XSOAR

Операционная система управления ИБ

Полное управление инцидентами:

Отслеживание метрик SLA, сбор улик и журналирование, мобильное приложение, соответствие требованиям регуляторов.

Умная автоматизация и оркестрация:

Автоматические плейбуки, высокая доступность, кросс--корреляция.

Интерактивное расследование:

War Room на основе ChatOps, инструментарий для расследования, совместная работа в режиме реального времени.

Гибкое и масштабируемое развертывание:

Решение доступно для развертывания как в облаке, так и в локальной сети заказчика, поддержка мультиарендных сред с изоляцией данных и расширяемой архитектурой, возможность работы в прокси режиме для сегментированных сетевых сегментов, поддержка внешних чатботов (Slack mirroring).

A SOC's Challenges

Специалисты SOC в своей работе постоянно сталкиваются с огромным числом эволюционирующих сложных угроз.

Аналитики Tier-1 тонут в огромном количестве событий и задачах, для решения которых требуется большое количество времени: идентификация ложных срабатываний, выполнение повторяющихся ответов и анализе событий с большого числа различных средств ИБ.

Перед аналитиками Tier-3 всегда стоит проблема поиска реального инцидента среди цифрового шума, аналогично поиску иглы в стогу сена. Им достаточно сложно координировать работу многочисленных решений ИБ, которые находятся в их распоряжении, наиболее эффективным образом. Ввиду своей высокой загрузки, у них также не хватает времени, чтобы обучать начинающих аналитиков для помощи себе.

Для менеджеров SOC проблемой является попытка посчитать ROI, которое приносят решения ИБ для их SOC. Также перед ними стоит проблема постоянного давления SLA и неполных метрик контроля и документирования. Кроме того, угроза недостатка уровня знаний всегда висит у них над головой: в случае увольнения ведущего аналитика мы получаем значимые недостатки экспертизы и сразу же много шагов назад для SOC.

Это тот момент, когда появляется решение Demisto – SOAR (Security Orchestration, Automation, and Respons) платформа, объединяющая в себе управление инцидентами, процессы автоматизации и оркестрации, а также расследования инцидентов для помощи командам ИБ в их повседневной работе.

CORTEX™ XSOAR
BY PALO ALTO NETWORKS

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

Последовательные, прозрачные и документированные процессы

- Реагирование на основе плейбуков
- Автоматическое документирование всех запросов по поиску и расследованию
- Автоматическое детектирование дублированных Расследований
- Поиск между расследованиями, индикаторами и Уликами

Ускорение времени решения и лучшая эффективность SOC

- Портфолио настраиваемых плейбуков для автоматизации повторяющихся и резервных шагов
- Виртуальная “War Room” для совместных расследований в режиме реального времени
- Детализированное отслеживание инцидентов и метрик аналитиков
- Улучшение продуктивности аналитиков и совместное обучение команды
- Платформа для совместной работы позволяет аналитикам делится результатами расследования
- Обучение аналитиков по результатам прошлых расследований
- Подсказки на основе машинного обучения для выбора аналитика, ответных действий или аналогичного инцидента

Полный процесс управления инцидентами

Платформа Demisto помогает управлять всеми аспектами жизненного цикла инцидента:

- Открытая и расширяемая платформа с интеграцией со всеми необходимыми средствами, включая средства по обогащению данных, фиды Threat Intelligence, SIEM, NGFW, EDR, песочницы, системы анализа, почтовые системы и многое другое.
- Интуитивные плейбуки в режиме plug'n'play для автоматизации всех процессов SOC.
- Автоматическое документирование на всех этапах расследования инцидентов для контроля SLA.
- Хранилище индикаторов с возможностью контекстного поиска для хантинга.
- Мощный поиск с автоматическим детектированием дублированных расследований.
- Удобная панель управления с настраиваемым отчетами и архивированием результатов.
- Агенты для Windows/Mac/Linux OS для сбора данных с конечных узлов.
- Мобильное приложение с персонализируемыми настройками рабочего стола и задачами по расследованию инцидентов.

Умная автоматизация и оркестрация

Оркестрация Demisto как идеальная связь между людьми, процессами и технологиями:

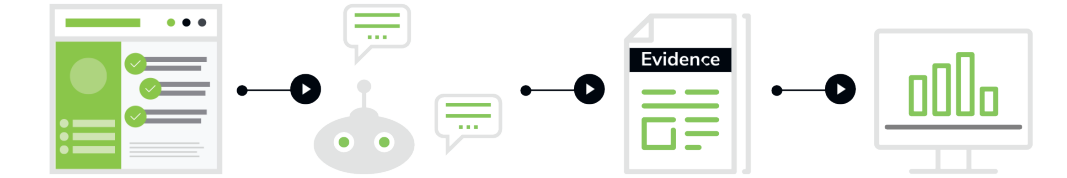
- Портфолио плейбуков для автоматизации, включая более 100 интеграций и 1000 выполняемых задач ИБ.
- Динамические плейбуки, избавляющие аналитиков от рутинных задач, а конечных пользователей от постоянного ответа на электронную почту.
- Гибкость в создании новых функций/блоков и переноса их между плейбуками.
- Отказоустойчивость и высокая доступность плейбуков.Очень легко проверить работоспособность и начать действие с любой точки плейбука.
- Машинные подсказки при работе с инцидентами, повторяющиеся индикаторы в разных инцидентах

Интерактивное расследование

Интерактивное расследование Demisto помогает аналитикам в совместной работе и делает их умнее с каждым инцидентом:

- Виртуальная 'War Room', основанная на ChatOps, где аналитики могут совместно общаться в режиме реального времени и выполнять различные задачи.
- Инструментарий по расследованию инцидентов, обеспечивающий настраиваемую карту взаимосвязи инцидентов во времени.
- Специальный бот (In-house security bot (DBot)), помогающий выполнять команды, предлагать помощь других аналитиков и будущее направление действия.
- Механизм сбора улик и автоматического документирования с возможностью комментирования и сохранения заметок. инцидентами, повторяющиеся индикаторы в разных инцидентах

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ | ОРКЕСТРАЦИЯ | СОВМЕСТНАЯ РАБОТА



DBot – бот с искусственным интеллектом

В дополнение к решению текущих проблем SOC's, Demisto Enterprise использует силу искусственного интеллекта и машинного обучения в своем боте. Подсказки DBot доступны в системе тикетов, анализе задач, выборе аналитика и аналогичного инцидента. Машинное обучение используется во всех трех основных компонентах решения – управлении инцидентами, автоматизации и оркестрации и интерактивном расследовании. С каждым новым инцидентом аналитик и DBot становятся умнее, что снижает общее время на защиту от новых сложных угроз.