

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

Тарасова Анастасия

12 марта 2015 г.

Исследователи 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 только техническая 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 ограничивает количество информации, получаемое при интервью. В своей работе Автор использует антропологический подход к решению этой проблемы, проводя интервью со студентами, выполняющими работу аналитиков.

1 Введение

Целью исследования является получение целостного взгляда на работу центра управления инцидентами и выделить следующие аспекты:

- Структура команд в 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 целями был принят антропологический подход к решению проблемы, в котором участвуют студенты компьютерных наук как аналитики в области безопасности академических и корпоративных SOC. Целью является понимание работающего окружения с точки зрения аналитика.

Два центра, говорится далее Corp1-SOC и Corp2-SOC, относятся к двум корпорациям, которые предлагают информационно-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 исследователей, осуществляющих критику на своем опыте и наблюдении в SOC.

2 Работа

Суть работы в том, что работники на месте 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 находится 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 уровня. 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