imperva

功能简介

数据风险分析

在产生损失前阻止数据泄露

数字化商业模式有赖于数据带来的机会，但与数据相关的金融风险的规模和范围也在不断扩大。伴随指数式增长的数据，正常的数据访问比以往任何时候都要多，这使得判断是否接受数据访问请求变得越来越困难。此外，安全团队经常疲于应对海量报警，更不消说其中夹杂着大量误报了。不当的数据和被忽略的安全告警事件，有可能会导致灾难性的数据泄露，相应的后果非常严重，包括：违规处罚、失去市场份额、股价下跌、声誉受损等等。

要想降低数据风险，就必须通过高级安全分析来识别存在风险的数据活动和不良的操作，获得数据使用方面的可应对的情报，加速潜在泄露的检测和调查。

数据风险分析

作为Imperva 数据安全方案 (Imperva Data Security) 的一项主要功能，数据风险分析可提供能够立即采取行动的安全情报。与用户行为分析工具不同，Imperva数据风险分析通过分析用户行为和数据访问活动来创建情境行为基线。通过学习和关联数据访问详情（例如：谁在什么时候接触了什么敏感数据，以及采用何种方式访问和使用数据），Imperva数据风险分析可以准确识别出重要数据所面临的主要威胁。可以按照优先级排序，从众多干扰项中筛选出少量需要立即调查的高风险事件。该功能使得安全团队能够更加有效地发觉并遏制潜在的数据泄露行为。有籍于此，首席信息安全官员(CISO)和首席信息官(CIO)能够更有信心地承诺杜绝数据泄露。

主要功能

- 通过机器学习在多至数十亿的审计事件中检测出关键事件
- 同类分组分析，揭示可疑的用户数据访问
- 以简明的语言提供可应对的情报
- 仪表板上可执行操作，有助于加速威胁调查和响应
- 开箱即用的分析功能，仅需些微调整

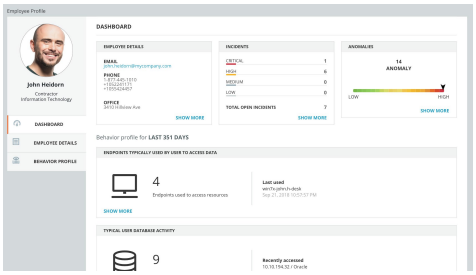

图1：仪表板提供了安全团队调查可疑用户数据访问所需的可见性，这些数据访问可能预示着数据泄露。

识别存在风险的数据活动，获得可应对的情报

查明数据的真正风险

要想减轻数据泄露的风险，必须能够检测和查明数据面临的实际威胁。数据风险分析DRA通过机器学习和行为分析来揭示可疑的数据访问和不良的操作习惯。它可以自动处理大量数据库和文件活动日志并将其关联，从而让重要的事件浮出水面。通过分析用户和数据访问情境，并不断了解各种详细情况，包括用户是谁、他们一般采用什么方式访问数据和使用企业数据等，分析引擎可以创建用户的行为基线，帮助分辨“正常”的行为和“正常但不正确”的行为。

优先处理最重要的事件

数据风险分析通过应用分组和评分算法，对关键事件进行优先级排序。事件的风险评分均基于复杂的算法，会将多种变量纳入考量：敏感数据量、特权帐户、普遍性等等。如果事件彼此相关（例如：所有事件都关联了同一用户帐户，或者同一服务帐户遭到多个用户滥用），那么这些事件将被归为同一类问题。因此，只有少数高风险事件才会浮出水面，而发送至SIEM的警报更是少之又少。

加速并简化事件响应

了解敏感数据是否被滥用，或者用户不当访问，数据威胁调查通常需要深入的数据库知识。IMPERVA DRA数据风险分析以简明的语言解读安全事件，并提供可应对的情报和建议，安全专业人员能够快速了解数据环境中发生的事情，甚至在不依赖数据库知识的情况下也能对威胁做出响应。DRA的仪表板直观且易操作，包含了安全专业人员开展调查所需的完整信息量和全部可见性。

总结

数据风险分析是Imperva数据安全(Imperva Data Security)产品的关键组件。它可以帮助安全团队检测并定位主要的数据威胁，对重要安全事件进行优先级排序，并提供可应对的风险情报和建议，帮助您加快威胁调查和响应。在数周而非数月时间，您就能够感受到该方案所带来的效益和变化。在造成真正的损害之前，您能够更加有效地应对数据泄露风险。

Imperva数据安全 (Imperva Data Security)

数据风险分析是ImpervaData-Security的关键组件，它可以降低数据泄露风险，同时实现数字化转型。该解决方案通过下列方式保障本地及云端的数据安全:

- 发现敏感数据
- 监测所有数据活动
- 阻止非授权的访问和活动
- 揭示存在风险的用户和可疑的行为
- 提供可应对的安全情报
- 对数据脱敏，以便在非生产环境中使用

欲进一步了解Imperva Data Security，请登录www.imperva.com。