YOUR LOGO HERE

MSP-Demo THREATDEFEND FOR ENERGY, OIL & GAS

PROTECTING CRITICAL INFRASTRUCTURE. SECURING OT AND IT ENVIRONMENTS. ENABLING OPERATIONAL RESILIENCE.

Top Cybersecurity Threats Facing Energy, Oil & Gas Companies

1. Ransomware attacks on operational technology (OT) environments
2. Nation-state actors targeting critical infrastructure
3. Supply chain compromises and third-party vulnerabilities
4. Credential theft and lateral movement within segmented networks
5. Non-compliance with regulatory standards (e.g., NERC CIP, NIST, CMMC)

Pain Points

Energy Sector

- Converged IT/OT networks with outdated security controls
- Large, distributed environments with limited centralized visibility
- High risk of operational disruption and safety incidents
- Regulatory pressure to prove cyber readiness and resilience

RELEVANT THREATDEFEND MODULES

Falcon Identity Protection
Secure user access across hybrid IT/OT networks

Falcon Discover
Monitor devices, access points, and network activity in real time

Falcon Exposure Management
Prioritize remediation of high-risk vulnerabilities

Falcon LogScale (Next-Gen SIEM)
Enable scalable detection across segmented systems

24/7 SOC Monitoring
Ensure continuous visibility and response for critical operations

Why It Matters

Energy and critical infrastructure organizations are high-profile targets for ransomware, espionage, and disruption. MSP-Demo ThreatDefend helps oil, gas, and energy companies strengthen their cyber defenses, maintain uptime, and meet compliance standards.

Take Action

Book a Critical Infrastructure Cybersecurity Consultation with MSP-Demo to evaluate your operational risk and implement a proactive security strategy tailored to your IT and OT environment.

View Website pedro.fialho@vijilan.com +1 (954) 334-9988