SHIELDWORKZ

Global OT Cyber Threat Intelligence Advisory

H1 2026

SHIELDWORKZ | OT CYBER INTELLIGENCE ADVISORY

Global OT Cyber Threat Intelligence Advisory – H1 2026

Emerging Threat Landscape, Operational Risks, and Defensive Priorities for Critical Infrastructure Operators

Intelligence Period: Q4 2024 – Q2 2026 | Advisory Date: May 28, 2026

TLP:AMBER — RESTRICTED DISTRIBUTION

Prepared By:	Shieldworkz Threat Intelligence Division
Advisory Date:	May 28, 2026
Coverage	H1 2026
Intelligence Basis:	Shieldworkz sensor telemetry (70+ honeypots & sensors), partner threat intelligence, and incident response observations.
Classification:	**TLP:AMBER — Distribution restricted to named recipient organizations and their authorized security personnel.**
Primary Audience:	CISOs, OT Security Leaders, SOC/CTI Teams, Critical Infrastructure Operators, Risk & Resilience Executives, Board Stakeholders

DISCLAIMER: Intelligence assessments in this advisory reflect Shieldworkz analytical judgments based on data from its honeypots, sensor telemetry, and vetted external intelligence from various sources monitored by Shieldworkz.

1. Summary

The global OT/ICS threat environment has reached an unprecedented level of operational severity. The period from H2 CY2025 through H1 CY2026 has been defined by a fundamental shift: adversaries have progressed beyond strategic pre-positioning and are now demonstrating a clear willingness and capability to execute disruptive, destructive, and operationally impactful cyber operations against industrial environments.

CRITICAL INTELLIGENCE: The Shieldworkz 2026 OT Threat Landscape Report confirmed a 77% increase in site-level cyber incidents in 2025. Nation-state attacks with confirmed physical consequences are also rising significantly.

33%	119	3x	3,300
Increase in OT physical disruption incidents in H12026 vs. H12025	Ransomware groups targeting industrial organizations in 2025 (up from 80 in 2024)	Tripling of nation-state attacks with confirmed physical consequences in 2024	Industrial organizations impacted by ransomware in 2025 globally

1.1 Key developments: H2 CY2025 – H1 CY2026

The following intelligence-confirmed developments define the current threat landscape for critical infrastructure operators:

- Sandworm/Russia GRU: Executed DynoWiper campaign in December 2025 targeting approximately 30 distributed energy sites in Poland, including combined heat-and-power (CHP) facilities and renewable energy dispatch systems. This marked the first major coordinated attack targeting distributed energy resources (DERs) at scale. No power outages occurred, but OT systems critical to grid operations were compromised.
- VOLTZITE/Volt Typhoon: China-linked threat actors maintained persistent presence across US critical infrastructure through H12026. A newly identified initial access broker has weaponized vulnerabilities in Ivanti VPN appliances and F5 devices, handing established footholds to VOLTZITE for deeper OT intrusions in electric and water utilities.
- BAUXITE (Iran/IRGC-CEC, overlaps CyberAv3ngers): Deployed custom wiper variants against targets during the Iran-Israel conflict across Q2 CY2026. Previously confirmed across healthcare, utilities, manufacturing, and food and beverage sectors. The attack path involves active internet scanning of OT/ICS devices via Modbus/TCP, DNP3, and other exposed protocols and exposed ports.
- Handala: Is one of the most active threat actors tracked by Shieldworkz. Not only is this group targeting businesses across the globe, it is also focusing its efforts on a narrow range of enterprises belonging to a select set of countries. Handala also maintains a very large reconnaissance program that covers nearly 70 plus countries where we have found IOCs linked to this Iranian group.
- FrostyGoop (Malware): Confirmed OT-targeting malware leveraging Modbus/TCP protocol causing multiple disruptions.
- Loitering payloads: Industrial Surge: Shieldworkz tracked over 125 suspisious payloads including loggers actively targeting industrial organizations in H1 CY2026, this represents a 29% increase over H2 CY2025. Over two-thirds of such payloads were detected across utilities, manufacturing and ports.
- ENISA 2025 Threat Landscape: Analysis of approximately 4,900 cybersecurity incidents from July 2024 to June 2025 confirmed critical infrastructure and ICS as prime targets for both state-aligned actors and hacktivist organizations. Over 80% of phishing emails used AI-assisted generation by early 2025. (Source: ENISA 2025)

1.2 Why OT Environments remain high-value targets

Strategic Rationale	Operational Implication for Defenders
Geopolitical Leverage	Nation-states target critical infrastructure — power, water, fuel — to create civilian pressure, signal military capability, and pre-position for conflict escalation without kinetic engagement.
Safety System Impact	Targeting safety instrumented systems (SIS) creates potential for mass casualty events, catastrophic equipment damage, and uncontrolled physical process outcomes.
Production Disruption	Operational downtime translates directly to financial loss. A single hour of manufacturing downtime can cost $100,000–$1M+. Ransomware operators understand and exploit this leverage.
Weak Security Posture	Legacy OT systems with long lifecycles (10–20+ years), unpatched vulnerabilities, flat network architectures, and limited monitoring create persistently exploitable attack surfaces.
IT/OT Convergence Gaps	Digital transformation and Industry 4.0 initiatives have created new, often inadequately secured pathways between IT enterprise networks and OT environments.
Supply Chain Access	Trusted vendor relationships, remote maintenance access, and software supply chains provide adversaries legitimate-appearing entry points that bypass traditional perimeter controls.

SECTION 2: THREAT ACTOR LANDSCAPE

The following threat actors have been identified by Shieldworkz as active threats against OT/ICS environments. Attribution and TTPs are based on confirmed public reporting; analytical assessments are explicitly noted.

2.1 Nation-State OT threat actors

Actor (Alias)	Attribution	Primary OT Targets	Objective	Key Confirmed Activity	Risk
VOLTZITE (Volt Typhoon)	Chinese APT eco-system linked to MSS	US/Western electric, water, comms, transport infrastructure	Pre-positioning for conflict disruption	Persistent LOTL operations in US critical infrastructure through 2025 and H1 2026; KV Botnet via SOHO routers; SYLVANITE feeds footholds into VOLTZITE pipeline. FBI/Five Eyes confirmed attribution.	**CRITICAL**
Infrastructure Destruction Squad (Dark Engine).	Mandarin-speaking (posts made in Chinese). The low price point ($600) suggests a "hacktivist-for-hire" or a state-sponsored "pre-positioning" unit pulling off an operation masked as low-level criminals	Critical infrastructure across EU and US	Strategic signalling. The goal is not destruction (at least in the short term), but proving that Chinese threat actors can gain access to critical infrastructure.	The compromise of Venice's San Marco flood control pumps that occurred in later March/Early April 2026	**CRITICAL**
ELECTRUM (Sandworm)	Russia/GRU Unit 74455	Energy grids, distributed energy resources, telecom, water	Disruption, destruction, deterrence	DynoWiper vs Poland distributed energy (Dec 2025); AcidPour wiper for OT embedded devices; KyivStar telecom attack; PathWiper vs Ukraine. Is a highly capable OT-focused adversary in world	**CRITICAL**
KAMACITE	Russia-linked	US critical infrastructure, control loop systems	Control loop mapping, future disruption capability	Systematically mapped control loops across critical infrastructure throughout H1 2026.	**CRITICAL**
AZURITE (Flax Typhoon)	China-nexus, Integrity Technology Group	Manufacturing, defense, automotive OT engineering workstations	OT network intelligence gathering, exfiltration	Sustained operations across US, Europe, Asia-Pacific. Targets OT engineering workstations, exfiltrating network diagrams, alarm data, process configurations. Sequenced botnet: 200,000+ compromised devices.	**HIGH**
Unknown (possibly a subgroup of APT 28)	Russia-aligned	Energy, oil & gas, logistics, government (West Asia, Eastern Europe)	Conflict-adjacent OT disruption	Active in sectors supporting Russian military operations in Ukraine. Targeting profile may shift with geopolitical developments.	**HIGH**
BAUXITE (CyberAv3ngers / IRGC-CEC)	Iran/IRGC Revolutionary Guards Cyber-Electronic Command	US/Western water, energy, manufacturing, food & beverage, chemical	Disruption, political pressure, destruction	Four confirmed campaigns since 2025. Stage 2 ICS Kill Chain impacts. Deployed wiper variants against Israeli targets (June 2025). Compromised PLCs at US, Israeli and Mexican water utilities. Internet scanning of exposed OT devices.	**HIGH**
APT 41	China-linked,	Edge infrastructure: VPN appliances,	Initial access brokering, data	Rapidly weaponized vulnerabilities, high level of reconnaissance, persistence and	**HIGH**

Actor (Alias)	Attribution	Primary OT Targets	Objective	Key Confirmed Activity	Risk
		servers, PLCs, firewalls	exfiltration and persistence	interest in critical infrastructure. Members are trained on real OT environments across manufacturing and power.	
APT 35	Iran linked	PLCs, SCADA systems, Windows servers and OT networks	High scale of reconnaissance; Possibly a massive pre-positioning or initial access-linked campaign	Rapid scale of activities across the globe. The exact objective of this group remains a mystery which makes APT 36 a major threat.	HIGH

2.2 Ransomware groups targeting industrial operations

Ransomware represents the most frequently observed and operationally impactful threat to industrial organizations. Shieldworkz tracked 29 groups targeting industrial organizations in H1 CY2026, a 33% year-over-year increase. Manufacturing represents over a third of all OT ransomware victims.

Group	Primary Sectors Targeted	Notable OT/Industrial Impact	Tradecraft Highlights	Risk
LockBit 3.0	Manufacturing, healthcare, energy, logistics	Confirmed attacks on automotive, aerospace manufacturers. OT operations disrupted via IT network compromise spreading to OT-adjacent systems.	Triple extortion: encryption, data theft, DDoS. Affiliate model with wide targeting. Despite law enforcement action, continues operating under multiple aliases.	CRITICAL
Black Basta	Manufacturing, critical infrastructure, construction	Confirmed attacks causing production shutdowns in manufacturing sectors. Rapid IT-to-OT propagation exploiting flat network architectures.	Qakbot-linked initial access. Fast dwell time (hours to ransomware deployment). Targets Active Directory for lateral movement. Sophisticated double extortion.	CRITICAL
RansomHub	Critical infrastructure, manufacturing, healthcare, water	CISA advisory confirms RansomHub as highly active against critical infrastructure. Fast-growing affiliate program post-LockBit disruption.	Exploits VPN vulnerabilities for initial access. Affiliate model attracting experienced operators from disrupted groups. Data exfiltration before encryption.	HIGH
Play Ransomware	Manufacturing, government, finance, critical infrastructure	Active against industrial targets. CISA-confirmed advisory. No ransom negotiation — direct publication of stolen data if payment refused.	Exploits ProxyNotShell (Exchange), FortiOS vulnerabilities. Intermittent C2 communication to evade detection. Custom tools for exfiltration.	HIGH

2.3 Hacktivist and geopolitically motivated actors

Hacktivists have evolved significantly. Previously limited to DDoS and website defacement, groups increasingly achieve OT access via internet-exposed HMIs, misconfigured engineering workstations, and open industrial protocols. The ENISA 2025 Threat Landscape confirmed hacktivists increasingly view OT as a "pressure point for visibility" — attacks designed for operational and symbolic impact rather than ransomware.

- Hacktivists targeting internet-exposed HMIs and Modbus/TCP-accessible devices increased 17 percent in H1 2026. Several groups demonstrated capability to modify process variables on exposed systems.

- BAUXITE/CyberAv3ngers (Iran-aligned) successfully achieved Stage 2 of the ICS Cyber Kill Chain — the first confirmed hacktivist group to do so across 2024, with continued operations confirmed through 2025 and H1 CY2026.
- Pro-Russia and pro-Ukraine hacktivist groups conducted sustained campaigns against each other's critical infrastructure. Groups targeting OT are now becoming increasingly visible, focused and wide spread.
- ENISA notes the majority of hacktivist attacks remain DDoS-based (approximately 95%), but the 5% achieving actual breaches or OT access represent a meaningfully elevated risk given the growing number of motivated groups.

2.4 Supply chain adversaries and insider risks

- Trusted vendor relationships provide adversaries with legitimate-appearing access to OT environments. The SYLVANITE group's exploitation of VPN and edge device vulnerabilities as an initial access broker represents the codification of supply chain access as a service.
- Software supply chain risks persist following Solarwinds, Kaseya, and MOVEit incidents. Industrial software vendors and engineering toolsets (Historian platforms, SCADA software, remote support tools) represent high-value targets.
- Insider threats — including disgruntled employees, compromised contractor credentials, and social engineering of OT personnel — remain a documented and underreported risk category. Third-party engineering and maintenance contractors frequently possess elevated OT network access with minimal monitoring.
- Contractor remote access — often via personal or insufficiently hardened devices through shared VPN credentials — creates persistent exposure that adversaries actively exploit. Shieldworkz incident response observations confirm contractor remote access as a leading initial access vector in OT environments.

SECTION 3: MAJOR THREAT LANDSCAPE TRENDS

3.1 Trend overview matrix

Trend	Intelligence Assessment	Trajectory	Risk
Wiper Malware Displacing Ransomware (Nation-State)	In H1 2026, at least six distinct wiper campaigns are active across ndustrial/critical infrastructure: DynoWiper (energy), PathWiper (infra), AcidPour (telecom), BAUXITE wipers (energy), PYROXENE (infra), Handala (global healthcare). Wipers are now being detected across all types of OT environments including remote sites	Increasing rapidly	CRITICAL
LOTL Techniques in OT Environments	VOLTZITE usually moves with trusted network traffic, using legitimate administrative tools (WMI, PowerShell, netsh, native OS utilities) and maintains a low detection footprint. In OT environments, LOTL extends to misuse of engineering software, historian access, and legitimate industrial protocols.	Dominant TTP	CRITICAL
Internet-Exposed OT Assets	Shieldworkz has identified 19000+ .internet-exposed critical ICS devices communicating via Modbus globally in H1 2026. Such ports are either accessible during certain windows or are accessible throughout the year. Shodan and Censys research consistently reveal exposed HMIs, PLCs, and engineering workstations. BAUXITE and hacktivist groups conduct systematic port scanning for OT-specific protocols (TCP 102, 502, 20000, 44818).	Persistent / Growing	CRITICAL
IT/OT Network Convergence Risks	Digital transformation, remote work, BYOD and Industry 4.0 adoption have eroded traditional air gaps. Nearly 77% of OT attacks with physical impact being through IT network compromise. Flat networks enabling IT-to-OT lateral movement are the primary risk multiplier for ransomware impact on operations.	Persistent	CRITICAL
Ransomware Groups Targeting OT	Ransom incidents are rising. With production shutdown or slowdowns considered unacceptable, there is pressure on OT teams to get things back to normal quickly in the aftermath of a cyber incident. This enables ransomware groups to demand exorbitant amounts as ransom.	Accelerating	CRITICAL
Edge Infrastructure Exploitation	VPN appliances, firewalls, and edge devices continue to be weaponized as OT access enablers. CISA ICS-CERT issued multiple key advisories in 2025, covering ICS-specific vulnerabilities across 39 vendors. (Shieldworkz 2025 Report)	Accelerating	HIGH
AI-Assisted Cyber Operations	ENISA confirmed >80% of phishing emails used AI generation by early 2025. AI enables: highly personalized spear-phishing targeting OT engineers/operators; automated vulnerability discovery and exploit development; AI-assisted malware obfuscation; faster threat actor decision-making in complex OT environments. OT personnel are not immune to AI-enhanced social engineering. Threat actors also use AI to build psychological profiles of key plant personnel. Such data is used to identify potential rogue employees, targets for phishing, determine profiles of employees who may bypass security measures and indulge in risky behaviour that may compromise systems.	Accelerating rapidly	HIGH
IoT/Wireless Sensor Attack Surface	Industrial IoT adoption has created new blind spots. Shieldworkz sensor network (70+ honeypots/wireless sensors) observed automated IoT botnet attacks infiltrating critical OT networks within 24 hours in 2026. Wireless sensor deauthentication attacks and data manipulation have been observed in manufacturing, oil & gas, and energy environments.	Increasing	HIGH
Data Manipulation as Primary Technique	Shieldworkz 2026 threat data found Data Manipulation was detected three times more often than any other technique across Manufacturing, Transportation, and	Increasing	HIGH

Trend	Intelligence Assessment	Trajectory	Risk
	Energy OT environments. Silent data manipulation — altering process values, sensor readings, or historical data — without triggering alarms is an emerging and underdetected threat vector.		

SECTION 4: MALWARE FAMILIES, PAYLOADS AND TTPS

The following malware families and tooling have been confirmed by verified public reporting as active threats to OT/ICS environments. New ICS-specific malware is being developed at an unprecedented rate.

INTELLIGENCE NOTE: Only confirmed, publicly documented malware families are referenced in this section. Analytical assessments are clearly marked. This section should be used to inform detection engineering, threat hunting, and security tool tuning.

4.1 ICS-Specific Malware — Confirmed Families

Malware	Confirmed Date	OT Protocol/Target	Confirmed Capability & Impact	Attribution	Risk
FrostyGoop	Confirmed Jan 2024	Modbus TCP (TCP/502)	Confirmed ICS malware using Modbus protocol directly to cause physical impact. Can alter/spoof industrial process commands.	Russia-aligned with presence across Eastern Europe	CRITICAL
DynoWiper	Confirmed Dec 2025	Windows systems at OT/DER sites	Windows PE wiper deployed against Poland distributed energy resources. Wiped Windows-based machines at ~30 DER sites (CHP, wind, solar. Since then this wiper has been found in OT linked environments across EU, US, India and the Middle East.	Sandworm / Russia GRU	CRITICAL
AcidPour	Confirmed 2025	Embedded Linux, OT embedded devices, UBI filesystems	Enhanced wiper variant capable of wiping embedded devices commonly used in OT environments. Expanded from AcidRain. Targets routers, modems, and embedded OT hardware.	Sandworm / Russia GRU	CRITICAL
PathWiper	Confirmed 2024-2025	Windows systems, MBR/MFT destruction	Destroys MBR and MFT before overwriting files, making recovery as difficult as possible. Targeted Ukrainian critical infrastructure. Recovery requires complete system overhaul.	Russia-aligned (OPSWAT analysis)	HIGH
PIPEDREAM / INCONTROLLER	Discovered 2022 (but is still relevant)	OPC-UA, Modbus, CODESYS, Schneider Electric, Omron	Most sophisticated ICS attack framework ever publicly disclosed. Modular capability to disrupt, degrade, or destroy a wide range of industrial devices. Targets OPC-UA, Modbus, CODESYS runtime environments. CISA/FBI/NSA confirmed advisory. Likely represents a capability class rather than single incident.	Nation-state (Russia-attributed, US Gov assessment)	CRITICAL
TRITON / TRISIS	Confirmed 2017 (ongoing capability)	Schneider Electric Triconex Safety Instrumented Systems (SIS)	Designed to disable safety systems to allow physical damage. Deployed against Middle Eastern and Venezuelan oil and gas	Russia-attributed	CRITICAL

Malware	Confirmed Date	OT Protocol/Target	Confirmed Capability & Impact	Attribution	Risk
			facility. First confirmed attack against SIS. Represents a persistent capability template.		

4.2 Common MITRE ATT&CK for ICS Techniques Observed

Tactic	Technique ID	Observed Application in OT Incidents	Associated Actors
Initial Access	**T0866**	Exploitation of Remote Services — VPN appliances, remote desktop, engineering software exposed to internet	*VOLTZITE, SYLVANITE, BAUXITE, Ransomware groups*
Initial Access	**T0865**	Spearphishing Attachment — targeted OT engineers and operators using AI-enhanced lures	*Multiple nation-state and criminal groups*
Execution	**T0807**	Command-Line Interface — LOTL via PowerShell, WMI, native tools to avoid detection	*VOLTZITE, ELECTRUM, KAMACITE*
Persistence	**T0891**	Hardcoded Credentials — reuse of default/hardcoded OT device credentials for persistent access	*BAUXITE, hacktivist groups, ransomware IABs*
Discovery	**T0840**	Network Connection Enumeration — mapping OT network topology, identifying PLCs/HMIs/historians	*VOLTZITE, KAMACITE, AZURITE, BAUXITE*
Collection	**T0802**	Automated Collection — systematic collection of engineering files, network diagrams, process configurations	*AZURITE, VOLTZITE, GRAPHITE*
Lateral Movement	**T0812**	Default Credentials — using vendor default credentials for lateral movement across OT devices	*BAUXITE, ransomware groups, hacktivists*
Impact	**T0831**	Manipulation of Control — directly manipulating process control values via HMI/SCADA or OT protocols	*BAUXITE, FrostyGoop (Modbus), PIPEDREAM*
Impact	**T0879**	Damage to Property — destructive payload deployment targeting physical processes	*ELECTRUM (DynoWiper), PYROXENE, BAUXITE*
Impact	**T0816**	Device Restart/Shutdown — forcing OT device reboots or shutdowns to cause process disruption	*Multiple ransomware groups, BAUXITE*

SECTION 5: RISK ASSESSMENT AND OPERATIONAL EXPOSURE

5.1 Sector risk heat map

The following matrix reflects Shieldworkz analytical assessment of threat actor targeting intensity and operational impact potential across critical infrastructure sectors, based on confirmed incident data and intelligence reporting through May 2026.

Sector	Nation-State	Ransomware	Hacktivist	Wiper Risk	Supply Chain	Insider Threat	Overall
Manufacturing	HIGH	CRITICAL	MEDIUM	HIGH	HIGH	MEDIUM	CRITICAL
Energy & Utilities	CRITICAL	HIGH	HIGH	CRITICAL	HIGH	MEDIUM	CRITICAL
Oil & Gas	CRITICAL	HIGH	MEDIUM	HIGH	CRITICAL	HIGH	CRITICAL
Water & Wastewater	HIGH	MEDIUM	HIGH	HIGH	MEDIUM	MEDIUM	HIGH
Chemicals	HIGH	HIGH	MEDIUM	HIGH	HIGH	HIGH	HIGH
Transportation	HIGH	HIGH	HIGH	MEDIUM	HIGH	MEDIUM	HIGH
Maritime	MEDIUM	HIGH	MEDIUM	MEDIUM	HIGH	HIGH	HIGH
Telecommunications	CRITICAL	HIGH	MEDIUM	HIGH	HIGH	MEDIUM	CRITICAL
Defense Industrial	CRITICAL	MEDIUM	LOW	HIGH	CRITICAL	HIGH	CRITICAL
Pharmaceuticals	HIGH	HIGH	LOW	MEDIUM	HIGH	MEDIUM	HIGH
Food & Beverage	MEDIUM	HIGH	LOW	MEDIUM	MEDIUM	LOW	HIGH
Mining & Metals	MEDIUM	HIGH	MEDIUM	MEDIUM	MEDIUM	MEDIUM	HIGH

NOTE: CRITICAL = confirmed active targeting with demonstrated impact; HIGH = confirmed targeting with significant exposure; MEDIUM = documented targeting with moderate exposure; LOW = limited confirmed targeting.

5.2 Operational impact categories

Impact Category	Examples of Realized Impact	Key Threat Vectors	Affected Sectors	Severity
Physical Process Disruption	Heating system shutdown (FrostyGoop, Ukraine); DER sites taken offline (DynoWiper, Poland); Water treatment HMI manipulation (BAUXITE)	Wiper malware, direct OT protocol manipulation, IT/OT lateral movement via flat networks	Energy, Water, Manufacturing, Chemical	CRITICAL
Production Shutdown / OT Downtime	Ransomware causing manufacturing lines to halt; IT systems underpinning OT scheduling/logistics disrupted; SCADA server encryption	Ransomware (LockBit, Black Basta, RansomHub), IT-to-OT propagation	Manufacturing, Energy, Food & Bev, Pharma	CRITICAL
Safety System Compromise	Safety relay manipulation (TRITON/TRISIS template); SIS disabling to enable physical damage; suppression of	Purpose-built ICS malware (PIPEDREAM template), insider access	Oil & Gas, Chemical, Nuclear	CRITICAL

Impact Category	Examples of Realized Impact	Key Threat Vectors	Affected Sectors	Severity
	alarms before destructive payload			
Data Exfiltration & IP Theft	OT network diagrams, engineering files, process configurations, alarm logic stolen; used for future attack planning	AZURITE, VOLTZITE, GRAPHITE — systematic exfiltration during long-term access	Defense Industrial, Energy, Pharma	HIGH
Supply Chain & Third-Party Compromise	Vendor software containing backdoors; remote access tools exploited; contractor credentials abused	Software supply chain attacks, SYLVANITE-style IAB operations, compromised vendor portals	All sectors	HIGH
Financial & Reputational Impact	Ransom payments averaging $1M+ for industrial victims; regulatory fines; customer/investor confidence loss; stock price impact	Ransomware, data breach/extortion	Manufacturing, Energy, Pharma, Defense	HIGH

SECTION 6: INDICATORS OF COMPROMISE AND DETECTION GUIDANCE

6.1 OT-Specific anomalous activity indicators

Indicator Category	Observable / Detection Guidance	Relevant Actor/Malware	Priority
Modbus/OT Protocol Abuse	Unexpected Modbus read/write commands to registers outside normal operational baseline. Coil manipulation or register value changes not initiated by engineering workstation. FrostyGoop uses Modbus function codes 3 (Read Holding Registers), 6, and 16 to alter setpoints.	*FrostyGoop, BAUXITE, PIPEDREAM*	CRITICAL
Internet-Exposed OT Services	Monitor for inbound connections on OT protocol ports from non-whitelisted external IP ranges: TCP/502 (Modbus), TCP/102 (S7comm), TCP/20000 (DNP3 over TCP), TCP/44818 (EtherNet/IP), TCP/4840 (OPC-UA). Any external connection to these ports is a high-confidence indicator.	*BAUXITE, Hacktivists, BAUXITE scanning*	CRITICAL
Engineering Workstation Anomalies	Logic changes, firmware uploads, or configuration modifications outside approved maintenance windows. New connections from engineering workstations to external IP addresses. Installation of unauthorized software on EWS. Process historian queries from anomalous user accounts.	*VOLTZITE, AZURITE, GRAPHITE, KAMACITE*	CRITICAL
LOTL Detection — IT/OT Boundary	Unusual PowerShell or WMI activity from OT-adjacent systems. netsh, ipconfig, arp, route command execution from accounts without prior OT access history. RDP or SMB lateral movement traversing IT/OT DMZ. Tools: scheduled task creation, net use commands from OT systems.	*VOLTZITE, ELECTRUM, KAMACITE*	CRITICAL
Mass File Operations on OT Systems	Bulk file enumeration, staging in temp directories, unusual archive creation on SCADA servers, historians, or EWS. Indicator of pre-exfiltration staging or wiper preparation. Correlate with outbound transfers.	*Ransomware groups, AZURITE, all wipers*	HIGH
Remote Access Anomalies	VPN/RDP connections during off-hours from new geographic locations. Concurrent sessions for a single user from geographically impossible locations. Third-party vendor accounts accessing systems outside contracted maintenance windows. Dormant accounts suddenly activated.	*All groups — most common initial access*	HIGH
Wiper Pre-Indicators	Shadow copy deletion (vssadmin delete shadows). Backup job failures or backup agent stops. System service disabling. Abnormal disk I/O patterns. Event log clearing (Event IDs 1102, 104). These behaviors frequently precede destructive payload deployment.	*All wiper families (DynoWiper, PathWiper, AcidPour)*	HIGH
Safety System Interaction	Any software or network access to Safety Instrumented Systems (SIS) outside of formally approved change management windows. Connections to SIS engineering ports from non-SIS-authorized workstations.	*TRITON/TRISIS template, BAUXITE*	CRITICAL
DNS & Network Beaconing	Periodic outbound DNS queries to low-reputation or newly-registered domains. HTTP/S beaconing with consistent timing intervals. DNS tunneling patterns (high-volume TXT/NULL record queries). Connections from OT/DMZ networks to cloud services outside whitelist.	*C2 for most nation-state and ransomware groups*	HIGH
Credential Abuse	Multiple failed authentication attempts followed by success (brute force). Account activity from multiple geographically diverse IPs simultaneously. Service account interactive logons. Default OT credentials used for authentication (confirm default passwords changed).	*All threat actors — universal*	HIGH

6.2 Threat hunting recommendations

- Hunt for VOLTZITE/LOTL behavior: search for unusual use of WMI, PowerShell remoting, and native Windows tools on OT-adjacent systems. Baseline normal admin behavior and flag deviations, particularly from non-IT accounts.
- Hunt for Modbus scanning: review firewall and network flow logs for systematic port scans of TCP/502, TCP/102, and other OT protocol ports. BAUXITE is confirmed to conduct such scans to identify attack-able devices.
- Hunt for dormant credential activation: review accounts that have been inactive for 30+ days and suddenly become active, particularly service accounts and contractor accounts. Cross-reference with change management records.
- Hunt for control loop mapping activity: look for systematic read-heavy operations on OT historian data, engineering file access, and process variable queries that deviate from normal operational patterns — consistent with KAMACITE activity.
- Hunt for OT engineering file exfiltration: monitor for access to network topology diagrams, P&ID documents, ladder logic files, and historian configuration files from non-standard user contexts.

6.3 Logging and telemetry recommendations for OT environments

- Enable protocol-level logging for all Modbus, DNP3, EtherNet/IP, and OPC-UA communications. Baseline normal traffic patterns and configure anomaly alerting. The Shieldworkz OT NDR platform provides passive protocol parsing without operational impact.
- Capture and forward all authentication events from OT systems including engineering workstation logons, remote access sessions, and SCADA server access to a centralized SIEM with OT-aware correlation rules.
- Enable process historian audit logging. Monitor for queries, modifications, or large data exports outside of normal operational parameters. Historian data is a primary target for intelligence-gathering threat actors.
- Implement network flow logging (NetFlow/IPFIX) at all IT/OT boundary points. Maintain at minimum 90 days of flow data for forensic investigation purposes.

SECTION 7: DEFENSIVE RECOMMENDATIONS AND MITIGATION PRIORITIES

7.1 Immediate actions: CISO Priority List (30-Day Sprint)

#	Required Action	Rationale / Threat Addressed	Owner	Priority
1	Audit and eliminate all internet-exposed OT device interfaces. Search for externally accessible Modbus (TCP/502), S7comm (TCP/102), DNP3 (TCP/20000), EtherNet/IP (TCP/44818), and OPC-UA (TCP/4840) services. Any exposure is an immediate critical finding.	*FrostyGoop, BAUXITE scanning, Hacktivist access*	OT Security / Network Eng	CRITICAL
2	Conduct emergency review of all VPN appliances and edge devices. Apply all available patches for Ivanti, Fortinet, Cisco, Palo Alto, and F5 products. SYLVANITE specifically weaponizes Ivanti and F5 vulnerabilities as OT access vectors.	*SYLVANITE, VOLTZITE, Ransomware IABs*	IT Security / Network	CRITICAL
3	Implement network segmentation validation. Verify that OT networks cannot be reached directly from enterprise IT networks without traversing a properly controlled industrial DMZ. Test with active network scanning.	*IT/OT convergence risk, ransomware lateral movement*	OT Engineering / Network	CRITICAL
4	Implement OT-aware passive network monitoring. Deploy a solution (Shieldworkz OT NDR or equivalent) capable of parsing OT protocols without active scanning. Establish baseline traffic profiles within 30 days.	*LOTL detection, FrostyGoop-style Modbus abuse, KAMACITE mapping*	SOC / OT Security	CRITICAL
5	Audit all remote access pathways to OT environments. Identify and remove unauthorized vendor VPN credentials and dormant accounts. Implement session recording and MFA for all third-party OT remote access.	*VOLTZITE LOTL, ransomware IABs, contractor abuse*	IAM / OT Security	CRITICAL
6	Inventory all Safety Instrumented Systems (SIS). Verify network isolation and access controls. No SIS should be reachable from enterprise IT or from internet-connected systems without explicit, documented justification.	*TRITON/TRISIS template, PIPEDREAM-class capability*	OT Engineering / Safety	CRITICAL
7	Review and harden all default and shared OT device credentials. BAUXITE and hacktivist groups routinely exploit default Unitronics, Siemens, Rockwell, and Schneider Electric credentials for initial access to HMIs and PLCs.	*BAUXITE, CyberAv3ngers, Hacktivist groups*	OT Engineering / IAM	HIGH
8	Test OT backup and recovery procedures. Verify that critical OT system backups (PLC logic, DCS configurations, historian data) are stored offline and that restoration procedures have been validated within the past 12 months.	*Wiper malware defense, ransomware recovery*	OT Engineering / BCP	HIGH

7.2 Strategic defensive architecture priorities

- Zero Trust for OT: Implement identity verification and least-privilege access for all OT network access — including engineering workstations, historian access, and HMI connections. No implicit trust based on network location.
- OT Network Segmentation: Implement ISA/IEC 62443 zone-and-conduit architecture. Each Purdue model level should have explicit, controlled access paths. Industrial DMZ between IT and OT is mandatory, not optional.
- Asset Visibility: Maintain a comprehensive, continuously updated OT asset inventory. You cannot monitor what you cannot see. Passive discovery using Shieldworkz OT Platform or equivalent is preferred to avoid operational disruption.
- Exposure Management (EASM): Continuously monitor the external attack surface for unintentionally exposed OT interfaces. BAUXITE conducts systematic Shodan-based scanning — organizations should identify their own exposure before adversaries do.

- Secure Remote Access: Implement OT-specific remote access solutions with MFA, session recording, and just-in-time access for all vendor/contractor remote connections. Prohibit direct VPN access to OT networks from general enterprise VPN solutions.
- OT Threat Intelligence Integration: Integrate ICS-specific threat intelligence (CISA ICS-CERT advisories, sector ISACs, Shieldworkz TI Platform) directly into SOC operations. Generic IT threat intel is insufficient for OT environments.
- Purple Team Exercises: Conduct OT-specific tabletop and simulation exercises using confirmed threat actor TTPs (VOLTZITE LOTL, FrostyGoop-style Modbus abuse, ransomware IT-to-OT propagation scenarios) to validate detection and response capabilities.

SHIELDWORKZ: Shieldworkz provides OT Risk Assessment services specifically designed to identify and quantify exposure to the threat vectors documented in this advisory. The Shieldworkz OT Security Platform delivers passive OT asset discovery, protocol-aware NDR, and threat intelligence integration without requiring active scanning or operational risk. Contact your Shieldworkz account team to schedule an OT Risk Assessment.

SECTION 8: OT SOC & DETECTION STRATEGY RECOMMENDATIONS

The IT-centric SOC model is fundamentally inadequate for OT environments. OT protocols, device behaviors, operational baselines, and engineering workflows require purpose-built detection logic, specialized analyst skills, and dedicated visibility tooling. Organizations operating with IT-only SOC coverage for OT environments have significant undetected risk.

8.1 OT SOC Capability Requirements

Capability	Requirement Detail	Tooling / Approach
OT Protocol Parsing	SIEM must ingest and correlate events from OT protocols: Modbus, DNP3, EtherNet/IP, S7comm, IEC 61850, OPC-UA, and Profinet. IT SIEM platforms cannot parse these natively without OT-specific integration.	Shieldworkz OT NDR Platform (passive, protocol-aware);
Passive Asset Discovery	Asset inventory must be built from passive network traffic analysis to avoid operational disruption. No active scanning of OT networks.	Shieldworkz OT Security Platform passive discovery module; deep packet inspection of OT traffic
Process Behavioral Baseline	Normal OT behavior (setpoints, process variable ranges, command sequences, engineering access patterns) must be baselined to enable anomaly detection.	Shieldworkz OT NDR behavioral analytics; historian integration for process baseline
IT/OT Threat Correlation	Threats frequently traverse IT/OT boundaries. Correlation rules must span both domains: IT initial access linked to OT lateral movement, ransomware IT infection propagating to OT-adjacent systems.	Unified SIEM/XDR with Shieldworkz OT data feeds; cross-domain playbooks in SOAR
ICS-Specific Detection Rules	SIEM detection logic must cover ICS-specific TTPs: unauthorized firmware upload, PLC logic modification, historian data manipulation, safety system access, and Modbus/DNP3 coil manipulation.	Shieldworkz detection rule library; CISA ICS-CERT detection guidance; MITRE ATT&CK for ICS mappings
OT-Aware Incident Response	SOC playbooks must include OT-specific containment procedures that account for safety, operational continuity, and the inability to simply "take systems offline" in process environments.	Shieldworkz OT IR playbooks; coordination with OT engineering during incident response

8.2 High-Value OT Detection Use Cases

- FrostyGoop-class Modbus manipulation: Alert on Modbus function codes 6 (Write Single Register) and 16 (Write Multiple Registers) targeting process control setpoints outside of approved maintenance windows. Correlate with source IP and time of day.
- VOLTZITE LOTL detection: Establish behavioral baselines for administrative tool use on OT-adjacent systems. Alert on first-seen use of PowerShell, WMI, or scheduled task creation from OT network segment user accounts.
- KAMACITE control loop mapping: Detect systematic Historian read queries that enumerate process variables across multiple control loops — consistent with adversary mapping for future disruption.
- Ransomware pre-deployment indicators: Detect shadow copy deletion commands, backup agent stops, and Event ID 1102 (audit log cleared) occurring in sequence within a short time window — high-confidence pre-ransomware deployment signal.
- Unauthorized PLC logic modification: Any firmware upload or logic change to PLCs, RTUs, or DCS controllers from a source other than the formally designated engineering workstation during a scheduled maintenance window should trigger an immediate critical alert.

SHIELDWORKZ: The Shieldworkz OT Security Platform and NDR solution delivers all capabilities described in this section — passive discovery, protocol-aware detection, behavioral baseline analytics, IT/OT threat

correlation, and pre-built ICS detection use cases — in a single purpose-built OT platform. The platform is deployed in passive mode and does not require active scanning, preserving operational integrity. Contact Shieldworkz for a platform demonstration or a proof-of-concept engagement.

SECTION 9: SECTOR-SPECIFIC RISK CONSIDERATIONS

The following sector profiles are based on confirmed incident data, verified threat intelligence reporting, and Shieldworkz operational experience. Each profile identifies sector-unique attack paths not captured in generic OT security guidance.

Manufacturing

SECTOR RISK: CRITICAL

Threat Summary	Key Threat Actors & Malware	Unique Attack Paths
• Largest single ransomware victim sector globally • Data Manipulation techniques detected 3x more frequently than any other technique in manufacturing OT environments (Shieldworkz 2026 Report). • Automated IoT botnet attacks have infiltrated critical manufacturing OT networks within 24 hours in documented incidents.	• LockBit 3.0, Black Basta, RansomHub (ransomware); AZURITE (OT engineering workstation targeting, exfiltration of process configs); VOLTZITE (pre-positioning in US manufacturing)	• Flat IT/OT networks enabling ransomware propagation from corporate email to plant floor SCADA within hours. • Historian servers accessible from enterprise network without DMZ controls. • Third-party maintenance engineers with standing VPN access to production OT networks. • Wireless sensor networks introduced without security controls creating new OT blind spots.

Shieldworkz Recommendation: Priority: Implement network segmentation between IT and OT immediately. Deploy Shieldworkz OT NDR for passive manufacturing floor monitoring. Conduct OT-specific ransomware tabletop exercise.

Energy & Utilities (Electric, Gas, Water)

SECTOR RISK: CRITICAL

Threat Summary	Key Threat Actors & Malware	Unique Attack Paths
• Nation-state attacks targeting energy infrastructure grew significantly in H1 2026 • Sandworm's December 2025 DynoWiper campaign against Polish distributed energy resources marked a new escalation — targeting DERs (wind, solar, CHP) as a coordinated infrastructure disruption method. This campaign is now continuing across EU and US in slow and stealth mode	• Sandworm (DynoWiper, AcidPour); VOLTZITE/KAMACITE (US grid pre-positioning); FrostyGoop (Modbus-based heating control manipulation)	• Grid management systems accessed via compromised engineering workstation credentials. • VPN appliances at remote substations and generating sites exploited as initial access vectors. • Distributed energy resources (solar inverters, wind turbine controllers) with internet connectivity and weak authentication. • OT-IT convergence at Energy Management System (EMS) and

• KAMACITE systematically mapped US energy control loops throughout 2025, assessed as pre-positioning for operational disruption.		Advanced Distribution Management System (ADMS) boundaries.

Shieldworkz Recommendation: Priority: Audit DER connectivity and authentication controls urgently. Deploy Shieldworkz OT Platform for substation and generation site monitoring. Review all remote access to EMS/ADMS/SCADA systems.

Oil & Gas

SECTOR RISK: CRITICAL

Threat Summary	Key Threat Actors & Malware	Unique Attack Paths
• Oil & gas remains a primary target for nation-state actors due to geopolitical leverage and critical supply chain role. • Safety Instrumented System (SIS) targeting (TRITON/TRISIS template) remains a documented adversary capability applicable to oil & gas safety systems globally. • Supply chain compromise of engineering software and automation vendor software used in upstream/midstream operations is a documented risk.	• GRAPHITE (energy/oil & gas targeting, Russia-aligned); VOLTZITE (pre-positioning); APT33/Magnallium (Iran, historical oil & gas targeting); Ransomware groups impacting operations	• Remote well site PLCs accessible via cellular modems without authentication. • Safety relay systems connected to corporate networks for monitoring without adequate isolation. • Process historian servers bridging safety and operational networks. • Vendor remote support portals providing direct access to production OT without session monitoring.

Shieldworkz Recommendation: Priority: Audit all remote well site and pipeline OT connectivity. Verify SIS network isolation. Implement Shieldworkz OT Risk Assessment specifically scoping upstream/midstream OT exposure.

Water & Wastewater

SECTOR RISK: HIGH

Threat Summary	Key Threat Actors & Malware	Unique Attack Paths
• BAUXITE (Iran/IRGC) conducted confirmed attacks on US water utilities via Unitronics PLC exploitation, with CISA advisory confirmation. • Water infrastructure is disproportionately targeted by hacktivists due to high symbolic impact and commonly	• BAUXITE/CyberAv3ngers (Unitronics PLC exploitation); Hacktivist groups (internet-exposed HMIs); ELECTRUM (demonstrated capability against water sector)	• Internet-exposed Unitronics, Siemens S7, or Allen-Bradley HMIs accessible via default credentials. • Chemical dosing controllers (chlorination, pH) accessible from insecure remote access connections. • Small utility operators with minimal IT/OT

weak OT security posture. • Municipal Utilities (Global): Russia-linked group confirmed to have remotely mis-operated two water treatment HMIs		security resources and no dedicated OT security monitoring. • SCADA vendors with standing remote access for maintenance creating persistent exposure.

Shieldworkz Recommendation: Priority: Immediately audit all external-facing OT interfaces for water treatment and distribution. Change all default credentials on PLCs and HMIs. Contact Shieldworkz for water sector OT security assessment.

Transportation and logistics

SECTOR RISK: HIGH

Threat Summary	Key Threat Actors & Malware	Unique Attack Paths
• Transportation control systems, rail signaling, port operations, and logistics networks are confirmed targets for both nation-state and ransomware actors. • GPS jamming and spoofing affecting aviation, maritime, and road logistics tripled in 2024, impacting operational safety and timing. • Ransomware targeting logistics operators creates cascading supply chain disruptions beyond the direct victim.	• Nation-state actors (GPS jamming campaigns); Ransomware groups (LockBit, Black Basta — confirmed logistics sector attacks); BAUXITE (transportation systems targeted in confirmed campaigns)	• Rail signal controller networks accessed via legacy IT/OT integration points. • Port operational technology (crane controllers, terminal management systems) connected to business networks without adequate segmentation. • Fleet management and dispatch systems bridging IT and vehicle/equipment OT. • GPS-dependent operational systems vulnerable to spoofing without authentication validation.

Shieldworkz Recommendation: Priority: Review GPS-dependent operational dependencies and resilience planning. Audit port OT networks and rail signaling system connectivity. Shieldworkz transportation sector OT assessment available.

Defense Industrial Base

SECTOR RISK: CRITICAL

Threat Summary	Key Threat Actors & Malware	Unique Attack Paths
• Defense industrial base (DIB) is a primary target for Chinese nation-state actors seeking technology exfiltration and supply chain intelligence. • AZURITE specifically targets manufacturing and defense OT engineering workstations to exfiltrate network	• AZURITE/Flax Typhoon (OT workstation exfiltration); VOLTZITE (pre-positioning); GRAPHITE (defense-adjacent targeting); nation-state espionage actors broadly	• Engineering workstations with OT design files connected to corporate IT networks without adequate data exfiltration controls. • Defense contractors with IT security programs but minimal OT visibility, especially in facilities with both commercial and defense production.

diagrams, alarm data, and process configurations. • CMMC Level 2 and Level 3 requirements are driving security investment, but OT environments within DIB suppliers remain a significant gap.		• Software supply chain exposure through shared engineering tools and automation vendor software used in DIB manufacturing.

Shieldworkz Recommendation: Priority: Implement OT data exfiltration monitoring as a CMMC-aligned capability. Deploy Shieldworkz OT NDR for continuous DIB manufacturing OT monitoring. Conduct OT-specific threat hunting aligned to AZURITE and VOLTZITE TTPs.

SECTION 10: EXECUTIVE AND BOARD-LEVEL GUIDANCE

10.1 Questions boards should ask security leaders

Board Question	What a Strong Answer Looks Like
Do we have visibility into what is happening on our OT networks in real time?	We have deployed passive OT monitoring (Shieldworkz OT NDR or equivalent) across our critical OT environments. We can detect anomalous protocol behavior, unauthorized device connections, and engineering workstation anomalies within minutes.
Have we confirmed that nation-state actors such as Volt Typhoon/VOLTZITE have not pre-positioned inside our critical infrastructure networks?	We have conducted a formal OT threat hunt using confirmed VOLTZITE TTPs (LOTL behavior, SOHO router compromise, deep OT network access). We have reviewed access logs, network flows, and OT device configurations for indicators documented in CISA and Shieldworkz advisories.
If ransomware hit our IT network tomorrow, how long before OT operations would be impacted?	We have validated network segmentation preventing IT-to-OT propagation. We have tested this with tabletop exercises. Our OT systems can operate in a degraded/manual mode for X hours/days while IT is restored.
Are our safety systems (SIS) isolated from our OT and IT networks?	Yes — we have documented isolation controls for all SIS. These have been independently validated. No SIS device is reachable from the corporate network or internet. We review this annually.
What is our OT incident response time from detection to containment?	Our OT-specific IR plan has been exercised within the past 12 months. Our target MTTD for OT anomalies is X minutes. We have pre-established relationships with an OT-specialized IR retainer (such as Shieldworkz) for immediate response support.
Are our critical infrastructure vendors and contractors properly monitored when they access our OT environments?	All third-party OT remote access is channeled through a monitored jump server with session recording, MFA, and just-in-time access. We conduct quarterly audits of third-party access logs.

10.2 OT Cybersecurity Investment Priorities

#	Investment Area	Business Case / Threat Addressed	Timeline	Priority
1	**OT Asset Visibility & NDR Platform**	Without knowing what is on your OT network, you cannot protect it. Passive NDR addresses VOLTZITE LOTL, FrostyGoop-class Modbus abuse, and enables all downstream detection capabilities. Foundation investment.	Immediate (0-90 days)	**CRITICAL**
2	**OT Network Segmentation (IT/OT DMZ)**	Prevents ransomware IT-to-OT propagation. The single most impactful structural control for production continuity resilience. Addresses the primary ransomware impact vector.	0-180 days	**CRITICAL**
3	**OT-Specific Incident Response Retainer**	Pre-negotiated IR capability with OT expertise prevents costly delays during active incidents. OT IR requires specialized skills not available in most IT-focused IR firms.	Immediate	**CRITICAL**
4	**Secure OT Remote Access Architecture**	Eliminates the leading initial access vector for both nation-state actors and ransomware groups. PAM, MFA, session recording for all OT remote access.	0-90 days	**HIGH**

#	Investment Area	Business Case / Threat Addressed	Timeline	Priority
5	**OT Threat Intelligence Program**	ICS-specific threat intel (CISA ICS-CERT, sector ISAC, Shieldworkz TI) enables proactive detection tuning against confirmed adversary TTPs. Generic IT threat intel does not address OT threats.	0-90 days	HIGH
6	**OT Risk Assessment & Penetration Testing**	Validate actual exposure. Shieldworkz OT Risk Assessment identifies exploitable paths before adversaries do. Required for regulatory compliance (NERC CIP, IEC 62443, NIS2) and cyber insurance underwriting.	0-90 days	HIGH
7	**OT Security Awareness Training**	OT engineers and operators are targeted by AI-enhanced social engineering. Role-specific training addressing OT-specific threats is distinct from IT security awareness.	0-180 days	MEDIUM
8	**OT Backup & Recovery Validation**	Validate that OT backups (PLC logic, DCS configs, historian data) are functional, tested, and protected from ransomware/wiper destruction. Mandatory for operational resilience.	0-180 days	HIGH

10.3 Key regulatory and compliance considerations

- NERC CIP (North America Electric): Critical Infrastructure Protection standards mandate OT security controls for bulk electric system operators. Recent updates reflect increasing OT-specific threat requirements.
- IEC 62443: The international standard for industrial automation and control system security. Provides zone-and-conduit architecture requirements directly applicable to all sectors.
- NIS2 Directive (EU): Significantly expands OT security obligations for EU critical infrastructure operators across energy, transport, water, health, and manufacturing. Mandatory implementation by member states.
- TSA Pipeline Security Directives: Mandatory cybersecurity measures for critical US pipeline operators, including OT network segmentation and incident reporting requirements.
- CISA Binding Operational Directives: Apply to US federal agencies but represent best practice benchmarks for all critical infrastructure sectors and are increasingly referenced in cyber insurance underwriting.

SECTION 11: FUTURE OUTLOOK — 12–24 MONTH HORIZON

The following analytical assessments represent Shieldworkz intelligence judgments regarding the trajectory of OT cyber threats through 2027. These assessments are based on confirmed trend data, adversary capability evolution, and geopolitical context. They are presented as analytical judgments, not confirmed intelligence.

INTELLIGENCE NOTE: ANALYTICAL ASSESSMENT: The following projections represent high-confidence analytical judgments based on confirmed trend trajectories. They are not confirmed intelligence of specific planned operations.

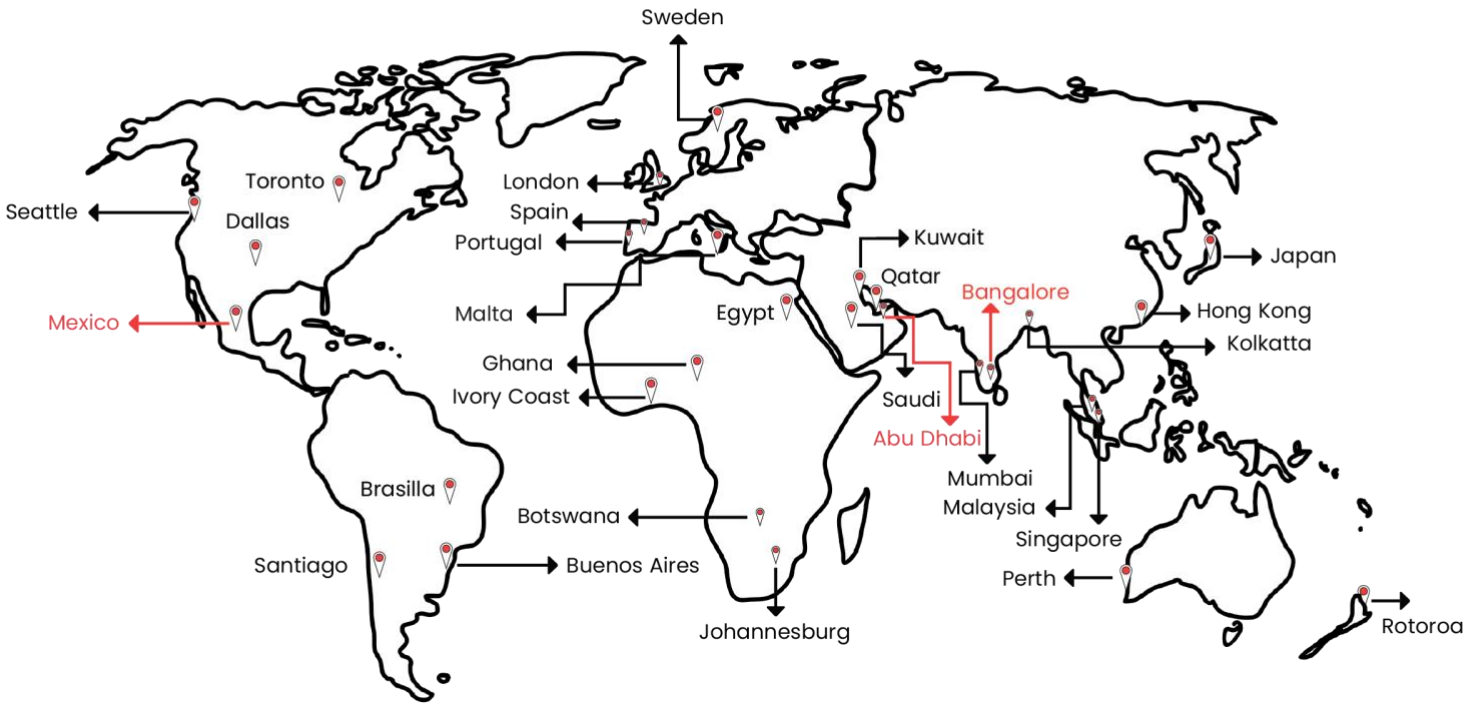
Emerging Risk	Analytical Assessment	Timeline	Confidence
Adversarial AI in OT Operations	AI-assisted adversary capabilities will expand to include automated OT network reconnaissance, AI-generated spear-phishing targeting OT engineers with plant-specific context, and AI-assisted malware adaptation to evade OT-specific detection. The 80%+ AI phishing rate (ENISA 2025) will approach near-universal adoption by threat actors.	6-12 months	High
DER & Grid Edge Targeting Escalation	ELECTRUM's December 2025 DynoWiper campaign against Polish DERs established a new targeting template. Distributed energy resources (solar, wind, battery storage) with internet connectivity and weaker security posture than traditional utility infrastructure will face sustained, coordinated nation-state targeting globally.	Ongoing / escalating	High
OT Ransomware-as-a-Service Maturation	The ransomware ecosystem will expand with increasingly OT-aware affiliates who understand industrial processes, timing, and leverage points. Custom OT ransomware variants targeting specific industrial verticals are assessed as a near-term development.	12-18 months	Medium-High
LOTL Capability Proliferation	VOLTZITE/KAMACITE LOTL techniques will proliferate to mid-tier threat actors as tooling and tradecraft are shared across the adversary ecosystem. Detection based on signatures and known IOCs will become increasingly ineffective. Behavioral analytics and OT protocol baselining become essential.	Ongoing	High
Safety System Targeting Expansion	The TRITON/TRISIS and PIPEDREAM capability templates will be adapted by additional nation-state actors. As OT security improves for operational systems, safety systems become the highest-value remaining target for actors seeking catastrophic physical impact.	18-24 months	Medium
Quantum Computing Risk to OT PKI	OT devices with long lifecycles increasingly rely on cryptographic authentication. Quantum computing advances threaten RSA and ECC-based OT authentication within the operational lifespan of equipment being deployed today. Organizations should audit OT cryptographic posture.	24-36 months	Medium
Autonomous Systems & Industrial AI Attack Surface	Industrial AI systems, digital twins, and autonomous manufacturing introduce new attack surfaces with direct physical process control authority. Adversarial manipulation of industrial AI training data or inference systems creates novel attack paths without clear existing detection coverage.	18-24 months	Medium

SHIELDWORKZ: Shieldworkz Defensive Capability Roadmap: As the threat landscape evolves toward AI-assisted adversary operations, DER targeting, and LOTL-dominant TTPs, Shieldworkz is advancing the Shieldworkz OT Security Platform with behavioral AI-based anomaly detection, AI-assisted OT threat hunting, and expanded OT protocol coverage. Engage your Shieldworkz team to discuss your organization's defensive capability roadmap aligned to the threats documented in this advisory.

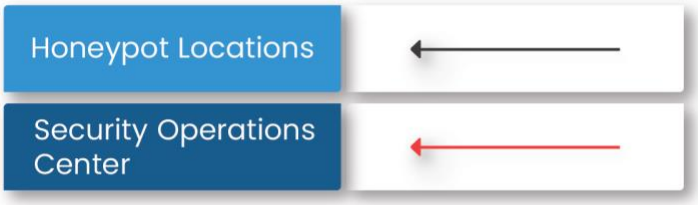
11.1 Defensive Capability Priorities for Future Resilience

- Behavioral Analytics over Signature Detection: As LOTL dominates nation-state tradecraft and ransomware groups adopt similar techniques, investments must shift toward behavioral analytics, OT process baseline monitoring, and anomaly detection rather than signature/IOC-based detection.
- AI-Resistant Security Architectures: Implement controls that remain effective against AI-enhanced adversary capabilities — specifically: multi-factor authentication resistant to AI-generated social engineering, behavioral detection of AI-assisted reconnaissance, and human-in-the-loop validation for high-consequence OT operations.
- OT Resilience by Design: As destructive wiper malware becomes a standard nation-state tool, OT resilience — not just prevention — becomes the essential design requirement. Offline OT backups, manual operation capability, and tested recovery procedures are as important as preventive controls.
- Threat Intelligence-Led Defense: The speed of adversary adaptation requires intelligence-led defense. Organizations must consume and operationalize current OT threat intelligence faster than adversaries adapt their TTPs. Shieldworkz TI integration into SOC operations enables this.

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