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

Конвертация VMWare в VirtualBox

- Загрузить OVF Tool. Также вы можете найти путь установки вашего VMware (там есть ovftool).
- Через CMD с правами администратора в каталоге установки ovftool:

```
ovftool <локатор источника> <локатор назначения>
C:\Program Files\VMware\VMware OVF Tool>ovftool.exe "D:\...\Ubuntu 64-bit.vmx"
"D:\...\ubuntu_wp_lesson.ova"
```

- Открыть файл .ovf с помощью VirtualBox.

Сфера ответственности SOC:

SOC - security operational center

- Активный мониторинг IT-среды и сбор данных об инцидентах в режиме 24/7. Для мониторинга и сбора данных специалисты могут использовать SIEM-решения и EDR-продукты.
- Анализ подозрительных событий.
- Реагирование на угрозы.
- Восстановление после инцидента.
- Расследование инцидентов.
- Ведение реестра ресурсов.
- Менеджмент соответствия требованиям таких как GDPR, HIPAA, CPPA и так далее.
- Обеспечение работоспособности инструментов SOC. Включает в себя поддержку работы граничных систем сетевой безопасности и инфраструктуры SOC, создание собственных правил и сигнатур, а также подбор и внедрение решений, использующихся в работе SOC.

Состав команды SOC

Аналитик 1-ой линии (L1 Analyst или Tier 1 Analyst) распределение и первичный отсев явных ложных срабатываний систем. (False Positive). Опираются на созданные сценарии для данного типа инцидента. Если аналитик 1-го уровня может, то реагирует. Иначе передает аналитику 2-го уровня.

Аналитик 2-ой линии (L2 Analyst или Tier 2 Analyst) получает фактуру по сложным инцидентам. Он анализирует уникальную ситуацию. В случае непонимания эскалация специалисту по реверс-инжинирингу или эксперту по форензике.

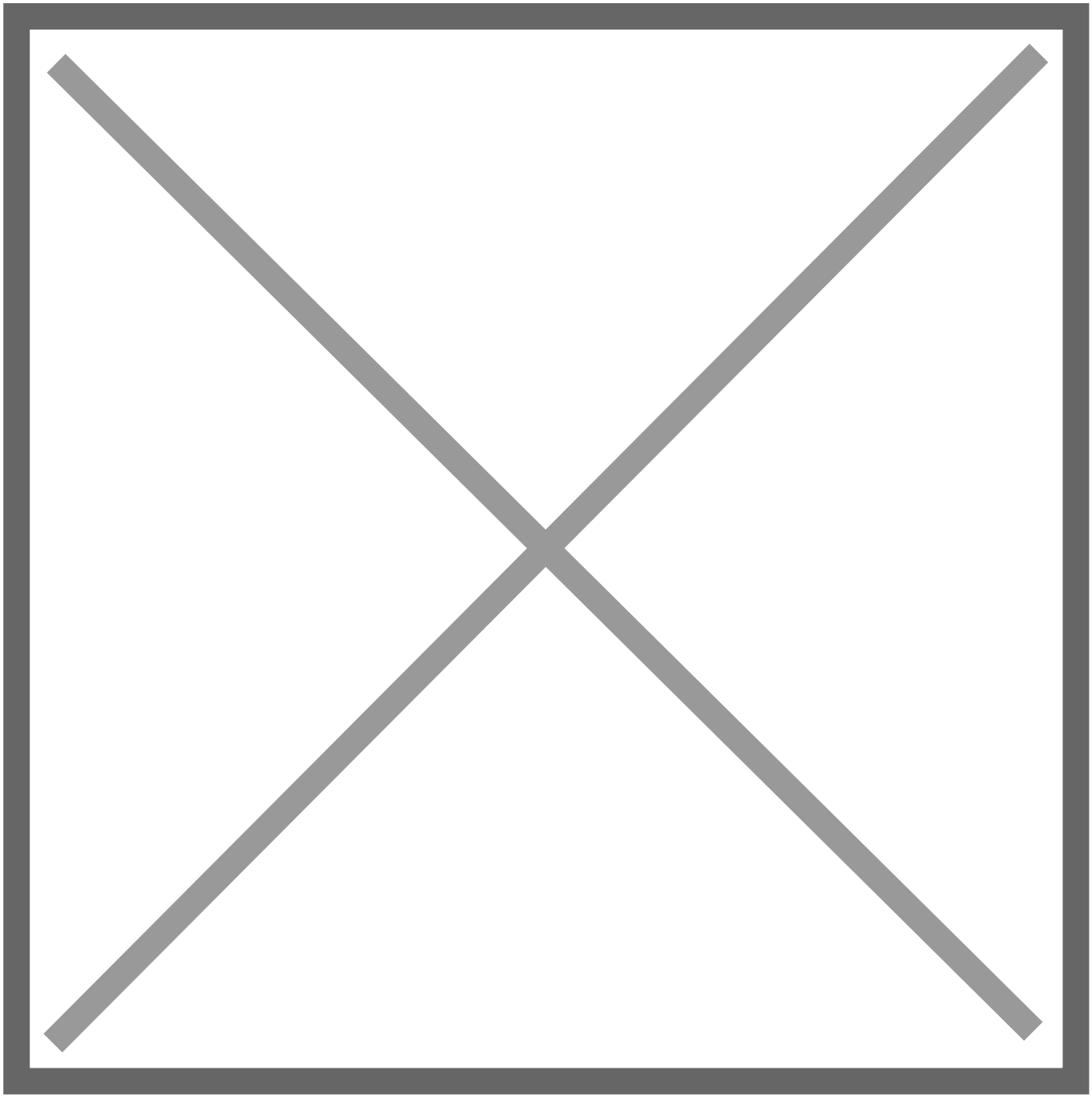
Аналитики 3-ей линии в основном состоят из профильных специалистов, которые хорошо разбираются в своей специализации, таких как:

- **Форензик-эксперт** (специалист по компьютерной криминалистике) делают:
  - что изменилось в атакованной системе (компьютере, сервере, смартфоне), какие данные были стерты, изменены или похищены вирусом,
  - какие еще системы были атакованы.
  - воссоздать полный путь распространения угрозы: определить, на каком компьютере был этот вирус впервые запущен, что он делал на зараженной системе, как затем развивалась атака и как был в итоге нанесен ущерб.
- **Специалист по реверс-инжинирингу** — профессиональный программист, изучающий вредоносное ПО для противодействия кибератакам. Задача - понять, как устроен вирус: запустить вирус в изолированной среде (т.н. песочнице) для анализа его поведения, провести процедуру обратной разработки и получить из файла-образца первоначальный программный код, чтобы уже в нем найти особенности, которые помогут понять, что именно делает данный вирус и как ему лучше противостоять. При этом хакеры знают, что их вирус рано или поздно попадет к такому эксперту на исследование, и поэтому применяют техники запутывания (обфусцирования) кода, чтобы усложнить задачу реверс-инжиниринга.
- **Специалист по киберразведке** (CyberThreat Intelligence) отвечает за поиск ранее не обнаруженных или затаившихся вредоносных программ, например вирусов-логических бомб, которые срабатывают только при наступлении определенных условий, а до этого никак себя не проявляют. Также такой эксперт ищет информацию о новых вирусах, новых киберпреступных группировках, пытается понять, не планируется ли атака на компанию-заказчика, нет ли «заказа» на кражу коммерческой информации защищаемой фирмы.
- **Специалист по разработке и настройке контента в системах SIEM, SOAR, IRP:**
  - составляет правила выявления реагирования в системах SOC-Центра.
  - правила автоматического реагирования, локализации, восстановления информационных систем при помощи SOAR и IRP решений. Если используются сигнатурные методы обнаружения угроз, то создает сигнатуры, т.е. описывает правила, по которым угроза должна быть обнаружена.

Инженер группы инфраструктуры — настраивает внутренние системы SOC-Центра, отвечает за стабильность получения данных.

Сервис менеджер координируют работу команды SOC, связывает друг с другом заказчиков и исполнителей, выполняет организационную работу. Контролирует соблюдение SLA (соглашение об уровне услуг).

Руководитель SOC — занимается организационной деятельностью, планированием развития и штата, в коммерческих SOC участвует во встречах с потенциальными Заказчиками для привлечения новых клиентов. Участвует в маркетинговых активностях с целью продвижения. Является точкой эскалации при решении возникших проблем.



Операционные модели SOC:

- собственный(in-house);
- сервисный(MSSP - Managed Security Service Provider);
- гибридный.

В первом случае **собственного**(**in-house) SOC** находится полностью в собственности организации с точки зрения владения оборудованием и найма специалистов. Это самый дорогой и длительный по времени вариант построения центра мониторинга. Попытка выстраивания процессов и реализации может занять годы и не всегда может увенчаться успехом.

В случае **сервисной модели SOC** (или MSSP) центр мониторинга находится полностью на стороне сервис-провайдера. В этом случае заказчику не нужно нанимать и содержать персонал, разрабатывать регламенты, корреляционные правила, заниматься закупкой оборудования и лицензий для ИБ-решений, такие как SIEM, SOAR, TIP. К тому же данный вариант является наиболее быстрым в плане подключения для заказчика и может составлять от 1 месяца.

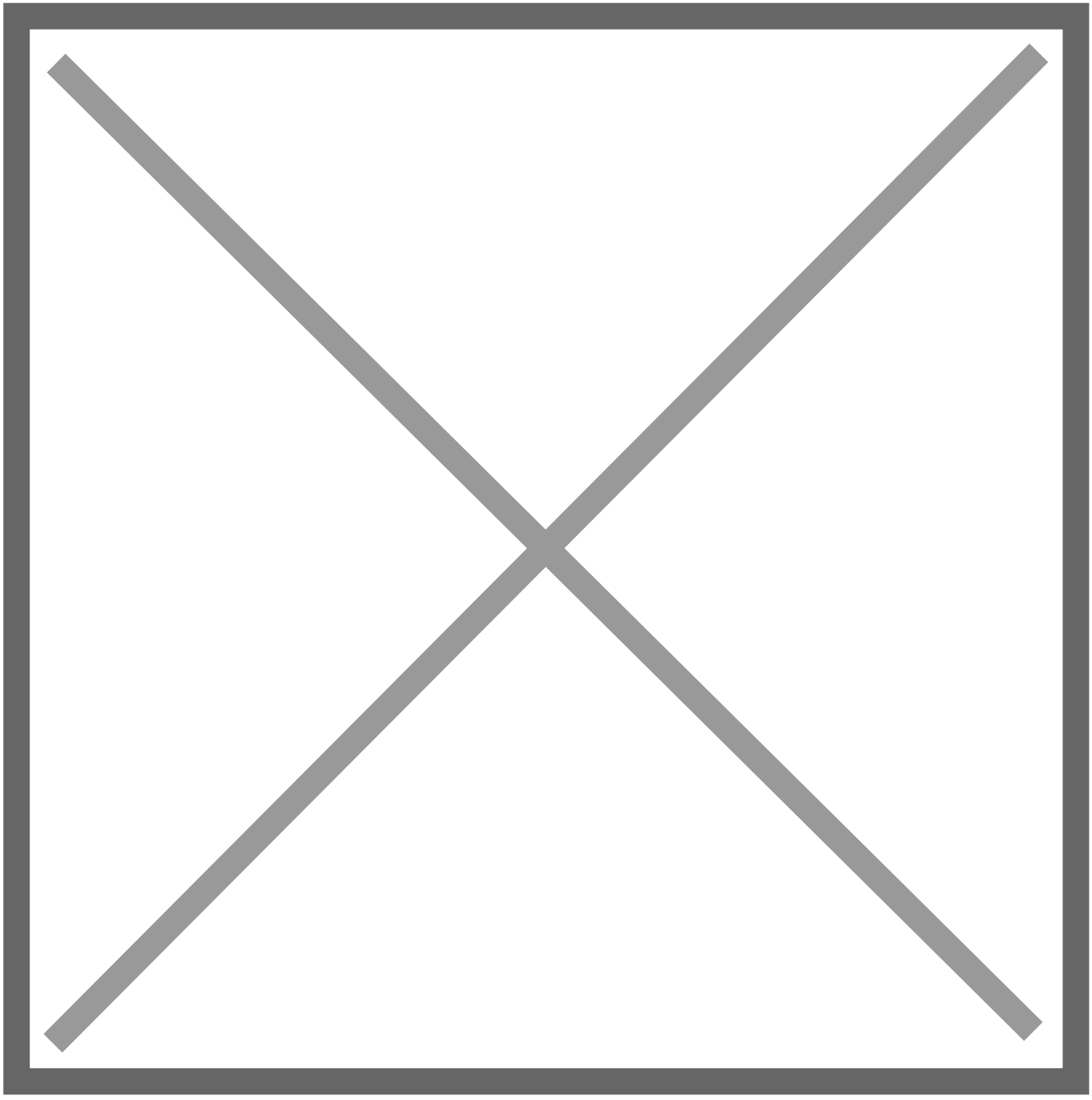


Схема сервисной модели SOC

В случае **гибридной модели SOC** оборудование приобретается на средства заказчика и разворачивается в его инфраструктуре, заказчиком закупаются лицензии для SIEM, SOAR решения, а управление осуществляется совместно с сервис-провайдером.

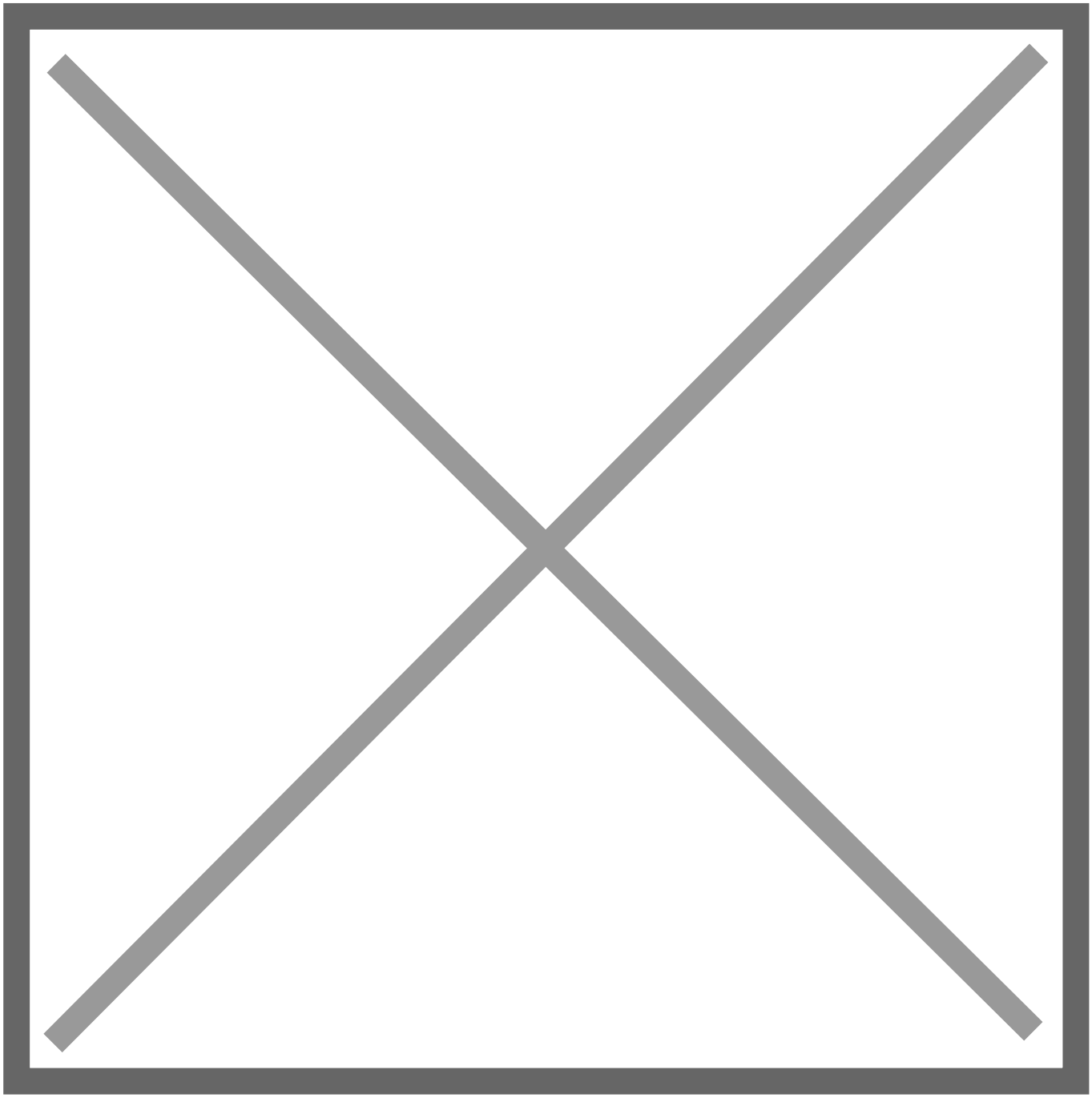


Схема гибридной модели SOC

Аутсорсинговая и, в меньшей степени, гибридная модели позволяют оптимизировать затраты на ИБ и сосредоточиться на профильных активностях компании-заказчика. Собственный SOC позволяет более глубоко углубиться в процессы и особенности инфраструктуры компании, поэтому у каждой модели есть свои сильные и слабые стороны.

Концепты информационной безопасности

Конфиденциальность. Сохранение целостности, защиты от утечки сведений, которые не предназначены для общего использования и несут интеллектуальную, экономическую ценность для обладателя. Отвечает на следующие вопросы:

- Насколько защищена информация?
- Насколько она должна быть защищена?

К механизмам защиты конфиденциальности относятся шифрование, пароли, аутентификация, брандмауэры и т.д.. Также в этот раздел попадает физическая защита - двери, заборы и камеры.

Целостность. Состояние информации, при котором отсутствует любое её изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право. Для определения целостности информации можно использовать:

- Насколько верна информация?
- Была ли она изменена или повреждена?

Хеширование, цифровые подписи и контрольные суммы помогают отслеживать и проверять целостность.

Доступность. Возможность своевременного и надёжного использования информации или сервисов. Отвечает на вопрос “Всегда ли данные, которые должны быть доступны пользователю, доступны?”

Избыточность систем хранения, питания и передачи данных помогает повысить доступность информации. Также относятся стратегии резервного копирования и аварийного восстановления данных в случае повреждения или утраты.

Риски и управление ими

Риск является центральной точкой другой триады: угрозы, уязвимости и активы.

- Если у вас нет ничего, что может быть украдено, то скорее всего вы ничем не рискуете.
- Если ваша система безупречна (вспомним сервер на подводной лодке), то уязвимостей нет.
- Если никому не нужны ваши активы или у них нет способов для их кражи, вы свободны от угроз.

Активы. Ресурс, которым владеет или который контролирует бизнес, в материальной или нематериальной форме, используемый для создания экономической выгоды.

- информация или данные;
- сетевое оборудование;
- серверы/компьютеры;
- программное обеспечение;
- персонал;
- процессы.

Уязвимости. Недостаток программно-технического средства или информационной системы в целом, который может быть использован для реализации угроз безопасности информации

Это внутренниме факторы. Патчи или дополнительные меры безопасности могут устранить эти недостатки. Иногда уязвимость находится вне вашего контроля, например, при использовании закрытого программного обеспечения. Задача инженера ИБ — компенсировать эти слабости.

Угрозы. Любое состояние, которое может привести к краже, потере, повреждению или компрометации актива.

К угрозам относятся стихийные бедствия, кибератаки или вредоносное ПО. Угрозы не обязательно должны быть преднамеренными: мать-природа тоже опасна, и случаются несчастные случаи. Задача отдела ИБ — закрыть уязвимости, соответствующие вашим угрозам, а НЕ победить саму угрозу.

Классификация угроз

Враждебные угрозы Иностранные правительства, поставщики и конкуренты.

Случайные угрозы

- Ошибки, которые наносят ущерб безопасности системы
- Опечатки или непреднамеренные действия, вредящие безопасности.
- Сотрудник случайно взял устройство домой
- Случайное нажатие кнопки питания, пожарной сигнализации и т. д.

Инфраструктурные угрозы

- Сбой оборудования, программного обеспечения или датчиков
- Сбой жесткого диска, перегрев, ошибки и сбои
- Причина, по которой компании делают резервное копирование и обеспечивают избыточную доступность данных.

Экологические угрозы

- Природные или техногенные катастрофы
- Пожары, наводнения, ураганы, отключение электроэнергии, обрывы проводов и т. д.
- Еще одна веская причина для резервного копирования и избыточности.
- Угрозы выходят за рамки «злоумышленников». Недовольные сотрудники, несчастные случаи и ошибки могут привести к потере активов или поставить под угрозу безопасность.

Риски меняются! Квантовые компьютеры сейчас не представляют угрозы, но могут стать ею через несколько лет, и могут радикально изменить подход к определению уязвимостей.

Обзор методологий

Lockheed Martin's Cyber Kill Chain

В 2011 году Lockheed Martin's была разработана методология Lockheed Martin's Cyber Kill Chain. Она используется для определения этапов эксплуатации компьютерных сетей.

Advanced Persistent Threats (APT). APT — это группы или организации, которые, вероятно, спонсируются национальными государствами. APT хорошо подкованы в области информационной безопасности, имеют доступ к огромным ресурсам, как финансовым, так и технологическим. Цель — получить несанкционированный доступ к системам и постоянно совершенствовать методы и тактику.

Цепочка Cyber Kill Chain

- Разведка
- Вооружение
- Доставка
- Эксплуатация
- Установка
- Управление и контроль (Command and Control, C&C, C2)
- Достижение конечной цели

MITRE ATT&CK

В 2013 году MITRE создала каталог техник, используемых в успешных APT-атаках. Подобно «Cyber Kill Chain», ATT&CK MITRE описывает активности атакующих от разведки до компрометации.

В отличие от Kill Chain, MITRE ATT&CK описывает конкретные технические детали действий, выполняемых над целью, и связывает их в общую картину или тактику. Cyber Kill Chain компании Lockheed Martin's описывает, почему злоумышленники следуют определенной серии шагов: от разведки до эксплуатации целевых машин. Методология MITRE ATT&CK описывает, как именно злоумышленники выполняют эти действия. Всего в матрице описано 14 тактик:

- разведка (Reconnaissance);
- подготовка ресурсов (Resource Development);
- первоначальный доступ (Initial Access);
- выполнение (Execution);
- закрепление в системе (Persistence);
- повышение привилегий (Privilege Escalation);
- обход средств защиты (Defense Evasion);
- доступ к учетным данным (Credential Access);
- исследование (Discovery);
- дальнейшее перемещение (Lateral Movement);
- сбор данных (Collection);

- управление и контроль (Command and Control);
- эксфильтрация данных (Exfiltration);
- воздействие (Impact).

Каждая тактика состоит из множества техник и подтехник. В конечном итоге, MITRE описывают конкретные действия, предпринимаемые атакующими, зачастую с указанием реальных примеров обнаруженных атак.

Ссылка на тактику “Закрепление в системе” с техниками и подтехниками:

https://attack.mitre.org/techniques/T1137/

Отчеты об атаках

При сравнении двух отчетов можно заметить некоторые сходства:

Фаза	Индикатор
Разведка	поиск публично доступных серверов Jenkins
Вооружение	Использование скрипта PowerShell для загрузки майнера Monero
Доставка	HTTP POST запрос в каталог CLI, содержащий код для скачивания эксплойта
Эксплуатация	Эксплойт CVE-2017-1000353 через скрипт PowerShell
Установка	C:\Windows\minerxmr.exe
Командование и контроль (C2)	222.184.79.11:5329
Достижение конечной цели	Майнинг Monero

И второй отчет:

Фаза	Индикатор
Разведка	поиск публично доступных серверов Oracle WebLogic
Вооружение	Использование скрипта PowerShell для загрузки майнера Monero
Доставка	HTTP POST запрос, содержащий XML, с кодом для скачивания эксплойта
Эксплуатация	Эксплойт CVE-2017-10271 через скрипт PowerShell
Установка	C:\minerxmr.exe
Командование и контроль (C2)	222.184.79.11:5329
Достижение конечной цели	Майнинг Monero

Обратите внимание на незначительные различия между двумя таблицами. Хотя злоумышленник использовал две разные уязвимости, остальные этапы цепочки практически не изменились.

Поскольку злоумышленник использовал одно и то же имя файла, скрипт PowerShell, путь установки и IP-адрес C2, это ускоряет выявление и устранение угрозы. Сходство показателей позволяет аналитикам определить, что атаки, вероятно, проводились одними и теми же преступниками.

Дополнительные материалы

- Хакеры Черные шляпы, Белые шляпы и Серые шляпы – определение и описание
- 14 типов хакеров, которых следует остерегаться
- Хакерские группировки
- Виды угроз информационной безопасности
- Управление рисками информационной безопасности
- Книга: Кибербезопасность: главные принципы.
- Цепочка Kill Chain: от моделирования до проектирования защищенного периметра
- Аналитические статьи Positive Technologies
- Материалы и исследования BI.ZONE
- MITRE ATT&CK: что это и как применять в целях кибербезопасности
- Матрица MITRE ATT&CK, переведенная на русский язык
- Инциденты информационной безопасности: выявление, расследование и реагирование

Revision #5
Created 15 October 2025 15:29:14 by Admin
Updated 28 October 2025 14:17:35 by Admin