Актуальные проблемы SOC

Никита Цыганков, *руководитель направления внедрения средств защиты информации, АО "ДиалогНаука"*
Иван Лопатин, *технический эксперт, АО "ДиалогНаука"*

Вопросы построения эффективного ситуационного центра мониторинга информационной безопасности (Security Operation Center, SOC) затрагивают практически все организации, обеспокоенные современными угрозами информационной безопасности. Такой интерес вызван прежде всего постоянно совершенствующимися атаками и потребностью в современном инструменте противодействия им.

Действительно, SOC является одним из ключевых компонентов подразделения информационной безопасности любой организации. В качестве базовой платформы для организации SOC, как правило, выступает система мониторинга событий ИБ (SIEM).

В настоящее время большинство SOC решают только задачи начального уровня:
- сбор и хранение событий ИБ в едином централизованном хранилище;
- верхнеуровневая простая корреляция событий между различными источниками;
- базовая визуализация и отчетность.

Однако атаки с каждым годом становятся все более сложными и часто направленными на конкретную компанию. Обнаружение таких атак требует не только достаточного объема обрабатываемых событий ИБ, но и эффективного, понятного и управляемого инструмента их выявления.

Говоря о других проблемах SOC, не имеющих достаточно высокого уровня зрелости, хотелось бы отметить:
- отсутствие глубокой интеграции SIEM в инфраструктуру компании;
- отсутствие единого подхода к созданию условий правил корреляций, их описания и документирования;
- использование в SIEM неэффективных правил корреляции, которые не позволяют выявлять многие актуальные угрозы ИБ;
- разрозненность и несистематизированность существующих правил корреляции SIEM, что ведет к затруднению их настройки, управления и модернизации;
- нехватка в составе SOC квалифицированного персонала;
- отсутствие механизма обнаружения целенаправленных атак.

Построение модели выявления инцидентов

В данной статье описывается подход, включающий средства и методы, которые позволят эффективно построить модель выявления инцидентов ИБ при помощи SIEM собственными силами.

Реализация данной модели требует построения сложной, многоуровневой системы обработки событий ИБ. Каждый из уровней должен выполнять четко определенный перечень задач, что позволяет облегчить процесс эксплуатации, администрирования и обеспечивает прозрачность работы всей модели в целом. Все уровни должны быть взаимосвязаны и должны использовать в своей работе результаты выполнения предыдущих (или даже нескольких) задач.

Ниже приведены задачи, решаемые моделью в целом:
- сбор и обработка инвентаризационной информации о ресурсах, активах, пользователях и т.д. на основе состава поступающих событий;
- категоризация поступающих событий на основе их логического значения;
- сбор и проведение аналитических вычислений, необходимых для выявления инцидентов;
- выявление инцидентов ИБ и их автоматическая классификация;
- выявление атак, определение связности произошедших инцидентов, стадий атак и их классификация согласно мировым стандартам.

Уровень инвентаризации

Уровень инвентаризации (Inventory level) выполняет интеллектуальную обработку поступающих событий, используя механизмы машинного обучения (Machine Learning), что позволяет проводить постоянное обучение и актуализацию информации о существующей ИТ-инфраструктуре. Одним из неоспоримых плюсов является возможность выявления компонентов инфраструктуры организации, которые могут быть даже не подключены к SIEM.

Так, например, анализ трафика в части используемых портов может сказать об источниках и сервисах, установленных на них, и т.д.

Уровень инвентаризации реализует следующие функции:
- на регулярной основе производит автоматическую оценку качества поступающих событий ИБ в SIEM;
- обеспечивает точную идентификацию источников в поступающих событиях аудита (например, IP-адрес, имя хоста и т.д.);
- назначает категории для источников событий и других компонентов инфраструктуры, а также названия сетей, используемых в компании (например, контроллер домена, БД, сеть DMZ и т.д.).

Результатом работы уровня инвентаризации является обеспечение достоверной информацией, "что, где и как" функционирует в компании в режиме реального времени и используется последующими уровнями модели выявления инцидентов ИБ.

Уровень категоризации

Реализация уровня категоризации (Categorization level) позволяет описать любые события на любом источнике и обогатить их дополнительной информацией – категориями, однозначно говорящими о сути произошедшего события.

Например, события успешной аутентификации в операционных системах Windows и Unix дополнятся информацией, отвечающей на вопросы:
- "Что произошло?" – "Аутентификация".
- "Где произошло?" – "Операционная система".
- "Каков результат?" – "Успех".

Необходимо выполнить следующие шаги для реализации данного уровня:
- определить события, используемые в процессе выявления инцидентов ИБ;

● определить категории данных событий в зависимости от производителя источника событий, выполняемых действий и их результата;
● обеспечить обогащение поступающих событий созданными категориями.
Например, для кода события 4624, говорящего об успешной аутентификации в ОС Windows:
● присваивается категория OS;
● выполняемое действие: попытка аутентификации, присваивается категория Authentication;
● успешный результат, присваивается категория Success.

Результатом реализации уровня категоризации является наличие у всех событий, участвующих в процессе выявления инцидентов, определенных категорий. Наличие данного уровня критически необходимо для функционирования всех последующих уровней. Реализация категоризации также позволит более тонко применять параметры агрегации, фильтрации, оповещения и решить проблему, связанную с особенностями разбора событий от нестандартных источников.

Аналитический уровень

Аналитический уровень (Analytical level) производит сбор, обработку и мониторинг с использованием элементов машинного обучения. Уровень является аналитическим движком модели выявления инцидентов ИБ.

На этом уровне модели производится работа только с категорированными событиями, полученными на предыдущем уровне.

Например, обнаружение попыток подбора пароля на внешнем ресурсе компании не является инцидентом, но нужно иметь механизмы выявления таких событий для проведения дальнейшей аналитики и возможности фиксации в составе цепочки атаки (Kill Chain).

Аналитический уровень базируется на следующих операциях:
● выполнить детализацию значимых действий на источнике событий для минимизации ложных срабатываний;
● произвести анализ событий, которые могут являться источником инцидента ИБ при определенных условиях;
● описать возможные действия предполагаемого нарушителя по каждому из источников, исходя из настроенных параметров аудита.

Неоспоримым плюсом данного уровня является возможность выявления значимых событий в инфраструктуре компании, которые могут быть использованы в реализации процесса выявления инцидентов и целенаправленных атак на компанию.

Данный уровень является неотъемлемой частью и базой для следующих уровней модели.

Уровень выявления инцидентов

Этот уровень обеспечивает выявление инцидентов ИБ и их автоматическую классификацию. На данном уровне создаются механизмы (правила) выявления инцидентов, базирующиеся на результатах работы предыдущих уровней.

Например, событие удачной аутентификации на внешнем ресурсе компании после обнаружения цепочки событий попыток подбора пароля будет являться инцидентом.

Реализация данного уровня требует выполнения следующих задач:
● наличие экспертной оценки в части определения актуальных угроз для компании, методов их реализации, а также способов их выявления;
● автоматическая классификация инцидентов по разработанной заранее матрице;
● наличие механизмов реагирования на инциденты ИБ.

Очевидный плюс реализации данного уровня – прозрачность работы и простота администрирования для аналитиков ИБ, он является быстрым и эффективным инструментом для добавления и изменения условий, параметров исключений и т.д.

Уровень выявления атак

На данном уровне реализуются механизмы выявления связности обнаруженных инцидентов и значимых событий ИБ в цепочку атаки (Kill Chain).

Уровень предполагает автоматическое определение и визуализацию стадии атаки и не должен быть привязан к конкретным техникам и методам проведения атак.

Только при грамотной организации работы всех четырех предыдущих уровней открывается возможность создания механизма выявления сложных атак, в том числе растянутых во времени. Кроме того, появляется возможность проведения ретроспективного анализа событий с целью определения атак, находящихся на той или иной стадии развития.

Для реализации данного уровня понадобится:
● знание принципов реализации атак на любой из компонентов инфраструктуры компании;
● наличие red team для контроля и совершенствования работы уровня и адаптации модели под новые угрозы и методы атак;
● наличие "песочницы" для отработки техник атак как по сложности, так и по времени;
● разработка скоринговой модели;
● разработка механизма визуализации векторов атак;
● разработка решений для сбора и обработки индикаторов компрометации (IoC);
● создание механизма автоматического определения связанности выявленных инцидентов, на основе различных критериев и последующего аналитического объединения их в одну цепочку Kill Chain.

Реализация данного уровня предоставляет механизмы выявления целенаправленных атак и злонамеренной деятельности на основе данных от всех уровней модели выявления инцидентов ИБ.

Уровень позволяет определять направление развития атаки, а также классифицировать инциденты ИБ в составе проводимой атаки или злонамеренной деятельности, согласно общепринятым международным практикам (например, матрице MITRE ATT&CK).

Пакет правил корреляции для ситуационного центра ИБ

Существуют различные подходы к выявлению инцидентов информационной безопасности, но множество из них так и остаются на бумагах. Сегодня рынок ИБ в России переполнен рекламными предложениями по "эффективному" выявлению инцидентов, которые очень далеки от практической реализации. Основным подходом компании "ДиалогНаука" является внедрение только проверенных, инновационных механизмов борьбы с целенаправленными атаками в рамках SOC-решений на базе SIEM Micro Focus ArcSight.

Нами был разработан и апробирован у ряда заказчиков пакет правил корреляции для ситуационного центра ИБ, который реализует описанную в статье модель на базе SIEM Micro Focus ArcSight в виде набора готовых правил корреляции и отчетов. Пакет создан на основе многолетнего опыта компании "ДиалогНаука" по внедрению и сопровождению ПО ArcSight в большом количестве компаний из различных отраслей. Пакет постоянно развивается, и в него добавляются новые виды правил корреляции, позволяющие обрабатывать информацию о компонентах компании, оценивать качество поступающих событий, эффективно выявлять инциденты и выявлять целенаправленные атаки различной сложности.

Пакет правил корреляции для ситуационного центра ИБ позволяет:
● значительно повысить эффективность существующей системы мониторинга событий ИБ ArcSight;
● сократить временные затраты на создание новых правил корреляции за счет использования готовых сценариев выявления угроз;
● реализовать многоуровневую обработку событий и унифицировать подход к созданию новых сценариев;
● выбрать готовые сценарии выявления инцидентов ИБ, исходя из актуальных угроз и существующих средств защиты;
● подключать новые источники без необходимости изменения логики работы правил. ●

NM Реклама
АДРЕСА И ТЕЛЕФОНЫ АО "ДИАЛОГНАУКА"
см. стр. 48