КАРЬЕРНЫЕ ПУТИ В КИБЕРБЕЗОПАСНОСТИ

АНАЛИТИКА И ИССЛЕДОВАНИЕ

01 ВИРУСНЫЙ АНАЛИТИК

Изучает вредоносные программы, их компоненты и функционал с целью обнаружения антивирусных баз

Проводит анализ вредоносного кода для определения того, как он работает, какие уязвимости использует, каким образом и какой ущерб может нанести. После анализа разрабатывает предложение по устранению последствий, обнаружению и блокированию подобных угроз, формирует сигнатуры кода. Добавляет записи о вредоносном объекте в базы антивирусных средств защиты. Разрабатывает технические отчеты по исследуемому вредоносному ПО.

Может быть специалистом: Внешним

Опыт
- Знание и опыт работы с дизассемблерами, декомпиляторами, отладчиками (например, Assembler, x64dbg)
- Знание архитектуры ОС Windows, *nix/*nix, macOS, Android, iOS, принципов их взаимодействия
- Знание JavaScript, PHP, Python, Go, Bash, умение разбирать сильно обфуцированный код на скриптовых языках
- Знание и понимание семейств, групп вредоносного ПО, их бизнес-целей, мотивации
- Устойчивое мышление вредоносного ПО (техники, методики, инструменты, эксплойт-пак, крипторы)
- Знание и понимание матрицы или MITRE ATT&CK
- Знание C/C++

02 АНАЛИТИК КИБЕРУГРОЗ

Помогает компании собирать данные об актуальных для нее киберугрозах

Осуществляет сбор информации об угрозах информационной безопасности, которые могут быть актуальны для объекта защиты; делает предположения об их реализации; оценивает критичность и последствия для объекта защиты в случае их реализации. Умеет работать с различными источниками информации, проводить мониторинг, анализировать большие объемы информации, опубликованными аналитическими отчетами и результатами расследования реализованных атак, данными об угрозах, поступающими от средств защиты, а также с информацией о уязвимостях ПО, ПАК, содержащимися с компонентами ИТ-инфраструктуры и средств защиты информации. Помогает специалистам внутренней ИБ поддерживать в актуальном состоянии модель угроз и нарушителей объекта защиты. Разрабатывает рекомендации по организационным и техническим мерам защиты от актуальных угроз.

Может быть специалистом: Внешним, Внутренним

Опыт
- Знание методов и основ оценки и управления рисками ИБ
- Знание международных и российских стандартов моделирования угроз ИБ
- Знание и понимание матрицы или MITRE ATT&CK
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Понимание современных методов, инструментов и технологий проведения этап. актуальных угроз ИБ и средств защиты

03 АНАЛИТИК ПО КИБЕРБЕЗОПАСНОСТИ

Проводит исследования и разрабатывает аналитические отчеты в сфере ИБ

Работает над предотвращением нарушений ИБ. Определяет ландшафт угроз ИБ, анализирует технологические, экономические, политические, экономические, социальные и иные факторов влияния. Анализирует изменение законодательства, развитие технологий, ИТ/ИБ-тренды, новости и информацию о деятельности киберпреступников. Проводит исследования, разрабатывает аналитические отчеты.

Может быть специалистом: Внешним

Опыт
- Понимание ландшафта современных угроз ИБ
- Понимание современных подходов к обеспечению ИБ
- Понимание современных методов, инструментов и технологий проведения этап. актуальных угроз ИБ и средств защиты
- Знание и понимание правовых актов Российской Федерации в области ИБ и их требований (ГО ФЗ, 98-ФЗ, 187-ФЗ, 683-П, ГОСТ Р 57580.1 и т. д.)
- Широкий кругозор в сфере ИТ и ИБ
- Знание нормативных требований в области ИБ (ФЗ «О персональных данных», 152-ФЗ, 149-ФЗ и др.)

04 OSINT-АНАЛИТИК (ЭКСПЕРТ ПО СБОРУ И АНАЛИЗУ ИНФОРМАЦИИ ИЗ ПУБЛИЧНО ДОСТУПНЫХ ИСТОЧНИКОВ)

Осуществляет поиск и сбор данных под конкретную задачу сферы ИБ

Проводит работы по поиску и анализу информации для различных целей: конкурентной разведки, тестирования на проникновение, фэрфэйна, мониторинга угроз ИБ, поиска и сбора данных о конкурентах, о потенциально действующих атаках, уязвимостях, эксплойтах, которые могут помочь злоумышленнику в реализации атак.

Может быть специалистом: Внешним, Внутренним

Опыт
- Навыки OSINT (в частности анализа сетевых угроз)
- Знание работы с различными поисковыми системами
- Навыки программирования на скриптовых языках (Python, Perl, Bash)
- Знание технологий обобщения и агрегирования классов СЗИ, как зарубежных, так и отечественных
- Опыт работы в ОС Windows, Linux/*nix на уровне уверенного пользователя
- Знание работы с виртуальными машинами
- Опыт работы с аналитическими системами, фреймворками, реализующими технологии OSINT

05 РАЗРАБОТЧИК РЕШЕНИЙ ПО ИБ

Разрабатывает решения по ИБ

Занимается разработкой решений по информационной безопасности (средства защиты информации и решения для автоматизации процессов информационной безопасности). Классы разрабатываемых решений могут быть абсолютно разными, как и стек используемых при разработке для данной специальности существует большая вариативность.

Может быть специалистом: Внутренним

Опыт
- Знание принципов разработки ПО, основы языков программирования
- Знание принципов архитектуры приложений
- Знание основных фреймворков и библиотек, используемых в разработке
- Знание инструментов, помогающих при разработке, продуктов в внедрении
- Опыт работы в ОС Windows, Linux/*nix на уровне уверенного пользователя
- Понимание принципов работы сред разработки (Visual Studio, Eclipse, IntelliJ IDEA, PyCharm, AppCode, Android Studio, Xcode, Visual Studio Code, Atom, Sublime Text)
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Знание принципов архитектуры ОС Windows, Linux/*nix, macOS, Android, iOS, структуры API указанных ОС
- Знание принципов, технологий и инструментов безопасной разработки
- Знание принципов работы с распространенными средствами криптографической защиты информации

РАЗРАБОТКА, ВНЕДРЕНИЕ И ПОДДЕРЖКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

06 ИНЖЕНЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Решает задачи по внедрению средств защиты, их настройке и поддержке штатного функционирования

Имеет техническую бюгтраунд и выполняет внедрение систем ИБ, их настройку и поддержку/администрирование. Разрабатывает техническую (функциональные требования к системе защиты, руководства пользователя, руководства по администрированию, технические задания, технические решения, технорабочие проекты, спецификации) документацию в рамках жизненного цикла систем ИБ. Проводит стандарное моделирование систем ИБ (настройка, тестирование, ПМИ, ОПЭ, ОПЭ, ОПЭ