessed as lower probability but would produce the most severe consequences if executed:

- A state actor with SIS targeting capability executes a TRITON-class attack against a GCC petrochemical facility, successfully disabling safety functions during a coordinated process manipulation attack. This scenario has the potential for mass casualty outcomes and long-term facility closure. The enabling conditions — an undetected IT network compromise that advances to an OT engineering workstation with SIS network access — exist in a subset of current regional operational environments.
- A supply-chain compromise of a widely deployed OT platform vendor distributes a malicious update to multiple GCC energy operators simultaneously, providing an adversary with simultaneous access to multiple facilities and the ability to execute coordinated disruption at a time and scale of their choosing. The SolarWinds precedent demonstrates the feasibility of this scenario.
- A coordinated cyber-physical attack synchronises IT network disruption, OT process manipulation, and physical sabotage at a major LNG export terminal, causing an extended outage with global energy market consequences. The December 2023 conflict dynamics demonstrated willingness by regional actors to accept escalatory risk.

Emerging Blind Spots

Shieldworkz has identified the following OT security blind spots commonly observed in regional assessments that represent elevated risk:

- OT Cloud Connectivity: The rapid adoption of cloud-based operational data platforms and IIoT connectivity is proceeding faster than security governance. Many operators have established cloud data connections without OT security team involvement or formal risk assessment, creating undocumented attack pathways into OT environments.
- Construction-Phase OT Security: Major industrial construction projects across the GCC are deploying new process automation with minimal OT security governance. Pre-commissioning network connectivity and contractor access during construction phases create enduring vulnerabilities that persist after commissioning.
- Dormant Vendor Accounts: Legacy vendor accounts created for equipment commissioning that were never formally decommissioned remain active on many OT networks assessed by Shieldworkz.

These accounts often retain privileged access and represent dormant insider threat and adversary exploitation vectors.

- OT Wireless Exposure: The deployment of industrial wireless networks (WirelessHART, ISA100, WiFi for mobile operations) without adequate segmentation is creating OT attack paths through inadequately secured wireless infrastructure.
- Legacy Protocol Exposure on Modern Networks: Operators migrating to modern Ethernet-based OT networks have in many cases maintained legacy serial-to-Ethernet converters that expose Modbus, DNP3, and proprietary protocols without authentication on the OT LAN, creating targets that did not previously exist in serial-connected environments.

OT Security Maturity Gaps Commonly Observed in the Region

Based on OT security assessments conducted by Shieldworkz across Gulf and wider Middle Eastern industrial operators, the following maturity gaps are consistently identified:

- Absence of OT-specific asset inventory covering firmware versions and communication protocols — without this, vulnerability management is effectively blind.
- No passive OT network monitoring capability — the majority of assessed environments have no visibility into OT network traffic, making intrusion detection impossible.
- Incomplete IT/OT segmentation — firewall rules at IT/OT boundaries are frequently outdated, over-permissive, or contain undocumented bidirectional access rules.
- Unmanaged engineering workstation security — EWS are frequently internet-connected, unpatched, and exempt from the security controls applied to IT endpoints.
- No OT-specific incident response capability — IT security teams are rarely trained or equipped to investigate and respond to OT security incidents, and OT operations teams do not have defined security incident roles.
- Inadequate OT backup and recovery posture — many operators cannot demonstrate that PLC logic and DCS configurations can be restored within an operationally acceptable timeframe.

Recommended Strategic Priorities for CISOs

- 1. Establish OT security as a board-level risk agenda item. Regional operators must elevate OT cyber risk from an engineering operations concern to a board-level strategic risk with defined governance, metrics, and accountability.
- 2. Invest in OT visibility before investing in OT controls. The highest-leverage near-term investment is understanding what is on the OT network and what it is doing. Without this foundation, all other security investments are navigating in the dark.
- 3. Treat vendor access as a first-order risk. Every active, unmonitored vendor connection to an OT environment is a potential adversary access pathway. Vendor access governance is a high-ROI control that is underinvested across the region.
- 4. Build OT incident response capability now, before an incident occurs. The cost of building IR capability before an incident is a fraction of the cost of responding to a major OT disruption without preparation.
- 5. Integrate OT security with IT security operations. Siloed OT security that does not share threat intelligence, monitoring data, and incident context with the IT security function misses the most important attack path — the IT-to-OT lateral movement that precedes the majority of OT attacks.

90-DAY EXECUTIVE ACTION PLAN

The following 10-action roadmap represents the minimum set of measures Shieldworkz recommends for immediate execution by Middle Eastern OT operators. These actions are sequenced by impact and feasibility and are designed to deliver the greatest risk reduction within a 90-day implementation horizon.

#	Action	Governance Owner	Expected Risk Reduction	Days
1	Eliminate internet exposure of all OT-facing systems. Run external scan, remediate all exposed OT management interfaces within 48 hours.	CISO / OT Security Manager	Eliminates the most commonly exploited initial access vector. Direct risk reduction against BAUXITE-class attacks.	0–7
2	Audit and restrict vendor remote access. Enforce JIT access, MFA, and session recording. Terminate all persistent, unused vendor connections.	CISO / OT Operations Manager	Closes the second-largest attack vector. Eliminates dormant adversary foothold risk via vendor channels.	0–14
3	Change all default OT device credentials. Inventory and vault all OT system credentials in a secured credential management system.	OT Engineering / OT Security	Eliminates trivial initial access on Modbus/HMI devices. Required to defeat BAUXITE-class PLC campaigns.	0–21
4	Patch critical vulnerabilities in VPN appliances and internet-facing systems. Prioritise CISA KEV entries.	IT Security / CISO	Eliminates the most frequently exploited initial access vulnerability class in OT-targeting campaigns.	0–30
5	Physically secure SIS engineering workstations. Set SIS keyswitches to RUN. Verify no network connectivity between SIS and IT networks.	OT Engineering / Safety Manager	Directly mitigates TRITON/TRISIS attack path. Protects highest-consequence OT asset class.	0–14
6	Deploy or verify OT network monitoring at IT/OT boundary and process network. Configure Modbus, OPC-UA, and protocol-specific alerts.	OT Security / SOC Manager	Provides first-ever OT network visibility. Enables detection of FrostyGoop, PIPEDREAM, and LOTL activity.	0–60
7	Commission independent IEC 62443 OT security gap assessment. Produce maturity baseline and risk-prioritised remediation roadmap.	CISO / Board Risk Committee	Provides authoritative current-state view. Directs all future investment. Supports regulatory compliance evidence.	30–90
8	Establish and test OT incident response procedure. Conduct tabletop exercise simulating ransomware pivot to OT environment.	CISO / OT Security / Legal	Dramatically reduces response time and outcome severity when an incident occurs. Validates IR capability.	30–60
9	Validate OT backup posture. Test restoration of critical PLC logic, DCS configuration, and SCADA databases to spare hardware.	OT Engineering / Business Continuity	Ensures recovery capability exists. Eliminates reliance on unverified backups discovered to be unusable during incident.	30–90
10	Brief board and executive leadership on OT cyber risk. Establish quarterly OT risk	CISO / CEO / Board Risk Committee	Ensures governance visibility, sustained investment, and	0–30

#	Action	Governance Owner	Expected Risk Reduction	Days
	reporting. Assign executive sponsor for OT security programme.		accountability for OT security programme outcomes.	

Shieldworkz Advisory Note

Organisations that execute all 10 actions within the 90-day timeline can expect to reduce their OT threat exposure by an estimated 60-70% against the most common attack scenarios currently observed in the region. Actions 1, 2, 3, and 5 are individually capable of preventing the majority of publicly disclosed OT attacks against regional operators in the past 24 months. The combination of internet exposure elimination (Action 1) and passive OT monitoring deployment (Action 6) addresses both the most common initial access vector and the absence of detection capability that currently allows adversaries to maintain undetected OT presence for extended periods.

DISCLAIMER

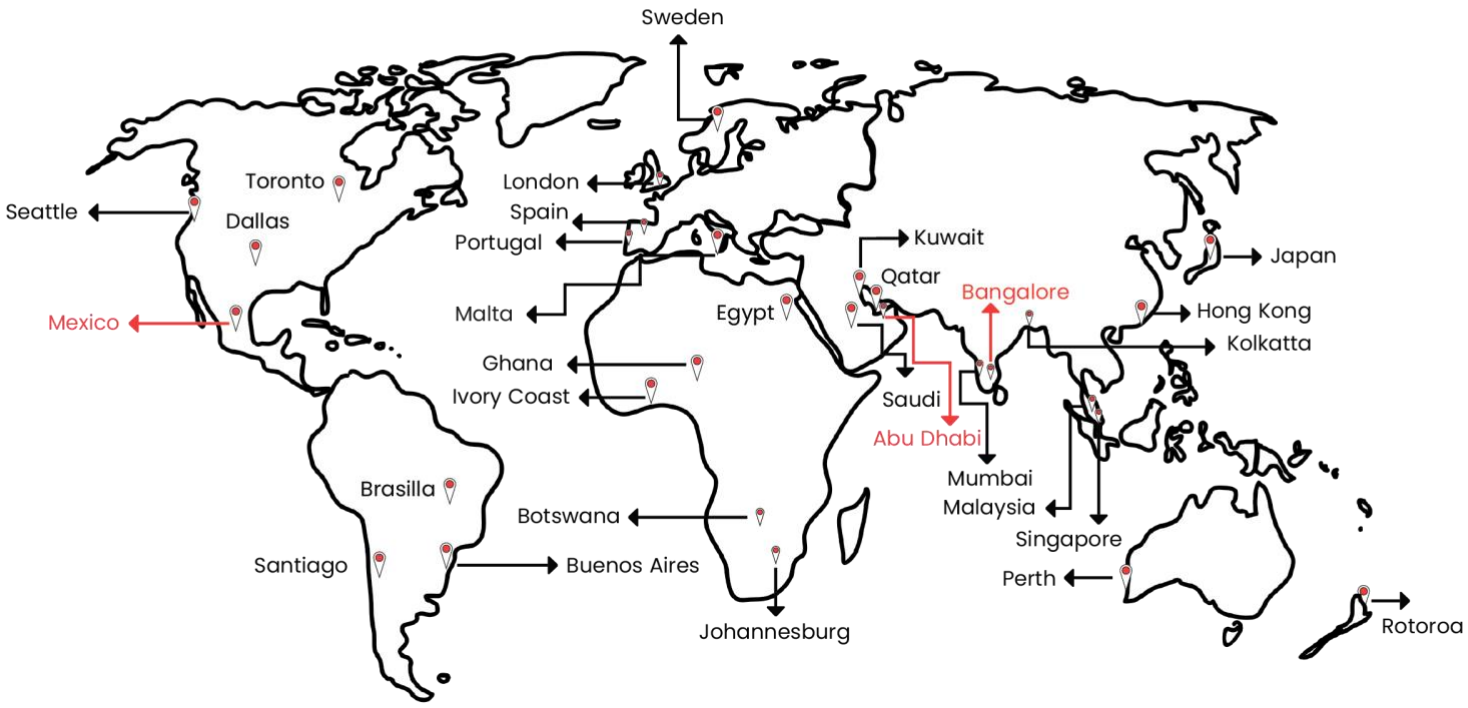
Intelligence Integrity Statement: All intelligence contained in this advisory is drawn from publicly available threat intelligence sources, disclosed incident reports, government and CERT advisories and Shieldworkz proprietary threat research and analysis. No fabricated, extrapolated, or speculative indicators have been included. All assessments are clearly labelled with confidence levels where stated. Shieldworkz does not include uncorroborated or single-source intelligence without explicit labelling.

Limitation of Liability: This advisory is provided for informational purposes only. Shieldworkz makes no warranty as to the completeness or accuracy of information derived from third-party sources. Recipients are responsible for their own risk management decisions. This advisory does not constitute legal, regulatory, or engineering advice.

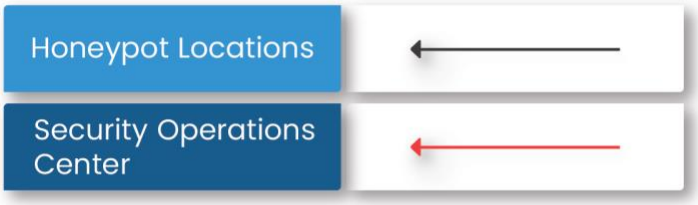
Currency: Intelligence in this advisory reflects the threat environment as assessed on 6 June 2026. The OT threat landscape evolves continuously; recipients should verify currency of specific threat actor and indicator data before operational use.

© 2026 Shieldworkz | OT Security Practice. This document is proprietary and confidential. Reproduction or distribution without written consent is prohibited.

About Shieldworkz



ISOC and Honeypot Locations



Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

Talk to us

From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

SHIELDWORKZ

CONTACT US

Fritz-Schäffer-Street 1,
4th floor

Bonn, 53113, Germany

+49 (0) 228 / 929 39210
europe@shieldworkz.com

Tenth floor,
FAB BUSINESS CENTER

Abu Dhabi,
United Arab Emirates

+971 56 660 5200
middleeast@shieldworkz.com

Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli

Bengaluru,
Karnataka 560093

+91 9059620557
apac@shieldworkz.com