Brett K. Fry

Эксперт по кибербезопасности & Разработчик.

fryonline.net • github.com/fryguy01 • frydigitalsolutions.com

ПРОФЕССИОНАЛЬНЫЙ ПРОФИЛЬ

Я — Бретт Фрай, специалист по кибербезопасности и разработчик с более чем двумя десятилетиями практического опыта защиты критической инфраструктуры в военных и корпоративных средах. От руководства совместными операциями по охоте за угрозами в USAFRICOM до управления засекреченными аккаунтами COMSEC в многонациональных учениях — я строил карьеру на пересечении наступательных знаний и оборонного мастерства. Ветеран армии США • Базируется в Европе • Доступен по всему миру для консалтинга, киберзащиты и разработки под заказ.

ПРОФЕССИОНАЛЬНЫЙ ОПЫТ

Ведущий аналитик/планировщик оборонительных кибероперaций

USAFRICOM

Сен 2021 – Май 2025

- Руководил совместными операциями по охоте за угрозами и оборонительными кибероперациями. Разрабатывал обнаружения на основе разведки, плейбуки и системы отчётности для повышения киберустойчивости организации.

Старший специалист по реагированию на инциденты / защитник киберсети

Армия США

Авг 2018 – Сен 2021

- Выполнял функции ISSM в засекреченных анклавах. Руководил реагированием на инциденты, охотой за угрозами и инженерией обнаружения, улучшая рабочие процессы автоматизации и эффективность SOC.

Старший менеджер аккаунта COMSEC / защитник киберсети

Армия США

Окт 2016 – Июл 2018

- Управлял средствами защищённой связи и деятельностью по киберзащите. Согласовывал соответствие требованиям, управление рисками и операции для защиты критически важных систем.

Специалист по сетевым операциям

Армия США

Мар 2013 – Окт 2016

- Эксплуатировал и обслуживал стратегическую сетевую инфраструктуру для поддержки многонациональных учений. Повышал время безотказной работы через проактивный мониторинг.

ТЕХНИЧЕСКИЕ НАВЫКИ

SIEM / Операции SOC
Splunk (SPL), Microsoft Sentinel (KQL), ELK Stack, Сортировка оповещений, Detection Engineering, SOAR Workflows

Разведка угроз
OSINT, GIAC GCTI, Обогащение IOC/TTP, Pivot DNS/WHOIS, Профилирование акторов угроз, MITRE ATT&CK;, CTI Lifecycle

Реагирование на инциденты & DFIR
GIAC GCIH, GIAC GCFA, Wireshark, Tcpdump, Корреляция логов, Форензический анализ, Анализ вредоносных программ

Тестирование на проникновение
GIAC GPEN, GIAC GWAPT, Metasploit, Burp Suite, Red Team Ops, Adversary Emulation, Purple Team Testing

Облако и Endpoint
AWS, Azure, CrowdStrike, SentinelOne, Шлюзы Email/Web, GIAC GCTD, Облачная безопасность

Управление & Соответствие
NIST 800-53, RMF / eMASS, ATO, ISSM/ISSO, DISA CCRI, Zero Trust, GIAC GDSA

Автоматизация & Разработка
Python, Bash, PowerShell, Правила YARA, PHP, Java, JavaScript, C/C++

Инфраструктура
Red Hat Linux, NGINX, Windows Server, MySQL, Cisco, SUSE Linux, Сетевая архитектура

ОБРАЗОВАНИЕ

Аспирантский сертификат по киберзащите
SANS Technology Institute • 2024
Интенсивный аспирантский курс с акцентом на современные методологии и операции киберзащиты.

M.S. Information Security Engineering
SANS Technology Institute • 2022
Аспирантская программа, посвящённая передовым принципам инженерии информационной безопасности.

B.S. Digital Media & Web Technology
University of Maryland University College • 2015 • GPA 4.0 / 4.0

B.S. Computer Science
University of Maryland University College • 2015 • GPA 4.0 / 4.0

СЕРТИФИКАЦИИ

- GDAT
- GOSI
- GCTD
- GWEB
- GSOC
- GAWN
- GDSA
- GWAPT
- GCPM
- GCWN
- GSLC
- GCFA
- GMON
- GCTI
- GCCC
- GCFE
- GSNA
- GPEN
- GCIA
- GCIH
- GPYC
- GCED
- GSEC
- CompTIA Security+
- CompTIA Network+
- CompTIA Linux+
- CEH
- EC-Council CNDA
- LPIC-1
- Cisco CCAI
- SUSE CLA
- XM-Cyber