[Fintech 2022] Программа курса и преподаватели

Темы курса для лендинга

Название темы	Описание	предварительный преподаватель
Введение в информационную безопасность	Расскажем, зачем нужна информационная безопасность в современном мире, какие направления существуют, чем отличаются и какие проблемы решают	Kubyshko Igor
Понимание сетевой безопасности	Изучим особенности построения корпоративных сетей, основные уязвимости и вектора атак на сетевое оборудование. Рассмотрим последствия компрометации сетевой инфраструктуры компании и способы защиты	Frolov Ilya
Понимание инфраструктурной безопасности	Рассмотрим уязвимости в ОС Linux и Windows и способы их компрометации. Изучим основные методы и приемы, которые используют злоумышленники, и способы им противостоять (**Примечание**: а тема и описание это точно про одно и то же? Инфраструктурная безопасность - это не про СЗИ, zero trust, сегментирование?)	Kolenchuk Aleksey
Безопасность и атаки на приложения.	Научимся находить и эксплуатировать основные уязвимости мобильных и web-приложений.	Morozov Aleksey D.
DevSecOps	Изучим основные методики и инструменты DevSecOps. Расскажем о том, как создавать и поддерживать DevSecOps пайплайны/конвейеры с помощью SAST, DAST и SCA на базе GitLab CI.	Korovenkov Maksim
Архитектура SOC	Познакомимся с такими классами решений как: SIEM, IRP, EDR, Antivirus и Sandboxes, а также полезные для расследования логи с конечных устройств.	Merzlyakov Stanislav
Incident Response	Познакомимся с процессом реагирования на инциденты, научимся выявлять вредоносную активность и искать скомпрометированные системы в инфраструктуре.	Khandoga Georgiy
Digitat Forensic & Threat Hunting	Рассмотрим основные цифровые доказательства, научимся их анализировать. Поговорим про поиск угроз в инфраструктуре, научимся формировать и доказывать гипотезы.	Frolov Ilya
Malware analysis	Рассмотрим динамический и статический анализ зловредов, вытаскиваем индикаторы для ретроспективного поиска и блокировке на СЗИ	Kolenchuk Aleksey

Преподаватели

Name	About	
Кубышко Игорь	Руководитель "Tinkoff Security Operations Center" В Tinkoff занимаюсь организацией "SOC, выстраиванием процессов реагирования, расследования инцидентов и детектирования злоумышленников в инфраструктуре, внедрением Best Practies в области SOC.	Kubyshko Igor
Мерзляков Станислав	Архитектор в "Tinkoff Security Operations Center" Занимаюсь развитием и выявлением проблем в разрабатываемой нами SIEM системе и связанных компонентах, рисую схемы связей, анализирую перспективные технологии и практики в ИБ.	Merzlyakov Stanislav
Хамитов Александр		Khamitov Aleksandr

Коленчук Алексей	Специалист "Tinkoff Security Operations Center" Занимаюсь поддержкой и развитием SIEM системы, разрабатываю правила обнаружения, участвую в расследовании инцидентов, увлекаюсь обратной разработкой зловредов	Kolenchuk Aleksey
Хандога Георгий	Руководитель "Computer Security and Incident Response Team" В SOC Tinkoff выстраиваю процессы реагирования, создания Playbooks и их автоматизации. Участвую в обнаружении и расследовании инцидентов.	Khandoga Georgiy
Фролов Илья	Специалист "Tinkoff Security Operations Center" Занимаюсь поддержкой и развитием SIEM системы, разрабатываю правила обнаружения, участвую в расследовании инцидентов.	Frolov Ilya
Коровенков Максим	DevSecOps специалист в AppSec. Занимаюсь внедрением и развитием систем выявления проблем безопасности на ранних этапах разработки внутренних сервисов Tinkoff.	Korovenkov Maksim
Морозов Алексей	Руководитель отдела процессов AppSec. Занимаюсь внедрением и развитием процессов безопасной разработки, выявлением и устранением уязвимостей в коде.	Morozov Aleksey D.

Расписание занятий

Когда:

Как долго:

Где:

FAQ

Q: Где рассылаются организационные сообщения?

A: Главный источник

Q: А будут ли домашние задания?

A: Да, будут. Их выполнение также учитывается в финальной оценке.

Q: Требования к ПО?

A: Требования к ПО и настройкам:

Ноутбук

- RAM: 8+ GB
- HDD: 80+ GB (желательно SSD)
- ОС: Любая

ПО

- Система виртуализации Oracle Virtual Box 6.1 + Extension pack
- BurpSuite Community

Для Windows:

- Putty
- WinSCP
- plink, pagent, puttygen

Виртуальные машины:

- Kali Linux VirtualBox Images
- Windows 7
- metasploitable
- Ubuntu

Q: Где найти материалы с лекций?

A: Материалы публикуются на данной странице курса.

Обучение на курсе

После лекций вы получаете домашние задания. Их надо решать и отправлять на соответствующую страницу курса. Проверять работу будут преподаватели. Каждая из задач имеет свою максимальную оценку, получить можно от 0 до максимума. У домашних заданий есть дедлайны. После дедлайна домашние работы не принимаются.

В начале каждой лекции проводится тест по материалам прошлой лекции.

Как успешно завершить курс

- Посетить все лекции
- Сделать все домашние задания
- Ответить на все вопросы тестов после лекций

Как успешно не завершить курс

- Не посещать лекции
- Не выполнять домашние задания
- Использовать чужие решения в домашних заданиях
- Списывать у других при выполнении домашних заданий

Собеседования

В конце курса преподаватели оценивают всех студентов по ряду показателей. Часть из них, но далеко не все:

- посещения
- выполнение заданий
- активность на курсе
- полученные знания
- вовлечённость
- усердность и настойчивость в учёбе
- коммуникативные навыки
- полнота и понятность в описании решений заданий

Студенты, которые проявили себя с лучшей стороны на курсе, будут приглашены на собеседование.

Между успешным окончанием курса/набранными баллами и приглашением на интервью нет прямой зависимости.

Работа с преподавателями

Преподаватели - опытные эксперты, которые будут делиться своими знаниями, оценивать ваши и отвечать по ходу курса на вопросы и возникающие сложности. У преподавателей нет цели поставить вам низкий балл или показать, что вы ничего не знаете. Цель преподавателей - найти себе новых коллег, которые успешно вольются в коллектив Департамента Информационной безопасности Тинькофф и усилят это направление.

У каждого свой подход и свои принципы, поэтому нет универсальной формы успешного прохождения курса и получения приглашения на собеседование. Но есть общие рекомендации по учёбе:

- Не стоит перекладывать ответственность за учёбу на преподавателей. Не ждите, что они будут вместе с вами решать задачи, изучать материал, спрашивать как дела, напоминать про HW или уговаривать вас что-то сделать. Ваша учёба и ваши знания - исключительно и только ваша ответственность. Никто вам ничего не должен. Задача преподавателей - указать вектор и дать общее представление куда смотреть. Всё остальное зависит от вас.
- Преподаватели - такие же люди со своей личной жизнью и проблемами, как и вы. Не стоит ожидать, что они будут на связи 24x7 и всегда будут оперативно отвечать на все ваши вопросы. Иногда это будет не сразу или даже не на следующий день.
- Прежде чем задать вопрос, подумайте - всё ли вы сделали для того, чтобы самостоятельно на него ответить? Попробовали все возможные варианты и поискали информацию в интернете? Спросили у других студентов по курсу не сталкивались ли они с подобным или может просто знают ответ? Общение, умение находить ответы и делиться знаниями с другими - важные навыки, которым тоже нужно учиться. Не бойтесь использовать для этого курс, он для этого и предназначен 🙂 И всегда помните о главном принципе - Try Harder.
- Не откладывайте решение домашнего задания на последний день. Чем быстрее вы приступите к заданию, тем более качественным получится решение.