CASE STUDY

Automated IoT Vulnerability Remediation at Enterprise Scale

Situation

A leading Silicon Valley technology company with close to 9000 IoT devices across 10 sites was not able to keep up with the pace of firmware updates. When the devices were first installed more than 5 years ago there were yearly firmware updates, typically to deliver new functionality, and the company did not establish a process for ensuring these updates would be installed quickly (or at all). But over the last few years multiple firmware updates per year were being issued by the device manufacturer, mainly to remediate known cyber vulnerabilities (also known as CVEs, or Common Vulnerabilities and Exposures). From a risk perspective the company decided it had to have a process to quickly patch these devices, especially since many of the CVEs had a severity score that classified them a high or critical severity.

The company contracted a third party security consultant to assess their situation. They determined that using the device manufacturer's manual method of firmware updating would require 86 new full-time professionals to keep pace, a headcount completely unbudgeted for. Most alarming was when the consultant highlighted that it would take over 6 weeks from when a patch was available to when the devices would have the vulnerabilities manually remediated – too large of a window for threat actors to exploit high severity known vulnerabilities. The company's board of directors required the CISO to come up with a plan to shrink the IoT attack surface, and quickly.

Solution

To both reduce their attack surface and meet their budget constraints, the decision was made to deploy an automated solution for firmware patching and updates. The search quickly narrowed based on their desire to have a small team manage all IoT firmware updates across their 10 sites. They found that Viakoo was the only provider who could (based on patented technology) automate updates across multiple geographies without having to have personnel physical present at each site. Viakoo's Device Firmware Manager (a solution module of the Viakoo Action Platform) was selected; deployment was complete within a few days.

Outcome

Today the company has a team of 2 people use Viakoo Action Platform (VAP) and the Device Firmware Manager module to ensure firmware updates are quickly implemented. Compliance to internal security policies is demonstrated through Viakoo's integrated reporting capability, showing how all devices have been updated within days of a new firmware version being available. In addition, the company has benefited from using the service assurance capabilities in VAP, reducing the company's maintenance budget for these IoT devices by 30%. Today the company is looking to extend it's Zero Trust initiative to include IoT devices, and is planning to use Viakoo's Device Certificate Manager (DCM) to automate the deployment and management of certificates across their infrastructure.

Master the security of your cyber-physical systems with the Viakoo Action Platform.