

Обнаружение угроз инсайдеров

Что такое угрозы инсайдеров



Общее описание

Платформы

- Кросс-платформенное решение

Сценарии использования Securonix

- Выявление инсайдерских угроз
- Выявление и предотвращение мошенничества
- Выявление и предотвращение кражи данных
- Выявление и предотвращение отслеживания ВИП-ов

Влияние на бизнес

- Прогнозируемое выявление угроз
- Уменьшение последствий ущерба
- Комплексный ответ угрозам и расследование
- Объективные отчёты о рисках и угрозах

Источники данных

- Журналы приложений и полномочия
- Кадровая/идентификационная информация
- Журналы прокси-серверов (опционально)
- Защита от утечек данных (опционально)

Соответствие требованиям стандартов и рекомендации по безопасности

- SOX
- PCI DSS
- HIPAA/HITECH
- FARC/NERC

Проблема: неправильные инструменты для работы

В организации сотрудники и подрядчики имеют значительное преимущество по сравнению с механизмами обеспечения первичной безопасности (например, межсетевыми экранами, средствами управления доступом и физическим контролем доступа), которые предназначены для защиты от внешних злоумышленников, а не доверенных инсайдеров. Кроме того, люди, работающие внутри организации или сотрудничающие с ней, осведомлены о существующих принципах и механизмах защиты и могут использовать эти знания, чтобы обойти её. Для того, чтобы противостоять этим преимуществам и реально бороться с внутренними угрозами, организациям необходимы расширенные возможности в организации таких сфер, как мониторинг на основе контекста, современная система выявления нестандартного поведения и расследование на базе анализа ссылок.

Решение: полностью готовая к работе платформа по выявлению и управлению угрозами со стороны инсайдеров

Решение Securonix создано для решения именно этих проблем. Все его возможности заключаются в готовом коробочном решении, которое не требует анализа многолетних данных и развёртывания проекта по обнаружению. Благодаря использованию специального целевого интеллектуального анализа данных, корреляции, совершенствования знаний и аналитики, решение Securonix обнаруживает не только пользователей с высокой степенью риска идентификационных данных, но высокорискованную активность, доступ и события в вашей организации, которые могут быть связаны с инсайдерской угрозой. Проще говоря, Securonix предоставляет аналитику инсайдерского риска. Это обеспечивается путем сбора и анализа разнообразных видов активности пользователей, систем, приложений, событий безопасности, физического доступа и даже телефонных разговоров, благодаря чему идентифицируется нестандартное поведение, связанное с кражей данных/неадекватного использования, мошенничества, или ИТ-саботажа. Помимо обнаружения, Securonix осуществляет непрерывный мониторинг, ранжирование, подготовку отчётов, а также предоставляет расширенные возможности расследования. Данное решение основано на передовой технологии, необходимой для осуществления полноценной программы управления инсайдерскими угрозами, которая будет сбалансировано управлять существующими системами безопасности и инвестиций вашей организации.

- Специально разработанная аналитика для быстрого, последовательного и качественного анализа по ключевым источникам
- Большой масштаб данных для поддержки интеллектуального анализа данных в реальном масштабе времени и обнаружения угроз крупным каналам данных
- Автоматизированная корреляция и обогащение информации об идентификации и угрозах по многочисленным внутренним и внешним источникам
- Групповой анализ поведения и доступа пользователей с аналогичными группами для автоматического выявления нестандартных отклонений
- Анализ поведения пользователей, аналогичных групп, учётных записей и систем для несигнатурного выявления инсайдерских угроз
- Наглядность риска данных и приложений для мониторинга внутренних угроз по отношению к целям
- Современная система ранжирования и визуализации для эффективного и непрерывного информирования об уровне инсайдерских рисков и угрозах

