F6

Центр обучения F6

Знания, которые отражают кибератаки

Современные B2B-программы для развития компетенций по кибербезопасности

Центр обучения F6 — уникальный источник знаний в области кибербезопасности

Мы обучаем на основе реального опыта первой в России команды Incident Response. Ваши сотрудники получают не абстрактную теорию, а практические навыки, проверенные в реальных сражениях с киберугрозами

Центр обучения F6 в цифрах

>5 000

технических специалистов из разных отраслей прошли курсы F6

70%

контента каждого курса содержит практические задания, основанные на реальных кейсах

20+

лет практики и уникальной экспертизы

10+

собственных ИБ-программ, которые доказали свою эффективность для бизнеса

Выстраиваем формат обучения под ваши требования

Корпоративные группы	Создаем закрытую среду обучения, где 100% фокуса – на вашей команде и специфике отрасли
Наборные группы	Записывайте сотрудников на нужные курсы по мере необходимости
Годовые пакеты	Предсказуемый бюджет и непрерывный доступ к знаниям для всей команды
Кастомизированные программы	Создадим курс с нуля под ваш уникальный запрос (риски, инфраструктуру, задачи)
Онлайн и выездное обучение	Выбирайте удобный формат: LMS-платформа / интерактивные вебинары или очное обучение: на нашей или вашей площадке

Наши коммерческие программы

Название программы	Длительность	Чему научитесь	Для кого	Больше информации
Аналитик SOC Сложность: ★★★☆☆	3 дня 6 часов в день	Осуществлять мониторинг событий информационной безопасности, быстро выявлять угрозы и отличать реальные инциденты от ложных срабатываний	Специалисты ИБ, сотрудники SOC/CERT/ CSIRT, технические специалисты	
Реагирование на инциденты ИБ Сложность: ★★★★☆	3 дня 6 часов в день	Отрабатывать полный цикл реагирования, собирать ключевые данные, анализировать артефакты ОС Windows/Linux	Специалисты ИБ, сотрудники SOC/ CERT, технические специалисты	

Название программы	Длительность	Чему научитесь	Для кого	Больше информации
Компьютерная криминалистика и реагирование на инциденты в ОС Linux Сложность: ★★☆☆☆	2 дня 6 часов в день	Собирать данные с Linux-систем, применять методы хостовой криминалистики и анализа памяти, восстанавливать картину инцидента	Специалистов по ИБ, команды реагирования на инциденты	
Компьютерная криминалистика и реагирование на инциденты в ОС Windows Сложность: ★★★★★	5 дней 6 часов в день	Проводить криминалистический сбор данных, анализировать артефакты и дампы памяти, выявлять TTP атакующих	Специалистов по ИБ, команды реагирования на инциденты	
Сетевая криминалистика Сложность: ★★★★☆	2 дня 6 часов в день	Собирать сетевые доказательства, анализировать трафик для расследования инцидентов, применять кибер разведку	SOC-аналитики, специалисты по ИБ и компьютерной криминалистике	
Исследование атак шифроваль-щиков Сложность: ★★★★★	3 дня 6 часов в день	Проводить хостовую криминалистику, определять TTP атакующих, применять меры противодействия	Специалисты по реагированию на инциденты, аналитики вредоносного ПО, криминалисты	
Анализ данных кибер разведки Сложность: ★★☆☆☆	2 дня 6 часов в день	Анализировать отчеты об угрозах, определять ландшафт угроз, выстраивать процессы TI	Специалисты ИБ, аналитики SOC/ CERT, руководители IT-отделов	
Проактивный поиск угроз Сложность: ★★★★☆	3 дня 6 часов в день	Применять методики Threat Hunting, генерировать гипотезы, использовать MITRE ATT&CK, проводить анализ логов с помощью Sysmon и ELK	Специалисты ИБ, Threat Hunters, сотрудники SOC/CERT/CSIRT	
Исследование киберпресту-плений Сложность: ★★★☆☆	2 дня 6 часов в день	Создавать среду для расследований, собирать цифровые улики, выявлять инфраструктуру злоумышленников через OSINT	Специалисты IT и ИБ, руководители отделов	

Название программы	Длительность	Чему научитесь	Для кого	Больше информации
Разведка: основной этап в пентесте Сложность: ★★☆☆☆	3 дня 6 часов в день	Научитесь собирать и анализировать информацию о целях с помощью современных техник разведки.	Специалисты ИБ, системные администраторы, сотрудники SOC/CERT/ CSIRT	
ASM в действии: автоматзиро-ванная защита внешних сервисов Сложность: ★★★☆☆	1 день	Выявлять уязвимости внешних сервисов, применять подход Zero Trust, использовать инструменты ASM для мониторинга и защиты	Специалисты ИБ, SOC-аналитики, системные администраторы и разработчики	
Основы защиты персональных данных (ПДн) Сложность: ★★☆☆☆	2 дня 4 часа в день	Разбираться в основах ПДн, выстраивать внутренние процессы обработки ПДн в соответствии с требованиями нормативных документов	Руководители подразделений, ответственных за обработку ПДн, специалисты ИТ и ИБ, юристы, HR-менеджеры, другие специалисты, осуществляющие работу с ПДн	
Программы повышения осведомленности о киберугрозах Сложность: ★☆☆☆☆	1,5 часа	Понимать мотивы и методы киберпреступников, настраивать защиту корпоративных и личных устройств, а также предотвращать утечки информации, компрометацию учетных данных и вредоносное заражение	Сотрудники компании, чья деятельность не связана с ИБ/ИТ	
Кибербезопас-ность для топ-менеджеров Сложность: ★★☆☆☆	по запросу	Оценивать киберриски для бизнеса, формировать стратегию ИБ, принимать эффективные решения в условиях инцидента	CEO, CISO, руководители отделов	

F6

Технологии для борьбы с киберугрозами

edu@f6.ru +7 495 984-33-64 f6.ru