FORESCOUT
Active Defense for the Enterprise of Things.

Oil & Gas

Managing cyberthreats and operational issues in Oil & Gas OT networks

Due to recent cyberattacks like the Triton malware that disabled safety controllers at a plant in the Middle East[1] and the ransomware attack that briefly shut down a natural gas pipeline in the U.S.,[2] cybersecurity is top of mind for oil & gas producers the world over.

Among the many challenges associated with protecting oil & gas OT infrastructure, three of the most difficult are:

- Achieving real-time network visibility
- Managing cyberthreats effectively
- Detecting networking and operational issues before they cause downtime

Implementing the right industrial control system (ICS) network monitoring solution can help oil & gas producers achieve all three of these goals.

Last year, cybersecurity was the #1 digital investment focus for oil & gas organizations, with 61% indicating they were actively investing in security technologies to detect and prevent threats.[3]

The Cyber Resilience Platform for Oil & Gas Operators: eyeInspect

Forescout eyeInspect (formerly SilentDefense™) offers passive asset discovery capabilities for complete visibility into sensitive industrial networks. eyeInspect also protects ICS networks from a wide range of threats with patented deep packet inspection (DPI) and anomaly detection technology combined with a library of over 3,500 IoCs for advanced cyberattacks, network misconfigurations and operational errors. Our protocol coverage is the most extensive on the market, with over 130 protocols supported, and counting.

By continuously monitoring and analyzing network communications and comparing them with a baseline of legitimate operations and with the "known bad" characteristics defined in a collection of checks, eyeInspect spots cyber and operational risks in real time. These baselining capabilities extend down to the asset level, so if an asset deviates from its baseline, operators are alerted in real time.

eyeInspect Use Cases for Oil & Gas ICS Networks

Get real-time network visibility

eyeInspect provides a continuously updated asset inventory for the entire ICS network. It automatically builds a detailed network map with extensive device details, baselines for each asset, and automatically groups by network and/or role. Grouping is provided in multiple formats, including Purdue level and communication relationship. Users can also proactively identify vulnerable OT devices and protocols to prioritize mitigation strategies with the Asset Risk Framework, the first centrally available, "impact-based" risk tool for OT networks. Discoverable details include:

- Network address
- Host name
- Vendor and model
- Serial number
- OS version
- Firmware version
- Hardware version
- Device modules' information

Manage cyberthreats

By continuously monitoring network communications, eyeInspect detects and alerts for cyberthreats in real time. A security risk score empowers security analysts to immediately identify assets with a high probability of being attacked.

eyeInspect uses a wide range of monitoring capabilities that include:

- Patented deep packet inspection (DPI) of 130+ protocols
- Continuous, configurable policy and behavior monitoring

SIMPLIFY NIST CYBERSECURITY FRAMEWORK COMPLIANCE

According to SANS, the NIST CSF is the number-one framework in use today.[4] Oil & gas producers can use Forescout's OT solution to increase their maturity levels within each Function of the NIST CSF:

1. **Identify** - Provides full visibility into your digital and physical assets, their interconnections and defined roles and responsibilities while helping you understand their current risks and exposure.
2. **Protect** - Deploys security controls to limit what is allowed on the OT network in real time, while also responding to failed policy conditions with automated network segmentation policy enforcement.
3. **Detect** - Continuously monitors OT infrastructure and alerts in real time to help catch early symptoms of emerging cyber and operational threats.
4. **Respond** - Facilitates root cause analysis with rich contextual alert information, such as source and target details and a PCAP of the suspicious event, as well as rapid response with bi-directional integration with third-party security tools.
5. **Recover** - Creates asset baselines and profiles for each device and provides an audit log of device firmware and software changes to help identify potential rollback points.

- Automatic assessment of device vulnerabilities, threat exposure, networking issues and operational problems
- Vulnerability and communication analysis

Detect networking and operational issues

Occasional networking and operational issues are inevitable, but they needn't result in significant system downtime. An operational risk score enables OT engineers to quickly spot assets that need immediate attention, including devices exhibiting signs of misconfiguration or malfunction that could cause unexpected downtime.

In addition, eyeInspect's comprehensive Industrial Threat Library (ITL) automated detection engines and network baselining capabilities allow operators to detect and respond to a wide range of networking and operational issues, including:

- Use of insecure protocols
- Routing/gateway issues
- Data sent in noncompliant formats
- Connectivity issues with field devices
- Failure of critical devices
- Unstable process values
- Incorrect process measurements
- Switch and device misconfigurations

MULTIFACTOR THREAT DETECTION

eyeInspect is the first OT network monitoring solution that puts together all these factors and individual data points to assign a single security and operational risk score for each network asset. These risk scores provide a consistent method for finding and prioritizing remediation actions for assets. eyeInspect can identify and help remediate a full range of both cyber and operational threats, including:

- Cyberattacks (DDoS, MITM & scanning, etc.)
- Unauthorized network connections, communications
- Suspicious user behavior / policy changes
- Device malfunction or misconfiguration
- New and non-responsive assets
- Malformed protocol messages used in exploits
- Unauthorized firmware downloads
- Usage of unsecure protocols
- Default credentials and unsecure authentications
- Logic changes

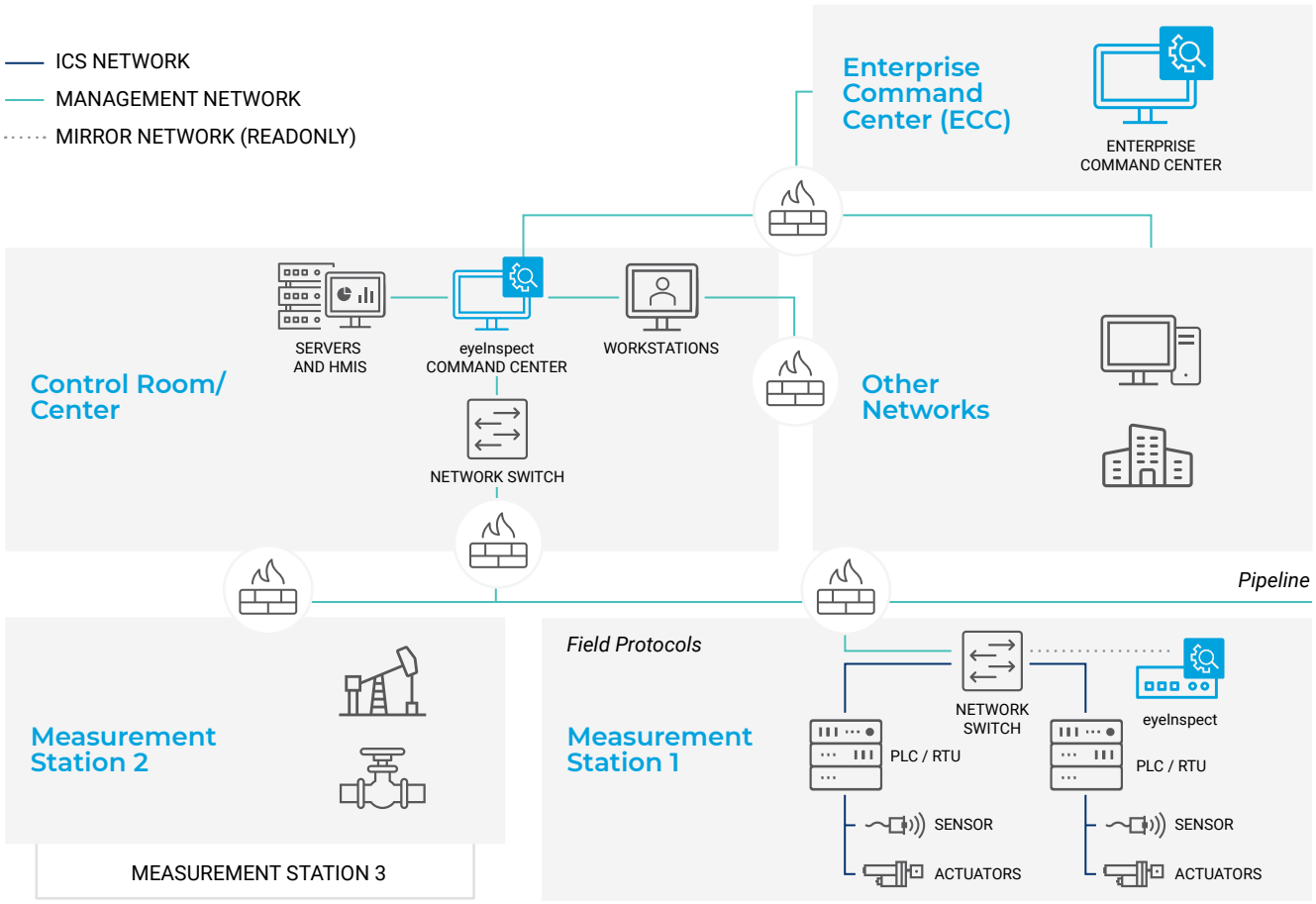

Figure 1: eyeInspect is part of Forescout's unified IT-OT security platform that provides situational awareness and automated control of both cyber and operational risk across the extended enterprise.

1. https://www.forescout.com/company/blog/ics-malware-conceived-to-disrupt-operations-found-in-the-middle-east/
2. https://www.forescout.com/company/blog/how-to-reduce-risk-of-disruptionware-attacks-for-oil-and-gas-producers/
3. https://www.accenture.com/us-en/insights/energy/trends-digital-investment
4. https://www.forescout.com/platform/operational-technology/2019-SANS-state-of-OT-ICS-cybersecurity-survey/

Don't just see it. Secure it.

Contact us today to actively defend your Enterprise of Things.

forescout.com/platform/eyeInspect salesdev@forescout.com toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com