**Лекция 15**

**Угроза ИБ**возникает при наличии следующих взаимосвязанных компонентов:

источник угрозы + уязвимость актива + способ реализации угрозы + объект воздействия + вредоносное воздействие и его последствия.

**Угроза ИБ –**это потенциальная**причина**возникновения**событий ИБ**и **инцидентов ИБ.**

**Событие ИБ**– это изменение состояния элементов ИТ-инфраструктуры, которое может свидетельствовать о возникновении инцидента ИБ.

**Инцидент ИБ**– это событие ИБ, приводящее к несанкционированному изменению состояния защищенности информации (конфиденциальности, целостности, доступности), т.е. к реализации угрозы ИБ.

**Определения по стандарту ISO 27000:2016:**

**Событие ИБ**– это определенное состояние системы, сервиса или сети, указывающее на вероятное нарушение политики ИБ или сбой мер защиты или на некую ранее неизвестную ситуацию, которая может иметь отношение к ИБ.

**Инцидент ИБ**– это одно или несколько нежелательных или неожиданных событий ИБ, которые со значительной вероятностью указывают на компрометацию бизнес-процессов или реализованную угрозу ИБ.

Причинно-следственная связь:

**Потенциальная угроза -> Событие -> Инцидент -> Реализованная угроза**

**Сбор событий ИБ из СЗИ и ПО (системного и прикладного) на примере настройки аудита в ОС Windows**

****

**Средства мониторинга и корреляции событий ИБ** (Log Management (LM) и SIEM-системы) осуществляют сбор, агрегацию, запись, хранение, поиск, таксономию, обогащение (SIEM), корреляцию (SIEM) событий ИБ от источников.

**Источники** событий ИБ:

* Активный источник - умеет сам передавать данные в системы LM/SIEM (проще настройка, достаточно лишь указать сетевой адрес LM/SIEM, пересылка происходит по протоколу Syslog)
* Пассивный источник - к нему должна обратиться SIEM-система (более сложная настройка, LM/SIEM-система должна иметь функционал интеграции с большим количеством типов источников).

**Системы управления событиями ИБ**(Log Management):

* Сбор/получение данных из различных источников событий ИБ
* Эффективное хранение
* Быстрый поиск
* Отсутствует полноценная корреляция событий
* Отсутствует дополнительный функционал
* Невысокая стоимость.

**Системы управления информацией о безопасности и событиями ИБ**(SIEM - Security Information and Event Management):

1. **Получение** журналов с разнообразных средств защиты: поддержка большого количества типов систем, проприетарных протоколов, API-запросов.
2. **Нормализация** полученных данных: преобразование данных в единообразный, пригодный для дальнейшего использования формат.
3. **Таксономия** нормализованных данных: классификация нормализованных сообщений для формирования и последующего анализа последовательности типов событий с определенным смыслом и временем наступления.
4. **Корреляция** классифицированных событий: соотнесение между собой событий, удовлетворяющих тем или иным условиям (**правилам корреляции**).
5. **Создание инцидента**, предоставление инструментов для проведения расследования.
6. **Хранение** информации о событиях и инцидентах в течение длительного времени (от 6 месяцев) с механизмами сжатия, оптимизации.
7. Быстрый **поиск** по хранящимся в SIEM данным.

**Пример правил корреляции**:

* если на двух и более ПК в течение 5 минут сработал антивирус с одинаковой сигнатурой, то это вирусная атака;
* если в течение 24 часов были зафиксированы чьи-то попытки удаленно зайти на сервер, которые в конце концов увенчались успехом, а затем с этого сервера началось копирование данных на внешний файлообменник, то это может свидетельствовать о том, что злоумышленники подобрали пароль к учетной записи, зашли на сервер и похищают информацию.

Характерная особенность SIEM-систем – **интеграция** со сторонними решениями для более комплексного анализа событий и инцидентов ИБ.

Один из типов таких решения – **системы киберразведки угроз**(Cyber Threat Intelligence), которые передают в SIEM-систему данные, называемые **источниками Threat Intelligence**(TI Feeds, или TI-фидами, источниками данных киберразведки).

**TI-фиды**– это набор индикаторов компрометации (Indicators of Compromise (IoC)), использование которых связано с подходом «Assumed Breach» («Считайте, что вас уже взломали») – сложное вредоносное ПО находится в инфраструктуре атакованной компании десятки/сотни дней до момента обнаружения.

**Индикатор компрометации**– это некий объект/артифакт, обнаруженный в ИТ-инфраструктуре компании, наличие которого с высокой долей вероятности может свидетельствовать о готовящейся, совершающейся или уже осуществленной компьютерной атаке.

**Cyber Threat Hunting (поиск киберугроз)**– это поиск угроз внутри сети: анализ потенциальных свидетельств атаки вирусов, поиск следов деятельности киберпреступных групп, поиск признаков заражений (руткиты/буткиты, прошивки), анализ сообщений от сторонних компаний.

**Cyber Threat Intelligence (киберразведка)**- это поиск информации о потенциальных атакующих, в том числе об APT-группировках (от «Advanced Persistent Threat», усложненная устойчивая угроза / целевая кибератака).

Киберразведка условно разделяется на:

* **Стратегическую** – поиск данных о потенциально опасных для защищаемой компании APT-группах, в том числе информации об их подготовке к совершению кибератаки;
* **Тактическую** – поиск данных о тактиках, техниках и процедурах атакующих, сокращенно TTPs (Tactics, Techniques, Procedures);
* **Оперативную** – поиск непосредственных признаков приготовления к атаке: специфических сетевых сканирований для анализа инфраструктуры и поиска уязвимостей, мошеннических входящих звонков и фишинговых писем.

Индикаторы компрометации (IoCs) могут представлять собой:

* **Статические** объекты – хэш-суммы файлов и их имена и расположение, IP-адреса, DNS-имена серверов в сети Интернет или конкретные URL (ссылки, например на фишинговые страницы), названия веток и ключей реестра Windows, названия мьютексов (mutex, специализированный механизм синхронизации исполняемого программного кода);
* **Динамические** объекты – определенная последовательность несанкционированных действий на атакуемой системе (это также называют индикатором атаки, Indicator of Attack (IoA)), необычное поведение учетных записей в системе, несанкционированное появление новых учетных записей (особенно высокопривилегированных), рост числа подозрительных DNS-запросов, ICMP-трафика, иных видов ранее нехарактерной сетевой активности.

Для точного обнаружения атаки менее подходят статические индикаторы (поскольку могут быть легко заменены/обновлены злоумышленником), а самыми надежными способами будут методы, использующие анализ TTPs злоумышленников - последовательности шагов, применяющихся атакующими, которые в том числе определяются динамическими индикаторами компрометации, например, последовательностью запуска определенных утилит и программ, доступом к памяти системных процессов, обращением к служебным сетевым ресурсам и т.д.

**Для обмена информацией** об индикаторах компрометации используются **Threat Intelligence фиды**(TI feeds, источники получения данных киберразведки):

* Список хэш-сумм вредоносных файлов;
* Список IP-адресов и DNS-имен вредоносных доменов
* Список URL-адресов подозрительных веб-ресурсов.

**Стандарты и протоколы**для получения данных киберразведки:

* STIX/TAXII
* OpenIOC
* CybOX.

**Существуют**:

* коммерческие центры получения данных Threat Intelligence (например, [IBM X-Force Exchange](https://exchange.xforce.ibmcloud.com/), [Cisco](https://talosintelligence.com/%22%20%5Ct%20%22_blank)[Talos](https://talosintelligence.com/) и т.д.)
* некоммерческие ([AlienVault](https://otx.alienvault.com/%22%20%5Ct%20%22_blank)[OTX](https://otx.alienvault.com/) , [Anomali](https://www.anomali.com/ru/platform/limo%22%20%5Ct%20%22_blank)[Limo](https://www.anomali.com/ru/platform/limo) и т.д.)
* государственные: в РФ это ГосСОПКА (НКЦКИ) и ФинЦЕРТ (ЦБ РФ).

**Реагирование на инциденты информационной безопасности**

По документу [NIST SP 800-61](https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final) «Computer Security Incident Handling Guide» («Руководство по обработке инцидентов компьютерной безопасности»), реагирование на инциденты ИБ состоит из нескольких взаимосвязанных процессов:

1. Подготовка

2. Детектирование

3. Анализ

4. Сдерживание/локализация

5. Устранение

6. Восстановление

7. Пост-инцидентные действия

**1. Подготовка**

Предварительный этап, документальная подготовка: разработка и согласование четких, подробных и удобных политик, процедур и инструкций по реагированию. Требуется разработать сценарии реагирования (playbooks/runbooks), по которым команда реагирования будет предпринимать заранее заданные действия в зависимости от деталей инцидента. Проводить регулярные тренировки по отработке шагов, определенных в написанных документах, обучение персонала компании и команды реагирования корректным техническим и организационным действиям во время инцидента. Обеспечить команду реагирования всем необходимым программным и аппаратным обеспечением. Выполнить превентивные действия по предотвращению инцидентов (защитить сеть и устройства компании, установить СЗИ, провести обучение сотрудников основам ИБ).

**2. Детектирование**

Для понимания инцидента можно руководствоваться заранее определенным списком возможных типов инцидентов ИБ и перечнем признаков возможных инцидентов.

Признаки можно условно разделить на прекурсоры и индикаторы инцидентов ИБ:

* **Прекурсор** - это признак того, что инцидент ИБ может произойти в будущем (например, сканирование портов).
* **Индикатор** - это признак того, что инцидент уже произошел или происходит прямо сейчас (например, сообщения от СЗИ, вредоносная активность, сбои в работе систем).

Выявление аномалий в сетевом трафике и поведении пользователей может осуществляться с помощью модуля анализа действий пользователей и сущностей (UEBA - User and Entity Behavior Analytics ), который интегрируется с СЗИ, SIEM-системами.

**3. Анализ**

Аналитик ИБ определяет, был ли зафиксированный инцидент «боевым» или это было ложноположительное срабатывание. Следует провести идентификацию и первичную обработку (триаж, англ. triage): определить тип инцидента и категорировать его. Далее определяются индикаторы компрометации, анализируется возможный масштаб инцидента и затронутые им компоненты инфраструктуры, проводится ограниченное форензик-обследование для уточнения типа инцидента и возможных дальнейших шагов по реагированию.

**4. Сдерживание / локализация инцидента**

Оперативная минимизация потенциального ущерба от инцидента ИБ и предоставление временного окна для принятия решения об устранении угрозы путем:

* включения более строгих запретительных правил на межсетевом экране для зараженного устройства,
* изоляция зараженного хоста от локальной сети компании,
* отключение части сервисов и функций,
* полное выключение зараженного устройства.

**5. Устранение**

Производятся активные действия по удалению угрозы из сети и предотвращению повторной атаки: удаляется вредоносное ПО, изменяются взломанные учетные записи (временно заблокировать / переименовать / сменить пароль / включить МФА), устанавливаются обновления и патчи для эксплуатированных уязвимостей, изменяются настройки средств защиты (например, для блокировки IP-адреса взломщиков). Указанные действия выполняются для всех затронутых инцидентом сущностей - устройств, учетных записей, программ.

**6. Восстановление**

Проверить надежность предпринятых мер защиты, вернуть системы в нормальный режим работы, возможно, восстановив какие-то системы из резервных копий или установив и настроив их заново.

**7. Пост-инцидентные действия**

Проанализировать причины инцидента для того, чтобы свести к минимуму вероятность повторного аналогичного инцидента в будущем, а также оценить корректность и своевременность действий персонала и средств защиты, и, возможно, оптимизировать какие-то процедуры реагирования и политики ИБ. Использовать агрегированную базу знаний для ведения накопленного опыта реагирования.

**Ситуационные центры информационной безопасности - Центры SOC (Security Operations Center)**

**Задачи SOC**- это мониторинг работы СЗИ и реагирование на инциденты ИБ. **Центр SOC**- это группа специалистов по защите информации, которые непрерывно осуществляют контроль за сообщениями, поступающими от технических средств, для того, чтобы оперативно устранить угрозу информационной безопасности.

SOC-Центры:

* Внутренние (выделенное структурное подразделение компании)
* Внешние (коммерческие / аутсорсинговые).

***SOC = технологии + процессы + сотрудники***

**1. Технологии SOC-Центров:**

* SIEM - Security Information and Event Management, системы управления информацией о безопасности и событиями информационной безопасности;
* IRP - Incident Response Platform, платформы реагирования на инциденты информационной безопасности;
* SOAR - Security Orchestration, Automation and Response, системы управления, автоматизации и реагирования на инциденты;
* SGRC - Security Governance, Risk-management and Compliance, системы управления информационной безопасностью, рисками и соответствия законодательству.

**2. Процессы SOC-Центров**

Сценарии реагирования (playbooks/runbooks), по которым команда реагирования будет предпринимать заранее заданные действия в зависимости от деталей инцидента. Отработка сценариев, тестирование, обучение сотрудников. Настройка правил корреляции в SIEM. Настройка, оптимизация SIEM/IRP/SOAR/SGRC-систем. Взаимодействие с заказчиками для уменьшения ложноположительных срабатываний.

**3. Сотрудники SOC-Центров:**

1. Системный администратор или инженер - тот, кто настраивает внутренние системы SOC-Центра, которые используются в обработке инцидентов заказчиков (это системы SIEM, SOAR, IRP и аналогичные), а также отвечает за стабильность получения данных из систем компании-заказчика.

2. Специалист по настройке правил в системах SIEM, SOAR, IRP получает от заказчика вводные данные о работе информационных систем и затем составляет правила выявления инцидентов и реагирования на них в используемых в SOC-Центре системах. Это могут быть:

* правила корреляции в системах SIEM,
* правила автоматического реагирования, локализации, восстановления информационных систем при помощи SOAR и IRP решений,
* сигнатуры, т.е. правила, по которым угроза должна быть обнаружена.

3. Аналитик 1-го уровня осуществляет первичную обработку киберинцидентов - так называемый "триаж" или распределение и первичный отсев явных ложноположительных срабатываний. Опираются на заранее созданные сценарии реагирования, в которых указана последовательность шагов, которые надо оперативно предпринять при поступлении того или иного типа инцидента. В случае, если аналитик 1-го уровня может самостоятельно выполнить все действия, он осуществляет реагирование своими силами. Если он столкнулся с необходимостью эскалации инцидента, то он передает его на следующий уровень - аналитику 2-го уровня.

4. Аналитик 2-го уровня получает данные с 1-го уровня реагирования, анализирует инцидент вручную, применяя свои экспертные знания. Может эскалировать инцидент еще выше - специалисту по реверс-инжинирингу, форензик-эксперту или в специализированные компьютерные лаборатории.

5. Специалист по реверс-инжинирингу - эксперт высшей категории, как правило, профессиональный программист, решивший посвятить себя изучению образцов вредоносного программного кода для противодействия осуществляемых с их помощью кибератакам. Задача реверс-инженера состоит в том, чтобы понять, что делает и 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.

6. Форензик-эксперт - это специалист по форензике (англ. forensics), т.е. компьютерной криминалистике. Эти специалисты могут понять, что изменилось в атакованной системе (компьютере, сервере, смартфоне), какие данные были стерты, изменены или похищены вирусом, какие еще системы в компании-заказчике были атакованы. Они даже способны воссоздать полный путь распространения угрозы, например, вируса: определить, на каком компьютере был этот вирус впервые запущен (чаще вирусы отправляют по email невнимательным сотрудникам), что именно он делал на зараженной системе (как правило, сначала вредонос "осматривается", пытаясь понять, куда попал, затем докачивает с сервера злоумышленников дополнительные компоненты, затем повышает свои права на атакованном ПК и начинает распространяться по сети компании), как затем развивалась атака и как был в итоге нанесен ущерб (чаще всего похищается либо важная коммерческая информация, либо денежные средства со счетов фирмы, либо персональные данные клиентов, сотрудников).

7. Специалист по киберразведке отвечает за поиск ранее не обнаруженных или затаившихся вредоносных программ в системах заказчиков (например, вирусов-логических бомб, которые срабатывают только при наступлении определенных условий, а до этого никак себя не проявляют). Также такой эксперт ищет в интернете, на специализированных закрытых хакерских форумах информацию о новых вирусах, новых киберпреступных группировках, пытается понять, не планируют ли злоумышленники массированную атаку на компанию-заказчика, нет ли "заказа" на кражу коммерческой информации защищаемой фирмы.

8. Менеджер SOC - это тот человек, который «переводит» техническую информацию об инциденте с языка ИТ и ИБ-специалистов на язык бизнеса, чтобы руководители компаний-заказчиков могли понять, насколько серьезным был ущерб или какую именно угрозу удалось предотвратить. SOC-менеджер также координируют работу всей команды SOC-Центра, связывает друг с другом заказчиков и исполнителей, выполняет организационную работу.