EMBEDDED SYSTEMS SECURITY ASSESSMENT

BLACKBERRY QNX SECURITY SERVICES

DATASHEET

The security of your embedded system is only as good as its least secure hardware and software components. This is why it's important to fully understand security across the supply chain and the entire lifecycle.

Backed by more than 30 years of experience in cybersecurity, BlackBerry QNX has developed a set of Security Services to support the attestation of the security of your embedded system. Our embedded security experts will perform services such as a Threat and Risk Assessment (TARA), Threat Models as well as assessments to support compliance attestation to Regulation and Standards such as ISO/SAE 21434 and WP.29 R155 as is well known and expected in the automotive domain.

The BlackBerry® QNX® Security Services team has deep expertise and decades of security research and development to help you protect your products. Our security experts are well known in the industry with published research and thought leadership across the embedded security space. BlackBerry QNX Security Services will support your organization from product design to preparing for regulatory certification of your embedded system. Our security assessment team can advise you on secure architecture design, development, deployment, and supply chain management whether you are looking to build a secure platform, harden a product, or deploy secure and effective IoT capability.

THE BLACKBERRY QNX ASSESSMENT FRAMEWORK

BlackBerry QNX Security Services will assess the security of your embedded system or component by meeting you where you are on your security journey. We know that some will be at the start while others may be somewhere along the path but find they need assistance in meeting their embedded security objectives.

We establish where you are by gaining an understanding of your security culture and by examining your security requirements, policies, procedures, and controls as they relate to the component under review. We then establish the component's security posture by identifying the vulnerabilities, threats, and countermeasures that are specific to the domain of the component. From here, our cybersecurity experts will make a set of recommendations that will bring the component to a secured yet robust state to support the achievement of regulatory compliance.

By making use of the BlackBerry QNX proprietary threat modeling and risk scoring framework, we will assess the security risks of your embedded system. Our framework is aligned with international standards and rooted in MITRE's TARA and the HEAling Vulnerabilities to Enhance Software, Security, and Safety (HEAVENS) framework using the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) methodology.

The specific techniques employed will be tailored to the domain and system being assessed, the strategy being that while all domains will suffer from the same categories of vulnerabilities such as Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privileges, each domain will have a different set of plausible attack vectors and applicable countermeasures.

Additionally, if the software binaries are available, the assessment will include the usage of the BlackBerry® Jarvis® Binary Scanning tool to uncover potential vulnerabilities that are buried within the codebase to take the assessment to a deeper level of visibility and understanding.

Following the assessment, the security assessment team will present the findings and mitigation recommendations during a virtual workshop.

About BlackBerry QNX: BlackBerry QNX is a trusted supplier of safe and secure operating systems, hypervisors, frameworks and development tools, and provides expert support and services for building the world's most critical embedded systems. The company's technology is trusted in more than 195 million vehicles and is deployed in embedded systems around the world, across a range of industries including automotive, medical devices, industrial controls, transportation, heavy machinery and robotics. Founded in 1980, BlackBerry QNX is headquartered in Ottawa, Canada and was acquired by BlackBerry in 2010.

BlackBerry QNX software and development tools are standards- based and enable companies to adopt a scalable software platform strategy across product lines and business units. The BlackBerry QNX software portfolio, including safety pre- certified products, is purpose-built for embedded systems and scales from single-purpose devices to highly complex systems of mixed criticality. Because we are successful only when you are, you can rely on our support and professional services teams to provide the expertise you need, when you need it—throughout the entire product development life cycle.