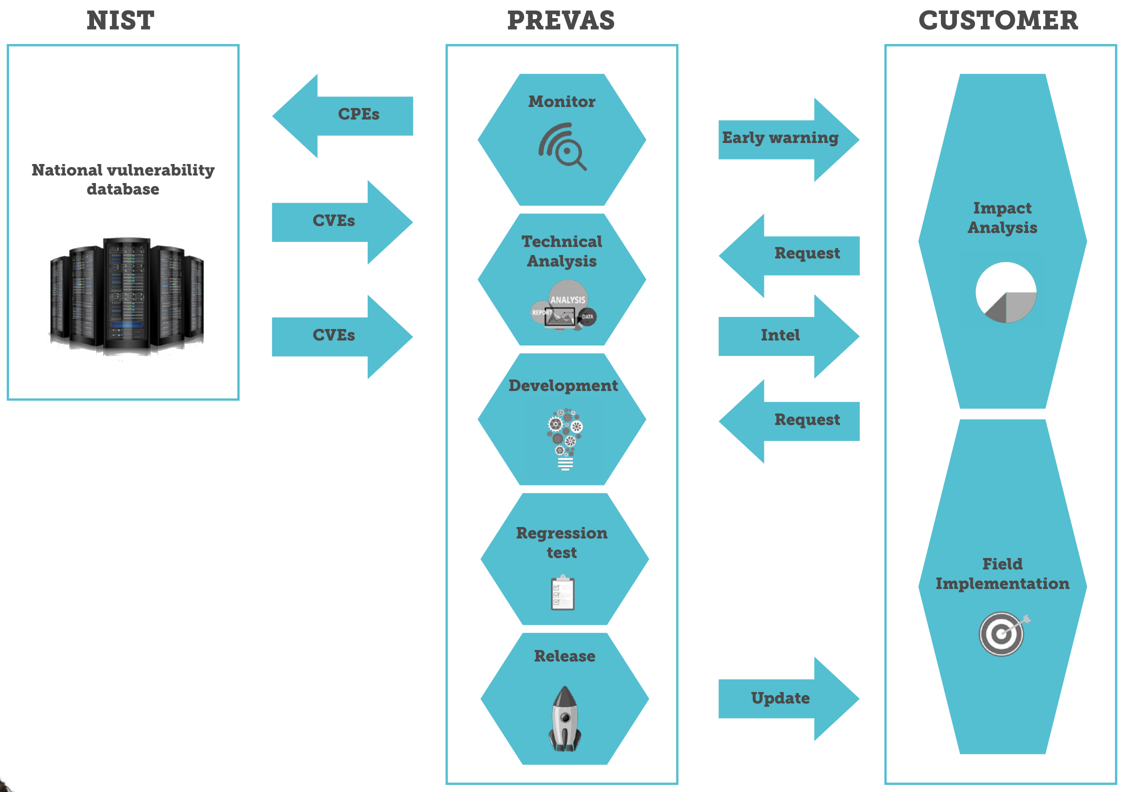
Prevas
Hello Possibility.

PREVAS CYBER SECURITY INTELLIGENCE (PCSI)

The Prevas Cyber Security Intelligence (PCSI) process is a proactive offer designed to assist our customers in mitigating risk, by getting early notification in case of public available security threats in product firmware components. An embedded Linux device typically builds on tens to hundreds of open-source components - e.g. the Kernel, webservers, bootloaders, shell, crypto libraries etc. During the normal lifespan of a device, a multitude of cyber security related vulnerabilities are publicly discovered and registered for these components. In principle, depending on the nature of the device, any of these vulnerabilities could be damaging to the vendor's business.

OUR OFFER

- Analyse Linux devices and break down firmware into a structured list of community driven components (CPEs).
- Cross examine CPEs against leading vulnerability databases (e.g. NIST NVD).
- Notify potential findings (Common Vulnerabilities and Exposures - CVEs) to customers, and provide technical assistance in the threat assessment.
- Assist in implementing recommended fixes and counter measures in the product firmware.



NIST

National vulnerability database

CPEs

CVEs

CVEs

PREVAS

Monitor

Technical Analysis

Development

Regression test

Release

Early warning

Request

Intel

Request

Update

CUSTOMER

Impact Analysis

Field Implementation

CONTACT
Rune Wiinberg - Head of Cyber Security
Tel.: +45 3169 3832 | Mail: rune.wiinberg@prevas.dk
www.prevas.dk

Prevas
Hello Possibility.

Prevas is a development hub with ingenuity at its core. With a high technical competence and a deep business understanding, we help customers from a wide variety of industries benefit through continuous technological innovation. Good for people, planet, and profit. Prevas was established in 1985 and currently employs 850 people in Sweden, Denmark and Norway. Prevas is listed on NASDAQ Stockholm since 1998. For more information about Prevas, visit www.prevas.com.