????? ??????????

Endpoint Detection & Response (EDR) — класс решений для обнаружения и изучения вредоносной активности на конечных точках, подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей и так далее. В отличие от антивирусов, задача которых бороться с типовыми и массовыми угрозами, EDR-решения ориентированы на выявление целевых атак и сложных угроз. При этом EDR-решения не могут полностью заменить антивирусы (EPP), поскольку эти две технологии решают разные задачи.

Endpoint Protection Platform (EPP) — комплексные защитные решения для конечных точек, в которые входит антивирус, технологии шифрования данных, технологии для отслеживания и устранения уязвимостей, контроля приложений и устройств и т.д.

Security Information and Event Management (SIEM) — решения для сбора и автоматического анализа информации о событиях безопасности.

Next Generation Firewall, межсетевой экран нового поколения (NGFW) — межсетевой экран для глубокой фильтрации трафика, интегрированный с IDS (Intrusion Detection System, система обнаружения вторжений) или IPS (Intrusion Prevention System, система предотвращения вторжений), и обладающий возможностью контролировать и блокировать трафик на уровне приложений.

Intrusion Detection System (IDS) — система обнаружения вторжений, программный продукт или устройство, предназначенные для выявления несанкционированной и вредоносной активности в компьютерной сети или на отдельном хосте. Задача IDS — обнаружить проникновение киберпреступников в инфраструктуру и сформировать оповещение безопасности (функций реагирования, например блокировки нежелательной активности, в таких системах нет), которое будет передано в SIEM-систему для дальнейшей обработки.

Песочница — специально выделенная (изолированная) среда для безопасного исполнения компьютерных программ.

Общие принципы

- Снижение активности в сети. Исключение сканирования или масштабного сканирования сети и работа только с прикладными легитимными протоколами и сервисами (LDAP, Kerberos, DNS, которые вы получаете напрямую из DNS записей домена).
- Использование шифрованных каналов связи с прикладными протоколами и только зашифрованная коммуникация с агентами / нагрузками в C&C.
- Использование нагрузок, подготовленных к противодействию обнаружению средствами EPP и EDR (использование упаковщиков, исполнения в памяти, кастомизация нагрузок от обнаружения).

Обнаружение хакера

Решения активной защиты, которые занимаются обнаружением хакерской или прочей аномальной активности в сети:

- IDS
- IPS
- NGFW
- SIEM
- EDR
- EPP

Нужно понимать, что подобные и прочие инструменты защиты умело используют только компании, в которых хорошо развита культура ИБ. Помимо подобных средств, которые хакер еще имеет возможность обойти, есть и средства более категоричные. Например, решения класса HoneyPot.

HoneyPot

Honeypot (с англ. — «горшочек с мёдом») — ресурс, представляющий собой приманку для злоумышленников.

Задача Honeypot — подвергнуться атаке или несанкционированному исследованию, что впоследствии позволит изучить стратегию злоумышленника и определить перечень средств, с помощью которых могут быть нанесены удары по реально существующим объектам безопасности. Реализация Honeypot может представлять собой как специальный выделенный сервер, так и один сетевой сервис, задача которого — привлечь внимание взломщиков.

Пример Honepot’a: веб-сервер, который не имеет имени и фактически никому не известен, не должен, соответственно, иметь и гостей, заходящих на него, поэтому все лица, которые пытаются на него проникнуть, являются потенциальными взломщиками. Honeypot собирает информацию о характере поведения этих взломщиков и об их способах воздействия на сервер. После чего специалисты по реагированию на инциденты разрабатывают и реализуют стратегии отражения атаки злоумышленника.

Команда реагирования на инциденты

Security Operation Center (SOC) — это центр управления безопасностью, где команда профессиональных аналитиков и инженеров работает в режиме 24/7 для обеспечения безопасности информационных систем и данных предприятия.

Основной задачей SOC является мониторинг и обнаружение возможных кибератак, а также реагирование на них. Сотрудники SOC используют различные инструменты и технологии для обнаружения аномальных активностей в сети, в том числе системы регистрации и анализа журналов, инструменты сетевого мониторинга и системы обнаружения вторжений.

Пример работы SOC

Представим ситуацию, когда в компьютерной сети предприятия была обнаружена аномальная активность, указывающая на возможный случай компрометации данных. SOC может реагировать на такой инцидент следующим образом:

- Определение и классификация угрозы: SOC аналитики начинают анализировать доступные журналы и логи, чтобы определить масштаб и характер возможной угрозы. Они могут использовать специальные инструменты для обнаружения и анализа аномалий, таких как системы обнаружения вторжений.
- Быстрое реагирование: SOC инженеры могут немедленно заблокировать доступ к компьютерной системе, которая могла быть скомпрометирована, чтобы предотвратить дальнейшую утечку данных или вредоносную активность.
- Расследование инцидента: команда SOC начинает расследование, чтобы выяснить, каким образом произошел инцидент и какие данные могли быть украдены или скомпрометированы. Это может включать в себя анализ журналов, обращение к другим участкам предприятия для выяснения, какие данные могли быть затронуты, а также сбор дополнительных фактов и доказательств.

Этапы реагирования SOC:

- Оповещение руководства: SOC руководство обычно своевременно информирует руководство предприятия.
- Восстановление: SOC инженеры принимают меры для восстановления нарушенных систем и данных.
- Документирование и анализ: после расследования и восстановления SOC инженеры и аналитики документируют произошедший инцидент и проводят анализ.

Revision #2
Created 13 October 2025 08:14:38 by Admin
Updated 13 October 2025 08:43:16 by Admin