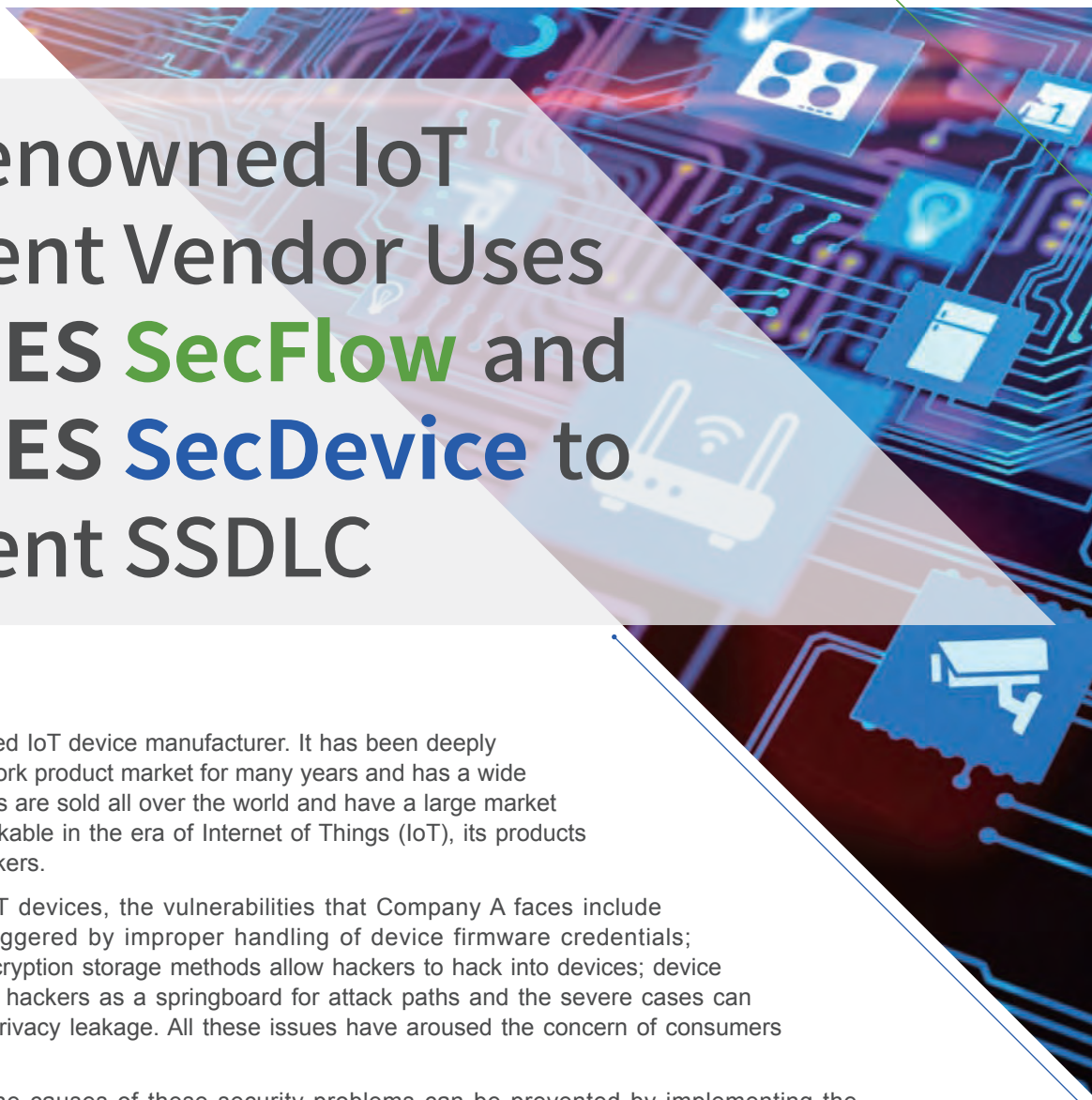
onward SECURITY



World-renowned IoT Equipment Vendor Uses HERCULES SecFlow and HERCULES SecDevice to Implement SSDLC

Overview

Company A is a world-renowned IoT device manufacturer. It has been deeply involved in the consumer network product market for many years and has a wide reputation. Many of its products are sold all over the world and have a large market share. Since everything is hackable in the era of Internet of Things (IoT), its products have become the target of hackers.

In the frequent attacks on IoT devices, the vulnerabilities that Company A faces include that malicious attacks are triggered by improper handling of device firmware credentials; account secrets with weak encryption storage methods allow hackers to hack into devices; device vulnerabilities can be used by hackers as a springboard for attack paths and the severe cases can lead to the risk of consumer privacy leakage. All these issues have aroused the concern of consumers and government agencies.

The company believes that the causes of these security problems can be prevented by implementing the Security by Design concept during the development process. Therefore, it decided to introduce the Secure Software Development Life Cycle (SSDLC) to reduce the chance of these problems early.

Challenge

When Company A decided to incorporate security factors into the development process early, the development team began to think about factors that may have caused product insecurity in the past during the development process, including:

1. **Numerous products make the process of checking product models and discovering vulnerabilities complicated and time-consuming;**
2. **Open source software packages are numerous and scattered, and using third-party packages is difficult to grasp their vulnerabilities;**
3. **The relevant personnel are too slow to obtain vulnerability information and unable to keep up with the speed at which vulnerabilities are revealed by security experts;**
4. **The existing management tools cannot meet the security requirements of SSDLC.**

After listing the problems needed to be solved, Company A began to look for the assistive tools that could solve the above challenges. However, the company found that many tools on the market can only meet a single requirement such as development management, vulnerability scanning, vulnerability management, etc. The introduction of "multiple sets of" new tools will inevitably increase the management burden, and the management work will also become complicated, thus making it time-consuming and laborious to solve the above security problems. Therefore, providing convenient management features has become one of the key considerations for its adoption of tools. After evaluation, Company A decided to adopt the "SecFlow product security management system" and "SecDevice automatic vulnerability assessment tool" that can meet the breadth of the development process and the depth of test security to solve the challenges it faces.

onward SECURITY

Onward's Solution

Company A uses the "SecFlow product security management system" for security flow management, security vulnerability database and proactive product security monitoring and reporting. The system assists its organization to link development, security and maintenance teams to quickly establish a secure SSDLC. Meanwhile, the company uses the "SecDevice automatic vulnerability assessment tool" for product testing and security assessment. After implementing the two solutions, the application focuses are as follows:

- **The product management team builds its own vulnerability database to automatically count Open Source vulnerabilities**
  By using SecFlow's built-in product management function to compare with the database storing the latest vulnerabilities, the product PM of Company A can perform security analysis and automatically screen out the Open Source vulnerabilities used by the outsourced development team. This function saves the PM team a lot of work for comparison of vulnerabilities. It also allows the team to avoid using the Open Source, which has vulnerabilities, in the process of product development to prevent possible product security issues in advance.
- **The security team uses real-time security information to formulate early countermeasures for newly revealed vulnerabilities**
  In the past, the security team members of Company A passively collected vulnerability information and used manual methods to notify the product owner in order to formulate measures to address the vulnerabilities. After adopting SecFlow, the system receives the risk events and vulnerability information from nearly 70 intelligence sources every day. Through the built-in information correlation function, the new vulnerabilities that are exposed can be automatically included in the security database. The system also notifies the PM, RD and the person in charge of security to deal with them. This allows the product security team to greatly increase the incident response time. SecFlow reduced the time needed to deal with vulnerabilities from 2~3 months to 2 weeks.
- **The testing team incorporates unknown vulnerabilities into the testing scope**
  During the quality test and verification stage before the product leaves the factory, in addition to verifying functions and specifications, the test team of Company A also uses the fuzzing test function of SecDevice to discover the unknown vulnerabilities hidden in the product such as buffer overflow, format string and command injection. It can verify the robustness of the product against malicious attacks. Besides, when delivered, SecDevice can also be used as a testing tool for vendors to verify product security. In this way, an extra quality control can be added to the product in the testing and delivery processes.
- **The security team integrates third-party tools and keeps the most complete test records**
  For third-party security test reports and processing records during product development, the security team of Company A uses the test report management function of SecFlow to save test reports from SecDevice and other third-party security test tools. It keeps the most complete security testing data for future internal and external inspections.

Benefits

After using SecFlow and SecDevice, the customer not only successfully implemented the Security by Design, but also obtained several overall benefits:

1. **A single system satisfies the needs of the product management team (product security risk management) and the security team (incident response), reducing management complexity;**
2. **A single system meets for all security management requirements of the security team in the SSDLC process, reducing personnel learning costs;**
3. **The built-in information collection and correlation functions help the security team find vulnerabilities in real time and speed up processing of vulnerabilities;**
4. **Assisting the testing team to detect known and unknown vulnerabilities during the development process improves product quality before mass production.**

In the world of the Internet of Everything, the types of devices that are connected to the Internet are increasing, allowing the vulnerabilities and attacks that hackers can use to be much broader. If all networked devices can strengthen the depth of testing before mass production and vendors incorporate security as a design consideration as early as the development stage, the risk of major vulnerabilities being exposed after mass production of products is bound to be greatly reduced.