Скрытые угрозы: проблемы и решения в детектировании сетевых атак

Станислав Грибанов, руководитель продукта «Гарда NDR»

Проблемы, с которыми сталкиваются специалисты ИБ

Исследование Vectra AI

- 62% специалистов SOC утверждают, что поставщики услуг безопасности заваливают их бессмысленными оповещениями, чтобы избежать ответственности за нарушение.
- 50% специалистов SOC считают, что они не могут успеть за растущим числом угроз безопасности.
- 55% специалистов SOC говорят, что более эффективные инструменты ИБ помогут облегчить их рабочую нагрузку.

Исследование Enterprise Strategy Group

- 45% респондентов неоднократно подвергались атакам посредством зашифрованного трафика.
- У 32% опрошенных ИБ-специалистов возникают проблемы с детектированием и блокированием соединений с C&C.
- 70% атак в зашифрованном трафике - эксфильтрация данных, 64% - коммуникации с C&C, также часто используется внедрение вредоносного ПО.

Скрытые угрозы в трафике

ГАРДА

- Атаки на конечные точки, не поддерживающие агентов (IoT, IIoT, Scada, специфический unix), проникновение через них в сеть.
- Угрозы от скомпрометированных УЗ. Аномальная сетевая активность, связанная с учетными записями, такая как чрезмерная выгрузка данных, несанкционированный доступ или использование shadow it.
- Скрытые коммуникации с C&C в зашифрованном трафике, DNS и DNS-over-HTTPS, SSH-туннели и т.п.
- Горизонтальное перемещение внутри сети после первоначального проникновения.
- Атаки на цепочку поставок. Инструменты NDR могут помочь отслеживать сетевой трафик между организацией и ее поставщиками, выявляя подозрительную активность. Она может указывать на скомпрометированного партнера в цепочке. PIM, BYOD, Services.
- Контроль доступа в сеть. Уязвимости в конфигурациях сетевого оборудования внутри сети.
- Продвинутое вредоносное ПО, способное блокировать отправку логов и подавлять СЗИ.

Сценарии детектирования сетевых угроз

Минимальный уровень

NGFW/IDS/NGIDS трафик north-south

Плюсы

Детектирование только известных угроз (IDS,TI)

Минусы

- Минимальные возможности детектирования атак в шифрованном трафике
- Не поддерживает детектирование lateral movement
- Не поддерживает детектирование zero-day
- Не поддерживает детектирование аномалий в поведении сетевых узлов при компрометации УЗ
- Минимальные возможности детектирования атак на конечные точки, не поддерживающие агентов
- Минимальные возможности детектирования атак на цепочку поставок
- Не поддерживает детектирование уязвимостей в конфигурации сетевого оборудования внутри сети

Сценарии детектирования сетевых угроз

Базовый уровень

IDS/NGIDS трафик north-south / east-west

Российский NTA (NGIDS + запись трафика) north-south / east-west

Плюсы

- Детектирование только известных угроз (IDS,TI)
- Работает из коробки за счет использований сигнатур IDS и фидов TI
- Минимальное количество детектов через аномалии в профиле поведения
- Ограниченные возможности детектирования shadow it
- Возможности расследований и Threat hunting

Минусы

- Минимальные возможности детектирования атак в шифрованном трафике
- Не поддерживает детектирование lateral movement
- Минимальные возможности детектирования zero-day
- Минимальные возможности детектирования аномалий в поведении сетевых узлов при компрометации УЗ
- Минимальные возможности детектирования атак на конечные точки, не поддерживающие агентов
- Минимальные возможности детектирования атак на цепочку поставок

Сценарии детектирования сетевых угроз

Продвинутый уровень

NDR для сетевого трафика и сетевой телеметрии, north-south/ east-west

Плюсы

- Преимущественное использование несигнатурных методов – аномалии, поведенческие модели, ML, подвинутая аналитика.
- Детектирование lateral movement, zero-day, аномалий в поведении сетевых узлов при компрометации УЗ, атак и аномалий на конечных точках, поддерживающих агентов.
- Детектирование shadow it — туннели, пробросы управляющих протоколов, некорпоративные сервисы.
- Детектирование неконтролируемых точек доступа в сеть, атак на цепочку поставок и уязвимостей в конфигурации.
- Продвинутые возможности расследований и Threat Hunting – интерактивные запросы, обогащение, сквозной поиск, drill down и другое.
- Базовое детектирование IDS,TI.
- Автоматическое активное реагирование — обогащение других СЗИ и блокирование атак.

Минусы

- Требует высокой компетенции персонала.
- Не работает из коробки на 100%, требуется построение профилей на сетевом трафике и тонкая настройка.

GARDA

Подписывайтесь
на телеграм-канал **garda.ai**

Спасибо за внимание!

garda.ai
info@garda.ai