onward SECURITY
a DEKRA company

HERCULE SecSAM

开源软件风险管理系统

SecSAM 可有效解决开源软件 (OSS) 风险管控及软件物料列表 (SBOM) 管理等复杂问题，并以软件风险列表 (CBOM) 为风险评估技术框架，整合第三方软件漏洞报告 (如源码扫描、漏洞扫描报告等)，对接问题追踪管理系统的 CI/CD 工具， 让使用者于安全开发基础上，以更弹性与便利的方式进行管理、追踪及警示。

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

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

产品特色

- **采用 SBOM 与 CBOM 架构管理弱点风险评估：**
  藉由 SBOM 的建立与维护，分析 CVE 漏洞，协同每日自动更新漏洞信息、漏洞测报管理及追踪审核机制，有效监控产品与开源套件漏洞，实现完整的 CBOM 管理。
- **毋须源码即可轻松分析开源软件组件：**
  透过固件分析 (Firmware Analysis/Binary Analysis) 技术，毋须源码即可分析第三方供应商提供的固件，并支持 CPE 标准格式，发掘产品开源软件组成。
- **支持开源软件与第三方套件授权分析：**
  自动分析开源软件授权模式，例如：GPL、Apache、LGPL 等，协助客户避免授权争议。
- **整合 CI/CD 系统提升修补效率：**
  可整合已有的开发管理系统与工具，完善 CI/CD 流程。

产品效益

- **轻松建立软件物料列表：**
  利用自动化技术分析软件中的开源软件组成，建立风险管理的基础，提高软件供应链安全性。
- **提升产品漏洞处理时效：**
  透过软件风险列表，在开发、测试、运维等阶段进行漏洞管理与追踪，并整合 CI/CD 开发工具，以利实时修补。
- **协助避免知识产权争议：**
  开源授权分析可协助检查开源软件组件之授权模式，避免影响企业知识产权的利益。
- **符合国际物联网信息安全标准要求：**
  采用国际物联网信息安全标准组织 ioXt 联盟的产品风险评估方法，可符合国际标准要求并掌握产品风险等级。

开源软件风险解决方案

内部风险

A 开源软件漏洞

Open Source Vulnerability Analysis
- NVD漏洞关联分析
- 提供漏洞建议解决方案

B 侵权问题

License Type Analysis
- OSS授权分类扫描
- 管理授权使用政策

外部风险

C OSS清单管理

Binary Analysis
- Binary特征值比对引擎
- 自动分析开源软件与授权组成

完整开源软件列表

Binary特征资料库 / 漏洞信息数据库 / 授权信息数据库

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

产品技术规格

功能	說明	云端版	就地部署版
使用者帐号及可管理专案数量	项目数量与使用者账号限制。	10 使用者 /25 项目	使用者及专案数量无限制
软件组件组成管理	支援 CPE、测报导入功能，进行开源软件清单管理。	Y	Y
第三方软件漏洞分析	每日扫描最新漏洞与信息，自动分析风险严重程度，漏洞数据含超过 15 万笔 CVE 漏洞、2 万个厂商与 50 万个产品信息。	Y	Y
漏洞报告及建议解决方案 (NVD)	提供详细的漏洞报告及相应解决方案。	Y	Y
进阶 SBOM 管理模组	支援产出国际标准之 SBOM(SWID) 及进阶编辑模式。	Y	Y
CI/CD 整合	支持 mantis 报告导入导出。	Y	Y
本地部署	提供本地部署软件及主机服务器。		Y
固件扫描流量	可透过固件扫描自动分析产品中之组成元件、CVE 漏洞、授权种类等等资讯。提供不同的漏洞扫描流量方案。	漏洞扫描 6GB / Year	1GB / Day

* 以上规格皆为云端版一年用户许可证
* 固件扫描流量可依需求提供其他方案

固件扫描支持的文件格式	
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