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

Тарасова Анасатсия

15 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