OT-Secure – Service Definition

Service overview

OT-Secure provides a cloud-based OT (Operational Technology) Security Maturity Assessment platform designed to help organisations assess, prioritise and improve the cybersecurity posture of industrial and critical infrastructure environments. The service supports risk-based decision-making aligned to recognised standards including IEC 62443, NIST and relevant UK and EU regulatory requirements.

The service is delivered as a SaaS platform, supported by optional expert services for onboarding, interpretation of results and improvement planning.

Service description

The OT-Secure platform enables organisations to:

- Perform structured OT security maturity assessments
- Identify gaps against best practice and regulatory expectations
- Prioritise remediation actions
- Track improvements over time
- Generate management-ready reports

The service is suitable for organisations operating industrial control systems, critical infrastructure, transport, energy, utilities and manufacturing environments.

Onboarding and implementation

Onboarding includes:

- Account setup and tenant configuration
- User provisioning
- Initial configuration and scope definition
- Optional assisted onboarding session

Typical onboarding can be completed within days, subject to customer readiness and scope.

Service management

The service is managed by OT-Secure and hosted in ISO 27001 certified Dutch datacentres via approved hosting providers. The platform is monitored and maintained to ensure availability, security and performance.

Support

Support is provided during business hours via designated support channels. Incidents and service requests are logged, prioritised and tracked. Response and resolution times are based on incident severity.

Security

The service includes:

- Multi-Factor Authentication (MFA)
- Role-based access control (RBAC)
- Encryption of data in transit and at rest
- Vulnerability management and patching
- Centralised logging and monitoring

Data hosting and sovereignty

Customer data is hosted in European (Netherlands) datacentres. Data is logically segregated per tenant. OT-Secure does not transfer customer data outside the EEA unless contractually agreed.

Compliance and standards

The service aligns with recognised best practices including:

- ISO 27001 aligned controls
- IEC 62443 principles for OT environments
- Secure software development best practices

Service levels

The platform is designed for high availability. Planned maintenance is communicated in advance. Incident response follows defined incident management procedures.

Exit management

Upon contract termination, customer access is revoked. Customer data can be exported upon request and is securely deleted in line with retention policies.

Dependencies and assumptions

The service depends on internet connectivity and customer-provided information for assessments. The accuracy of outputs depends on the accuracy and completeness of customer input