

Brett K. Fry

Експерт з кібербезпеки & Розробник.

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

ПРОФЕСІЙНИЙ ПРОФІЛЬ

Я — Бретт Фрай, фахівець з кібербезпеки та розробник з понад двома десятиліттями практичного досвіду захисту критичної інфраструктури у військових та корпоративних середовищах. Від керівництва спільними операціями полювання на загрози у USAFRICOM до управління засекреченими обліковими записами COMSEC у багатонаціональних навчаннях — я побудував свою кар'єру на перетині наступальних знань та оборонної майстерності. Ветеран Армії США • Базується в Європі • Доступний у всьому світі для консалтингу, кіберзахисту та розробки на замовлення.

ПРОФЕСІЙНИЙ ДОСВІД

Провідний аналітик/планувальник оборонних кібероперацій

USAFRICOM

Вер 2021 – Тра 2025

- Керував спільними операціями полювання на загрози та оборонними кіберопераціями. Розробив розвідувально-орієнтовані виявлення, плейбуки та звітні фреймворки для підвищення кіберстійкості організації.

Старший спеціаліст з реагування на інциденти / захисник кібермережі

Армія США

Сер 2018 – Вер 2021

- Виконував функції ISSM у засекречених анклавах. Керував реагуванням на інциденти, полюванням на загрози та інженерією виявлення, покращуючи робочі процеси автоматизації та ефективність SOC.

Старший менеджер облікового запису COMSEC / захисник кібермережі

Армія США

Жов 2016 – Лип 2018

- Управляв засобами безпечного зв'язку та діяльністю з кіберзахисту. Узгоджував відповідність, управління ризиками та операції для захисту критично важливих систем у багатонаціональних середовищах.

Фахівець з мережевих операцій

Армія США

Бер 2013 – Жов 2016

- Експлуатував та обслуговував стратегічну мережеву інфраструктуру для підтримки багатонаціональних навчань. Підвищував час безвідмовної роботи завдяки проактивному моніторингу.

ТЕХНІЧНІ НАВИЧКИ

SIEM / Операції SOC

Splunk (SPL), Microsoft Sentinel (KQL), ELK Stack, Сортуння сповіщень, Detection Engineering, SOAR Workflows

Реагування на інциденти & DFIR

GIAC GCIN, GIAC GCFA, Wireshark, Tcpdump, Кореляція логів, Форензичний аналіз, Аналіз шкідливого ПЗ

Розвідка загроз

OSINT, GIAC GCTI, Збагачення IOC/TTP, Pivots DNS/WHOIS, Профілювання акторів загроз, MITRE ATT&CK, CTI Lifecycle

Тестування на проникнення

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

Хмара та Endpoint

AWS, Azure, CrowdStrike, SentinelOne, Email/Web Gateways, GIAC GCTD, Хмарна безпека

Автоматизація & Розробка

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

Управління & Відповідність

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

Інфраструктура

Red Hat Linux, NGINX, Windows Server, MySQL, Cisco, SUSE Linux, Мережева архітектура

ОСВІТА

Аспірантський сертифікат з кіберзахисту

SANS Technology Institute • 2024

Іntenсивний аспірантський курс з сучасних методологій та операцій кіберзахисту.

M.S. Information Security Engineering

SANS Technology Institute • 2022

Аспірантська програма, зосереджена на передових принципах інженерії інформаційної безпеки.

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

СЕРТИФІКАЦІЇ

- 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