FOSSID

CUSTOMER CASE STUDY

Business value through operational excellence, compliance, and risk management

Case study of how a leading Asian bank is leveraging FossID's technology to achieve business value through increased operational excellence while honoring standards fulfillment, software license compliance, and managing risk.

CUSTOMER

An Asian bank with several software suppliers

With operations in multiple countries, this Asian bank creates value through a portfolio of software-based products and services for both businesses and consumers. Their portfolio is regulated to a high degree and relies on state-of-the-art front and backend software platforms with high requirements on security, confidentiality, availability, and

CHALLENGE

Creating business value through operational excellence

With stringent requirements on security, confidentiality, availability, and sustainability, the bank needs to execute their operations as efficiently as possible while also minimizing risk.

As software is the primary enabler for creating business value, the bank needs to be in absolute control of what software platforms and components are introduced into their systems and to be aware of which commercial and open source licenses need to be honored. This is important for minimizing risk and possible liabilities. Since the software, to large extent, is built upon open source components, it is also important to monitor any security vulnerabilities and their remediation in the open source community.

The challenge is two-fold;

- Having the development team staying true to the bank's policies and processes around software development, and particularly the inclusion of free and open source components, and
- Ensuring that any software delivered into the organization from third parties is compliant with said policies.

SOLUTION

Software composition analysis tools and services from FossID

The bank was mature in the sense that policies and processes were already in place, and there was great organizational awareness around open source compliance, but the software base had grown too rapidly; partly as a consequence of recent mergers and acquisitions. No one had full control of what the codebase looked like, so the decision was made to have FossID conduct a blind audit of their codebase which would provide them a comprehensive and detailed understanding of their code composition via the creation of a complete Software Bill of Materials (BoM). The BoM is a list of

proprietary and open source components in the bank's source code and comes with a comprehensive set of reports listing all the findings in open data formats (SPDX).

The FossID blind audit is performed remotely and, for security and confidentiality reasons, the source code is never exposed to anyone outside of the bank. To initiate the process, the bank uses a tool to create a digital signature of the code, and that signature is sent securely to FossID. The signature cannot be reverse engineered but can be used by FossID to create the BoM.

With the SBOM the bank has a good starting point for understanding their software composition. Not only do they understand which open source components are in use, but the audit also shows files and snippets of code that originate from non-approved sources according to the open source policy.

After remediating some of the findings in the blind audit and seeing the value of the process, the bank chose to license the FossID software scanner and integrate it into their development process to automatically scan old and newly committed code; including that of suppliers regularly. The bank also introduced a set of rules whereby the scanner would send automated alerts to appropriate personnel about policy breaches and security vulnerabilities.

RESULT

Lightweight deployment and accurate results

FossID's machine learning-powered scan engine and comprehensive knowledge base brings accurate, uncluttered scan results and keeps manual intervention at a minimum. The intuitive interfaces, ease of integration, and light-weight deployment adds to seamless operations. The comprehensive, dynamic reports provide detailed insight into the source code, so that policy breaches and security vulnerabilities can be avoided.

This enables the bank and its developers to leverage the full power of open source software for maximum business and bottom-line value for itself and its customers. When developers have clear policies, processes, and tools to rely on, they are enabled to make effective and efficient use of their time for the benefit of the organization.

BENEFITS

- Greater operational excellence
- Better risk management
- Greater compliance and standards fulfillment
- Lower exposure to security vulnerabilities

FossID offers a state-of-the-art open source scanner that integrates in your development process seamlessly and detects pieces of Free and Open Source Software (FOSS) in your code base, from entire components to code snippets. FossID's software uncovers license obligations and compliance issues so that you can focus on creating great products.

www.fossid.com
@fossid_ab
linkedin.com/company/fossid-ab

GET IN TOUCH!

Discover all FossID products and services at **www.fossid.com**

FossID AB
Gåsgränd 3
111 27 Stockholm
Sweden

FossID K.K.
1-10-3-200 Roppongi, Minato-ku
Tokyo 106-0032
Japan