



IoT Inspector

The Firmware Security Analysis Platform

Die Automatisierte Sicherheitsanalyse für IoT-Firmware.

Einfach die Firmware hochladen, die Analyse starten und wenige Minuten später stehen die Ergebnisse zur Verfügung.

www.iot-inspector.com

IoT Inspector

Schwachstellen in Firmware auf der Spur.

Smarte Maschinen, vernetzte Geräte, neue Firmware – jede Anschaffung und Änderung im System birgt die Gefahr neuer Sicherheitslücken. Ob als Produktentwickler oder User: IoT Inspector deckt diese ‚Schwachstellen ab Werk‘ auf, noch bevor sie von Cyberkriminellen ausgenutzt werden können.

Die bislang zu Forschungszwecken genutzte Firmware-Analyseplattform steht nun erstmals vollautomatisiert Unternehmen zur Verfügung und damit auch das jahrzehntelange Know-how der Cyber Security Experten von IoT Inspector. Plugins erkennen Schwachstellen und nutzen dabei zusätzlich auch Datenquellen wie die IoT-Suchmaschinen Shodan und die National Vulnerability Database von NIST. Eine große Bandbreite an vernetzten Geräten wie IP Kameras, Router sowie Drucker wird abgedeckt. Unternehmen ist es so möglich, die Firmware von IoT-Devices vor und nach Inbetriebnahme auf Schwachstellen zu überprüfen – selbstständig und schnell.

- **Einfache Nutzung, 100 % automatisiert**

Nach dem Hochladen der Firmware Images oder Update Files überprüft IoT Inspector völlig automatisiert die Software nach etwaigen Schwachstellen. Die ausgewerteten Daten stehen innerhalb weniger Sekunden bereit. Source Code ist dazu nicht notwendig.

- **Übersichtliches Web GUI, durchgehende Beobachtung**

Das übersichtliche und konfigurierbare Web GUI stellt Analyse-Ergebnisse und Statistiken visuell dar. Auch PDF Reports können erstellt werden. Bereits hochgeladene Firmware wird dank Real-Time-Alert durchgehend im Auge behalten.

- **Plugins, Plugins, Plugins**

IoT Inspector basiert auf Plugins die ständig weiterentwickelt werden. So kann künftigen Bedrohungen möglichst flexibel und schnell entgegengetreten werden.

- **Tausende Schwachstellen und Geräte**

Jahrzehnte von Security-Know-How aus den Bereichen Embedded Systems und IoT fließen in die Produktentwicklung. Unternehmen können sich diesen Informationsvorsprung zunutze machen. Alle Geräte werden laufend gegen alle hinterlegten Schwachstellen geprüft.

