Бнятов Сергей Иванович

Мужчина, 32 года, родился 26 июня 1993

+7 (987) 5530342
+7 (987) 5530342
deepdata@protonmail.com — предпочитаемый способ связи
Telegram: https://t.me/na_soc

Проживает: Москва
Гражданство: Россия, есть разрешение на работу: Россия
Не готов к переезду, готов к командировкам

Желаемая должность и зарплата

Руководитель SOC

Специализации:
— Специалист по информационной безопасности
Тип занятости: полная занятость
Формат работы: удалённо, на месте работодателя
Желательное время в пути до работы: не имеет значения

Опыт работы — 10 лет 8 месяцев

Июнь 2023 — настоящее время
2 года 11 месяцев

Ecom.tech

Москва, ecom.tech
Информационные технологии, системная интеграция, интернет
• Разработка программного обеспечения

Head of SOC and Incident Response

Head of SOC and Incident Response (Холдинг, 4 компании)

Управляю сервисной командой SOC (12 человек), обеспечивающей мониторинг и реагирование на инциденты для 4 самостоятельных компаний внутри холдинга.

Построил гибридную модель SOC: внутренняя команда + MSSP-провайдер.

Пережил три этапа объединений и реорганизаций компаний, адаптировал процессы SOC под новые организационные модели.

Вёл расследование инцидентов, связанных с компрометацией сервисов и инфраструктуры (без права раскрытия деталей); осуществлял сбор, анализ и обработку артефактов, атрибуцию причин возникновения инцидентов, написания отчетов.

Знаком с FortiSIEM, ELK/OpenSearch, QRadar на уровне настройки процессов мониторинга, управления инцидентами и контроля качества корреляций.

Организовал разработку внутренних решений: приложение для учёта активов безопасности, телеграм-боты для алертинга, проверки IOC и поддержки расследований и другие.

Подготавливаю регулярные отчёты для топ-менеджмента: показатели эффективности SOC, инцидентные сводки, рекомендации по снижению рисков.

Прошёл внешний аудит от одного из крупнейших банков: подготовка процессной документации, защита архитектуры и процессов SOC.

Планировал бюджет SOC, вёл закупку и внедрение ключевых решений: MSSP, SOAR, TI-платформа, Brand Protection, SIEM, EDR.

Март 2022 — Июнь 2023
1 год 4 месяца

Самокат (ООО Умное пространство)

Москва, samokat-team.ru

Информационные технологии, системная интеграция, интернет

- Интернет-компания (поисковики, платежные системы, соц.сети, информационно-познавательные и развлекательные ресурсы, продвижение сайтов и прочее)
- Разработка программного обеспечения
- Системная интеграция, автоматизация технологических и бизнес-процессов предприятия, ИТ-консалтинг

Розничная торговля

- Розничная сеть (продуктовая)
- Интернет-магазин

Senior Cyber Security Engineer

- Make DevSecOps process
- Penetrations testing company resources
- Analyze network perimeter
- Analyze Data leaks
- Make Digital Risk Protection process
- OSINT
- Cyber Security Research
- Developing internal security tools (Analyze Cybersquatting, Analyze Leaks, Security Monitoring)

Ноябрь 2021 — Март 2022
5 месяцев

Buyk Corp

Москва

Senior Cyber Security Engineer

- AWS security analyze
- Make DevSecOps process
- Penetrations testing company resources
- Analyze network perimeter
- OSINT
- Digital Risk Protection
- Cyber Security Research

Сентябрь 2019 — Ноябрь 2021
2 года 3 месяца

АльфаСтрахование

Москва, www.alfastrah.ru

Финансовый сектор

- Страхование, перестрахование

Head Cyber Security Analyst

- RedTeam&BlueTeam
- Анализ защищенности web-приложений
- Анализ защищенности мобильных приложений
- Анализ защищенности внешнего периметра компании
- Анализ защищенности внутреннего периметра компании
- Участие в расследовании инцидентов ИБ
- OSINT
- Консультирование команд и бизнеса в вопросах ИБ
- Работа с поставщиками ИБ услуг, в качестве заказчика
- Участие в построение DevSecOps

Октябрь 2017 — Сентябрь 2019
2 года

ФГУП НПП ГАММА

Москва

Информационные технологии, системная интеграция, интернет

- Разработка программного обеспечения
- Системная интеграция, автоматизация технологических и бизнес-процессов предприятия, ИТ-консалтинг

Инженер

Работа по направлению сертификации программно-аппаратных комплексов по линии ФСТЭК,ФСБ,МО.

- Анализ уязвимостей в соответствии с требованиями регулятора
- Разработка методик тестирования
- Разработка и внедрение новых вектор\инструментов для проведения анализа уязвимостей
- Расследование инцидентов информационной безопасности
- Взаимодействие с SOC в качестве эксперта по ИБ
- Проведение тестов на проникновения внешний\внутренний периметр
- Разработка и поиск новых вектор атаки для пентестов
- Разработка инструментов для проведения и демонстрации APT атак
- Работы по Web application Fuzzing
- Опыт разработки на C# (утилиты для автоматизации, клиент-сервер и.т.п.).

Ноябрь 2016 — Октябрь 2017
1 год

Индивидуальное предпринимательство / частная практика / фриланс

Нижний Новгород

Специалист по информационной безопасности

Анализ защищенности сетевых и информационных инфраструктур;

Анализ защищенности и составление рекомендаций и правил пользования для мобильного сегмента заказчика (телефоны, планшеты и прочие гаджеты);

Выявления угроз ИБ на основе сведений об уязвимостях (классификация угроз, формирование рекомендаций по устранению уязвимостей и минимизации бизнес-рисков);

Приведение организации в соответствие ФЗ 152 как с документальной стороны так и с технической;

Сентябрь 2015 — Ноябрь 2016
1 год 3 месяца

TLC group

Специалист по информационной безопасности

• Анализ защищенности сетевых и информационных инфраструктур;
• Анализ защищенности и составление рекомендаций и правил пользования для мобильного сегмента заказчика (телефоны, планшеты и прочие гаджеты);
• Выявления угроз ИБ на основе сведений об уязвимостях (классификация угроз, формирование рекомендаций по устранению уязвимостей и минимизации бизнес-рисков);
• Работа с основными методиками, классификациями и международными практиками (OSSTMM, OWASPи др.);
• Разработка нормативных и регламентирующих правил по работе с компрометирующей и конфиденциальной информацией;
• Разработка и применение на практике новых методик пентеста и таргетированных векторов атаки;
• Проведение полного цикла социотехническогопентеста: соц-инженерия, фишинг, и.т.п.;
• Участие в проектах по тестированию на проникновение в режимах white,grey,black-box;
• Постоянный мониторинг рынков продажи специализированного ПО для проведения атак и тестирования;
• Разработка и проектирования собственного инструментария для пентеста и аудита информационных систем;

• Проектирование системы для тестирования детектов рабочего инструментария, на современных антивирусных системах;
• Составления отчетов о состоянии ИС, рекомендации заказчикам по исправлению и устранению угроз, аналитика и аудит ИС;
• Опыт работы с Kali Linux, VPN, TOR;
• Опыт работы с современным инструментарием для анализа web-application (Acunetix, Burp, OwaspZAP);
• Небольшой опыт написания простых скриптов на: (JS, PS);
• Опыт разработки на C# (утилиты для автоматизации, клиент-сервер и.т.п.).
• Опыт работы с инструментом упаковки файлов nsis.

Образование

Магистр

2016
Магистр

Нижегородский государственный университет им. Н.И. Лобачевского (Национальный исследовательский университет), Нижний Новгород
Институт информационных технологий математики и механики, Магистр

2014
Магистр

Нижегородский государственный университет им. Н.И. Лобачевского (Национальный исследовательский университет), Нижний Новгород
Факультет вычислительной математики и кибернетики (ВМК), Бакалавр

Тесты, экзамены

2021

ВКС-IH Moscow
ВКС-IH Moscow, General English Pre-Intermediate

Электронные сертификаты

2021

DevSecOps : Master Securing CI/CD | DevOPs Pipeline(2021)
Learn C# Course
Learn Java Course
Learn JavaScript Course
Learn PHP Course
Learn Python 3 Course
Software Design as an Element of the Software Development Lifecycle

Навыки

Знание языков

Русский — Родной
Английский — B1 — Средний

Навыки

OSINT · Kali Linux · ELK · SOAR · BlueTeam · Incident Response · Digital Risk Protection · Brand Protection · Python Development for Security Operations · Security Product Development · Budgeting and Vendor Management · MSSP Management and Integration · Asset Security Management · Post-Incident Review · Leadership Skills · Team management · SOC Operations

Executive Reporting for Top-Management IBM QRadar FortiSIEM EDR Threat Hunting

Опыт вождения

Имеется собственный автомобиль
Права категории B

Дополнительная информация

Обо мне

Автор Telegram-канала «Строим SOC in-house» — https://t.me/na_soc

Спикер на отраслевых конференциях по информационной безопасности.

Разрабатываю внутренние продукты для автоматизации работы SOC.

Активный участник HackTheBox: развитие навыков offensive security — https://www.hackthebox.eu/home/users/profile/278008

Интересуюсь применением Big Data и ML для оптимизации мониторинга угроз.

Ориентирован на построение зрелых, масштабируемых процессов безопасности.

Развиваю управленческие навыки и наставничество команд SOC.

Иногда пишу статьи на https://habr.com/, можно почитать тут:
https://habr.com/ru/post/538774/
https://habr.com/ru/post/545132/
https://habr.com/ru/post/554416/

Выступления:

VK Security MeetUP 2023 — «Купил SOC — оказался носок»
https://vk.com/video-164978780_456239308

OFFZONE 2024 — «Как картинки в интернете забирают твои деньги и данные»
https://vkvideo.ru/playlist/-172362100_11/video-172362100_456239202

Ecom.tech Security MeetUP 2024 — «Как не сойти с ума в SOC? Объединения, изменения, процессы, боли»
https://www.youtube.com/live/pyaiG613xgY

BiZone Day 2024 — «Опыт работы с MSSP глазами заказчика» (закрытое мероприятие)

CISO Forum 2025 — «Приоритизация инцидентов, или как не утонуть в бесконечном потоке»

Интересно всё новое и сложное, не останавливаюсь на достигнутом, всегда стараюсь идти вперёд и открывать новое.
Не хочу тратить время на никому не нужную или неинтересную работу.
Есть желание развиваться и совершенствоваться в профессиональной области.
Не боюсь трудностей и новой, незнакомой для меня работы, области или технологии.
Ответственно подхожу к тому, что делаю.
Играю в волейбол, люблю читать интересные книги, пишу музыку.