Эссе №2

Тарасова Анасатсия

3 марта 2015 г.

1 Введение

Нв сегодняшний день растет потребность в области информационной безопасности работников, особенно в компюерной сети. Однако работники не решаются делиться информацией для исследований с посторонними, ссылаясь на нехватку времени и загруженность, и это является наиболее огорчающим фактором.Цель исследования заключалась в разработке понимания правительства NOC в качестве основы для будущей сети исследований понимания ситуации. Но тем не менее, ориентированное на человека, исследование информационной безопасности работников имеет ряд проблем. В этой статье Автор описывает свои соображения, допущенные при разработки плана исследований, и уроки, извлеченные при проведении исследований в NOC.

2 Практический пример

Средой назначеня был операционный центр, отвечающий за безопасность и защиту крупной государственной сети. Доступ к информации был только у работников этажа. Принимая во внимание методику и способы исследования, Автор остановил вывод на этнографическом подходе. Из-за сложной исследовательской среды, мне нужно методов, которые были гибкими с минимальным воздействием на окружение. Встречи проводились 12 месяцев.

2.1 Встречи

Первые встречи были направлены на сбор информации для минимизации исследований н окружающиюу среду, если можно так выразиться. Семь интервью были проведены с мужчинами, которые имели опыт работы с или в NOC. Длились интервью от 45 минут до 1,5 часов. Первые четые интервью были проведены с суррогатных пользователей.Автор использовал этоттермин для описания людей, которые похожи целевых пользователь общими знаниями или опытом. Их используют, когда целевые пользователи сильно загружены или недоступны. Это очень часто бывает с загруженной сетью оборонных аналитиков. Важно, что суррогатные пользователи не являются целевыми пользователями и принимают риск, используя свои собственные предубеждения на представление о том, что может сделать и подусвть целевой пользователь. Первые два интервью были с исследователями в научно-исследовательской организацией, связанной с родительской агентства NOC.Исследователи они были в состоянии предоставить общую информацию о NOC. Также были проведены интервью с аналитиками и менеджерами NOC, цель их организации стояла в обеспечении организации технологии аналитической поддержки. Последние три интервью были с людьми, которые на самом деле работали в NOC. Последнее интервтю было с менеджером NOC, который смог предоставить Автору доступ к NOC по мере необходимости.

2.2 Наблюдения

Наблюдения происходили в основном во время ночной смены. Автор наблюдал за связью между менеджерами и аналитиками, за запланированными втречами, за моделированием кибер-событий. Автор присутствовал на учениях, предназначенных для тестирования новых страегий. Эти наблюдения дали мне ценную информацию для НОК операций, сильные и слабые стороны, и потенциальные области для будущего исследования.

2.3 Card Sorting

Card sorting провели с 12 аналитиками и менеджерами (все мужчины) с использованием 44 кибер ситуаций. Каждый вопрос был написан на карточке. Вопрос были получены из интервью и наблюдений.Результаты этого исследования дали результаты, подтвержающие, что связанные с

кибер-аналитической работой аналитики и менеджеры чувствуют себя наиболее важными в вопросах информирования ситуации.

3 Discussion

Проведение исследований, сосредоточенных на человеке, в сетевых операционных центрах является проблемой.Интенсивность работы аналитиков, чувствительность информационной среды, а также доступ к среде и люди создают барьеры для ведения исследований, сосредоточенных на человеке, в NOC.Ниже приводится краткое изложение основных выводов из этого исследования, как результаты этого исследования были использованы до настоящего времени, и извлеченные уроки, которые могли бы способствовать разработке будущих исследований в этой области.

3.1 Главные выводы

Наиболее сложный аспект работы NOC менеджера заключался в поддержании "миссии на уровне"осведомленности о состоянии сети. NOC является эффективным при своей миссии где менеджеры видят значительные улучшения, которые могут быть достигнуты благодаря использованию новых инструментов или артефактов.

3.2 Применение результатов

На сегодняшний день Автор использовал результаты этого исследования в нескольких направлениях. Ушлубленный анализ исследования card sorting привел к систематизированию в вопросах кибер обстановки, что может быть использовано в разработке NOC, ориентированной на пользователя.

3.3 Накопленный опыт

Разрабатывается план исследований, который выполнится в течение длительного периода времени. Одного визита недостаточно, и через несколько часов недостаточно. Необходимо регулярно и часто посещать NOC. Эир минимизирует воздействие на деятельность и обеспечит долгосрочную перспективу. Посещать достаточно часто чтобы поддерживать от-

ношение, но не так часто чтобы отвлекать. Можно выбрать методологию исследования с низким воздействием на окужающую средц. Несколько больших исследований могут быть сделаны в течение долгого времени и корректироваться по сере результатов развития научно-исследовательского проекта. Слишком дружественные отношения могут породить конфликт интересов и оказать сильное влияние на исследование.