WNDRVR

Professional Services
Security Assessment

SECURING YOUR EMBEDDED DEVICE

The approaches to security are varied and confusing — and dynamic, due to the ever-changing threat landscape and increasing regulatory requirements. Wind River® Professional Services has a deep understanding of the threat landscape that your device will encounter.

The Wind River Helix™ Security Framework is a systematic approach to securing your embedded system and protecting your device from cyberattacks. The Helix Security Framework is based on the industry-standard model that represents security: the CIA Triad. Confidentiality, Integrity, and Availability are the fundamental principles in protecting a device from an attack. Wind River has decomposed those principles into security implementations that are then layered together to provide a strong defense for your system.

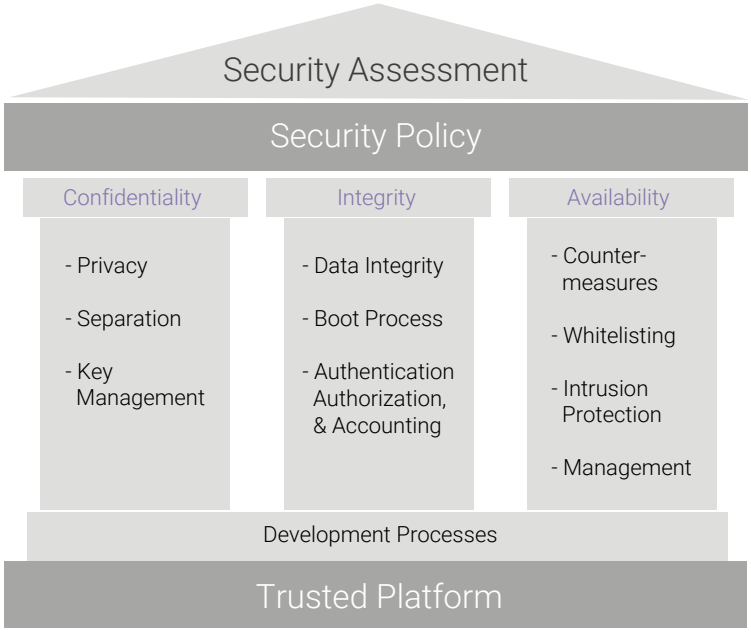

Figure 1. CIA Triad principles

WHAT DOES WIND RIVER PROFESSIONAL SERVICES OFFER?

Professional Services will provide a detailed written assessment of how to secure your embedded system, including:

- Identified assets
- Identified threats to those assets
- A clearly defined security policy that describes:
  - A list of security implementations that will protect each asset from the listed threats
  - A list of security-related log events that should be recorded
  - A list of responses to those security audit log events
- A prioritized list of recommendations

The assessment is customized to your needs, which may include:

- A software architecture review
- New product development
- A tech refresh of the existing device
- Maintenance of the device
- A program protection plan (PPP)
- A risk management framework (RMF)
- Security policy documentation

WHO IS INVOLVED DURING A SECURITY ASSESSMENT?

The Security Assessment is specific for each device. Because of this, the project team that is developing the embedded system is closely involved with the development of the assessment.

Once the necessary information about the embedded system is gathered, Wind River engages the project team representative regularly to ensure that the approach does not violate project goals related to cost, schedule, and/or technical issues.

At the conclusion of the assessment, Wind River provides a formal presentation of the findings.

WHEN TO ENGAGE WIND RIVER FOR A SECURITY ASSESSMENT

The engagement process begins by contacting your Wind River account team. Wind River will then discuss with you the attributes of your embedded system and determine an approach to performing the Security Assessment.

Each Security Assessment is unique and targeted to your needs. A typical security engagement is shown in Figure 2.

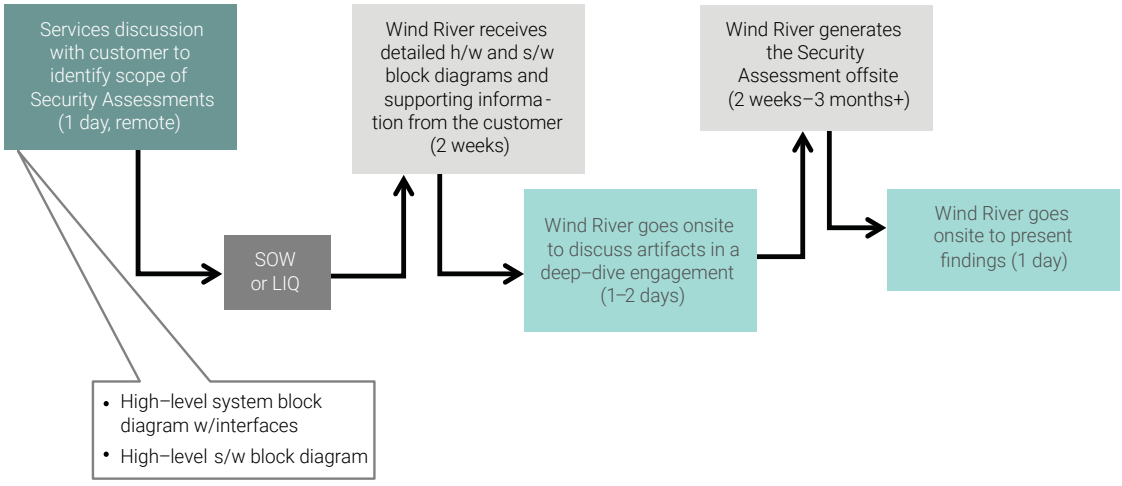

Figure 2. Typical Security Assessment engagement

As shown in Figure 3, a Wind River Security Assessment includes both your internal and external customer cybersecurity requirements, along with the regulatory requirements your system needs to comply with.

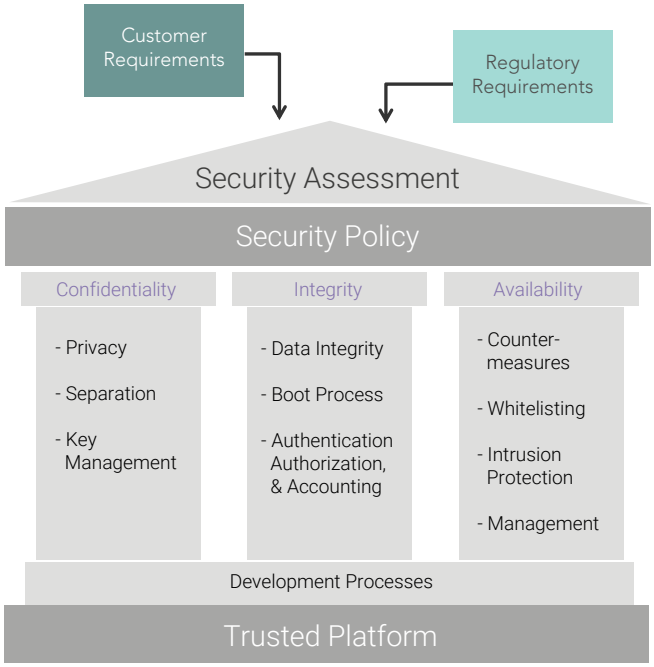

Figure 3. Wind River Security Assessment

WIND RIVER PROFESSIONAL SERVICES

Wind River Professional Services has a strong track record of guiding our customers through the complexities of new technology adoption. Certified to CMMI Level 3 across all of our global development centers, our proven engagement methodology, timely delivery, and in-depth understanding of market and technology dynamics have made Professional Services a valuable implementation partner to our customers. Our experts provide consultation services that help our customers improve the security of their systems.

Contact us today for more information about how Professional Services can assist your company with your security needs. To find your local Wind River sales contact, visit www.windriver.com/l/contact, call 800-545-WIND (9463), or email security-solutions@windriver.com.

WNDRVR

Wind River is a global leader of software for the intelligent edge. Its technology has been powering the safest, most secure devices since 1981 and is in billions of products. Wind River is accelerating the digital transformation of mission-critical intelligent systems that demand the highest levels of security, safety, and reliability.