Compstyle
TECHNOLOGY

Программа обучения



Кибербезопасность

Blue Team

Защита, SOC и реагирование на инциденты

Splunk | Wazuh | Elastic | Wireshark | Zeek

Уровень	Программа	Формат	Занятия	Язык
С нуля	8 модулей	Онлайн	Группа или индивидуально	Азербайджанский

О курсе

Атаки происходят каждый день – разница в том, как быстро вы их замечаете. Вы изучаете повседневную работу аналитика SOC на реальных логах, алертах и сценариях инцидентов.

Для кого этот курс

01 **Новички**
Для тех, кто хочет войти в кибербезопасность со стороны защиты – с самым широким рынком труда.

02 **IT-поддержка и администраторы**
Если вы работаете в helpdesk или системным либо сетевым администратором, это самый короткий путь в SOC.

03 **Студенты**
Для тех, кто хочет ещё до диплома получить практические навыки, которые требуют вакансии аналитика SOC.

Как проходит неделя

01
Онлайн-занятие
Ментор объясняет тему в реальном времени, вопросы вы задаёте прямо на занятии.

02
Лаборатория
Ту же тему вы повторяете своими руками в лаборатории в браузере.

03
Еженедельное задание
Задание на основе реального сценария проверяет, что вы усвоили.

04
Проверка ментором
Ментор проверяет вашу работу, показывает ошибки и подсказывает следующий шаг.

Это не видеокурс: занятия проходят онлайн, вживую с ментором. В группе до 5 человек или индивидуально – ментор видит работу каждого. Обучение на азербайджанском языке.

Программа обучения

8 модулей – от основ до профессии

Каждый модуль закрепляется онлайн-занятием, лабораторией и еженедельным заданием. К следующему модулю вы переходите, когда освоили предыдущий на практике.

01

Основы безопасности и сетей

Не зная нормы, аномалию не увидеть.

OSI и TCP/IP · Основные протоколы · Межсетевые экраны и сегментация · Типы угроз

02

Логи Windows и Linux

Каждая атака оставляет след – где его искать.

Windows Event ID · Sysmon · Linux auditd · Источники логов

03

Анализ сетевого трафика

Подозрительная активность на уровне пакетов.

Wireshark · Zeek · Suricata IDS/IPS · Анализ PCAP

04

SIEM и анализ логов

Найти одну атаку среди миллионов строк.

Splunk · Wazuh · Поисковые запросы · Правила корреляции

05

EDR и расследование на конечных точках

Что произошло внутри компьютера.

Алерты EDR · Дерево процессов · Velociraptor · Признаки вредоносного ПО

06

Threat intelligence и MITRE ATT&CK

Распознавать тактику атакующего.

MITRE ATT&CK · IOC и IOA · Источники CTI · Картирование атаки

07

Реагирование на инциденты

От алерта до закрытого инцидента.

Этапы IR · Изоляция и устранение · Основы форензики · Отчёт об инциденте

08

Threat hunting и рабочий процесс SOC

Искать угрозы, не дожидаясь алерта.

Поиск на основе гипотез · Триаж · Эскалация · Подготовка к собеседованию

По итогам курса вы сможете

- Проводить триаж алертов как аналитик SOC L1
- Писать поисковые запросы и правила корреляции в SIEM
- Находить подозрительную активность в сетевом трафике и логах
- Картировать атаку по MITRE ATT&CK
- Действовать пошагово по плану реагирования на инциденты
- Писать отчёт об инциденте для руководства

Инструменты, с которыми вы будете работать

Splunk · Wazuh · Elastic · Wireshark · Zeek · Suricata · Sysmon · Velociraptor · MITRE ATT&CK · CyberChef

Где работают наши выпускники

Kapital Bank · Rabitəbank · birmarket · RISK COMPANY · BMU Bakı Mühəndislik Universiteti · AZTU

Следующий шаг

Приходите на бесплатный онлайн-урок – познакомьтесь с ментором, а потом решайте.

Группа или индивидуально - выбор за вами. Цену, расписание и дату старта следующей группы пришлём в WhatsApp. Обучение на азербайджанском языке.

WhatsApp и звонки	+994 70 639 33 09
Сайт	compstyle.tech/ru/kursy/blue-team
Instagram	@compstyle.az
Telegram	@compstylekanal
YouTube	@Compstyle



Compstyle TECHNOLOGY

Учись сам, создавай сам.

© Compstyle Technology