АНАЛИТИК SOC L1 · DFIR · PENTEST

Филипп Огородников

SOC-аналитик L1, развивающийся в направлении Purple Team

Москва +7 912 105-98-28 scrockwork@gmail.com t.me/scrock_0 resume.scrock.ru

Профессиональный профиль

Действующий аналитик SOC L1. Самостоятельно разбираю алерты SIEM: составляю KQL-запросы в Elastic, определяю масштаб события, закрываю или эскалирую его и готовлю рекомендации. Развиваю практику DFIR и атакующих техник на лабораторных стендах, чтобы работать на стыке обнаружения, расследования и проверки защищённости. Есть опыт преподавания студентам и экспертной оценки участников профильных соревнований.

Опыт работы

Младший аналитик SOC L1

октябрь 2025 — настоящее время

UserGate

- Получаю и самостоятельно разбираю алерты SIEM: определяю масштаб, закрываю либо эскалирую события и формирую рекомендации.
- Пишу KQL-запросы и расследую события в Elastic.
- Анализирую журналы Windows и Linux; участвовал в написании правил детектирования для Elastic.

Участник команды #au.team

июнь 2024 — настоящее время

Лаборатория сетей и систем передачи информации

- Исследую и администрирую учебные стенды по сетям и информационной безопасности.
- Разрабатываю лабораторные работы и провожу занятия для студентов.
- Разворачивал Windows-стенд во вложенной виртуализации VMware / VirtualBox и публиковал ресурсы для внутреннего использования.

Эксперт компетенций

2024 — 2025

Росатом · АтомЛаб · SHIFT

- Разрабатывал задания, проверял решения, оценивал и консультировал участников, проводил профильные занятия.
- Направления работы: сетевое и системное администрирование, кибербезопасность и компьютерная криминалистика.

Образование

РГУ нефти и газа (НИУ) имени И. М. Губкина

2021 — настоящее время

10.05.03 «Информационная безопасность автоматизированных систем», специалитет

Технические навыки

SOC и реагирование	Разбор и реагирование на алерты; Elastic и KQL; анализ фишинга, подозрительных PDF и активности на конечных точках; сдерживание инцидентов; KUMA и PT MaxPatrol SIEM; KATA; журналы Windows и Linux; MITRE ATT&CK.
DFIR	Артефакты Windows и браузеров; анализ файловых систем и восстановление данных; создание и проверка образов; Autopsy, FTK, Volatility; анализ памяти и подозрительных файлов; сохранение доказательств и подготовка отчётов.
Pentest	Практика на лабораторных стендах: разведка, ручное тестирование веб-приложений, эксплуатация, повышение привилегий, анализ и атаки на Active Directory, lateral movement, post-exploitation, закрепление и подготовка отчётов.
Системы и сети	Linux и российские ОС; Windows и Active Directory; усиление защищённости систем; TCP/IP, VLAN, STP, маршрутизация, DNS, DHCP, NAT, VPN, Wireshark; администрирование NGFW; виртуальные лаборатории; базовое знакомство с облаками.
Автоматизация	Скрипты на Python и Bash для рабочих и лабораторных задач; интеграции систем безопасности и обогащение событий через API; PowerShell и SQL; Docker и Git; базовое знакомство с Ansible, Terraform и CI/CD.

Достижения

- **Кандидат в мастера спорта** по спортивному программированию, приказ № 186 от 18 июня 2026 года.
- **2 место** на Кубке России 2026 года по спортивному программированию в дисциплине «программирование продуктовое».
- **1 место** в соревнованиях по информационной безопасности Consyst-CTF, 2025 год.
- **4 научные публикации** по инфраструктуре киберполигона, российским ОС и информационной безопасности.
- Более 40 соревновательных и экспертных событий в информационной безопасности и системном администрировании.

Дополнительное обучение

- Школа преподавателей кибербезопасности Positive Technologies, 2024–2025.
- Курсы и практические программы по Astra Linux, Альт, РЕД ОС, ROSA Linux, сетевому администрированию, PT Network Attack Discovery и NGFW.

Дополнительная информация

Английский: B1, чтение технической документации.

Формат работы: удалённый / гибридный.

Дата рождения: 22.02.2003.

Подтверждающие документы и полная хронология: https://resume.scrock.ru/it-path