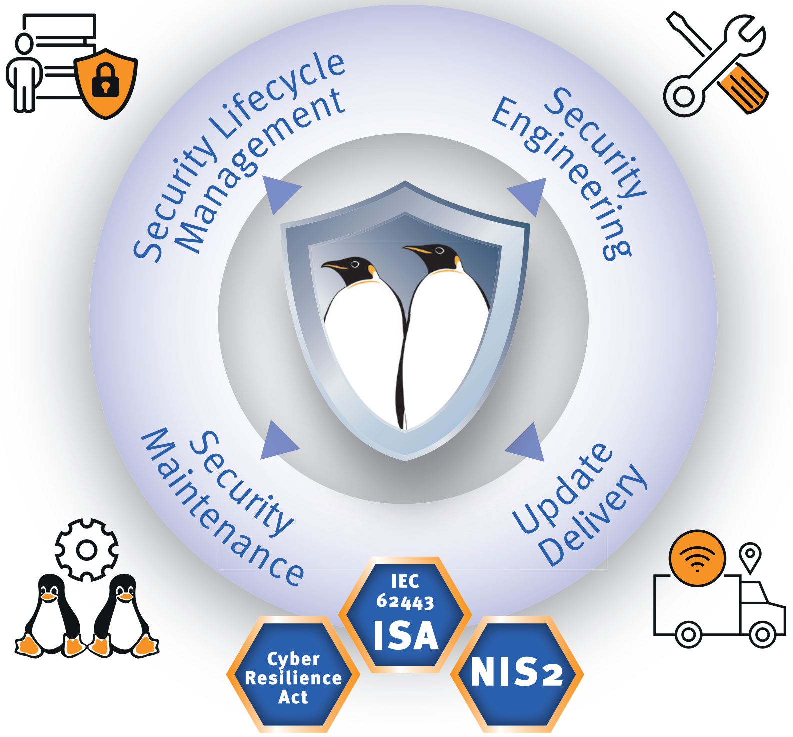
emlix
embedded linux systems

Embedded Linux security

IEC 62443 und EU Cyber Resilience Act (CRA)

Since more than 15 years our customers rely on our embedded Linux security services.

We support the composition and optimization of embedded Linux systems to make them perfectly equipped for secure operation in the context of IEC 62443 and analogously the Cyber resilience Act (CRA) with the Technical Guideline TR-03183 as well as EN18031 in context of RED (Radio Equipment Directive).



emlix service components

The emlix services include:

- threat modeling and risk assessments
- security requirements and architecture workshop
- selection and qualification of open source software
- system hardening and implementation of security features
- security acceptance testing and documentation
- CVE security monitoring and response
- patch and update management
- open source security lifecycle management

Usually, the cooperation with our customers starts with a requirements and architecture workshop and/or a threat modeling and risk assessment to understand the product vision or to get an overview about an existing, probably already rolled-out system.

Depending on the goal we will prepare a security concept (e.g. with a defense in depth strategy) and the corresponding software requirements specification.

An important step is the derived selection and qualification of components in compliance with the relevant security standards but as well with Open Source Compliance as of IEC 5230:2020 (Open Source Compliance / Lizenz-Compliance) and IEC 18974:2023 (OpenChain security assurance specification). As a result the Linux BSP is reduced to the minimum necessary to meet the requirements. This focus leads to a reduction of complexity and increase in quality. Thus, it heavily supports curation of the Linux system. An efficient lifecycle management is the topmost direct benefit for our customers.

Typical mitigations

Further typical mitigations are e.g. the zoning and segmentation of the system (IPTables, NFTables, SELinux, containers with namespaces and cgroups), ensuring integrity (secure boot, dm-verity, LUKS, hashing, signatures), reduction of access rights (SELinux, AppArmor, RBAC, namespaces, privileges management), authentification and authorisation (Public-Key, PAM, RADIUS) or the encryption of communication and data (SSL/TLS, OpenSSL, SSH, TPM, TEE, HSM, HUB, dm-crypt, LUKS, eCryptfs).

Furthermore the logging of security related events (syslog, rsyslog, elos), secure provision of software updates and patches with cryptografic signatures as well as a security and factory reset are usual measures to meet security requirements according to the relevant standards.

Our services also include the long-term security lifecycle management. Subsequent to our well established CVE security and mainatenance management against a software bill of material (SBOM) our kernel system and security experts will assess and contextualize each system specific finding and thus usually significantly reduce the number of critical findings which need to be processed.

Our CVE security report (pdf or CycloneDX, VEX or SPDX) will not only list the relevant findings but also their criticality level and a recommandation how to handle the issue. This will be evaluated in a regular meeting.

Besides the obligatory reporting of security occurences (Incident Response) a qualified impact analysis with prioritized measures to resolve the issues is a precondition to enable the product management to take action.

The sum total of these strategies, measures, technologies and processes impact the whole product lifecycle. They make sure that a high security level of an industrial embedded Linux based system can be reached and kept in an very effective and efficient way.

Our own security management fully supports the achievement of the overall capability security level of the product. It helps to show correctness of the product‘s implementation of security capabilities. The known security vulnerabilities in the product are identified and eliminated as aligned and agreed on with our customer as described in emlix security monitoring.

Find out more. Our experts will be happy to provide consulting.

Phone +49 551 304460

solutions@emlix.com