Brett K. Fry

Cybersecurity Leader | DCO / SecOps Planning | Threat Hunting & Detection Engineering | Incident Response

Grand Prairie, TX • Open to US & Europe • Remote/Hybrid | brett.k.fry@… | +1 (210) 526-4589 | +49 15164345445 | https://www.fryonline.net/ | https://www.linkedin.com/in/brettfry2002

Summary

Cybersecurity and secure communications professional with 20+ years of US Army experience spanning Defensive Cyber Operations (DCO), security operations/continuous monitoring, incident response support, and COMSEC program management.
Leads joint/CCMD Defensive Cyber Operations (DCO) planning using deliberate and crisis action planning (JOPP/JOPES-aligned), translating mission objectives into executable cyber and C4I/enterprise IT plans.
Specializes in ATT&CK-aligned; threat hunting, detection engineering, and telemetry-driven investigations across SIEM/EDR/network/cloud sources; experienced producing executive-ready reporting and remediation plans.
Graduate-level focus areas include auditing & monitoring, CIS Critical Controls, intrusion detection, incident handling, cyber threat intelligence, and defensible security architecture/engineering.
Proven record (evaluation-documented) of improving readiness and inspection outcomes through disciplined accountability, policy/process development, and hands-on training/mentoring.
Open to US and Europe opportunities (remote/hybrid); available for travel and on-site engagements as needed.

Core Competencies

Threat Hunting & Detection Engineering (MITRE ATT&CK;), SIEM Content & Analytics (Splunk / ELK / Sentinel; SPL/KQL), Incident Response Support & DFIR (endpoint, log, network), Cyber Threat Intelligence (OSINT, IOC/TTP enrichment), Cloud Threat Detection Concepts (AWS / Azure / GCP), Vulnerability Assessment & Web App Testing, NIST / RMF / eMASS / ATO Support, COMSEC / KMI Program Leadership, Executive Communication, Training & Mentorship

Experience

Lead Defensive Cyber Operations Analyst/Planner — USAFRICOM
Defensive Cyber Operations • Stuttgart, Germany • Sep 2021 – May 2025

- Led a 27-member cyber threat hunting and defensive cyber operations (DCO) team within a Joint/Combatant Command (CCMD) environment, developing proactive cyber threat detection strategies and ensuring mission-critical security resilience.
- Directed advanced threat hunting and adversarial simulations to detect persistent threats, behavioral anomalies, and attack vectors in enterprise IT and embedded systems.
- Designed and executed offensive security assessments using MITRE ATT&CK;, adversary emulation, and purple team testing to enhance cyber defense capabilities (including purple-team/tabletop exercises to validate detections and playbooks).
- Developed threat intelligence and behavioral analytics frameworks to identify cyber adversaries' tactics, techniques, and procedures (TTPs), integrating machine learning-based anomaly detection for improved risk assessment.
- Led red team operations, penetration testing, and breach simulation exercises utilizing Metasploit, Burp Suite, Wireshark, and custom exploit development, identifying high-impact vulnerabilities and misconfigurations.
- Served as an ISSM and cybersecurity governance leader, ensuring RMF, NIST, and Zero Trust Architecture compliance while managing cyber risk assessments for classified enclaves.
- Executed proactive threat mitigation strategies, continuously refining Threat Hunting Playbooks, Indicators of Compromise (IOCs), and attack detection techniques (TTP/IOC codification to improve triage; fed into detection rules and incident response playbooks).

- Developed and led a Cyber Threat Intelligence (CTI) initiative, leveraging OSINT, threat feeds, and advanced data correlation techniques to predict and disrupt cyber threats before exploitation (monitoring emerging threats, zero-days, and vulnerability trends to prioritize investigative leads).
- Managed cyber risk assessments and secured a 3-year Authority to Operate (ATO) through proactive compliance with NIST 800-53, DISA CCRI, and eMASS security protocols.
- Designed and implemented a real-time attack surface monitoring framework, reducing time-to-detection for cyber incidents by 40%.
- Drove cyber strategy alignment with business objectives, ensuring seamless integration of cloud security (AWS, Azure), SIEM (Splunk, ELK), and endpoint protection (CrowdStrike, SentinelOne).
- Spearheaded blue team threat detection improvements, optimizing YARA rule development, network flow analysis, and forensic artifact collection.
- Enhanced proactive detection and response capabilities by deploying behavior-based analytics, deception technologies, and threat-hunting automation.
- Developed and delivered enterprise-wide cybersecurity training on threat hunting methodologies, TTP mapping, and cyber incident containment, elevating team proficiency in threat detection and response.
- Managed large-scale cybersecurity initiatives, implementing automated threat detection processes and streamlining cybersecurity response frameworks to enhance operational efficiency (enhanced incident response tools/workflows and lightweight scripts to improve investigation efficiency).
- Led real-time cyber event correlation and forensic investigations, providing executive-level briefings on cyber risk posture, threat actor trends, and recommended countermeasures (supported detection, containment, eradication, recovery, and post-incident technical reporting).
- Continuously refined detection engineering and TTP-based defense mechanisms, ensuring resilience against Advanced Persistent Threats (APTs) and evolving cyber adversaries.
- Planned and executed strategic cyber initiatives, aligning proactive cyber defense, risk analytics, and intelligence-driven security operations with enterprise risk management strategies.
- Led a 27-member cyber threat hunting and defensive cyber operations (DCO) team within a Joint/Combatant Command (CCMD) environment, overseeing SOC monitoring and alert investigations; personally led escalated investigations across endpoint, network, and cloud/identity telemetry.
- Designed and executed offensive security assessments using MITRE ATT&CK;, adversary emulation, and purple team testing to enhance cyber defense capabilities.
- Executed proactive threat mitigation strategies, continuously refining Threat Hunting Playbooks, Indicators of Compromise (IOCs), and SIEM detection logic (event/log parsing, enrichment, behavior analytics) to improve signal quality, reduce false positives, and expand visibility.
- Developed and led a Cyber Threat Intelligence (CTI) initiative, leveraging OSINT, threat feeds, and advanced data correlation techniques to predict and disrupt cyber threats before exploitation.
- Performed threat-infrastructure pivots using DNS/WHOIS and hosting/ASN context to correlate related domains/IPs, enrich investigations, and drive URL/domain block recommendations and remediation guidance.
- Drove cyber strategy alignment with business objectives, ensuring seamless integration of cloud security (AWS, Azure), SIEM (Splunk, ELK), endpoint protection (CrowdStrike, SentinelOne), and secure email/web gateway controls.
- Managed large-scale cybersecurity initiatives, implementing automation and SOAR-style workflows while partnering with tooling teams/vendors to improve detections, playbooks, and SOC performance metrics (MTTD/MTTR); provided continuous feedback to improve telemetry quality and analyst workflows.
- Led security incident investigations and forensic analysis, ensuring timely containment and root-cause determination; authored Findings Reports with documented evidence and prioritized remediation recommendations for stakeholders and partner teams.
- Executed proactive threat mitigation strategies, continuously refining Threat Hunting Playbooks, Indicators of Compromise (IOCs), and attack detection techniques.
- Managed large-scale cybersecurity initiatives, implementing automated threat detection processes and streamlining cybersecurity response frameworks to enhance operational efficiency.
- Led real-time cyber event correlation and forensic investigations, providing executive-level briefings on cyber risk posture, threat actor trends, and recommended countermeasures.
- Led joint/CCMD Defensive Cyber Operations (DCO) planning and contributed to C4I/enterprise IT planning, developing secure communications and cyber frameworks to support mission■critical operations—including crisis response, continuity, and wartime scenarios.

- Applied the Joint Operations Planning Process (JOPP) to produce adaptive defensive cyberspace strategies, assessing operational impacts and integrating planning across joint and coalition partners.
- Developed and synchronized cyberspace plans, orders, and annex inputs (e.g., cyber support to OPLAN/CONPLAN/FRAGOs), ensuring alignment with mission objectives, risk posture, and DoD/JCS directives.

Senior Incident Responder/Cyber Network Defender — US Army

392ND ESB, Network Operations and Security Branch • Baltimore, Maryland • Aug 2018 – Sep 2021

- Served as an ISSM for three classified enclaves, overseeing mission-critical cyber threat detection and incident response operations. Managed 30+ cybersecurity projects, developed cyber threat hunting strategies, and implemented proactive risk mitigation aligned with DoD and NIST 800-53 standards.
- Designed, integrated, and led proactive threat-hunting programs, correlating TTP-based detections, machine learning analytics, and anomaly-based defense techniques to protect critical networks.
- Developed and led real-time cyber threat intelligence fusion, mapping nation-state and cybercriminal adversary TTPs using MITRE ATT&CK;, behavioral analytics, and forensic analysis to preemptively mitigate cyber threats.
- Spearheaded strategic threat intelligence integration, leveraging threat modeling, adversary simulation, and network forensics to enhance proactive cyber defenses and minimize dwell time of sophisticated threats.
- Developed and executed automation frameworks for vulnerability scanning, leveraging custom Python-based tools to accelerate threat detection by 30%, increasing red team efficiency and reducing false positives (expanded to automated triage and faster investigative evidence collection).
- Authored white papers and internal threat intelligence guides, providing actionable insights into evolving cyber threats, APT methodologies, and zero-day exploit detection for executive leadership (including post-incident technical reports and remediation recommendations).
- Led the development of automated threat-hunting workflows, leveraging SIEM data analysis (Splunk, ELK Stack, Sentinel), anomaly detection algorithms, and network flow analytics to reduce response time to cyber incidents (improved alert fidelity and reduced time-to-containment for high-severity incidents).
- Developed and refined risk scoring models, analyzing attack surface vulnerabilities, asset criticality, and threat intelligence correlation to prioritize high-risk security gaps for remediation.
- Led advanced cyber audits and forensic investigations across 100+ networks and 2,000 systems, identifying and mitigating vulnerabilities through real-time network traffic analysis, packet inspection (Wireshark, Tcpdump), and log correlation (determined extent/scope of compromise and drove tactical/strategic remediation plans).
- Implemented AI-driven cyber threat analytics, reducing false positive alerts by 40% and improving endpoint detection and response (EDR) tuning across enterprise security platforms.
- Delivered enterprise-wide cybersecurity training on threat hunting methodologies, equipping teams with advanced skills in malware analysis, TTP-based hunting, and proactive security engineering.
- Saved $200,000 in operational costs by implementing automated data integrity solutions, enhancing threat intelligence processing and cybersecurity incident response readiness.
- Led security awareness programs and cyber readiness exercises, training 100+ personnel on incident response, cloud security threats (AWS, Azure), and cyber resilience strategies (included incident response tabletop exercises and containment drills).
- Developed and executed automation frameworks for vulnerability scanning, leveraging custom Python-based tools to accelerate threat detection by 30%, increasing red team efficiency and reducing false positives.
- Authored post-incident findings reports and internal threat intelligence guides, providing actionable insights into evolving cyber threats, APT methodologies, and remediation recommendations for leadership.
- Led the development of automated threat-hunting workflows, leveraging SIEM data analysis (Splunk, ELK Stack), anomaly detection algorithms, and network flow analytics to enable faster alert triage and reduce response time to cyber incidents.
- Led advanced cyber audits and forensic investigations across 100+ networks and 2,000 systems, collecting and analyzing evidence via network traffic analysis (Wireshark, Tcpdump) and log correlation to determine scope, impact, and remediation actions.
- Led security awareness programs and cyber readiness exercises, training 100+ personnel on incident response, cloud security threats (AWS, Azure), and cyber resilience strategies.
- Authored white papers and internal threat intelligence guides, providing actionable insights into evolving cyber threats, APT methodologies, and zero-day exploit detection for executive leadership.
- Led the development of automated threat-hunting workflows, leveraging SIEM data analysis (Splunk, ELK Stack), anomaly detection algorithms, and network flow analytics to reduce response time to cyber incidents.

- Led advanced cyber audits and forensic investigations across 100+ networks and 2,000 systems, identifying and mitigating vulnerabilities through real-time network traffic analysis, packet inspection (Wireshark, Tcpdump), and log correlation.
- Managed 30+ mission■critical cybersecurity initiatives/projects, refining plans and procedures to address emerging threats while aligning outcomes with DoD standards and timelines.
- Prepared for and supported cybersecurity compliance/readiness inspections (e.g., CCRI) by coordinating vulnerability remediation, evidence collection, and control validation across stakeholders.
- Leveraged enterprise vulnerability management tooling (e.g., ACAS) to prioritize remediation, reduce exposure, and sustain continuous monitoring baselines.

Senior COMSEC Account Manager (Additional Duty) — US Army
HHC, 392nd Expeditionary Signal Battalion (ESB) • Baltimore, MD • Aug 2018 – Aug 2020

- Saved a neglected COMSEC account from the brink of closure resulting in the account passing the CSLA inspection.
- Obtained GCFA and recertified GSLC and improved Unit's ability to reimage systems repair by 100%.
- Exceeded Unit requirement for PME and successfully completed the Master Leader Course.
- Reduced unit readiness data discrepancies and improved reporting by more than 70%.
- Conducted AIP to four downtrace companies spread across three states.
- Displayed the highest level of integrity, ingenuity, & confidence to advocate for others resulting in recognition from higher HQs.
- Trained and mentored 6 Soldiers on SMART-T and COMSEC operations throughout the Command.
- Trained and mentored 8 Soldiers while processing more than 600 COMSEC actions to pass inspections by AAA and CSLA.
- Input more than 30 Soldiers for schools and mentored subordinates on career paths.
- Honor Graduate of the AEHF Mission Planners Course; increased entire Brigade AEHF readiness by 100 percent.
- Obtained GIAC Certified Windows Security Administrator (GCWN) and SANS Security Awareness Professional (SSAP).
- Exceeded Unit requirement for PME and successfully completed the Senior Enlisted Joint Professional Military Education II.
- Successfully completed the Joint C4 Planners course; and was essential in planning for CSTX 78-20-04.
- Selected by CSLA to serve on Army-wide panel for COMSEC based on technical expertise.
- Planned, coordinated, and trained more than 32 Soldiers on the SMART-T; increased the number of trained from 6 to 38.
- Trained and mentored more than 30 mobilizing Soldiers on Signal maintenance and Soldier tasks.
- Created 4 policies and processes that increased accountability and readiness; resulted in adoption and recognition by DIV/BDE.

Senior COMSEC Account Manager/Cyber Network Defender — US Army
35th ESB, Cyber and Communications Security Branch • Fort Allen, Puerto Rico • Oct 2016 – Jul 2018

- Managed over 1,000 classified assets and led cyber threat defense strategies, ensuring secure handling, proactive cyber threat detection, and APT mitigation to protect mission-critical networks from emerging cyber threats.
- Maintained and enhanced security compliance frameworks, ensuring System Security Plans (SSPs), vulnerability mitigation records, and cyber risk assessments aligned with NIST, MITRE ATT&CK;, and DoD cybersecurity standards.
- Developed and executed scalable cyber defense strategies, translating threat intelligence and behavioral analytics into actionable security operations that reduced dwell time of malicious actors.
- Monitored real-time industry threat intelligence, integrating MITRE ATT&CK; updates, zero-day vulnerabilities, and adversary TTPs into advanced threat detection and incident response strategies (updated detections/playbooks with adversary TTPs and IOCs identified in the wild).
- Led proactive threat-hunting programs, leveraging behavioral analytics, SIEM-based detections (Splunk, ELK) and endpoint forensics to identify stealthy attacks before exploitation.
- Designed and led cyber threat intelligence fusion efforts, applying threat modeling, deception technologies, and red teaming insights to predict and neutralize cyber adversary activities.
- Led cross-domain cybersecurity operations, ensuring secure communications, network segmentation, and cloud security hardening across land, air, space, and cyberspace environments.
- Spearheaded disaster recovery and incident response strategies, securing 100% operational continuity of mission-critical communication systems during Hurricanes Irma and Maria, mitigating cyber risks in

high-stress environments (executed recovery procedures and continuity communications during major outages).

- Conducted large-scale threat assessments, auditing 100+ networks and 2,000 systems, identifying and eliminating high-risk vulnerabilities using network forensics, packet analysis (Wireshark, Tcpdump), and exploit simulation.
- Reduced cyber incidents by 75% by implementing automated anomaly detection, adversary tracking, and cyber readiness programs, while training 60+ personnel in cyber defense tactics and security operations.
- Developed cutting-edge threat detection frameworks, utilizing adversary emulation, purple team testing, and machine learning-based anomaly detection to enhance proactive threat hunting.
- Generated cyber risk reports and strategic action plans, aligning security operations with business risk priorities to drive enterprise-wide resilience against cyber threats.
- Served as a key cybersecurity strategist, organizing cybersecurity forums and intelligence-sharing collaborations, improving threat visibility, risk mitigation strategies, and cross-team cyber readiness.
- Designed and maintained a robust cyber infrastructure, ensuring secure network architecture, cloud security best practices, and threat intelligence-driven access control policies for enhanced security resilience.
- Monitored real-time industry threat intelligence, integrating MITRE ATT&CK; updates, zero-day vulnerabilities, and adversary TTPs into advanced threat detection and incident response strategies.
- Spearheaded disaster recovery and incident response strategies, securing 100% operational continuity of mission-critical communication systems during Hurricanes Irma and Maria, mitigating cyber risks in high-stress environments.
- Generated cyber risk reports and strategic action plans with documented findings and prioritized remediation steps, aligning security operations with business risk priorities to drive enterprise-wide resilience against cyber threats.
- Led proactive threat-hunting programs, leveraging behavioral analytics, SIEM-based detections (Splunk, ELK, Sentinel), and endpoint forensics to identify stealthy attacks before exploitation.

Network Operations Specialist — US Army

7th MSC, Network Operations and Security Center • Kaiserslautern, Germany • Mar 2013 – Oct 2016

- Led cybersecurity operations for the largest NATO exercise in two decades, ensuring secure communication infrastructure, real-time threat detection, and cyber resilience across multinational networks. Coordinated secure information flow and cyber defense protocols to mitigate state-sponsored cyber threats and espionage risks.
- Served as a cybersecurity SME and digital forensics lead, optimizing real-time cyber threat intelligence, adversary tracking, and risk mitigation strategies to strengthen network resilience and improve incident detection and response.
- Managed end-to-end cyber threat detection and response strategies, overseeing network intrusion analysis, log correlation (SIEM), and behavioral analytics-based security for high-priority classified communications and mission-critical IT environments (SIEM alert triage, network intrusion analysis, and rapid escalation for incident response).
- Provided direct cybersecurity leadership support to senior executives, ensuring secure command communications and implementing cyber threat mitigation measures to prevent cyber-physical attacks on mission systems.
- Led the integration of advanced cyber defense technologies, improving real-time threat monitoring, network segmentation, and endpoint protection solutions across complex, multi-domain network environments.
- Designed and implemented advanced cyber threat detection policies and frameworks, utilizing MITRE ATT&CK-based; attack simulations, adversary emulation, and red team exercises to proactively hunt for advanced persistent threats (APTs).
- Developed, monitored, and optimized cybersecurity governance policies, ensuring compliance with NIST 800-53, RMF, and Defense-in-Depth Security frameworks to reduce the attack surface and fortify enterprise security posture.
- Directed cyber operations for multinational exercises, aligning cyber threat intelligence, attack surface management, and security operations center (SOC) enhancements to streamline cyber incident response and mitigate threat actor tactics.
- Served as an Information Systems Security Officer (ISSO) and cyber risk leader, overseeing threat mitigation strategies, risk assessments, and enterprise cybersecurity frameworks to protect classified infrastructure and ensure regulatory compliance.
- Led cyber threat intelligence fusion operations, correlating threat indicators, log analysis, and SIEM-driven detections (Splunk, ELK) to rapidly identify and neutralize cyber threats targeting mission-critical systems.

- Developed and refined cyber threat-hunting workflows, integrating behavior-based anomaly detection, network traffic analysis, and digital forensics methodologies to proactively identify and disrupt adversarial operations.
- Executed large-scale cybersecurity initiatives during multinational exercises (BALTOPS, NATO operations), ensuring real-time network defense, adversary engagement, and cross-domain threat intelligence sharing to secure mission-critical cyber operations.
- Managed end-to-end cyber threat detection and response strategies, reviewing alerts, performing network intrusion analysis, correlating logs (SIEM), and escalating high-confidence incidents for containment and remediation.
- Managed end-to-end cyber threat detection and response strategies, overseeing network intrusion analysis, log correlation (SIEM), and behavioral analytics-based security for high-priority classified communications and mission-critical IT environments.
- Developed, monitored, and optimized cybersecurity governance policies, ensuring compliance with NIST 800-53, RMF, and Zero Trust Security frameworks to reduce the attack surface and fortify enterprise security posture.
- Led cyber threat intelligence fusion operations, correlating threat indicators, log analysis, and SIEM-driven detections (Splunk, ELK, Sentinel) to rapidly identify and neutralize cyber threats targeting mission-critical systems.
- Served as NCOIC/J6 lead during a major NATO exercise, overseeing mission communications infrastructure and ensuring availability, integrity, and confidentiality across a multinational environment.
- Acted as the unit's Signal Digital Master Gunner—optimizing and troubleshooting digital communications systems and integrating digital assets to enable resilient, secure network operations.

Information System Instructor — US Army

Training Command (TASS) • Sacramento, California • Oct 2010 – Mar 2013

- Served as the lead technical instructor, responsible for training more than 300 students in cybersecurity principles, information systems security, and defensive cyber operations, ensuring compliance with cybersecurity standards and best practices.
- Prepared classroom materials and lesson plans, developing and implementing comprehensive cybersecurity-focused curricula that covered information security protocols, cyber defense techniques, and the use of specialized tools.
- Conducted classes in accordance with the Total Army School System (TASS), Army Regulations, and published Standard Operating Procedures (SOPs), ensuring that instructional content adhered to guidance and promoted secure information systems management.
- Directed, supervised, planned, and coordinated classroom activities, fostering an interactive learning environment that equipped students to handle real-world cybersecurity challenges, perform risk assessments, and apply INFOSEC protocols.

Information System Team Chief — US Army

325th Combat Support Hospital • Independence, Missouri • Dec 2006 – Oct 2010

- Led a small information systems support team, coordinating day-to-day IT operations to keep mission and administrative services available; assigned tasks, tracked issues to closure, and mentored junior personnel.
- Supported local network and endpoint operations (workstations, printers, user accounts, and basic server services), troubleshooting outages and restoring service rapidly.
- Maintained configuration and accountability records for IT equipment; produced status updates and hand-offs to leadership and partner technical teams.
- Applied information assurance practices (access control, patching, backups, and incident reporting) to sustain readiness and support inspections.

Senior Local Area Network Manager — US Army

Medical Deployment Support Command • Seagoville, Texas • Mar 2006 – Dec 2006

- Managed local area network operations and end-user support, maintaining connectivity and resolving workstation and network issues to keep unit services operational.
- Assisted with server and desktop administration tasks (account provisioning, configuration, patching, and basic maintenance) in accordance with unit procedures.
- Documented network changes, outages, and corrective actions; coordinated restoration activities and escalated complex issues as required.

Network Manager — US Army

Aviation Intelligence Communications Support • Fort Knox, Kentucky / Kuwait / Iraq • Jun 2004 – Mar 2006

- Supported network operations and communications services across multiple locations, helping install, configure, and troubleshoot systems to maintain availability under operational timelines.
- Performed user support and account management tasks, including workstation setup, permissions, and incident documentation.
- Assisted with configuration control and equipment accountability, maintaining records for network and endpoint assets.

Information Systems Operator-Analyst (74B10) — US Army
Operation Iraqi Freedom (OIF) • Iraq • Jun 2004 – Nov 2005

- Deployed to Iraq in support of Operation Iraqi Freedom (OIF) from 2004-11-08 to 2005-10-14.
- Served in MOS 74B10 (Information Systems Operator-Analyst) during service period 2004-06-06 to 2005-11-06.
- Awards during this period include Army Commendation Medal, Iraq Campaign Medal, Global War on Terrorism Service Medal, and Armed Forces Reserve Medal (w/ M Device) (see DD214).
- Provided day■to■day information systems operations support: account provisioning, workstation configuration, and troubleshooting for both administrative and mission environments (e.g., NIPR/SIPR when applicable).
- Performed preventative maintenance and incident documentation; escalated complex issues and coordinated with signal/cyber teams to restore service quickly.

Information Systems Specialist — US Army
Information Systems Support • Multiple Locations (incl. Fort Eisenhower) • Jun 2002 – Jun 2004

- Provided entry-level information systems support, assisting with workstation setup, user support, troubleshooting, and routine maintenance to sustain daily operations.
- Supported basic networking and systems administration tasks under supervision, building foundations in secure system handling, documentation, and customer support.

Education

Master of Science, Information Security Engineering
SANS Technology Institute • 2022-10-10 • GPA 3.55

- Cumulative GPA 3.55 (37 credits awarded)

Graduate Certificate, Cyber Defense Operations
SANS Technology Institute • 2024-04-28 • GPA 3.33

- Cumulative GPA 3.33 (12 credits awarded)

Graduate Coursework, Cybersecurity
University of Maryland Global Campus (UMGC) • 2016-05 • GPA 4.00

- CSEC 610 Cyberspace and Cybersecurity (6 credits) — Grade A

Bachelor of Science, Computer and Information Science; Digital Media and Web Technology (Double Major)
University of Maryland Global Campus (UMGC) • 2015-12-30 • GPA 4.00 • Summa Cum Laude

- Degree GPA 4.000; Degree Honors: Summa Cum Laude

Associate of Arts, General Studies – Computer Studies Curriculum
University of Maryland Global Campus (UMGC) • 2015-12-30 • GPA 4.00

- Degree GPA 4.000

Certifications

- GIAC Defending Advanced Threats (GDAT)
- GIAC Open Source Intelligence (GOSI)
- GIAC Cloud Threat Detection (GCTD)
- GIAC Certified Web Application Defender (GWEB)
- GIAC Security Operations Certified (GSOC)
- GIAC Assessing and Auditing Wireless Networks (GAWN)
- GIAC Defensible Security Architect (GDSA)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Certified Project Manager (GCPM)
- GIAC Certified Windows Security Administrator (GCWN)

- GIAC Security Leadership (GSLC)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Continuous Monitoring (GMON)
- GIAC Cyber Threat Intelligence (GCTI)
- GIAC Critical Controls (GCCC)
- GIAC Certified Forensic Examiner (GCFE)
- GIAC Systems and Network Auditor (GSNA)
- GIAC Penetration Tester (GPEN)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Certified Incident Handler (GCIH)
- GIAC Python Coder (GPYC)
- GIAC Certified Enterprise Defender (GCED)
- GIAC Security Essentials (GSEC)
- SUSE Certified Linux Administrator (SUSE Linux Enterprise Server 11)
- CompTIA Linux+ Powered by LPI (and LPIC-1)
- EC-Council Certified Digital Marketer
- EC-Council Certified Ethical Hacker (CEH)
- EC-Council Certified Network Defense Architect (CNDA)
- Cisco Certified Academy Instructor (CCAI)
- Cisco Certified Network Associate (CCNA)
- SANS Security Awareness Professional (SSAP)
- XM-Cyber Exposure Management Certification
- CompTIA Security+ (CE)
- CompTIA Network+ (CE)
- CompTIA Security+ (historical)
- CompTIA Network+ (historical)
- LPI LPIC-1 (Linux Professional Institute Certification)
- Certified Authorization Professional (CAP)

Selected Training

- DoD Mission Assurance Assessment Course (GQ55000APCIL)
- Cyber Common Technical Core (CCTC)
- Army Information Operations Planners' Course (AIOPC)
- Joint Command, Control, Communications, and Computers Planners Course (Joint C4 Planners) (4C-F55/260-F15)
- AEHF Mission Planning Element Communications Tactical (4C-F72/260-F24 (CT))
- Antiterrorism Officer Basic Course (AT OBC) (Class #731-2019)
- Cyber Network Defender Senior Leader Course (SLC) 230-25D40-C46 (CP)
- Cyber Network Defender 230-25D30 (CP)
- COMSEC Account Manager Course (CAMC) 4C-F22/160-F23
- Key Management Infrastructure (KMI) Management Client (MGC) Operator Course (Spiral 2 / Spin 2)
- Information Technology Specialist Senior Leader Course (SLC) 531-25B40-C46
- Signal Digital Master Gunner 531-F75 (CT)
- Certified Authorization Professional (CAP-RMF/eMASS) (5 days)

Links

- Website: https://www.fryonline.net/
- LinkedIn: https://www.linkedin.com/in/brettfry2002
- GIAC Profile: https://www.giac.org/certified-professional/Brett-Fry/157586
- SANS Paper: https://www.sans.org/white-papers/automating-rmf-steps-using-lightweight-scripts-and-tools