МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ ЭЛЕКТРОННО-ИНФОРМАЦИОННЫХ СИСТЕМ
Кафедра интеллектуальных информационных технологий

РЕФЕРАТ

по дисциплине
«Современные методы защиты компьютерных систем»

Выполнил:
студент 4-го курса,
ФЭИС,
группы ИИ-22
Заречный А.О.

Брест 2024

1 SOC

SOC (англ. Security Operations Center — рус. Центр управления безопасностью) — подразделение, отвечающая за защиту организации от киберугроз. Аналитики SOC осуществляют круглосуточный мониторинг сети организации и расследуют любые потенциальные инциденты, связанные с безопасностью. В случае обнаружения кибератаки аналитики SOC несут ответственность за принятие любых мер, необходимых для ее устранения. Она включает в себя три основных элемента для управления и повышения уровня безопасности организации: персонал, процессы и технологии. Таким образом, управление и соблюдение нормативных требований обеспечивают основу, связывающую воедино эти компоненты.SOC в здании или на объекте - это центральное место, из которого персонал контролирует работу объекта, используя технологию обработки данных.

SOC — это центр, где круглосуточно ведётся наблюдение за сетевыми и системными событиями, чтобы предотвратить кибератаки и минимизировать их последствия. Важным аспектом работы SOC является использование технологий, таких как системы управления событиями информационной безопасности (SIEM), которые позволяют собирать и анализировать данные из множества источников. SOC также включает использование автоматизации и оркестрации (SOAR), что ускоряет реагирование на инциденты. Организация SOC включает несколько уровней аналитиков, от начинающих (L1) до экспертов (L3), которые обеспечивают как рутинный мониторинг, так и решение сложных задач. Современные вызовы SOC связаны с растущей сложностью угроз, необходимостью анализа больших данных, автоматизацией процессов и адаптацией к облачным и гибридным инфраструктурам.

SOC может быть как внутренним, так и внешним. В последнем случае организация передает услуги безопасности, такие как мониторинг, обнаружение и анализ, на аутсорсинг поставщику услуг управляемой безопасности (MSSP). Это типично для небольших организаций, у которых нет ресурсов для найма, обучения и технического оснащения аналитиков по кибербезопасности.

2 FW/NGFW

Межсетевые экраны, или Firewalls — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

FW являются основой сетевой безопасности, защищая системы от несанк-

ционированного доступа. Традиционные Firewalls обеспечивают фильтрацию трафика на основе правил. Firewall нового поколения (Next-Generation Firewalls, NGFW) предлагают более продвинутую функциональность.

Межсетевые экраны нового поколения (NGFW) представляют собой современную технологию сетевой безопасности, которая значительно превосходит традиционные Firewalls по функциональности. NGFW сочетают в себе возможности классического межсетевого экрана с расширенными инструментами анализа и защиты, такими как глубокая инспекция пакетов, контроль приложений и встроенные системы обнаружения и предотвращения угроз (IDS/IPS).

Основным отличием NGFW от традиционных межсетевых экранов является способность работать на уровне приложений (седьмой слой модели OSI), что позволяет не только анализировать заголовки пакетов, но и понимать содержание трафика. Это даёт возможность идентифицировать конкретные приложения, например, Facebook или YouTube, и применять к ним политику безопасности — блокировать, ограничивать или разрешать доступ. Такой подход особенно важен в условиях широкого распространения веб-приложений.

При внедрении NGFW важно учитывать:

- производительность устройства, чтобы оно справлялось с высоким объёмом трафика и не снижало скорость сети;
- настройку правил и политик безопасности, которые обеспечат баланс между безопасностью и доступностью ресурсов;
- интеграцию с существующими системами безопасности и облачными решениями.

Современные NGFW поддерживают облачные и гибридные среды, что делает их универсальным инструментом для защиты как локальных, так и распределённых инфраструктур.

3 IDS/IPS

Системы обнаружения и предотвращения вторжений (IDS/IPS) представляют собой технологии, которые анализируют сетевой или системный трафик с целью выявления угроз. IDS предназначена для пассивного мониторинга и уведомления о подозрительной активности, тогда как IPS активно блокирует обнаруженные атаки.

IDS (Intrusion Detection System) — система обнаружения вторжений, предназначенная для мониторинга сетевого трафика и анализа активности на предмет наличия признаков атак или иных нарушений. IPS (Intrusion

Prevention System) — система предотвращения вторжений, которая не только выявляет потенциальные угрозы, но и активно принимает меры для их устранения.

Системы IDS и IPS классифицируются по различным признакам:

1. По методу анализа:
   - Сигнатурные системы — идентифицируют угрозы по заранее известным шаблонам (сигнатурам).
   - Поведенческие системы — выявляют аномалии, сравнивая текущую активность с базовым поведением сети.
   - Гибридные системы — сочетают сигнатурный и поведенческий подходы.
2. По месту развертывания:
   - Сетевые системы (NIDS/NIPS) — мониторят и защищают сетевой трафик.
   - Хостовые системы (HIDS/HIPS) — работают на уровне отдельных устройств.

Преимущества IDS/IPS

- IDS:
  1. Выявление сложных атак.
  2. Возможность интеграции с другими системами безопасности.
- IPS:
  1. Прямая защита от атак.
  2. Автоматизация процессов реагирования.

Недостатки IDS/IPS

- IDS:
  1. Высокая вероятность ложных срабатываний.
  2. Невозможность блокировать атаки.
- IPS:
  1. Риск блокировки легитимного трафика.
  2. Сложности настройки.

4 NTA

Анализ сетевого трафика (Network Traffic Analysis, NTA) фокусируется на мониторинге и изучении сетевых потоков данных для выявления аномалий и угроз. Это технология, позволяющая анализировать даже зашифрованный трафик с использованием методов анализа метаданных, что становится особенно важным в условиях растущего объёма шифрования. NTA применяется для обнаружения сложных угроз, таких как атаки типа "нулевого дня DDoS, утечки данных или скрытая активность злоумышленников. Современные платформы для NTA активно используют машинное обучение и искусственный интеллект для автоматизации выявления аномалий. Эти решения являются важным дополнением к SOC, помогая выявлять угрозы, которые могут быть пропущены другими системами, такими как IDS/IPS. Основные вызовы включают обработку больших объёмов данных, минимизацию ложных срабатываний и интеграцию с существующими системами безопасности. В будущем NTA будет всё больше использоваться для анализа поведения пользователей и устройств (UEBA) и адаптации к облачным инфраструктурам.

Network Traffic Analysis (NTA) или анализ сетевого трафика — это процесс мониторинга, анализа и интерпретации данных, передаваемых в сети, с целью выявления аномалий, обнаружения угроз и обеспечения безопасности сетевой инфраструктуры. Данный подход стал особенно актуальным в условиях возрастающей сложности кибератак и необходимости защиты от сложных угроз (Advanced Persistent Threats, APT).

Цели NTA:

- Анализ сетевого поведения позволяет выявлять отклонения от нормального состояния, что может свидетельствовать о наличии вредоносной активности.
- Современные атаки часто не используют вредоносные файлы, а основываются на злоупотреблении легитимными процессами (например, lateral movement или data exfiltration).
- NTA обеспечивает глубокое понимание происходящего в сети, включая межсетевые взаимодействия, даже в зашифрованном трафике.
- Позволяет аналитикам кибербезопасности быстрее обнаруживать и реагировать на угрозы.

Примеры использования NTA:

- Атаки с использованием скрытых туннелей или эксплуатирующие редкие протоколы можно обнаружить через мониторинг аномальных потоков трафика.

- IoT-среды уязвимы из-за слабой защиты устройств. NTA позволяет мониторить трафик IoT для обнаружения нетипичных взаимодействий.
- Анализ большого количества пакетов позволяет отличить легитимный трафик от вредоносного.
- Выявление подозрительных соединений с внешними IP-адресами или передач больших объемов данных.