kaspersky

Product security maturity assessment

The problem

IoT, IIoT, and M2M product vendors face difficulties in formalizing an assessment of their security level and demonstrating it as a competitive advantage.

The solution

A reliable assessment of the security maturity of a product, including an analysis of security mechanisms and measures throughout the product lifespan, results in a certificate confirming that the product is sufficiently secure and will stay that way.

Target audience

Vendors producing smart and connected devices for specific purposes, such as network equipment, industrial internet of things systems, transportation, logistics, energy, agriculture, building automation and technological processes.

Vendors producing IoT products with specific functionalities, such as smart video cameras, wearable gadgets (watches, wristbands, etc.), smart toys and kids' assistants, augmented reality systems, and smart pet feeders.

Manufacturers of chips, modems, SoCs, etc.

Vendors producing technological solutions, such as license managers, PLC environments, OTA systems for updating IoT devices, cloud platforms, etc.

The issue

A mature security system contains sufficient protection technologies that do not negatively affect its functionality. It's important to note that the definitions of "sufficient protection" and "negatively affect functionality" are unique to each system.

Different products and solutions require different cybersecurity levels and procedures. Each vendor independently prioritizes the cybersecurity standards necessary to protect its product. Maturity is mostly defined by how effectively different measures are implemented, not by their presence.

Businesses need a systematic approach to selecting the necessary security measures and means that balance business priorities, security goals and

methodologies with the desired effect. Since there are myriad methods to secure a system, it is necessary to describe, organize and clarify the criteria for making the best choices.

To demonstrate to customers that products are appropriately protected, vendors must provide information about the security goals and priorities used, as well as any resulting limitations. For example, security measures cannot interfere with real-time operations if that is required by the solution. This information is included in the product's security maturity profile. The profile, used alongside the security maturity certification, specifies what consumers can expect from the product with regard to cybersecurity measures and methodologies.

Limitations may not seem like a competitive advantage for products and services. In practice, however, a precise description of the underlying functionality and conditions enables vendors to manage customer expectations and to focus on the real strengths of the product or service.

About the IoT Security Maturity Model

In 2019, the Industrial Internet of Things (IIoT) Consortium released a practical guide for implementing the IoT Security Maturity Model. The model is meant to ensure that cybersecurity methodologies align with business needs.

> The goal was to provide a clear description of a sufficient state of security for systems and to help those responsible for system security identify the most effective methods for achieving that state and the appropriate security measures.

Using the security model enables:

- Optimizing the process of identifying security goals, i.e., defining the "sufficient security" and describing all reasonable limitations.
- Evaluating and planning the detailed scope of work required to achieve sufficient security.
- Conducting a technical evaluation that compares the current state of security with the security maturity model based on business requirements and issuing a security certification if they are comparable.

What we offer

We assess the security maturity of products or technological solutions. We profile and comprehensively assess products or solutions according to their unique features, market position and industry specifics.

This profiling results in an individual security maturity profile containing the necessary and sufficient requirements for organizing and implementing practical security measures while identifying the limitations of these measures. These measures are called security practices.

Security practice assessments take into account the technical and organizational aspects of security implementation. The assessment includes a vulnerability analysis of the current version of the product or solution, among other things.

Once the assessment is complete, Kaspersky certifies that the implemented security practices conform to the security maturity profile for the product or solution in question.

Benefits

- The assessment is unique and based on an individually tailored security profile, rather than generic cybersecurity criteria developed for multiple products.
- Profiling and assessment methodologies are based on the Model for IoT established by the IIoT Consortium Security Maturity, in which we actively participated.
- We examine limitations on implementing security practices based on industry standards or the unique traits of the given product or solution. This allows for the development of compensatory measures.
- A targeted search and vulnerability assessment are integral elements of product evaluation and serve as criteria for evaluating security maturity.

What we do

Together with the vendor, we establish security maturity targets for the product and examine the environment where it will be used, as well as any other necessary conditions. We then compare these targets with the goals that must be achieved to reduce security risks. Ultimately, we examine three classes or domains: managing security issues throughout the product's lifecycle, implementing protection measures, and supporting the product's security during use.

Based on the data provided by the vendor, we:

- Prioritize tasks to ensure product security.
- Set the degree to which each task should be completed.
- Describe existing limitations.

These steps help us create an individual profile for assessing the end product or technological solution based on security requirements.

The security maturity profile specifies the organizational security measures and protection technologies required to achieve the described security targets and protect against cyberattacks.

We use the profile to determine which tasks the vendor's technical personnel must complete to reach the desired security maturity levels, taking into account the unique characteristics of the industry and product.

We then use the security maturity profile to assess the product and vendor processes, determining the extent to which they align with the profile requirements. To obtain the necessary information about the development, release and maintenance processes, we consult various specialists and representatives from different vendor departments. Product research covers architecture and security functionality analysis, as well as search and vulnerability analysis.

If we detect areas where a process or mechanism does not conform to the profile, we provide the vendor with recommendations on how to resolve the discrepancy. Once the recommendations are implemented, we reassess the process or mechanism.

We modify the security maturity profile only when we uncover critical nonconformities that cannot be resolved for reasons that were not identified at the time of profile development.

After creating a final security maturity profile for a product, we can provide the vendor's customers with objective data about the product and its security state. This data is provided in the form of a certificate containing a link to the profile.

Result

The vendor receives a certificate confirming the product's security maturity state and containing a link to the security maturity profile. The certificate independently confirms that the necessary security measures and mechanisms have been implemented, which can serve as a competitive advantage when selling the product.

In addition, the customer receives:

- A full report analyzing the product itself, as well as the development, release and support processes.
- A vulnerability analysis of the current product version.
- Recommendations for improving the product and processes that can be applied to similar products and processes.

How the product vulnerability assessment service differs

Product vulnerability assessment cannot certify the security maturity state of a product or solution since no vulnerability discovery methodology can detect all potential vulnerabilities. It can only determine whether vulnerabilities were discovered at the time of the assessment. The Kaspersky product security maturity assessment identifies vulnerabilities and provides recommendations to address them. It also confirms that the vendor has implemented the necessary measures to protect against additional vulnerabilities and to fix any future vulnerabilities promptly, should any be detected.

Moreover, the security maturity assessment:

- Accounts for the environment in which the product will be implemented, industry limitations and requirements for other security aspects and functionality.
- Can be applied not only to the current product version but also to future versions, provided that support continues to be implemented.
- Allows vendors to develop other products using the security maturity profile of the original product along with related recommendations for improving the product and processes.

When it comes to improving product and process security, we can compare the security maturity profile to industry standards or regulatory recommendations. Using the profile excludes a formal approach and recommends only those methods that ensure security and conform to the environment and scenario in which the products will be used.

Sample scenarios

Assessing the security maturity of an existing product on the market

A vendor can submit a product that has already been released to the market for a security maturity assessment. This is the simplest use case since there is no uncertainty regarding how the product is implemented or supported. We then

build a security maturity profile based on the vendor's priorities, evaluate the results and compare them.

In some cases, the technical and organizational security measures conform to the security maturity profile established for the given industry and device, taking into account all limitations and unique security implementation realities. In such cases, Kaspersky issues a certificate confirming the security maturity of the product or solution. The certificate links to a detailed description of the security maturity profile. These documents should always be viewed together.

However, the only way to resolve discrepancies between the security maturity profile and the real-life situation for an existing product is to lower the maturity level guaranteed in the profile. The vendor will then receive recommendations for fixing the product's architectural security issues, which can be implemented in the next product version of the product.

Assessing the security maturity of several existing products or a product line on the market

A more complicated but cost-effective method is to assess the security maturity of several similar products or an entire product line. In this case, a single security maturity profile is created. Kaspersky works with the vendor to evaluate either all the products or a representative product from a product line (usually the one with the most complete functionality). In the latter scenario, technical experts analyze the use of a single programming code and the hardware requirements for each solution or product being evaluated.

Kaspersky issues a certificate of security maturity for the products or product line when the technical and organizational security measures conform to the security maturity profile established in accordance with all limitations and unique aspects of ensuring security in the given industry and for the given device. The certificate lists the products and their identifying data, as well as a link to a detailed description of the security maturity profile. These two documents should always be viewed together.

As in the scenario above, if Kaspersky uncovers any discrepancies, we will recommend lowering the security maturity level guaranteed in the profile and provide suggestions for improving the next product version.

Preparing a security maturity profile for a new product. Helping develop the product around the profile. Certifying the results

If a customer needs a product to conform exactly to business requirements, the optimal approach is to develop a security maturity profile based on these requirements. This profile can then be translated into technical requirements to ensure the product and processes conform exactly to the profile.

The sooner work on a security maturity profile begins, the easier it is to implement the requirements in a new product. The assessment largely depends on the development process, including the maturity of the processes, precise security criteria for working with external vendors and open-source code, and procedures for establishing requirements and testing security. Processes cannot be changed overnight if it becomes clear that this is necessary.

However, it is possible to develop a profile and conduct a security maturity assessment at any stage of product development up to the final release.

In this scenario, we first create a profile according to vendor expectations. Then, we assess the existing technical requirements, processes and decisions involved in product development. We present the results in a report describing the product's current security maturity and providing recommendations for improving processes and decision-making. These recommendations ensure that the final product conforms to the security maturity profile. They are presented as a roadmap for improving product security maturity prior to release and commissioning.

It is important to be aware that the business requirements may change during development, so we periodically review the target security maturity profile, our recommendations and the product roadmap. We support the development process by conducting periodic, agreed-upon reviews of the security maturity up to product release. We also monitor and support product development during testing and integration, conducting vulnerability assessments to ensure any detected vulnerabilities are fixed before release.

The process ends when the product is released. The product is assessed in accordance with the target security maturity profile. The same process can be applied to a group of products or a product line, which naturally requires a longer timeline.

Request a consultation

Learn more

- The internet of things security maturity model: a nudge for IoT cybersecurity
- Cinterion EHS5 3G UMTS/HSPA Module Research
- The secrets of Schneider Electric's UMAS protocol
- Dynamic analysis of firmware components in IoT devices
- ISaPWN – research on the security of ISaGRAF Runtime
- Practical example of fuzzing OPC UA applications
- VNC vulnerability research
- Security research: CODESYS Runtime, a PLC control framework. Part 1
- Security research: CODESYS Runtime, a PLC control framework. Part 2
- Security research: CODESYS Runtime, a PLC control framework. Part 3
- How we hacked our colleague's smart home, or morning drum & bass
- Security research: ThingsPro Suite – IIoT gateway and device manager by Moxa
- OPC UA security analysis
- Somebody's watching! When cameras are more than just 'smart'
- A silver bullet for the attacker. A study into the security of hardware license tokens

Related services

- ICS vulnerability data feed
- Incident response at industrial organizations
- Analytical Reports on ICS threats and vulnerabilities on the Kaspersky Threat Intelligence Portal

Request a consultation

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com