onward SECURITY
a DEKRA company

Free Trial

HERCULES
SecSAM

Security Assessment Management System for OSS

SecSAM is a Security Assessment Management platform that can effectively solve open-source software(OSS) risk control and Software Bill of Materials (SBOM) management and other complex issues. Utilizing Cybersecurity Bill of Materials (CBOM) as the technical framework for risk assessment, it integrates the third-party software vulnerability reports (such as source code scanning and vulnerability scanning report), the CI/CD tool that interfaces with the problem tracking management system, and allows users to manage, track, and warn, in a more flexible and convenient way on the basis of secure development.

CYBER SECURITY EXCELLENCE AWARDS WINNER 2023

2023 Cybersecurity Excellence Awards
- Open Source Security - ASIA Gold Winner

2022 GLOBEE AWARDS BRONZE WINNER INFORMATION TECHNOLOGY

2022 IT World Awards
- Hot Technology of the Year
- Security Software

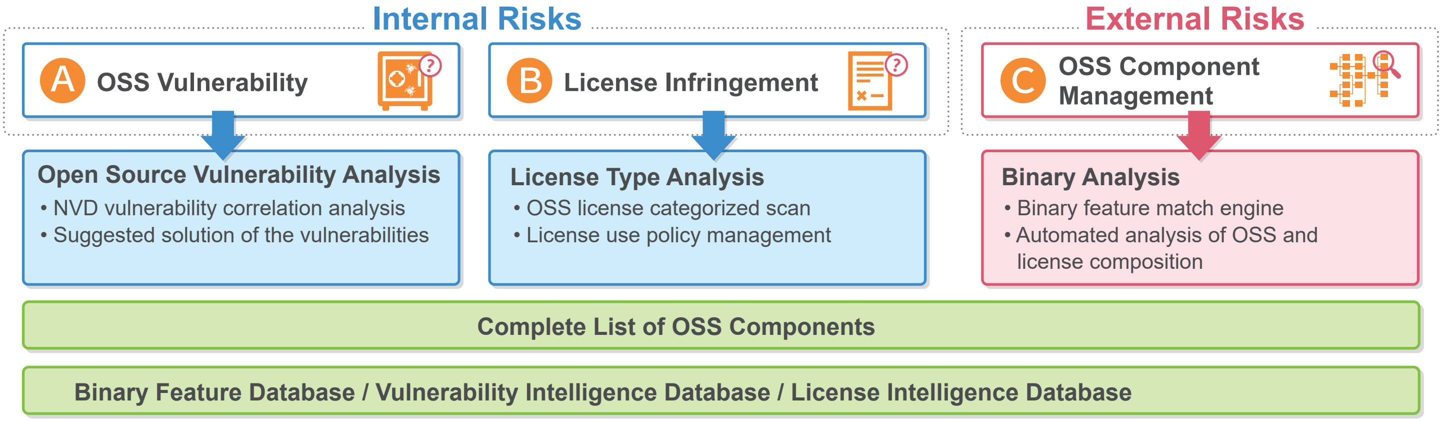
Features

- **Manage Vulnerability Risk Rating Based on SBOM and CBOM structure:**
  Through the establishment and maintenance of SBOM, analysis of CVE, daily automatic update of vulnerability information, vulnerability report management, and tracking mechanism to effectively monitor the vulnerabilities of products and open-source suites to achieve complete CBOM management.
- **Easily analyze OSS components without source code:**
  Through firmware analysis (Firmware Analysis/Binary Analysis) technology, SecSAM analyzes the firmware provided by the 3rd party vendor without source code, supports CPE standard format, and discovers the OSS composition of the product.
- **Support OSS and 3rd party suite license analysis:**
  Automated analysis of OSS license mode, such as GPL, Apache,LGPL, and more, SecSAM helps customers avoid license disputes.
- **Improve efficiency of vulnerability fix with CI/CD integration:**
  SecSAM can Integrate with the current development and management system and tool to perfect CI/CD procedure.

Benefits

- **Easily create SBOMs:**
  By utilizing automation technology to analyze the composition of OSS in software, SecSAM creates the basis of risk management and improves the security of software supply chain.
- **Quickly investigate and resolve vulnerabilities:**
  Through CBOM, SecSAM manages and tracks vulnerabilities in the stages of development, testing, and maintenance, and integrates CI/CD development tools to facilitate instant resolution.
- **Avoid intellectual property disputes:**
  SecSAM's open source license analysis can check the license mode of OSS components to avoid affecting the interests of corporate intellectual property rights.
- **Comply with global IoT security standards:**
  By adopting the global standard for IoT security, ioXt Likelihood to assess product risks rating. SecSAM complies with international standard requirements and master product risks.

Solution of OSS Risks



Internal Risks

External Risks

A OSS Vulnerability

B License Infringement

C OSS Component Management

Open Source Vulnerability Analysis
- NVD vulnerability correlation analysis
- Suggested solution of the vulnerabilities

License Type Analysis
- OSS license categorized scan
- License use policy management

Binary Analysis
- Binary feature match engine
- Automated analysis of OSS and license composition

Complete List of OSS Components

Binary Feature Database / Vulnerability Intelligence Database / License Intelligence Database

Contact us - contact@onwardsecurity.com   Learn more at - www.onwardsecurity.com

Specification

Function	Description	Cloud Version	On-Premise Version
Account management	Project and user account quantity	10 users / 25 projects	Unlimited users and projects
Software composition	Supporting CPE, the test report imported to manage the OSS component list	Y	Y
3rd party software vulnerability analysis	Daily scanning the latest CVE and automated analyzing risk severity level including 150K vulnerabilities (CVE), 20K vendors, and 500K product info	Y	Y
Vulnerability report and suggested solutions (NVD)	Providing the detailed vulnerability report and an according solution	Y	Y
Advanced SBOM management module	Producing international standard of SBOM (SWID) and advanced editing mode	Y	Y
CI/CD integration	Supporting mantis reports import and export	Y	Y
On-premise	Providing on-premise software and server	✕	Y
Firmware scan (Optional)	The firmware scan to automate analyze the product components, CVE, license types, and more, providing diverse firmware scan data plans	6GB / Year	1GB / Day

* The above specs are one-year licenses for the cloud versions
* Additional Firmware scan data plan can be provided upon request

Supported File Formats of Firmware Scan	
Platforms & File System	• Package Type : Docker, Android, iOS, Ubuntu, openSUSE, Fedora, CentOS, Debian, Vxworks, QNX • File System : Cramfs, ext, JFFS2, romfs, squashfs, yaffs2, ubifs, Android Sparse
Programming Languages	• C, C++, C#, Java, JavaScript, Python, Go
CPU Architecture	• Intel, Power PC, ARM, Sparc, MIPS
Compress Format	• 7z, chm, lzip, rzip, lzma ,tar, cpio, lzop, upx, ar(Archive in Unix), gzip, msi, xar, bzip2, zip ,cab, lrzip, rar, arj
File Format	• elf, Android Dex/Odex, APK (Android Application Package), Android Resource, IPA for iOS and iPad OS, Java class files, Windows PE(.exe), bFLT, symbolic links, Linux Kernel, Linux Kernel Module, Linux Shared Object, Java Archive, Intel HEX, SREC, uBoot