SCANOSS

Automating cryptographic detection

How a global ERP vendor met export compliance at scale

KEY TAKEAWAYS

Export compliance automated

SCANOSS replaced manual ECCN classification with a single-query cryptographic detection process across all source code files.

Proprietary code made visible

Detection extended beyond open source components to cover the vendor's full codebase, regardless of code origin.

Dataset expanded through collaboration

The vendor contributed additional cryptographic algorithm definitions, incorporated into SCANOSS's Encryption dataset and available to all users.

THE SITUATION

Manual cryptographic detection at scale was unsustainable

A large ERP software vendor needed complete visibility into the cryptographic algorithms present across their entire codebase. As a global software exporter, the company was subject to ECCN classification requirements, which mandate identifying and declaring the encryption algorithms contained in software shipped across borders. Meeting these requirements manually — scanning code, identifying algorithms, classifying them — had become a significant bottleneck, consuming excessive time and resource.

The company had been using CryptoDetector, an open source tool for detecting cryptographic algorithms, but it did not meet their requirements at scale. Critically, it could not cover proprietary source code — only open source components. The vendor needed a single query capable of returning a comprehensive list of every cryptographic algorithm in use across all source files, regardless of origin.

THE SOLUTION

Full-codebase visibility through the SCANOSS Encryption dataset

SCANOSS addressed the detection gap by leveraging its Encryption dataset and extending its Crypto Finder capability beyond open source components to cover all source code files, regardless of origin. This required modifying the underlying software to scan proprietary code — a capability that did not previously exist within SCANOSS's standard offering.

The collaboration also expanded the algorithm dataset. The vendor contributed additional cryptographic algorithm definitions that were not previously covered, and SCANOSS incorporated these into its detection engine. When benchmarked against CryptoDetector, the tool the vendor had previously relied on, SCANOSS detected everything CryptoDetector identified, and more.

The practical output was a new Export Control API feature allowing teams to submit a PURL — a package identifier — and receive a structured list of every cryptographic algorithm detected in that component, including strength values. This made ECCN classification a single-query process rather than a manual one.

THE OUTCOME

Export compliance automated, detection capabilities expanded

With these enhancements in place, the vendor was able to meet its ECCN export compliance requirements without the manual overhead that had previously created a bottleneck. Cryptographic algorithm detection across the full codebase — both open source and proprietary — became an automated, repeatable process.

The collaboration also had a broader effect. The algorithm definitions contributed by the vendor and incorporated into SCANOSS's Encryption dataset are now available to all users, strengthening the detection capabilities of the tool beyond this single engagement.

> **A single query returning a comprehensive list of every cryptographic algorithm in use, across all source files, regardless of origin.**

Facing similar challenges with cryptographic visibility and export compliance? Contact us to find out how SCANOSS can help.

sales@scanoss.com