КАРЬЕРНЫЕ ПУТИ В КИБЕРБЕЗОПАСНОСТИ

01 ВИРУСНЫЙ АНАЛИТИК

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

Может быть специалистом: Внешним

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, формирует сигнатуры для антивирусов, а также рекомендации по нейтрализации кода. Добавляет записи о вредоносном объекте в базы антивирусных средств защиты. Разрабатывает технические отчеты по исследованию вредоносному ПО.

Опыт
- Знание и опыт работы с дизассемблером, декомпилятором, отладчиком (например, Ghidra, x64dbg)
- Знание архитектуры ОС Windows, macOS, Android, iOS, Linux (PE, Mach-O, ELF)
- Знание JavaScript, PHP, Python, Go, Bash, знание разбираться сильно обфуцированный код на скриптовых языках
- Знание и понимание сигнатур, групп сигнатур, эвристик, баз репутации (например, ПО Kaspersky)
- Понимание индустрии вредоносного ПО (фишинг, шифровальщики, ботнеты, APT, криптомайнинг)
- Знание и понимание матрицы этапа MITRE ATT&CK
- Знание C/C++

02 АНАЛИТИК КИБЕРУГРОЗ

Помогает компании собирать данные об актуальных для нее киберугрозах

Может быть специалистом: Внешним, Внутренним

Осуществляет сбор информации об угрозах информационной безопасности, которые могут быть актуальны для объекта защиты: делает предположение об их реализации; оценивает критичность и последствия для объекта защиты в случае их реализации. Умеет работать с различными источниками информации, включая социальные сети, форумы, сайты, специализированные, опубликованные аналитическими отчеты и результаты расследований реализованных атак, данные об угрозах, поступающие от специализированных компаний, данные в событиях безопасности, собираемые с компонентов ИТ-инфраструктуры и средств защиты информации. Помогает специалистам по анализу и расследованию инцидентов в выявлении угроз и нарушителей объекта защиты. Разрабатывает рекомендации для организационных и технических мерам защиты от актуальных угроз.

Опыт
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Знание международных и российских стандартов моделирования угроз ИБ
- Знание методов и основ аудитов и управления рисками ИБ
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание и понимание матрицы этапа MITRE

03 АНАЛИТИК ПО КИБЕРБЕЗОПАСНОСТИ

Проводит исследования и разрабатывает аналитические отчеты в сфере ИБ

Может быть специалистом: Внешним

Работает над предотвращением нарушений ИБ. Определяет ландшафт угроз, анализирует мотивацию злоумышленников, влияние политических, экономических, социальных и иных факторов влияния. Анализирует изменение законодательства, развитие технологий, ИТ/ИБ-тренды, новости и информацию о деятельности киберпреступников. Проводит исследования, разрабатывает аналитические отчеты.

Опыт
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д.)
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание и понимание матрицы этапа MITRE ATT&CK
- Знание C/C++
- Знание JavaScript, PHP, Python, Go, Bash, знание разбираться сильно обфуцированный код на скриптовых языках
- Знание и понимание сигнатур, групп сигнатур, эвристик, баз репутации (например, ПО Kaspersky)

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

Осуществляет поиск и сбор данных под конкретную задачу сферы ИБ

Может быть специалистом: Внешним, Внутренним

Проводит работы по поиску и анализу информации для различных целей: конкурентной разведки, тестирования на проникновение, расследования инцидентов ИБ, выявления угроз, а также информации о потенциалах(действующих атаках, уязвимостях, эксплоитах), которые могут помочь злоумышленнику в реализации атак.

Опыт
- Знание OSINT и умение/навыки анализа сетевых угроз
- Знание технологий обеспечения ИБ (например, ПО Kaspersky) и их уязвимостей, баз и известных атак на них
- Глубокое знание современных методологий
- Знание протоколов формирования вредоносных пакетов (Python, Powershell, Bash)
- Опыт работы в ОС Windows, Linux/*nix на уровне уверенного пользователя
- Опыт работы с аналитическими системами формирования, реализующими технологии OSINT
- Умение работать с метаданными

05 РАЗРАБОТЧИК РЕШЕНИЙ ПО ИБ

Разрабатывает решения по ИБ

Может быть специалистом: Внутренним

Занимается разработкой решений по информационной безопасности (средства защиты информации и решения для автоматизации процессов информационной безопасности). Классы разрабатываемых решений зависят от бизнес-задачи, которую они должны решать, или от технологии, для данной специальности существует большая вариативность.

Опыт
- Знание архитектуры ОС Windows, Linux/*nix, macOS, Android, iOS, структуры API указанных ОС
- Опыт работы в ОС Windows, Linux/*nix на уровне уверенного пользователя
- Знание принципов архитектуры приложений
- Знание основных фреймворков и методологий, используемых в разработке
- Знание инструментов, помогающих при разработке продуктов и решений
- Знание регулирующей законодательной базы (например, ПП РФ о импортозамещении ПО и оборудовании, требования к обязательным настройкам ПО, оборудованию, СЗИ
- Понимание принципов работы сред контейнеризации
- Опыт работы в ОС Windows, Linux/*nix на уровне уверенного пользователя

06 ИНЖЕНЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Может быть специалистом: Внешним, Внутренним

Может технической бригадой и выполняет задачи внедрения систем ИБ, их настройку и поддержку/администрирование. Разрабатывает техническую функциональные требования к системе защиты, руководства пользователей и администратора, подготовка методических инструкций и проектную документацию. Выполняет задачи по обеспечению информационной безопасности в рамках жизненного цикла систем ИБ. Проводит стандарт моделирование систем ИБ (настроек, интеграции и т.д.). Внедряет системы ИБ и инфраструктуру взаимодействия, отслеживает настройки конфигурации и полноту покрытия. Взаимодействует с вендорами по поиску и разработке решений вопросов по эксплуатации и внедрению ИБ. Обеспечивает работоспособность и штатные функционирование систем ИБ (устранение аварий и решение возникающих ошибок в работе).

Опыт
- Знание нормативных требований к обеспечению безопасности систем защиты
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Знание подходов к обеспечению безопасности ОС Windows, Linux/*nix, приложений и баз данных
- Знание технологий обеспечения ИБ (например, ПО Kaspersky) СЗИ, как аппаратных, так и отечественных
- Понимание и опыт эксплуатации СЗИ (сетевых или хостовых)
- Знание рекомендаций производителей ПО по обеспечению безопасности, ГОСТ Р 56939 «Защита информации. Разработка безопасного ПО. Общие требования»
- Знание ГОСТ Зи для возможности написания документации в соответствии с его требованиями
- Знание и опыта решений по защите информации обнаружения АСУ ТП (Genuna, Telegrab, Kaspersky Industrial Cybersecurity, Securonix, Bezkoshtovnik ACT ТС)

07 СПЕЦИАЛИСТ ПО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Работает с средствами криптографической защиты информации и криптографическими алгоритмами

Может быть специалистом: Внутренним

Администрирует и эксплуатирует средства криптографической защиты информации, обеспечивает криптографическую защиту каналов связи, работает с данной информацией, на таким может исследовать стойкость и недостатки криптографических алгоритмов.

Опыт
- Знание основ криптографической защиты информации, существующих алгоритмов, подходящих к построению защищенных каналов связи
- Знание и опыт работы с дизассемблером, декомпилятором, отладчиком (например, Ghidra, x64dbg)
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Опыт работы с распространенными средствами криптографической защиты информации
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д. — в зависимости от отрасли и специфики компании)

08 АРХИТЕКТОР БЕЗОПАСНОСТИ

Разрабатывает комплексные системы обеспечения ИБ

Может быть специалистом: Внешним, Внутренним

Разрабатывает и контролирует внедрение организационных и технических мероприятий по обеспечению ИБ. Определяет ландшафт угроз и разрабатывает сложные архитектуры безопасности. Выступает в качестве члена комиссии безопасности, который участвует в проектах за пределами отдела безопасности (например, помогает построить систему безопасности, необходимую для пользовательского приложения, которое разрабатывает другой отдел компании). Проверяет и согласовывает технические задания, которые проектируют различные элементы корпоративной ИТ(телеой инфраструктуры).

Опыт
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Знание подходов к обеспечению безопасности ОС Windows, Linux/*nix, приложений и баз данных
- Знание технологий обеспечения ИБ (например, ПО Kaspersky) СЗИ, как аппаратных, так и отечественных
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание международных стандартов ISO/IEC 27001, ISO/IEC 27002, NIST, PCI DSS, GDPR и др.
- Знание ГОСТ Зи для возможности написания документации в соответствии с его требованиями
- Знание принципов работы и обеспечения защиты элементов ИТ-инфраструктуры
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д.)

09 МЕТОДОЛОГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Развивает и поддерживает в актуальном состоянии нормативно-методологическую документацию по ИБ

Может быть специалистом: Внешним, Внутренним

Формирует методологическую базу для развития ИБ в компании. Разрабатывает и поддерживает в актуальном состоянии документацию, определяющую подходы к обеспечению ИБ (политики, регламенты, процедуры, положения и т.д.). В связи со специфической работы должен быть погружен во все направления ИБ, реализуемые в компании.

10 СПЕЦИАЛИСТ ПО УПРАВЛЕНИЮ РИСКАМИ ИБ

Поддерживает процесс управления рисками ИБ компании

Может быть специалистом: Внешним, Внутренним

Отвечает за процесс управления рисками ИБ компании. Выявляет риски ИБ путем проведения аудита ИБ и анализа бизнес-процессов компании. Для выявленных рисков ИБ проводит их анализ и оценку для определения приоритетности и последующего ранжирования. Определяет последствия. Предлагает руководству компании адекватные и оптимальные меры защиты от критичных рисков ИБ. Выступает и поддерживает в актуальном состоянии методологическую и отчетную базу управления рисками ИБ (методологию управления рисками ИБ, реестр рисков ИБ, план обработки рисков ИБ и т. д.).

Опыт
- Знание международных стандартов моделирования угроз ИБ (ISO/IEC 27005, ISO/IEC 27001, ISO/IEC 27002, NIST 800-30 и др.)
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д.)
- Знание принципов обеспечения ИБ и управления рисками ИБ
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д.)
- Знание подходов к обеспечению ИБ

11 СПЕЦИАЛИСТ ВНУТРЕННЕЙ СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечивает безопасность внутри организации, выполняя огромный пласт работ

Может быть специалистом: Внутренним

Включает в себя множество другие специальностей, но характеризуется именно тем, что обеспечивает информационную безопасность конкретной организации или группы компаний. Может заниматься реализацией технических мероприятий, обеспечивать сетевую безопасность, администрировать СЗИ и пр.

Опыт
- Понимание их уровня архитектурования ОС Windows, Linux/*nix
- Широкий кругозор в сфере ИТ и ИБ
- Знание международных и российских стандартов моделирования угроз ИБ
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание нормативных требований к обеспечению безопасности систем защиты
- Знание СУБД (Oracle, Postgre, MS SQL)
- Знание технологий обеспечения ИБ (например, ПО Kaspersky) СЗИ, как аппаратных, так и отечественных
- Знание принципов, технологий и инструментов безопасной разработки ПО

12 АУДИТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проводит аудиты на соответствие требованиям различных стандартов и нормативно-правовых актов в сфере ИБ

Может быть специалистом: Внешним, Внутренним

Проводит аудиты персонала, ИТ-инфраструктуры, информационных систем, организационных и технических мер на соответствие требованиям стандартов и нормативно-правовых актов в сфере ИБ. По результатам аудита выявляет недостатки и разрабатывает рекомендации по их устранению. Разрабатывает методологическую базу проведения аудитов ИБ и отчетную документацию о проведенном аудитах ИБ.

Опыт
- Понимание принципов работы и обеспечения защиты элементов ИТ-инфраструктуры
- Широкий кругозор в сфере ИТ и ИБ
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д. — в зависимости от отрасли и специфики компании)
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание технологий обеспечения ИБ (например, ПО Kaspersky) СЗИ, как аппаратных, так и отечественных
- Знание международных стандартов моделирования угроз ИБ (ISO/IEC 27005, ISO/IEC 27001, ISO/IEC 27002, NIST 800-30 и др.)
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание подходов к обеспечению ИБ

13 КОНСУЛЬТАНТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Помогает заказчику в зависимости от контекста выстроить ИБ в организации или решить различные возникающие проблемы с точки зрения ИБ

Может быть специалистом: Внешним

Обладает хорошим soft скиллами и методологической базой. Выстраивает коммуникацию с заказчиком, понимает его потребности или сложности заказчика, а иногда побыть «плохой и грубим» — например, помочь подготовиться к проверке, выполнить требования регуляторов или стандартов, помочь с формированием стратегии развития ИБ на годы вперед.

Опыт
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание подходов к обеспечению безопасности ОС Windows, Linux/*nix, приложений и баз данных
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Знание международных стандартов моделирования угроз ИБ (ISO/IEC 27005, ISO/IEC 27001, ISO/IEC 27002, NIST 800-30 и др.)
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д. — в зависимости от отрасли и специфики компании)
- Знание и понимание матрицы этапа MITRE ATT&CK
- Знание принципов работы и обеспечения защиты элементов ИТ-инфраструктуры
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д.)

14 СПЕЦИАЛИСТ ПО СООТВЕТСТВИЮ НОРМАТИВНЫМ ТРЕБОВАНИЯМ

Помогает компании соблюдать законодательство, которое к ней применимо

Может быть специалистом: Внешним, Внутренним

Помогает компании обеспечить соблюдение нормативно-правовых актов (как РФ, так и зарубежных), которые к ней применимы. Проводит мониторинг изменений законодательства, оценивает их влияние на компанию и организацию. Участвует в рамках работ в модернизации ИТ-инфраструктуры или бизнес-процессов компании, которая может повлечь за собой регуляторные риски. Участвует в контрольных мероприятиях, которые проводятся со стороны регуляторов в области ИБ (ФСТЭК, ФСБ, отраслевые органы). Для ответов на запросы регуляторов ИБ и подготавливает ответы на запросы в части, касающейся выполнения требований.

Опыт
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д. — в зависимости от отрасли и специфики компании)
- Знание международных стандартов в области ИБ (ISO/IEC 27001, NIST, PCI DSS, GDPR и др.)

15 СПЕЦИАЛИСТ ПО ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ/ ПЕНТЕСТЕР

Имитирует действия злоумышленника и проверяет возможность реализации атак на приложения и ИТ-системы

Может быть специалистом: Внешним, Внутренним

Помогает бизнесу предотвращать кибератаки, проводя анализ защищенности систем компании или отдельных их элементов. Пентестер эмулирует реальные хакерские атаки, чтобы понять, насколько сложно компании противостоять злоумышленникам. Участвует в проекте по оценке эффективности SOC, чтобы проверить, насколько сложенно работает команда расследования.

Опыт
- Знание архитектуры ОС Windows, Linux/*nix, macOS, Android, iOS, структуры API указанных ОС
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Знание принципов, технологий и инструментов безопасной разработки ПО
- Знание технологий и инструментов проведения атак (например, фреймворки, сценарии сканеров, эксплоитеры уязвимостей, анализаторы кода, эксплоитеры и т.д.)
- Знание принципов и технологий обеспечения безопасности уязвимых выше ОС
- Понимание принципов работы и обеспечения защиты элементов ИТ-инфраструктуры
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание уязвимостей и способов их эксплуатации

16 ИССЛЕДОВАТЕЛЬ УЯЗВИМОСТЕЙ

Исследует элементы ИТ-инфраструктуры на наличие потенциальных уязвимостей (в том числе 0-days)

Может быть специалистом: Внешним, Внутренним

Исследует программное обеспечение (в том числе на наличие уязвимостей неуловимого дня (0-days)), компьютерные системы, базы данных, сети и другие части ИТ-инфраструктуры в поисках потенциальных уязвимостей. Проводит тестирование на проникновение, чтобы проверить, насколько они опасны. Разрабатывает отчеты о выявленных уязвимостях с детальными рекомендациями по их устранению.

Опыт
- Знание принципов и технологий обеспечения безопасности ОС Windows, Linux/*nix
- Понимание принципов работы и обеспечения защиты элементов ИТ-инфраструктуры
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание уязвимостей и способов их эксплуатации
- Знание принципов, технологий и инструментов безопасной разработки ПО
- Знание архитектуры ОС Windows, Linux/*nix, macOS, Android, iOS, структуры API указанных ОС
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Знание уязвимостей и способов их эксплуатации
- Знание подходов к обеспечению безопасности ОС Windows, Linux/*nix, приложений и баз данных
- Знание технологий и инструментов для тестирования на проникновение (сценарии сканеров, фреймворки, эксплоитеры кода, анализаторы кода)
- Знание принципов и технологий обеспечения безопасности уязвимых выше ОС
- Знание принципов работы и обеспечения защиты элементов ИТ-инфраструктуры
- Знание и понимание матрицы этапа MITRE ATT&CK

17 АРХИТЕКТОР SOC

Проектирует центры реагирования на инциденты (SOC), а также координирует процессы их создания

Может быть специалистом: Внешним, Внутренним

Обеспечивает разработку концептуальной архитектуры SOC, участвует в реализации комплексных проектов по построению/модернизации SOC. Проектирование и внедрение решений, моделирование процессов.

Опыт
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Навыки администрирования SIEM, EDR/XDR, BP/SOAR систем, TI-платформ
- Понимание и опыт решения задач проектирования и архитектурирования ИБ
- Понимание на уровне архитектурования ОС Windows, Linux/*nix
- Знание технологий обеспечения ИБ и различных классов СЗИ, как аппаратных, так и отечественных
- Понимание необходимых процессов для эффективного функционирования SOC
- Знание лучших мировых практик по созданию SOC (SANS, NFSE, FIRST и т. п.)
- Широкий кругозор в сфере ИБ и ИТ
- Навыки программирования на скриптовых языках (Python, Powershell, Bash)
- Знание подходов к обеспечению безопасности ОС Windows, Linux/*nix, приложений и баз данных

18 ИНЖЕНЕР -АНАЛИТИК SOC

Осуществляет настройку компонентов SOC

Может быть специалистом: Внешним, Внутренним

Настраивает компоненты экосистемы SOC: системы сбора и корреляции событий (SIEM) и системы реагирования на инциденты (SIR). Подключает источники сбора данных на мониторинг, разрабатывает коннекторы. Участвует в разработке правил корреляции, правил реагирования на инциденты ИБ (playbooks), настраивает в соответствии с ними СЗИ и компоненты ИТ-инфраструктуры.

Опыт
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Понимание принципов работы и обеспечения защиты элементов ИТ-инфраструктуры
- Навыки администрирования SIEM, EDR/XDR, BP/SOAR систем, TI-платформ
- Знание принципов работы и обеспечения безопасности ОС Windows, Linux/*nix, приложений и баз данных
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Знание и понимание синтаксиса, групп и нормативных особенностей вендорского ПО
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д. — в зависимости от отрасли и специфики компании)
- Знание и понимание матрицы этапа MITRE ATT&CK

19 АНАЛИТИК ЦИФРОВОЙ КРИМИНАЛИСТИКИ

Расследует киберпреступления

Может быть специалистом: Внешним, Внутренним

Осуществляет поиск и сбор информации (со сменных носителей, ОЗУ, журналов событий и т. д.), которая является доказательством совершенного преступления. Анализирует собранные доказательства киберпреступлений для составления картины происходящего инцидента.

Опыт
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание принципов, протоколов и технологий обеспечения сетевой безопасности
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Знание ОС анализов системной и сетевой памяти, сетевого трафика, журналов событий
- Знание принципов и обеспечения безопасности ОС Windows, Linux/*nix, приложений и баз данных
- Знание основ цифровой криминалистики
- Опыт работы с скриптами и платформами TI

20 АНАЛИТИК SOC 1-Й ЛИНИИ

Осуществляет базовую аналитику и классификацию инцидентов ИБ

Может быть специалистом: Внешним, Внутренним

Осуществляет мониторинг инцидентов ИБ в системах сбора и корреляции событий (SIEM) и системах реагирования на инциденты (SIR). Обрабатывает заявки в системе работы с заявками. Принимает инциденты ИБ в обработку (назначает себе заявку, берет в работу, профилирует) и выполняет первичную обработку. Осуществляет базовую аналитику и классификацию инцидентов ИБ. Формирует карточки инцидентов ИБ. Фильтрует ложные срабатывания. Эскалирует сложные инциденты 2-й линии обработки инцидентов. Предоставляет выгрузки данных из SIEM-системы по запросу 2-й линии обработки инцидентов.

Опыт
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Знание подходов к обеспечению безопасности ОС Windows, Linux/*nix, приложений и баз данных
- Базовое понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Базовые навыки по реагированию, оценке и расследованию инцидентов и работе с технологическими (требованиями) ИБ
- Понимание общих принципов реагирования на инциденты

21 АНАЛИТИК SOC 2-Й ЛИНИИ

Осуществляет глубокий анализ инцидентов ИБ, проводит расследования, оказывает постинцидентную поддержку

Может быть специалистом: Внешним, Внутренним

Работает с заявками, поступившими от 1-й линии: глубокий анализ информации из систем сбора и корреляции событий обнаружения ИТ-инцидентов (SIEM, SIR), анализ журналов регистрации событий ИТ-инфраструктуры и СЗИ, анализ сетевого трафика, анализ вредоносного ПО, расследование ИТ-инцидентов ИБ. Осуществляет постинцидентную поддержку пользователей, в том числе консультация по вопросам восстановления. Участвует в настройке систем обнаружения и предотвращения вторжений, SIEM, SIR, а также в аналитических методах для обнаружения угроз. Участвует в разработке правил корреляции событий ИБ для выявления инцидентов и атаки. Участвует в разработке правил реагирования на инциденты ИБ (playbooks). Эскалирует сложные инциденты 3-й линии обработки инцидентов. Предоставляет выгрузки данных из SIEM-системы по запросу 3-й линии обработки инцидентов.

Опыт
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Знание и понимание принципов регистрации событий СЗИ, журналов ОС, журналов приложений и баз данных
- Знание и понимание принципов работы сетевых протоколов HTTP, HTTPS, HTTA2X, DNS, и т.д.
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание подходов к обеспечению безопасности ОС Windows, Linux/*nix, приложений и баз данных
- Знание и понимание синтаксиса, групп и нормативных особенностей вендорского ПО
- Знание принципов, протоколов и технологий обеспечения сетевой безопасности
- Знание основ цифровой криминалистики
- Знание принципов работы и обеспечения защиты элементов ИТ-инфраструктуры
- Знание и понимание матрицы этапа MITRE ATT&CK
- Знание и опыт эксплуатации SIEM систем, IDP-систем

22 АНАЛИТИК SOC 3-Й ЛИНИИ

Выявляет сложные цепочки атак, проводит расследование инцидентов ИБ

Может быть специалистом: Внешним, Внутренним

Работает с заявками, поступившими от 2-й линии. Разрабатывает правила корреляции событий ИБ для выявления инцидентов и атак. Идентифицирует и приоритизирует крупномасштабные события. Проводит тонкую настройку систем мониторинга и реагирования под конкретную инфраструктуру. Ведет базу знаний, методологическую базу, отчетную и иную документацию. Участвует в совершенствовании процессов. Осуществляет проактивный поиск и обнаружение угроз. Проводит расследования инцидентов ИБ (киберрасследования). Разрабатывает правила реагирования на инциденты ИБ (playbooks).

Опыт
- Знание и опыт аналитической обработки информации из разнообразных источников
- Знание принципов, протоколов и технологий обеспечения сетевой безопасности
- Знание подходов к обеспечению безопасности ОС Windows, Linux/*nix, приложений и баз данных
- Навыки программирования на скриптовых языках (Python, Powershell, Bash)
- Широкий кругозор в сфере ИБ и ИТ
- Навыки администрирования SIEM, EDR/XDR, BP/SOAR систем, TI-платформ
- Знание сетевых технологий, основ сетевого взаимодействия и построения сетей
- Понимание на уровне архитектурования ОС Windows, Linux/*nix
- Знание технологий обеспечения ИБ (например, ПО Kaspersky) СЗИ, как аппаратных, так и отечественных
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание и понимание матрицы этапа MITRE ATT&CK
- Понимание и опыт эксплуатации СЗИ (сетевых или хостовых)

23 CISO (РУКОВОДИТЕЛЬ СЛУЖБЫ/ ДЕПАРТАМЕНТА/ОТДЕЛА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ)

Руководит внутренней службой ИБ в организации

Может быть специалистом: Внешним, Внутренним

Контролирует деятельность по ИБ в организации. В небольших организациях может быть совмещен с другими обязанностями (например, с ролью CTO). В крупных организациях может быть выстроена иерархичная структура из менеджеров среднего звена (руководителей отделов, департаментов), но курирует деятельность по ИБ как раз CISO.

Опыт
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д. — в зависимости от отрасли и специфики компании)
- Понимание принципов, протоколов и технологий обеспечения сетевой безопасности
- Знание и понимание матрицы этапа MITRE ATT&CK
- Знание международных стандартов ISO/IEC 27001, NIST, PCI DSS, GDPR и др.
- Знание технологий обеспечения ИБ (например, ПО Kaspersky) СЗИ, как аппаратных, так и отечественных
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание и понимание матрицы этапа MITRE ATT&CK
- Знание и понимание сигнатур, групп сигнатур, эвристик, баз репутации (например, ПО Kaspersky)
- Понимание современных подходов к обеспечению ИБ
- Знание и умение применять на практике методологии и инструменты управления проектами
- Широкий кругозор в сфере ИТ и ИБ
- Системное мышление, умение выстраивать отношения с командой и клиентами

24 BISO (БИЗНЕС-ПАРТНЕР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ)

Повышает согласованность кибербезопасности и бизнеса

Может быть специалистом: Внутренним

Выступает в роли директора по безопасности - переводит цели и политики центрального безопасности в конкретные практики и процедуры для бизнес-подразделений. Переводит технические риски ИБ для технических специалистов и пути разработчиков по вопросам связанным с безопасностью. Действует как заместитель директора по информационной безопасности и помогает укрепить доверие к безопасности.

Опыт
- Знание нормативно-правовых актов Российской Федерации в области ИБ и их требований (ВЗ.152, ВЗ.1-ВЗ, ВЗ.127-ФЗ, 149-ФЗ, ГОСТ 57580 и т.д.)
- Знание международных стандартов ISO/IEC 27001, NIST, PCI DSS, GDPR и др.
- Широкий кругозор в сфере ИТ и ИБ
- Понимание специфики деятельности компании, бизнес-цепей, основных бизнес-процессов компании
- Понимание современных подходов к обеспечению ИБ

25 СЕЙЛ/ПРЕСЕЙЛ -МЕНЕДЖЕР

Помогает продавать и продвигать услуги и решения по ИБ

Может быть специалистом: Внешним, Внутренним

Обладает хорошим soft скиллами, участвует в предпродажной деятельности, подготовке технико-коммерческих предложений, расчете спецификаций. Занимается консультированием менеджеров компании (Salesforce) и заказчиков по вопросам технических решений, помогает менеджерам выстраивать воронку по услуге. Занимается подготовкой технических заданий, регистрацией сделок, выстраивает взаимоотношения и плотное взаимодействие с вендорами и дистрибьюторами. Разрабатывает и реализует мероприятия по продвижению решений, проводит презентации и семинары для клиентов (заказчиков), занимается подготовкой различных маркетинговых материалов.

Опыт
- Знание потребностей рынка ИБ/ИТ
- Знание навыков и типов СЗИ и их основных принципов работы
- Знание принципов/методологии решений по ИБ
- Знание рынка ИБ/ИТ
- Знание конкурентных преимуществ аналогичных продуктов
- Знание потребностей клиентов, потребителей продукта
- Знание принципов продвижения продуктов

26 ПРЕСЕЙЛ -ИНЖЕНЕР

Помогает продавать и продвигать услуги и решения по ИБ пресейл-менеджеру

Может быть специалистом: Внешним

Занимается организацией пилотных проектов для заказчиков, демонстрацией решений по ИБ на демостенде, подготовкой технико-коммерческих предложений, разработкой ТЗ, считает спецификации на решения ИБ, помогает пресейл-менеджеру в достижении продаж.

Опыт
- Знание классов и типов СЗИ
- Знание принципов разработки ТКП(техническо-коммерческого)
- Знание порядка согласования услуг на рынке ИБ
- Знание основных методов на рынке ИБ

27 МЕНЕДЖЕР ПРОДУКТА (PRODUCT MANAGER)

Продвижение и развитие продукта/решения

Может быть специалистом: Внешним, Внутренним

Занимается разработкой стратегии продукта, продвижением продукта и ценообразованием. Анализирует рынок, формирует матрицу сравнения с конкурентами, формирует конкурентные преимущества, обучает менеджеров по продажам и пресейл-менеджеров. Определяет ЦА, сегмент, потребности, боли, возможности. Взаимодействует с командой разработки и другими смежными подразделениями, занимающимися развитием продукта.

Опыт
- Знание рынка ИБ/ИТ
- Знание конкурентных преимуществ аналогичных продуктов
- Знание потребностей клиентов, потребителей продукта
- Знание принципов продвижения продуктов

28 МЕНЕДЖЕР/ РУКОВОДИТЕЛЬ ПРОЕКТОВ ПО ИБ

Управляет проектами в области ИБ

Может быть специалистом: Внешним, Внутренним

Обеспечивает руководство проектами по оказанию услуг в области информационной безопасности. Отвечает за планирование, организацию и их выполнение проектной командой, мониторинг и управление расписанием, бюджетом, содержанием и качеством выполнения работ, контроль и управление рисками проекта.

Опыт
- Понимание современных подходов к обеспечению ИБ
- Знание и умение применять на практике методологии и инструменты управления проектами
- Широкий кругозор в сфере ИТ и ИТ
- Системное мышление, умение выстраивать отношения с командой и клиентами

29 ИНЖЕНЕР DEVSECOPS

Обеспечивает безопасность в процессе разработки ПО

Может быть специалистом: Внешним, Внутренним

Автоматизирует обеспечение информационной безопасности на всех этапах жизненного цикла разработки программных приложений. Обеспечивает безопасность при проектировании, развертывании, доставке. Контролирует, что безопасность присутствует на всех этапах жизненного цикла поставки ПО.

Опыт
- Понимание процессов CI/CD, Secure SDLC, DevSecOps
- Знание языков программирования
- Знание принципов и методологий безопасного кодирования (SANS/ CWE, OSWA, Mozilla)
- Знание уязвимостей и способов их эксплуатации
- Знание принципов и технологий обеспечения безопасности уязвимых выше ОС
- Понимание принципов работы и обеспечения защиты элементов ИТ-инфраструктуры
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание и понимание матрицы этапа MITRE ATT&CK
- Знание принципов, технологий и инструментов безопасной разработки ПО

30 SECURITY CHAMPION

Обеспечивает безопасность в процессе разработки ПО

Может быть специалистом: Внешним, Внутренним

Находится в команде разработки и заинтересован в безопасности продукта. Является единой точкой входа в команду разработки по вопросам безопасности, отвечает за использование ИБ-инструмента (SAST, DAST, IAST, SCA, etc) на всех этапах жизненного цикла разработки, обеспечивает Security Code Review и контролирует выполнение разработчиком по вопросам ИБ.

Опыт
- Знание языков программирования и их эксплуатации
- Знание архитектуры ОС Windows, Linux/*nix, macOS, Android, iOS, структуры API указанных ОС
- Знание CI/CD (Oracle, Postgre, MS SQL)
- Знание международных и российских стандартов моделирования угроз ИБ
- Знание принципов и технологий обеспечения безопасности уязвимых выше ОС
- Знание принципов и технологий обеспечения безопасности уязвимых выше ОС
- Знание технологий и инструментов для тестирования на проникновение (сценарии сканеров, фреймворки, эксплоитеры кода, анализаторы кода, эксплоитеры и т.д.)
- Знание принципов, технологий и инструментов безопасной разработки ПО
- Знание и умение применять на практике методологии и инструменты управления проектами
- Знание принципов и технологий обеспечения безопасности уязвимых выше ОС
- Понимание современных методов, инструментов и технологий проведения атак, актуальных угроз ИБ и средств защиты
- Знание и понимание матрицы этапа MITRE ATT&CK
- Знание и опыт экс