txOne networks | Keep the Operation Running

White Paper

Safeguarding Production:

OT Cybersecurity for Legacy and Transient Assets in Oil and Gas

As oil and gas operations continue to digitize, aging infrastructure and transient assets are increasingly exposed to sophisticated cyber threats – creating a perfect storm of vulnerability.

From legacy control systems still running outdated software to mobile laptops and USB devices that cross into secured operational technology (OT) environments, upstream and midstream operators face an expanded attack surface that traditional IT security models fail to protect.

This white paper provides an overview of the modern cyber risk landscape facing oil and gas producers, examining high-profile incidents – including the Colonial Pipeline ransomware attack and Shamoon malware campaigns – to highlight often-exploited weak points in IT/OT converged networks.

By reading this white paper, you'll gain:

- Insights into the most common attack vectors, including compromised remote access, removable media, and third-party equipment
- A detailed breakdown of vulnerabilities in critical technologies such as LEO terminals, OPC UA protocols and SOHO devices
- Real-world examples of ransomware and ICS-targeted campaigns that have impacted energy sector operations worldwide
- A strategic roadmap of mitigations, aligned to NIST and ISA/IEC 62443 frameworks, to help reduce cyber risk, improve visibility, and safeguard production continuity

Whether you're a plant manager, cybersecurity leader, or operational executive, this whitepaper offers practical guidance to strengthen defenses where they're weakest and most critical. In an industry where downtime is costly and safety is critical, securing legacy and transient assets isn't just good practice but essential to future-proofing your operations.

A Prime Target for Cyberattacks

Cyberattacks in the oil and gas industry have become increasingly sophisticated, frequent, and damaging in recent years. The oil and gas sector is a high-value target due to its economic importance, reliance on aging OT systems, and interconnected global supply chains. As a critical infrastructure sector, any disruption to oil and gas operations can have far-reaching consequences for national security, economic stability, and public safety.

Many of the industry's operational technology (OT) systems are legacy assets that lack basic cybersecurity controls such as authentication, encryption, and logging, making them especially susceptible to intrusion.

Additionally, the global nature of oil and gas operations, which involves multinational facilities, remote assets, and complex supply chains, further increases the attack surface and introduces challenges in standardizing security measures.

Financially, the high urgency of maintaining production and uptime makes oil and gas companies attractive targets for ransomware attacks, as adversaries can demand and often receive substantial payouts. Moreover, the sector holds valuable intellectual property and sensitive operational data, making it a target not just for cybercriminals but also for nation-states and competitors engaged in espionage.

Why Cybersecurity Matters in Oil & Gas: Lessons from Major Attacks

Cybersecurity is no longer just an IT concern – it's a frontline defense for operational continuity, safety, and national security in the oil and gas industry. These high-profile incidents highlight just how devastating cyberattacks can be when security gaps go unaddressed.

Colonial Pipeline Ransomware Attack (May 2021)

When One Password Shuts Down an Industry

A ransomware attack by the DarkSide group brought the largest refined oil pipeline in the U.S. to a standstill, leading to widespread fuel shortages across the East Coast. The attackers gained access through a VPN account that lacked multi-factor authentication (MFA). Colonial Pipeline paid $4.4 million to regain control – some of which was later recovered by the Department of Justice – but the disruption to critical infrastructure was already done.

Saudi Aramco Shamoon Attacks (2012, 2016, 2017)

A Wake-Up Call for Industrial Cybersecurity

Over 35,000 workstations were wiped clean in the 2012 attack on Saudi Aramco by suspected nation-state actors. The malware, known as Shamoon, was designed not to steal – but to destroy. It shut down business operations and sent a global warning: destructive malware targeting OT environments is a real and growing threat.

Norsk Hydro Ransomware Attack (2019)

Transparency in the Face of Crisis

Though not an oil company, Norsk Hydro's global operations resemble those in energy and refining. When LockerGoga ransomware hit, the company refused to pay. Instead, it responded with openness and resilience – though the attack still caused an estimated $70 million in losses and halted production across multiple sites.

Dragonfly and Dragonfly 2.0 (2014–2017)

Silent Intrusion, Serious Implications

These long-running campaigns, believed to be backed by nation-state actors, infiltrated the networks of energy companies across the U.S. and Europe. Their goal wasn't immediate disruption, but surveillance and access to industrial control systems – laying the groundwork for potential future sabotage.

Bottom Line:

Cyberattacks in oil and gas aren't theoretical – they're happening, and the consequences are real. From ransomware crippling supply chains to malware that wipes out entire networks, the industry's digital exposure has physical consequences. Investing in cybersecurity isn't optional; it's critical to keeping operations running, protecting national interests, and ensuring safety at every level.

The Evolution of the Digital Ecosystem in Oil and Gas Industry

The oil and gas industry is increasingly digitalized, integrating various technologies to enhance operational efficiency. The sector spans upstream (exploration and production), midstream (transportation and storage), and downstream (refining and distribution) – each adopting advanced digital tools to optimize production.

Technologies such as CNC machinery, inspection robots, and digital twins enable predictive analytics and improved asset management. At the same time, increased connectivity through protocols like OPC UA, Low Earth Orbit (LEO) satellite terminals, and small office/home office (SOHO) network devices support real-time data exchange across remote and distributed environments. However, these digital transformations raise concerns about cybersecurity vulnerabilities.

Here are some of the more commonly exploited technologies:

Vulnerabilities in LEO Terminal Communications

LEO technology is used for communications in remote areas and is vital for remote operations in the oil and gas sector, but it presents significant security vulnerabilities. These vulnerabilities can be exploited by attackers to gain unauthorized access to control networks.

Vulnerabilities include hardcoded credentials, insecure protocols, and undocumented features in various LEO terminal brands. Attackers can intercept signals and tamper with data, leading to potential control network exploitation. The Hughes BGAN M2M terminals are particularly vulnerable, allowing unauthorized command execution if compromised.

Security Challenges in OPC UA Protocol

Employing a trust list mechanism for client authentication, OPC UA is a widely used protocol for integrating IT and OT environments, but it has notable security flaws that can be exploited by attackers. The need for internet connectivity certificate management conflicts with traditional OT network isolation principles.

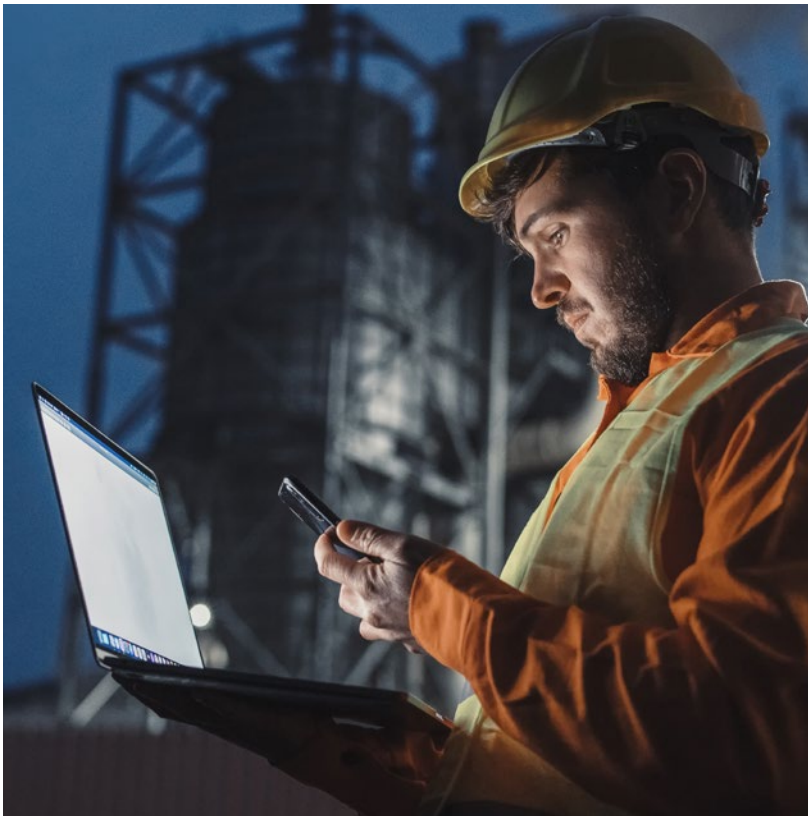
These vulnerabilities can lead to unauthorized access and data manipulation. Issues include missing support for trust lists, trust lists disabled by default, and insecure trust list configurations. Attackers can exploit these flaws to gain access to field device data, posing significant risks to operational safety.

SOHO Device Risks in Critical Infrastructure

SOHO devices are playing an increasingly critical role in network infrastructure – and cybercriminals have taken notice. Because these devices often lack strong security protections, they've become a prime target for attackers looking for easy entry points.

High-profile threats like the Mirai botnet and VPNFilter malware have shown just how easily attackers can exploit SOHO vulnerabilities. More recently, the Volt Typhoon group has used compromised SOHO devices as a stepping stone to access sensitive critical infrastructure environments.

Security competitions like Pwn2Own continue to expose vulnerabilities in today's SOHO equipment, making it clear that stronger safeguards and better hardening are urgently needed.



Intrusion Tactics, Techniques, and Procedures (TTPs)

As the oil and gas sector becomes more digitally interconnected, cyber adversaries are employing a broad range of TTPs to infiltrate and disrupt operational environments. In this section we'll highlight the various ways attackers are able to breach OT environments. In many cases, initial access is achieved through third-party vendors or misconfigured field equipment, underscoring the need for layered defenses, strong access control, and continuous monitoring across all ICS and OT assets.

Common Attack Vectors

- **Phishing & Spear Phishing:** Emails targeting employees with malicious links or attachments
- **Compromised Remote Access (VPN):** Weak or misconfigured remote access with no MFA
- **Supply Chain Infiltration:** Malware or backdoors introduced via third-party software or hardware
- **USB & Removable Media:** Infected devices physically inserted into air-gapped OT networks
- **Legacy System Vulnerabilities**: Unpatched Window XP/2000 systems still used in refineries or control rooms
- **Network Bridging (IT/OT Convergence):** Lateral movement from IT to OT environments via poorly segmented networks

Vulnerabilities in Industrial Control Systems

Historical incidents highlight the significant vulnerabilities in Industrial Control Systems (ICS), particularly in legacy assets. Attackers can exploit these weaknesses to escalate their attacks, often using ransomware that targets known vulnerabilities.

- Attackers breach control networks to exploit service vulnerabilities
- Ransomware like Bad Rabbit and WannaCry primarily spread through SMB service vulnerabilities
- Legacy oil and gas facilities are particularly at risk due to outdated systems

The oil and gas sector is a high-value target due to its economic importance, reliance on aging OT systems, and inter-connected global supply chains.

Ransomware Attack Techniques and Impact

Ransomware attacks, such as those from Bad Rabbit, utilize various techniques to infiltrate and disrupt operations. These attacks can lead to significant losses in productivity and revenue for affected organizations.

- Bad Rabbit spreads through drive-by attacks and exploits SMB vulnerabilities.
- Infected organizations, particularly in transportation, have reported encrypted computers and operational disruptions
- The impact of ransomware can result in severe financial losses and operational downtime

Vulnerabilities in Programmable Assets

Programmable assets in digital Operational Technology (OT) environments are attractive targets for cybercriminals due to their ability to affect physical operations. Successful breaches can have direct and dangerous repercussions on OT operations.

- PLCs and CNC machines are vulnerable to exploitation through service vulnerabilities
- Industrial robots can be compromised, leading to manufacturing defects and safety risks for operators
- Legacy systems in oil and gas installations remain susceptible to modern attack techniques

Exploiting Modern Windows Systems

Recent research demonstrates that even updated systems, like Windows Server 2022, can be exploited through vulnerabilities such as MS-RPC. This highlights the ongoing risks associated with digital infrastructure in critical industries.

- A successful exploit against Windows Server 2022 was demonstrated using an MS-RPC vulnerability
- The attack mimics techniques used in the Stuxnet incident, showcasing the potential for serious breaches
- Continuous updates and security measures are essential to protect modern systems

Initial Access Techniques in ICS

Initial access techniques are critical for attackers seeking entry into ICS environments, targeting both operational technology assets and IT resources. Various third-party entities can serve as potential entry points for these attacks.

- Attackers exploit vulnerabilities in LEO terminals, OPC servers, and SOHO equipment
- Privileged third parties, such as suppliers and maintenance crews, are often targeted
- Effective network segmentation and security measures are necessary to mitigate risks

Cybersecurity Response Roadmap

Now that you are aware of the ways in which cyber criminals can get into your OT network and environment, below are step-by-step strategies and recommended actions to respond to and defend against potential TTPs.

1. Phishing & Spear Phishing

TTPs: Social engineering, credential theft, malware delivery

Initial Access Vector

Steps	Actions
Identify	Conduct risk assessments for personnel roles (NIST ID.RA)
Protect	> Enforce security awareness training (E187-6.3) > Implement advanced email filtering and sandboxing > Enforce MFA for email and VPN access (62443-3-3 SR 1.2)
Detect	Monitor for anomalous email behavior and phishing indicators (NIST DE.CM)
Respond	Isolate impacted endpoints and analyze payloads; notify stakeholders
Recover	Restore from clean backups; adjust training and filters based on IOC findings
TXOne Response	**StellarOne** • Host-based protection for engineering workstations and jump servers • Prevents payload execution, detects suspicious activity **Portable Inspector** • Scans email attachments saved to USB or portable storage before transferring to OT assets

2. Compromised Remote Access (VPN)

TTPs: Credential stuffing, brute-force, MFA bypass

Initial Access Vector

Steps	Actions
Identify	Inventory and review all remote access paths (62443-2-1 SMR 7)
Protect	> Enforce MFA across all remote access > Use jump servers and hardened bastions > Decommission unused VPN accounts
Detect	Log and alert on abnormal login patterns, geo-location mismatches
Respond	Disable compromised accounts, revoke credentials, perform root-cause analysis
Recover	Re-establish secure VPN access; update remote access policy
TXOne Response	**EdgeFire** • Industrial next-gen firewall to segment remote access from OT zones • Controls protocols, enforces zero trust across zones **StellarOne** • Hardens VPN endpoints and HMIs with host-based AV/EDR • Protects against credential dumping and privilege escalation

3. Supply Chain Infiltration

TTPs: Software backdoors, malicious firmware, third-party compromise

Initial / Secondary Access Vector

Steps	Actions
Identify	Classify suppliers by criticality and access level (62443-2-1 SMR 4)
Protect	> Implement secure procurement policies > Conduct SBOM analysis for software > Segment third-party access (62443-3-3 SR 1.1)
Detect	Monitor third-party traffic for anomalies and new executable drops
Respond	Quarantine infected devices/software, notify vendors
Recover	Replace compromised assets; reassess vendor risk management controls
TXOne Response	**EdgeIPS** • Virtual patching for unpatchable or legacy devices from third-party vendors **Portable Inspector** • Ensures vendor USBs or laptops are malware-free before connecting to OT **StellarOne** • Detects execution of unauthorized binaries from vendor-provided software

4. USB & Removable Media

TTPs: Sneakernet malware introduction, autorun scripts

Initial Access Vector

Steps	Actions
Identify	Catalog all removable media and authorized user
Protect	> Implement TXOne Portable Inspector or equivalent for USB scanning > Enforce GPO/device control policies (62443-3-3 SR 1.13)
Detect	Alert on unauthorized USB use or unexpected autorun activity
Respond	Isolate infected endpoints and conduct forensic analysis
Recover	Remove malicious code, reinforce media control policy
TXOne Response	**Portable Inspector** • Primary defense: Scans all removable media offline before allowing file transfer • Enforces allowlist policies **StellarOne** • Prevents malware execution if an infected file is opened • Device control can block USB use altogether on OT hosts

5. Legacy System Vulnerabilities

TTPs: Exploiting outdated OS, no patching, default creds

Persistence / Lateral Movement Vector

Steps	Actions
Identify	Inventory and risk-rank legacy systems
Protect	> Deploy virtual patching with TXOne EdgeIPS/EdgeFire > Remove unnecessary services, enforce ACLs (62443-3-3 SR 3.1)
Detect	Monitor SMB, RPC, RDP traffic for exploits like EternalBlue
Respond	Segregate compromised legacy devices, disable exposed services
Recover	Restore from clean image; develop phased obsolescence roadmap
TXOne Response	**EdgeIPS** • Provides virtual patching to block exploit signatures without modifying the system **EdgeFire** • Enforces strict segmentation to isolate vulnerable devices **StellarOne** ***(on legacy Windows 7/XP/2000)*** • Lightweight endpoint protection for legacy OS

6. Network Bridging (IT/OT Convergence)

TTPs: Lateral movement, credential reuse, pivoting

Tactical Movement Vector

Steps	Actions
Identify	Map out data flows and convergence points (Purdue Model)
Protect	> Implement TXOne EdgeFire firewalls at IT/OT boundaries > Apply least privilege and role-based access control (62443-3-3 SR 1.5)
Detect	Alert on abnormal inter-zone communication
Respond	Block east-west traffic; investigate pivoted credentials
Recover	Rebuild affected zones and revalidate access controls
TXOne Response	**EdgeFire** • Sits at IT/OT boundary; enforces network zoning based on Purdue model • Deep packet inspection for OT protocols **EdgeIPS** • Provides protocol filtering and traffic inspection between zones **StellarOne** • Hardens jump servers or dual-homed engineering stations

7. Exploits in Industrial Control Systems (ICS)

TTPs: Drive-by exploits, SMB worms, malware propagation

Execution / Impact Vector

Steps	Actions
Identify	Assess ICS firmware and protocol vulnerability exposure
Protect	> Apply whitelisting and secure boot where possible > Use host-based protection like StellarOne
Detect	Behavior-based threat detection on PLCs and SCADA systems
Respond	Disconnect and contain infected ICS nodes
Recover	Flash clean firmware; test control integrity before restart
TXOne Response	**EdgeIPS** • Blocks SMB/RPC exploits (e.g., EternalBlue) via DPI and signature-based IPS • No system patching needed **StellarOne** • Detects and prevents ransomware behavior on OT endpoints **Portable Inspectore** • Ensures malware doesn't enter via USB

8. Programmable Assets (PLCs, CNCs, Robots)

TTPs: Manipulation of logic, firmware tampering

Impact Vector

Steps	Actions
Identify	Inventory programmable assets; define protection levels (62443-2-1 SMR 5)
Protect	> Lock down logic uploads/downloads > Use tamper detection and logging (62443-3-3 SR 6.2)
Detect	Alert on unexpected programming or firmware updates
Respond	Roll back firmware or logic, isolate asset from network
Recover	Restore validated logic from secured backup
TXOne Response	**EdgeIPS** • Monitors communications to/from PLCs, SCADA devices • Blocks abnormal commands or unauthorized write attempts **EdgeFire** • Restricts access to only trusted HMIs or engineering workstations **StellarOne** • Protects programming stations that interface with programmable assets

9. Modern Windows Exploits (e.g., MS-RPC)

TTPs: Lateral movement, remote code execution

Execution / Lateral Movement Vector

Steps	Actions
Identify	Maintain up-to-date asset management with vulnerability scanner integrations
Protect	> Patch MS-RPC and other common services > Use host firewall rules to block unnecessary ports
Detect	Monitor RPC traffic for signs of exploit chains (e.g., CVE-2022-26809)
Respond	Contain affected systems, update IOCs and detection rules
Recover	Rebuild from baseline image; reapply hardened configurations
TXOne Response	**EdgeIPS** • Blocks exploit attempts via protocol inspection (MS-RPC, SMB) **StellarOne** • Protects against modern ransomware, privilege escalation, and process injection • Supports Windows Server 2022 and modern OS hardening

10. Third-Party Initial Access (LEO, OPC, SOHO Devices)

TTPs: Exploiting trusted remote access paths

Initial Access Vector

Steps	Actions
Identify	Identify all vendor and third-party access routes
Protect	> Enforce MFA and session monitoring > Require zero trust network segmentation
Detect	Watch for unusual commands or sessions from third-party devices
Respond	Terminate suspicious connections; investigate third-party logs
Recover	Re-establish secure access with tighter controls
TXOne Response	**EdgeFire** • Controls third-party vendor network access through strict allowlisting **Portable Inspector** • Mandatory scanning for contractor laptops and drives before OT access **StellarOne** • Used to enforce application control and restrict behavior on third-party engineer devices

TXOne Networks offers cybersecurity solutions for ICS and OT environments, employing the OT zero trust methodology for Cyber-Physical Systems (CPS). We foster collaborations with leading manufacturers and infrastructure operators to devise effective defense strategies, addressing security vulnerabilities in industrial settings.

Contact TXOne Networks today to begin your OT journey with confidence.

txOne networks

txone.com

TXOne Networks | Keep the Operation Running

Contact Us