Чек-лист Карьерный путь аналитика SOC (Blue Team)

Аналитик Security Operations Center (SOC) сегодня — одно из самых востребованных направлений в ИБ. Аналитики Blue Team в SOC отвечают за мониторинг, обнаружение и реагирование на кибератаки. Работа строится на признанных фреймворках (NIST CSF, MITRE ATT&CK, Cyber Kill Chain).
Мы подготовили чек-лист компетенций с учётом актуальных техник, инструментов и фреймворков для трёх уровней: Junior (L1), Middle (L2) и Senior (L3). Отметьте, что уже знаете, изучайте навыки и двигайтесь шаг за шагом.

→ Для начальных позиций работодатели чаще всего требуют:

- Знания сетей и протоколов (OSI, TCP/IP, DNS/HTTP/SMTP/VPN);
- Базового администрирования Windows и Linux (логи, пользователи, службы);
- Умения работать с логами и простыми средствами защиты (SIEM/EDR, антивирус, почтовые/веб-шлюзы);
- Базового понимания MITRE ATT&CK и типовых инцидентов (фишинг, брутфорс, малварь на хосте).

→ В этом чек-листе вы найдёте:

- Фундаментальные компетенции, с которых стартует SOC-аналитик L1;
- Направления развития — от мониторинга и триажа до threat hunting, форензики и IR;
- Подсказку, что учить в первую очередь, чтобы выйти на рынок труда и расти до L2/L3.

I - Базовые знания и навыки для SOC (старт L1)

→ Приоритеты для старта

- Сети и протоколы: модель OSI, TCP/UDP, базовые разборы DNS/HTTP/SMTP/SMB/VPN; чтение NetFlow/sFlow и понимание, что видно/не видно по метаданным;
- ОС и логи: Windows Event Log (ключевые EventID: 4624/4625/4688/4776 и др.), Linux (syslog/auditd, auth.log), основы AD/LDAP, учётки/группы;
- SIEM-грамотность: что такое событие/источник/корреляция, базовые запросы (KQL/SPL/SQL-like, регулярные выражения (regex), работа с дашбордами и алертами, постановка тикетов;
- EDR/AV-консоль: просмотр алертов/процесс-деревьев, быстрая проверка хэшей/доменов, базовая изоляция хоста по регламенту;
- Инструменты повседневности: Wireshark/tcpdump для быстрой выборки, PowerShell/Bash для рутинного триажа, утилиты репутации (VT-подобные, whois/dig).

→ Следующий шаг

- Углубление логирования: установка и базовая настройка Sysmon (Windows) и auditd/osquery (Linux), централизованный сбор в SIEM;
- Детект-мышление: знакомство с MITRE ATT&CK, чтение Sigma-правил, понимание разницы IoC vs IoA/TTP, базовые охоты по аномалиям доступа;
- Скриптинг для триажа: PowerShell/Bash/Python для парсинга логов/артефактов;
- Практики IR: работа по плейбукам (фишинг, brute-force, подозрительный процесс/вложение), корректная эскалация и фиксация артефактов (скриншоты, хэши, логи).

Junior SOC-аналитик (L1)

Младший аналитик (первая линия) ведёт непрерывный мониторинг и первичную оценку инцидентов.

→ Основные компетенции:

- Мониторинг через SIEM и оповещения. Работа с SIEM (напр., Splunk, ELK/Elastic Stack, QRadar) для сбора/корреляции логов в реальном времени; быстрое отделение ложных срабатываний от реальных угроз.
- Первичный анализ и триаж. Следование IRP/SOP для типовых инцидентов; оперативная оценка критичности и релевантности алерта, обогащение контекстом и, при необходимости, регистрация инцидента для передачи выше; аккуратное документирование.
- Документирование и эскалация. Ведение журнала инцидентов (принятые меры/результат). Своевременная эскалация на L2 с полным пакетом собранной информации.
- Базовый анализ угроз и корреляция. Понимание основных типов атак и признаков компрометации; умение связать, например, подозрительные логи аутентификации с сетевыми событиями.
- Настройка и фильтрация. Участие в настройке мониторинга: корректировка правил/порогов, внесение легитимных событий в белые списки для снижения false positive и повышения точности детекции.
- Обучаемость и ИТ база. Основы сетей (OSI, TCP/IP, HTTP, DNS), ОС Windows/Linux и их журналы, базовый Bash/PowerShell; знакомство с отчётами об инцидентах; работа с базовыми инструментами (консоли антивирусов, EDR-агенты, тикет-системы).

Middle SOC-аналитик (L2)

Аналитик среднего уровня принимает эскалации от L1 и выявляет более тонкие угрозы, ушедшие от автоматики.

→ Основные компетенции:

- Глубокий анализ логов и данных. Ручной разбор разнородных журналов (ОС, брандмауэры, прокси, сетевые устройства, приложения, БД); поиск аномалий и скрытых IoC (последовательности команд, активность учёток, нетипичный трафик). Обязателен навык Wireshark для анализа пакетов, сессий и всплесков.
- Расследование и реагирование. Базовая форензика: сбор образцов ВПО, анализ дампов памяти, просмотр системных артефактов (в т. ч. используя YARA правила). Построение таймлайна атаки, определение метода проникновения и масштаба. Контейнмент: изоляция заражённых хостов, блокировка вредоносных IP/доменов, временные правила на файрволах. После нейтрализации — участие в восстановлении (патчи, изменение правил).
- Проактивный threat hunting. Поиск признаков скрытых атак, которые могли пройти мимо SIEM: анализ статистики активности учётных записей, аномалий времени/географии входов, сверка с актуальными IoC из TI-отчётов. Важно учитывать, что злоумышленники используют легитимные инструменты (пример: несанкционированная установка TeamViewer, не классифицируемая AV/EDR как вредоносная) — помогает внимательный контекстный анализ.
- Работа с Threat Intelligence. Регулярный просмотр сводок CERT/ISI/TI-платформ (напр., MISP, VirusTotal, ThreatCrowd), сверка IoC (IP/хэши/домены) с внутренними логами. Для серьёзных кейсов — атрибуция, понимание тактик и рекомендуемых мер.
- Детекты и улучшение процессов. Создание кастомных правил корреляции в SIEM, настройка сигнатур IDS/IPS, написание Sigma-правил; поддержание актуальности плейбуков реагирования с учётом новых техник.
- Наставничество и коммуникация. Помощь L1 в разборе кейсов, объяснение причинно-следственных связей, взаимодействие со смежными командами для совместного решения инцидента.

Senior SOC-аналитик (L3)

Ведущий эксперт, на которого эскалируются самые сложные инциденты; сочетает глубокую технику и стратегию.

→ Основные компетенции:

- Экспертное расследование и форензика. Глубокий разбор APT-активности и вредоноса: анализ памяти (Volatility, Rekall), диска, разборка кода (IDA Pro, Ghidra), сетевой анализ; формирование IoC и корректировка мер защиты.
- Проактивный Threat Hunting и ресёрч. Инициирование кампаний по актуальным сценариям, выявление несигнатурных аномалий; постоянное изучение новых техник (база MITRE ATT&CK), отчётов TI (атаки на облака, 0-day и методы эксплуатации) с переводом знаний в практические меры (детекты/конфигурации).
- Разработка средств защиты и автоматизация. Создание собственных инструментов/скриптов (напр., Python) для обработки логов, интеграции SIEM/TI/тикетинга, автоматического сбора артефактов; участие во внедрении/настройке SOAR для ускорения типовых инцидентов; ответственность за архитектуру мониторинга (оценка EDR/XDR, NDR, аналитических платформ) и оптимизацию стека.
- Обзор фреймворков и покрытие атак. Сопоставление возможностей мониторинга с ATT&CK/kill chain; запуск Purple Team-упражнений, проверка эффективности детектов по этапам; устранение «слепых зон» через новые use-case или контроли.
- Incident management и руководство ответом. Координация серьёзных инцидентов (в т. ч. шифровальщики): приоритеты (изоляция сегментов/сервисов), подключение IT/DevOps/внешних форензиков, коммуникация с менеджментом и, при необходимости, регуляторами/правоохранительными органами; обеспечение пост-инцидентного разбора.
- Оценка защищённости и улучшения. Участие в управлении уязвимостями и оценке рисков: планирование пентестов с Red Team/подрядчиками, анализ результатов сканеров (напр., Nessus, OpenVAS), приоритизация критичных уязвимостей; аудит конфигураций и соответствия стандартам (напр., CIS Controls, ISO 27001); отслеживание метрик SOC (время обнаружения/реагирования, доля инцидентов в срок) и выдача стратегических рекомендаций.
- Лидерство и развитие команды. Наставничество для всей Blue Team: тренинги, разбор сложных инцидентов, лучшие практики; планы развития для младших аналитиков, рекомендации по курсам и сертификациям.

Фундаментальные навыки

F402 - Инженер по информационной безопасности (Security Engineer)

F107 - Введение в информационную безопасность (Introduction to InfoSec)

F108 - Операционная система Linux (OS Linux)

F109 - Локальные сети (Local Area Network)

F110 - Доменная структура Windows (Windows Domain Infrastructure)

F111 - Администрирование СЗИ (Administration of Information Security Tool)

Эксплуатация средств и процессов информационной безопасности. Менеджмент в ИБ

Развитие в AppSec и DevSec

S235 - Основы безопасной разработки (Secure Development Fundamentals)

↓

S410 - Специалист по безопасной разработке приложений (Specialist in secure application development)

S232 - Безопасная разработка приложений в рамках SDL цикла (Security Development Lifecycle)

S224 - Безопасность окружения приложений (Applications Environment Security)

Развитие в Red Team

бесплатно

R101 - Профессия Белый хакер

R218 - Программирование на Python для пентестеров (Python Programming For Penetration Testing)

↓

R301 - Пентестер (Penetration Testing Specialist)

R301-GM1 - Тестирование на проникновение внешнего периметра компании(External Perimeter Penetration Testing)

R301-GM2 - Повышение привилегий в операционных системах (Operating System Privilege Escalation)

R301-GM3 - Тестирование на проникновение локальных сетей компаний (Local Network Penetration Testing)

↓

R319 - Анализ защищенности веб-приложений (Web Application Security Analysis)

R220 - Анализ безопасности мобильных приложений (Mobile Application Security Analysis)

Развитие в Blue Team

бесплатно

B101 - Специалист по противодействию кибератакам

↓

B301 - Аналитик Центра противодействия кибератакам (Security Operations Center Analyst)

↓

B410 - Специалист по защите корпоративной инфраструктуры (Corporate Infrastructure Protection Specialist)

B207 - Угрозы корпоративной инфраструктуры (Cyber Infrastructure Threats)

B208 - Системы Информационной Безопасности (Information Security Systems)

B228 - Аналитик SOC (Security Operations Center Analyst)

↓

B236 - Реагирование на инциденты и компьютерная криминалистика в ОС Windows (Digital Forensics and Incident Response in Windows OS)

TIA - Кибербразведка: Threat Intelligence

→ Карьерный путь в SOC — это движение от мониторинга по инструкциям к сложным расследованиям, охотам по TTP и, в итоге, к управлению инцидентами, архитектурой мониторинга и автоматизацией.

Если хотите получить системные знания и практику под руководством экспертов — подключайтесь к нашим курсам. Там вы сможете пройти путь от L1-мониторинга и работы с SIEM/EDR до Threat Intelligence и компьютерной криминалистики.

