CYBERPRISM

Digital Use Case - ProcessGuard™ Protecting your Historian Data Flow

Sector	North Sea Oil and Gas Platform
Client Need	Ensure the safe, secure and continuous operation of offshore platforms. Guard the Integrity and Confidentiality of the Historian data flow between the onshore site and offshore sites. Protect data repositories from ingress of malware and data exfiltration from known threat actors targeting Oil & Gas platforms. The solution must adhere to IEC 62443 and HSE OG86.
Solution	ProcessGuard will protect the entire Historian network and data flow process. It will prevent the ingress of malware from connected IT networks and will alert the IACS Responsible Person of any suspicious activity by internal or third-party users. With ProcessGuard your sensitive data will be protected from exfiltration or unauthorised viewing, whilst continuing to provide access to authorised users with the correct permission set.

OIL & GAS DIGITAL TRANSFORMATION AGAINST MODERN-DAY CYBER ATTACKS

The rising tide of cyber-attacks targeting the energy sector has reached new heights. According to an independent survey on the Global State of Industrial Cyber Security in 2021, a staggering 80% of respondents experienced an attack, with 47% reporting an impact to their Industrial Control System (ICS) environment. Whilst the threat has increased, so too has the consequence of an attack. Remote cyber-attacks against offshore platforms could result in severe consequences to human and environmental safety (ruptures, fires, spills), including lost production due to downtime and equipment damage.

CUSTOMER REQUIREMENT

Guard the Integrity and Confidentiality of Historian data flow between onshore and offshore sites from cyber threats such as:

- Ingress of malware from external sources through: email phishing, watering hole attacks, malicious files and removable media.
- Data exfiltration from internal or external third-party users.
- Compromise of safety critical operational data.

Maintain high quality data integrity that is readily accessible to authorised users.

Monitor and Alert suspicious behaviour to the ICT or Ops Support Manager.

CYBERPRISM SOLUTION

CyberPrism developed ProcessGuard to protect IT and OT networks critical for safe and secure operations. The proposed solution would see ProcessGuard installed in front of the Historian Server and the Connectors on each offshore platform. Once in place, ProcessGuard will safeguard the entire Historian data process by:

- Preventing attackers from moving laterally from connected networks through effective segregation.
- Blocking any attempt to exfiltrate data by external actors or unauthorised internal/third party users.
- Detect and alert any suspicious activity.
- Ensuring sensitive data is accessible to authorised users only.

RESULTS

- High-Grade Segregation:

ProcessGuard offers unified protection that goes beyond the functionality of other firewalls. This includes smart segregation, access control, network detection and alert services.

ProcessGuard will isolate the Historian from connected IT whilst allowing the data flow to continue operating safely.

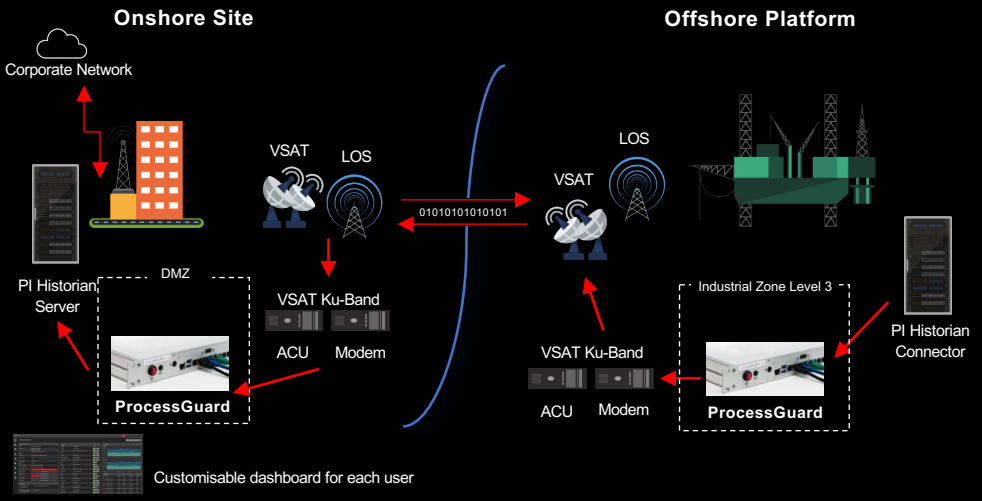
- Improved Visibility and Alerting:

ProcessGuard will detect and alert suspicious activity to the IACS responsible person.

- 100% Compliance:

ProcessGuard will help you achieve network segregation in line with standards such as IEC 62443 and HSE OG86 guidance.

Deployment



CyberPrism would provide a complete "turnkey" cyber security solution to protect the entire Historian network. Firstly, we would conduct a Cyber Risk Assessment in close liaison with the Group ICT Manager to understand the ICSS/Telecoms Network Architecture and associated vulnerabilities around the Historian network.

In a typical scenario, CyberPrism would install ProcessGuard at the onshore telecoms site. The Guard would sit in front of the PI Historian Server in the Demilitarised Zone (DMZ) facing the corporate's external network. In addition, Guard would also be installed at each offshore platform in front of the PI Connector. CyberPrism would configure the Guard to protect against known cyber threats targeting O&G companies. An alert system would be enabled to send real-time notifications of any suspicious activity to the nominated IACS responsible person for further investigation.

FEATURES

- ✓ Next Generation UTM/Firewall
- ✓ Application network management
- ✓ Traffic shaping
- ✓ Web and content filtering
- ✓ Network access control
- ✓ Remote access control
- ✓ Fully customisable dashboards
- ✓ Works with all manufacturers' equipment
- ✓ Client-specific configurations - modular
- ✓ 'Lightweight' solutions for isolated/offshore use

BENEFITS

- ✓ Safe, continuous segregation and monitoring of the entire Historian network
- ✓ Allows safe interaction with third-party users
- ✓ Will send an alert if it detects any suspicious activity
- ✓ Comes with our services, delivered directly by our experts – Security as a Service
- ✓ Multifunctional device saves money on other solutions

TAKE CONTROL OF YOUR OPERATIONAL TECHNOLOGY