

Brett K. Fry

Esperto di Cybersecurity & Sviluppatore.

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

PROFILO PROFESSIONALE

Sono Brett Fry — professionista della cybersecurity e sviluppatore con oltre due decenni di esperienza pratica nella protezione di infrastrutture critiche in ambienti militari e aziendali. Dalla guida di operazioni congiunte di threat hunting presso USAFRICOM alla gestione di account COMSEC classificati in esercitazioni multinazionali, ho costruito la mia carriera all'incrocio tra conoscenza offensiva ed eccellenza difensiva. Veterano dell'Esercito USA • Basato in Europa • Disponibile a livello globale per consulenza, difesa cyber e sviluppo su misura.

ESPERIENZA PROFESSIONALE

Analista/Pianificatore Lead di Operazioni Cyber Difensive

USAFRICOM

Set 2021 – Mag 2025

- Ha guidato operazioni congiunte di threat hunting e cyber difensivo in ambienti enterprise e ad alta sicurezza. Ha costruito rilevamenti basati sull'intelligence, playbook e framework di reporting per migliorare la resilienza cyber.

Senior Incident Responder / Cyber Network Defender

US Army

Ago 2018 – Set 2021

- Ha operato come ISSM in enclavi classificate. Ha guidato incident response, threat hunting e detection engineering migliorando i flussi di automazione e l'efficacia del SOC.

Senior COMSEC Account Manager / Cyber Network Defender

US Army

Ott 2016 – Lug 2018

- Ha gestito asset di comunicazione sicura e attività di cyber difesa. Ha allineato conformità, gestione del rischio e operazioni per proteggere sistemi mission-critical in ambienti multinazionali.

Specialista in Operazioni di Rete

US Army

Mar 2013 – Ott 2016

- Ha operato e mantenuto infrastrutture di rete strategiche a supporto di esercitazioni multinazionali. Ha migliorato uptime e affidabilità tramite monitoraggio proattivo.

COMPETENZE TECNICHE

SIEM / Operazioni SOC

Splunk (SPL), Microsoft Sentinel (KQL), ELK Stack, Alert Triage, Detection Engineering, SOAR Workflows

Incident Response & DFIR

GIAC GCIH, GIAC GCFA, Wireshark, Tcpdump, Correlazione log, Analisi forense, Analisi malware

Cloud & Endpoint

AWS, Azure, CrowdStrike, SentinelOne, Gateway Email/Web, GIAC GCTD, Sicurezza Cloud

Threat Intelligence

OSINT, GIAC GCTI, Arricchimento IOC/TTP, Pivot DNS/WHOIS, Profilazione attori, MITRE ATT&CK, CTI Lifecycle

Penetration Testing

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

Governance & Compliance

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

Automazione & Sviluppo

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

Infrastruttura

Red Hat Linux, NGINX, Windows Server, MySQL, Cisco, SUSE Linux, Architettura di rete

FORMAZIONE

Certificato Post-Laurea in Cyber Defense

SANS Technology Institute • 2024

Focus intensivo di livello post-laurea su metodologie e operazioni moderne di cyber defense.

M.S. Information Security Engineering

SANS Technology Institute • 2022

Programma post-laurea focalizzato su principi avanzati di ingegneria della sicurezza informatica.

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

CERTIFICAZIONI

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