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
Варицкий М.И.

Брест 2024

Введение

С развитием технологий информационная безопасность стала важным аспектом для любого бизнеса и государственных организаций. Кибератаки становятся более изощренными, их последствия — более разрушительными, что вынуждает компании внедрять комплексные решения для защиты своих данных и инфраструктуры. Данный реферат охватывает такие аспекты, как Центры управления безопасностью (SOC), брандмауэры нового поколения (FW/NGFW), системы обнаружения и предотвращения вторжений (IDS/IPS) и анализ сетевого трафика (NTA). Эти технологии являются основными элементами современных систем киберзащиты.

SOC (Security Operations Center)

SOC (Центр управления безопасностью) — это оперативный центр, где группа экспертов круглосуточно занимается мониторингом и управлением событиями безопасности в инфраструктуре организации.

Основные задачи SOC:

1. **Мониторинг событий безопасности**: использование SIEM (Security Information and Event Management) для сбора, анализа и корреляции данных.
2. **Реагирование на инциденты**: разработка и реализация планов действий для устранения угроз.
3. **Анализ данных**: глубокий разбор атак для выявления уязвимостей и разработки мер защиты.
4. **Обеспечение соответствия нормативным требованиям**: соблюдение стандартов, таких как ISO 27001, PCI DSS и GDPR.

Уровни SOC:

- **Первый уровень**: Аналитики начального уровня занимаются базовой проверкой событий безопасности и фильтрацией ложных срабатываний.
- **Второй уровень**: Специалисты углубленного анализа работают с подтвержденными инцидентами.
- **Третий уровень**: Эксперты по угрозам и реагированию разрабатывают стратегии и обновляют правила безопасности.

Преимущества SOC:

- Централизованный контроль безопасности.
- Быстрая реакция на инциденты.
- Постоянное повышение уровня защиты за счет анализа угроз.

FW/NGFW (Firewalls and Next-Generation Firewalls)

Брандмауэры (Firewall) — это устройства или программы, предназначенные для фильтрации входящего и исходящего трафика на основе заранее определенных правил. NGFW (брандмауэры нового поколения) расширяют функциональность стандартных решений и включают более глубокий анализ данных.

Основные возможности NGFW:

1. **Фильтрация приложений**: NGFW способен идентифицировать приложения по сигнатурам и контролировать их поведение, независимо от порта или протокола.
2. **Интеграция с IDS/IPS**: добавление функциональности для обнаружения и предотвращения вторжений.
3. **SSL-дешифровка**: проверка трафика, передаваемого через защищенные соединения.
4. **Управление пользователями**: идентификация трафика на основе учетных записей пользователей.

Преимущества NGFW:

- Защита от сложных атак, включая APT (Advanced Persistent Threat).
- Возможность централизованного управления политиками безопасности.
- Гибкость и адаптивность при работе в современных сетевых архитектурах.

Примеры использования:

- Разделение трафика в корпоративных сетях.
- Защита облачных ресурсов.
- Обеспечение безопасности удаленных пользователей.

IDS/IPS (Intrusion Detection and Prevention Systems)

IDS (Intrusion Detection Systems) и IPS (Intrusion Prevention Systems) — это технологии, используемые для обнаружения и предотвращения сетевых атак. IDS ориентированы на пассивный мониторинг, тогда как IPS способны активно блокировать угрозы.

Принципы работы:

1. **Сигнатурный анализ**: поиск известных шаблонов атак, например, вредоносного кода или аномального поведения.
2. **Анализ аномалий**: использование моделей нормального поведения системы для выявления отклонений.
3. **Гибридный подход**: комбинация сигнатурного и поведенческого анализа для повышения эффективности.

Основные функции:

- Анализ входящего и исходящего трафика.
- Логирование событий безопасности.
- Реализация политики предотвращения угроз.

Преимущества:

- Быстрое обнаружение новых атак.
- Интеграция с SOC для централизованного управления инцидентами.
- Возможность настройки под конкретные нужды организации.

NTA (Network Traffic Analysis)

NTA (Network Traffic Analysis) — это метод анализа сетевого трафика с целью выявления аномалий, которые могут указывать на угрозы безопасности.

Как работает NTA:

1. **Сбор данных**: захват пакетов в сети с помощью систем мониторинга (например, NetFlow или sFlow).
2. **Анализ аномалий**: сравнение текущего трафика с базовыми метриками.
3. **Идентификация угроз**: выявление подозрительных IP-адресов, нехарактерного поведения пользователей и других признаков угроз.

Ключевые особенности:

- Поддержка машинного обучения (ML) для автоматизации анализа.
- Интеграция с SIEM для предоставления контекстной информации.
- Высокая точность обнаружения сложных угроз, таких как скрытые каналы передачи данных.

Преимущества:

- Выявление Zero-Day угроз.
- Анализ трафика за пределами корпоративной сети, включая облачные сервисы.
- Мониторинг в реальном времени и создание отчетов для SOC.

Заключение

SOC, FW/NGFW, IDS/IPS и NTA являются важными элементами современной киберзащиты. Их взаимодействие позволяет организовать проактивный подход к управлению информационной безопасностью, минимизировать риски и защитить критически важные данные. Будущее этих технологий связано с дальнейшим развитием искусственного интеллекта и машинного обучения, что сделает их еще более эффективными в борьбе с киберугрозами.