Министерство образования Республики Беларусь
Учреждение образования
«Брестский государственный технический университет»
Кафедра ИИТ

Реферат
За седьмой семестр
По дисциплине: «Современные методы защиты компьютерных систем»

Выполнила:
Студентка 4 курса
Группы ИИ-21(II)
Соболева П.С.

Проверила:
Хацкевич М. В.

Брест 2024

Вариант 11(2)

Вопросы:

1. SOC.
2. FW/NGFW.
3. IDS/IPS.
4. NTA.

1. Центр управления безопасностью (**SOC**) — это **организованная** и **высококвалифицированная команда**, миссия которой заключается в **постоянном мониторинге и улучшении состояния безопасности** организации при **предотвращении, обнаружении, анализе и реагировании** на **инциденты** кибербезопасности с помощью **как технологий**, так и четко определенных **процессов и процедур**.

Поскольку стратегия SOC должна быть четко определена и специфична для бизнеса, она строго зависит от поддержки и спонсорства со стороны руководства, в противном случае сам SOC не сможет работать должным образом, и он не будет восприниматься остальной частью организации как критически важный актив. SOC должен быть направлен на удовлетворение потребностей компании, и для его успеха необходима сильная поддержка со стороны руководства.

Создание SOC требует тщательного планирования; необходимо принимать во внимание его физическую безопасность; Кроме того, **планировка** операционного центра должна быть тщательно продумана, чтобы быть одновременно удобной и функциональной — нельзя упускать из виду вопросы **освещения** и **акустики**. Ожидается, что SOC будет состоять из нескольких зон, включая оперативную комнату, «военную комнату» и кабинеты руководителей. Комфорт, видимость, эффективность и контроль являются ключевыми терминами в этом сценарии, и каждая отдельная зона должна быть спроектирована соответствующим образом.

После того, как миссия и сфера деятельности SOC определены, необходимо спроектировать его базовую инфраструктуру; Для создания полноценной технологической среды необходимо множество компонентов: **межсетевые экраны, IPS/IDS, решения для обнаружения нарушений**, зонды и, конечно же, **SIEM,** и это лишь некоторые из них. Эффективный и действенный сбор данных имеет основополагающее значение для успешной работы SOC. Потоки данных, телеметрия, захват пакетов, системный журнал и несколько типов событий должны быть собраны, сопоставлены и проанализированы с точки зрения безопасности. Также большое значение имеет обогащение данных и информация об уязвимостях, влияющих на всю отслеживаемую экосистему.

Несмотря на то, что технические требования имеют первостепенное значение, самая современная и лучше всего оборудованная диспетчерская была бы бесполезной без **людей и процедур**, воплощающих ее в жизнь! Помимо технологий, люди и процессы являются столпами успешной SOC.

Как было сказано выше, **SOC — это команда**; И, как и в каждой победившей команде, все правила должны выполняться должным образом. Потребуются лидеры (и лидерство), в то время как инженерные, аналитические и операционные роли должны быть охвачены. Необходимо выполнить множество функций, и аналитики будут **распределены по двум или трем уровням**. Основными функциями членов команды будут анализ, основанный на реальном мониторинге событий, обнаружение **инцидентов безопасности или утечек данных**, реагирование на эти инциденты (после необходимой фазы сортировки) и, наконец, устранение последствий каждого обнаруженного инцидента. Все действия должны быть скоординированы: сотрудничество, сроки и эффективность должны иметь первостепенное значение для всей организации SOC. Каждый член команды должен быть **полностью осведомлен как о миссии, так и о стратегии** SOC; Таким образом, эффективное лидерство имеет огромное влияние. Менеджер SOC должен уметь формировать команду, мотивировать ее членов, удерживать людей и вызывать у них желание создавать **ценность** для бизнеса и для себя. Это непростая задача для менеджера SOC: «машина» должна работать 7 дней в неделю, 24 часа в сутки, поэтому стресс будет вероятным фактором риска. Выбор правильных членов команды для выполнения правильных задач — очень сложная задача, поскольку диапазон требуемых компетенций довольно широк: от **управления уязвимостями** до **компьютерной криминалистики** **анализа вредоносного ПО**. Установление надлежащего числа сотрудников является еще одной трудной и ответственной задачей; Несмотря на то, что не следует нанимать ненужных работников и необходимо соблюдать определенный уровень бюджета, необходимо избегать риска нехватки персонала и, следовательно, неэффективности.

В этом сценарии принятие гибридной модели, предусматривающей сотрудничество между внутренними и внешними поставщиками управляемых услуг, является жизнеспособным выбором.

Более глубокий анализ технологических компонентов, поддерживающих SOC, не может быть отделен от сильного акцента на безопасности; **Нельзя**упускать из виду каждую деталь глубокого подхода: сегментация локальной сети, **NAC, VPN,** усиление защиты конечных точек, **шифрование** данных при хранении, использовании и перемещении, защита с помощью хорошо **настроенных и контролируемых IPS/IDS, межсетевых экранов, маршрутизаторов и коммутаторов**. Поскольку SOC является командой, инструменты для совместной работы должны быть тщательно разработаны, чтобы предоставить участникам наилучший пользовательский опыт, что, в свою очередь, даст SOC наилучшие возможности для создания ценности для бизнеса: эта цель должна быть достигнута с учетом всех требований

к обеспечению безопасности, необходимых для центра управления безопасностью. Мобильные устройства (и их безопасность) — еще один аспект, которым нельзя пренебрегать при проектировании и создании SOC. Особое внимание следует уделять мерам по предотвращению потери данных, начиная от конечных точек и заканчивая серверами, от электронной почты до смартфонов.

Не хочу быть исчерпывающим, но следует упомянуть и многие другие технологические компоненты, которые вносят свой вклад в завершение всей экосистемы SOC: веб-прокси, песочницы, решения для обнаружения утечек конечных точек и инструменты криминалистики. Все задействованные системы генерируют **события, журналы, потоки и телеметрические данные**, которые должны быть приняты, обработаны и проанализированы машиной и, в конечном итоге, человеком. На этом этапе приема, обработки и корреляции стоит еще раз вспомнить о ключевой роли **SIEM** для Центра управления безопасностью.

Чтобы повысить уровень безопасности организации, SOC должен быть как активным, так и упреждающим при выполнении процесса управления уязвимостями. **Оценка рисков**и разумный подход к работе с уязвимостями является приоритетом для SOC (методология **OWASP** в этом случае может быть вариантом). Кроме того, необходимо использовать контекстнозависимый подход к **анализу угроз**, чтобы обеспечить большую ценность и быть более эффективным в обнаружении/предотвращении нарушений и сдерживании ущерба.

Как только SOC заработает в реальной среде, команде придется выполнять свою миссию и реагировать на инциденты. Это этап, на котором SOC имеет возможность показать ценность, которую он предоставляет бизнесу. Когда возникает инцидент, открывается тикет и дело будет расследовано. В инцидент будут вовлечены многие члены команды, возможно, кто-то за пределами SOC (часть той же организации или даже сторонний субъект), в зависимости от характера, масштаба и серьезности инцидента. Могут быть введены различные уровни эскалации, которые могут привести к **CSIRT**, и команда должна сотрудничать, используя все доступные инструменты и процедуры до закрытия дела.

Для достижения успеха обнаружение и мониторинг инцидентов безопасности, а также последующий этап реагирования на инциденты требуют правильного сочетания надежных технологий, четко определенных (и повторяемых) процессов и процедур, а также узкоспециализированных навыков. Интуиция, умение быстро и точно реагировать даже в стрессовых условиях и опора на ранее полученные уроки являются ключевыми моментами для эффективной команды SOC.

Создание и эксплуатация SOC — это очень сложная задача, для выполнения которой могут оказаться полезными многие передовые практики, фреймворки и стандарты (например, **ITIL** и **COBIT),** а другие могут быть обязательными для соблюдения (например, **PCI DSS** и **ISO/IEC 27001:2013**).

ITIL заслуживает особого упоминания как потенциально беспрецедентный источник советов и рекомендаций по**стратегии и проектированию обслуживания, управлению уровнем обслуживания** (**SLA** и **KPI** должны быть четко сформулированы, измеряться и контролироваться) и по созданию интерфейса между процессами управления инцидентами/проблемами организации и процессами, специфичными для SOC.

С другой стороны, COBIT — и, в частности, **COBIT MM (модель зрелости)** — может быть принят в качестве первостепенного ориентира для измерения зрелости SOC.

Вообще говоря, эффективность SOC должна быть тщательно измерена во всех ее аспектах, четкое определение KPI является обязательным, а разумное применение постоянного улучшения услуг (ITIL, опять же, должно быть принято во внимание) может дать SOC наилучшие результаты в плане успеха и восприятия его как ценности для организации.

Широкий спектр — можно сказать, полный спектр — аспектов кибербезопасности, которые необходимо учитывать, высокоспециализированные компетенции и навыки, необходимые для эффективного управления SOC, тесная взаимосвязь с бизнес-стратегией и процессами делают задачу проектирования и управления Security Operations Center образцовым примером прикладной и целостной информационной безопасности.

Лидерство, мотивация и навыки лидерства в команде являются обязательными для менеджера SOC, желающего создать отличную команду. Непрерывное обучение и взаимодействие необходимы для того, чтобы темп SOC соответствовал неустанному развитию угроз и неустанным, все более изощренным усилиям злоумышленников. Управление SOC является столь же сложной задачей, как и решение столь же широкой, всеобъемлющей и безграничной проблемы обеспечения информационной безопасности в настоящее время.

2. Межсетевой экран или FireWall (FW) — это программный или программно-аппаратный комплекс, предназначенный для фильтрации сетевого трафика на основании набора правил. Основной задачей межсетевого экрана является предотвращения несанкционированного доступа к сети организации.

Устанавливается FireWall как правило на границе сети так, чтобы весь сетевой трафик проходил через него. Принцип работы заключается в анализе и блокировке подозрительного трафика до того, как он попадет в сеть организации. Подобный принцип защиты периметра сети используется и развивается давно.

В современном мире межсетевые экраны дополнены различным набором инструментов и перешли в другой класс решений — UTM (Unified threat management — универсальное управление угрозами) и NGFW (Межсетевые экраны следующего поколения).

Межсетевые экраны уже давно являются краеугольным камнем сетевой безопасности, выступая в качестве первой линии защиты от киберугроз. С годами технология межсетевых экранов значительно претерпела изменения, и межсетевые экраны нового поколения (NGFW) стали революционным достижением. В этой статье мы сравним межсетевые экраны NGFW и традиционные межсетевые экраны на основе ключевых параметров, чтобы помочь вам принять обоснованное решение при выборе подходящего межсетевого экрана для вашей организации.

1. Видимость приложений и контроль приложений:

- *Традиционный брандмауэр:* Обеспечивает частичную видимость приложений и ограниченный контроль.
- *Межсетевой экран нового поколения (NGFW):* Предоставляет подробные аналитические сведения о приложениях и обеспечивает детальный контроль над ними. NGFW могут идентифицировать и контролировать приложения на уровне 7, что делает их очень эффективными в управлении сетевым трафиком.

2. Капитальные и эксплуатационные расходы:

- *Традиционный брандмауэр:* Как правило, это влечет за собой более высокие капитальные (CAPEX) и операционные (OPEX) затраты, поскольку организациям необходимо приобретать и обслуживать несколько устройств для различных услуг безопасности.
- *Межсетевой экран нового поколения (NGFW):* Обеспечивает значительное снижение затрат, поскольку объединяет несколько служб в одном устройстве. Такая консолидация не только снижает первоначальные затраты, но и упрощает текущее техническое обслуживание.

3. IPS (система предотвращения вторжений):

- *Традиционный брандмауэр:* Не поддерживает систему предотвращения вторжений.
- *Межсетевой экран нового поколения (NGFW):* Поддерживает IPS, повышая безопасность за счет активного мониторинга и предотвращения попыток вторжения.

4. NAT (трансляция сетевых адресов):

- *Традиционный брандмауэр:* Поддерживает NAT, что позволяет транслировать частные IP-адреса в публичные.
- *Межсетевой экран нового поколения (NGFW):* Также поддерживает NAT, обеспечивая совместимость с существующими сетевыми конфигурациями.

5. Услуги по репутации и идентификации:

- *Традиционный брандмауэр:* Не поддерживает службы репутации и идентификации.
- *Межсетевой экран нового поколения (NGFW):* Предоставляет надежные службы репутации и идентификации, которые имеют решающее значение для расширенного обнаружения угроз и аутентификации пользователей.

6. Фильтрация трафика (на основе порта, IP-адреса и протокола):

- *Традиционный брандмауэр:* Поддерживает базовую фильтрацию трафика на основе портов, IP-адресов и протоколов.
- *Межсетевой экран нового поколения (NGFW):* Предлагает те же возможности фильтрации трафика, но добавляет расширенную осведомленность на уровне приложений для более точного управления.

7. VPN (виртуальная частная сеть):

- *Традиционный брандмауэр:* Поддерживает функцию VPN для безопасного удаленного доступа.
- *Межсетевой экран нового поколения (NGFW):* Также поддерживает VPN, обеспечивая безопасную связь по публичным сетям.

8. Осведомленность на уровне приложения:

- *Традиционный брандмауэр:* Недостаточная осведомленность на уровне приложения.
- *Межсетевой экран нового поколения (NGFW):* Превосходно осведомлен о приложениях на уровне приложений, обеспечивая детальный контроль над приложениями и их поведением.

9. Рабочий слой:

- *Традиционный брандмауэр:* Работает от уровня 2 до уровня 4 модели OSI.
- *Межсетевой экран нового поколения (NGFW):* Функционирует от уровня 2 до уровня 7, что делает его способным к глубокой проверке пакетов и принятию решений на уровне приложений.

10. Пропускная способность и производительность:

- *Традиционный брандмауэр:* Обеспечивает меньшую пропускную способность и может значительно снизить производительность при внедрении дополнительных служб безопасности.
- *Межсетевой экран нового поколения (NGFW):* Обеспечивает гораздо более высокую пропускную способность по сравнению с традиционными межсетевыми экранами и поддерживает стабильную производительность даже при включенных дополнительных службах безопасности.

11. Отчетность:

- *Традиционный брандмауэр:* Обычно предлагает стандартные отчеты.
- *Межсетевой экран нового поколения (NGFW):* Предоставляет настраиваемые параметры отчетности, позволяя организациям создавать отчеты, адаптированные к требованиям пользователя. Он также предлагает подробную информацию практически в режиме реального времени и поддерживает различные форматы загрузки.

В заключение следует отметить, что межсетевые экраны нового поколения (NGFW) превосходят традиционные межсетевые экраны в различных аспектах, включая видимость приложений, экономичность, функции безопасности и производительность. Межсетевые экраны межсетевого экранирования (NGFW) разработаны в соответствии с требованиями современных сетей, в которых первостепенное значение имеют контроль на уровне приложений, предотвращение угроз и эффективное управление.

При выборе между межсетевым экраном межсетевого экрана и традиционным межсетевым экраном важно учитывать конкретные требования вашей организации, а также уровень безопасности и контроля, необходимый для эффективной защиты вашей сети.

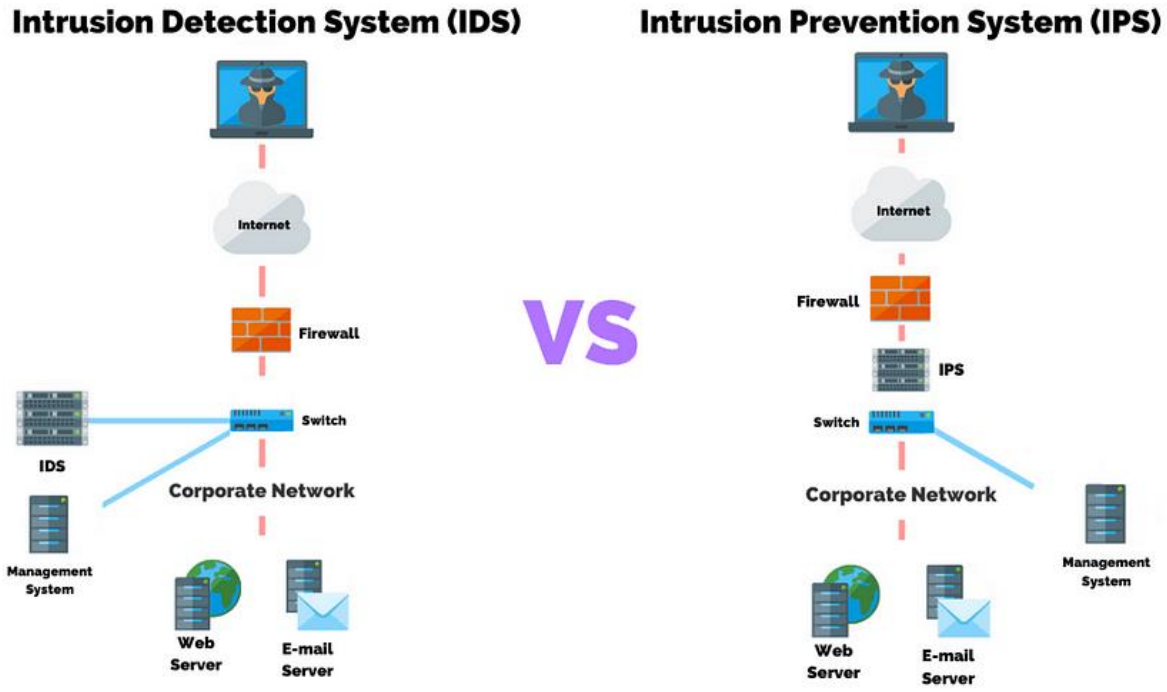
3. IDS (Intrusion Detection System) и IPS (Intrusion Prevention System) — это как цифровые охранники для вашей компьютерной сети.

Обнаружение вторжений — это процесс мониторинга сетевого трафика и его анализа на наличие признаков возможных вторжений, таких как попытки использования эксплойтов и инциденты, которые могут представлять непосредственную угрозу для вашей сети. В свою очередь, предотвращение вторжений — это процесс обнаружения вторжений и последующей остановки обнаруженных инцидентов, обычно выполняемый путем отбрасывания пакетов или завершения сеансов. Эти меры безопасности доступны в виде систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS), которые являются частью мер безопасности сети, принимаемых для обнаружения и предотвращения потенциальных инцидентов, и включены в функции межсетевых экранов нового поколения (NGFW).

- IDS отслеживает сетевой трафик и ищет подозрительную активность или признаки несанкционированного доступа, например, камера видеонаблюдения следит за необычными движениями.
- IPS не только обнаруживает подозрительную активность, но и принимает меры по ее блокировке или предотвращению в режиме реального времени, как охранник, который не только замечает злоумышленников, но и не дает им проникнуть в здание.

IDS/IPS отслеживает весь трафик в сети для выявления любого известного вредоносного поведения. Одним из способов, с помощью которого злоумышленник может попытаться скомпрометировать сеть, является эксплуатация уязвимости в устройстве или в программном обеспечении. IDS/IPS выявляет эти попытки использования эксплойтов и блокирует их до того, как они успешно скомпрометируют любые конечные точки в сети. IDS/IPS являются необходимыми технологиями безопасности как на границе сети, так и в центре обработки данных, именно потому, что они могут остановить злоумышленников во время сбора информации о вашей сети.

Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) — это технологии кибербезопасности, которые отслеживают сетевой трафик на предмет подозрительной активности. IDS обнаруживает атаки и техники, в то время как IPS останавливает обнаруженные инциденты.



IDS использует три методологии обнаружения:

- Обнаружение на основе сигнатур: сравнивает сигнатуры с наблюдаемыми событиями
- Обнаружение на основе аномалий: сравнивает определения нормальной активности с наблюдаемыми событиями
- Анализ протокола с отслеживанием состояния: сравнивает заранее определенные профили доброкачественной активности протокола с наблюдаемыми событиями

IDS обнаруживает угрозы и отправляет оповещения при обнаружении угрозы. IDS может быть развернута на определенном узле или на сетевом уровне. Существует два типа IDS:

- Сетевые (NIDS): развертываются в стратегических точках компьютерной сети
- Host-based (HIDS): еще один тип IDS

IPS отслеживает сетевой трафик в режиме реального времени, сравнивает его с известными шаблонами атак и сигнатурами и блокирует любую вредоносную активность или трафик, нарушающий сетевые политики. IPS может немедленно блокировать или предотвращать подозрительные или несанкционированные действия, такие как отбрасывание пакетов, закрытие соединений или перенастройка сетевых правил.

IDS и IPS могут работать вместе с межсетевыми экранами, чтобы помочь блокировать злоумышленников, которые стремятся украсть конфиденциальные данные, вызвать утечку данных и установить вредоносное ПО. Как IDS, так и IPS могут страдать от ложноположительных или ложноотрицательных срабатываний. Более сложная система будет иметь меньший процент ошибок.

Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) постоянно следят за вашей сетью, выявляя возможные инциденты и регистрируя информацию о них, останавливая инциденты и сообщая о них администраторам безопасности. Кроме того, некоторые сети используют IDS/IPS для выявления проблем с политиками безопасности и предотвращения нарушения политик безопасности. IDS/IPS стали необходимым дополнением к инфраструктуре безопасности большинства организаций именно потому, что они могут остановить злоумышленников, пока они собирают информацию о вашей сети.

Короче говоря, IDS предупреждает вас о потенциальных угрозах, в то время как IPS активно защищает вашу сеть, пресекая эти угрозы.

4. Анализ сетевого трафика (NTA) — это метод мониторинга доступности и активности сети для выявления аномалий или потенциальных угроз безопасности. Его цель — понять и оптимизировать поток данных в сети.

Анализ сетевого трафика обычно используется в следующих областях:

1. Улучшение внутренней видимости сети. NTA также предоставляет вам надлежащий контекст вашей сети, такой как пользователи в вашей сети, с какими устройствами они взаимодействуют, какие данные они обмениваются и т. д. Сбор записей о том, что происходит в вашей сети в режиме реального времени.
2. Заблаговременное обнаружение угроз. например, обнаружение вредоносных программ или программ-вымогателей, а также любых угроз безопасности.
3. Возможность мониторинга всех узлов сети, устранение неполадок в медленной сети, устранение слепых зон и т.д.

Ключевые преимущества анализа сетевого трафика:

1. Высокая производительность сети
2. Улучшенная видимость сети
3. Высочайшая доступность сети
4. Мониторинг трафика/устройств IoT
5. Автоматическое обнаружение аномалий

Инструменты, используемые для анализа сетевого трафика:

1. Анализатор сетевого трафика Cisco
2. Анализатор NetFlow
3. Анализатор трафика SolarWinds NetFlow
4. Управление модулем NetFlow Analyzer
5. Эластичный стек

Цель или задача анализа и мониторинга сетевого трафика:

1. **Комплексная визуализация вашей сети:** Прозрачность является одним из основных преимуществ анализа сетевого трафика. Анализ сетевого трафика (NTA) может помочь повысить безопасность, обеспечивая

лучшую видимость сетей и аномальную сетевую активность, которая может указывать на потенциальную атаку.

2. **Обнаружение потоков в режиме реального времени:** Инструменты анализа сетевого трафика предоставляют возможности мониторинга и анализа в режиме реального времени, позволяя просматривать сетевой трафик по мере его возникновения. NTA может помочь организации обнаружить вредоносную деятельность, способствуя обнаружению кибератак и оповещая команду безопасности об угрозе. Эта функция имеет решающее значение для оперативного выявления инцидентов безопасности и реагирования на них.

3. **Автоматическое определение потока:** Инструмент сетевого анализа обеспечивает автоматический мониторинг сетевого трафика. Он автоматизирует процессы обнаружения угроз, обнаруживает любую подозрительную активность и группирует ее как атаку с помощью заранее определенного алгоритма, который обнаруживает любую подозрительную активность. Это помогает сократить объем ресурсов, необходимых для эффективной защиты критически важных активов предприятия.

Анализ сетевого трафика — это важный способ мониторинга доступности и активности сети для выявления аномалий, максимизации производительности и отслеживания атак. Анализ сетевого трафика добавляет еще один уровень в вашу среду кибербезопасности и обеспечивает улучшенную видимость корпоративной среды. NTA обеспечивает упреждающий мониторинг, обнаружение угроз и реагирование на инциденты, помогая организациям выявлять и снижать риски безопасности.