Министерство образования Республики Беларусь

Учреждение образования

«Брестский государственный технический университет»

Кафедра интеллектуально-информационных технологий

РЕФЕРАТ

по дисциплине

«Современные методы защиты компьютерных систем»

Выполнила:
студентка 4 курса,
ФЭИС,
группы ИИ-22
Леваневская Н.И.

Брест-2024

SOC

Security Operations Center (SOC) — это централизованное подразделение, ответственное за мониторинг, обнаружение, анализ и реагирование на инциденты информационной безопасности в режиме реального времени. SOC играет ключевую роль в защите цифровой инфраструктуры организации, обеспечивая круглосуточное наблюдение за безопасностью.

Основные задачи SOC

1. **Мониторинг безопасности**. SOC анализирует данные, поступающие из различных источников, включая сети, серверы, приложения, базы данных и конечные устройства. Используются инструменты SIEM (Security Information and Event Management), чтобы обрабатывать большие объемы логов и событий.
2. **Обнаружение угроз.** SOC занимается выявлением подозрительных действий, включая попытки взлома, утечку данных и нарушения политик безопасности. Используются технологии анализа поведения пользователей и устройств (UEBA) и системы раннего предупреждения.
3. **Реагирование на инциденты**. Команда SOC разрабатывает и выполняет планы по ликвидации последствий инцидентов. Это может включать изоляцию зараженных систем, устранение уязвимостей и восстановление инфраструктуры.
4. **Управление угрозами и уязвимостями.** Регулярное сканирование системы на наличие слабых мест, внедрение патчей и управление рисками.
5. **Аналитика и отчетность.** Постоянный анализ эффективности мер безопасности и предоставление отчетов руководству для принятия стратегических решений.

Структура и компоненты SOC

1. **Технологическая инфраструктура:**
   1.1. SIEM-системы: для сбора и анализа данных.
   1.2. Инструменты угрозоаналитики (Threat Intelligence Platforms).
   1.3. Средства автоматизации и оркестрации (SOAR).
2. **Процессы:**
   2.1. Регламенты реагирования на инциденты.
   2.2. Стандарты управления логами.
   2.3. Процессы регулярного обновления и тестирования.
3. **Команда SOC:**
   3.1. Аналитики первого уровня: мониторят события и передают критические инциденты выше.
   3.2. Аналитики второго уровня: проводят глубокий анализ инцидентов и занимаются реагированием.
   3.3. Инженеры SOC: обеспечивают поддержку инфраструктуры и оптимизируют инструменты SOC.
   3.4. Менеджеры SOC: зуководят операциями, координируют действия команды.

Плюсы использования SOC (Security Operations Center)

1. **Круглосуточный мониторинг.** SOC обеспечивает постоянное наблюдение за безопасностью, позволяя быстро обнаруживать и реагировать на угрозы в любое время суток.
2. **Централизованный контроль безопасности**. Все данные об инцидентах, уязвимостях и угрозах собираются в одном месте, что повышает эффективность управления.
3. **Сокращение времени реагирования.** Благодаря интеграции с SIEM-системами и автоматизации процессов SOC может быстро идентифицировать и изолировать угрозы.
4. **Повышение уровня защиты.** SOC активно отслеживает новые типы угроз, используя платформы Threat Intelligence и передовые аналитические инструменты.
5. **Снижение затрат на последствия атак**. Своевременное обнаружение и нейтрализация угроз позволяет минимизировать ущерб от инцидентов.
6. **Соответствие нормативным требованиям**. SOC помогает соблюдать требования законодательства и стандартов безопасности, таких как GDPR, ISO 27001, PCI DSS и др.
7. **Автоматизация процессов.** С использованием SOAR (Security Orchestration, Automation, and Response) автоматизируются повторяющиеся задачи, что снижает нагрузку на сотрудников.

Недостатки использования SOC

1. **Высокая стоимость внедрения и поддержки**. Создание и управление SOC требует значительных инвестиций в оборудование, программное обеспечение и найм специалистов.
2. **Дефицит квалифицированных кадров.** Для работы SOC требуются опытные специалисты в области кибербезопасности, которых на рынке часто не хватает.
3. **Избыточность данных.** SOC обрабатывает огромное количество событий, из которых не все представляют реальную угрозу, что может усложнять анализ (проблема ложных срабатываний).
4. **Сложность настройки и управления**. Настройка инструментов SOC, таких как SIEM, требует времени и глубоких знаний, а неправильная конфигурация может снизить эффективность работы.
5. **Зависимость от технологий.** Системы SOC сильно зависят от используемого программного обеспечения, которое может быть уязвимо к сбоям и атакам.
6. **Риск перегрузки команды.** Если аналитики SOC сталкиваются с большим количеством инцидентов, это может привести к выгоранию сотрудников и снижению качества работы.
7. **Эволюция угроз.** Современные угрозы становятся все более сложными, и SOC может не успевать адаптироваться к их новым формам, особенно если недостаточно инвестиций в обновление технологий.

Примеры использования SOC

1. **SOC в банках.** Банки активно используют SOC для защиты финансовых данных, мониторинга транзакций и предотвращения мошенничества.
2. **SOC в промышленности.** В промышленности SOC обеспечивает безопасность IoT-устройств, защищая производственные линии и системы управления.
3. **SOC в здравоохранении.** SOC помогает защищать конфиденциальные данные пациентов, медицинские устройства и системы управления больницами.

FW/NGFW

Firewall (FW) — это программное или аппаратное средство, предназначенное для фильтрации сетевого трафика между внутренними и внешними сетями. Он защищает сеть, разрешая или блокируя данные на основе установленных правил.

Next-generation firewall (NGFW) — это усовершенствованная версия традиционного брандмауэра, которая объединяет классическую фильтрацию трафика с дополнительными функциями, такими как контроль приложений, встроенные системы предотвращения вторжений (IPS), SSL-дешифровка, защита от угроз на уровне приложений.

Классификация FW

1. **Пакетные фильтры.** Анализируют заголовки IP-пакетов и принимают решения на основе IP-адресов, портов и протоколов.
2. **Межсетевые экраны на уровне сеанса (Stateful Firewalls).** Отслеживают состояние соединений и обеспечивают фильтрацию на основе контекста.
3. **Прокси-брандмауэры**. Действуют как посредники между пользователем и сетью, анализируют содержимое трафика.
4. **Аппаратные и программные FW.** Аппаратные решения устанавливаются как отдельные устройства, программные — запускаются на сервере или устройстве.

Функции FW

1. Фильтрация входящего и исходящего трафика.
2. Защита от несанкционированного доступа.
3. Управление доступом к определённым сервисам.
4. Логирование и мониторинг сетевой активности.

Дополнительные функции NGFW

1. **Контроль приложений.** NGFW позволяет идентифицировать и управлять использованием приложений в сети. Это достигается благодаря глубокому анализу пакетов (DPI), который позволяет:
   1.1. Определять тип приложения (например, YouTube, Skype, Slack), даже если используется нестандартный порт.
   1.2. Разрешать или блокировать доступ к определённым приложениям на основе корпоративных политик.
   1.3. Контролировать доступ к функциям внутри приложений (например, запрет загрузки файлов в облачные хранилища).

2. **Обнаружение и предотвращение вторжений (IDS/IPS).**
   2.1. NGFW включает встроенные системы IDS/IPS для мониторинга и анализа сетевого трафика в реальном времени.
   2.2. Эти системы выявляют аномалии и известные угрозы (вредоносный трафик, эксплойты, попытки проникновения).
   2.3. NGFW не только обнаруживает угрозы, но и может автоматически блокировать их (например, прекращать сессию, если обнаружен вредоносный код).
   2.4. IDS/IPS обеспечивают защиту от уязвимостей на уровне приложений, включая SQL-инъекции, XSS-атаки и т.д.
3. **Интеграция с другими системами безопасности.**
   3.1. NGFW может быть интегрирован с внешними системами безопасности, такими как антивирусы, системы управления уязвимостями и SIEM-платформы.
   3.2. Поддержка Threat Intelligence позволяет NGFW получать актуальные сигнатуры угроз и обновлять базы данных вредоносного ПО.
   3.3. Интеграция с Active Directory или другими системами аутентификации помогает контролировать доступ пользователей на уровне ролей.
   3.4. Возможность синхронизации с облачными решениями безопасности для обеспечения защиты гибридных инфраструктур.

Критерий	FW	NGFW
Фильтрация	На основе IP-адресов, портов и протоколов	Фильтрация на основе приложений и пользователей
Контроль приложений	Отсутствует	Встроен
Система предотвращения атак (IPS)	Не интегрирована	Интегрирована
Дешифровка SSL	Не поддерживается	Возможна
Защита от угроз	Ограниченная	Расширенная, включая анализ трафика на уровне приложений
Обновления	Редкие	Частые, для защиты от актуальных угроз

Плюсы NGFW

1. Глубокий анализ трафика, включая уровень приложений.
2. Интеграция с другими инструментами безопасности (IDS/IPS, антивирусы).
3. Возможность детектирования современных угроз, таких как целевые атаки.
4. Более высокая степень контроля над трафиком (идентификация пользователей и устройств).

Минусы NGFW

1. Более высокая стоимость по сравнению с традиционными FW.
2. Требует больше вычислительных ресурсов.

3. Сложность настройки и управления.

Плюсы FW

1. Простота установки и управления.
2. Низкая стоимость.
3. Небольшие требования к оборудованию.

Минусы FW

1. Неспособность анализировать современный трафик, шифрованные данные.
2. Ограниченные функции по защите от сложных угроз.

Примеры использования

Традиционные **FW** используются для фильтрации трафика в малых и средних предприятиях и разграничения сетевого доступа на базовом уровне.

В то время как **NGFW** используется для защиты корпоративных сетей от сложных угроз, включая DDoS-атаки, фишинг, эксплойты. Контроля трафика в облачных инфраструктурах (например, AWS, Azure). Мониторинга и управление доступом сотрудников в больших организациях.

IDS/IPS

Intrusion Detection System (IDS) — это система обнаружения вторжений, которая анализирует сетевой трафик или события на устройствах с целью выявления подозрительных действий или атак. IDS сигнализирует администратору о возможной угрозе, но не предотвращает её.

Intrusion Prevention System (IPS) — это система предотвращения вторжений, которая не только обнаруживает угрозы, но и автоматически блокирует их. IPS работает в режиме «inline», то есть на пути прохождения трафика.

Типы IDS

1. **HIDS (Host-based Intrusion Detection System)** — обнаружение вторжений на уровне хоста:
   1.1. Мониторит действия на конкретном устройстве.
   1.2. Анализирует журналы событий, файлы, системные вызовы и процессы.
2. **NIDS (Network-based Intrusion Detection System)** — обнаружение вторжений на уровне сети:
   2.1. Анализирует весь сетевой трафик, проходящий через мониторинг-систему.
   2.2. Работает на границе сети или в определённом её сегменте.

Характеристика	IDS	IPS
Режим работы	Мониторинг (passive)	Превентивный (inline)
Действие при обнаружении	Уведомление, запись логов	Блокировка трафика, уведомление

Риск влияния на производительность	Низкий	Высокий (так как работает inline)

Методы работы IDS/IPS

1. **Сигнатурный анализ.** Сравнивает данные с базой известных сигнатур атак. У него высокая точность для известных угроз, но неэффективен против новых атак (нуль-день).
2. **Анализ аномалий.** Определяет отклонения от нормального поведения системы. Он способен на обнаружение новых, неизвестных угроз, но высокий уровень ложных срабатываний.
3. **Гибридные методы.** Комбинация сигнатурного анализа и анализа аномалий, что создает баланс между точностью и обнаружением новых угроз.

Примеры использования IDS

1. **Snort (NIDS)** — это широко используемая система обнаружения вторжений с открытым исходным кодом. Она работает на основе сигнатурного анализа. Используется для мониторинга сетевого трафика в корпоративных сетях, выявления подозрительных активностей, таких как сканирование портов или попытки взлома, логирование атак для последующего анализа.
2. **OSSEC (HIDS)** — это хостовая IDS, которая анализирует системные логи, файлы и процессы. Используется для обеспечения безопасности серверов в облачных средах, контроля действий пользователей и изменений в системных файлах.

Примеры использования IPS

1. **Cisco Firepower** — это интегрированное решение для предотвращения атак, включающее анализ трафика и блокировку угроз. Используется для защиты корпоративных сетей от атак типа DDoS, интеграции с межсетевыми экранами для максимального уровня безопасности.
2. **Palo Alto Networks** — это аппаратно-программное решение, включающее в себя IPS и возможности межсетевого экрана нового поколения. Используется для защиты банковских и финансовых учреждений от целевых атак, автоматического предотвращение проникновения вредоносного ПО.

Плюсы IDS

1. **Раннее обнаружение атак**. IDS позволяет выявить попытки взлома до того, как они приведут к ущербу.
2. **Анализ данных.** Логи событий помогают в дальнейшем изучении инцидентов и поиске уязвимостей.
3. **Минимальное влияние на сеть.** IDS работает в пассивном режиме, не влияя на пропускную способность сети.

Минусы IDS

1. **Отсутствие защиты в реальном времени**. IDS только сигнализирует об угрозах, но не предотвращает их.
2. **Ложные срабатывания**. Высокий уровень ложных тревог требует ручной проверки.
3. **Неэффективность против сложных атак.** Сигнатурный анализ не справляется с атаками «нуль-день».

Плюсы IPS

1. **Автоматическое предотвращение атак**. IPS активно блокирует угрозы, предотвращая их проникновение в сеть.
2. **Реакция в реальном времени.** IPS быстро реагирует на инциденты без вмешательства человека.
3. **Интеграция с другими системами безопасности**. Может быть частью комплексных решений (например, межсетевые экраны нового поколения).

Минусы IPS

1. **Высокая вероятность ложных блокировок**. Может блокировать легитимный трафик, нарушая работу системы.
2. **Снижение производительности**. Работая «inline», IPS может замедлить прохождение трафика через сеть.
3. **Сложность настройки.** Для эффективной работы требуется тщательная настройка, чтобы минимизировать ложные срабатывания.

NTA

Network Traffic Analysis (NTA) — это процесс мониторинга, анализа и интерпретации сетевого трафика с целью выявления угроз, аномалий и обеспечения кибербезопасности. NTA позволяет собирать данные о сетевых взаимодействиях, анализировать их в реальном времени или постфактум и выявлять потенциальные угрозы, такие как несанкционированный доступ, утечка данных или действия злоумышленников.

Главной задачей NTA является проактивное обнаружение атак на основе анализа поведения трафика, что позволяет защищать сети даже от новых и ранее неизвестных угроз, которые не могут быть выявлены традиционными системами, основанными на сигнатурах.

Основные концепции и технологии NTA

1. **Методы анализа сетевого трафика.**
   1.1. Потоковый анализ (Flow-based analysis) использует метаданные сетевых потоков, такие как NetFlow, sFlow или IPFIX, для выявления аномалий. Потоковый анализ фокусируется на характеристиках взаимодействий (например, объем трафика, частота запросов) без детального анализа содержания.
   1.2. Глубокий анализ пакетов (Deep Packet Inspection, DPI) изучает содержимое сетевых пакетов, включая заголовки и полезную нагрузку, что позволяет

обнаруживать специфические угрозы или подозрительные данные. Этот метод часто применяется в дополнение к потоковому анализу.

1.3. Анализ поведенческих аномалий — это выявляет нетипичное поведение пользователей или устройств в сети на основе сравнения текущей активности с базовой линией (baseline).

2. **Использование машинного обучения и искусственного интеллекта.**
   2.1. Обучение на основе исторических данных используется для создания моделей нормального поведения трафика и выявления отклонений.
   2.2. Классификация аномалий, когда машинное обучение помогает не только находить аномалии, но и классифицировать их (например, как DDoS-атаки, фишинг или проникновение).
   2.3. Автоматизация реагирования — ИИ позволяет автоматизировать принятие решений по предотвращению угроз (например, блокировку подозрительного IP-адреса).
3. **Инструменты и платформы для анализа NTA.**
   3.1. Zeek (ранее Bro) — это система анализа сетевого трафика с возможностью создания пользовательских политик безопасности.
   3.2. Wireshark — популярный инструмент для анализа сетевых пакетов в режиме реального времени.
   3.3. Corelight — это платформа корпоративного уровня для анализа трафика на основе Zeek.
   3.4. Darktrace использует машинное обучение для автоматического выявления аномалий и угроз в сетевом трафике.
4. **Реализация NTA в реальном времени и в режиме оффлайн.**
   4.1. Реальное время (Real-time monitoring). Системы анализа трафика обрабатывают данные мгновенно, что позволяет оперативно реагировать на инциденты.
   4.2. Анализ после события (Post-event analysis). Используется для расследования инцидентов и улучшения стратегий защиты.
5. **Интеграция с другими системами безопасности**. NTA может быть интегрирована с системами обнаружения вторжений (IDS), межсетевыми экранами (firewalls) и SIEM-системами для повышения уровня киберзащиты.

Плюсы NTA

1. **Проактивное обнаружение угроз.** NTA позволяет выявлять аномалии и угрозы, которые не могут быть обнаружены традиционными средствами защиты, такими как антивирусы или межсетевые экраны.
2. **Широкая видимость сети.** Анализ трафика даёт полное представление о том, что происходит в сети, включая скрытые или несанкционированные взаимодействия.
3. **Поддержка машинного обучения и автоматизации.** Использование интеллектуальных алгоритмов снижает нагрузку на специалистов и ускоряет реакцию на инциденты.
4. **Гибкость в настройке.** NTA-системы можно адаптировать под конкретные потребности компании или организации.

5. **Реализация в реальном времени.** Возможность оперативного анализа сетевого трафика позволяет блокировать угрозы ещё до того, как они нанесут ущерб.

Минусы NTA

1. **Высокая стоимость внедрения.** Настройка и поддержка NTA-систем требуют значительных инвестиций в оборудование, программное обеспечение и специалистов.
2. **Сложность настройки.** Создание базовой линии для анализа требует времени и экспертизы, а некорректная настройка может привести к высокому количеству ложных срабатываний.
3. **Большой объём данных.** Анализ сетевого трафика генерирует огромное количество данных, что может быть проблемой для хранения и обработки.
4. **Ложные срабатывания.** NTA может ошибочно классифицировать легитимные действия как угрозы, что увеличивает нагрузку на специалистов по безопасности.
5. **Ограничения в зашифрованных сетях.** Зашифрованный трафик затрудняет анализ, так как NTA не имеет доступа к содержимому пакетов.
6. **Зависимость от качества данных.** Эффективность NTA зависит от точности данных, собираемых с помощью сетевых сенсоров. Пропущенные данные могут снизить точность анализа.

Применение NTA в киберзащите

1. **Выявление аномалий и кибератак.** NTA активно используется для обнаружения аномального поведения в сети, которое может свидетельствовать о вредоносной активности, что подразумевает атаки типа DDoS (распределённые атаки на отказ в обслуживании), проникновения в сеть (например, через эксплойты или фишинг), вредоносные программы, использующие сеть для передачи данных.
2. **Обнаружение угроз нулевого дня (Zero-day).** Использование моделей машинного обучения позволяет выявлять неизвестные ранее угрозы, которые не обнаруживаются традиционными методами, основанными на сигнатурах.
3. **Защита IoT-устройств.** Сети, включающие устройства Интернета вещей (IoT), уязвимы к атакам из-за слабой защиты этих устройств. NTA помогает идентифицировать подозрительное поведение IoT-устройств и предотвращать использование их в ботнетах, таких как Mirai.
4. **Обеспечение соответствия требованиям безопасности.** NTA используется для мониторинга и документирования сетевой активности, что важно для соблюдения стандартов безопасности, таких как GDPR, PCI DSS и HIPAA.