DEVICE-CENTRIC VULNERABILITY MONITORING AND THREAT INTELLIGENCE FOR EMBEDDED PRODUCTS

PCA CERVUS

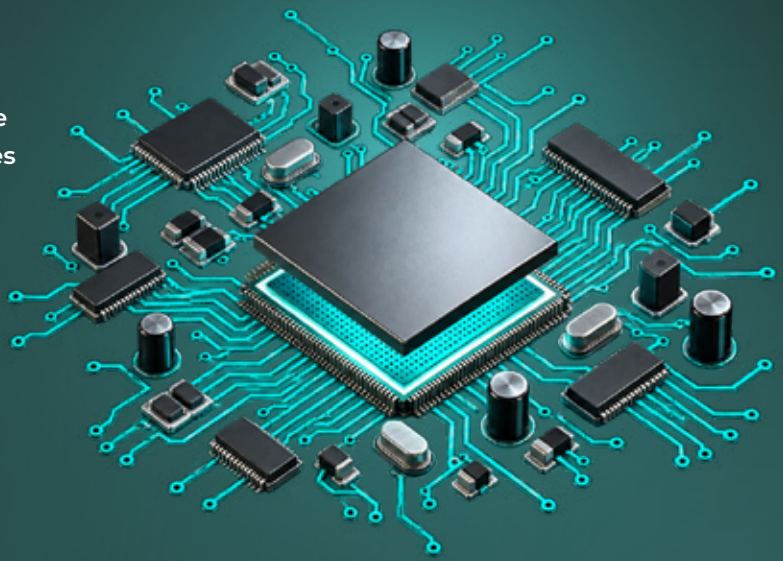
Know which vulnerabilities matter to your devices. Monitor threats throughout their lifecycle.

PCA CERVUS combines vulnerability intelligence, threat hunting and device composition analysis to help product security teams identify relevant risks, reduce noise and manage device security throughout the product lifecycle.

WHY EMBEDDED DEVICE SECURITY NEEDS A DIFFERENT APPROACH

Limited visibility

Standard vulnerability databases & threat intelligence sources rarely establish whether known vulnerabilities are relevant to a specific embedded device.



Specialized expertise

Embedded devices have distinct attack surfaces, architectures & operational constraints. Effective analysis requires device-specific & industry-specific security knowledge.

Fragmented information

Incomplete SBOMs & limited information sharing across manufacturers, suppliers & operators make it difficult to understand the actual composition and exposure of deployed devices.

Too much noise

High volumes of alerts, irrelevant findings & false positives consume security teams' time and make prioritization difficult.

Limited verification

Component names & versions alone cannot reliably establish whether a vulnerability affects the actual device or whether a security fix is present.

ONE PLATFORM. CONTINUOUS DEVICE SECURITY INTELLIGENCE.

PCA CERVUS combines multiple sources of security intelligence with device specific context to help teams focus on the threats that matter.

- **Continuous vulnerability monitoring** - Track emerging vulnerabilities and threats relevant to your products.
- **Device-focused threat intelligence** - Correlate threats with device architecture, components and SBOMs.
- **AI-assisted analysis and prioritization** - Identify relevant risks using PCA's embedded security expertise.
- **SBOM and supply-chain visibility** - Analyze device composition and component-related risks.
- **Lifecycle and change tracking** - Monitor findings, firmware updates and remediation progress.
- **Reporting and collaboration** - Access dashboards, alerts and structured reports.

FROM COMPONENT LISTS TO EVIDENCE-BASED ANALYSIS

Integrated Software Composition Analysis (SCA) within PCA CERVUS

Integrating our SCA toolset with PCA CERVUS combines continuous threat intelligence with binary-level analysis to validate findings against actual software composition and support more reliable risk assessment and remediation.

Move from supplier-provided component data towards evidence-based visibility into device security.

BUILT ON EMBEDDED SECURITY EXPERTISE

PCA CERVUS was developed specifically for embedded products based on PCA Cyber Security's penetration-testing, security-assessment and threat intelligence expertise.

Discover PCA CERVUS in detail.

Book a demo to see how it would support your product security team.

WWW.PCACYBERSECURITY.COM/PLATFORM

CONTACT

info@pcacybersecurity.com
www.pcacybersecurity.com

HQ

Záhony str. 7C
1031 Budapest
Hungary

DACH OFFICE

Maximilianstr. 35a
80539 Munich
Germany