Аналитическое чтение тезисов с лекции 2 (от 16 фев 2015)

Тарасова Анасатсия

26 марта 2015 г.

Исследователь безопасности пытались понять работу центра управления инцидентами (SOC) и как аналитики в области безопасности выполняют свою работу. Эта работа обусловлена тем, что мониторинг и анализ безопасности - это не толькотехническая проблема. Исследователи должны принимать во внимание человеческий фактор. Большая работа в этом направлении благодаря интервью аналитиков безопасности в SOC. Но интервью не всегда возможно так как аналитики ограничены во времени и работают в стрессовой ситуации. Существует также вопрос доверия, который ограничевает количество информациии, получаемое при интетрвью. В своей работе Автор использует антропологческий подход к решению этой проблемы, проводя интервью со студентами, выполняющими работу аналитиков.

1 Введение

Целью исследования является получение целостного взгляда на работу центра упрправления инцидентами и выделить следубщие аспекты:

- Структура команда общих и учебных центрах.
- Обучение методологии для новых аналитиков
- Оперативные рабочие потоки
- Использование средств безопасности и программного обеспечения
- График работы смен аналитиков

- Метрики, используемые для оценки эффективности SOC

С указанными выше ценлями был принят антропологический подход к решению проблемы, в котором участвуют студенты компьютерных наук как аналитки в области безопасности академических и корпоративных SOC. Целью является понимание рботающего окружения с токи зрения аналитика.

Два центра, говорится далее Corp1-SOC и Corp2-SOC, относятся к двум корпорациям, которые предлагают информационо-технические услуги, со штаб-квартирок в США. Третий SOC, далее U-SOC, - операционный центр при общественном университете в США. Один студент прикреплен в каждый SOC как аналитик безопасности в течение двух месяцев. Студенты обучаются выполнять действующие задачи аналитиков. Студенты документируют свои ежедневные наблюдения. Записи периодически анализируются антропологом, профессором Майклом Уэском (университет штата Канзас). Таким образом работники играют роль как аналитиков SOC, так и иссле исследователей, осуществляющих критику на своем опыте и наблюдении в SOC.

2 Работа

Суть работы в том, что работники на метсе пытаются получить перспективу SOC отличную от аналитика (родной) точки зрения. Родная точка зрения включает в себя неявное знание в наблюдаемом SOC которое может быть получено только через обучение, как мы делаем в нашей работе.

3 Тренинг

Каждый из работников, который нходится на месте под наблюдением профессора Майкла Уэска. Двое из работников прошли курс антропологии профессора Уэска в Университете штата Канзас. Третий исследователь получил ускоренный курс антропологии профессора Уэска удаленно. Студенты должны делать замечания и записать только факты, а не мнения или предубеждения. Каждый из студентов поддерживал цифровой журнал, где они документируют каждое событие и связь в SOC.

4 CORPORATION-I (CORP-I) SOC

Аспирант в области компьютерных наук работает аналитиком первого уровня в течение двух месяцев. Корпорация является многонациональной компанией, с филиалами во всем мире.

4.1 Команды

В SOC каждая команда работает во главе с менеджером, и все команды во главе с одним менеджером.

4.1.1 Управление

Оперативная группа состоит из аналитиков двух уровней во главе с менеджером операций. Управление осуществляется 24 часа в сутки и 365 дней в году.Оперативная группа в настоящее время состоит из 20 аналитиков первого уровня и 2 L2 аналитиков второго уроовня. Каждый аналитик работает 4 дня в неделю по 10 часа в сутки. Существуют три смены каждый день, утренние, дневные, и ночные смены. Сдвиги спланированы таким образом, что существует по крайней мере, 2 аналитика первого уровня в каждой смене.

4.1.2 Engineering

Команда инженеров отвечает за обеспечение и поддержание SOC при наличии необходимых аппаратных и программных средств. Одна из главных инфраструктур, которую поддерживают инденеры - система управления информацией о безопасности и событиях безопасности (SIEM). Инженеры также записывают и налаживают механизмы корреляции, которые определяют безопасность критических событий из исходных данных журналов.

4.1.3 Управление инцидентами

Команда управления инцидентами обрабатывает события, которые выросла с операций, требующих глубокого изучения. Например, расследование взлома аккаунтов, анализ памяти для понимания вредоносного поведения и т. д.

4.1.4 Интеллект

Разведка предоставляет информацию о различных угрозах, которые могут повлиять на организацию, например, следующим образом.

- IP-адреса, которые, как известно, являются воронки для вредоносных программ командования и контроля сервера связи.
- Список IP-адресов, которые, как известно, пройдет вредоносный контент.
- Выполнить вредоносные программы в песочнице и определить показатели компромисса (MOK).

4.1.5 Red Team

Rea Team исследует уязвимости в корпоративной IT - инфраструктуре. Если команда находит уязвимость, то комана отправляет мейл об операциях, содержащих информацию об уязвимости.

4.2 ПО и инструменты

Безопасность проведения операций зависит от целого ряда программных приложений и инструментов. В этом разделе мы описывается каждый из инструментов и их назначение.

4.2.1 Система управления информацией о безопасности и событиях безопасности (SIEM)

SIEM - наиболее важное приложение, использующееся в работе. Решение SIEM использует концепцию Enterprise Security Manager (ESM), с которым взаимодействуют аналитики. Данные из различных источников событий, таких как, брандмауэры, прокси-серверы, системы предотвращения вторжений (IPSES) и т.д. собираются с каждого источника, направляются в ESM, где нормализуются для хранения и анализа. Аналитики L1 обрабатывать сигналы, поступающие от ESM-G. Они поступают к ESM-C, если им понадобится дополнительная информация о правиле, которое вызвало коррелированное событие или если им понадобится дополнительная информация об истории вируса для хозяина или IP-адреса.

4.2.2 SOC Inbox

SOC имеет почтовый ящик, куда стекаются и обрабатываются все электронные письма, связанные с операциями по обеспечению безопасности.В почтовый ящк принимаются следующие типы писем:

- Информация о новых угрозах от интеллектуальной команды
- Сообщения об украденных устройствах
- Сканирование вирусов и повторные ответы
- Технческие коммуникации

4.2.3 Wiki knowledge base

Вики поддерживается там где все команды-операции, инжиниринг,менеджемнт событий и разведка - распределяют эту информацию. Аналитики первого уровня документируют информацию как новое множество заражений. Информация о работе с различными типами событий, новых аналитик onboarding, аналитик настройки рабочей среды, а также ссылки на различные материалы для чтения также описаны в вики. Команда инженеров документирует различные случи,технические детали различных источников событий для включения в систему SIEM информации о действующих аппаратных средствах, а также другие связанные SIEM технические детали.

4.2.4 Ticketing Systems

- Система отслеживания событий (Incident tracking system) - используется аналитиками первого уровня для создания и отслеживания объявлений инцидентов безопасности.
- Инженерная(Engineering ticketing system) - используется аналитиками первого уровня для уведомления команды инженеров с просьбой изменения в правила корреляции.
- Сетевые (Networking ticketing system) - аналитики помечают файл с просьбой найти владельца хоста или блока потенциально зараженных и распространяющих вирус в сети команды.

4.3 SOC Workflow

В ESM используется концепция каналов для отображения события, отфильтрованного по запросу. В основном канале отображаются коррелированные события, отправленные с ESM-C. Если это занимает более 3 минут, событие аннотируется и отправляется в канал 2 в ESM-G.

4.3.1 Стадии аннотации

Аннотирование является процессом маркировки событий, основанным на анализе, выполненного аналитиком. Событие, прибывающее в основной канал, аннотируется по умолчанию как поставленное в очередь. На основе анализа аналитик может аннотировать события как:

- Добавленное в список - событие подозрительно, но детальный анализ не дает окончательного решения. Обычно IP-адресат добавляется в лист наблюдения.
- Добавлено в прецедент - либо это событие требует создание нового прецедента или является частью существующего. В обоих случаях детали событий добавляются к прецеденту и его номер записывается в аннотацию замечаний.
- Требующее изменение содержания - событие является ложным срабатыванием и должны быть найдены лучшие способы корреляции. Отправляется запрос и номер запроса входит в аннотацию.
- Требующее дополнения - анализ этого события идет в запрос команде инженеров для создания нового правила
- Требующее блокировки - пилот считает, что событие ложного срабатывания и блокирует любое событие, связанное с IP-адресом или именем хоста, появляющееся в канале в течение нескольких часов.
- События интересов - данное событие требует большего, чем 3 минут на анализ и запись, представляющих интерес канала для анализа пилотом.
- Возможное без фильтрации - это событие не попадает ни в одну из вышеперечисленных категорий, классифицируется категорией по умолчанию.

Для событий, аннотируемых как "События интересов"применяются следующие этапы аннотирования:

- Добавление в список
- Добавление в прецедент
- Требование изменения содержания
- Требование дополнения
- Требование блокировки - пилот хочет заблокировать это событие на более долгое время.
- Возможное без фильтра
- Second Level Assist - событие требует поддержки аналитика второго уровня для дальнейшего исследования

Для событий, аннотированных "Second Level Assist"применяются следующие этапы аннотирования:

- Добавление в список - анатилик второго уровня подтверждает запись в списке для постоянной блокировки.
- Аномалия - L2 Аналитик считает, что событие связано с изменением правил, что привело к потоку событий в основном канале, которые не действительны.
- Возможное без фильтра - данное событие не будет признано ложноположительным и не может быть отфильтровано
- Добавление в прецедент - событие становится частью существующих или новым прецедентом.

4.3.2 Note on case severity

Как мы видели ранее, одной из аннотации к событию может быть создан прецедент. Прецедент обычно создается для следующих событий: инцидент требует владелец устройства связи для антивирусной проверки хозяина; скомпрометированный девайс должен находиться в командной сети; критический инцидент, требующий участия команды управления инцидентами.

4.3.3 Staging Channel

В основном канале должны содержаться мероприятия, действенные на каждый момент времени. Канал не должен быть заполнен ложноположительными событиями, так как в этом случае аналитики могут не заметить реальную угрозу. Чтобы предотвратить это, прежде чем источник события добавляется в основной канал, он испытывается в промежуточном канале в ESM-C. Аналитики L2-уровня, иногда аналитики L1, анализируют события в этом канале, определяют возможную методику анализа и измерения истинной и ложноположительной динамики событий (качественно). Иногда запрос модификации может быть отправлен инженерам. После достаточного анализа и определения, что сигналы, поступающие от этого канала являются действенные, источник события будут перенесен на основной канал.

4.4 Rationale behind the workflow

SOC полагает, что наиболее важным звеном по вопросам бзопасности человека является аналитик. Инструмент определения приоритета мероприятий показывает только те предупреждения, у которых превышен порог. Они считают, что человек должен принять решение при анализе каждого случая безопасности из своего опыта.

4.5 Description of two real security incidents

4.5.1 Инцидент 1

Red team отправила письмо в SOC с оповещением, что один из веб-сервером Corp-I уязвим к SQL-инъекции. Также в письме было описано какие типы атак они были в состоянии выполнить и IP адерса веб-сервера. Аналитики SOC, используя ESM искали трафик, идущий из уязвимых веб-серверов. Это было связано с тем, что если Red team была в состоянии нарушить безопасность системы следует считать, что злоумышленник в интернете будет в состоянии сделать то же самое. Аналитики обнаружили, что по крайней мере один IP адрес, кроме Re team, с которого была запущена SQL-инъекция против их же сервера. SOC передали IP для менеджмента инцидентом. Между тем инцидент-менеджмент был вызван с Red team, для получения дополнительных

деталей атаки.Программист, который написал код для веб-сервера также связался, чтобы получить подробную информацию о коде источника. План восстановления прогрессирует для исключения из веб-приложения такую уязвимость в будущем.

4.5.2 Инцидент 2

Аналитик мониторил основной канал и собирал предупреждение от системы предотвращения вторжений (IPS). Предупреждение об опасности говорит, что файл был загружен, используя уязвимость в Java клиентах. IPS обнаружила, что сервер выполнял функцию главного уязвимого файла, который получен с клиента, потенциального Java клиента. Аналитик сначала узнал что рассматриваемый сервер запускал веб-сервер как 80 порт источника предупреждения. Аналитик управляя веб-сайтом при помощи б браузера заметил, что сервер выполнял функцию главного хорошо известного эмулятора Linux-термнала клиента для Windows (?). Страница сама по себе выглядела странно, так как была только одна гиперссылка, в которой говорилось что это эмулятор терминала клиента и файл, связанный с ним. Затем аналитик скачал файл и загрузил его на зараженные просканированные веб-сайты. Сканирование указало, что файл был классифицирован как вредоносное ПО большинством сканеров. Это повысило доверие аналитика, хост которого был скомпрометирован. Инцидент передан администратору, который попросил аналитика разобрать логи для всех хостов подсети. Хосты в этом частном случае подсети были найдены. После поиска с помощью ESM, аналитик обнаружил, что с нескольких других хостов в этой подсети на самом деле отправлялся и получался подозрительный трафик. Был создан прецедент и менеджмент выполняет анализ основных причин возможной опасности.

5 CORPORATION-II (CORP-II) SOC

5.1 Teams and organization

Corp-II SOC имеет членов команды в трех местах, раположенных в Азии, Европе и США. Цели SOC команды включают интиллектуальную координацию ресурсов для реагирования на инциденты, точной и своевременной идентификации рисков, информационной безопасности, а так-

же снижжения рецедива по средствам уменьшения стратегического риска.В настоящее время команда США состоит из девяти членов, и каждый член выполняет несколько функций имеет различные специализированные навыки. Есть два менеджера, которые наблюдают за командой. Один из них настроен реагировать на инциденты и другие угрозы.

5.2 Software and Tools

Система-посредник (агрегатор) моет собирать и индексировать практически любые данные из хост-машины и хранить их в репозитории. После того как данные доступны в репозитории, аналитик может подключиться к агрегатору через браузер и запустить поиск по всем данным. Аналитик может также составлять отчеты и графики, основанные на данных, прямо из браузера. Сигналы от идентификаторов устройств идут в журнал агрегатора где они используются для дальнейшего анализа. Система документооборота автоматически создает тикеты на сигналы, поступающие от IDS чтобы аналитик смог сделать дополнительную проверку.

5.3 Analyst Training

Существует тренинг подготовки L1 аналитиков. Первый день уходит на настройку ноутбука, инструментов аналитика безопасности, виртуальных машин и запрос доступа к различным порталам. Начиная со второго дня аналитик приступает к самостоятельному изучению программ. Обучение состоит из чтения материалов с последующими задачами по ряду тем, таких как команды UNIX, Булева логика, сетевые протоколы, Wireshark, Nmap, Snort и т. п. После того как программа самообучения завершена, аналитики являются тенью опытных L1 аналитиков. За аналитиком наблюдает опытный аналитик. Аналитики обрабатывают сигналы, поступающие от ESM и задают вопросы в ходе работы. Через несколько недель, аналитик затеняет аналитика L1, После процесса затенения аналитик готов перейти на смены. Весь процесс занимает не менее 2 месяцев.

5.4 SOC Workflow

SOC следует рабочему процессу, построенному вокруг системы управления инцидентами. Новые события/предупреждения отправляются в

начало/конец очереди для проверки согласно приоритету угроз. Аналитики могут получать доступ к системе документооборота через веббраузер для работы над тикетами. В каждом тикете есть немного автоматической работы, которую тянут ресурсы об инцидене и отрадают его в тикете аналитика. Оповещения об инцидентах могут быть закрыты аналитиками или по средствам автоматизированных процессов.

6 UNIVERSITY SOC

U-SOC (UNIVERSITY SOC) - это часть многоуровневой команды, предоставляющей операции обеспечения безопасности персонала. Университет разделен на подразделения 3 уровней.

6.1 Teams and organization

Группа эксплуатации - подразделение 3 уровня, состоит из 4 аналитиков во главе с начальником информационной безопасности (CISO). Всн аналитики обработки инцидентов иногда выполняют задачи других аналитиков. Аналитики выполняют в первую очередь следующие действия. A1 - криминалист, A2 - управляющий брандмауэром, A3 -управление брандмацэром и соблюдение PCI, A4 - PCI и руководство по CISO

6.1.1 Systems Administration

Это подразделение 3 уровня, занимющееся усилением безопасности университетского дата-центра и техобслуживанием серверов кампуса. Служба также обиспечивает кампус широким спектром услуг, таки как электронная почта, службы каталогов Active Directory, и DNS, а также аппаратного и программного обеспечения мониторинга корпоративных серверов и программного обеспечения.

6.1.2 Networking

Это еще одно подразделение 3 уроня, занимающееся сетями в кампусе. Подразделение занимается созданием беспроводных точек доступа, обработкой маршрутизации, настройкой виртуальных локальных сетей, а иногда блокирует узлы сети.

6.1.3 Miscellaneous Operations

Служба 2 уровня. В настоящее время служба имеет дело с фишинг-атаками и антивирусным менеджментом.

6.1.4 Help Desk

Техподдержка - подразделение 1 уровня. Это служба для студентов, сотрудников и преподавателей по оказанию помощи по компьютерным вопросам.

6.2 Software and Tools

6.2.1 Log Management

Существует коммерческое решение SIEM в месте, которое собирает и объединяет журналы из ряда сетевого оборудования. Срок хранения журналов зависит от классификации данных. Например, журналы с устройств, которые находятся в сфере PCI хранятся не менее 1 года, в то время как журналы из устройств не относящихся к PCI могут быть удалены после 3 месяцев. SIEM solution также имеет интерфейс запросов, которые аналитики могут использовать для оформления необработанных запросов.

6.2.2 Ticketing System

Тикет-система используется для создания и управления инцидентами параллельно различными командами. Существует 4 категории тикетов: (1)инцидент-аномалия, которая должна быть устранена однажды, (2) проблема - событие происходит часто в течение короткого промежутка времени, (3) управление изменениями - пересмотр изменения в нормативных требованиях, (4) запросы связи - добавить исключение брандмауэра. Система тикетов также позволяет расчитать показатели, такие как время на решение задачи.

6.2.3 Security Appliances

Университет также управляет несколькими другими инструментам безопасности на территории кампуса, такими как Network Access Control (NAC). Приборы позволяют SOC блокировать пользователей, которые

работают в одноранговой сети (P2P) и другие запрещенные приложения. Наконец, весь интернет-трафик сети кампуса проверяется.

6.3 Analyst Training

Аналитики обучаются, комбинируя несколько стратегий, в зависимости от предыдущего опыта. Новые аналитики являются тенью более опытных аналитиков и помогают им, когда могут, например, объединяются, чтобы изменить огромный набор правил брандмауэра. Аналитики могут учиться посредством самостоятельного изучения и использования онлайн-ресурсов, для получения необходимой технической информации.

6.4 SOC Workflow

В начале недели собирают совещание для обсуждения заданий по проекту и ближайших планов на неделю. Это необходимо для оценки времени проекта. Большая часть оставшегося времени используется для проработки смежных тикетов. Если системный администратор знает службу, ответственную за инцидент, тикет создается и присваивается им. В остальных случаях, тикеты пройдут через процесс эскалации.Тикеты на инциденты обрабатываются аналитиком. Например, запросы брандмауэра будут обработаны аналитиком A2 в то время как тикеты на наличие вредоносных программ инфицированных хозяев обрабатываются аналитиком A1. После обработки тикета, аналитики комментируют тикет, в журнал активности для этого случая. Как и в SOC Corp-II, система тикетов является отправной точкой для любых операций по обеспечению безопасности.

7 REFLECTIONS ON THE FIELDWORK

Каждый SOC строится по-разному Corp-I SOC имеет два уровня аналитиков управления инцидентами, образующих третий верхний слой, а в Corp-II SOC нет такой иерархии. Все аналитики в Corp-II выполняют одну и ту же работу, но события основываются на их опыте. В SOC постоянно сталкиваются с проблемой обоснования цены управления. Контроль безопасности, в отличие от любого другого бизнеса, не может быть

оценен количественно. Никто не замечает значение SOC тех пор, пока нет нарушений.

8 CONCLUSIONS AND FUTURE WORK

В этой работе автор принимает антропологический подход для понимания того, как выполняют свою работу специалисты безопасности SOC. Трое студентов Computer Sience работали в университете двух корпораций SOC. В этой статье описан рабочий процесс, и то как команды вместе устраняют инциденты. Целью данной работы являлся обзор замечаний, высказанных работниками SOC. Автор планирует получить более глубокие выводы, полученные из углубленного анализа и представить их в другой статье.