TERMA SOFTWARE SECURITY UPDATES

Undivided Cybersecurity Focus
Do we comply? Are we protected? A natural area of concern for owners of critical surveillance infrastructure, for whom data security and operational availability is imperative, is whether their solutions are cybersecure. Hence, with an increasing number of threats aimed at exploiting software vulnerabilities, it is an obvious requirement to software vendors that serious attention is aimed at keeping software resilient to malicious attacks.

To comply to these requirements, Terma offers software security update services designed to keep Terma delivered software continuously security updated to better resist digital intruders while complying with organizational cybersecurity requirements and national legislation.

Be Compliant, Stay Compliant
There is no doubt that focused cybersecurity awareness is a necessity when ensuring uninterrupted system operation and protecting data. Therefore, all new Terma SCANTER products are based on a software platform that is designed to comply with international standards for cybersecurity (IEC 62443).

As new cybersecurity threats appear, today's software security measures are soon rendered deficient. To enable our SCANTER solutions to withstand new threats, Terma systematically monitors our software components for vulnerabilities (CVSS rating "7.0 High" and above). This means that when new vulnerabilities are identified, we can quickly engage in corrective measures and produce software security updates for fast implementation at our customers operational SCANTER sites.

Flexible Implementation at your SCANTER Site
Software security updates are made available for download* from a secure file location facilitated by Terma. All software is accompanied by a documentation package containing release notes, installation guides and verification test specifications. New software security updates are made available annually or at a higher frequency based on severity, depending on agreement.

Customers who do not wish to take on installation and verification testing can get assistance from Terma, who offers to:

- Install the software security update packages at the designated SCANTER sites. Service window is agreed in advance.
- Perform thorough post-installation verification testing according to specification, to ensure that the installation has completed successfully and that the SCANTER radar is fully operational.
- Register the updated software version in our Operations Center records and journal relevant verification test documentation for future reference.

Installation and verification testing is done remotely through a secure remote connectivity solution recommended by Terma or as preferred by customer.

Other available features in the portfolio of software security update services include Critical Threat Notifications, Quarterly Incident Reports and access to Terma Support Hotline.

* Access to the individual customer file location is only available for authenticated customers with a valid software security update subscription.