SECURITY OPERATIONS CENTRE (SOC)

1. CUSTOMER SITE
Logs and network data are continuously collected and automatically transferred from site to office network.

2. CUSTOMER OFFICE
Received data is automatically analysed and anomalies detected. If suspicious behavior is detected, alarm is raised and forwarded to SOC for further investigations.

3. VPN
If SOC suspects that there is a security incident at site they connect over secure VPN to the office for further investigations.

4. SECURITY OPERATIONS CENTRE (SOC)
SOC analyses customer’s site 24/7 using the info received from customer.

5. Wärtsilä Product Security Incident Response Team (PSIRT)
Wärtsilä Product Security Incident Response Team (PSIRT) contacts customer and PSIRT, and starts incident response process.

YOUR BENEFITS
- Minimise losses from cyber security incident
- Increase asset uptime
- Detect and respond to anomalies in a pro-active manner