Strengthen cybersecurity for connected product development

UL IoT Security Starter Kit

Cybersecurity challenges

- Determining the right level of security for connected products or systems
- Developing security knowledge and skill set of internal teams
- Embedding security into product development and lifecycle management processes
- Gaining insight into product or system security risks

Accelerate your internal IoT cybersecurity capabilities

Building cybersecurity into connected products is a critical component needed to unlock the vast potential of IoT innovation. If done well, it empowers companies to successfully implement their business strategy, mitigate risks, protect their brand reputation, create product differentiation and establish market leadership.

Even with the advancement of connected product innovation across industries, most products today are still built to functional, cost and time-to-market objectives. Security is not a primary consideration, or an after-thought at best. To mitigate organizational risk, security needs to be a consistent and thorough consideration throughout product development and lifecycle management processes.

Many organizations are looking to advance their IoT cybersecurity capabilities and are asking:

- How can we best incorporate security as part of our connected products, systems or services?
- What can we do to learn about key IoT security by design principles?
- How can we help educate our development and security teams so they incorporate security by design principles into product design, development and maintenance?
- How can we evaluate the security maturity of our product design, development and maintenance processes?
- How can we help ensure secure product life cycle management?

To empower organizations of varying security maturity, UL offers the IoT Security Starter Kit to help improve internal cybersecurity capabilities. Based on Secure Development Lifecycle (SDL) best practices, offerings within the UL IoT Security Starter Kit include:

- Security by Design Training
- SDL Gap Analysis
- Product Security Architecture Review
- Penetration Testing

Benefits of the UL IoT Security Starter Kit

- Helps advance in-house security knowledge and capabilities
- Ability to compare internal security processes and practices to industry frameworks and standards
- Ability to prioritize processes and practices that require improvements to meet industry frameworks and standards
- Insight to understand product, security architecture and design risks through testing for vulnerabilities and exploits

Why UL for cybersecurity?

With more than two decades of cybersecurity experience, UL is a recognized leader in markets regulated for cybersecurity, including payments and federal procurement. UL's portfolio of IoT security solutions includes the UL IoT Security Rating, UL Supplier Cyber Trust Level and services for IEC 62443 and UL 2900 Series of Standards. We offer security by design training, advisory and testing services that address secure product development, cybersecurity in smart ecosystems and supply chain risk management.

IoT Security Starter Kit – Key Offerings

The UL IoT Security Starter Kit helps to improve internal cybersecurity capabilities for a Secure Development Lifecycle to enable secure product development and lifecycle management. This set of offerings is customizable based on an organization's specific and unique security needs.

SECURITY BY DESIGN TRAINING

Help improve internal cybersecurity capabilities and expertise tied to a Secure Development Lifecycle.

UL will empower you with knowledge on:

- Security by design principles
- Secure Development Lifecycle frameworks
- Concrete implementation and product roadmap suggestions

Training formats available include:

- Remote half-day interactive training
- Remote or on-site 1-2 day workshop, tailored to a product strategy and roadmap

SDL GAP ANALYSIS

Review and prepare for a security assessment by performing a gap analysis focused on required security processes and documentation.

UL will perform a gap analysis, comparing your security processes and practices to industry frameworks, which helps:

- Scope products and systems and their applicable security requirements
- Identify areas for improvement and readiness for potential cybersecurity assessment

PRODUCT SECURITY ARCHITECTURE REVIEW

Perform product security architecture design review focused on required security features. UL identifies the potential risks or gaps with a focus on must-have security by design features, based on a detailed examination of the architecture and design documentation.

A product security architecture review helps:

- Identify the product's assets and possible attack scenarios
- Evaluate adherence to essential security by design principles
- Spot potential security flaws early in the development process

PENETRATION TESTING

Penetration testing involves discovering and exploiting software vulnerabilities with extensive hacking techniques. UL testing looks at common security weaknesses and controls, based on IoT and cybersecurity best practices, including:

- **Black box** – outsider security assessment
- **Grey box** – moderately in-depth security assessment
- **White box** – comprehensive, full access security assessment

This testing provides security level insights, including demonstrated vulnerabilities and remediation advice.

For more information on UL IoT Security Starter Kit offerings, email us at imsecurity@UL.com or visit IMS.UL.com/IoT-Security-Starter-Kit.

Empowering Trust®