Основные виды СЗИ

Teach Me Skills

Вопросы по предыдущим темам или ДЗ

Mini-quize по прошлым темам:

1. **Какие принципы работы WAF вы знаете?**
2. **Какие задачи можно решать с помощью скриптов автоматизации?**
3. **Для чего предназначены команды ifconfig, netsat, tcpdump**
4. **Какой командой можно посмотреть список сервисов на linux?**

Mini-quize по новой теме:

1. **Какие отделы есть в SOC?**
2. **Для чего предназначено средство PAM?**
3. **Что такое YARA?**
4. **Для чего предназначена Data Leak Prevention?**
5. **Для чего применяется NGFW и как она работает?**

Teach Me Skills

План занятия

1. Антивирусы, сигнатурный поиск
2. Firewall, Web Application Firewall и Next Generation Firewalls
3. Data Leak Prevention, защита от утечек и PAM
4. Понятие Security Operation Center
5. XDR, EDR, MDR - теория

Основные визы СЗИ

WAF защита

По модели защиты:
- Основанный на сигнатуре (Signature-based)
- Основанный на правилах (Rule-based)

По реакции на «плохой» запрос:
- «Очистка» опасных данных
- Блокировка запроса
- Блокировка источника атаки

Основные визы СЗИ

WAF интеграция

- Мост/Маршрутизатор
- Reverse прокси-сервер
- Встроенный

Основные визы СЗИ

WAF как усиление ИБ

- Аналитика по аномалиям
- Обогащение информацией об атаках или их развитие
- Быстрая защита от уязвимостей (Virtual patching)
- Защита от самих атак и DDoS (опционально)
- Защита от Ботов

Основные визы СЗИ

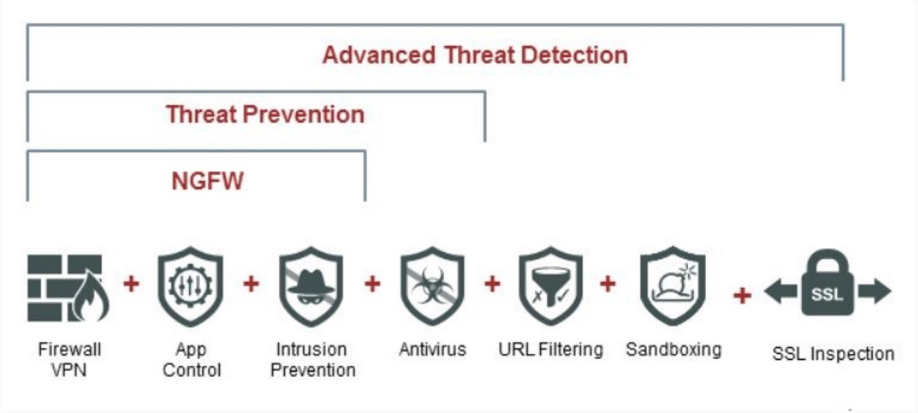
NGFW

• NGFW - Next Generation Firewall (Ранее UTM, FW) - межсетевые следующего поколения (NGFW) фильтруют сетевой трафик для организаций от внутренних и внешних угроз
• Анализирует протоколы L3-L7

Основные визы СЗИ

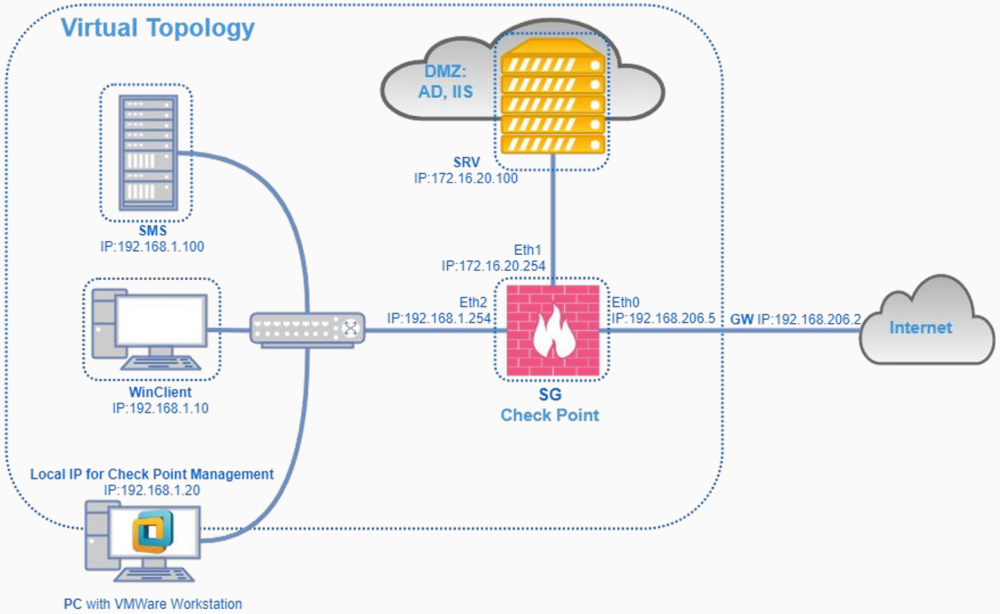
NGFW функционал

- Application control
- URL filtering
- VPN
- IPS
- Anti-Virus
- Anti-Spam
- DLP
- Sandboxing
- Log analyzer and correlation unit



Основные визы СЗИ

NGFW схема



NGFW варианты внедрения

- Физическое устройство
- Виртуальное устройство (VMware, Xen)
- Облачный сервис (IaaS NGWF)

NGFW факторы оценки

Критерий	Принцип оценки
Популярность	Анализ отзывов
Гибкость	Возможности интеграции с инфраструктурой, обратная совместимость, масштабируемость
Производительность	Пропускная способность, CPU, RAM, xCore
Отказоустойчивость	Технологии для отказоустойчивости
Удобство платформы и Поддержка	Собственные отделы аналитики
Инновационность решений	Скорость релизов, технологии защиты AV-аналитики

NGFW отказоустойчивость

• High Availability. Одна нода кластера активная и маршрутизирует трафик, вторая нода пассивная и находится в горячем резерве, готовая стать активной в случае проблем с первой
• Load Sharing. Обе ноды активны и трафик “делится” между ними

Основные визы СЗИ

NGFW лидеры рынка

Основные визы СЗИ

NGWF: FortiGate

Запросить демо
Запросить демо

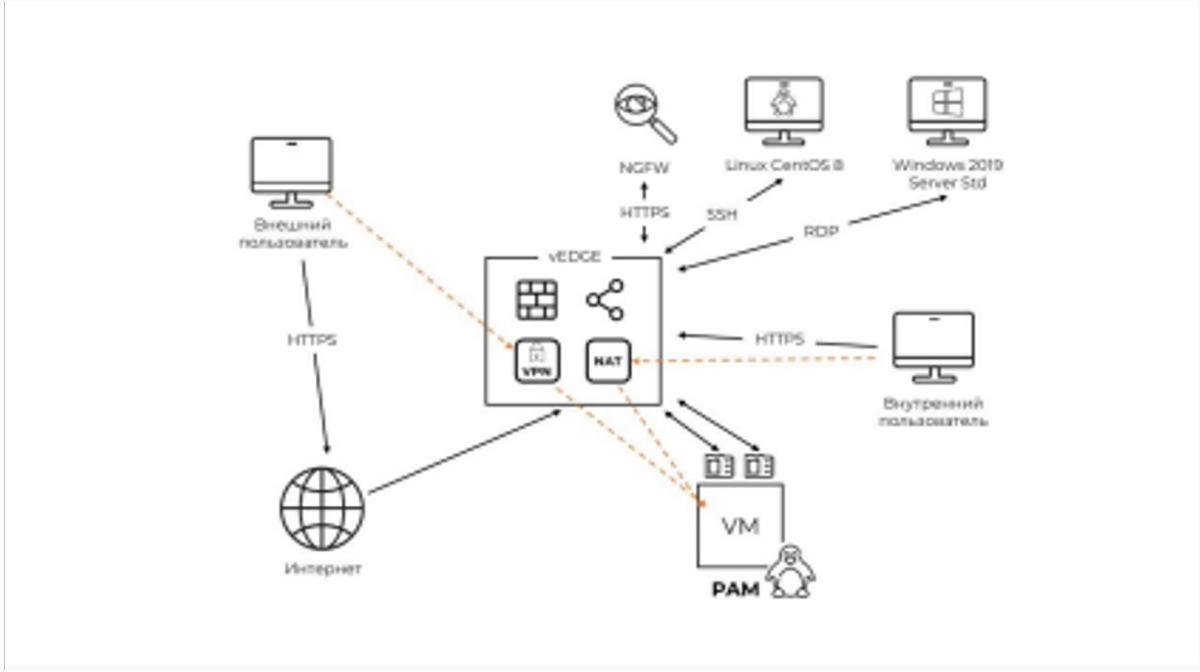
Check Point®
SOFTWARE TECHNOLOGIES LTD

FORTINET®

Основные визы СЗИ

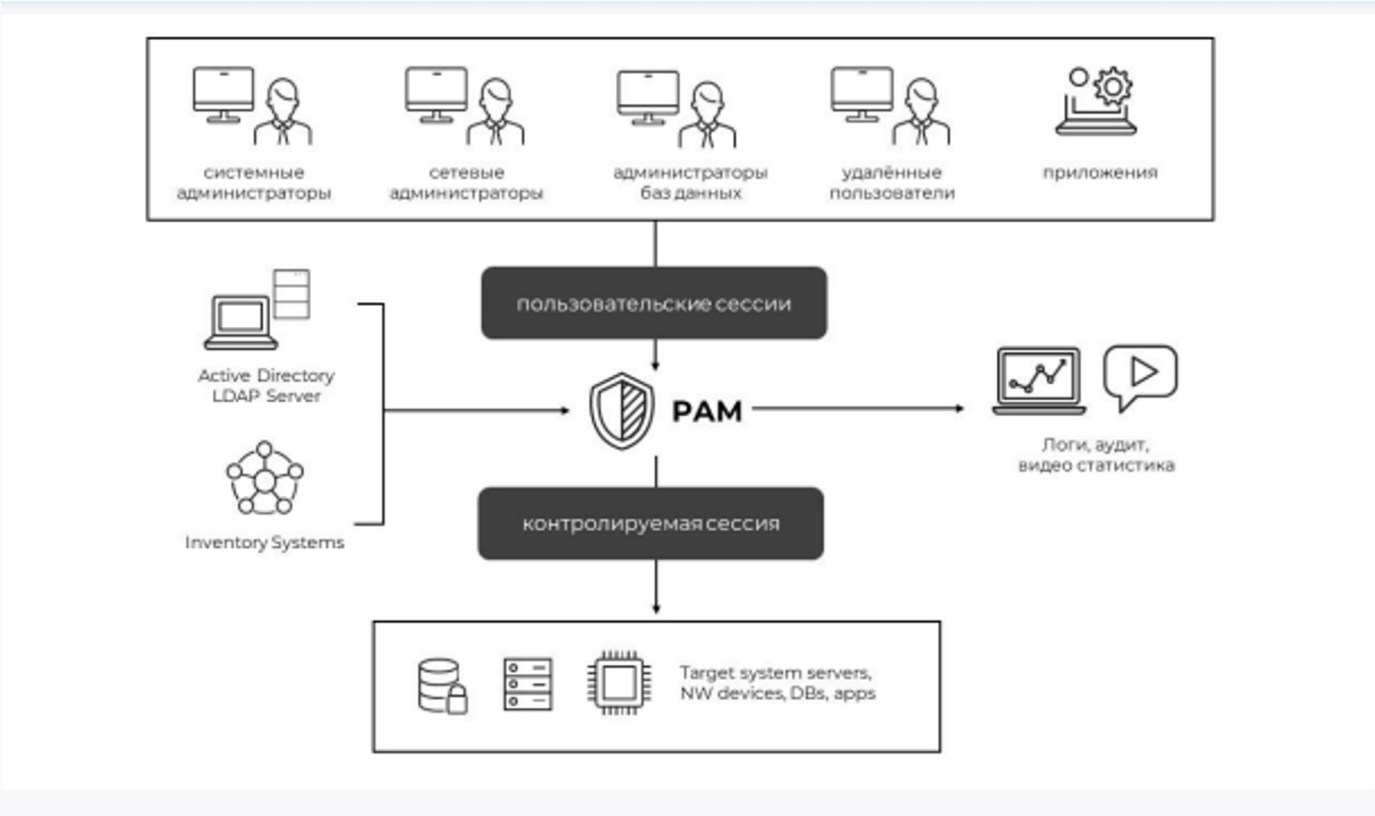
PAM

Privileged Access Management (PAM) — это решение для управления доступом привилегированных пользователей.



Основные визы СЗИ

PAM



Основные визы СЗИ

PAM

Что умеют PAM:

• Протоколирование сеансов удалённого доступа пользователей по SSH, SCP/SFTP, RDP, VNC, Telnet
• Запись работы с клавиатурой, видеофиксация.
• Использование стандартных средств подключения по SSH- или RDP-консоли (например, Putty и mstsc).

Основные визы СЗИ

PAM

Что умеют PAM:

• Единая точка входа и управления паролями привилегированных пользователей с возможностью прозрачной аутентификации на целевых устройствах (без необходимости ввода реквизитов доступа).
• Масштабируемость и географически распределённые инсталляции.
• Мониторинг введённых команд текстовых сессий, клавиатурного ввода, запуска приложений; анализ изображения (OCR), поддержка чёрных списков действий и команд.

Основные визы СЗИ

PAM

Что умеют PAM:

• Интеграция с внешними каталогами, такими как Active Directory и LDAP(s).
• Поддержка работы с брокером фермы RDP серверов Windows версии 2012 и выше.
• Возможность интеграции с внешними системами посредством собственного API.
• Работа без использования агентов. Работа в формате Virtual Appliance и ПАК

Основные визы СЗИ

PAM

Решения	
INDEED ID	Indeed Privileged Access Manager
ПТ	SafeInspect
ZECURION	Zecurion PAM
JumpServer	Jumpserver как настроить

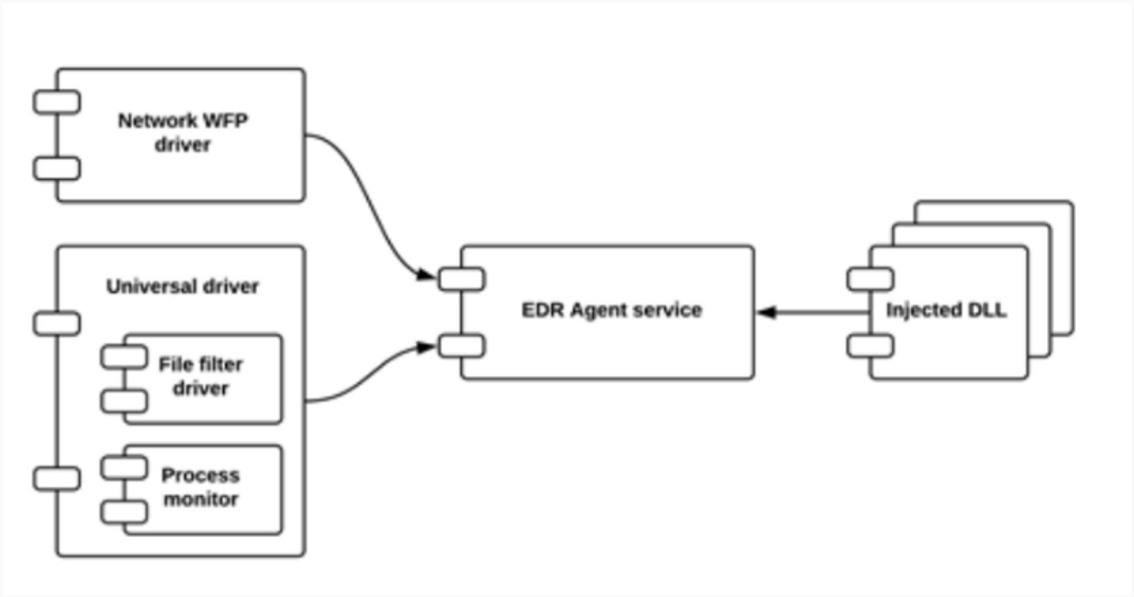
Основные визы СЗИ

EDR

Endpoint Detection and Response (EDR) – продвинутая система безопасности, представляющая собой интегрированное решение для обеспечения безопасности конечных точек (компьютерных аппаратных устройств) от потенциальных угроз. Технология сочетает в себе непрерывный мониторинг и сбор данных о конечных точках в режиме реального времени.

Основные визы СЗИ

EDR Архитектура



EDR Архитектура

Core Library — базовый фреймворк, который содержит основные функции и является ядром системы;
• EDR Agent service — собственно само приложение EDR;
• Process Monitor — DLL-библиотека, которая внедряется в различные процессы для перехвата вызовов API и инструментарий для работы с ней;
• File filter driver — мини-фильтр файловой системы, который перехватывает запросы ввода-вывода файловой системы, отслеживает доступ к реестру, обеспечивают защиту компонентов и настроек EDR и тп;
• Network monitor — компонент мониторинга сетевой активности;

EDR Возможности

Непрерывный мониторинг широкого диапазона конечных устройств в корпоративных сетях и за их пределами позволяет организациям отслеживать не только злонамеренные атаки из внешних источников, но также для отслеживания аномальной активности внутри организации (например, добычи криптовалюты или кражи данных сотрудниками).

- Запись огромных объемов активности в сети.
- Интеграция с расширенными функциями, такими как песочница, для поиска спящих угроз.
- Включение упреждающего поиска индикаторов атаки, чтобы увидеть угрозы, которые еще не были обнаружены.

Основные визы СЗИ

EDR Возможности

Расширенные возможности анализа, позволяющие командам безопасности быстрее оценивать и блокировать последующие атаки. К ним относятся поиск индикаторов компрометации; упреждающий поиск индикаторов атаки и определение первопричины заражения; кибер-инцидент и включение защиты от него.

• Исправление последствий осуществленных атак с возможностью отката конечных точек до ранее известного исправного состояния.

• Создание детализированных политик для обработки USB-устройств с целью блокировки неизвестных и потенциально вредоносных USB-ключей.

• Включение защиты для удаленных сотрудников, которые не могут полагаться на защиту периметра.

Основные визы СЗИ

EDR Решения

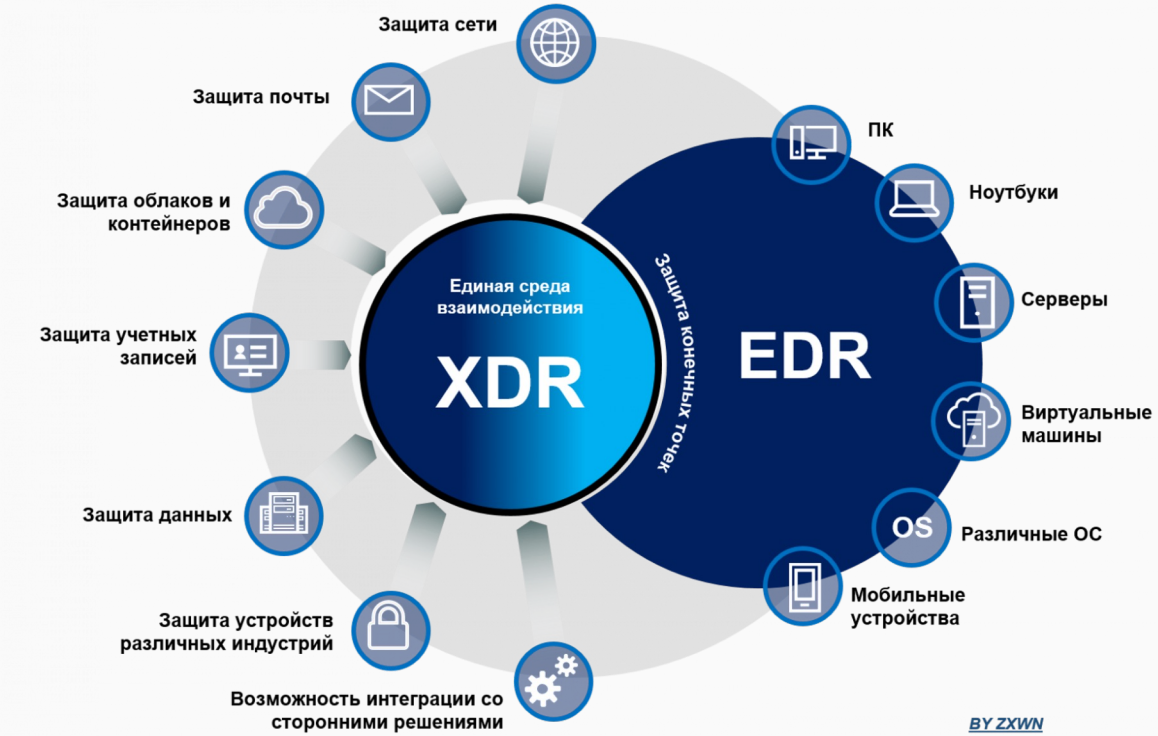
- Kaspersky Endpoint Detection and Response Expert
- Positive Technologies PT XDR

kaspersky

Основные визы СЗИ

XDR

Концепция Extended Detection and Response (XDR)



Основные визы СЗИ

XDR

XDR (Extended Detection and Response) – это расширенное обнаружение и реагирование на сложные угрозы и целевые атаки. В основе решения данного класса лежат продукты от одного вендора, то есть, это, в большей степени, моновендорная история.

Основные визы СЗИ

XDR

- EDR (Endpoint Detection and Response) – это ключевой элемент XDR. Без EDR не может быть XDR.
- XDR должен строиться на сильном EDR, который сам по себе в рамках конечных точек должен охватывать большое количество источников данных: ПК, ноутбуки, виртуальные машины, мобильные устройства, плюс различные операционные системы (Windows, Linux, MacOS, Android, iOS, пр.).
- XDR не равно EDR. XDR основан на расширении технологии EDR.
- Буква “X” в начале сокращенного варианта названия “XDR” означает количество подключаемых источников/продуктов, которые участвуют в процессе обнаружения, расследования и реагирования. Количество подключаемых “X” зависит от потребностей заказчика, от уже внедренных решений от одного вендора, а также от выбранного поставщика XDR, то есть от его поддерживаемых источников (классов продуктов).
- XDR – это, в большей степени, концепция, которая представляет собой кросс-продуктовую историю, обогащенную поверх дополнительными значимыми функциональными возможностями по реагированию на инциденты. Это единый центр сбора, нормализации, анализа, корреляции данных, расширенного расследования и реагирования с применением максимально возможной автоматизации. В составе также единая база данных, единая консоль, единая видимость того, что происходит в инфраструктуре, единый инструментарий по анализу первопричин и проактивному поиску угроз, единый улучшенный процесс приоритезации инцидентов, одна точка взаимодействия с Threat Intelligence и пр.
- XDR подразумевает постоянную доставку обновлений, новых правил, плейбуков и т д. Это не просто отгружаемая коробка – это живой и растущий организм, актуализируемый с каждым изменением в ландшафте угроз.

Основные визы СЗИ

XDR

Отличия XDR от других систем информационной безопасности

Некоторые инструменты киберзащиты схожи с XDR, но из-за более узкой специализации в них, как правило, меньше функций. Например:

- **EDR** обеспечивают защиту только на уровне конечных точек, без сетевых и облачных служб.
- **SIEM** осуществляют только сбор и анализ информации во внутренней сети, без реагирования.
- **UEBA** анализируют только поведение пользователей, устройств и приложений, без реагирования на аномалии.
- **SOAR** охватывают большую часть инфраструктуры, но работают в основном по сигнатурам и типовым сценариям реагирования, не обеспечивая проактивную защиту. Кроме того, у решений типа SOAR более низкий уровень совместимости с решениями и приложениями, служащими источниками данных.

XDR

Недостатки XDR-решений

Технологии XDR относительно новы и очень перспективны, однако их использование сопряжено с определенными сложностями и рисками:

- На данный момент разные XDR-системы обладают очень разным набором возможностей, что усложняет их сравнение и выбор.
- Системы класса XDR включают в себя много различных функций, при этом вендоры, поставляющие эти системы, чаще всего специализируются в одном или нескольких направлениях, не охватывая все, что может привести к попыткам реализовать те или иные возможности без необходимой экспертизы. А это, в свою очередь, повышает вероятность ошибок.
- Некоторые XDR-системы совместимы только с защитными решениями определенного вендора или ограниченного числа вендоров. В связи с этим возможны ситуации, когда пользователям XDR придется искать компромисс между оптимальными для них узкоспециализированными решениями и полнотой использования XDR.

Основные визы СЗИ

MDR

Managed Detection and Response (MDR) - это подход к кибербезопасности, который объединяет мониторинг, обнаружение и реагирование на угрозы в единую службу. MDR-провайдеры предоставляют компаниям экспертную поддержку в области безопасности, используя передовые технологии и искусственный интеллект для выявления и предотвращения кибератак.

MDR - принцип работы

Основной принцип MDR заключается в том, что специалисты по кибербезопасности постоянно мониторят и анализируют активности на сетях, серверах, конечных точках и других ресурсах организации. Это позволяет своевременно обнаруживать аномальное поведение и потенциальные угрозы.

После обнаружения инцидента MDR-провайдеры предпринимают меры по его реагированию. Это может включать в себя проведение расследования, удаление вредоносного программного обеспечения, восстановление системы и дополнительные меры по укреплению безопасности, чтобы предотвратить возникновение аналогичных инцидентов в будущем.

MDR также предоставляет компаниям ценную информацию и отчеты о текущем состоянии безопасности, обнаруженных угрозах и предложениях по улучшению общего уровня защиты. Это помогает организациям принимать обоснованные решения и улучшать свою стратегию кибербезопасности.

Основными преимуществами MDR являются оперативность реагирования на угрозы, проактивное обнаружение новых видов кибератак, возможность выявления ложных срабатываний и устранение слабых мест в системах безопасности. В конечном итоге, это помогает предотвращать потенциальные киберпреступления и минимизировать возможные убытки для организации.

Пример архитектуры на базе Касперского

Основные визы СЗИ

UBA

User [and Entity] Behavioral Analytics (UEBA/UBA) — класс систем, позволяющих на основе массивов данных о пользователях и ИТ- сущностях (конечных станциях, серверах, коммутаторах и т. д.) с помощью алгоритмов машинного обучения и статистического анализа строить модели поведения пользователей и определять отклонения от этих моделей, как в режиме реального времени, так и ретроспективно.

Основные визы СЗИ

UBA

UBA работает только с информацией о пользователях, а UEBA анализирует данные о пользователях и об объектах ИТ-инфраструктуры.

Эти системы могут выступать как отдельными программными продуктами, так и расширениями в составе продуктов ИБ (например: SIEM, DLP, EDR).

Основные визы СЗИ

UBA Возможности

Прикладная аналитика данных из различных источников, как простая статистическая, так и расширенная, с использованием методов машинного обучения, в режиме реального времени и/или с определенной периодичностью.

• Быстрая идентификация атак и других нарушений, большинство из которых не определяются классическими средствами ИБ.

• Приоритезация событий, консолидированных из разных источников (SIEM, DLP, AD и т. д.), для более оперативного реагирования со стороны администраторов ИБ.

• Более эффективная реакция на события за счет предоставления администраторам ИБ расширенной информации об инциденте, включающей все объекты, которые были вовлечены в аномальную активность.

Основные визы СЗИ

UBA Возможности

Выявление скомпрометированных учётных записей.
• Выявление инсайдерских угроз.
• Мониторинг прав доступа пользователей по уровню и целевым системам.

UBA решения

• Kaspersky Fraud Prevention (создание профилей добросовестного и мошеннического поведения на основании действий во время сессии)
• InfoWatch Prediction (прогнозирует угрозы ИБ, обнаруживает инсайдеров и скомпрометированные учётные записи)
• DLP-система Zecurion DLP (обнаруживает инсайдерские угрозы)

Основные визы СЗИ

DLP

DLP-система (от англ. Data Leak Prevention) это специализированное ПО, которое защищает организацию от утечек данных и гарантирует информационную безопасность.

Данная технология – это не только возможность блокировать передачу конфиденциальной информации по различным каналам, но и инструмент для наблюдения за ежедневной работой сотрудников, который позволяет найти слабые места в безопасности до наступления инцидента.

Основные визы СЗИ

DLP

Принцип работы DLP-системы прост и заключается в анализе всей информации: исходящей, входящей и циркулирующей внутри компании. ДЛП-система при помощи алгоритмов анализирует, что это за информация и в случае, если она критичная и отправляется туда куда ей не положено — блокирует передачу и/или уведомляет об этом ответственного сотрудника.

Основа DLP — набор правил. Они могут быть любой сложности и касаться разных аспектов работы. Если кто-то их нарушает, то ответственные лица получают уведомление.

DLP

Как выбрать DLP-систему?

Если вы убедились, что система защиты данных вам необходима, возникает вопрос, как ее выбрать исходя из разнообразия, представленного на рынке. Для начала задайте себе несколько вопросов:

- Какие каналы передачи информации она должна контролировать
- Будет ли использоваться система в расследованиях или работать только на перехват
- Какой бюджет и оборудование будут выделены на систему

Чтобы максимально полно ответить на эти вопросы, лучше всего запросить демо-версию продукта. Большинство разработчиков предоставляет DLP на некоторое время, чтобы вы могли посмотреть, как она работает. Во время тестового периода можно понять, насколько хорошо выбранный программный комплекс закрывает задачи, а также сравнить с другими.

Основные визы СЗИ

Неочевидные способы использования DLP-системы

Обзор

Казалось бы, система, созданная для контроля утечки данных, больше ничем не может быть полезна. Однако современные DLP имеют и другие возможности, неочевидные на первый взгляд.

- **Анализ загруженности персонала.**

Многие DLP-системы способны вести учет рабочего времени сотрудников. Рабочий процесс каждого пользователя можно представить в виде статистики, которая позволяет проанализировать, насколько сотрудник вовлечен в трудовой процесс.

- **Обеспечение юридической поддержки.**

Задача DLP состоит не только в том, чтобы предотвратить утечки, но еще и при наличии судебного разбирательства, предоставить доказательства злоумышленной деятельности.

- **DLP как инструмент мотивации.**

Когда сотрудники осознают, что их трудовая деятельность находится под мониторингом, появляется большая ответственность за рабочий процесс. И это в свою очередь приводит к улучшению климата в коллективе.

- **DLP как хранилище.**

DLP-технология гарантирует сохранность всей информации, поскольку содержит в своём архиве все коммуникации сотрудников, к которым в случае необходимости можно будет обратиться.

- **DLP как контроль рабочего времени сотрудника.**

Система DLP SecureTower от белорусского разработчика Falcongaze предоставляет учет рабочего времени, позволяющий узнать, как эффективно работник распределяет свой распорядок дня.

Основные визы СЗИ

YARA

YARA (Yet Another Recursive Acronym) - это мощный язык и инструмент для создания сигнатур (**правил**) для обнаружения вредоносных программ. YARA часто используется в области информационной безопасности для поиска и анализа вредоносных файлов.

YARA-правила для идентификации новых образцов ВПО могут появляться раньше, чем вендорские сигнатуры, таким образом их использование будет упреждать заражение неизвестными образцами ВПО.

Многие коммерческие решения помимо собственных закрытых баз сигнатур поддерживают YARA для анализа файлов.

Ссылка на github

Пример работы

Основные визы СЗИ

Антивирусы, сигнатурный поиск

Для того, чтобы установить Clam AV на устройство, необходимо выполнить команду:
sudo apt install clamav clamav-daemon

Для того, чтобы установить графический интерфейс Clam AV, необходимо выполнить команду:
sudo apt install clamtk

После установки необходимо будет скачать актуальные версии баз вирусных сигнатур (БВС). Для этого необходимо отключить службу автоматического обновления командой:

sudo systemctl stop clamav-freshclam.service

и поставить на скачивание БВС следующей командой:
sudo freshclam

Основные визы СЗИ

Антивирусы, сигнатурный поиск

После того, установки БВС, необходимо заново включить службу автоматического обновления:

sudo systemctl start clamav-freshclam.service

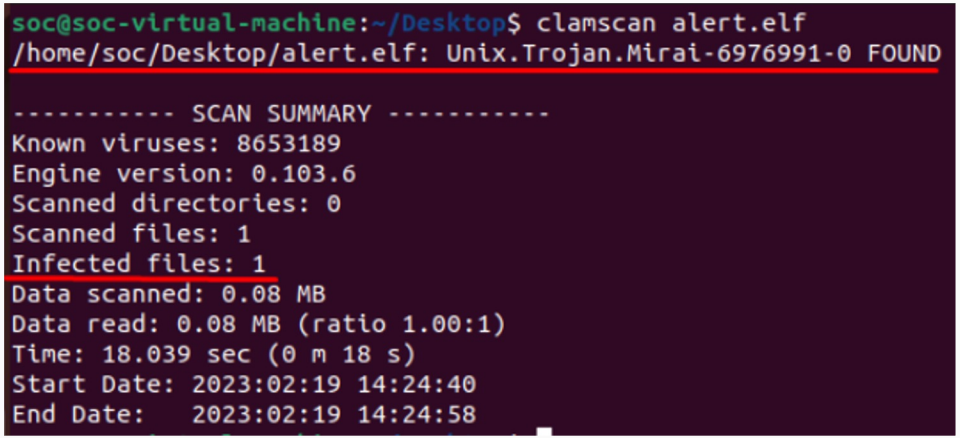
и проверить её работоспособность:
sudo systemctl status clamav-freshclam.service

Важно! В настоящее время разработчики Clam AV ограничили доступ до своих продуктов IP-адресам из RU сегмента интернета. Поэтому все вышеперечисленные действия необходимо выполнять через VPN.

Основные визы СЗИ

Антивирусы, сигнатурный поиск

Для запуска сканирования одиночного файла используется следующая команда:
clamscan <filename>
где filename – абсолютный путь до файла, например:
/home/soc/Desktop/sample/infected.elf
Вывод для зараженного файла имеет следующий вид:



Основные визы СЗИ

Антивирусы, сигнатурный поиск

Для того, чтобы просканировать директорию, необходимо выполнить команду:
clamscan <directory>
где directory – абсолютный путь до директории,
например: /home/soc/Desktop/sample/infected

Полезные флаги для сканирования:
«-i» - выводит только ВПО:
clamscan -i Desktop/sample/infected
«-r» - проходит директории рекурсивно:
clamscan -r Desktop/sample/infected
«-l» - пишет информацию в лог файл:
clamscan Desktop/sample/infected -l log.txt
При сканировании директорий рекомендуется указывать вышеперечисленные флаги:
clamscan -ir Desktop/sample/infected -l log.txt

Понятие Security Operation Center

Security Operation Center (SOC) – это одно из подразделений организации, занимающееся мониторингом инфраструктуры, на предмет наличия (предпосылок к созданию) угроз информационной безопасности.

SOC разворачивается в целях обнаружения, предупреждения, и ликвидации последствий компьютерных атак.

Цель SOC:
Минимизация (исключение) возможных рисков и негативных последствий для организации (объекта КИИ) за счет своевременного выявления и оперативного реагирования на инциденты информационной безопасности.

Основные визы СЗИ

Понятие Security Operation Center

Задачи SOC:
1. Организация и осуществление постоянного мониторинга инфраструктуры организации.
2. Своевременное реагирование на компьютерные инциденты.
3. Анализ компьютерных инцидентов.
4. Выработка предложений по устранению последствий компьютерных инцидентов.
5. Проведение мероприятий по предотвращению возникновения компьютерных инцидентов.
6. Проведение аналитики по ландшафту угроз (Threat Intelligence).
7. Проведение периодического поиска актуальных угроз в защищаемой инфраструктуре (Threat Hunting).
8. Построение и постоянное совершенствование системы защиты информации в организации.
9. Администрирование используемых СЗИ и других средств, систем развернутых в интересах SOC.
10. Взаимодействие с вендорами в вопросах поддержки предоставляемых ими СЗИ.

Основные визы СЗИ

Понятие Security Operation Center

В рамках выполнения поставленных задач, в SOC организовывают следующие типовые подразделения:

- Отдел реагирования на компьютерные инциденты (Дежурная смена).
- Отдел расследования компьютерных инцидентов (РКИ).
- Отдел администрирования средств защиты информации (СЗИ).
- Отдел администрирования сетевой инфраструктуры.
- Отдел оценки защищенности инфраструктуры.

Понятие Security Operation Center

Отдел реагирования на компьютерные инциденты.

Специалисты дежурной смены (или первой линии) отвечают за своевременное обнаружение компьютерных инцидентов и первичное реагирование на них.
Основными задачами является:

- фильтрация инцидентов ИБ (ложное срабатывание, срабатывание на легитимные действия, истинный инцидент);
- проведение мероприятий реагирования на истинные инциденты ИБ и закрытие их, если инцидент не требует проведения расследования.
- Дежурная смена может нести как круглосуточное, так и дневное (ночное) дежурство. Также возможно вынести обязанности дежурной смены на аутсорсинг.

Специалисты отдела реагирования работают с системами мониторинга (IRP, SIEM), системами обнаружения вторжений (СОВ), системами предотвращения утечек (DLP), средствами защиты информации.

Понятие Security Operation Center

Отдел расследования компьютерных инцидентов (РКИ).

Специалистов отдела расследования КИ иногда называют 2 линией SOC, но зачастую они являются отдельным подразделением. Их основной задачей является определение причины и ликвидация последствий КИ.

К данным специалистам предъявляются довольно высокие требования. Они должны уметь работать с событиями ИБ, собираемыми с различных источников (СОВ, SIEM, САВЗ, Песочницы, YARA и др.), знать обратную разработку (Reverse Engineering), компьютерную криминалистику (Forensic), устройство основных ОС, основы программирования.

Также на отдел РКИ в некоторых случаях может быть возложена задача Threat Intelligence (TI) и Threat Hunting (TH) (в части заведения в СЗИ новых правил для детектирования инцидентов).

Основные визы СЗИ

Понятие Security Operation Center

Отдел администрирования средств защиты информации (СЗИ).

Данное подразделение отвечает за развертывание, поддержание работоспособности средств ЗИ, совершенствование и масштабирование системы ЗИ.

Администраторы средств ЗИ должны понимать принципы работы используемых ими средств, технологии на которых они построены. Обычно один-два специалиста отвечают за одну систему.

Необходимыми знаниями являются:

− системное администрирование различных ОС, программирование хотя бы на основных скриптовых языках (так как многие вендоры предоставляют скрипты для выполнения различных задач по обслуживанию систем, а решения с открытым исходным кодом иногда приходится «докручивать» руками);

− умение работать с базами данных, системами виртуализации, виртуальной контейнеризацией.

Основные визы СЗИ

Понятие Security Operation Center

Отдел оценки защищенности инфраструктуры.

Данный отдел проводит мероприятия по выявлению угроз безопасности информации в организации (аудит информационной безопасности, тестирование на проникновение, имитация действий злоумышленников, red teaming).

Аудит – процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности в соответствии с определенными критериями и параметрами безопасности.

Тестирование на проникновение (Pentest) – процесс активного анализа системы на наличие потенциальных уязвимостей.

Имитация действий злоумышленника (Adversary Simulation) – процесс тестирования целевой системы защиты информации, посредством выполнения в инфраструктуре организации безопасных тестов.

Редтиминг (Red Team/Red Hat) – «реальные» атаки на инфраструктуру.

Также специалисты отдела оценки защищенности осуществляют моделирование угроз безопасности информации и выполняют мероприятия превентивного устранения уязвимостей – процесс моделирования угроз и процесс управления уязвимостями (Vulnerability Management) соответственно.

Основные визы СЗИ

Понятие Security Operation Center

Специалисты разных линий SOC, в рамках своей рабочей деятельности, пользуются следующими процессами:

Threat Intelligence – процесс получения информации об актуальных угрозах и группировках киберпреступников.

Threat Hunting – процесс проактивного поиска следов взлома или функционирования вредоносного программного обеспечения, которые не смогли обнаружить СЗИ.

Vulnerability Management – непрерывный, циклический процесс выявления и устранения
уязвимостей в инфраструктуре организации.

Incident Response – процесс реагирования на инциденты информационной безопасности.

Forensic – многоуровневый процесс выявления артефактов компрометации на локальной машине, дампе сетевого трафика, в аппаратном обеспечении и т.д. Выделяют следующие виды форензики – Computer Forensics, Network Forensics, Forensics Data Analysis, Mobile Device Forensics, Hardware Forensics.

Reverse Engineering – процесс обратной разработки. То есть, когда из скомпилированного файла необходимо получить исходный код программы.

Teach
Me
Skills

Спасибо за внимание!