Аналитическое чтение

Дедков Сергей

2015

Содержание

1 Human-Centered Study of a Network Operations Center: Experience Report and Lessons Learned

В данной статье Силеста Лин Пол описывает человеко-оринетированное изучение Сетевых Операционных Центров(NOC). NOC - станция обработки данных направляющая сигналы тревоги на пост мониторинга, которые были сформированы различными охранными системами.

Цель статьи - поделиться опытом извлеченным из проведения собеседований и полевых наблюдений для тех, кто будет изучать подобные центры в будущем.

Актуальность.

Защита сети на сегодняшний день одно из важных направлений развития компьютерной науки. Одним из средств обеспечения подобной безопасности являются NOC. А в работе NOC играет огромную роль человеческий фактор, поэтому для исследования были выбраны как раз люди.

Введение.

Методы исследования работы NOC используемые автором - интервью, наблюдение, распределение карточек, продолжительное исследование, совмещение методов, построение доверетельных отношений с сотрудниками центра. Допуск в центр получить не просто, а после этого методы исследования не должны влиять на работу центра. Работники зачастую перегружены работой, посвещать время исследованию они могли крайне не много. Они работаю 24/7 по две смены и передача смены - самы сложный момент, т.к. нужно полностью ввести в курс дела новую смену.

Исселдования продолжались 12 месяцев.

Интервью.

Еще до визита объекта были проведены интервью с работниками центра была выяснена основная информация, проведено 7 интервью по 45 минут. После чего один из работников будучи заинтересован в данном исследовании обеспечил доступ на объект.

Наблюдение.

Наблюдение осуществлялось 2 - 4 часа. При этом всего времени было потрачено 30 часов. Прводимые работы - упраженения, плановые встречи, наблюдение за ежедневными операциями.

Распределение карточек.

Для проведения данного метода выдавались карточки с проблемами, их нужно было разбить по группам в зависимости от методов применяемых для исследования. Метод позволил выявить наиболее важные аспекты работы персонала.

Вывод.

В работе важны:

- Взаимодействие персонала
- Описание работ для других коллег, при сдаче смены
- Быть постоянно в курсе состояния сети

2 A Tale of Three Security Operation Centers

Даннная статья описывает процесс и результаты работы по изучению Центров Информационной Безопасности(SOC) исследователями в области компьютерной безопасности. Работа была мотивирована помимо прочего тем, что мониторинг и анализ безопасности не только техническая проблема. Исследователи должны принимать во внимание человеческие и организационные факторы успешности исследования.

В отличие от предыдущего автора они решили, что интервью не самый лучший метод исследования и пошли другим путем. Они внедряли студентов в реальные объекты. Всего было внедрено три студента. Они вели электронные журналы, в котороых документировали все случаи происходившие в SOC.

Студенты были внедрены в следующие три SOC:

- CORPORATION-I (CORP-I) SOC

  Должность - аналитик первого уровня. Количество устройств - 350000. У этой компании имеется множество центров по всему миру, которые постоянно сотрудничают друг с другом. Задача - анализ и устранение угроз безопасности. Смена - 20 аналитиков и 2 аналитика второго уровня. За время робаты студента произошло 2 инцедента: SQL-иньекция и загрузка вредоносного файла.

- CORPORATION-II (CORP-II) SOC

  Должность - аналитик безопасности. Этот SOC корпоротивно оринетрованный. Задача - поддержать нормальное производство и непрерывность бизнеса, улучшить безопасность и жизнеспособность против будущих инцидентов, удержать и предотвратить будущие инциденты актами расследования и судебного преследования, и обучить аналитиков через акты действия контрразведки или разведки.

- UNIVERSITY SOC

  Место работы третьего студента был Общественный университет США и Олимпийский комитет США. Количество усройств - 50000. Задача - обеспечение безопасности данной сети.

Стоит отметить, что работа у каждой SOC производиться по-своему. Все зависит от модели работа SOC, количества сотрудников, задач на которые направлена работа SOC.

3 An Exploratory Study of White Hat Behaviors in a Web Vulnerability Disclosure Program

В тертьей стате описываются результаты исследования уязвимостей обнаруженных Белыми шляпами (White hats). Белые шляпы - те, кто тестируют сети и компьютеры, исследуя их производительность и определяя их уязвимости для взлома. Обычно хакеры в белой шляпе взламывают свои собственные компьютеры или компьютеры клиентов, специально нанимающих их для анализа безопасности.

Было проведено исследование и анализ 3254 документов собраных за три с половиной года, которые описывали 16446 уязвимостей. Данные предоставлены Белыми шляпами, которые рабтали по программе раскрытия Web-уязвимостей в Китае, за вознаграждение. Компания проводившая исследование - Wooyun. После того, как находилась уязвимость, компании давалось 2 недели на устранение, после чего данные публиковались. Среднее число уязвимостей на белу шляпу - 4.8, максимальное количество отчетов - 291. Основные уязвимости - SQL-иньекции и XSS. Большинство специалистов утверждают, что работа белых шляп способствует уменьшению количества уязвимостей увеличения безопасностей ПО и web-ресурсов. Важны успехи не только самых активных и высококвалифицированных белых шляп, а также тех, кто находит уязвимости не так часто, но большое количество таких белых шляп покрывает значительную область уязвимостей.

4 Выводы

Уязвимость в Интернет - одна из важных проблем компьютерной науки. Для организации должного уровня безопасности существуют как большие компании, специализированные на этом вопросе, так и отдельные специалисты. Подобными проблемами занимаются такие организации, как Сетевые Операционные Центры(NOC) и Центры Информационной Безопасности(SOC). Так же существуют отдельные специалисты, так называемые белые шляпы.

Помимо работ по обнаружению уязвимостей, которые уже известны, аналитики пытаюся найти новые уязвимости в системах, основываясь на метожах анализа сетей. В организациях NOC и SOC ведется круглосуточное наблюдение за состоянием сети, документация инцедентов и последующий анализ. Это очень большие компании, которые могут существовать в разных странах, при этом постоянно поддерживая связь.

Так же свою нишу в подобных мероприятиях занимают специалисты одиночки - белые шляпы. Многие компании проводят программы для того, чтобы специалисты в области безопасности находили уязвимости в их системах легально, с последующим вознаграждением.

Усислиями подобных организаций и специалистов поддерживается обеспечение безопасности в сети Интернет.