Privileged Threat Analytics™

Обнаружение и реагирование на атаки в режиме реального времени с подачей сигналов тревоги с обратной связью для самых важных данных - данных привилегированных аккаунтов.

Рисунок 1. Панель управления
The Cyber-Ark: Визуальные представления профилей и событий, позволяющих легко выявить нетипичное поведение аккаунтов

Почему CyberArk?

CyberArk - единственная компания, которая может обеспечить полную защиту от комплексных внешних и внутренних угроз, снизить Ваши риски и удовлетворить жесткие требования соответствия.

CyberArk имеет больше успешных внедрений в крупномасштабных распределенных и виртуальных средах, а также наибольшее число решенных проблем с безопасностью привилегированных аккаунтов, чем любая другая компания.

CyberArk Privileged Threat Analytics™ - интеллектуальная экспертная система защиты привилегированных аккаунтов, обеспечивающая специализированный анализ угроз с моментальной подачей сигналов обратной связи благодаря обнаружению ранее не регистрируемой активности привилегированных пользователей.

CyberArk Privileged Threat Analytics - единственная специализированная система анализа, использующая проприетарные алгоритмы для привлечения внимания к самым серьезным из угроз – угрозам, направленным на привилегированные аккаунты. Применяя запатентованную технологию статистического анализа накопленной информации о характере поведения привилегированных аккаунтов, CyberArk Privileged Threat Analytics предоставляет возможность немедленного реагирования при отклонения поведения от «нормального», что позволяет немедленно приступить к отражению атаки. Данные также могут быть также переданы в используемые компанией SIEM-решения, чтобы повысить качество и эффективность защиты.

Видеть главное

CyberArk Privileged Threat Analytics фокусируется на тех данных, что действительно важны: данных о действиях привилегированных аккаунтов. В крупных компаниях ежедневно возникает огромное количество срабатываний системы безопасности. Они включают в себя множество ложных срабатываний, что создает сложности для организаций при определении реакции на сигнал тревоги: какая из угроз реальна? CyberArk фокусируется на привилегированных аккаунтах, с которыми связан самый высокий риск причинения ущерба компании.

Наблюдение за пользователями, а не аккаунтами

Привилегированные аккаунты обычно являются разделяемым - не привязанными к конкретному пользователю. Это не позволяет использовать существующие решения мониторинга, связывающие активность с конкретным пользователем. CyberArk Privileged Threat Analytics анализирует поведение аккаунта на уровне поведений индивидуальных пользователей, обеспечивая точные, контекстно-зависимые сигналы тревоги с немедленной обратной связью.

Реакция на атаку в реальном времени, а не расследование инцидентов

Стандартный подход к расследованию инцидентов, при больших объемах данных позволяет разбираться в случившемся, но не реагировать в режиме реального времени. CyberArk Privileged Threat Analytics обеспечивает подачу сигналов тревоги в режиме реального времени, что позволяет организациям немедленно предпринять меры по противодействию.

Запатентованные алгоритмы анализа

При помощи статистических алгоритмов, изучающих типичное поведение привилегированного пользователя, CyberArk Privileged Threat Analytics сравнивает в режиме реального времени действия привилегированного аккаунта с его прошлыми действиями для обнаружения возможных аномалий в его поведении. Эти аномалии сопоставляются с моделью поведения, чтобы немедленно определить, представляют ли они собой угрозу.

Интеграция с SIEM-решениями

Помимо собственной панели управления, встроенной в систему, данные и сигналы тревоги из CyberArk Privileged Threat Analytics могут направляться на существующую в организации SIEM-систему. Тонкий анализ поведения привилегированных пользователей повышает эффективность работы SIEM-системы за счет обнаружения атак, направленных на привилегированные аккаунты.

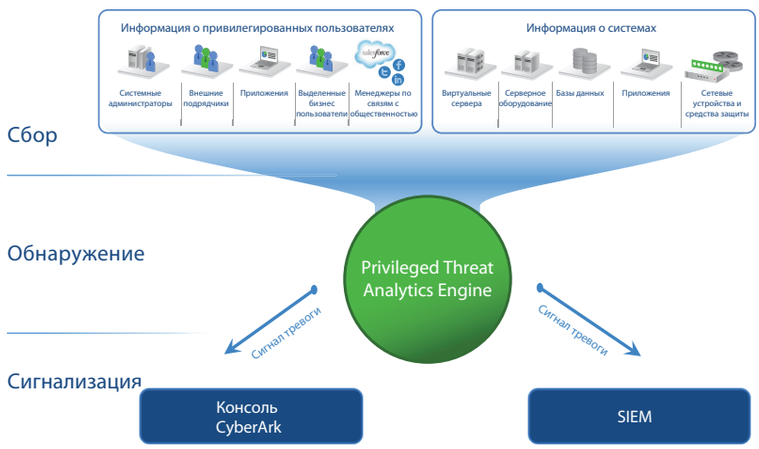
CyberArk Privileged Threat Analytics™

Обнаружение, подача сигналов тревоги и остановка атак в режиме реального времени

Ядро CyberArk Privileged Threat Analytics Engine использует данные о привилегированных пользователях для построения профиля поведения каждого пользователя в организации и непрерывно производит самообучение, чтобы подстраиваться под нормальные изменения в поведении пользователей. Как только установлена "эталонная" модель поведения, ядро CyberArk Privileged Threat Analytics начинает искать отклонения от установленного профиля для обнаружения аномалий в поведении привилегированного пользователя.

Данное решение автоматически обнаруживает и фиксирует каждую индивидуальную аномалию, а затем при помощи запатентованных алгоритмов определяет уровень угрозы на основе корреляции событий. Сигналы тревоги могут моментально посылаться по электронной почте с подробным описанием инцидента и ссылкой на систему CyberArk Privileged Threat Analytics, что позволит сотруднику службы безопасности детально и подробно рассмотреть ее.

CyberArk Privileged Threat Analytics проводит непрерывный процесс самообучения, для повышения эффективности уровня срабатываний. Данная непрекращающаяся адаптация делает ее лучшей системой подачи сигналов тревоги на рынке сегодня.



Защита, Отчётность, Аналитика

Преимущества CyberArk Privileged Threat Analytics

- Обнаружение атак при помощи анализа поведения пользователей, устранение зависимости от необходимости заранее знать сигнатуры атак или использовать sandbox.
- Значительное сокращение "окна возможностей" нападающего и снижение ущерба за счет точного оповещения о происходящих атаках в режиме реального времени
- Повышение качества работы существующих SIEM-решений за счет эффективной интеграции с ними
- Снижение числа "ложных срабатываний" за счет фокуса на привилегированных пользователях, а не на разделяемых аккаунтах
- Оперативное устранение проблем за счет немедленного получения подробной инфор-мации об атаке
- Подстройка системы обнаружения угроз к изменениям среды за счет механизмов самообучения, непрерывно адаптирующих профили "типичного" поведения пользователей в соответствии с изменениями среды
- Улучшение процессов аудита благодаря данным о паттернах поведения пользователей и их действиях
- Возможность просмотра пользовательской активности в виде удобочитаемых графиков и таблиц

Характеристики

Решение поставляется в виде образа виртуальной машины, запускаемого на VMware:

- VMware Player 4.0 и выше
- VMware Workstation 8.0 и выше
- VMware ESX/i 4.0 и выше

Минимальные требования к виртуальной машине:

- 4-ядерный центральный процессор
- 8Гб оперативной памяти
- 50Гб на жестком диске