TERMA SCANTER RADARS CYBERSECURITY

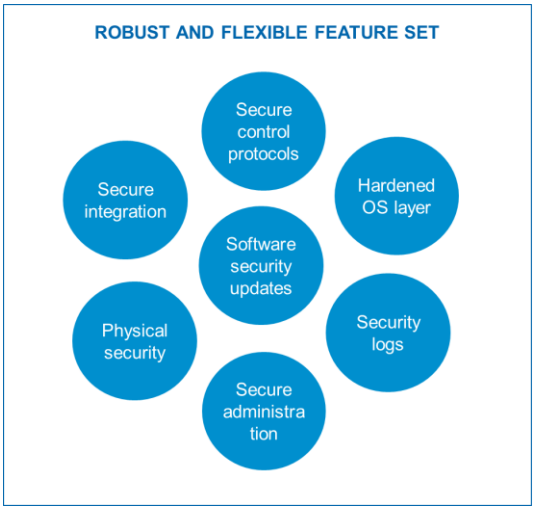
Terma SCANTER radars and cybersecurity
When building the critical surveillance solutions of today and tomorrow, risks posed by ever emerging and evolving cybersecurity threats is cause for growing concern.

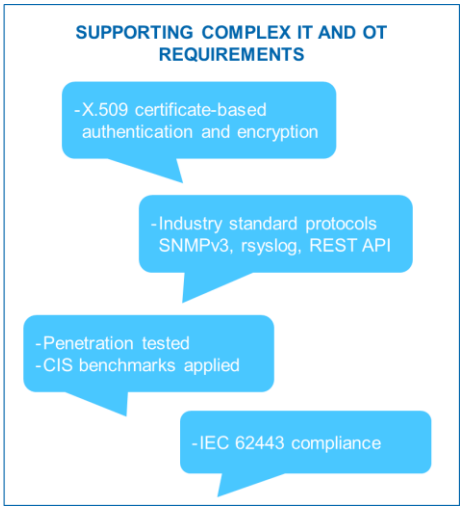
Successful risk mitigation quickly translates into extensive security requirements on each and every element of the solution, be it servers, radar transceivers or other sensors – and the chain only becomes as strong as the weakest link.

For Terma, it is a strategic priority to deliver solutions that support our customers in establishing secure systems - and to us, cyber security forms an integrated part of product development.

Radar solutions supporting your cybersecurity requirements
Terma radar systems include a robust suite of features providing you full flexibility to securely integrate our products in complex IT and OT infrastructures, including:

- *Secure control interfaces* – X.509 certificate-based authentication and encryption of control protocols
- *Security logs* – security related events logged and made available for central monitoring
- *Network interface management* – firewall rules, VLAN setup and interface access are fully configurable
- *Administration interface* – easy and secure management of users, system configuration and updates





Compliant, hardened and verified
SCANTER Radars are designed to comply with the requirements and recommendations of a spectrum of national and international cybersecurity standards and legislation, including industry standard IEC 62443.

Where applicable, software configurations are hardened according to CIS benchmarks. As part of the verification and release process, software baselines are subject to penetrations testing.

Stay up to date
New cybersecurity threats are continuously crafted by ill intending individuals or organizations. Acknowledging the importance of ensuring that your SCANTER radars include up to date protection, Terma offer as complementing suite of software security services including periodic software security updates, critical threat notifications and quarterly incident reports.