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 Security Operations Center (SOC)

Security Operations Center (SOC) — это специализированный центр мониторинга и управления безопасностью, который отвечает за защиту информационных активов организации от киберугроз. SOC является важнейшим элементом современной системы защиты компьютерных систем, предоставляя централизованную платформу для мониторинга, анализа и реагирования на инциденты безопасности.

Основная цель SOC — обеспечение непрерывного мониторинга сетевой активности с использованием передовых технологий, таких как системы обнаружения вторжений (IDS/IPS), средства управления информацией и событиями безопасности (SIEM), а также механизмы автоматического реагирования на угрозы. Это позволяет выявлять подозрительное поведение, анализировать атаки и минимизировать риски в реальном времени.

Основные функции SOC

1. Мониторинг и анализ событий. SOC круглосуточно отслеживает сетевой трафик и активность, собирая данные из различных источников, таких как межсетевые экраны, антивирусные программы, системы аудита и облачные сервисы. Анализ этих данных позволяет выявлять аномалии и потенциальные угрозы.
2. Управление инцидентами безопасности. Команда SOC занимается обработкой инцидентов, начиная с их классификации и заканчивая устранением последствий. Это включает оперативное реагирование на атаки, минимизацию ущерба и предотвращение повторных инцидентов.
3. Углубленный анализ угроз. SOC использует технологии искусственного интеллекта и машинного обучения для анализа сложных атак, таких как продвинутые постоянные угрозы (APT). Такие инструменты позволяют находить ранее неизвестные уязвимости и прогнозировать новые виды атак.
4. Разработка рекомендаций по улучшению безопасности. На основе выявленных угроз SOC предлагает организационные и технические меры для усиления уровня защиты. Это может включать обновление политик безопасности, настройку оборудования или проведение обучения сотрудников.

Команда SOC

Работа SOC требует высококвалифицированных специалистов, таких как аналитики безопасности, инженеры по мониторингу и архитекторы безопасности. Эти профессионалы используют как технические, так и организационные навыки для эффективной защиты систем.

Важность SOC в современной защите

В условиях роста числа кибератак и их сложности SOC становится необходимым элементом для обеспечения безопасности данных. Централизованный подход к мониторингу и управлению позволяет организациям быстрее реагировать на угрозы, минимизировать ущерб и сохранять свою репутацию.

2 Брандмауэры и Next-Generation Firewall (FW/NGFW)

Брандмауэры (Firewall, FW) и их усовершенствованная версия — брандмауэры нового поколения (Next-Generation Firewall, NGFW) — являются ключевыми инструментами защиты компьютерных систем. Они играют роль первой линии обороны, предотвращая несанкционированный доступ к корпоративным сетям и обеспечивая контроль над сетевым трафиком.

Классические брандмауэры (FW)

Традиционные брандмауэры функционируют на основе заданных правил, фильтруя входящий и исходящий сетевой трафик. Эти устройства работают на уровне сетевого и транспортного протоколов модели OSI и основываются на таких параметрах, как IP-адрес, номер порта и тип протокола.

Основные функции традиционных брандмауэров:

1. Фильтрация трафика по правилам доступа.
2. Защита сети от внешних атак, таких как сканирование портов и DoS-атаки.
3. Предотвращение несанкционированного использования сетевых ресурсов.

Однако классические брандмауэры имеют ряд ограничений, включая невозможность анализа трафика на уровне приложений и отсутствие средств для противодействия современным сложным атакам.

Брандмауэры нового поколения (NGFW)

NGFW расширяют функциональность традиционных брандмауэров, предоставляя возможность анализа трафика на более глубоком уровне. Они интегрируют технологии защиты, включая системы предотвращения вторжений (IPS), контроль приложений и инспекцию зашифрованного трафика.

Основные возможности NGFW:

1. Контроль приложений. NGFW позволяет идентифицировать и управлять трафиком приложений независимо от используемых портов и протоколов. Это обеспечивает детальную настройку

политики доступа.
2. Инспекция зашифрованного трафика. Современные брандмауэры способны анализировать данные, передаваемые через протоколы HTTPS, выявляя угрозы даже в зашифрованных соединениях.
3. Интеграция с системами обнаружения угроз. NGFW используют базы данных угроз, чтобы в реальном времени блокировать вредоносные IP-адреса, сайты и файлы.
4. Защита от сложных атак. Благодаря использованию машинного обучения и анализа поведения, NGFW могут обнаруживать аномалии и предотвращать сложные атаки, такие как продвинутые постоянные угрозы (APT).

Преимущества NGFW перед классическими брандмауэрами

NGFW обеспечивают более высокий уровень защиты, адаптируясь к современным киберугрозам. Их способность к глубокому анализу трафика и интеграция с другими инструментами кибербезопасности делает их незаменимыми для корпоративных сетей.

Выбор между FW и NGFW

Для организаций, стремящихся минимизировать риск кибератак, использование NGFW является предпочтительным выбором. Однако для небольших сетей с ограниченным бюджетом классические брандмауэры могут быть подходящим решением.

3 Системы обнаружения и предотвращения вторжений (IDS/IPS)

Системы обнаружения (IDS — Intrusion Detection System) и предотвращения вторжений (IPS — Intrusion Prevention System) являются важными элементами защиты компьютерных систем, обеспечивающими выявление и блокирование попыток несанкционированного доступа, атак и других угроз.

Системы обнаружения вторжений (IDS)

IDS предназначены для мониторинга сетевого трафика и выявления подозрительных действий. Эти системы работают в режиме анализа и уведомления, предоставляя администраторам информацию о возможных угрозах.

К основным функциям IDS относятся:

1. Анализ трафика в реальном времени с использованием сигнатур угроз.
2. Сигнализация о подозрительных действиях через уведомления.
3. Сбор данных для последующих расследований и анализа атак.

IDS можно разделить на два основных типа. Сетевые IDS (NIDS) работают на уровне всей сети и анализируют сетевой трафик, в то время как хостовые IDS (HIDS) защищают отдельные устройства, отслеживая их события и логи.

Системы предотвращения вторжений (IPS)

IPS являются логическим продолжением IDS, добавляя возможность автоматического предотвращения угроз. Эти системы интегрируются в сетевую инфраструктуру и работают в режиме реального времени.

Функции IPS включают:

1. Автоматическую блокировку подозрительного трафика или разрыв вредоносных соединений.
2. Интеграцию с другими системами безопасности, такими как брандмауэры или SIEM.
3. Противодействие сложным атакам с использованием поведенческого анализа и машинного обучения.

Отличия IDS и IPS

Главное различие между IDS и IPS заключается в их подходе к обработке угроз. IDS выполняют только функцию обнаружения, уведомляя специалистов о возможных атаках, тогда как IPS активно предотвращают угрозы. IDS требует вовлечения специалистов для анализа данных и принятия мер, в то время как IPS действует самостоятельно, что может ускорить процесс защиты, но также повысить риск ложных срабатываний.

Преимущества и вызовы

Использование IDS позволяет организациям эффективно мониторить сеть и собирать данные для анализа инцидентов. Однако они требуют значительных ресурсов для реагирования на угрозы. IPS обеспечивают более высокий уровень защиты за счет автоматизации, но требуют тщательной настройки для минимизации ложных тревог.

Значение IDS/IPS в современной безопасности

IDS и IPS являются ключевыми элементами стратегии кибербезопасности, обеспечивая проактивный подход к защите информационных активов. Эти технологии помогают организациям своевременно выявлять угрозы и предотвращать атаки, снижая риск компрометации данных.

4 Анализ сетевого трафика (NTA)

Анализ сетевого трафика (Network Traffic Analysis, NTA) — это

современный метод защиты компьютерных систем, который фокусируется на детальном изучении и мониторинге сетевого трафика для выявления аномалий и угроз. Этот подход становится всё более востребованным в условиях роста числа сложных кибератак и использования зашифрованного трафика.

Принципы работы NTA

Системы NTA анализируют данные о сетевом трафике, собирая метаинформацию, такую как IP-адреса, порты, протоколы и объем данных, а также содержимое пакетов (при необходимости). На основе этих данных системы выявляют аномальное поведение, которое может свидетельствовать о наличии угроз.

Основные задачи NTA:

1. Обнаружение аномалий. NTA отслеживает трафик в режиме реального времени, выявляя отклонения от стандартного поведения, которые могут указывать на попытки вторжения, утечку данных или деятельность вредоносного ПО.
2. Мониторинг зашифрованного трафика. В условиях, когда большая часть интернет-коммуникаций осуществляется через зашифрованные соединения (HTTPS), NTA позволяет анализировать трафик без расшифровки данных, используя поведенческие характеристики.
3. Углубленный анализ атак. Системы NTA способны обнаруживать сложные угрозы, такие как продвинутые постоянные угрозы (APT), которые часто остаются незамеченными традиционными средствами защиты.

Преимущества NTA:

1. Обнаружение скрытых угроз. В отличие от сигнатурных методов, которые зависят от наличия баз известных атак, NTA использует поведенческий анализ, что позволяет выявлять новые и неизвестные угрозы.

2. Применение машинного обучения. Современные системы NTA интегрируют алгоритмы машинного обучения, которые позволяют анализировать огромные объемы данных и повышать точность обнаружения.

3. Интеграция с другими системами. NTA может дополнять традиционные методы защиты, такие как IDS/IPS и SIEM, усиливая их эффективность.

Недостатки NTA:

1. Высокие требования к вычислительным ресурсам для обработки

большого объема данных.
2. Необходимость обучения алгоритмов для повышения точности.
3. Риск ложных срабатываний, особенно в сложных и динамичных сетях.

Анализ сетевого трафика становится незаменимым инструментом для организаций, стремящихся минимизировать риски утечек данных и сложных кибератак. Использование NTA позволяет повысить прозрачность сетевой активности, оперативно реагировать на угрозы и обеспечивать высокий уровень безопасности.