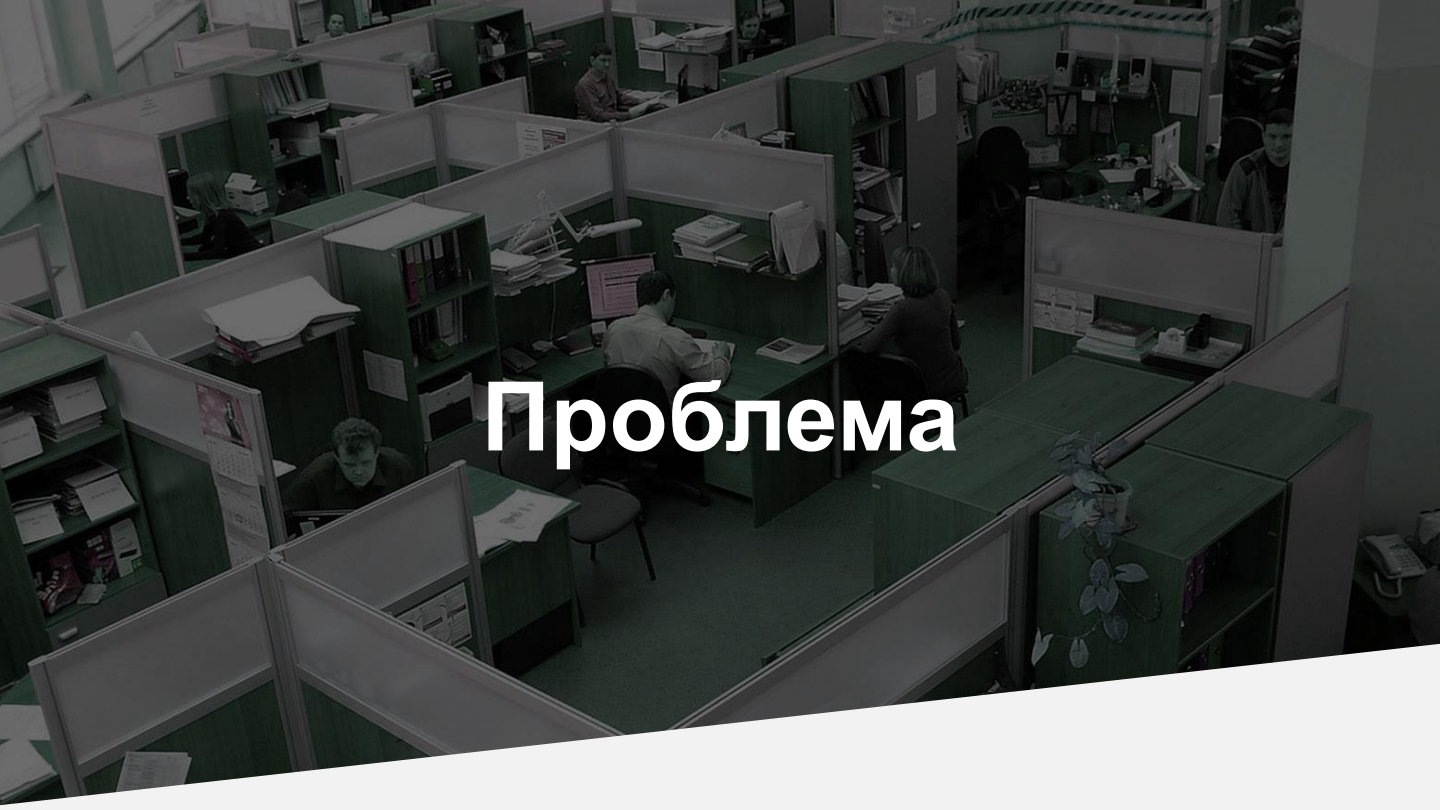
Определение инсайдерских угроз с помощью Teramind

Программное обеспечение для мониторинга сотрудников с мощными функциями обнаружения угроз изнутри и учетом рабочего времени

TERAMIND | SOFTPROM



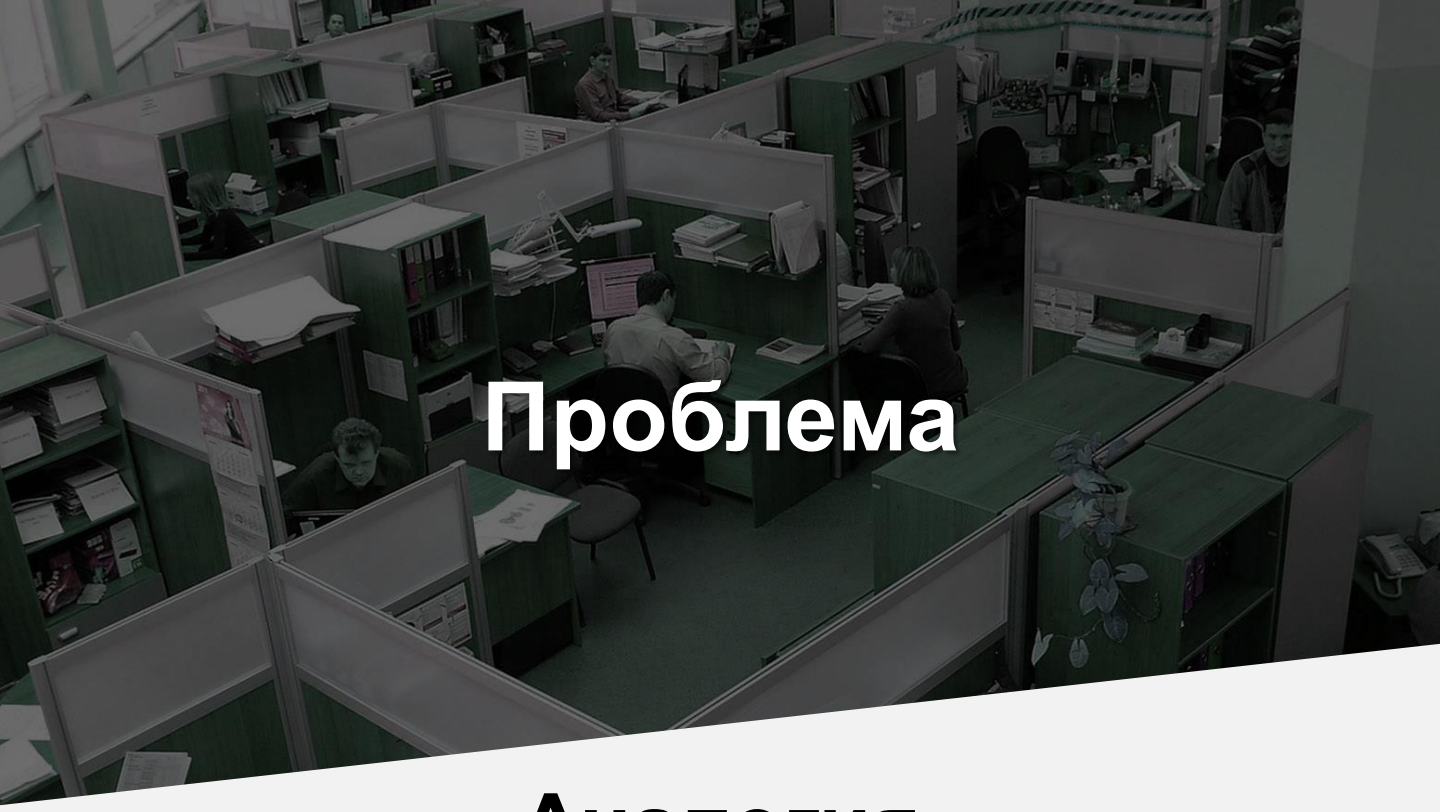
Проблема

Люди – это основа вашего бизнеса…

…а также причина 90% инцидентов безопасности*

- Пользователи являются причиной 90% инцидентов безопасности (Verizon Data Breach Investigations Report)
- “75% инсайдерских угроз остаются незамеченными.” (Source: CERT Insider Threat Center)
- “1 из 5 сотрудников готов продать свой пароль меньше чем за 1000$.” (SailPoint’s Market Pulse Survey)

TERAMIND | SOFTPROM



Проблема

Аналогия

Отделения банка

Работают с деньгами

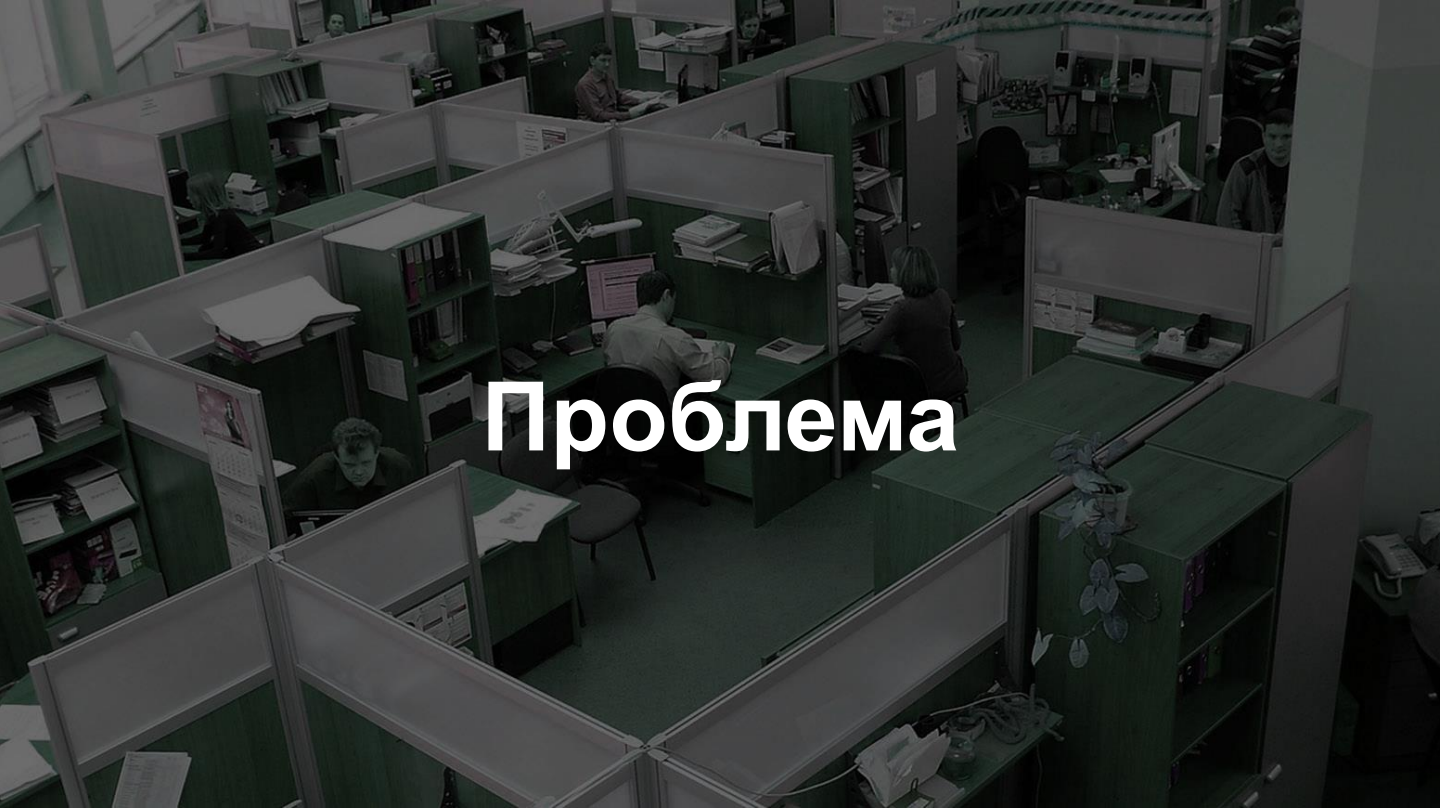
В отделениях всегда ведется видеосъемка.

Банковские сервера

Имеют контроль доступа

На серверах - нет

TERAMIND | SOFTPROM



Проблема

Куда смотреть?

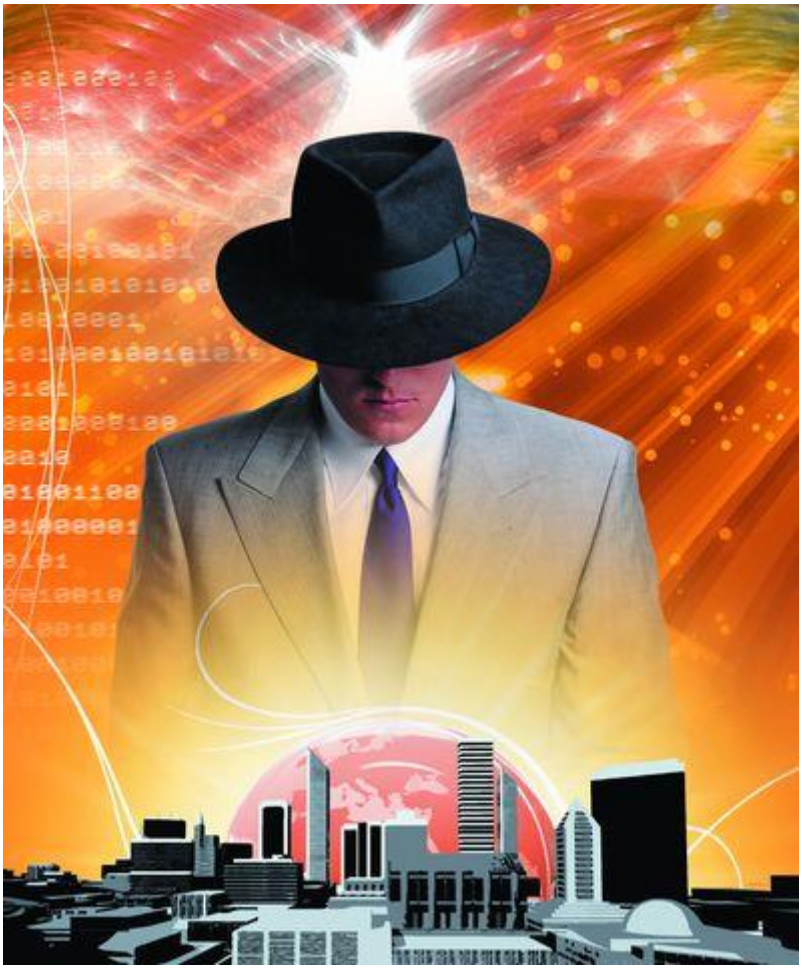
TERAMIND | SOFTPROM

Модели инсайдерских угроз

Небрежные пользователи

- Не придают значения риску
- Не исполняют политики ИБ
- Руководствуются «благими намерениями»

Модели инсайдерских угроз



Злонамеренные действия

- Хорошо прячутся
- Их сложно вычислить
- Их атаки внезапны и скрытны

Для уменьшения вероятности нарушений

Исправляйте поведение!

Небрежные пользователи

- Информировать – Вы нарушаете!
- Требовать подтверждение о прочтении
- Блокировать потенциально опасные действия

Злонамеренные действия

- Повышение админских привилегий
- Обход контроля безопасности
- Необоснованный доступ

TERAMIND SOFTPROM

Немного статистики

Сговор сотрудников является источником внутренних угроз

Основными причинами инцидентов, вызванных инсайдерской ситуацией, является сговор со стороны сотрудников и третьих лиц.

48% Инсайдерский сговор

17% Сговор сотрудников и третьих лиц

Привилегия сотрудника повышает риск утечки конфиденциальных данных

По данным онлайн опроса Cybersecurity Insiders 400 000 пользователей, опубликованного в отчете The Insider Threat 2018.

37% чрезмерная привилегия

34% рост количества конфиденциальных данных

Сотрудники являются серьезной проблемой безопасности

Предприятия соглашаются, что сотрудники - их самая большая слабость в ИТ-безопасности - согласно Лаборатории Касперского и B2B International более 5000 предприятий.

52% предприятия соглашаются, что сотрудники - самая большая слабость

Многие сотрудники проводят время на работе не эффективно

По данным FinancesOnline, 64% сотрудников используют рабочие места в целях, не связанных с работой, каждый день, а 85% сотрудников используют электронную почту в личных целях

64% Обзор сторонних сайтов

85% Использую email в личных целях

Teramind Starter

Программное обеспечение для мониторинга сотрудников с мощными функциями обнаружения угроз изнутри и учетом рабочего времени

TERAMIND | SOFTPROM

Teramind Starter: Упрощенный мониторинг сотрудников

Основные преимущества использования программного обеспечения для мониторинга сотрудников:

- Повышение производительности труда
- Сокращение административной работы
- Повышение вовлеченности сотрудников
- Определение технологических пробелов
- Обнаружение внутренних угроз
- Защита конфиденциальных данных и ресурсов
- Минимизация расходов
- Улучшенное управление временем
- Повышение безопасности сотрудников и организации
- Формирование корпоративной культуры

Teramind Starter: Функциональные возможности

Мониторинг в режиме реального времени:
Teramind Starter позволяет отслеживать всю активность сотрудников для таких системных объектов, как веб-сайт, приложения, социальные сети, чаты. Поиск в режиме реального времени для Windows, Mac, виртуальных ПК и терминальных серверов.

Отчеты об активности:
Подробные журналы фиксируют всю активность в Интернете/приложении, продолжительность, IP/URL. Отфильтруйте отчет для отдельных лиц, групп или отделов по продуктивным/непродуктивным или пользовательским категориям. Оповещения в режиме реального времени и отчеты о тенденциях показывают, какие правила были нарушены, когда, кем, какие действия были предприняты и их контекст.

Интеллектуальная система политик и правил:
Интеллектуальный анализ поведения может обнаруживать ненормальное поведение и внутренние угрозы, такие как посещение запрещенных веб-сайтов или подозрительное поведение с помощью отслеживаемого приложения. Создайте автоматизированные правила, чтобы предупредить или заблокировать сотрудника или уведомить руководителя, когда система обнаружит любую аномалию.

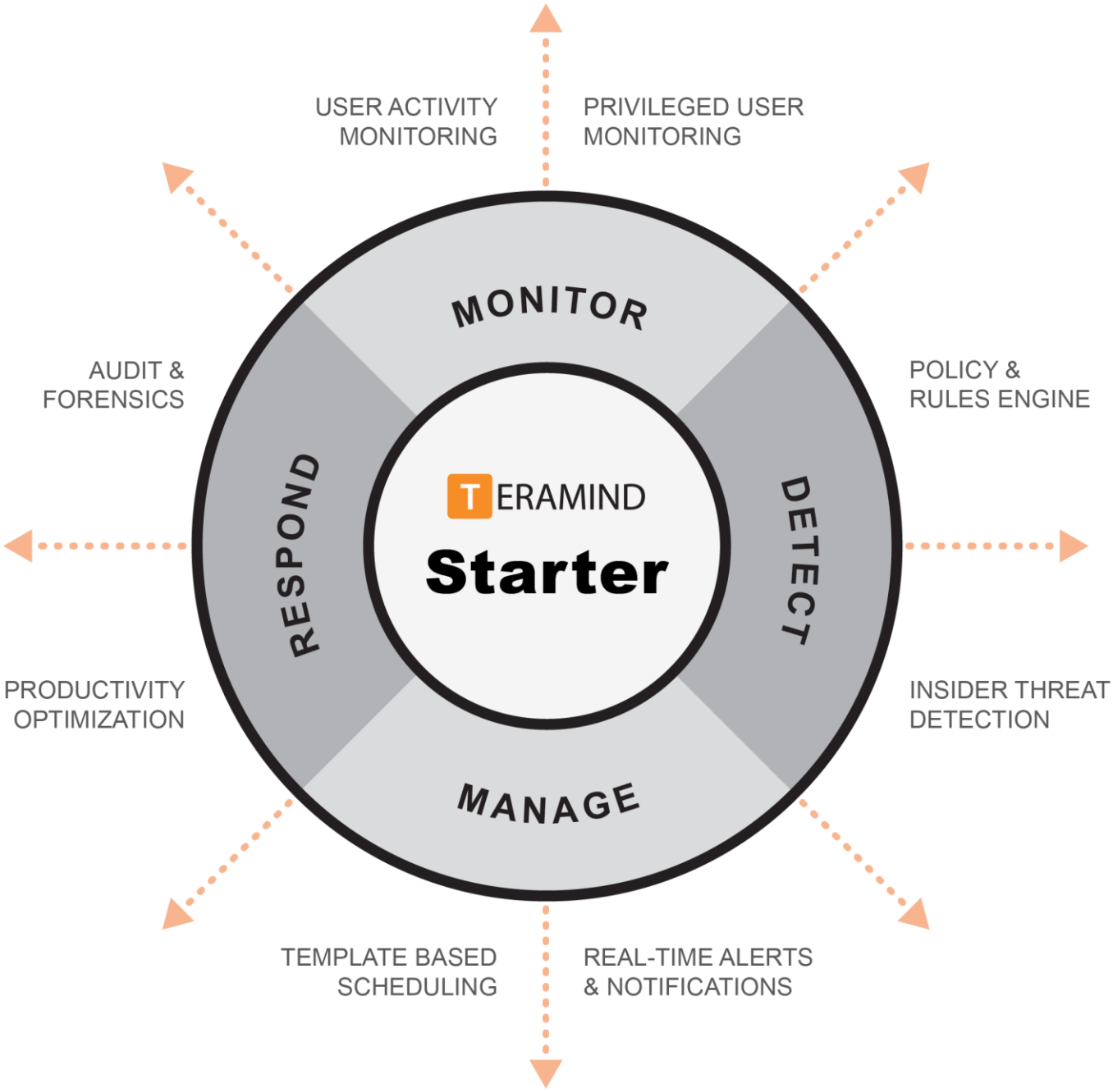
Конфиденциальность сотрудников:
Мониторинг отдельных объектов, таких как «Экран», «Поиск», «Чат», может быть отключен при необходимости. Кроме того, параметры мониторинга могут быть настроены на сбор необходимых данных при соблюдении конфиденциальности сотрудников. Например, автоматически приостанавливать мониторинг, когда сотрудник посещает определенные веб-сайты/приложения (т.е. личную электронную почту).

Аудит и инциденты:
Видеозапись активности сотрудников, запись сессий, постоянные журналы, оповещения - вот лишь несколько примеров мощных возможностей Teramind в области аудита и инцидентов. Вместе они предоставляют обширную коллекцию данных расследования для точного определения источника и внутренней угрозы.

Встроенные инструменты повышения производительности: Определите, какие приложения и веб-сайты вы считаете продуктивными, и получайте подробные отчеты о том, как ваши сотрудники проводят свой день. Определите отстающие или высокоэффективные с активным анализом против простоя. Создайте непрерывную петлю обратной связи, чтобы уточнить и скорректировать рабочий процесс организации путем отслеживания графиков, проектов и уровня вовлеченности сотрудников для общего повышения производительности.

Мониторинг привилегированных пользователей: контролируйте привилегированных и удаленных сотрудников, которые имеют доступ к вашим критически важным системам, чтобы предотвратить саботаж или кражу данных. Например, прекратить создание учетной записи бэкдора, редактирование реестра или попытку повысить доступ к системе со стороны ИТ-администраторов.

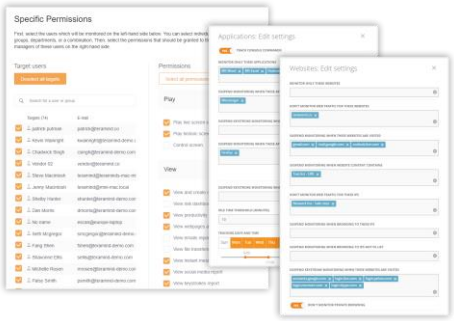
Teramind Starter: программное обеспечение для мониторинга сотрудников с мощными функциями обнаружения внутренних угроз и анализа производительности



Teramind Starter - это многофункциональное решение для мониторинга сотрудников с ощутимыми бизнес-преимуществами.

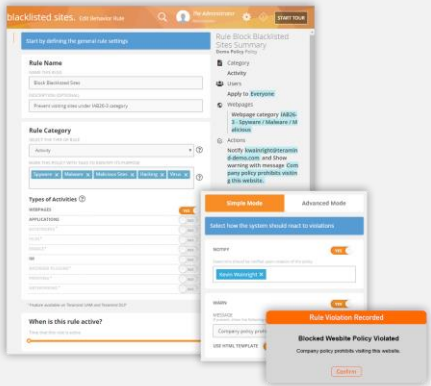
Monitor employee activity in real-time

Сотрудники проводят большую часть своего времени на рабочем столе, используя приложения или веб-сайты. Teramind Starter позволяет визуально записывать каждое действие, которое пользователь выполняет на своем рабочем столе (экране), в приложениях, веб-сайтах, социальных сетях и мессенджерах. Получите все необходимые данные о деятельности, такие как имя приложения/сайта, URL-адрес, продолжительность и т. д., Все в самой мощной и удобной панели мониторинга сотрудников.



Обеспечить конфиденциальность сотрудников с помощью управляемого отслеживания

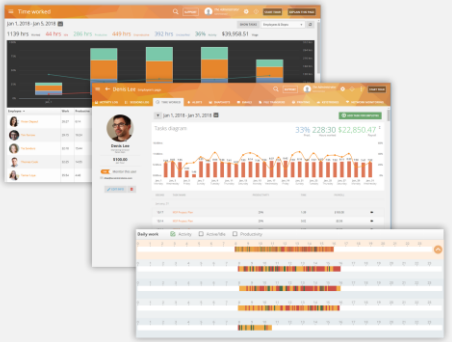
Каждый отслеживаемый объект, такой как экран/приложение/веб-сайт и т. д, может быть сконфигурирован так, чтобы принимать во внимание то, что необходимо отслеживать и измерять, и кто имеет доступ к отслеживаемым записям. Вы можете контролировать, кого вы хотите контролировать, когда и как долго. Это позволяет осуществлять мгновенный административный контроль для соблюдения требований конфиденциальности сотрудников.



Обнаружение внутренних угроз с помощью интеллектуальной системы политик и правил

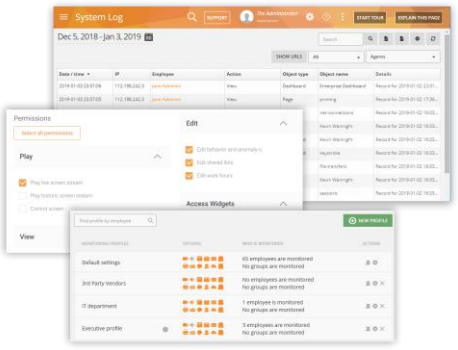
Определите поведение с высоким уровнем риска, то есть загрузку файлов и вложений с неизвестного веб-сайта, запуск опасного приложения и т.д. Затем примените правила на основе поведения, чтобы определить, когда пользователи нарушают правила. Система автоматически заблокирует вредоносную деятельность сотрудников или предупредит пользователя с помощью персонализированного сообщения о потенциальной опасности, уменьшая ложные срабатывания при минимальном наблюдении. Система также может уведомлять вас о случаях нарушения правил, которые требуют вашего личного внимания.

Teramind Starter - это многофункциональное решение для мониторинга сотрудников с ощутимыми бизнес-преимуществами



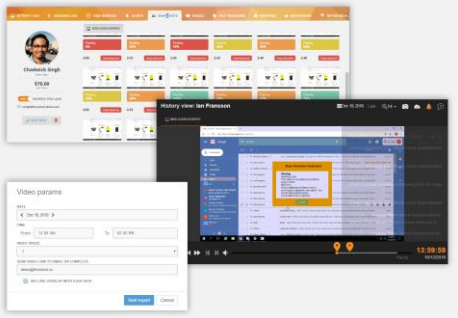
Повысить производительность сотрудников и повысить организационную эффективность

Используйте инструменты производительности труда для отслеживания активного и неактивного времени, поздних смен, длительных перерывов и т.д. Используйте интеллектуальные правила, основанные на активности, для автоматического определения признаков неудовлетворенности клиентов (гневные настроения в сообщениях в социальных сетях/не отвеченные запросы клиентов в мессенджере и т.д.) и внедрите правила для обеспечения лучшего обслуживания.



Monitor privileged users for extra security

Teramind позволяет организациям создавать профили для удаленных и привилегированных сотрудников, а затем определять, к какой информации и системным ресурсам может обращаться каждый профиль. Создайте автономные правила, чтобы уведомлять руководство о любых подозрительных действиях привилегированных пользователей, таких как незапланированный вход в систему, доступ к конфигурации системы, создание учетных записей бэкдора и т. д.



Аудит инцидентов безопасности и криминалистика

Вы можете просматривать подробные оповещения для всех пользователей, включая любое событие безопасности и какие действия были предприняты, какое приложение/сайт был задействован, какие данные были доступны и т.д. Записи сеансов и воспроизведение истории можно использовать для просмотра рабочего стола пользователя или экспорта в формате MP4. для последующего использования. Используется в качестве доказательства в любом расследовании. Неизменяемые системные журналы и отчеты о сеансах предоставляют дополнительную информацию для отслеживания источника и причины