



Ежемесячный информационный бюллетень по безопасности

Карьера в кибербезопасности

Обзор

Кибербезопасность то, о чем мы читаем регулярно в новостях. Разные организации и правительства по всему миру ежедневно могут подвергаться атаке. Существует огромный спрос на людей, прошедших подготовку в области кибербезопасности, чтобы помочь защититься от этой растущей угрозы. На самом деле, по оценкам, в мире почти 3 миллиона вакансий. Вы рассматривали бы карьеру как профессионал в области кибербезопасности? Это быстро и динамично развивающаяся область с огромным количеством специальностей на выбор, включая криминалистику, безопасность конечных точек, критическую инфраструктуру, реагирование на инциденты, безопасное кодирование, а также осведомленность и обучение. Кроме того, карьера в области кибербезопасности позволяет вам работать практически в любой точке мира с удивительными преимуществами и возможностью добиться реальных результатов.

Нужно ли вам образование в области компьютерных наук?

Абсолютно нет! Некоторые из лучших специалистов в области безопасности имеют нетехническое образование: от английского, до медицинского или исторических специальностей до автомехаников, художников и домохозяек. Главное - это страсть к обучению. Изучение того, как кибербезопасность работает. Как только вы поймете, как работают технологии, вы сможете лучше их обезопасить. Что интересного в кибербезопасности, так это то, что вы можете изучать, как технологии работают когда вам это удобно, не выходя из собственного дома.

Как начать

Не знаете, с чего начать? Начните изучать различные технологии и посмотрите, что вас больше заинтересует.



Кодирование: изучите основы программирования. Начните с - Python, HTML или Javascript. Не знаете, с чего начать обучение? Подумайте о сайте онлайн-обучения или возьмите любую книгу для начинающих по программированию.



Системы: изучите основы администрирования операционной системы, такой как Linux или Windows. Если вы действительно хотите заняться изучением, начните с Linux. Научиться администрировать систему Linux из командной строки - это мощный навык, который поможет вам, независимо от того, какой путь вы выберете.



Приложения: узнайте, как настраивать, запускать и поддерживать приложения, такие как веб-сервер или DNS-сервер.



Сеть: узнайте, как функционирует сеть, включая изучение того, как компьютеры и устройства общаются друг с другом, собирая и анализируя сетевой трафик. Это может быть очень весело, так как ваш дом, скорее всего, уже является сетевым окружением со всеми видами устройств, подключенных к нему.

Отличный способ учиться - это создать собственную лабораторию дома. Это довольно просто, поскольку вы можете создать несколько виртуальных операционных систем на одном физическом компьютере или настроить лабораторию, используя облачные ресурсы, такие как Amazon AWS или Microsoft Azure. Как только вы запустите свои операционные системы, начните взаимодействовать с ними и изучите все, что сможете. Другим вариантом является встреча и работа с другими людьми в сфере кибербезопасности. Подумайте о посещении местной конференции по кибербезопасности (часто называемой «кон»). Почти в каждом крупном городе проводится несколько таких мероприятий в год. Хорошо известная серия мероприятий по кибербезопасности, предназначенная для помощи новичкам, называется Bsides. Самое сложное - найти такое мероприятие или встречу. Как только вы посетите одно из таких мероприятий, ваши возможности будут расти в геометрической прогрессии. Другие варианты обучения включают видео YouTube, онлайн-форумы, подписку на блоги от специалистов по безопасности или участие в онлайн-мероприятиях Capture the Flag (CTF). Наконец, есть множество программ, которые помогут вам начать свою карьеру, в том числе CyberTalent Immersion Academy, Cyber Aces и Cyber Patriot.

В конце концов, не позволяйте вашему образованию или прошлому вам препятствовать. Неважно, какой у вас опыт, вы сделаете что-то уникальное и особенное, в чем отчаянно нуждается компьютерная безопасность. Главное - это страсть к обучению. После того, как вы начнете развитие ваших навыков, и вы начнете общаться с другими в этой области у вас появятся новые возможности.

Приглашенный

Хизер Махалик (@heathermahalik) директор по криминалистике в ManTech CARD и старший преподаватель и автор курсов SANS по цифровой криминалистике и реагированию на инциденты (DFIR). Она занимается кибербезопасностью почти 17 лет и любит свою работу. Она ведет блог на www.smarterforensics.com.



Ресурсы

Bsides: <http://www.securitybsides.com>
CyberTalent Immersion Academies: <https://www.sans.org/cybertalent/cybersecurity-career/seekers>
Cyber Aces: <https://www.cyberaces.org>
Cyber Patriot: <https://www.uscyberpatriot.org/>
Code Academy: www.codeacademy.com

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 4.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: www.sans.org/security-awareness/ouch-newsletter. Редакция: Уолт Скривенс, Фил Хоффман, Алэн Вэггонер, Шерил Конли