

# Brett K. Fry

Cybersecurity Expert & Developer.

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

---

## PROFESSIONAL SUMMARY

---

I'm Brett Fry — a cybersecurity professional and developer with over two decades of hands-on experience securing critical infrastructure across military and enterprise environments. From leading joint threat hunting operations at USAFRICOM to managing classified COMSEC accounts across multinational exercises, I've built my career at the intersection of offensive knowledge and defensive excellence. US Army veteran • Europe-based • Available globally for consulting, cyber defense, and custom development engagements.

## PROFESSIONAL EXPERIENCE

---

### Lead Defensive Cyber Operations Analyst / Planner

USAFRICOM

Sep 2021 – May 2025

- Led joint threat hunting and defensive cyber operations across enterprise and high-security environments. Built intelligence-driven detections, playbooks, and reporting frameworks to improve organizational cyber resilience.

### Senior Incident Responder / Cyber Network Defender

US Army

Aug 2018 – Sep 2021

- Served as ISSM across classified enclaves. Led incident response, threat hunting, and detection engineering while improving automation workflows and SOC effectiveness.

### Senior COMSEC Account Manager / Cyber Network Defender

US Army

Oct 2016 – Jul 2018

- Managed secure communications assets and cyber defense activities. Aligned compliance, risk management, and operations to protect mission-critical systems across multinational environments.

### Network Operations Specialist

US Army

Mar 2013 – Oct 2016

- Operated and maintained strategic network infrastructure supporting multinational exercises. Improved uptime and reliability through proactive monitoring and troubleshooting.

## TECHNICAL SKILLS

---

### SIEM / SOC Operations

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

### Incident Response & DFIR

GIAC GCIH, GIAC GCFA, Wireshark, Tcpdump, Log Correlation, Forensic Analysis, Malware Analysis

### Cloud & Endpoint

AWS, Azure, CrowdStrike, SentinelOne, Email/Web Gateways, GIAC GCTD, Cloud Security

### Threat Intelligence

OSINT, GIAC GCTI, IOC/TTP Enrichment, DNS/WHOIS Pivots, Threat Actor Profiling, 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

## Automation & Development

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

## Infrastructure

Red Hat Linux, NGINX, Windows Server, MySQL, Cisco, SUSE Linux, Network Architecture

## EDUCATION

---

### Graduate Certificate in Cyber Defense

[SANS Technology Institute](#) • 2024

Intensive graduate-level focus on modern cyber defense methodologies and operations.

### M.S. Information Security Engineering

[SANS Technology Institute](#) • 2022

Graduate-level program focused on advanced information security engineering principles.

### 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

## CERTIFICATIONS

---

- 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