CORTEX XDR

Вовремя распознайте и остановите скрытые атаки, объединив информацию из сети, конечных устройств и облачных данных

Преимущества для бизнеса

- Автоматическое обнаружение скрытых атак: постоянное обнаружение угроз с помощью искусственного интеллекта, анализа поведения и настраиваемых пользователем правил и политик обнаружения.
- Снижение нагрузки на персонал: мгновенное отсеивание ложных срабатываний, повышение производительности аналитиков
- Сокращение среднего времени обнаружения угрозы (MTTI): сочетание точного определения атак с быстрой расстановкой приоритетов относительно уведомлений об опасности существенно сокращает временные затраты.
- Сокращение среднего времени на сдерживание угроз (MTTC): быстрое обнаружение и безошибочная реакция на внешние атаки и внутренние угрозы без многолетнего опыта.
- Быстрый возврат инвестиций: решение всех вопросов безопасности посредством экосистемы надежных приложений при использовании существующей инфраструктуры в качестве средств и точек контроля доступа.

Уберите препятствия и упростите расследование

Довольно часто службе безопасности не хватает наглядности и автоматизации для предотвращения атак. Отдельные продукты, например, система защиты конечных точек от сложных угроз (EDR), а также система анализа сетевого трафика (NTA) агрегируют большие объемы информации. Они вынуждают аналитика использовать множество консолей для обнаружения угроз, что повышает сложность и замедляет расследование. Сталкиваясь с отсутствием специалистов по кибербезопасности, команды вынуждены упрощать операции или прилагать огромные усилия для проведения расследования и сдерживания атак.

Быстрый способ обнаружения, расследования и реакции на угрозы

Cortex XDR™ – это первое в мире приложение, в которое изначально интегрированы данные о сети, конечных устройствах и облаке для предотвращения сложных атак. Эффективно используя поведенческую аналитику, приложение определяет неизвестные и труднообнаружимые угрозы сети. Машинное обучение и модели искусственного интеллекта определяют угрозы, исходящие из любых источников, включая управляемые и неуправляемые устройства.

Cortex XDR ускоряет расстановку приоритетов относительно угроз и скорость реагирования на инциденты, предоставляя полную картину по каждой угрозе и автоматически определяя основную причину такой угрозы. Объединяя различные типы данных и упрощая анализ, Cortex XDR снижает время реагирования на угрозу, а также требования к знаниям и опыту, необходимому для осуществления операций по сортировке и поиску угроз. Тесная интеграция с точками контроля доступа позволяет быстро реагировать на угрозы, а также применять знания, полученные в результате расследования, для обнаружения схожих атак в будущем.

Защита от известных и неизвестных угроз с помощью Traps™

Безопасность начинается с надежного предотвращения угроз. Приложение Traps™ для защиты конечных устройств, интегрированное в решение Cortex XDR, использует комплексные методы предотвращения атак для защиты конечных точек от вредоносных программ и средств эксплуатации уязвимостей. Traps и Cortex XDR позволяют последовательно предотвращать, обнаруживать, отвечать на угрозы, которым могут подвергаться цифровые активы. Встроенная интеграция с облачным анализом угроз позволяет скоординировано предотвращать сетевые угрозы, на конечных устройствах и облачных ресурсах.

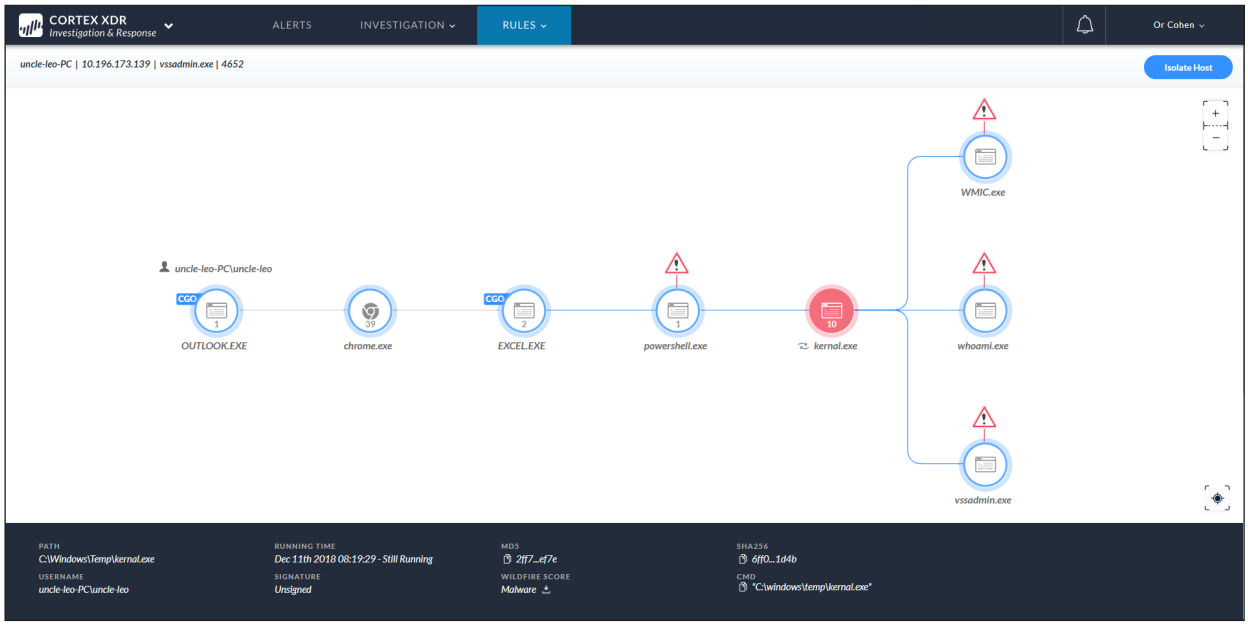

Рисунок 1: Расстановка приоритетов и расследование угроз с помощью Cortex XDR

Основные возможности

Наглядность

Соотносит данные о сети, конечных устройствах и облачных данных, чтобы упростить обнаружение и реакцию на угрозы. Cortex XDR позволяет сэкономить время, затрачиваемое на анализ данных вручную, путем автоматического объединения и сопоставления данных, собранных из сети, конечных устройств и облачных ресурсов. Система объединяет разрозненные типы данных с помощью Cortex Data Lake, которое представляет собой масштабируемое и эффективное облачное хранилище данных, используемое в целях точного определения атак и упрощения расследования инцидентов ИБ.

Автоматическое обнаружение атак с помощью искусственного интеллекта

Обнаружение скрытых угроз с помощью поведенческой аналитики. Cortex XDR автоматически определяет активные атаки, позволяя службе безопасности правильно расставлять приоритеты и отражать угрозы, прежде чем будет нанесен ущерб. Используя машинное обучение, Cortex XDR постоянно анализирует профили пользователей и поведение устройств для выявления аномальной активности, свидетельствующей об атаках. Анализируя большой массив данных, Cortex XDR может определять такие атаки, как кража идентификационных данных, угрозы DNS-туннелирования, которые практически невозможно определить при чтении стандартных логов или при анализе сетевого трафика верхнего уровня приложений. Автоматизированное обнаружение угроз работает бесперебойно каждый день.

Обнаружение угроз с помощью мощных поисковых инструментов

Обнаружение скрытого вредоносного ПО, целенаправленных атак, внутренних атак. Служба безопасности может осуществлять поиск, планирование и сохранение запросов для определения трудно обнаружимых угроз. Гибкие возможности поиска позволяют аналитикам отслеживать угрозы и осуществлять поиск индикаторов компрометации (IoCs), не прибегая к изучению нового языка запросов. Используя встроенный анализ угроз в рамках сети, конечных устройств и облачных данных, службы безопасности смогут обнаруживать вредоносное программное обеспечение, внешние угрозы и внутренние атаки, которые осуществляются в текущий момент времени или осуществлялись ранее.

Мгновенное расследование событий

Автоматическое определение источника каждого уведомления безопасности. С помощью Cortex XDR аналитики могут в один клик анализировать предупреждения о нарушении безопасности из любого источника. Cortex XDR автоматически обнаруживает первопричину проблемы, выявляет историю и последовательность событий, связанных с каждым предупреждением, что снижает требования к опыту, необходимому для точного подтверждения проблемы. При расследовании график всех атак предоставляет детальную информацию для изучения инцидента, позволяя аналитикам мгновенно определять объем и масштаб ущерба, а также последующие действия.

Скоординированный ответ с использованием точек контроля доступа

Быстрое и надежное отражение угроз. Cortex XDR позволяет службе безопасности оперативно отражать угрозы сети, конечных точек и облачных ресурсов из единой консоли. Аналитик может быстро остановить распространение вредоносного ПО, ограничить активности сети определенными устройствами, обновить список источников угроз, например, список неблагонадежных доменов посредством тесной интеграции с точками контроля доступа. С помощью Cortex XDR можно оперативно останавливать сложные атаки, что позволяет быстро вернуть инвестиции, вложенные в ИБ.

Адаптивная защита для остановки потенциальных атак

Определение тактики, методов, процедур и правил поведения атакующих. С Cortex XDR служба безопасности сможет получать новые знания из каждого расследования и применять их для сокращения масштабов поражения и ускорения последующего расследования, изменив тип защиты с реактивного на проактивный. Аналитики могут создавать детализированные правила поведения, которые позволят определять вредоносную активность, свойственную конкретной сети. Информативны оповещения позволят ускорить анализ, быстро идентифицируя подозрительное поведение, а также упрощает понимание сложных событий.

Защищайте конечные устройства с помощью лучшего отраслевого решения

Используйте единого агента для отражения угроз и предотвращения сбора данных на конечных устройствах. В подписку Cortex XDR включены агенты Traps, которые обеспечивают лучшую на сегодняшний день защиту конечных устройств. Traps позволяет останавливать известные и неизвестные вредоносные программы, средства эксплуатации уязвимостей, программы-вымогатели путем блокирования случаев подозрительного поведения и проникновения. Облачная система анализа вредоносного ПО с интегрированной службой защиты - Palo Alto Networks WildFire® - улучшает точность обнаружения и зону покрытия. Агент Traps записывает всю активность конечного устройства и пересылает данные в Cortex Data Lake для последующего анализа и позволяет выбрать правильную реакцию.

Простота развертывания и облачная поставка

Развертывание системы за считанные секунды. Облачное приложение Cortex XDR позволяет быстро и без затрат организовать развертывание системы защиты, устраняя потребность в установке новых локальных служб сбора данных и средств контроля. В качестве средств и точек контроля система использует существующие продукты Palo Alto Networks, тем самым, сокращая число продуктов, которыми вам нужно управлять. Новым клиентам достаточно развернуть одно средство контроля, например, Next-Generation Firewall или Traps, для обнаружения и предотвращения угроз с помощью Cortex XDR. Cortex XDR создано на единственной в отрасли SOC-платформе Cortex на базе искусственного интеллекта. Оно существенно упрощает защиту систем и позволяет добиваться лучших результатов применяя автоматизацию процессов.

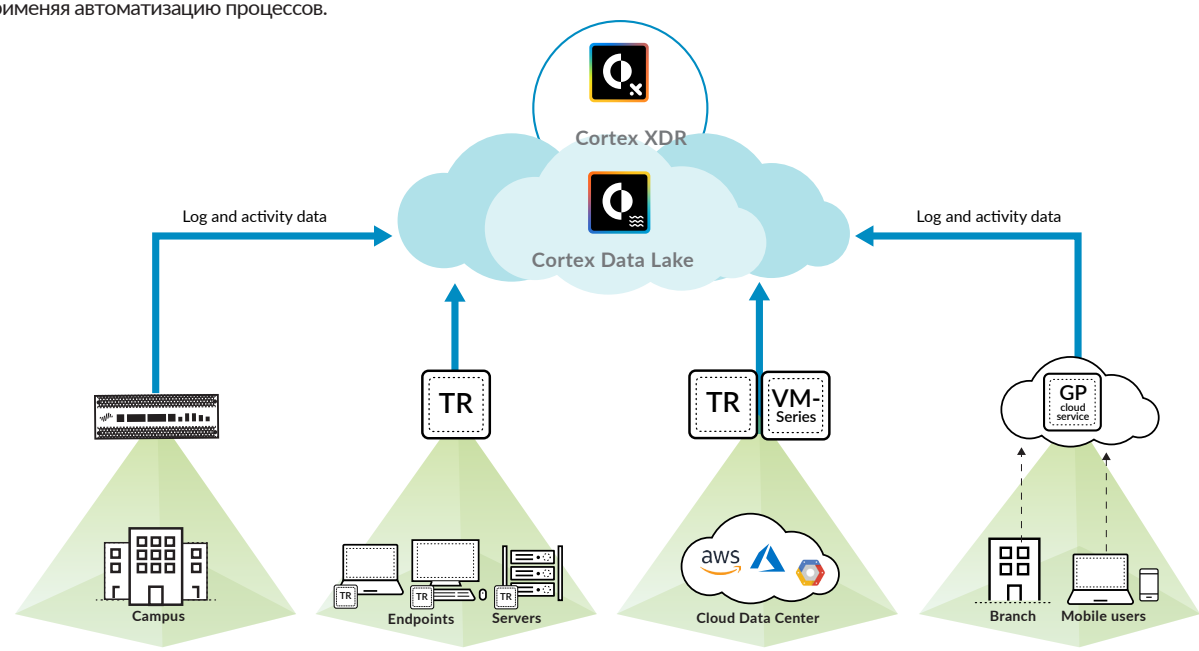

Рисунок 2 : Анализ данных из любого источника для предотвращения и реагирования на угрозы

Технологический эффект

Визуализация сети, конечных точек и облачных данных: сбор и корреляция большого объема данных сети, конечных устройств и облачных данных для обнаружения, расстановка приоритетов для реагирования и предотвращения угроз.

Автоматическое обнаружение сложных и скрытых атак в режиме 24/7: Постоянное использование функции машинного обучения и создания индивидуальных правил для обнаружения целевых кибератак и прочих хитросплетений злоумышленников.

Обработка оповещений без задержек: Упрощает расследование угроз, в том числе анализ корневых проблем и позволяет создавать хронологию событий, тем самым, снижая требования к навыкам сотрудников, которые необходимы для оценки и анализа оповещений.

Значительное сокращение количества ложноположительных оповещений безопасности: Применяет знания, полученные в ходе каждого расследования, для постоянного обновления правил определения поведенческих особенностей и уменьшает количество времени, затрачиваемого на проведение анализа в будущем, снижая уровень риска.

Повышает производительность SOC: Собирает рабочие процессы в единую консоль, объединяя функции расстановки приоритетов в отношении оповещений, расследования, ответа на угрозы в рамках всей сети, конечных устройств и облачной среды.

Восстанавливает систему без последствий для бизнеса: Предотвращает атаки с высокой точностью, не допуская перебоев в работе системы и пользователей.

Позволяет избегать целенаправленных кибератак: Защищает сети от внутренних злоумышленников, нарушителей правил, внешних угроз, безфайловых атак и атак на оперативную память, атак 0-дня.

Разгружает службу безопасности: купирует атаки, обнаруживая нарушения нормального функционирования системы безопасности, аномальное поведение, вредоносный характер активности.

Особенности Cortex XDR	
Автоматическое расследование предупреждений	Определение угроз, исходя из индивидуального характера поведения
Поиск источника возникновения угроз	Машинное обучение
Реагирование на инцидент	Определение вредоносных и безфайловых атак
Предотвращение инцидента и восстановление	Определение целевых кибератак
Анализ последствий после инцидента	Обнаружение внутренних угроз
Поиск угроз	Поведенческая аналитика
Индикаторы компрометации и аналитика угроз	Предотвращение атак с помощью вредоносного, хакерского ПО и использование уязвимостей посредством Traps

Технические характеристики	
Модель поставки	Облачная поставка
Хранение данных	30 дневное неограниченное хранение данных

Поддержка ОС

Traps поддерживает работу с оконечными устройствами на Windows®, macOS® и Linux ОС. Полный перечень системных требований и поддерживаемых ОС вы найдете в таблице совместимости Traps.

Минимальные требования Cortex XDR Pathfinder: 2-х ядерный процессор, 8 Гб оперативной памяти, устройство хранения данных на 128 Гб с тонкой резервацией памяти, VMware ESXiTM версия 5.1 или позже, или Microsoft Hyper ® версии 6.3.96 или более поздняя версия гипервизора.

Лицензия Cortex XDR включает право пользования:

- Cortex XDR – приложение для анализа
- Cortex XDR – приложениедля расследования и реагирования на угрозы
- Агент Traps для защиты конечных точек и отражения атак
- Cortex XDR – Pathfinder служба анализа в конечных точках (альтернативаTraps без использования агента)

CORTEX XDR™ BY PALO ALTO NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Основной телефон: +1.408.753.4000
Отдел продаж: +1.866.320.4788
Служба поддержки: +1.866.898.9087

www.paloaltonetworks.com

cortex-xdr-ds-053119