

CyberED

# СПЕЦИАЛИСТ ПО ЗАЩИТЕ КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЫ

[ КАК ВОЙТИ В BLUE TEAM БЕЗ РОЗОВЫХ ОЧКОВ: ОТ СЕТЕЙ И WINDOWS ДО SOC,  
РЕАГИРОВАНИЯ И АРХИТЕКТУРЫ ЗАЩИТЫ ]

[ СПИКЕР ]

CyberED

# СЕРГЕЙ СИДОРИН

РУКОВОДИТЕЛЬ НАПРАВЛЕНИЯ МОНИТОРИНГА И  
РЕАГИРОВАНИЯ В КОМПАНИИ **ИНФОРМЗАЩИТА**

■ Образование:

МАИ (НИУ) — ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ  
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ (2020)

МАИ (НИУ) — КИБЕРБЕЗОПАСНОСТЬ (2022)

■ Ключевые навыки:

МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ  
НАСТРОЙКА СЗИ И SIEM-СИСТЕМ (НАПИСАНИЕ ПРАВИЛ КОРРЕЛЯЦИИ)  
АДМИНИСТРИРОВАНИЕ WINDOWS И СЕТЕЙ  
ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ (PEN)



# 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?



# ЧТО БУДЕТ НА ВЕБИНАРЕ

- А) ЗНАКОМСТВО
- Б) КАКОЕ МЕСТО ЗАНИМАЕТ СПЕЦИАЛИСТ ПО ЗАЩИТЕ  
КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЫ
- В) СУТЬ РАБОТЫ И КЛЮЧЕВЫЕ ЗАДАЧИ
- Г) ТРЕБОВАНИЯ РАБОТОДАТЕЛЕЙ И РЫНКА
- Д) КАК УСТРОЕНА ПРОГРАММА И ПОЧЕМУ ИМЕННО ТАК
- Е) КАК МЫ ОБУЧАЕМ СПЕЦИАЛИСТОВ



# ПОЧЕМУ ТЕМА ГОРЯЧАЯ

НЕ АБСТРАКТНЫЕ «ХАКЕРЫ ГДЕ-ТО ТАМ», А РОССИЙСКИЕ КОМПАНИИ И РЕАЛЬНЫЕ СБОИ

АЭРОФЛОТ, 2025

массовые отмены рейсов; оценки потерь за сутки — от сотен млн ₽

РЖД, 2025

DDoS по сайту и мобильному приложению, перебои с онлайн-сервисами

СДЭК, 2024

несколько дней не работали сайт и приложение, остановка приема/выдачи

УТЕЧКИ ДАННЫХ

сотни публичных инцидентов, рост значения объема и чувствительности данных

За каждой новостью стоит не «айтишный сбой», а вопрос: кто должен был увидеть, остановить и восстановить?

CyberED

# КАК БИЗНЕС ВИДИТ ИБ

[ НЕ «СКОЛЬКО АЛЕРТОВ», А СКОЛЬКО ДЕНЕГ МОЖНО ПОТЕРЯТЬ ]

- |    |                    |                                                     |
|----|--------------------|-----------------------------------------------------|
| 01 | Простой            | продажи, логистика, производство, SLA               |
| 02 | Утечка             | штрафы, суды, компенсации, доверие                  |
| 03 | Шифрование         | восстановление, простой, потеря данных              |
| 04 | Репутация          | отток клиентов, публичный кризис                    |
| 05 | Регуляторика       | проверки, предписания, персональная ответственность |
| 06 | Операционные риски | ручные процессы, ошибки, перегрузка команды         |

Задача специалиста по защите инфраструктуры — не «купить СЗИ».

Задача — сделать так, чтобы атака не стала бизнес-катастрофой.

# КЛЮЧЕВАЯ ЗАДАЧА

ОТВЕТИТЬ НА ВОПРОСЫ, ОТ КОТОРЫХ  
ЗАВИСИТ УСТОЙЧИВОСТЬ БИЗНЕСА

**01** Что у нас самое критичное?

активы, процессы, данные, сервисы

**02** Кто и как может это атаковать?

ландшафт угроз и сценарии атак

**03** Какие меры защиты реально работают?

архитектура, СЗИ, настройки, контроль

**04** Как понять, что атака уже идет?

логи, корреляции, мониторинг, SOC

**05** Как быстро остановить и  
восстановить?

IR, коммуникация, lessons learned

**ЗАЩИТА ИНФРАСТРУКТУРЫ** — ЭТО НЕ НАБОР ЖЕЛЕЗОК, А СПОСОБНОСТЬ  
ОТВЕЧАТЬ НА ПРАВИЛЬНЫЕ ВОПРОСЫ РАНЬШЕ АТАКУЮЩЕГО.

# ИДЕАЛЬНЫЙ РЕЗУЛЬТАТ

50% 75% 100% РАБОТЫ СПЕЦИАЛИСТА ИБ

ЭТО НЕ ОТСУТСТВИЕ АТАК, А УПРАВЛЯЕМОСТЬ РИСКА

[ КАК? ]

## Видимость

мы знаем, что происходит в инфраструктуре

## Контроль

системы защиты настроены и проверены

## Улучшение

после инцидента защита становится сильнее

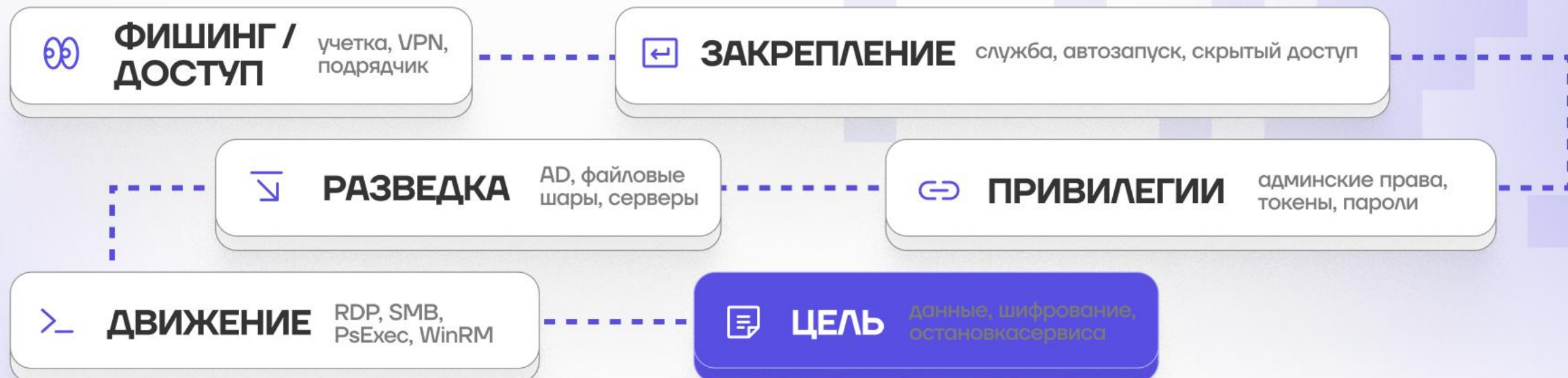
## Обнаружение

подозрительная активность попадает в мониторинг

## Реагирование

команда понимает, что делать и кто отвечает

# КАК ПРОИСХОДИТ НАСТОЯЩАЯ АТАКА



АТАКА РЕДКО ВЫГЛЯДИТ КАК ОДИН «ВЗЛОМ». ЭТО ПРОЦЕСС, И ЗАЩИТНИК ДОЛЖЕН ВИДЕТЬ ЕГО РАНЬШЕ ФИНАЛЬНОГО УДАРА.

# MITRE ATT & CK

## ЭТО НЕ ТАБЛИЦА ДЛЯ ЗУБРЕЖКИ

### ЗАЧЕМ ЭТО СПЕЦИАЛИСТУ?

- говорить на общем языке с командой
- понимать, на каком этапе атака
- строить детекты и сценарии реагирования
- объяснять бизнесу: «мы видим атаку до ущерба»

MITRE | ATT&CK

Матрицы | Тактика | Методы | Защитные сооружения | CTI | Ресурсы | Благотворители | Способствовать | Блог

Поиск

| Разведка                                                                                                                                                                                                                                                                                                                                 | Разработка ресурсов                                                                                                                                                                                                                                                                                                                               | Первоначальный доступ                                                                                                                                                                                                                                                                                                                                                                                       | Исполнение                                                                                                                                                                                                                                                                                                                                                                                        | Упорство                                                                                                                                                                                                                                                                                                                                                                                                                                       | Повышение привилегий                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Оборонительное уклонение                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Доступ по учетным данным                                                                                                                                                                                                                                                                                                                                                                                       | Открытие                                                                                                                                                                                                                                                                                                                                                                  | Боковое движение                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11 техник                                                                                                                                                                                                                                                                                                                                | 8 техник                                                                                                                                                                                                                                                                                                                                          | 11 техник                                                                                                                                                                                                                                                                                                                                                                                                   | 17 техник                                                                                                                                                                                                                                                                                                                                                                                         | 23 техники                                                                                                                                                                                                                                                                                                                                                                                                                                     | 14 техник                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 47 методов                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 17 техник                                                                                                                                                                                                                                                                                                                                                                                                      | 34 техники                                                                                                                                                                                                                                                                                                                                                                | 9 техник                                                                                                                                                                                                                                                                                                                                                      |
| Активное сканирование (9)<br>Соберите информацию о пострадавшем хозяине (4)<br>Соберите информацию о личности жертвы (3)<br>Соберите информацию о сети жертвы (4)<br>Соберите информацию об организации-жертве (4)<br>Фишинг информации (4)<br>Поиск в закрытых источниках (2)<br>Поиск в открытых технических базах данных (6)<br>Поиск | Получить доступ (9)<br>Приобретение инфраструктуры (3)<br>Компромиссные счета (3)<br>Компромиссная инфраструктура (3)<br>Развитие потенциала (4)<br>Создание счетов (3)<br>Получить информацию об организации-жертве (4)<br>Возможности сценария (4)<br>Поиск в закрытых источниках (2)<br>Поиск в открытых технических базах данных (6)<br>Поиск | Вставка контента (9)<br>Компромисс проеда (3)<br>Использование уязвимостей в общедоступных приложениях (3)<br>Внешние удаленные сервисы (3)<br>Дополнительные аппаратные средства (3)<br>Фишинг (4)<br>Получить информацию об организации-жертве (4)<br>Возможности сценария (4)<br>Компромисс в цепочке поставок (3)<br>Доверительные отношения (3)<br>Действительные учетные записи (4)<br>Сети Wi-Fi (3) | Команда администрирования облака (3)<br>Интерпретатор команд и скриптов (13)<br>Команда управления контейнерами (3)<br>Развернуть контейнер (3)<br>Команда администрирования ESX (3)<br>Эксплуатация для исполнения клиентскими операциями (3)<br>Ввод входных данных (3)<br>Межпроцессная коммуникация (3)<br>Нативный API (3)<br>Исполнение отлаженного трубопровода (3)<br>Запланированная (3) | Манипулирование учетной записью (7)<br>Вакансии в BITS (3)<br>Выполнение автозапуска при загрузке или входе в систему (14)<br>Сценарии инициализации загрузки или входа в систему (14)<br>Интерпретация облачных приложений (3)<br>Компрометировать двоичный файл программного обеспечения хоста (3)<br>Создать аккаунт (3)<br>Создание или изменение системного процесса (3)<br>Выполнение, инициированное событием (14)<br>Побег к хосту (3) | Механизм контроля за повышением уровня насилия (4)<br>Манипулирование токенами доступа (3)<br>Вакансии в BITS (3)<br>Создание образа на хосте (3)<br>Обход отладчика (3)<br>Отложенное исполнение (3)<br>Деобфускация/декодирование файлов или информации (3)<br>Сценарии инициализации загрузки или входа в систему (14)<br>Создание или изменение системного процесса (3)<br>Изменение политики домена или арендатора (3)<br>Изменение политики домена или арендатора (3)<br>Побег к хосту (3) | Механизм контроля за повышением уровня насилия (4)<br>Манипулирование токенами доступа (3)<br>Вакансии в BITS (3)<br>Создание образа на хосте (3)<br>Обход отладчика (3)<br>Отложенное исполнение (3)<br>Деобфускация/декодирование файлов или информации (3)<br>Сценарии инициализации загрузки или входа в систему (14)<br>Создание или изменение системного процесса (3)<br>Изменение политики домена или арендатора (3)<br>Изменение политики домена или арендатора (3)<br>Побег к хосту (3) | Противник посередине (4)<br>Грубая сила (4)<br>Учетные данные из хранилищ паролей (4)<br>Эксплуатация для получения доступа к учетным данным (3)<br>Принудительная аутентификация (3)<br>Подделка веб-учетных данных (2)<br>Захват ввода (4)<br>Изменение процесса аутентификации (6)<br>Перехват многофакторной аутентификации (3)<br>Генерация запроса на многофакторную аутентификацию (3)<br>Использование | Обнаружение удаленных сервисов (4)<br>Обнаружение окон приложений (3)<br>Обнаружение информации в браузере (3)<br>Обнаружение облачной инфраструктуры (3)<br>Панель управления облачными сервисами (3)<br>Обнаружение облачных сервисов (3)<br>Обнаружение объектов в облачном хранилище (3)<br>Обнаружение объектов и ресурсов (3)<br>Обход отладчика (3)<br>Обнаружение | Использование учетных записей (4)<br>Внутренний фишинг (3)<br>Боковое движение (3)<br>Перехват сеанса удаленной службы (3)<br>Удаленные сервисы (3)<br>Размножение с помощью съемных носителей (3)<br>Инструменты развертывания программного обеспечения (3)<br>Загрязнение общего контента (3)<br>Использование альтернативных материалов аутентификации (4) |

MITRE интересен не матрицей, а тем, что превращает хаос событий в понятную историю атаки.

# ГДЕ ДОЛЖЕН СРАБОТАТЬ СПЕЦИАЛИСТ ИБ

[ ЧЕМ РАНЬШЕ ЭТАП, ТЕМ ДЕШЕВЛЕ ИНЦИДЕНТ ] 

| INITIAL ACCESS       | EXECUTION             | CREDENTIAL ACCESS | LATERAL MOVEMENT | IMPACT             |
|----------------------|-----------------------|-------------------|------------------|--------------------|
| дешево<br>ОСТАНОВИТЬ | МОЖНО<br>ЛОКАЛИЗОВАТЬ | опасно            | критично         | поздно<br>и дорого |

**Роль Blue Team — сместить обнаружение влево: увидеть не «серверы зашифрованы», а первые признаки атаки.**

В профессии ценится не героизм после катастрофы, а способность заметить атаку до Impact.

# КАК ВЫГЛЯДИТ СОВРЕМЕННАЯ ЗАЩИТА КОМПАНИИ

## 1. CISO + CEO

### Риск и стратегия

- что критично для бизнеса
- какие угрозы приоритетны
- какой риск приемлем
- сколько инвестировать
- как измерять результат

## 2. Архитектура и инженерия

### Контуры защиты

- сегментация сети
- AD и права доступа
- FW / IDS / EDR / DLP
- hardening Windows/Linux
- сбор логов и видимость

## 3. Операции и реагирование

### Люди и процессы

- мониторинг 24/7
- расследование алертов
- реагирование и изоляция
- форензика
- улучшение правил и защиты

**ИБ** — это не только инструменты. Это связка управленческих решений, инженерной реализации и ежедневной операционной работы.

# BLUE TEAM

## — ЭТО НЕ ТОЛЬКО SOC

Защита корпоративной инфраструктуры — это экосистема ролей: аналитики, инженеры, разработчики, автоматизаторы, архитекторы, CTI и руководители.

 SOC / Monitoring

 Threat Intelligence

 DevSecOps / AppSec

 IR / DFIR

 Security Engineering

 Vulnerability  
Management

 Detection Engineering

 Infrastructure Security

 Security Architecture

 Threat Hunting

 Automation / SOAR

 GRC / Management

Выбор трека начинается не с названия должности, а с вопроса: какую часть защиты вам интереснее строить?

# ОПЕРАЦИИ, РАССЛЕДОВАНИЯ И ДЕТЕКТЫ

Эти роли отвечают за обнаружение атак, разбор инцидентов и улучшение качества мониторинга.

 **SOC / Security Operations**

**Что происходит прямо сейчас?**

- SOC L1 / L2 / L3 Analyst
- SOC Shift Lead
- SOC Manager

 **Incident Response / DFIR**

**Как остановить и расследовать?**

- IR Specialist
- Forensic Analyst
- Malware Analyst

 **Detection Engineering**

**Как обнаруживать атаки лучше?**

- Detection Engineer
- SIEM Content Developer
- Correlation Rules Developer

 **Threat Hunting / CTI**

**Что мы могли пропустить и кто нас атакует?**

- Threat Hunter
- CTI Analyst
- Tactical / Strategic TI
- Vulnerability Intelligence Analyst
- Adversary Emulation Analyst

**SOC** ВИДИТ СИГНАЛ, **IR** ТУШИТ ПОЖАР, **DETECTION** УЛУЧШАЕТ «ДАТЧИКИ», **THREAT INTELLIGENCE** ОБЪЯСНЯЕТ, К КАКИМ УГРОЗАМ ГОТОВИТЬСЯ.

# КТО СТРОИТ И РАЗВИВАЕТ ЗАЩИТУ

Эти роли делают так, чтобы защитные меры не просто были куплены, а реально работали в инфраструктуре и разработке.

## Security Engineering

Как настроить контур защиты?

- FW / IDS / IPS / EDR / DLP

## Infrastructure Security

Как защитить AD, серверы и доступы?

- Windows / Linux Security

## Automation / SOAR

Что можно автоматизировать?

- SOAR Engineer

## DevSecOps / AppSec

Как встроить безопасность в разработку?

- DevSecOps Engineer

## Vulnerability Management

Что чинить первым?

- Vulnerability Analyst

## Architecture / GRC

Какую систему защиты строить?

- Security Architect

**ЗАЩИТА ИНФРАСТРУКТУРЫ** — ЭТО СВЯЗКА ИНЖЕНЕРИИ, РАЗРАБОТКИ, АВТОМАТИЗАЦИИ, УПРАВЛЕНИЯ РИСКАМИ И ОПЕРАЦИОННОГО МОНИТОРИНГА.

# СХОЖИЕ ПРОФЕССИИ,

→ КОТОРЫЕ ПОМОГАЮТ ПЕРЕЙТИ **BLUE TEAM**

- Системный администратор (Linux/Windows)
- Сетевой инженер
- HelpDesk / поддержка
- Разработчик / QA
- DevOps / Cloud-инженер
- ИБ-аудитор / классический ИБ
- Аналитик данных / скриптер



**BLUE  
TEAM**



В Blue Team можно прийти из разных ролей. Главное — понять, какая часть вашего опыта уже помогает защищать инфраструктуру.

# ТРИ ТИПА РОСТА В BLUE TEAM

## ■ 1. ОПЕРАЦИОННЫЙ ТРЕК

- SOC L1 → SOC L2 → SOC L3 → SHIFT LEAD → SOC LEAD
- ФОКУС: TRIAGE, РАССЛЕДОВАНИЯ, ЭСКАЛАЦИЯ, РЕАГИРОВАНИЕ.
- ПОДХОДИТ ТЕМ, КОМУ ИНТЕРЕСНЫ АТАКИ, РАССЛЕДОВАНИЯ И РАБОТА С СОБЫТИЯМИ.

## ■ 2. ИНЖЕНЕРНЫЙ ТРЕК

- SECURITY ENGINEER → PLATFORM/SIEM/EDR ENGINEER → SECURITY ARCHITECT
- ФОКУС: ВНЕДРЕНИЕ СЗИ, ЛОГИ, AD, СЕТИ, HARDENING, ИНТЕГРАЦИИ.
- ПОДХОДИТ АДМИНАМ, СЕТЕВИКАМ, DEVOPS, ИНЖЕНЕРАМ.

## ■ 3. ЭКСПЕРТНО-АНАЛИТИЧЕСКИЙ ТРЕК

- DETECTION → THREAT HUNTING → THREAT INTELLIGENCE → IR/DFIR
- ФОКУС: ТТР, MITRE, ГИПОТЕЗЫ, ПРАВИЛА, РАЗВЕДКА УГРОЗ.
- ПОДХОДИТ ТЕМ, КТО ЛЮБИТ ИССЛЕДОВАНИЕ И СИСТЕМНОЕ МЫШЛЕНИЕ.

# МАТРИЦА КАРЬЕРНОГО ПУТИ

CyberED

|        | OPERATIONS / SOC                                                                                               | ENGINEERING                                                                                                             | DETECTION / HUNTING                                                                                                        | THREAT INTEL                                                                                                         | MANAGEMENT                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| JUNIOR |  SOC L1<br>Triage, аперты     |  Junior SecEng<br>логи, СЗИ            |  Junior Detection<br>Sigma/KQL база     |  Junior CTI<br>IOC, обзоры        | —                                                                                                       |
| MIDDLE |  SOC L2<br>расследования      |  SecEng<br>AD, EDR, SIEM               |  Detection Eng<br>use cases             |  CTI Analyst<br>TTP, кампании     |  Team Coordinator    |
| SENIOR |  SOC L3 / IR<br>сложные кейсы |  Platform Eng<br>интеграции            |  Threat Hunter<br>гипотезы              |  Senior CTI<br>профили угроз      |  Service Owner       |
| LEAD   |  SOC Lead<br>SLA, качество  |  Security Architect<br>дизайн защиты |  Detection Lead<br>стратегия детектов |  Intel Lead<br>приоритеты угроз |  Head / CISO-track |



**ВЫВОД:** РОСТ — ЭТО НЕ ТОЛЬКО ПОВЫШЕНИЕ ДОЛЖНОСТИ,  
НО И СМЕНА СПЕЦИАЛИЗАЦИИ **БЕЗ ВЫХОДА ИЗ BLUE TEAM.**

# БЕЗ РОЗОВЫХ ОЧКОВ

## [ РЕАЛЬНОСТЬ ПРОФЕССИИ ] ➤

+ Работодатель ждет доказуемые навыки, а не «интерес к ИБ»

+ Отчеты и коммуникация так же важны, как технический анализ

+ Придется понимать сети, ОС, логи и бизнес-контекст

+ Учиться придется постоянно: атаки, продукты и инфраструктура

+ Инструменты не думают за специалиста

+ CTF и лаборатории полезны, но не заменяют реальную инфраструктуру

## [ ХОРОШАЯ НОВОСТЬ ]

Вход возможен из разных ролей: админ, сетевик, DevOps, HelpDesk, классический ИБ, аудит, разработка. Побеждает не тот, кто «родился хакером», а тот, кто системно закрывает базу и много практикуется.

# СТЕРЕОТИП: «АНАЛИТИК SOC ПРОСТО СМОТРИТ АЛЕРТЫ»

CyberED

## СТЕРЕОТИП

- ✗ НАЖИМАЕТ “ЗАКРЫТЬ”
- ✗ СМОТРИТ КРАСИВЫЕ ГРАФИКИ
- ✗ ЖДЕТ, ПОКА SIEM ВСЁ СКАЖЕТ
- ✗ РАБОТАЕТ ПО ЧЕК-ЛИСТУ БЕЗ ПОНИМАНИЯ

**ПРОФЕССИЯ НЕ ПРО «СМОТРЕТЬ В ЭКРАН».**  
ОНА ПРО МЫШЛЕНИЕ РАССЛЕДОВАТЕЛЯ  
ВНУТРИ СЛОЖНОЙ ИНФРАСТРУКТУРЫ.

## РЕАЛЬНОСТЬ

- ✓ РАССЛЕДУЕТ АТАКИ
- ✓ ИЩЕТ ЗЛОУМЫШЛЕННИКА В ИНФРАСТРУКТУРЕ
- ✓ АНАЛИЗИРУЕТ ПОВЕДЕНИЕ И ГИПОТЕЗЫ
- ✓ ПОНИМАЕТ WINDOWS, LINUX, СЕТИ И AD
- ✓ ОБЪЯСНЯЕТ РИСК БИЗНЕСУ И ИНЖЕНЕРАМ

# ЧТО ХОТЯТ РАБОТОДАТЕЛИ

## База ОС и сетей

+ Windows, Linux, TCP/IP, DNS, HTTP, AD

## Логи и SIEM

+ события, корреляции, поиск, false positive

## СЗИ

+ FW, IDS/IPS, EDR, DLP, proxy, AV

## Атаки и MITRE

+ понимать тактики, техники, kill chain

## Скрипты

+ PowerShell, Bash, Python как плюс

## Коммуникация

+ описать инцидент, объяснить риск, эскалировать

**Вакансии требуют не магии, а комбинации базы:  
инфраструктура + угрозы + инструменты + коммуникация.**

# [ АНАЛИЗ ВАКАНСИЙ ]

CyberED



Билайн

## Аналитик SOC L1



Опыт работы: 1-3 года

### Итак, вам предстоит:

- Мониторинг и анализ событий информационной безопасности со средств защиты информации (SIEM, AV, FW, IPS\IDS, DLP и др.).
- Расследование типовых инцидентов ИБ.
- Эскалация инцидентов на вышестоящие линии.
- Анализ систем мониторинга СЗИ.
- Предложения по исключению ложно-положительных срабатываний правил корреляции.
- Посменная работа для обеспечения функционирования SOC в режиме 24x7.

### Мы будем рады рассмотреть вашу кандидатуру, если у вас есть:

- Знание основ информационной безопасности.
- Базовое понимание работы windows/nix систем.
- Опыт в расследовании инцидентов ИБ.
- Знание и понимание работы сетевых протоколов (OSI, tcp/ip).
- Базовое понимание принципов работы Active Directory (механизмы аутентификации, атаки).
- Знание и понимание основных тактик и техник злоумышленников (MITRE ATT&CK /Cyber KillChain).
- Опыт работы с системами сбора логов (SIEM).

# [ АНАЛИЗ ВАКАНСИЙ ]

**РОСГОССТРАХ**

Росгосстрах

**Специалист отдела  
администрирования СЗИ**



**Опыт работы: 1-3 года**

## Обязанности:

- ✦ Внедрение и сопровождение средств защиты информации (СЗИ) в компании;
- ✦ Взаимодействие с вендорами и подрядчиками для обеспечения эффективной работы СЗИ;
- ✦ Поиск уязвимостей в информационных системах и создание статистических отчетов по выявленным уязвимостям;
- ✦ Разработка и реализация мер по устранению уязвимостей;
- ✦ Обеспечение соответствия информационных систем требованиям безопасности.

## Требования:

- ✦ Опыт работы в области информационной безопасности от 1 до 3 лет;
- ✦ Знание современных средств защиты информации и методов поиска уязвимостей;
- ✦ Умение работать с вендорами и подрядчиками;
- ✦ Аналитические способности и внимание к деталям;
- ✦ Знание основных принципов работы сетей – стек протоколов TCP/IP, адресация, маршрутизация, межсетевое экранирование, основные сетевые сервисы, аудит сети, настройка электронной почты;
- ✦ Знание средств защиты – антивирусы DrWeb, KES, KSC, Сканеры уязвимостей, DLP, SIEM, песочницы, NGFW и пр.;
- ✦ Готовность к обучению и развитию в области информационной безопасности.

# [ АНАЛИЗ ВАКАНСИЙ ]



Транснефть-Технологии

## Дежурный инженер систем информационной безопасности



Опыт работы: 1–3 года

### Задачи:

- Мониторинг систем/задач информационной безопасности;
- Проведение первичной диагностики, выполнение типовых процедур согласно инструкциям;
- Выполнение типовых запросов на обслуживание от пользователей систем;
- Сбор информации и эскалация сложных проблем старшим специалистам;
- Взаимодействие с инженерами других служб и подразделений;
- Выполнение регламентированных процедур.

### Ожидаем от Вас:

- Высшее техническое образование (информационные технологии/ физика/ математика);
- Опыт администрирования SIEM, SOAR, СЗИ;
- Знание и/или опыт администрирования любых Unix/Linux/Windows ОС;
- Знание принципов работы стека протоколов TCP/IP.

# ПОЧЕМУ ПРОСТО ТЕОРИИ НЕДОСТАТОЧНО

## [ ПРОБЛЕМА НОВИЧКА ]

- знает термины, но не видел инфраструктуру
- понимает атаку отдельно от защиты
- не умеет объяснить ход расследования
- не может показать результат в резюме

### Что должно быть вместо этого

- + Стенд, задачи, ошибки, разборы, отчеты, настроенные системы и понимание: как угроза превращается в защитную меру, а событие в расследование.

# КАК ИИ МЕНЯЕТ BLUE TEAM



**SOC-АНАЛИТИК** СУММАРИЗАЦИЯ АЛЕРТОВ, ОБЪЯСНЕНИЕ КОМАНД, ЧЕРНОВИК ОТЧЕТА



**DETECTION ENGINEER** ЧЕРНОВИКИ SIGMA/KQL/YARA, REGEX, НОРМАЛИЗАЦИЯ ЛОГОВ



**SECURITY ENGINEER** ПРОВЕРКА КОНФИГУРАЦИЙ, HARDENING CHECKLIST, ДОКУМЕНТАЦИЯ



**IR / DFIR** ТАЙМЛАЙН ИНЦИДЕНТА, ГИПОТЕЗЫ, ПЕРВИЧНЫЙ РАЗБОР АРТЕФАКТОВ



**ПРОДУКТЫ ИБ** UEBA, ML-ДЕТЕКТ АНОМАЛИЙ, ПРИОРИТИЗАЦИЯ АЛЕРТОВ



**РУКОВОДИТЕЛЬ** КРАТКИЕ ОТЧЕТЫ, РИСК-КОММУНИКАЦИЯ, ПОДГОТОВКА СЦЕНАРИЕВ

# КАК ПЕРЕВЕСТИ ОБУЧЕНИЕ В КАРЬЕРНЫЙ РЕЗУЛЬТАТ

[ Что делать уже во время курса ]

1



## ВЕСТИ ЖУРНАЛ ПРАКТИКИ

что настроил, что сломал, как починил

2



## ОПИСЫВАТЬ КЕЙСЫ

проблема → действия → результат → вывод

3



## СОБИРАТЬ ПОРТФОЛИО

стенд, скрипты, отчеты, схемы

4



## ТРЕНИРОВАТЬ СОБЕСЕДОВАНИЯ

объяснять не термины, а ход мысли

5



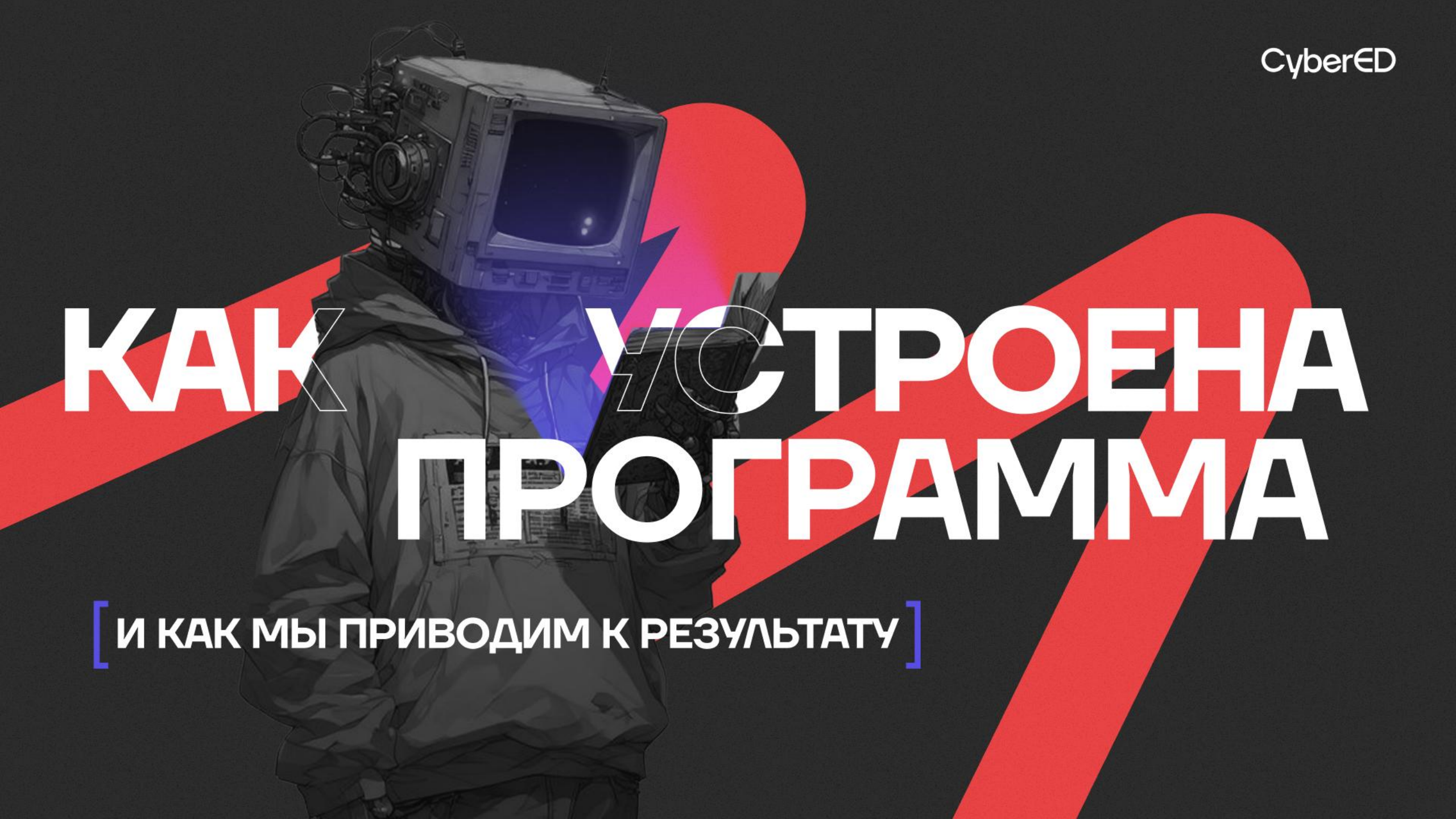
## ВЫБИРАТЬ ТРЕК

SOC, инженерия, IR, DevSecOps, архитектура



ДАВАЙТЕ РАЗБЕРЕМ  
ВАШИ   
ВОПРОСЫ





# КАК УСТРОЕНА ПРОГРАММА

[ И КАК МЫ ПРИВОДИМ К РЕЗУЛЬТАТУ ]

# КАК ПОСТРОЕН ТРЕК

[ ТРИ МОДУЛЯ ЗАКРЫВАЮТ ЦЕПОЧКУ: УГРОЗА → ЗАЩИТА → МОНИТОРИНГ И РЕАГИРОВАНИЕ ]

## В-207

### Угрозы корпоративной инфраструктуры

как атакуют  
инфраструктуру:  
разведка, сканирование,  
web, brute force, malware,  
Wi-Fi

## В-208

### Системы информационной безопасности

как строить защиту:  
FW, IDS/IPS, Proxy, AD,  
SIEM, IR, HoneyPot, DLP

## В-228

### Аналитик SOC

как мониторить и  
расследовать:  
Windows, persistence,  
hijacking, priv esc,  
credential access, lateral  
movement, IR

# ЭТАП 1:

## ПОНИМАНИЕ УГРОЗЫ [ В-207 ]

### Итог модуля:

Перестаете воспринимать атаку как «черный ящик» и начинаете видеть сценарии: где атакующий входит, какие ошибки использует и какие следы оставляет.

1. Безопасность корпоративной инфраструктуры
2. Сбор информации, проведение рекогносцировки и социальная инженерия
3. Сканирование сети корпоративной инфраструктуры
4. Перечисление
5. Проникновение за периметр инфраструктуры. SSH-Tunneling
6. Вредоносное программное обеспечение в корпоративной среде
7. Хакинг веб-приложений
8. Особенности атак, использующих метод грубой силы
9. Хакинг системы – порядок действий
10. Безопасность Wi-Fi сетей

# ЭТАП 2:

## ПОСТРОЕНИЕ ЗАЩИТЫ [B-208]

### Итог модуля:

Получите навыки и опыт из лучших практик в настройке групповых политик с точки зрения обеспечения безопасности корпоративной инфраструктуры.

1. Межсетевые экраны - Firewalls (Pfsense & iptables)
2. Межсетевые экраны следующего поколения и системы обнаружения вторжений - IDS / IPS (SNORT and Suricata)
3. Proxy Servers (Squid)
4. Reverse Proxy Servers (Nginx)
5. Endpoint Security (Antiviruses) и почтовые шлюзы (Mail Security GW)
6. Системы анализа аномального трафика в корпоративной сети (Network traffic anomaly analysers)
7. Microsoft AD and Group Policy Security Settings
8. Центры мониторинга инцидентов информационной безопасности. SIEM (ElasticSearch Logstash and Kibana)
9. Реагирование на инциденты ИБ. Incident Responce
10. Приманки для хакеров. Системы HoneyPot или HoneyNet
11. Системы обнаружения утечек данных. DLP

# ЭТАП 3:

## РАССЛЕДОВАНИЕ РЕАГИРОВАНИЕ

[ В-228 ]

### Итог модуля:

Научитесь не просто видеть событие, а задавать вопросы: что произошло, где масштаб, есть ли компрометация, как остановить, кому эскалировать.

1. Security Operation Center (SOC)
2. Внутреннее устройство и безопасность Windows
3. Корреляция и что такое Persistence
4. Атаки класса Hijacking
5. Повышение привилегий
6. Credential Access
7. Разведка и горизонтальное перемещение в Windows
8. Горизонтальное перемещение в Windows и тактики Collection, Command and Control, Exfiltration и Impact
9. Расследование инцидента компьютерной безопасности
10. Административный и операционный SOC

# ИИ-АГЕНТЫ В ЗАЩИТЕ КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЫ

МОДУЛЬ **B410** • 2 ЭКСПЕРТНЫЕ ВСТРЕЧИ • РЕАЛЬНЫЙ ОПЫТ ВНЕДРЕНИЯ



## АНАЛИТИКА & SOC



ИИ в SOC и мониторинге



Автоматизация триажа



Разбор инцидентов



## ИНФРАСТРУКТУРА & DEVSECOPS



Локальные / облачные LLM



Архитектура агентов + MCP



Hardening рабочих станций



## БЕЗОПАСНОСТЬ АГЕНТОВ



Управление доступами (PoLP)



Prompt injection & риски



Новые артефакты безопасности



Архитектурные  
подходы и ограничения



Защита данных  
при работе с LLM



Безопасная  
оркестрация агентских систем



Практические кейсы  
Blue Team



# ФОРМАТ И АРТЕФАКТЫ

---

## ✓ 31 занятие

250 ак.ч., 4 месяца, занятия 2 раза в неделю

## ✓ 70% практики

собственная виртуальная среда и задачи руками

## ✓ Диплом

документ о профессиональной переподготовке

## ✓ Артефакты

стенды, сеть, DNS/DHCP, ELK SIEM, DLP, скрипты

- настроенные виртуальные машины
  - DNS и DHCP
  - скрипты детектирования атак
  - сеть на гипервизоре
  - анализ аномального трафика
  - DLP и SIEM на ELK
-

# ЧТО ВЫ СДЕЛАЕТЕ СВОИМИ РУКАМИ?



Спроектировать инфраструктуру и разобрать атаки



Провести Subdomain enumeration



Написать инструкцию по SSL-Split



Создать инфраструктуру в EVE-NG



Написать инструкцию по DNS-туннелю



Разобрать кейс реагирования на атаку



Развернуть проактивную антивирусную защиту



Развернуть SIEM на ELK



Продемонстрировать атаку с аномальным трафиком

# УСПЕЙ НА НОВЫЙ ПОТОК ПРОГРАММЫ

CyberED



СТАРТ 17 ИЮЛЯ



+ 3 миникурса в подарок

ОСТАВЛЯЙ ЗАЯВКУ!