MODERN CYBERSECURITY FOR THE OIL & GAS INDUSTRY

SECURING INDUSTRIAL CONTROL SYSTEMS (ICS)

Digitalisation and the interconnectivity of operational technology (OT) drastically increases cyber security risk in the oil and gas industry. The security challenges, requirements and potential consequences in industrial environments significantly differ from those in a traditional office IT environment. While the impact of a security breach in office environments is often limited to financial loss, attacks on industrial systems have the potential to stop production, cause physical damage, harm the environment and even put people's lives at risk.

Addressing the security requirements of industrial environments requires a holistic and integrated approach to identify, assess and manage cyber risk in these unique and mission critical environments.

A COMPLETE MANAGED SECURITY SOLUTION FOR THE OIL & GAS INDUSTRY

Argus for Industrial Control Systems is a complete and fully managed security solution to secure industrial environments and specifically designed to address the unique security challenges in the oil and gas industry – onshore and offshore.

At the heart of the solution is the Argus ICS Defender - purpose-built for protecting ICS and SCADA environments from modern threats. Combining advanced threat detection with in-depth knowledge about industrial environments, the Argus ICS Defender detects attacks against production systems, uncovers protocol anomalies, and discovers unexpected traffic and misconfigurations.
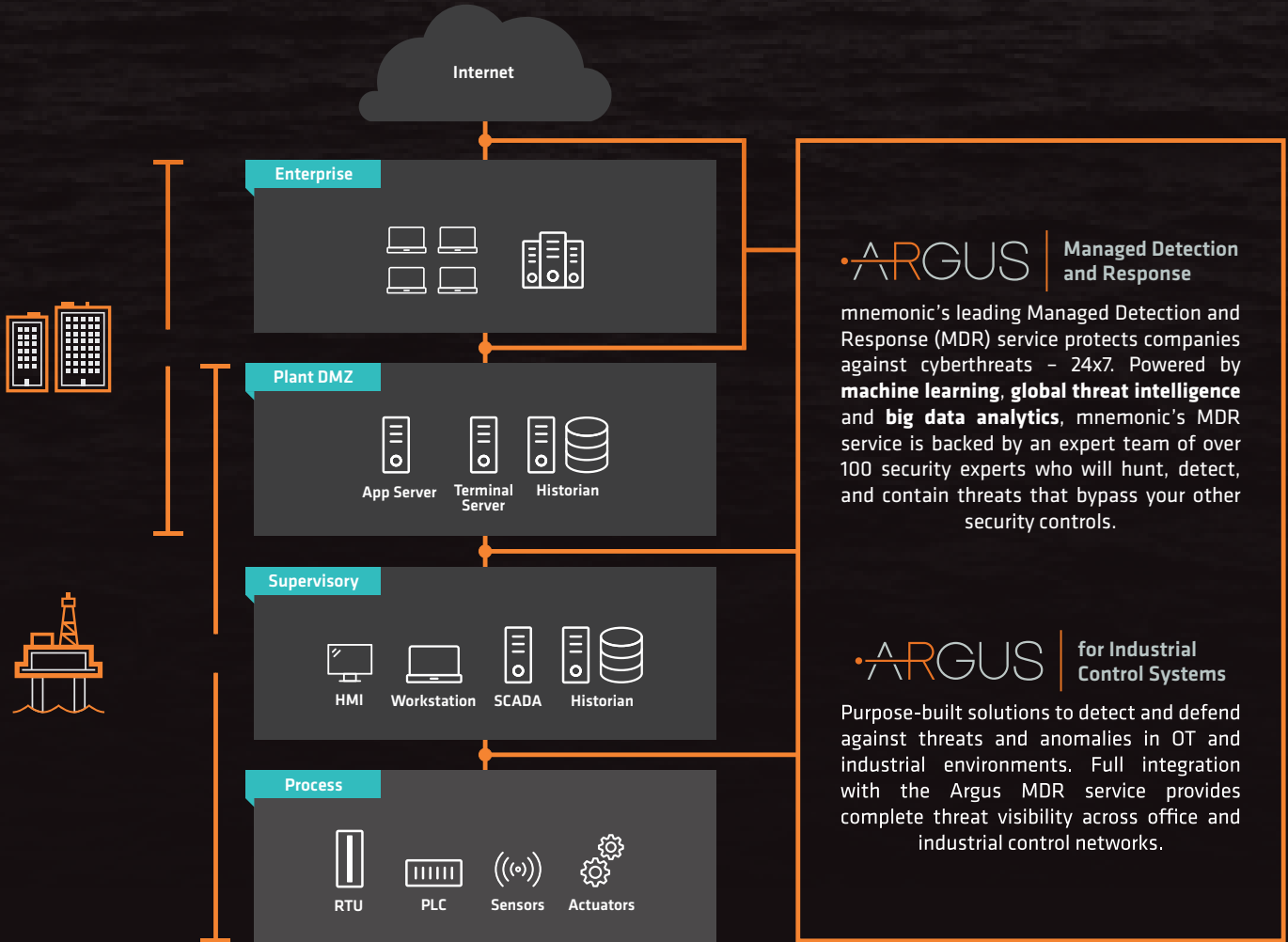
Supported 24x7 by mnemonic's Security Operations Center, the Argus ICS Defender protects your mission critical systems against modern threats and ensures safe and reliable operations.

Argus for Industrial Control Systems is augmented with complementary service modules designed to support your unique security requirements in both new and legacy production facilities. From hybrid management to a fully managed service, mnemonic combines a remote service delivery with custom grades of on-premise involvement to adapt to each company's policies, regulations and capabilities.

Available service components include:

- Argus Managed Detection and Response (MDR)
- SOC & CERT service
- Argus ICS Defender
- Log Management
- Patch Management
- Change Management
- Asset Management
- Health Monitoring
- Security sensors
- Device Management
- Vulnerability Management
- Authentication Management

ADVANCED THREAT DEFENCE FOR INDUSTRIAL CONTROL SYSTEMS

Internet

Enterprise

Plant DMZ

App Server

Terminal Server

Historian

Supervisory

HMI

Workstation

SCADA

Historian

Process

RTU

PLC

Sensors

Actuators

·ARGUS | Managed Detection and Response

mnemonic's leading Managed Detection and Response (MDR) service protects companies against cyberthreats – 24x7. Powered by **machine learning**, **global threat intelligence** and **big data analytics**, mnemonic's MDR service is backed by an expert team of over 100 security experts who will hunt, detect, and contain threats that bypass your other security controls.

·ARGUS | for Industrial Control Systems

Purpose-built solutions to detect and defend against threats and anomalies in OT and industrial environments. Full integration with the Argus MDR service provides complete threat visibility across office and industrial control networks.

Enable the secure digitalisation of operational technology with mnemonic's purpose-built, holistic and non-intrusive managed security solution