????????????

Средства защиты

Мониторинг ИБ автоматизируют с помощью LM/SIEM, UBA/UEBA, IRP/SOAR, TIP, IDS/IPS, NTA, EDR, XDR, DDP. Постоянно развивается.

Log Management

Может быть в виде специализированного решения или унифицированного варианта, типа Elastic Stack. Централизованное хранилище журналов событий различных источников, приведенные к единой модели данных. Простой, гибкий и производительный поиск по событиям, отчёты и визуальные панели (дашборды) на основе таких поисков, но без корреляции событий на потоке. LM дешевле SIEM решение. Может работать рядом с SIEM. Задачи Log Management;

- Изучение логов в производительной среде.
- Оценка нагрузки на источник от передачи событий в стороннюю систему. Можно изучить и нагрузку на сеть. Помню случай, когда трафик проходил через межсетевой экран по пути от одной подсети сегмента в другую. Поток Syslog-событий большого объёма привёл к отказу в обслуживании на данном файрволе.
- Понимание необходимости дополнительных логгеров на существующих источниках по результатам расследований. События Sysmon могут быть информативнее событий Windows. А Auditbeats фиксирует то же, что и auditd, но не дробит единое событие на четыре строки, что требует дополнительной корреляции и лицензионной квоты.
- Оценка потока событий. У интеграторов и производителей есть калькуляторы, которые позволяют теоретически оценить какое количество событий в среднем генерирует каждый тип источника событий. На практике генерация событий источниками зависит от их функций и нагруженности.
- Привести инфраструктуру в соответствие с политиками и регламентами. Для большинства этих кейсов корреляция не требуется. LM позволит выявлять несоответствие политикам (использование неразрешенного ПО, не регламентированных подключений к сетевым портам и т.д.).
- Организовать Threat Hunting и расследование инцидентов. LM для данной задачи — единственная необходимая платформа. Например, вы видите вредоносный DNS-запрос на межсетевом экране, в журнале МЭ фигурирует в качестве инициатора контроллер домена, для выявления хоста инициатора необходимо еще проанализировать журналы DNS-сервера для определения какой хост выполнял запрос и на нем анализировать вредоносный процесс.

Security Information and Event Management(SIEM)

Система управления информацией и событиями в системе безопасности. Объединяет в одной точке данные об инцидентах ИБ. Собирает информацию из журналов событий средств защиты, сетевого оборудования, рабочих станций сотрудников и других ресурсов — тем самым исключает необходимость проверять их по отдельности и снижает риск возникновения слепых зон. Задачи SIEM:

- нормализация данных различных источников в единообразный и пригодный для обработки формат;
- мониторинг и консолидация событий безопасности со всех систем и устройств корпоративной сети;
- обогащение данных о событиях связанной информацией из других ресурсов;
- регистрация инцидентов на основе заданных правил корреляции — взаимосвязей между событиями и их цепочками, в том числе из разных источников;
- информирование оператора об инциденте через чат-бот, email-сообщение, уведомление в интерфейсе системы и другими способами;
- хранение исторических данных о всех событиях ИБ и поддержка при расследовании инцидентов;
- анализ и управление рисками безопасности, проверка на соответствие стандартам и требованиям регуляторов;
- формирование отчетных документов для внутренних целей и контролирующих органов.

Компоненты SIEM

- агенты, устанавливаемые на инспектируемую информационную систему (актуально для операционных систем (агент представляет собой резидентную программу (сервис, демон), которая локально собирает журналы событий и по возможности передает их на сервер);
- коллекторы на агентах, которые, по сути, представляют собой модули (библиотеки) для понимания конкретного журнала событий или системы;
- серверы-коллекторы, предназначенные для предварительной аккумуляции событий от множества источников;
- сервер-коррелятор, отвечающий за сбор информации от коллекторов и агентов и обработку по правилам и алгоритмам корреляции;
- сервер баз данных и хранилища, отвечающий за хранение журналов событий.

ServiceDesk, IRP, SOAR

Система обработки заявок. Изначально при построении SOC, может не быть Incident Response Platform(IRP) или Security Orchestration, Automation and Response(SOAR), для фиксации и описания деталей инцидента в минимальном формате подходит ServiceDesk.

IRP/SOAR — это специализированный ServiceDesk с функцией исполнения скриптов. Если у вас получится закрыть часть требований встроенным функционалом, вам необходимо получить более простые и стабильные способы работы со скриптами или дать службе мониторинга отдельный от ИТ инструмент со специализированным интерфейсом.

Автоматизация способна ускорить реагирование на часть кейсов на 1-2 порядка. Второй вариант использования — учёт действий аналитика. Если в инциденте участвует критичный актив, например, АСУ ТП, каждый шаг должен быть выполнен компетентным сотрудником, который ответственен за решение, ничего не должно быть пропущено, действия должны журналироваться.

Основные функции IRP, SOAR

- Единая регистрация всех инцидентов безопасности в системе. IRP поддерживает работу в режиме «одного окна», где происходит создание, выполнение задач, контроль их состояния.
- Ускорение отклика на инциденты. За счет автоматизированного анализа, сбора дополнительной информации для расследования инцидентов путем интеграции различных СЗИ, проведения коррекции ответных мер на основании анализа разных источников угроз.
- Своевременное оповещение соответствующих лиц в системе о наступлении критически важных инцидентов. Реализуется за счет локальных сообщений в местных интерфейсах, электронной почты, мессенджеров, sms.
- Предоставление актуальной статистики, иллюстрирующей текущее состояние IT-активов, число инцидентов, уязвимостей, выборка данных по требующимся метрикам.
- Предоставление единого централизованного инструмента для выполнения инвентаризации IT-активов компании. Посредством IRP можно собрать полную информацию о текущих IT-активах на базе одного решения, предоставить пользователям права доступа в систему на основе разграничения прав. Эти процессы автоматизированы, затрагивают полный жизненный цикл IT-активов, что в разы повышает удобство и эффективность управления ими.

Пример информации:

- время первого и последнего события;
- плановые сроки взятия в работу и решения;
- таймлайн событий инцидента и общее количество событий;
- критичность;
- признак массового инцидента;
- принадлежность к техникам и тактикам;
- тэги инцидента и другое.

Жизненный цикл инцидента

Для оценки уровня реагирования на инциденты ИБ необходимо понимание жизненного цикла инцидента. Основные метрики жизненного цикла инцидента:

- Среднее время регистрации заявки с подозрением на инцидент(MTTD). Отправка события ИБ в SIEM, регистрация заявки в IRP, предобработка, обогащение данными.

- Среднее время подтверждение инцидента(MTTA). Аналитик берет инцидент в работу, анализирует и подтверждает инцидент.
- Среднее время локализация инцидента(MTTC). Изоляции зараженного хоста от рабочего сегмента сети.
- Среднее время, необходимое на восстановление работоспособности системы после получения сигнала о сбое или кибератаке(MTTR).

EDR

Входит в состав антивирусной защиты, систем защиты от утечек данных и т.д. Но функционал — это дополнительная телеметрия (Detection в Endpoint Detection and Response) и возможности по реагированию (Response).

Телеметрия расширяет и унифицирует функции штатных журналов операционных систем. То, что раньше выявлялось SIEM на основе нескольких событий или не выявлялось вовсе, теперь фиксируется как единая запись агента EDR, обогащённая различными метаданными. И, насколько это возможно, не зависит от семейства и версии операционной системы, на которую установлен агент. EDR содержит следующие функции:

- сбор артефактов, нетипичных журналов событий из системы, например если вам надо оперативно получить потенциально вредоносный файл для анализа, то можно это сделать из консоли управления EDR;
- интерактивный веб-шелл для выполнения удаленно команд на хосте, например для завершения работы вредоносного процесса в системе;
- возможность удаленно и централизованно настраивать аудит событий или фильтрацию.

Реагирование средствами EDR делает процесс максимально оперативным и гибким. Результат использования EDR — расширенная телеметрия и локальное автоматизированное реагирование. На сегодняшний день наиболее эффективны коммерческие решения EDR, но так же есть Open-source EDR решение, например SOLDR или Wazuh.

TIP

Средство обработки входящего Threat Intelligence(TI). TI содержит в себе совокупность индикаторов компрометации (Indicator of Compromise) — IP(Internet Protocol), FQDN(Fully Qualified Domain Name), URL(Uniform Resource Locator), Hash и т.д., которые известны как злонамеренные, так как были ранее зафиксированы в компьютерных атаках. Цель TI - сокращение разрыва между первым обнаружением атаки где-то в мире и возможностью выявлять её у нас в инфраструктуре.

Разве нельзя IOC использовать в средствах защиты напрямую, зачем TIP? Этот класс решений предоставляет функционал управления TI — нормализация, обогащение, дедупликация, приоритезация, хранение, устаревание, удаление.

В систему приходит IOC и подвергается нормализации – приведению к единому набору полей заданного формата. С ним можно связать другие индикаторы – узнать FQDN по IP или всё семейство хэшей по исходному. Если IOC уже есть в базе – добавить атрибуты, например, что мы видели его в данных ещё одного источника в такое-то время. И присвоить ему оценку.

При работе с индикатором аналитик исследует гипотезу, подтверждает или опровергает её, строит граф связей. Результат использования TIP – на средства защиты, в том числе в систему мониторинга, попадает более качественный, однозначно трактуемый и актуальный TI. А перечни IOC сокращаются на порядок, что позволяет повысить эффективность средств защиты, их использующих.

MISP

Одним из основных open-source TIP-платформ является MISP. MISP (Malware Information Sharing Platform) — это открытая платформа для обмена информацией о угрозах, которая используется для обмена, обработки и проверки информации о киберугрозах и их контрмерах. Она была разработана для обеспечения быстрого и эффективного обмена информацией между различными организациями.

MISP предоставляет инструменты для обмена, совместного использования и хранения информации о киберугрозах, включая индикаторы компрометации (IOC), тактики, техники и процедуры (TTP) атак, и пр. Это позволяет организациям быстро адаптироваться к новым угрозам и обеспечивать своевременный и эффективный ответ на инциденты безопасности.

Примеры использования MISP

- Совместное использование информации об угрозах: Компания А может поделиться информацией о недавней фишинговой атаке через MISP. Это поможет другим банкам узнать об этой атаке и принять меры по защите от аналогичных атак.
- Анализ угроз: Исследовательская группа по безопасности может использовать MISP для анализа информации об угрозах, собранной из разных источников, и создания отчетов об угрозах для своих клиентов.
- Обучение и симуляции: Учебные заведения и обучающие центры могут использовать MISP для создания реалистичных сценариев для обучения и симуляции кибератак.

SandBox

При выявлении подозрительных файлов приходится их анализировать. Для безопасного анализа созданы песочницы(SandBox). Запускают файл в изолированной среде и фиксируют все выполненные действия, такие как: запуска процессов, загрузки библиотек, сетевые соединения, DNS-запросы, вызовы WinAPI-функций, создание/удаление файлов и т.д.

Так же события полученные от потоковых песочниц, которые проверяют файлы поступившие на почтовый сервер, можно направить в SIEM-систему, если песочница работает в режим мониторинга без блокировки.

ANYRUN

Удобство и особенность песочницы ANYRUN в том, что есть возможность самому запускать файлы или открывать веб-страницы в интерактивном режим.

Области песочницы поделены на три блока:

- Интерактивное окно виртуальной машины.
- Информация о сетевых соединениях, HTTP, DNS-запросах, IDS-сигнатурах.
- Запущенные процессы и команды.

Cuckoo

Загрузка файлов в облачных песочницах может быть недопустима. Для локального анализа есть open-source решение класса песочницы Cuckoo Sandbox, которую можно развернуть у себя в инфраструктуре. Три блока с информацией:

- О размере файла, тип файла, хэш-суммы.
- Какие YARA-правила сработали и выявлии аномалии.
- Показатель вредоносности файла по 10 бальной шкале.

Ниже детальная информация о сигнатурах. Красным цветом выделены наиболее критичные сигнатуры.

Другие зарубежные облачные песочницы

- https://www.hybrid-analysis.com/
- https://www.vmray.com/

NTA/NBA

Network Traffic Analysis — запись трафика для его последующего исследования. Гораздо больший по сравнению с LM/SIEM объем хранилища и необходимость предварительной расшифровки данных.

Трафик объединяет в себе и информацию, и факт её передачи. В отличие от событий, генерация которых избирательна, он полностью описывает, что произошло между двумя взаимодействующими системами, и его нельзя удалить или сфабриковать. События собираются в LM или SIEM с некоторой задержкой, если это не Syslog, в случае которого возможен спуфинг. А если успеть очистить журнал источника (действие, подозрительное само по себе), что точно случилось узнать будет трудно.

Можно использовать решения класса Network Behavior Analysis — аналог U(E)BA для сети. Чаще выпускаются в виде обособленных продуктов. Основных сетевых протоколов несколько десятков, что делает решение «из коробки» довольно эффективным.

NTA и NBA — это аналоги SIEM и U(E)BA, позволяющие в более удобном и гибком варианте анализировать сетевой трафик.

В качестве opensource решения NTA можно рассмотрим Arkime, которое парсит и складывает трафик в Elasticsearch и pcap(Packet Capture) файлы. Это позволяет анализировать сетевой трафик из веб-интерфейса. Предусмотрена интеграция с Suricata – Arkime умеет сопоставлять алерт с сессией и отображать это в интерфейсе.

BAS

Системы Breach and Attack Simulation (BAS) - комплексное тестирование киберзащиты инфраструктуры компании путём автоматизированной симуляции реальной атаки злоумышленника.

Современные системы киберзащиты инфраструктур быстро эволюционируют, развиваются и становятся более комплексными с каждым годом. Происходит не только повышение сложности самих систем, но и постоянная оптимизация процессов защиты в компании. Становится всё труднее определить вектор движения по усилению защиты. Компании проводят пентесты, «редтиминг», сканирование на уязвимости — ищут различные решения, которые помогут как-то оценить текущий уровень защищённости и увидеть слабые места. Рутинность процессов требует автоматизации решений. Данных о прогнозировании потенциальных векторов уже недостаточно, необходим систематический запуск симуляции реальных действий злоумышленника. Решения BAS помогают автоматизировать такую симуляцию, а полученные результаты — увидеть актуальную картину того, каково состояние защиты компании. В контексте SOCa BAS может помочь для выявления собираются ли всех необходимые события аудита систем, для выявления не детектируемых техник и процедур атакующих из матрицы MITRE ATT&CK с последующей разработкой и для проверки корректности работы корреляционных правил выявления атак.

Примеры

- Infection Monkey
- Invoke-Atomic от RedCanary Atomic Red Team.

UBA/UEBA

User and Entity Behavior Analytics (UEBA, «поведенческий анализ пользователей и сущностей») — технология выявления киберугроз, основанная на анализе поведения пользователей, а также устройств, приложений и иных объектов в информационной системе. Бывают самостоятельные и в виде модуля SIEM.

Подозрительное действие пользователя (User в User Behavior Analysis) и сущность (Entity в UEBA; чаще всего это хост), приводит к добавлению баллов. После уровня создаётся подозрение на инцидент или аналитик сам следит за ТОП подозрительных пользователей. «Репутация» обнуляется со временем. Например, сумма баллов уменьшается на фиксированную величину или процент каждый час. Работа с такими данными не отличается от стандартных подозрений на инциденты.

Основные компоненты UEBA

- Сбор данных: UEBA работает на основе обширного сбора данных из различных источников, таких как журналы аутентификации пользователей, журналы сетевого трафика, данные об использовании привилегий и многое другое.
- Машинное обучение и анализ данных: После сбора данных UEBA применяет машинное обучение и анализ данных для выявления поведенческих шаблонов. Алгоритмы машинного обучения выявляют нормальные поведенческие тренды пользователей и сущностей, а затем ищут аномалии, которые могут указывать на подозрительную активность.
- Профили пользователей и объектов: UEBA создает профили пользователей и объектов с типичным поведением сущности. Это включает часы работы, местоположение, уровень доступа и другие характеристики. Затем система использует эти профили для сравнения с текущим поведением и обнаружения отклонений.
- Детектирование угроз и инцидентов: При обнаружении аномалий UEBA генерирует предупреждения для ИТ-специалистов, указывая на потенциальные угрозы безопасности или необычное поведение. Это позволяет оперативно реагировать на инциденты и предотвращать возможные атаки.

Результат использования U(E)BA — выявление угроз методами с высоким уровнем ложных срабатываний(false-positive) или методами, для которых невозможно создать и поддерживать простой алгоритм без ущерба для качества обнаружения инцидентов.

DDP

Distributed Deception Platform(«платформа с распределенными ловушками») - сокрытие реальных объектов инфраструктуры компании, запутывания атакующих и направления их «по ложному следу». Также используют Deception-платформы для проактивного поиска киберугроз, заманивая атакующих в контролируемую среду и позволяя им «украсть» поддельные данные (приманки), движение которых можно будет затем отследить: например, позволив атакующим «украсть» специально созданные тестовые учетные данные, можно будет затем отследить попытки их применения или публикации и сделать соответствующие выводы. Таким образом, Deception-платформы могут дополнять другие методы обнаружения атак (сигнатурные и на основании выявления аномалий) и предоставлять команде SOC ценную информацию для выявления скрытой вредоносной активности.

Deception-решения позволяют автоматизированно «раскидать» приманки по инфраструктуре компании, анализировать действия, выполняемые атакующими, контролировать их перемещение между приманками. В отличие от классических Honeypot/Honeynet-технологий, Deception-системы позволяют автоматизировать создание и контроль приманок, направлять по ложному следу атакующих, обеспечивать проактивный поиск и анализ киберугроз. Таким образом классический Honeypot является частью системы Distributed Deception Platform. Приманки могут представлять из себя

- поддельные учетные записи, документы, файловые «шары», размещенные на определенном устройстве;
- поддельные системы, сервисы, серверы, которые на первый взгляд неотличимы от настоящих, но оснащены технологиями «песочниц» для контроля и анализа действий атакующих;
- поддельные объекты Active Directory, которые могут заинтересовать атакующих;
- периметровые приманки, похожие на настоящие веб-сервисы, для отвлечения атакующих путем наведения их на ложные цели.

Внедрение Deception-решения оправдано для зрелых команд SOC, осознающих риски и сложности: от необходимости настройки Deception-инфраструктуры до возможности захвата Deception-инфраструктуры атакующими и использования ее в качестве плацдарма для дальнейших атак на компанию. Перед внедрением Deception-платформы следует убедиться в общей зрелости и готовности команд SOC к разумному использованию Deception-решения, выделить соответствующие ресурсы, разработать правила работы с обнаруженными атаками (например, порядок принятия решений о дальнейшем мониторинге действий атакующих или блокировании их действий).

DDP решение для SOCa будет хорошим дополнением для выявления сложных атак, которые тяжеловато выявить обычными корреляционными правилам, такие как например Kerberoasting. Из open-source решений DDP можно рассмотреть Dejavu.

IDS/IPS

Анализирует копию трафика (Detection в Intrusion Detection Systems) или блокирует вредоносную активность (Prevention). Обычно гибридный режим. Аналог антивируса для сети. Метод обнаружения - сигнатуры, от обновления которых зависит эффективность работы системы.

Системы IDS делят по месту установки и принципу действия.

По месту установки

- Network Intrusion Detection System (NIDS). Система глубоко анализирует трафик всех сетевых устройств с канального уровня до уровня приложений. Распознают внешние и внутренние угрозы. Большой объём данных тормозит NIDS или провоцирует пропуск отдельных пакетов, что несёт за собой риски.
- Host-based Intrusion Detection System (HIDS). Ставятся на один хост внутри сети, анализируют и защищают только его трафик. HIDS делает снимок текущей версии хоста и сравнивает его со сделанной ранее, обнаруживая возможные угрозы. Установка такого решения рекомендована для критически важных хостов, в конфигурации которых изменений практически не бывает.
- Perimeter Intrusion Detection Systems (PIDS). Не обеспечивает защиту всей сети, уведомляя лишь о возможных нарушениях границы сети. Ближайший аналог — забор вокруг дома.

- Virtual Machine-based Intrusion Detection Systems (VMIDS). На базе виртуализации, позволяет отказаться от развёртывания системы обнаружения на отдельном устройстве. Чтобы своевременно распознавать подозрительную активность, достаточно развернуть VMIDS на виртуальной машине.
- Application Protocol-based Intrusion Detection System (APIDS). Система обеспечивает контроль пакетов, которые передаются по протоколу прикладного уровня. Например, используемого для обращения к БД SQL.
- Hybrid Intrusion Detection System (HyIDS). Решение фактически представляет собой гибридное решение, сочетающее свойства двух или более типов решений, перечисленных выше.

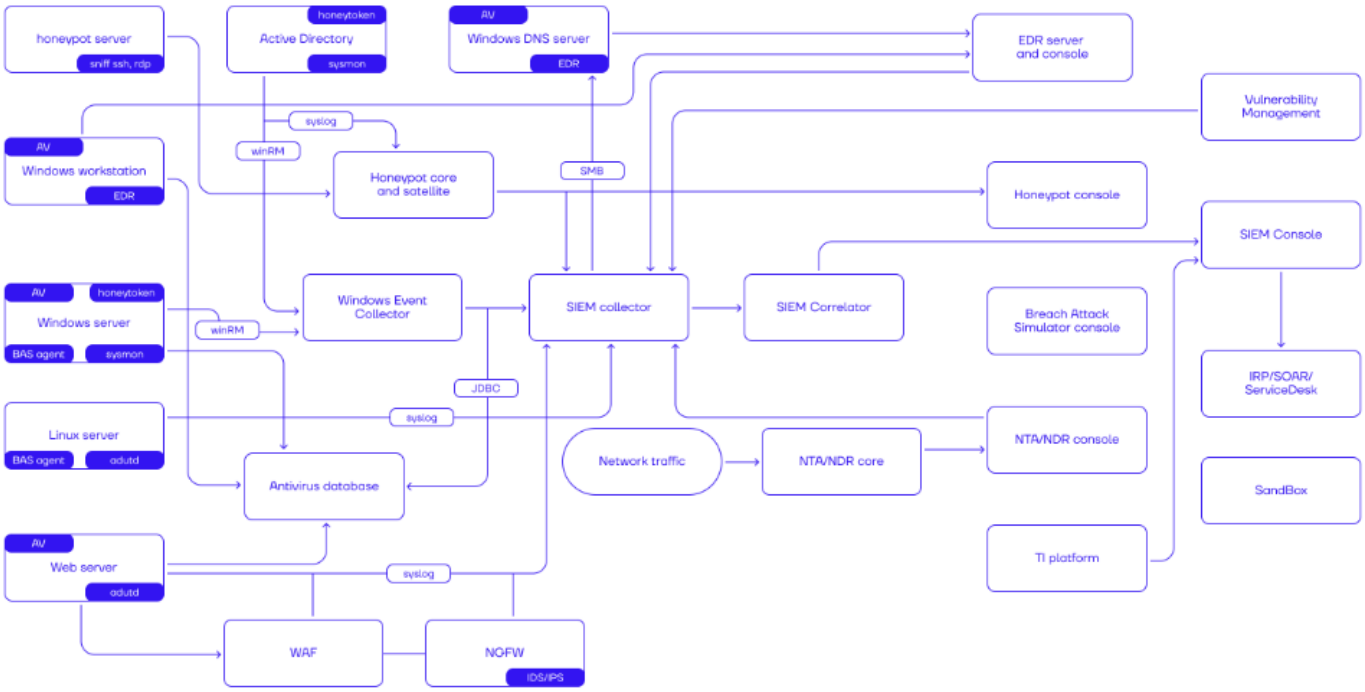
По принципу действия

- Сигнатурные. Анализируют сигнатуры с имеющимися в постоянно обновляемой базе. Если доступа к базе нет или она устарела, эффективность сигнатурного решения снижается. Есть риск и с некорректным распознаванием новой атаки с неизвестной сигнатурой. Сигнатурные IDS отслеживают состояние системы, а не события.
- Основанные на аномалиях. Решение использует технологии машинного обучения. Чтобы оно корректно работало на объекте, необходимо провести предварительное обучение. Срок обучения зависит от сложности ИТ-инфраструктуры компании. Принцип работы следующий: система изучает работу сети на текущий период времени и сравнивает с аналогичным периодом в поиске аномалий трёх типов — статистических, аномалий протоколов и трафика. Такие системы защиты эффективны, но сложны.

Основные решения IDS/IPS

- Zeek(Bro): сетевая система обнаружения вторжений, основанная на Unix-системе. Использует собственный язык для написания политик, которые будут определять последовательность действий при обнаружении атаки или срабатывании датчиков тревоги.
- Snort: кроссплатформенное IDS/IPS решение с открытым исходным кодом. Умеет вести протоколирование, анализировать и искать по содержимому. Применяется для активного блокирования или пассивного обнаружения широкого спектра атак и зондирований.
- Suricata: решение с открытым кодом, в котором используются актуальные технологии, позволяющие увеличить скорость работы. Suricata сочетается со стандартными приложениями и поддерживает большинство доступных модулей. Работает по принципу анализа сигнатур.

Пример схемы СЗИ



Revision #3
Created 15 October 2025 16:18:06 by Admin
Updated 28 October 2025 14:16:29 by Admin