

[ГРУППОВАЯ КОНСУЛЬТАЦИЯ
ПО ПРОГРАММЕ ОБУЧЕНИЯ]

АНАЛИТИК SOC



CyberED

О ЧЁМ ПОГОВОРИМ НА ЭФИРЕ?

- 01 Знакомство
- 02 Какое место занимает аналитик SOC среди других специальностей ИБ?
- 03 Суть работы и ключевые задачи
- 04 Требования работодателей и рынка
- 05 Как устроена программа и почему именно так
- 06 Как мы обучаем аналитиков SOC: разбор на кейсах

CyberED —

CyberED



**НИШЕВАЯ ПЛАТФОРМА
ОБУЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ.**

7 лет

обучаем на практике
у лучших экспертов в России

20 +

образовательных
программ по ИБ

5000 +

выпускников

200+

корпоративных клиентов

50+

преподавателей-практиков

80 +

лабораторных стендов

— Групповая консультация / Аналитик SOC —

CyberED —

КЛЮЧЕВОЙ ОБРАЗОВАТЕЛЬНЫЙ ПРОЕКТ ФОНДА РЕЗУЛЬТАТИВНОЙ КИБЕРБЕЗОПАСНОСТИ **CYBERUS**



Фонд с капиталом 25+ млрд ₽ объединяет компании и команды в сфере кибербезопасности, создавая основу для обучения на реальной индустриальной экспертизе.



15+ компаний объединились
в фонде Cyberus

 **INNOSTAGE**

Крупнейший в РФ
системный
интегратор в сфере
кибербезопасности

 **кибердом**

Вендор решений для
защиты информации и
предотвращения утечек

F6

Ведущий российский
разработчик
технологий для борьбы
с киберпреступлениям

CYBEROK

Разработчик систем
контроля кибератак и
реагирования на
угрозы

 **positive
technologies**

Разработчик продуктов
для защиты от киберугроз,
единственная публичная
кибербез-компания в РФ

СОЗДАЁМ ПРОГРАММЫ ВМЕСТЕ С CYBERUS,

ЧТОБЫ ОБУЧЕНИЕ СООТВЕТСТВОВАЛО
ТОМУ, КАК СЕГОДНЯ РАБОТАЮТ РЕАЛЬНЫЕ
КОМАНДЫ КИБЕРБЕЗОПАСНОСТИ

01

Эксперты Cyberus участвуют
в занятиях и разборе практик

02

Доступ к инструментам и подходам, которые
используют корпоративные команды ИБ

03

Актуальные техники и сценарии
атак в программах обучения

04

Стажировки студентов CyberED
в компаниях-партнёрах

кибердом



Сайберус

positive technologies



КИБЕР
ИСПЫТАНИЕ

ОБУЧАЕМ СОТРУДНИКОВ КРУПНЫХ КОМПАНИЙ

 В РОССИИ И ЗАРУБЕЖОМ:



Банк России



SBER TECH



МТС



ПСХБ



НОРНИКЕЛЬ



ВТБ

Яндекс



КРОК



Ростелеком



BI.ZONE
Cybersecurity



Т БАНК



БСПБ

CyberED ВСТРОЕН



Партнёрства
с топ-компаниями
ИБ-индустрии

В РАБОЧУЮ ЭКОСИСТЕМУ КИБЕРБЕЗОПАСНОСТИ

ГОТОВИМ КАДРЫ ПОД СЕБЯ И ДРУГИХ ИГРОКОВ РЫНКА



Агентство белых хакеров
Singleton Security

Лучшие студенты курсов:

- проходят стажировку
- попадают в реальные проекты и команды

ПРАКТИКА В РЕАЛЬНЫХ КОМПАНИЯХ И НА РЕАЛЬНЫХ КЕЙСАХ



Кибериспытание

Студенты во время обучения:

- находят уязвимости в реальных компаниях
- получают вознаграждение ещё до окончания курса



Standoff365

Для студентов CyberED:

- разработаны специальные реалистичные стенды
- тренировки проходят в условиях, близких к боевым

[О СПИКЕРЕ]

CyberED

КРИСТИНА ЖЕЗЛОВА



■ Интересы:

- Threat Hunting
- Расследование хакерских инцидентов. Основы форензики Threat intelligence
- Реагирование на инциденты и компьютерная криминалистика в ОС Windows
- Специалист центра мониторинга инцидентов ИБ (SOC)

■ Компания: Бастион

■ Должность: Аналитик SOC, L4



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)

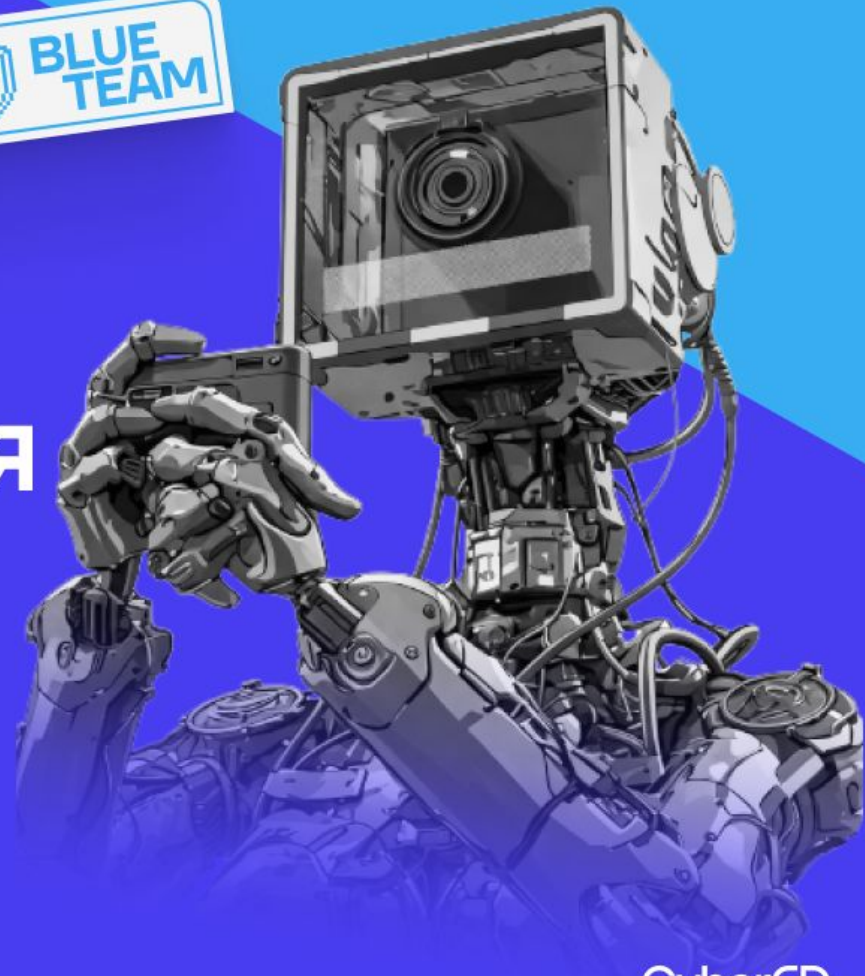
КАКИЕ У ВАС ЦЕЛИ
НА ВСТРЕЧУ?





АНАЛИТИК ЦЕНТРА ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ

[АНАЛИТИК SOC] [L1]



КАРТА НАПРАВЛЕНИЙ

CyberED

[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



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.

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

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

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

GRC / ARCH

Проектирование архитектуры безопасности, управление рисками и обеспечение соответствия нормам.

■ Тип мышления:
стратегический, управленческий.

■ Верхние роли:

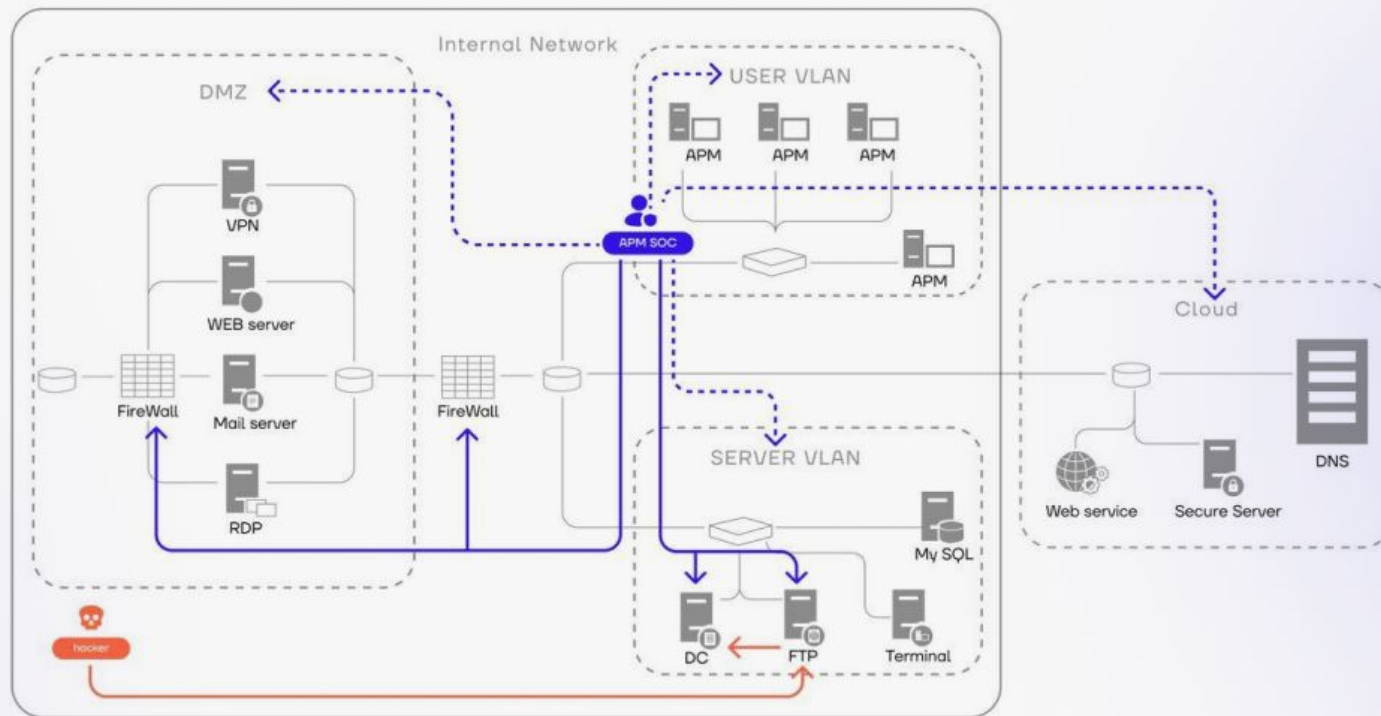
Управление рисками

Архитектор безопасности

Безопасность поставщиков

Аудитор

Суть работы и ключевые задачи аналитика SOC



[АНАЛИТИК SOC_L1]

СУТЬ РАБОТЫ И КЛЮЧЕВЫЕ ЗАДАЧИ



ПЕРВЫЙ УРОВЕНЬ АНАЛИТИКОВ ЦЕНТРА МОНИТОРИНГА КИБЕРАТАК (L1)

— специалист, который отслеживает события безопасности через специальные программы, получает входящие алерты (сигналы тревоги) и решает, есть ли в них признаки атаки.

ГЛАВНАЯ ЗАДАЧА:

— быстро и правильно определить, является ли срабатывание безопасности реальной угрозой или ложной, и при необходимости оперативно передать инцидент на следующий уровень (L2/L3).

ТРЕБОВАНИЯ РАБОТОДАТЕЛЕЙ:

АНАЛИЗ
ВАКАНСИЙ

CyberED

Требования:

- Высшее/незаконченное высшее техническое образование;
- Опыт работы в области ИБ от года;
- Знание подходов в области мониторинга безопасности, оповещения (опционально **аналитика**);
- Понимание концепций межсетевых экранов, прокси-серверов, SIEM, антивирусов и IDPS;
- Стремление к получению новых знаний в области ИБ;
- Способность работать по гибкому графику в условиях круглосуточной работы операционного центра безопасности (**SOC**);
- Понимание сетевой модели OSI, стек TCP/IP, сетевые протоколы HTTP/HTTPS, DNS, DHCP, ARP.
- Аналитическое мышление, внимательность, скрупулёзность, умение работать с большим объемом информации, в многозадачном/интенсивном режиме, ответственность, коммуникабельность, доброжелательность, стрессоустойчивость.

Нужно знать и уметь:

- Базовое понимание принципов и сценариев реализации компьютерных атак;
- Желательны знания в области технологий ИТ сервиса;
- Опыт работы с SIEM платформами;
- Умение работать в режиме многозадачности, высоком темпе решения задач и не бояться брать на себя ответственность;
- Высокая обучаемость, желание развиваться и повышать квалификацию в области информационной безопасности;
- Работа с межсетевыми экранами;
- Работа с IRP системами.

hh.ru/vacancy/130847534

Вам предстоит:

- Мониторинг событий безопасности с использованием Wazuh и MaxPatrol SIEM;
- Анализ и классификация инцидентов ИБ, определение их критичности;
- Реагирование на инциденты уровня L1 в соответствии с регламентами **SOC** и playbook;
- Настройка и обновление правил детектирования в Wazuh;
- Взаимодействие с другими отделами для уточнения контекста инцидентов;
- Ведение журналов инцидентов, формирование отчетов и документирование процессов;
- Участие в улучшении процессов мониторинга, корреляции и реагирования;
- Своевременное эскалация критических инцидентов руководству;
- Выполнение задач в рамках компетенции **аналитика SOC** по указанию руководителя;
- Поддержание актуальных знаний в области кибербезопасности и используемых технологий.

Мы ожидаем:

- Знание основ информационной безопасности, сетевых технологий и архитектуры **SOC**;
- Опыт работы с SIEM-системами, в частности Wazuh/MP10;
- Умение настраивать правила, корреляции и дашборды в Wazuh/MP10;
- Навыки анализа логов, событий безопасности и инцидентов в Wazuh/MP10;
- Базовые знания по реагированию на инциденты (IR) и следование playbook;
- Понимание современных киберугроз, методов атак (MITRE ATT&CK) и средств защиты;
- Опыт работы с системами мониторинга, EDR, IDS/IPS, сетевыми фильтрами;
- Знание нормативных требований в области ИБ (ФЗ-152, ISO 27001, ГДН);
- Аналитическое мышление, внимательность, умение работать в режиме многозадачности;
- Готовность к работе в сменном графике при необходимости;
- Умение документировать процессы, инциденты и формировать отчеты.

hh.ru/vacancy/130467251

ТРЕБОВАНИЯ РАБОТОДАТЕЛЕЙ:

АНАЛИЗ
ВАКАНСИЙ

CyberED

Что для нас важно:

- Высшее/незаконченное высшее техническое образование;
- Опыт работы в области ИБ от года;
- Знание подходов в области мониторинга безопасности, оповещения (опционально аналитика);
- Понимание концепций межсетевых экранов, прокси-серверов, SIEM, антивирусов и IDPS;
- Стремление к получению новых знаний в области ИБ;
- Способность работать по гибкому графику в условиях круглосуточной работы операционного центра безопасности (SOC);
- Понимание сетевой модели OSI, стек TCP/IP, сетевые протоколы HTTP/HTTPS, DNS, DHCP, ARP.

Будет преимуществом:

- Базовое понимание принципов и сценариев реализации компьютерных атак;
- Желательны знания в области технологий ИТ сервиса;
- Опыт работы с SIEM платформами;
- Умение работать в режиме многозадачности, высоком темпе решения задач и не бояться брать на себя ответственность;
- Высокая обучаемость, желание развиваться и повышать квалификацию в области информационной безопасности;
- Работа с межсетевыми экранами Cisco ASA, Checkpoint, User Gate;
- Работа с IRP системами.

hh.ru/vacancy/130715658

Требования:

- + знание принципов работы операционных систем Windows/Unix (как плюс на уровне продвинутого пользователя),
- + знание базовых принципов работы сетевых технологий и протоколов,
- + понимание процессов работы SOC (Security Operation Center) – реагирование, приоритизация/эскалация инцидента, постанализ и т.д.,
- + базовое знание принципов работы систем сбора и корреляции событий ИБ,
- + базовое понимание структуры журналов информационных систем и их назначения,
- + базовое знание принципов работы существующих классов средств защиты информации.

Задачи:

- + мониторинг событий информационной безопасности, поступающих из различных источников инфраструктуры Компании,
- + выявление инцидентов информационной безопасности и их первоначальная приоритизация,
- + обработка инцидентов информационной безопасности низкого и среднего уровней,
- + выполнение утвержденных SLA по реагированию на инциденты информационной безопасности,
- + своевременная эскалация инцидентов информационной безопасности на L2,
- + участие в корректировке планов реагирования и процедур, улучшении работы правил корреляции.

hh.ru/vacancy/130746542

ТРЕБОВАНИЯ РАБОТОДАТЕЛЕЙ:

АНАЛИЗ
ВАКАНСИЙ

CyberED

ЧЕМ ПРЕДСТОИТ ЗАНИМАТЬСЯ:

- Осуществлять мониторинг событий информационной безопасности
- Реагировать на инциденты информационной безопасности
- Расследовать инциденты информационной безопасности, фиксировать материалы при расследовании

НАШИ ПОЖЕЛАНИЯ К КАНДИДАТУ:

- Высшее образование (ИБ, ИТ)
- Опыт работы в SOC
- Понимание сетевой модели OSI, стека TCP/IP, сетевых протоколов HTTP/HTTPS, DNS, DHCP, ARP и т.п
- Понимание принципов работы операционных систем Windows, Linux
- Знание основных типов Windows, Linux событий
- Понимание основных тактик и техник злоумышленников, знание и применение матрицы Mitre ATT&CK, понимание KillChain
- Понимание принципов работы средств защиты информационной безопасности EDR, WAF, ABPO и т.д.)
- Внимательность, стрессоустойчивость
- Следование инструкциям
- Готовность к сменному графику

hh.ru/vacancy/130952778

Principle Responsibilities

- Analyze security events from endpoints (Windows, Mac, Linux), Network IDS, Web-proxies, Mail-gateways, Active Directory infrastructure
- Detect and investigate information security incidents
- Propose Incident response actions and remediation plan.
- Identification of potential vectors of attacks, develop detection methods of these attacks by existing technological solutions
- Adjust detection logic to fit Customer needs (filter out false positives, customize correlation rules, etc)
- Communicate with Customers regarding detected incidents and suspicious activities.

Mandatory skills

- Practical experience in the identification and investigation of information security incidents, development of recommendations to prevent similar incidents in the future
- Understanding of the methods, tools and processes to respond to information security incidents
- Experience in network traffic and log-files analysis from various sources
- Knowledge of current threats, vulnerabilities, typical of attacks on information systems and tools to implement them, as well as methods for their detection and response
- Knowledge of network protocols, the architectures of modern operating systems and information security technologies

Other requirements

- Experience in work with ELK stack is welcome
- Certifications (Offensive Security, GIAC) are welcome

hh.ru/vacancy/130573035

ГЛАВНЫЕ ВЫВОДЫ ИЗ АНАЛИЗА ВАКАНСИЙ

- Знание основ ОС и навыков анализа событий
- Знание основ сетевых технологий
- Понимание (на уровне основ) работы СЗИ
- Понимание как и с чем работает SOC аналитик (процессы, SIEM, IRP, etc)
- Понимание актуального ландшафта угроз (как совершаются атаки + кто их совершает)

МОЖНО ВЫРАЗИТЬ ТАК:

- Понимание, как устроена инфраструктура в современной организации (ОС + сеть + сервисы)
- Понимание, как действует атакующий (MITRE ATT&CK + OWASP + множество ресурсов)
- Понимание того как, на основе этой информации обнаруживать атаки

ГЛАВНЫЕ ВЫВОДЫ ИЗ АНАЛИЗА ВАКАНСИЙ



Основные инструменты

01

MITRE ATT&CK

02

Windows/Linux,
а также Networks

03

C3И (AV, EDR,
NGFW, DLP, а также
SIEM, IRP)

НА ЧТО СМОТРЯТ ПРИ ПРИЁМЕ НА РАБОТУ?

☐ Практические кейсы (Умение “думать вслух”, Честность)

☐ Понимание vs зазубривание

☐ Умение рассказать о себе

☐ Знакомство с вакансией и компанией (!)



[АНАЛИТИК SOC]

АРХИТЕКТУРА ПРОГРАММЫ

О ПРОГРАММЕ

Объём часов – 270 ак.ч

Длительность – 4 мес

Работа с преподавателем – 56 ак.ч

Самостоятельная работа – 214 ак. ч

АРХИТЕКТУРА ПРОГРАММЫ “АНАЛИТИК SOC”



Модуль 1. Обнаружение злоумышленника на этапе работы с внешним периметром

3 семинара, 12 ак.ч. встреч с преподавателем

- Техника обнаружения внешнего сканирования периметра
- Техника обнаружения сканирования на уязвимости
- Техника обнаружения подбора директорий. Фаззинг.
- Техника обнаружения атак на веб-сайты через SQL- инъекции
- Техника обнаружения атак на веб-сайты через межсайтовый скриптинг (XSS)
- Техника обнаружения атак на веб-сайты через подделку межсайтовых запросов (CSRF)
- Техника обнаружения атак на веб-сайты через обход механизмов авторизации
- Техника обнаружения атак на веб-сайты через path traversal
- Техника обнаружения подбора паролей на веб-ресурсы
- Техника обнаружения фишинговых атак

Модуль 2. Обнаружение злоумышленника на этапе разведки во внутренней сети

4 семинара, 16 ак.ч. встреч с преподавателем

- Техника обнаружения использования вредоносных утилит на Windows/Linux хостах
- Техника обнаружения аномальной активности рабочих процессов на хосте Windows
- Техника обнаружения аномальной активности на хостах Linux
- Техника обнаружения эксплуатации уязвимостей в Windows
- Техника обнаружения эксплуатации уязвимостей в Linux
- **Группа техник «Обнаружение атак на беспроводные сети»**
- Техника обнаружения атак на беспроводные сети. Подслушивание.
- Техника обнаружения атак на беспроводные сети. Подмена MAC-адресов клиентских устройств.
- Техника для выполнения и детектирования атаки деаутентификации на беспроводную сеть при помощи фреймворка De-auth
- Техника обнаружения атак на беспроводные сети. Ложные точки доступа (атака Evil Twin).
- Техника обнаружения атак на беспроводные сети. Подбор паролей.

АРХИТЕКТУРА ПРОГРАММЫ “АНАЛИТИК SOC”

Модуль 3. Обнаружение атак на доменную инфраструктуру, построенную на базе Windows Active Directory

6 семинаров, 24 ак.ч. встреч с преподавателем

- Техника обнаружения сбора информации об Active Directory
- Техника обнаружения классических методов быстрой компрометации внутри Active Directory
- Техника обнаружения взаимодействия с SAM и LSASS на хостах
- Техника обнаружения брутфорса и спрейинга пароля в Active Directory
- Техника обнаружения эксплуатации известных уязвимостей Active Directory
- Техника выявления перемещения по внутренней сети и в Active Directory
- Техника обнаружения атак на слабою конфигурацию службы сертификации в Active Directory
- Техника всестороннего контроля за Kerberos TGT
- Техника выявления использования атак Pass the ticket и pass the hash
- Техника выявления классических Kerberos атак
- Техника детектирования DCSync и DCShadow

Модуль 4. Обнаружение закрепления злоумышленника на хостах и анализ сетевого трафика

1 семинар, 4 ак.ч. встреч с преподавателем

- Обнаружение закрепления в windows машинах
- Обнаружение закрепления в Linux машинах
- Техника обнаружения вредоносной активности в сетевом трафике
- Техника обнаружения внутреннего сканирования (по портам, по хостам)

АРХИТЕКТУРА ПРОГРАММЫ “АНАЛИТИК SOC”

Модуль 5. Дополнительный. Техники атак хакера

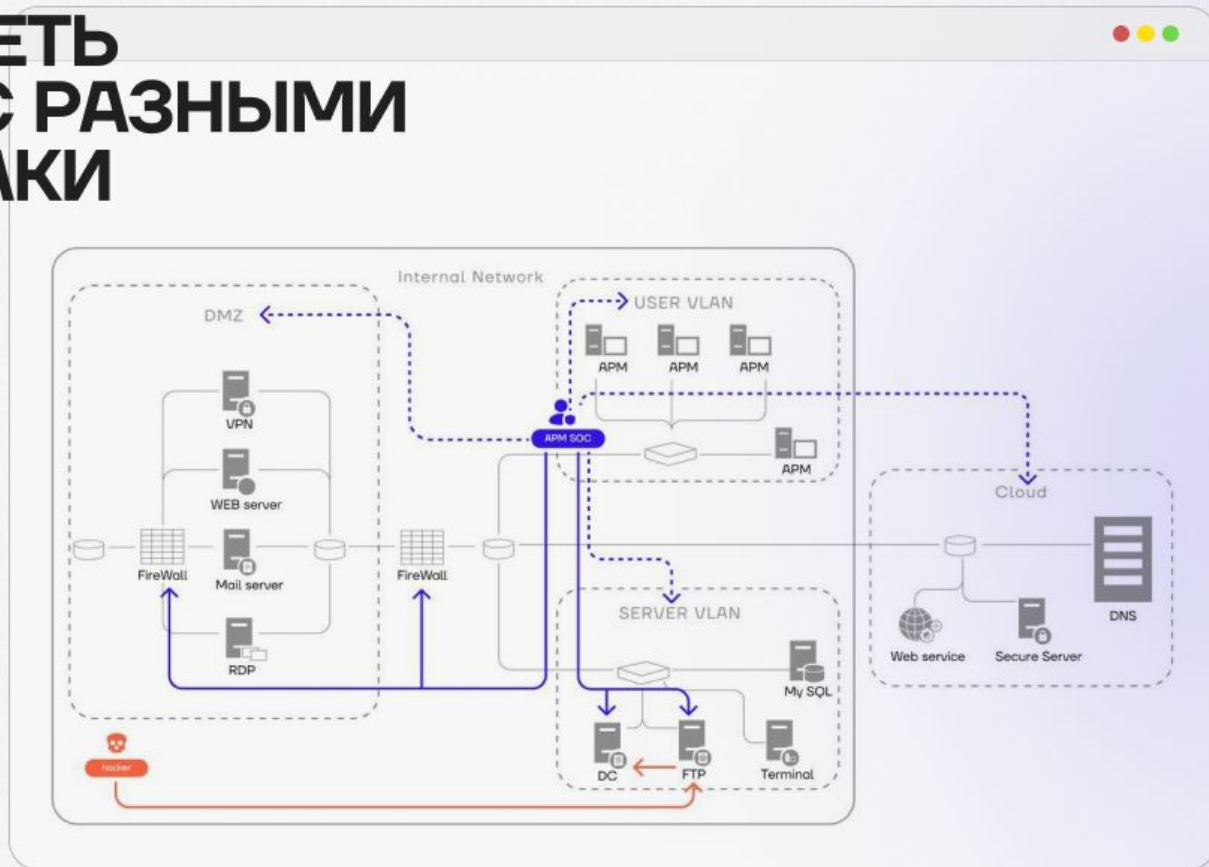
- Техника сканирования IP-адресов;
- Техника сканирования портов;
- Техника эксплуатации SQL injection Stacked queries;
- Техника эксплуатации SQL injection Union-based;
- Техника SQL injection Error-based;
- Техника эксплуатации OTP code bypass;
- Техника детектирования уязвимостей контроля доступа;
- Техника эксплуатации Directory/Path traversal;
- Техника онлайн-атак методом грубой силы;
- Техника брутфорса директорий и файлов на веб-сервере.

ВЫ БУДЕТЕ УМЕТЬ РАБОТАТЬ С РАЗНЫМИ ЭТАПАМИ АТАКИ

Будете уметь обнаруживать атаки

- как на этапе первоначального доступа злоумышленника.
- так и на этапах закрепления в элементах сети , повышения привилегий, бокового перемещения и др.

б) продвинутого уровня: на active directory, AD CS и др.



НАУЧИТЕСЬ ДУМАТЬ КАК АНАЛИТИК SOC

Потому что сами будете взламывать систему, чтобы понимать, как мыслит и действует атакующий и как обнаруживается каждая атака на:

■ Внешнем периметре и внутреннем

через одни из самых популярных техники атак на компании.

Модуль 5. Дополнительный. Техники атак хакера

- Техника сканирования IP-адресов;
- Техника сканирования портов;
- Техника эксплуатации SQL injection Stacked queries;
- Техника эксплуатации SQL injection Union-based;
- Техника SQL injection Error-based;
- Техника эксплуатации OTP code bypass;
- Техника детектирования уязвимостей контроля доступа;
- Техника эксплуатации Directory/Path traversal;
- Техника онлайн-атак методом грубой силы;
- Техника брутфорса директорий и файлов на веб-сервере.

СМОЖЕТЕ ПОНИМАТЬ И ПРЕДСКАЗЫВАТЬ ПОВЕДЕНИЕ АТАКУЮЩЕГО

Матрица MITRE ATT&CK-
фреймворк, который
описывает действия
атакующего

MITRE ATT&CK												Matrices	Tactics	Techniques	Defenses	CTI	Resources	Benefactors	Contribute	Blog	Search
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection											
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques											
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (3)	Abuse Elevation Control Mechanism (3)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)											
Gather Victim Host Information (4)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Scripting Interpreter (13)	BITS Jobs	Boot or Logon Autostart Execution (14)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)											
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Initialization Scripts (3)	Account Manipulation (7)	Build Image on Host	Credentials from Password Stores (3)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture											
Gather Victim Network Information (4)	Compromise Infrastructure (3)	External Remote Services	Deploy Container	Cloud Application Integration	Boot or Logon Autostart Execution (14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (3)	Automated Collection											
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (3)	Delay Execution	Forced Authentication	Cloud Service Dashboard	Remote Services (3)	Browser Session Hijacking											
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary	Create or Modify System Scripts (3)	Deobfuscate/Decode Files or Information	Forge Web Credentials (3)	Cloud Service Discovery		Clipboard Data											
Search Closed Sources (3)	Obtain Capabilities (7)	Replication Through Removable Media	Input Injection	Create or Modify System Binary	Create or Modify System Process (3)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage											
Search Open Technical Databases (3)	Stage Capabilities (3)	Supply Chain Compromise (3)	Inter-Process Communication (7)	Create or Modify System Process (3)	Domain or Tenant Policy Modification (3)	Direct Volume Access	Modify Authentication Process (3)	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository (3)											
Search Open Websites/Domains (3)		Trusted Relationship	Native API	Event Triggered Execution (13)	Escape to Host	Domain or Tenant Policy Modification (3)	Multi-Factor Authentication Interception	Device Driver Discovery	Taint Shared Content	Data from Information Repositories (3)											
Search Threat Vendor Data		Valid Accounts (4)	Poisoned Pipeline Execution	Event Triggered Execution (13)	Exploitation for Privilege Escalation	Email Spoofing	Multi-Factor Authentication Request Generation	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Local System											
Search Victim-Owned Websites		Wi-Fi Networks	Scheduled Task/Job (3)	Exclusive Control	Hijack Execution Flow (12)	Execution Guardrails (3)	Multi-Factor Authentication Request Generation	File and Directory Permissions Modification (3)		Data from Network Shared Drive											
			External Remote Services	Hijack Execution Flow (12)	Process Injection (12)	Hide Artifacts (14)	Network Sniffing	Local Storage Discovery		Data from Removable Media											
			Software Deployment Tools	Implant Internal Image	Modify Authentication Process (3)	Indicator Removal (13)	OS Credential Dumping (3)	Log Enumeration		Data Staged (3)											
			System Services (3)	Valid Accounts (4)	Indirect Command Execution	Impersonation	Steal Application Access Token	Network Service Discovery		Email Collection (3)											
			User Execution (3)	Modify Authentication Process (3)	Indirect Command Execution	Impersonation	Steal or Forge Authentication Certificates	Network Share Discovery		Input Capture (4)											
			Windows Management Instrumentation	Modify Authentication Process (3)	Indirect Command Execution	Impersonation	Steal or Forge Authentication Certificates	Network Sniffing		Screen Capture											



Это программа – маршрут

в интернете много материалов на год и больше.

на курсе эксперт дает вспомогательные материалы: книги, статьи, видео – после всего этого, если их вобрать в себя, ты будешь крут
самые глупые вопросы ты можешь задавать эксперту и быстрее расти.

Эксперт помогает в любых вопросах:

я правильно вот сюда иду? а я правильно понял, что вот так?



[АНАЛИТИК SOC]

РАЗБЕРЁМ НА КЕЙСАХ, КАК МЫ ОБУЧАЕМ

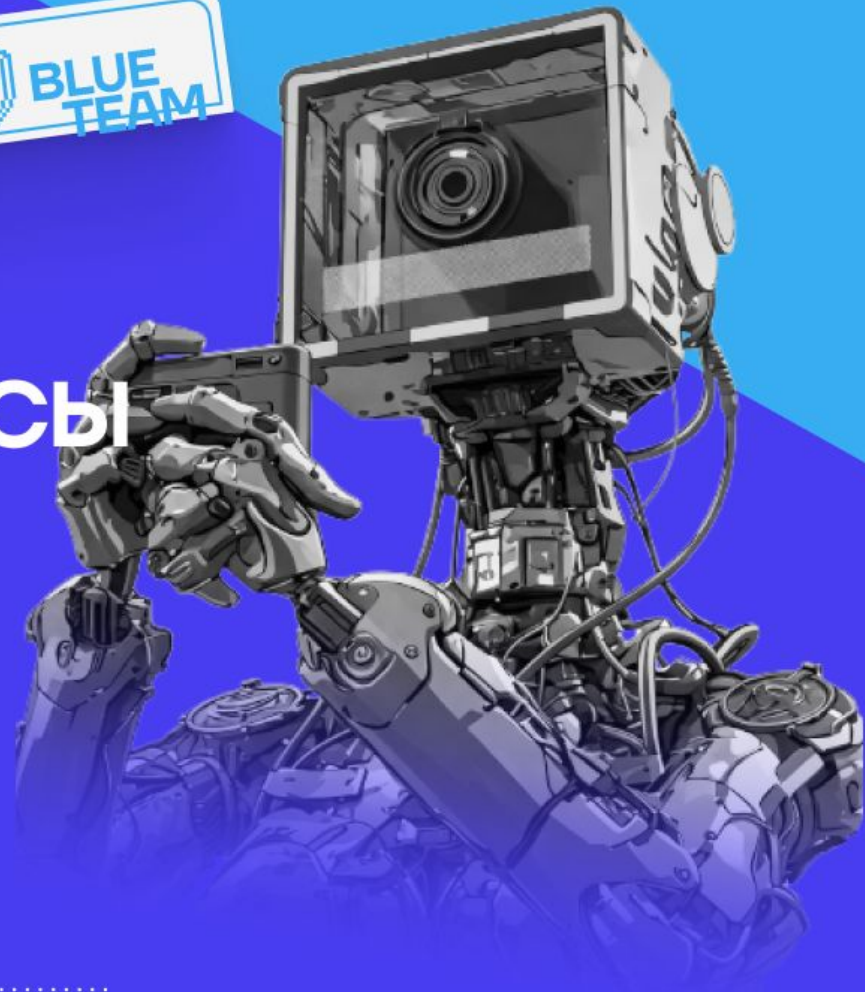


— Групповая консультация / Аналитик SOC —

CyberED



ЗАДАВАЙТЕ ВОПРОСЫ И КЕЙСЫ





ПОНИМАНИЕ ПОЛНОГО ЦИКЛА РАБОТЫ АНАЛИТИКА SOC +



Курс
**АНАЛИТИК
SOC**

+



**В ПОДАРОК 1
КУРС ПО
THREAT
INTELLIGENCE:**

инструменты анализа
киберугроз

Подарок только для
ближайшего старта

**ЛОГИЧНОЕ
ПРОДОЛЖЕНИЕ ДЛЯ
РОСТА АНАЛИТИКА SOC**



Чек-лист для роста
до грейдов:
от junior до senior



Доступ
к закрытому чату
с вакансиями в ИБ



3 карьерные
встречи
с экспертами по ИБ

Скидка 10%
при брони курса

