C2A Security Releases 'Claude Inside' Version of EVSec to Advance AI-Driven Product Security Orchestration

The new dedicated release uses Claude by Anthropic to enhance contextual threat analysis, vulnerability intelligence, SBOM analysis, and compliance automation

JERUSALEM, ISRAEL, May 27, 2026 /EINPresswire.com/ -- C2A Security today announced the release of a dedicated “Claude Inside” version of EVSec, its product security orchestration and context platform for software-defined and cyber-physical products.

> “Our customers are not asking us to find more issues. They need help understanding what actually matters, what is exploitable in their product context, and what action should be taken first.”
>
> *Roy Fridman*

The new release uses Claude by Anthropic to enhance EVSec’s AI-driven capabilities across threat modeling, vulnerability analysis, SBOM intelligence, regulatory compliance workflows, and product security automation for automotive, medical device, industrial, IoT, and other regulated markets.

The announcement comes as manufacturers and operators face growing pressure to manage cybersecurity across increasingly complex products, software supply chains, and regulatory environments. Frameworks including UN R155, ISO/SAE 21434, FDA cybersecurity requirements, IEC 62443, and the EU Cyber Resilience Act are pushing product security teams toward continuous, evidence-based security processes that traditional manual workflows were not designed to support.

Modern product security teams must continuously evaluate new vulnerabilities, evolving product architectures, supplier evidence, SBOM data, regulatory changes, and deployment context across dozens of products and thousands of components. Without automation grounded in real product context and domain expertise, teams are left with fragmented tools, static documents, and time-consuming manual analysis.

The challenge is now intensifying with the rise of advanced AI cyber systems and agents, including Anthropic’s Claude Mythos Preview, OpenAI’s GPT-5.5 with Trusted Access for Cyber, Google DeepMind’s CodeMender, Google’s Big Sleep, and AI-enabled adversarial tooling tracked

by Google Threat Intelligence Group. Together, they signal a new reality: AI is accelerating vulnerability discovery, exploit analysis, patch generation, and adversarial automation, forcing product security teams to distinguish faster between theoretical risk and exploitable product risk.

“AI will dramatically increase the speed and scale at which vulnerabilities are discovered, analyzed, and potentially exploited,” said Roy Fridman, CEO of C2A Security. “Our customers are not asking us to find more issues. They need help understanding what actually matters, what is exploitable in their product context, and what action should be taken first. By combining Claude’s advanced reasoning capabilities with EVSec’s product security expertise, cyber model, and contextual risk engine, we are giving manufacturers a practical way to use AI for real security outcomes.”

EVSec addresses this challenge by creating a contextual cyber model of the product and connecting product architecture, software components, vulnerabilities, threat scenarios, compliance obligations, and live risk workflows in one platform, all grounded in true product understanding. By using Claude within EVSec’s AI layer, C2A is expanding the platform’s ability to ingest complex technical and regulatory information, reason over product-specific context, and help teams move faster from raw data to defensible action.

The “Claude Inside” version of EVSec supports advanced reasoning across several product security workflows, including:

* Threat modeling and attack path analysis
Generating and refining threat models from product specifications, architecture files, engineering documentation, and security inputs.

* SBOM and vulnerability intelligence
Analyzing software component data, vulnerability information, supplier evidence, and code-level reachability context to help teams prioritize what matters.

* Regulatory and compliance reasoning
Mapping engineering and security evidence to frameworks including UN R155, ISO/SAE 21434,

FDA cybersecurity requirements, IEC 62443, and the EU Cyber Resilience Act.

* Workflow, reporting, dashboard automation, and decision support
Reducing manual analysis and helping generate audit-ready outputs for engineering, security, compliance, product, and executive stakeholders.

Unlike generic AI tools, EVSec applies AI within a structured product security expert environment. Claude operates alongside C2A's cyber model, contextual risk engine, and orchestration workflows, enabling AI-assisted analysis that is grounded in each customer's actual product architecture, components, vulnerabilities, and domain-specific security data.

In addition to the "Claude Inside" version of EVSec, the platform can integrate with other LLM services under each customer's data governance requirements. EVSec is used by leading manufacturers across automotive, medical device, and industrial markets to manage product cybersecurity across the full lifecycle, from design and development through vulnerability management, compliance, and post-market operations.

About C2A Security
C2A Security is the only AI-based, context-driven product security orchestration platform that addresses the specific needs of software-defined products in heavily regulated sectors. Founded in 2016, C2A Security's customers and technology partners include top-tier global players as Bayer, BMW Group, Daimler Truck AG, Ascensia, Elekta, NVIDIA, Siemens, Orcanos, HARMAN, Marelli, NTT Data, and Deloitte.

A CLEPA Innovation Award recipient for its industry-pioneering DevSecOps platform, C2A Security empowers companies to bridge the visibility gap between security and engineering teams towards a unified security posture. By leveraging AI-driven contextual analysis, advanced security automation, and automated compliance reporting, C2A Security transforms product security to shorten software release times and decrease costs in the healthcare, industrial, robotics, automotive, and other Cyber-Physical Systems.

C2A Security was founded by NDS/Cisco veteran Michael Dick, with its global headquarters in Jerusalem, Israel. c2a-sec.com/.

David Leichner
C2A Security
email us here
Visit us on social media:
LinkedIn

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.