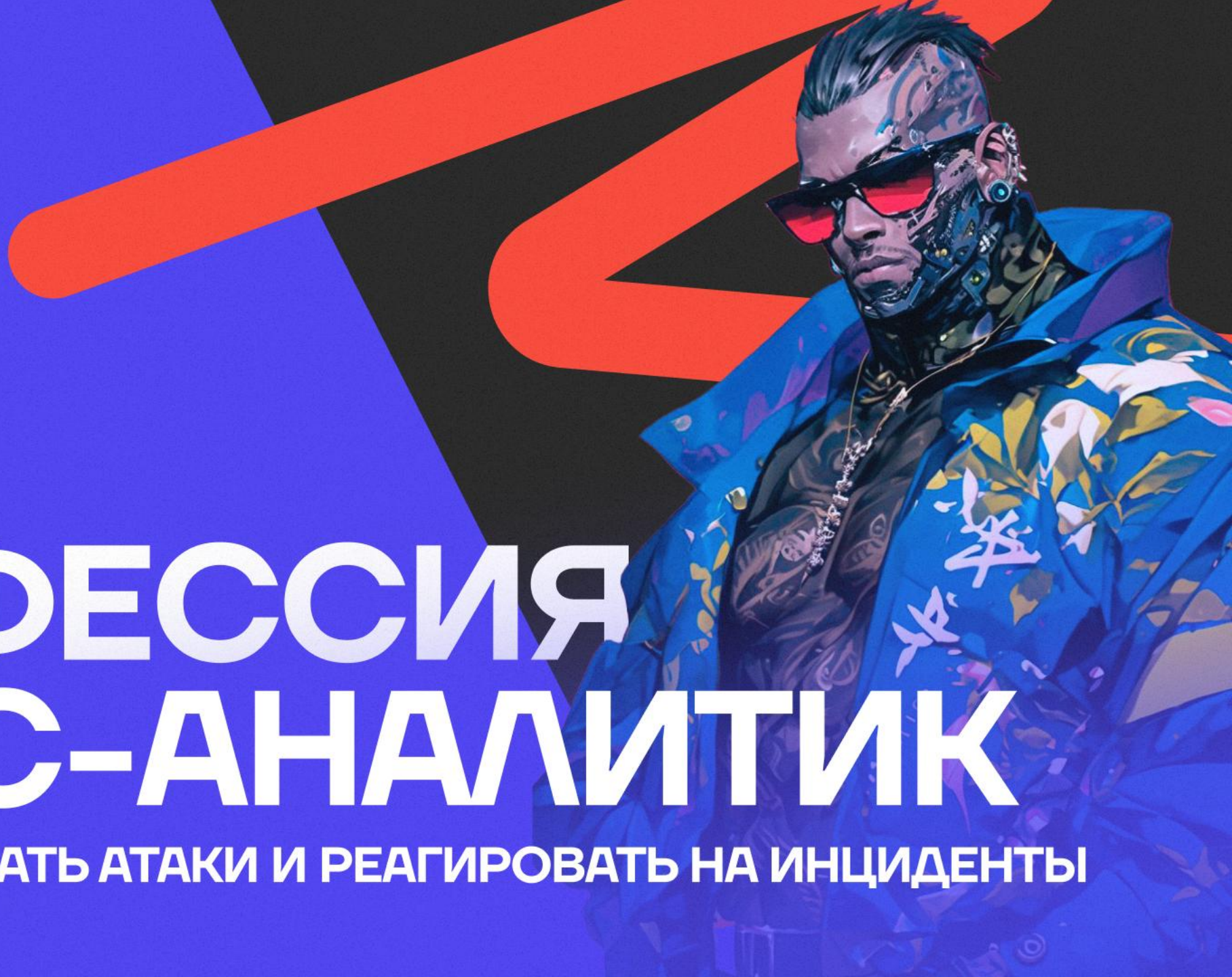


[ВЕБИНАР]

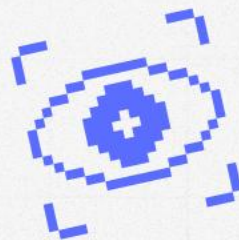
CyberED

ПРОФЕССИЯ [🔍] SOC-АНАЛИТИК

КАК ОБНАРУЖИВАТЬ АТАКИ И РЕАГИРОВАТЬ НА ИНЦИДЕНТЫ



[О СПИКЕРЕ]



CyberED

БУРЦЕВ ВЛАД

ТЕКУЩАЯ ДОЛЖНОСТЬ И МЕСТО РАБОТЫ
РУКОВОДИТЕЛЬ ОТДЕЛА АНАЛИЗА КИБЕРУГРОЗ В BI.ZONE



КЛЮЧЕВЫЕ НАВЫКИ:

АДМИНИСТРИРОВАНИЕ WINDOWS ИНФРАСТРУКТУРЫ
НАПИСАНИЕ ДЕТЕКТИРУЮЩИХ ПРАВИЛ SIEM
СИСТЕМНОЕ ПРОГРАММИРОВАНИЕ
РЕВЕРС ИНЖИНЕРИНГ



ДАВАЙТЕ ПОЗНАКОМИМСЯ

А)

ОТМЕТЬТЕ, КТО ВЫ
И ОТКУДА ПРИШЛИ:

- 01 Новичок: без ИТ / ИБ бэкграунда
- 02 Новичок с ИТ-бэкграундом
- 03 Работаю в ИТ
- 04 Работаю в ИБ

Б)

КАКИЕ У ВАС ЦЕЛИ
НА ВСТРЕЧУ?

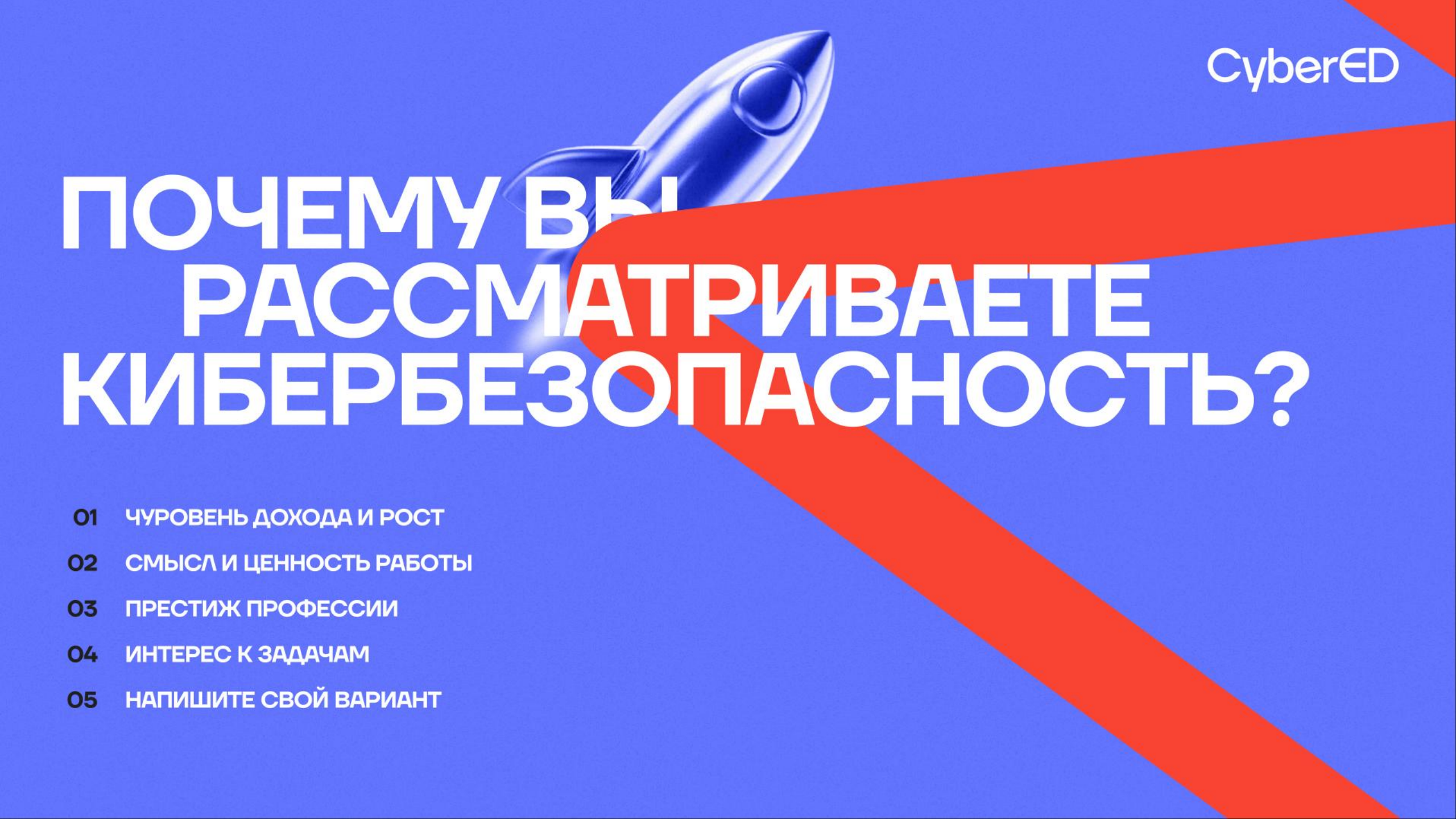


ДАВАЙТЕ ПОЗНАКОМИМСЯ

В)

**ЧТО ВАС БОЛЬШЕ ВСЕГО
НАСТОРАЖИВАЕТ / ОСТАНАВЛИВАЕТ
В ВЫБОРЕ НАПРАВЛЕНИЯ?**





ПОЧЕМУ ВЫ РАССМАТРИВАЕТЕ КИБЕРБЕЗОПАСНОСТЬ?

- 01 ЧУРОВЕНЬ ДОХОДА И РОСТ
- 02 СМЫСЛ И ЦЕННОСТЬ РАБОТЫ
- 03 ПРЕСТИЖ ПРОФЕССИИ
- 04 ИНТЕРЕС К ЗАДАЧАМ
- 05 НАПИШИТЕ СВОЙ ВАРИАНТ

КАРТА НАПРАВЛЕНИЙ

[В КИБЕРБЕЗОПАСНОСТИ]



BLUE TEAM

Защита систем от атак, мониторинг и реагирование на инциденты.

■ Тип мышления:
аналитический, с фокусом на расследование.

■ Верхние роли:

Аналитик SOC

Incident Responder / DFIR

Аналитик киберугроз

Аналитик BPO

INFRA SEC

Обеспечение безопасности IT-инфраструктуры, включая сети, серверы и операционные системы.

■ Тип мышления:
технический, системный.

■ Верхние роли:

Инженер по безопасности инфраструктуры

Сетевой инженер безопасности



Кибербезопасность —
это не набор направлений.

Это цикл защиты, в котором у каждой роли есть своё место и своя функция. Вам важно понять, какие проблемы/боли вам интереснее решать.

APP SEC

Безопасная разработка и тестирование приложений.

■ Тип мышления:
креативный и технический, с акцентом на анализ кода.

■ Верхние роли:

AppSec-инженер

Специалист по анализу кода

Аналитик по безопасности приложений

DevSecOps

RED TEAM

Имитация кибератак для тестирования систем на проникновение и оценки уязвимостей.

■ Тип мышления:
творческий, наступательный.

■ Верхние роли:

Внешний пентест

Red Teaming

Внутренний пентест

Исследование уязвимостей

GRC / ARCH

Проектирование архитектуры безопасности, управление рисками и обеспечение соответствия нормам.

■ Тип мышления:
стратегический, управленческий.

■ Верхние роли:

Управление рисками

Архитектор безопасности

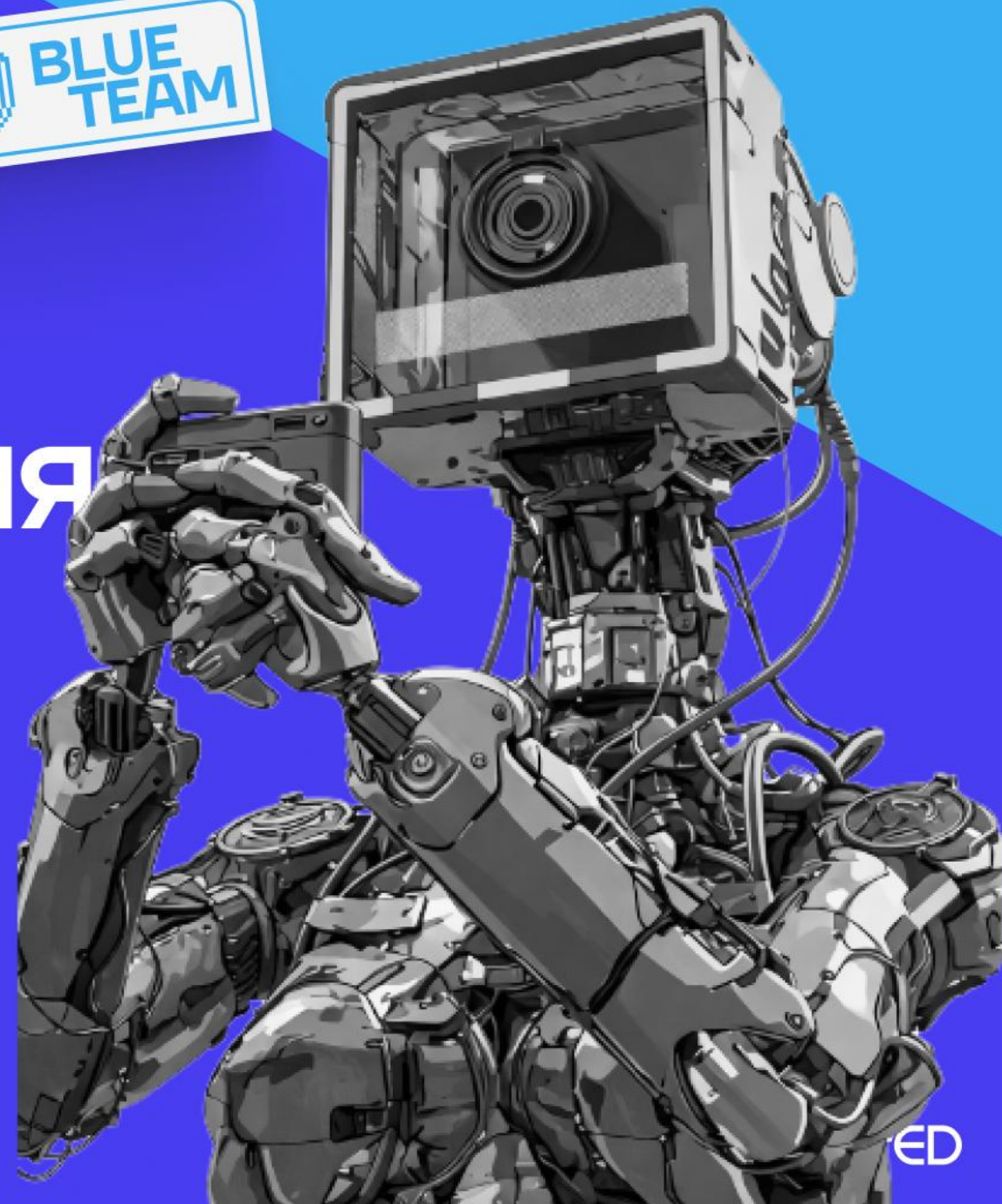
Безопасность поставщиков

Аудитор



АНАЛИТИК ЦЕНТРА ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ

[АНАЛИТИК SOC]



КАКИЕ БЫВАЮТ ВИДЫ АНАЛИТИКОВ SOC

ПОЗИЦИЯ:
SOC L1

Аналитик
первого уровня,
начинающий SOC

Что делает:

Смотрит на сигналы системы безопасности. Решает это реальная угроза или ложная тревога. Если непонятно — передаёт дальше.

ПОЗИЦИЯ:
SOC L2

Аналитик
второго уровня

Что делает:

Разбирается в подозрительных ситуациях. Смотрит логи, поведение, помогает понять: что произошло, кто виноват.

ПОЗИЦИЯ:
SOC L3

Старший аналитик /
эксперт

Что делает:

Работает со сложными атаками. Ищет улики, проверяет память и файлы, помогает настраивать защиту. Иногда участвует в расследованиях.

[АНАЛИТИК SOC_L1]

ПРИМЕРЫ ЗАДАЧ

01

Просматривать сигналы системы безопасности и понимать, есть ли реальная угроза

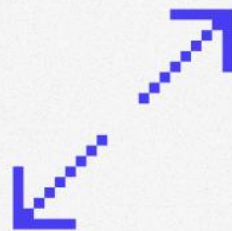
02

Отсеивать ложные тревоги, когда система «паникует зря»

03

Передавать серьёзные инциденты дальше, если нужна более глубокая проверка или срочные действия

ПРИМЕРЫ ЗАДАЧ



Расследование переданного инцидента:



- анализ цепочек процессов на конечных точках, поиск аномалий;
- изучение логов сетевых устройств для определения полного масштаба атаки

Сдерживание угрозы:



Просматривать сигналы системы безопасности и понимать, есть ли реальная угроза

[АНАЛИТИК SOC_L3]

ПРИМЕРЫ ЗАДАЧ

01

Создание новых
корреляционных правил

02

Написание скриптов
для автоматизации
расследований или
сбора данных

03

Расследование сложных
инцидентов; моделирование
инцидентов

КОМБИНАЦИЯ ИНСТРУМЕНТОВ

[✓] [ОПРЕДЕЛЯЮЩИХ СПЕЦИАЛИСТА]

01



ФОРЕНЗИКА:

IDA Pro, Ghidra, Rekall, Volatility, KAPE, Redline.

02



АНАЛИЗ ВРЕДОНОСНОГО ПО:

Capa, YARA, Sysmon, PESTudio.

03



THREAT HUNTING:

Elastic/Kibana Query Language, Splunk SPL высокого уровня, Osquery, Sysmon, Falco.

04



ДЕТЕКТ-ИНЖЕНЕРИЯ:

Sigma, Suricata/Snort, ATT&CK Navigator, Atomic Red Team, Malcolm, Maltrail.

05



АРХИТЕКТУРА МОНИТОРИНГА:

EDR/XDR/NDR (CrowdStrike, SentinelOne, Defender, Corelight).

06



УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ:

Nessus, Qualys, OpenVAS.

[АНАЛИТИК SOC_L1-L3]

ЧТО НРАВИТСЯ + + + + +

01 Быстрый рост экспертизы
Ты видишь настоящие атаки,
а не теорию.

02 Сильный фундамент
для любой роли в ИБ

Аналитики SOC становятся лучшими:

- Threat Hunters
- Malware Analysts
- Security Engineers
- Архитекторами
- CISO

Потому что они понимают, как атака выглядит изнутри.

03 Много вариантов развития
дальше (15+ направлений).

04 Большая востребованность
на рынке (в России и мире)

SOC — один из самых стабильных треков:

высокий спрос

рост зарплат

релокационная устойчивость

огромный рынок MSSP и корпоративных SOC

05 Возможность работать в крупном
бизнесе и больших командах SOC есть у:

- банков
- телекома
- госкорпораций
- крупного retail и e-commerce
- международных компаний

[АНАЛИТИК SOC_L1-L3]

ЧТО БЕСИТ



01 **Высокий уровень стресса и ответственность за инциденты**

02 **Рутинные задачи на младших уровнях (особенно L1)**

L1 часто делает:

- быстрая первичная проверка
- фильтрацию ложных срабатываний
- базовые расследования

03 **Неудобные графики: ночные смены, дежурства, 24/7 (часто, но не всегда)**

04 **Требуется быстрое принятие решений при неполной информации**

05 **Комбинация факторов:**

Стресс + рутинность + ночи + ответственность + информационный поток

[АНАЛИТИК SOC]

ОТРАСЛИ, ГДЕ ВОСТРЕБОВАНЫ



ФИНАНСЫ

банки, финтех, платежные
системы, страхование



ГОСУДАРСТВЕННЫЙ СЕКТОР

госкорпорации, органы
власти, КИИ



ТЕЛЕКОММУНИКАЦИИ И IT

операторы связи, крупные
IT-компании.

БЕЗ РОЗОВЫХ ОЧКОВ

[РЕАЛЬНОСТЬ ПРОФЕССИИ]

➤ Рынок ждёт не мотивацию, а **доказуемые навыки**

+ Конкуренция **выросла**

+ Инструменты **не заменяют** мышление

+ Ложные срабатывания — **часть работы**

+ Отчёты и коммуникация **обязательны**

+ **Требуется** системность и спокойствие

+ Без сетей, ОС, логов и базовой инфраструктуры **будет тяжело**

+ Нужно понимать не только защитные инструменты, но и **действия атакующих**

СХОЖИЕ ПРОФЕССИИ,

→ КОТОРЫЕ ПОМОГАЮТ ПЕРЕЙТИ SOC

- Системный администратор (Linux/Windows)
- Сетевой инженер
- Аналитик уязвимостей (Vulnerability Assessment Analyst)
- Специалист по инфраструктуре
- DevOps / Cloud-инженер

SOC
АНАЛИТИК



Но студентами курса становятся и те, кто не имеет опыт работы в ИТ; важно соответствовать базовым требованиям входа на курс.

ТРЕБОВАНИЯ РАБОТОДАТЕЛЕЙ

[L1] Знать теорию и базовые инструменты.

➤ Сети:

- TCP/IP, OSI, DNS, DHCP, HTTP/HTTPS
- NAT, Proxy, Firewall
- (ИБ): Атаки (ARP Spoofing, SYN flood) и защита

➤ Windows:

- AD, группы/GPO
- Event IDs: 4624, 4625, 4688
- (ИБ): Атаки (Pass-the-Hash, Golden Ticket)

➤ Linux:

- Права 777/755, пользователи
- Команды: grep, tail, ps, netstat, ss
- Логи: /var/log

➤ Логи и ИБ:

- Чтение, фильтрация, поиск аномалий
- MITRE ATT&CK (знать тактики/техники)
- Виды ВПО (трояны, шифровальщики)

ИНСТРУМЕНТЫ И ОБЯЗАННОСТИ

[L1]

Работа руками в мониторинге 24/7; Первичное реагирование;
Эскалация на L2; Написание простых правил / исключений

➤ **СЗИ (классы):**

AV, EDR, WAF, NTA, Sandbox, DLP, IDS/IPS

➤ **Опыт работы (SIEM):**

QRadar, Splunk, ELK, KUMA, MaxPatrol

➤ **Выделяет из толпы (бонус):**

SQL, Regex (\d{1,3}\.\d{1,3}); Wireshark, Sysmon; TryHackMe / HTB, CTF

Зарплатная вилка в РФ: 60 000 – 130 000 ₽



ТРЕБОВАНИЯ РАБОТОДАТЕЛЕЙ

[L2] Расследовать, писать правила и копать глубже.

- Нужно знать всё, что для L1, но глубже (Kerberos, глубокие логи)
- MITRE: Понимать как техника выглядит в логах (Source: Sysmon, EDR)
- Память и диски: анализ дампа RAM, триаж диска
- Скрипты:
 - Bash / PowerShell (обязательно)
 - Python (большой плюс)
- Трафик: профессиональный анализ (Wireshark/tcpdump)
- Процессы:
 - Threat Hunting (базово)
 - Threat Intelligence (базово)
- Правила: Yara / Sigma

ИНСТРУМЕНТЫ И ОБЯЗАННОСТИ

[L2] Закрывать сложные инциденты и развивать SOC.

► **Обязанности L2:**

Эскалация от L1: Написание детектирующей логики (Content Development) :
Расследование инцидентов (IR); Наставничество L1: Скрипты автоматизации;
Обогащение Wiki / базы знаний

► **Софт-скиллы (критичны)::**

- Аналитическое мышление\$ Дотошность / Внимательность\$
Коммуникабельность (общение с заказчиком); Готовность работать в
особом режиме в случае инцидентов

Зарплатная вилка в РФ: 150 000 – 250 000 ₽



[АНАЛИТИК SOC]

ЗАРПЛАТА

СТАРТ L1	L2	L3	АРХИТЕКТОР	LEAD/CISO	МЕЖДУНАРОД. УРОВЕНЬ
0-1 года	1-1,5 года	2-4 лет	5+лет	600 ТЫС. -1,2 МЛН	500 ТЫС -1,2 МЛН
60-90 ТЫС.	130 -150 ТЫС.	150-350 ТЫС.	350-600 ТЫС.		

ВАРИАНТЫ ДОП. ДОХОДА:

- 01 Разовые расследования инцидентов
- 02 Подработка в ночные/выходные смены
- 03 Консультации по построению SOC, обучение.

[АНАЛИТИК SOC] [ВОЗМОЖНЫЕ ТРАЕКТОРИИ РАЗВИТИЯ]



SOC — это самый понятный и доступный вход в ИБ, который быстро открывает путь в расследование, хантинг, инженерию и архитектуру защиты

[АНАЛИТИК SOC]

ЭТА СПЕЦИАЛЬНОСТЬ ДЛЯ ВАС, ЕСЛИ



Хотите видеть кибератаки в реальном времени и быть на передовой обороны.



Готовы к работе в команде 24/7 и несете ответственность за результат.



Умеете работать в условиях неполной информации и быстро принимать решения.



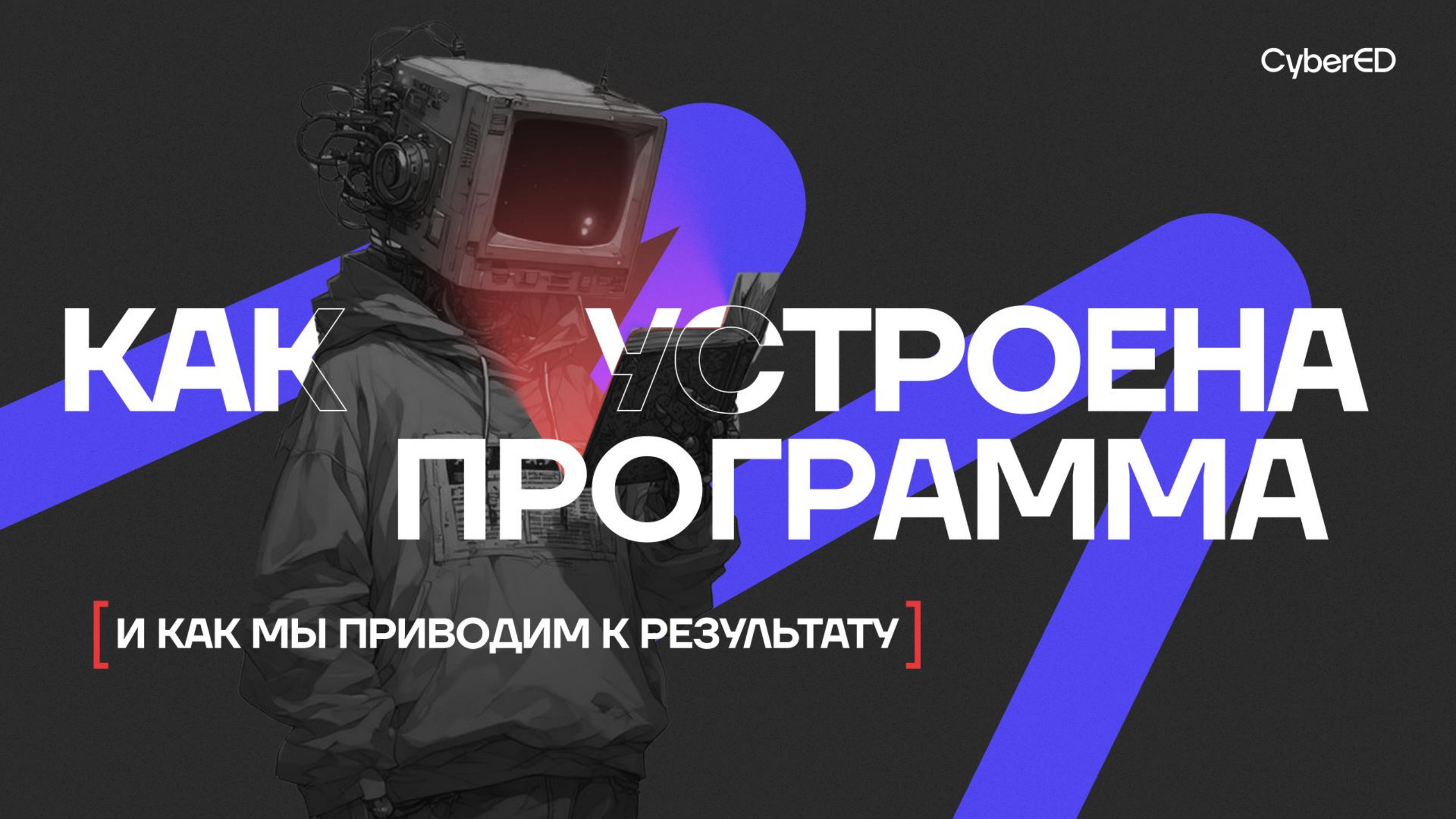
Обладаете аналитическим складом ума и любите разбираться в причинах событий.



Видите себя в будущем экспертом в области расследования инцидентов или хантинга угроз

ДАВАЙТЕ РАЗБЕРЕМ
ВАШИ 
ВОПРОСЫ





КАК УСТРОЕНА ПРОГРАММА

[И КАК МЫ ПРИВОДИМ К РЕЗУЛЬТАТУ]

АНАЛИТИК ЦЕНТРА ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ [В301]

- 🎯 35 КОМПЕТЕНЦИЙ
- 📖 ПОЛНАЯ КАРТА НАВЫКОВ ПРОФЕССИИ
- 📁 5 МОДУЛЕЙ
- 📅 365 ДНЕЙ ДОСТУПА
- 🧩 40+ ЗАДАНИЙ
- 👤 3 КАРЬЕРНЫЕ ВСТРЕЧИ

КУРС БУДЕТ ПОЛЕЗЕН:

- СИСТЕМНЫМ АДМИНИСТРАТОРАМ И СЕТЕВЫМ ИНЖЕНЕРАМ
- СПЕЦИАЛИСТАМ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
- SOC-АНАЛИТИКАМ 1/2 ЛИНИИ
- DEVOPS-ИНЖЕНЕРАМ
- СТУДЕНТАМ СТАРШИХ КУРСОВ И ВЫПУСКНИКАМ НАПРАВЛЕНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ ПРОГРАММЫ:

- ОБНАРУЖЕНИЕ АТАК НА ВНЕШНЕМ ПЕРИМЕТРЕ
- ОБНАРУЖЕНИЕ АТАК ВО ВНУТРЕННЕЙ СЕТИ
- ОБНАРУЖЕНИЕ АТАК В КРИТИЧЕСКИ ВАЖНЫХ СЕГМЕНТАХ
- РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ
- НАСТРОЙКА ЗАЩИТЫ
- АНАЛИЗ ИНФРАСТРУКТУРНЫХ УЯЗВИМОСТЕЙ
- ТЕХНИКИ АТАК ХАКЕРА С РАЗБОРОМ ПРИМЕРОВ

HARD SKILLS, ФОРМИРУЕМЫЕ В ХОДЕ ПРОГРАММЫ



ВНЕШНИЙ ПЕРИМЕТР И ВЕБ-АТАКИ

- Выявление сканирования инфраструктуры
- Обнаружение фаззинга и подбора директорий
- Детектирование SQL Injection
- Детектирование XSS и CSRF
- Выявление обхода авторизации
- Обнаружение Path Traversal
- Выявление брутфорса веб-ресурсов
- Обнаружение фишинговых атак



WINDOWS / LINUX И ВНУТРЕННИЕ СЕТИ

- Выявление вредоносной активности на хостах
- Анализ аномального поведения процессов
- Обнаружение эксплуатации уязвимостей
- Выявление доступа к SAM и LSASS
- Детектирование внутреннего сканирования
- Обнаружение закрепления в Windows и Linux



ACTIVE DIRECTORY И ДОМЕННАЯ ИНФРАСТРУКТУРА

- Обнаружение разведки Active Directory
- Выявление перемещения внутри инфраструктуры
- Детектирование Password Spraying и Brute Force
- Контроль Kerberos TGT
- Выявление Pass-the-Ticket и Pass-the-Hash
- Детектирование Kerberos-атак
- Обнаружение атак на AD CS
- Детектирование DCSync и DCShadow



БЕСПРОВОДНЫЕ СЕТИ

- Выявление атак на Wi-Fi инфраструктуру
- Детектирование прослушивания трафика
- Обнаружение MAC Spoofing
- Детектирование Deauthentication Attack
- Выявление Evil Twin
- Обнаружение подбора паролей Wi-Fi

ПРАКТИЧЕСКАЯ РАБОТА С ИНСТРУМЕНТАМИ



Elastic SIEM



Wireshark



Suricata



Sysmon



Windows Event Viewer



Process Monitor



Nmap



Dirsearch



Kismet



Aircrack-ng



MitmAP



Autoruns

[КАК МЫ ДОВОДИМ ТЕМУ]

ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

Формат: асинхрон + live разбор 🔴



ПРОХОДИШЬ ТЕОРИЮ САМ

+ разбираешь с наставником



ВСТРЕЧА С ЭКСПЕРТОМ

- + ответы на вопросы по практике
- + углубление
- + дополнительные техники

Формат помогает понять материал и сформировать навык, а **не** просто посмотреть материал.

ЭТО **НЕ**

«ПОСМОТРЕЛ И ПОШЁЛ ДАЛЬШЕ»

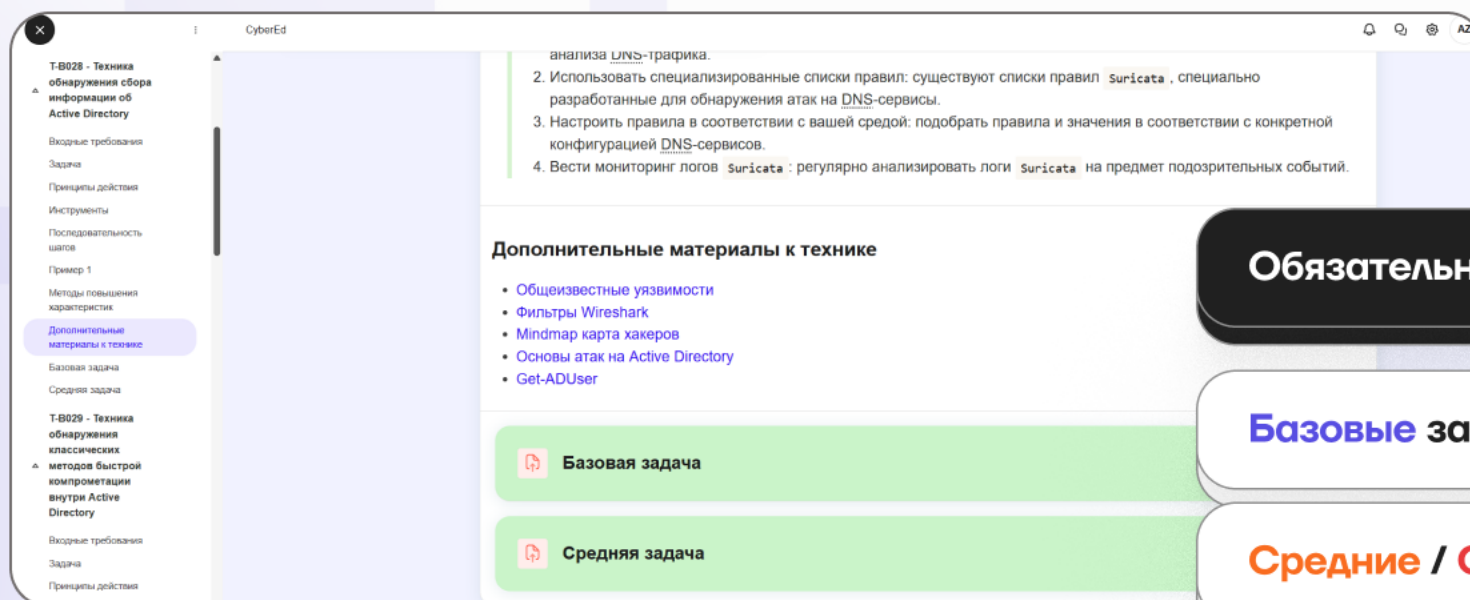
ЭТО

«РАЗОБРАЛ, ДОКРУТИЛ, ПОНЯЛ, ГДЕ **ОШИБСЯ**»

[КАК МЫ ДОВОДИМ ТЕМУ]

ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

ПРОГРАММУ МОЖНО ОСВАИВАТЬ
ДО УРОВНЯ **СЛОЖНОСТИ**,
→ КОТОРЫЙ ПОТЯНЕШЬ



■ Встроенная система давления на результат → Нельзя «проскочить»

Обязательная база → Добровольный рост

Базовые задачи — обязательны (иначе нет сертификата)

Средние / Сложные — для прокачки уровня

Карта компетенций

🔗 Поделиться

Аналитик Центра противодействия кибератакам

Аналитик SOC. Демо-курс 29 / 100

Обнаружение агрессивного на стадии
работы с периметром 9 / 80

Пентестер (Penetration Testing Specialist)

Цели исследования 0 / 0

Атаки в локальных сетях 0 / 0

Получение первичного доступа через
механизм аутентификации 0 / 0

Общие показатели по направлениям



35%

Red



66%

Blue



24%

AppSec



24%

Fundamentals

Модуль: Не выбрано ▾

🔍 Скрыть неосвоенные

Аналитик SOC. Демо-курс

R301 - M0A

Техника обнаружения аномальных активностей в
логировании сетевых устройств и рабочих станций через
аппаратные средства

Базовый 3/3 Средний 3/3 Продвинутый 3/3

R301 - M0A

Форензика

Базовый 3/3 Средний 3/3 Продвинутый 3/3

R301 - M0A

Аудит безопасности

Базовый 3/3 Средний 3/3 Продвинутый 3/3

КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ

КАЖДАЯ ЗАДАЧА → ЗАКРЫВАЕТ НАВЫК

УРОВЕНЬ: **БАЗОВЫЙ** / **СРЕДНИЙ** / **СЛОЖНЫЙ**Видно, что ты
реально умеешьНе «написал в CV»
а подтвердил

Карта компетенций

🔗 Поделиться

Аналитик Центра противодействия кибератакам

Аналитик SOC. Демо-курс 29 / 100

Обнаружение агрессивного на стадии
работы с периметром 9 / 80

Пентестер (Penetration Testing Specialist)

Цели исследования 0 / 0

Атаки в локальных сетях 0 / 0

Получение первичного доступа через
механизм аутентификации 0 / 0

Общие показатели по направлениям



35%

Red



66%

Blue



24%

AppSec



24%

Fundamentals

Модуль: Не выбрано ▾

🔍 Скрыть неосвоенные

Аналитик SOC. Демо-курс

R301 - MOA

Техника обнаружения аномальных активностей в
логировании сетевых устройств и рабочих станций через
Базовый 3/3 Средний 3/3 Продвинутый 3/3

R301 - MOA

Форензика

Базовый 3/3 Средний 3/3 Продвинутый 3/3

R301 - MOA

Аудит безопасности

Базовый 3/3 Средний 3/3 Продвинутый 3/3

КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ ПУБЛИЧНЫЙ ПРОФИЛЬ

МОЖНО ОТКРЫТЬ ССЫЛКУ / ПОКАЗАТЬ НАВЫКИ РАБОТОДАТЕЛЮ

■ Это уже не обучение,
это **переход к найму**

ПРЕИМУЩЕСТВА НАШЕЙ ПРОГРАММЫ

ТИПИЧНЫЙ ПОДХОД



Работа с алертами SIEM



Следование плейбукам



Анализ известных индикаторов



Базовые техники атак



Реакция на уже обнаруженные события

НАШ ПОДХОД



Понимание логики атакующего



Практика против реальных техник



Воспроизведение атак своими руками



Анализ поведения вместо сигнатур



Поиск решений вне шаблонов

ЧТО ПОЛУЧАЕТ СПЕЦИАЛИСТ:



Сетевые атаки



Фишинг



Kerberos



AD CS



DCSync /
DCShadow



Wi-Fi атаки



Обход MFA



Повышение
привилегий



Закрепление в
инфраструктуре



ОТЗЫВЫ

[В301] ПО ПРОГРАММЕ

Владимир, 43, отдел системного администрирования

Прошел курс «Аналитик Центра противодействия кибератакам (SOC Analyst)» на платформе CyberEd. Программа обучения продумана и структурирована, сочетает в себе теоретическую базу и практические задания, направленные на развитие прикладных навыков по анализу и реагированию на инциденты информационной безопасности.

В процессе обучения получил новые знания по принципам работы SOC, методам расследования кибератак и использованию современных инструментов мониторинга. Полученные компетенции уже применяю в практике работы руководителя отдела системного администрирования.

Отдельно отмечу высокий профессиональный уровень преподавателей и актуальность учебных материалов. Курс будет полезен не только специалистам в области информационной безопасности, но и ИТ-профессионалам различных направлений — системным администраторам, сетевым инженерам и другим специалистам, заинтересованным в расширении своих знаний в сфере кибербезопасности.

Рекомендую данный курс всем, кто стремится повысить квалификацию и укрепить компетенции в области защиты информационных систем.

Евгений, 48 лет, ИБ

Прошел курс «Аналитик Центра противодействия кибератакам (SOC Analyst)» на платформе CyberEd. Программа обучения продумана и структурирована, сочетает в себе теоретическую базу и практические задания, направленные на развитие прикладных навыков по анализу и реагированию на инциденты информационной безопасности.

В процессе обучения получил новые знания по принципам работы SOC, методам расследования кибератак и использованию современных инструментов мониторинга. Полученные компетенции уже применяю в практике работы руководителя отдела системного администрирования.

Отдельно отмечу высокий профессиональный уровень преподавателей и актуальность учебных материалов. Курс будет полезен не только специалистам в области информационной безопасности, но и ИТ-профессионалам различных направлений — системным администраторам, сетевым инженерам и другим специалистам, заинтересованным в расширении своих знаний в сфере кибербезопасности.

Рекомендую данный курс всем, кто стремится повысить квалификацию и укрепить компетенции в области защиты информационных систем.

[НОВИНКА]

AI ДЛЯ SOC АНАЛИТИКОВ

НОВЫЙ МИНИ-КУРС В
РАМКАХ ПРОГРАММЫ

ПРАКТИЧЕСКИЕ
ВОРКШОПЫ

- 01 Практические сценарии применения AI в работе SOC-аналитиков
- 02 Автоматизация рутинных задач и снижение нагрузки на L1
- 03 Ускорение анализа инцидентов и обработки событий безопасности
- 04 Ограничения, риски и сложности внедрения AI в процессы SOC
- 05 Воркшопы и разбор реальных кейсов применения AI



НАЧНИ УЧИТЬСЯ И ПОЛУЧИ ДОПОЛНИТЕЛЬНЫЕ ТЕХНИКИ В ПОДАРОК

CyberED

Red Team-направление

Изучишь техники атак глазами злоумышленника, чтобы лучше распознавать их признаки, понимать логику развития атаки и эффективнее расследовать инциденты.

- «Исследование целей тестирования»
- «Получение первичного доступа через атаки на аутентификацию»
- «Получение первичного доступа через атаки на веб-приложения»
- «Получение первичного доступа через атаки социальной инженерии»
- «Эксплуатация известных уязвимостей»
- «Повышение привилегий в Linux»
- «Повышение привилегий в контейнерных средах»
- «Повышение привилегий в Windows»
- «Проброс сетевого трафика (Pivoting)»
- «Атаки на локальные сети»
- «Атаки на Active Directory»
- DETA "Оценка устойчивости средств защиты" (совместно с Егором Зайцевым)

Фундаментальное направление

Закроешь пробелы в базовых знаниях об инфраструктуре, операционных системах, сетях и средствах защиты, необходимых для полноценного анализа событий и расследования инцидентов.

- Основы. Введение в информационную безопасность»
- «Операционная система Linux»
- «Локальные сети»
- «Доменная структура Windows»
- «Администрирование СЗИ»

[ДЛ Я УЧАСТНИКОВ ВЕБИНАРА]

ТОЛЬКО ДО 21 ИЮНЯ



Аналитик SOC + Мини-курс «ИИ для SOC»

Обычная цена 153 900 Р

за 130 000 рублей Скидка 15%

Аналитик SOC + Мини-курс «ИИ для SOC» + Дополнительный курс на выбор

Обычная цена 183 900 Р

за 145 000 рублей Скидка 20%

Аналитик SOC + Мини-курс «ИИ для SOC» + Treat Intelligence

Обычная цена 205 800 Р

за 165 000 рублей Скидка 20%

