CASE STUDY

Automating Crypto Audits in the Development Build using CS Analyzer

Problem: Expensive Code Review

Our client, a world leader in financial services, has an internal consulting team covering 6 large business projects, representing at least 35 applications from banking and retail segments. The cryptography in this code has to be reviewed by the team to maintain compliance at least once a year. Each year, this activity represents an estimated 105 person days (PD) of work, both from the team members and from external consultants.

Solution: Scaling Cryptography Expertise

A very deep knowledge of cryptography and related protocols is required to understand and analyze applications. Automated tools are prerequisite because manual methods cannot discover what types of cryptography and key management are used. Aside from the significant cost of this process, it mobilizes a lot of internal resource that could be leveraged for other value-added projects.

CS Analyzer DevOps Integration

Cryptosense Analyzer in SaaS, was deployed for all 6 projects, integrated via a Jenkins plug-in into the CI/CD pipe-line. This provided a continuous overview of crypto compliance during development process.

How CS Analyzer Works

CS Analyzer traces all crypto calls made within each application in run-time. Its analysis engine then processes the traces and identifies crypto vulnerabilities at scale inside the code.

Reports indicate how to correct the flaws and show passed crypto as well as vulnerabilities. Each of the 6 projects has its own work space where analysis and remediation data is stored. Progress can be tracked over time. Traces are also generated during QA tests and confirmed before every release of an application using CS Analyzer reporting.

Main Benefits of the Solution

- Reduces the time spent by the team on cryptography code review (**from 105 PD/year to 17,5 PD/year**): reports are generated automatically and ready-for-use with auditors.
- Allows allocation of team members' time on greater value-added tasks.
- Reduces dependency on external cryptography consultants for maintaining compliance.
- Cryptographic compliance is continuously analyzed using CI/CD pipe-lines, providing overview for developers if there is non-compliance, reducing time to release application.
- Provides a better awareness of cryptography and related protocols.

Examples of Typical Flaws Found

CS Analyzer finds new flaws every day, mostly in proprietary code. Sometimes clients use the tool on widely used software, resulting in CVEs that become public, such as:

- CVE-2018-3210 Repeated IV in Java EE JSF
- CVE-2017-10356 Lack of encryption in JKS keystores
- CVE-2017-10345 Weak encryption in JCEKS Keystore
- CVE-2017-1000486 Weak encryption in Primefaces

"CS Analyzer helps us to streamline procedures connected with cryptography testing in our software, ensuring compliance with standards and reducing costs and time during the releasing process."

- Director IT Consulting & QA, International Financial Services Provider