onward SECURITY
a DEKRA company

DEKRA

HERCULES

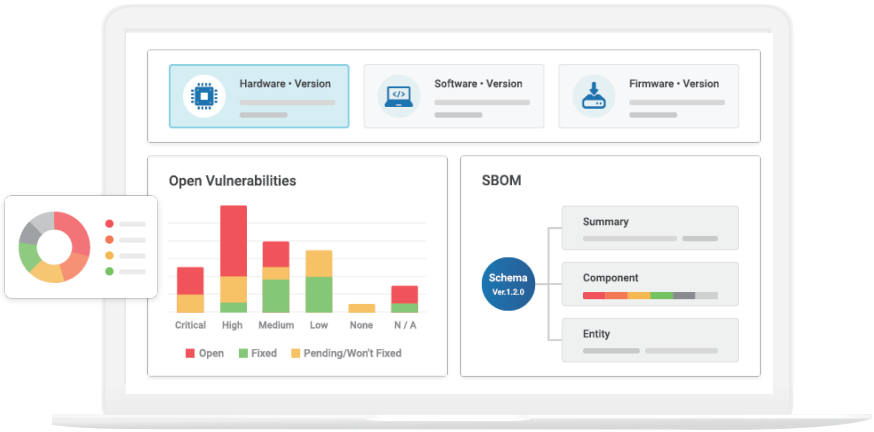
SecSAM 开源软件风险管理系统

轻松找出产品中开源软件的潜在风险

CYBER SECURITY EXCELLENCE AWARDS WINNER 2023

2023 Cybersecurity Excellence Awards
开源软件安全金奖

HERCULES SecSAM 开源软件风险管理系统可有效管理开源软件 (Open Source Software, OSS) 的风险，通过分析产品组成并建立软件物料清单 (SBOM)，藉此找出并管理项目 (产品) 中第三方组件的漏洞、授权等问题，并提供建议的漏洞修复方案，亦可接入问题追踪管理系统进行 CI/CD 的整合。



如何选择安全的 Open Source 组件

美国政府针对软件供应链安全已下达行政命令。未来通过软件物料清单进行供应链管理已势在必行，其中开源软件组成复杂的特性，使其成为软件供应链管理中极为重要的一环。

Gartner

未来两年内，软件购买者在购买产品时，会要求厂商提供软件物料清单 (SBOM)

找出开源漏洞并提供修补建议

通过持续性的漏洞分析、警示，协助团队提早发现所需处理的信息安全风险及授权问题，在设计阶段初期即可处理漏洞，或使用更安全的第三方组件，降低后续修补时间及成本。

分析开源组件授权

通过固件扫描自动分析产品中第三方组件的授权类型，例如：GPL、Apache、LGPL 等，协助客户避免授权争议，保护企业知识产权。

onward SECURITY a DEKRA company

DEKRA

SecSAM 六大功能

固件扫描

通过固件扫描进行软件溯源、分析软件供应链组成，无需源码即可分析软件中的第三方组件组成。

OSS 清单管理

持续性的管理产品项目中的 OSS 清单，通过 SecSAM 的安全组件选择功能，协助开发者选用安全、合适的组件进行开发。

新闻模组

每日收集 70 个以上的主流信息安全新闻网站资讯，归纳分析与产品相关的内容并进行警示，快速通知最新信息安全事件。

漏洞分析

提供超过 1,600,000 个的已知弱点资料库，与 6,900,000 个第三方组件风险资料，自动分析产品中的高风险清单，并提供建议方案。

CI/CD 整合

通过问题追踪文件或提供标准 API 接入等模式，进行产品的持续开发整合流程，让使用者不需花费过多时间进行繁琐的操作。

SBOM 管理

藉由 SBOM 的建立与维护，分析 CVE，协同每日自动更新漏洞信息、测报管理追踪审核机制，有效监控产品与开源组件漏洞，并提供 SBOM 模板编辑功能，可自行定义符合需求的 SBOM 文件。

轻松进入安全开发的正向循环

1 建立项目

通过固件扫描辨识合作厂商组件与开源组件组成，建立产品开源组件清单。

2 安全设计评估

- 开源软件组件选用
- 开源软件漏洞风险评估
- 开源软件授权风险评估

3 开发流程整合

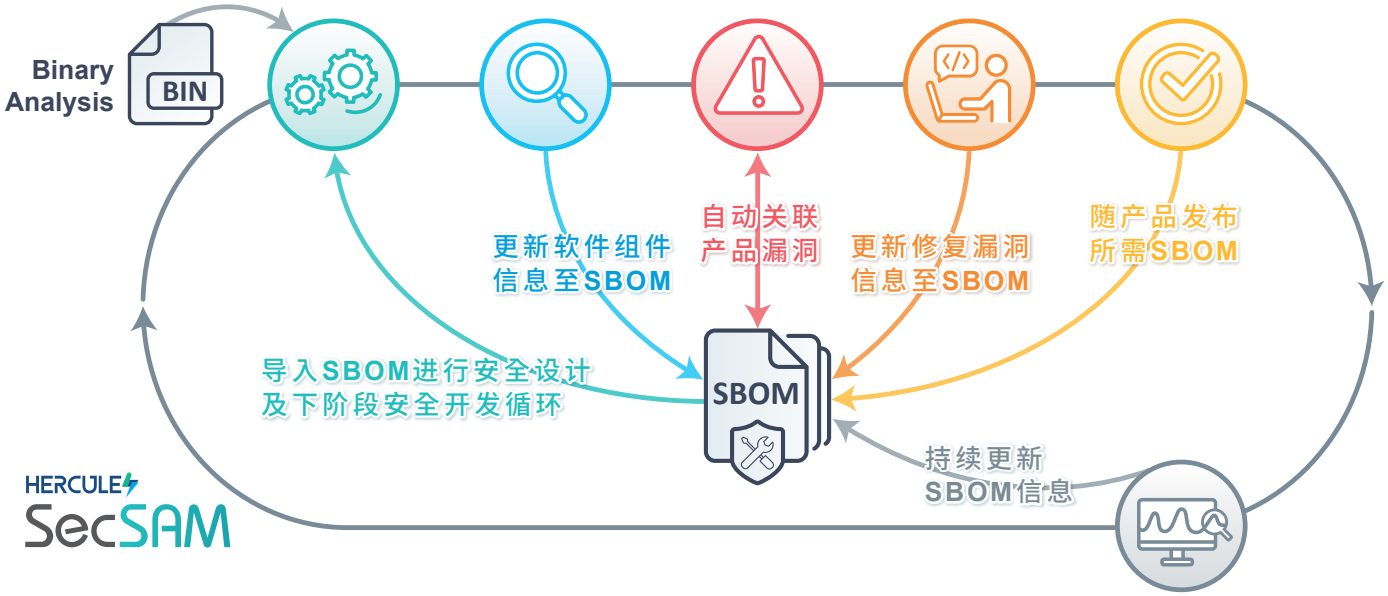
CI/CD 漏洞修复&追踪

mantis BUG TRACKER

Jira

4 项目发布

- 项目报告
- SBOM 发布



仲至信息科技 (DEKRA 德凯集团成员)

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