

Software Risk Manager

简化企业级AppSec项目管理

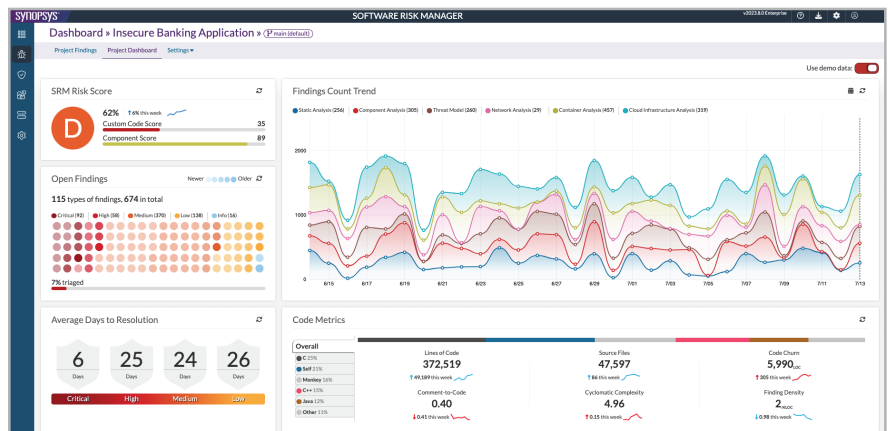
概述

Black Duck Software Risk Manager™是一款部署在本地的应用安全态势管理 (ASPM) 解决方案, 能够帮助安全和开发团队简化应用安全工作流, 提升风险控制能力。它将策略、测试编排、问题关联以及内置的静态应用安全测试 (SAST) 和软件组成分析 (SCA) 引擎结合在一起, 以智能且一致的方式将整个软件开发生命周期 (SDLC) 中的安全活动整合在一起。通过Software Risk Manager, 安全和开发团队可基于单一可信数据源做出明智的决策, 并大规模交付弹性应用。

Software Risk Manager能够消除孤岛并提供可操作的洞察

通过将透明、效率和可追溯引入应用安全 (AppSec) 工作流, Software Risk Manager为整合SDLC各阶段的检查奠定了必要的基础。Software Risk Manager为扩展测试、修复和风险管理提供了以下关键功能:

- 与超过135种安全工具集成 —— 超过了市场上任何其他的ASPM工具
- 集中管理扫描前和扫描后的策略
- 内置业界领先的Black Duck SAST和SCA测试引擎
- 支持20多项合规标准
- 可定制、可扩展的关联规则
- 与常用的问题跟踪工具和开发者工具 (包括 Jira、ServiceNow、Azure DevOps、GitLab、GitHub、Jenkins、TeamCity和Bamboo) 以及Visual Studio、Eclipse、Visual Studio Code和IntelliJ的IDE插件双向集成
- 16种内置的开源测试工具 —— 自动检测语言并推荐合适的工具



Software Risk Manager仪表板上显示的应用安全测试结果和性能指标

主要优势

查看中央AppSec记录系统

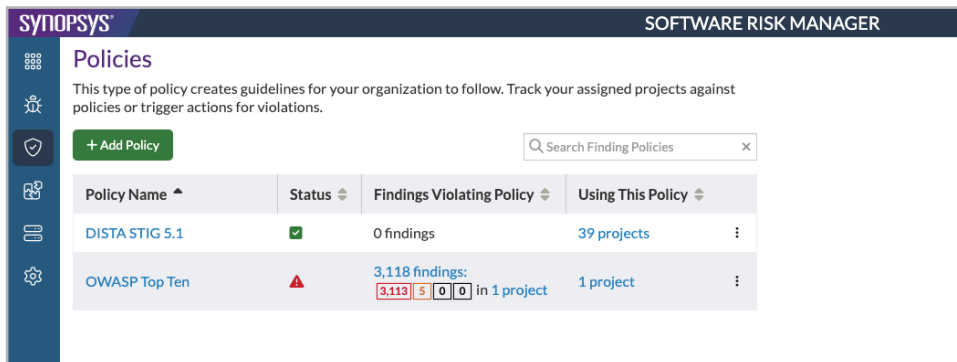
- 将所有手动和自动测试结果汇总到跟踪所有AppSec测试活动、安全数据和策略的记录系统中,让您在SDLC的每个阶段都能清晰地了解应用安全态势
- 自动关联来自不同测试源的结果并消除重复,以提供统一的用户体验,更方便您查看问题并对问题进行优先级排序
- 支持超过135种最常用的安全测试工具,包括SAST、SCA、DAST、IAST、InfraSec和威胁建模,以及针对移动设备、容器和云基础架构的测试
- 自动选择最适合贵组织代码库的AppSec工具
- 通过内置SAST和SCA的自动导引,动态发现SCM库、应用以及相关的开发人员和安全用户

加速分类、测试和修复 workflow

- 通过风险的统一评估自动识别并优先处理关键问题
- 与问题跟踪系统双向同步,因此可将高优先级漏洞直接发送给开发人员,包括精准指向代码行的链接
- 内置SAST和SCA引擎能够快速准确地检测源代码和开源代码中的漏洞,预设规则基本无需设置即可完成所需的测试 workflow
- 根据语言、漏洞类型和来源,为开发人员提供上下文相关的修复指导,并根据历史趋势推荐修复操作
- 显示分支级别的安全活动,使开发人员能够高效地测试修复方案,降低构建中断的频率
- 集中编排Black Duck (内置或独立) 或第三方工具的扫描

集中展示与治理风险

- 针对所有项目和代码源 (定制构建、第三方和开源) 的风险评分、测试结果和关键性能趋势提供360°全方位视图
- 将测试结果映射到监管合规标准 (包括NIST、PCI、HIPAA、DISA和OWASP Top 10),并提供重大违规事件的审计报告
- 同时提供基于UI和API的 workflow,以创建、实施和监控跨软件资产的安全策略
- 允许安全团队为多项事务制定风险阈值,例如问题类型、期望的应用安全测试工具、修复时间SLA以及向开发负责人发送的必要通知等



可按项目、来源和严重程度来跟踪违反策略的事件。

Black Duck与众不同

Black Duck® 提供业界最全面、最强大、最值得信赖的应用安全解决方案组合。我们拥有无与伦比的专业知识和经验,来帮助世界各地的组织机构快速保护其软件,在其开发环境中高效集成安全性以及使用新技术进行安全创新。作为软件安全领域公认的领导者、专家和 innovator, Black Duck拥有您构建可信软件所需的一切。如预了解更多信息,请访问www.blackduck.com。