BLACKDUCK

黑鸭 HUB
查找并修补开源漏洞

黑鸭 Hub 可帮助安全和开发团队识别并规避应用组合中的开源相关风险。

使用黑鸭 Hub 来：

- 扫描代码以发现在用的具体开源
- 自动将在用的开源与已知的漏洞进行映射
- 分类 – 评估风险并对漏洞进行优先排序
- 计划并追踪修复操作
- 识别许可证和社区活动

虽然其他静态分析解决方案专注于发现那些开发人员在编写代码时所产生的代码相关漏洞，但这些技术只能识别长期报告的一小部分漏洞。像 Heartbleed、Shellshock、Poodle 和 Ghost 这样的漏洞已突显了常用开源组件所能带来的风险水平。这些广为人知的漏洞仅占到每年报告的 4000 多种开源漏洞的一小部分。

只有黑鸭子软件能够提供：

- 最为全面的语言覆盖和开发工具集成
- 业界最完整的开源软件知识库
- 集成的修复追踪和管理

安全始于可见性

了解代码库中使用了哪些开源是保护开源的第一步。可见性意味着不仅要了解库中使用了哪些开源，而且要了解它们在哪里使用及如何使用。黑鸭 Hub 可持续扫描您的代码来识别具体的开源库和版本。通过从国家漏洞数据库 (NVD) 和更全面、更及时的漏洞数据库 VulnDB 中定期更新，黑鸭® 知识库™ 将开源库与有关漏洞、许可、社区活动和版本的元数据进行映射。

黑鸭 Hub 持续扫描您的项目以发现新引入的开源，帮助您管理安全漏洞，以防它们演变成问题。通过它，您可以查看漏洞并进行优先排序，指定修复日期，并追踪其解决进度。黑鸭 Hub 可针对您应用中所用的开源库来自动监视后期报告的新漏洞，让您能够快速应对新发现的漏洞。

黑鸭 HUB 的主要特点

快速扫描和识别	了解您的代码。Hub 的自动扫描功能可识别和清查您应用和容器中的所有开源，包括软件包文件中未公布的组件。
构建工具集成	使用 Jenkins 插件将 Hub 与您的持续集成 (CI) 环境相集成，以进一步自动化开源材料清单的扫描、识别和填充。
可自定义的材料清单 (BOM)	使用可编辑的开源 BOM 来保持代码的可见性，组合来自自动化扫描、构建工具和软件包管理器清单及手动录入的结果。
全面的开源数据库	黑鸭知识库™ 是世界上 100 多万开源项目的最全面的数据库，可对您项目内所用的开源实现精准的发现、可靠的识别及实时的漏洞映射。
自动漏洞映射和警报	识别与您应用中的开源相关的已知漏洞，并在报告了会影响到您的新漏洞时收到警报。使用 VulnDB 附加选项来获知更多漏洞及获得提前通知。
漏洞研究工具	根据 CVE 编号、漏洞 ID 或名称来搜索漏洞，以从多种来源获知漏洞信息，包括国家漏洞数据库 (NVD) 和 VulnDB。深入探究任何漏洞的详情，以进一步分析风险，识别所有受影响的内部项目版本，锁定源文件，及查看/追踪修复流程。
修复追踪	追踪单个项目内的计划内和实际漏洞修复进度。通过 CSV 导出功能将修复报告轻松导入到第三方工具中。
政策管理	制定针对开源项目、许可证类型和漏洞容忍度的政策。快速识别政策违规并根据项目和组件来管理意外情况。
风险控制面板和报告	使用易于理解的安全、许可证、社区活动风险，以及修复进度控制面板和报告，分析各个项目之内和之间的风险。
IBM APPSCAN 企业集成	通过结合使用黑鸭 Hub 和 IBM AppScan 时所生成的单个控制面板，查看和管理整个开源和自定义代码中的应用安全风险。

关于黑鸭子软件

全球的组织都使用黑鸭子软件的业界领先产品来自动化其保护和管理开源软件的流程，消除与安全漏洞、开源许可证合规和营运风险相关的痛苦。黑鸭子软件的总部位于马萨诸塞州伯灵顿，并在加州圣何塞、伦敦、法兰克福、香港、东京、首尔和北京设有办事处。有关详情，请访问 www.blackducksoftware.com。

联系方式

欲知详情，请联络：sales@blackducksoftware.com 或 +1 781.891.5100
有关详情，请浏览：www.blackducksoftware.com