

# Solution spotlight

## Industrial control systems



In the past, industrial control systems (ICSes) were often isolated from external networks (including the internet) and physically protected. As digital transforms businesses, these internal networks are being moved online – exposing them to malicious actors. Our ICS services – including the development of cyber security frameworks, gap and risk assessments, penetration testing, security services and incident response strategies – help prevent data being destroyed, production being delayed or – in a worst case scenario - lives being put at risk.

### Prepare



- Architecture design and assessments
- Governance and strategy
- Maturity assessments
- Site security assessments
- Gap assessments

### Protect



- Compliance with ICS standards
- Control design and implementation
- System configuration management
- Solution implementation

### Detect



- Security monitoring and intrusion detection
- Penetration testing and attack simulations
- Vulnerability and configuration assessments

### Respond



- Incident and breach response
- Threat hunting
- Breach assessments
- Contingency planning
- Disaster recovery

### Our ICS services

#### Cyber security frameworks

Use of machines, systems and appropriate networks and assessment of operational requirements

#### Risk assessments

Analysis of media used and entity's hosts, networks and applications

#### Gap assessments

Identification of gaps in security systems and processes

#### Penetration testing

Network tests - using scanning tools and open FTP portals - to detect vulnerabilities

#### Security services

Tools and custom scripts to identify process exploitations

#### Incident response

Findings, risk ratings and recommendations



Srikant Ranganathan  
Senior Director  
T +973 1720 6827  
[srikant.ranganathan@keypoint.com](mailto:srikant.ranganathan@keypoint.com)



Sagar Rao  
Manager  
T +973 1720 6802  
[sagar.rao@keypoint.com](mailto:sagar.rao@keypoint.com)