imperva

功能簡介

資料庫風險分析

在成為漏洞之前發現風險

資料是必須加以保護的重要企業資產。對於資源及工具有限的企業安全小組來說，這可能是一項艱鉅的任務。

諷刺的是，許多安全工具有時也是問題的一部分。安全人員經常被大量的安全工具警報所淹沒，其中許多警報皆為誤判，這使得他們難以得知應該採取什麼行動，或從何著手。

為了更有效地降低資料庫風險，組織需要進階的安全分析，以幫助安全人員獲得針對威脅的可行性見解，並加速漏洞偵測。

資料庫風險分析

資料庫風險分析是 Imperva 資料庫安全的重要功能，它提供了可立即採取行動的安全見解。與典型的使用者行為分析工具不同， Imperva 資料庫風險分析透過分析使用者行為及資料存取活動來建立脈絡行為的基準線。藉由學習及連結資料細節，例如誰在何時接觸了哪些敏感資料，以及如何使用及存取資料。Imperva 資料庫風險分析可以準確地辨識資料的重要威脅並消除誤判的的異常狀況。不僅消除了噪音，同時也優先考慮少數需要立即調查的高風險事件，使安全小組能夠保持專注，更有效地遏制潛在威脅。

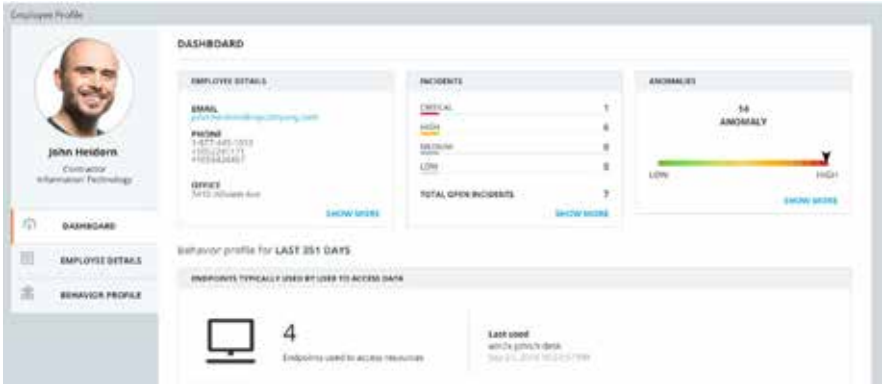

圖1：儀表板提供了安全團隊需要的可視性，以調查可能指出資料洩露的可疑使用者資料存取

主要功能：

使用機器學習在數十億個稽核事件中偵測重要事故

發現可疑使用者資料存取的同儕團體分析

以淺顯易懂的用語提供可行見解

幫助加速威脅調查及反應的執行儀表板

只需微調的開箱即用分析功能

提升員工效率的可行性見解

找出整個企業的資料風險

為降低整個企業的資料洩露風險，您需要能在所有敏感資料庫中偵測並找出對資料的威脅。資料庫風險分析利用機器學習及行為分析，找出可疑資料存取及其他安全分析遺漏的惡意操作。自動處理大量的資料庫活動日誌，並將它們與表面相關的威脅建立關聯。透過不斷了解使用者身份、平常存取資料庫的方式及使用企業資料的細節，分析引擎可建立脈絡行為的基準線，幫助區分僅查看一個資料庫日誌的正常行為，及查看所有日誌的異常行為。這是很難以人工作業實現的。

優先考慮最重要的事情

資料庫風險分析透過使用分組及評分演算法來確定重要事件的優先順序。根據複雜的演算法為每個事件分配一個風險分數，該演算法可考量各種變數，例如敏感資料量、特權帳戶、盛行率等。相關的事件（例如，它們都與同一個使用者帳戶有關，或者多名使用者濫用同一個服務帳戶）將被歸類為一項問題。因此，只會出現少數高風險事件，而發送到 SIEM（安全資訊及事件管理）的警報也會相對減少。

加速及簡化事故反應

調查資料威脅通常需要淵博的資料庫知識，以了解是否有任何敏感資料被濫用，或者使用者是否正不恰當地存取資料。資料庫風險分析以淺顯易懂的用語解釋安全事件，並提供可行性見解及風險脈絡，讓安全專業人員能快速了解資料環境發生了什麼事，即使對資料庫一知半解或是一無所知，也能對威脅做出反應。直覺易用的儀表板，包含了安全專業人員執行調查所需的所有可視性及資訊。

摘要

資料庫風險分析是 Imperva 資料安全的重要組成部分。其有助於安全團隊偵測及找出資料的重要威脅、優先考慮最重要的事情， 並提供可行性見解，使您能加速進行威脅調查及反應。不必等上數個月， 您可以在幾週內看到這些優點及改變。 Imperva 資料庫風險分析可幫助您在資料洩露風險威脅事件發生前，就及早發現並降低風險。

IMPERVA 資料安全

資料庫風險分析是 Imperva 資料安全的重要組成部分，可在實現數位轉型的同時降低洩漏風險。該解決方案可透過以下功能保護本地及雲端的資料：

發現敏感資料

監控所有資料庫活動

封鎖未經授權的存取及活動

發現危險的使用者及可疑的行為

提供可行的安全見解

掩飾非生產用的資料

Imperva 是分析師認可的網路安全領導者，致力於保護存放在各處的資料及應用程式的安全。

FAIRLINE
Quality Service Through Team Work

台北總公司
台北市內湖區
瑞光路583巷32號5樓
電話：02-2658-1818

台中辦事處
台中市北屯區文心路四段83號19樓301室

高雄辦事處
高雄市前鎮區一心二路128號9樓之1

Copyright © 2020 Imperva。版權所有