vijilan
IT Security: Enabled

THREATDEFEND FOR UTILITIES & WATER

Protecting operational uptime and compliance in OT-heavy environments

Relevant ThreatDefend Modules

Falcon EDR/XDR
Real-time identification of security threats

Falcon Identity
Advanced correlation using threat data feeds

Falcon Discover
Identification of potential risks in IT enviornments

Falcon Exposure
Step-by-step response recommendations

Cribl Stream
Log routing from Google, Microsoft, and firewall systems

Corelight + Zeek
Inspect traffic in segmented utility environments

Top Cybersecurity Threats Facing Utilities & Water

1. **Ransomware or Sabotage**
   Targeting SCADA, causing outages in public services
2. **Lateral Movement**
   Bridging OT and IT networks for broader compromise
3. **Compliance Failures**
   Penalties from unmet federal/state security mandates

Take Action

Protecting critical infrastructure means detecting threats before they disrupt operations, affect safety, or trigger fines.

Why It Matters

Downtime in utilities doesn't just lose money, it risks public safety and trust. OT cybersecurity is now a non-negotiable priority.