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/ | 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

Professional 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

Skills

Threat Hunting & Detection

threat hunting, behavioral analytics, adversary emulation, MITRE ATT&CK, kill chain defenses, purple teaming, alert triage, log analysis, IOC/TTP enrichment, hypothesis-driven hunts, playbooks, detection tuning, false-positive reduction

SIEM & Telemetry

Splunk, Elastic/ELK, Microsoft Sentinel, detection content, use cases, dashboards, continuous monitoring, SPL, KQL, CrowdStrike, SentinelOne, EDR telemetry, alert triage

Incident Response & DFIR

incident response support, triage, forensic analysis, Windows security, evidence collection, containment & remediation, DFIR, YARA, network forensics, packet capture, Wireshark, Tcpdump, containment & eradication

Cloud & Platform Security

cloud threat detection, AWS concepts, Azure concepts, GCP concepts, monitoring & visibility, cloud identity telemetry, hybrid environments

GRC / Compliance

NIST, RMF, controls, audit readiness, risk management, policy & procedures, eMASS, ATO support, ISSM/ISSO concepts, DISA CCRI

Secure Communications

COMSEC, KMI, LCMS, keying material accountability, inventory, physical security, inspections

Leadership

team leadership, training, mentorship, stakeholder engagement, program management, executive briefings

Professional Experience

Lead Defensive Cyber Operations Analyst/Planner — USAFRICOM

Defensive Cyber Operations | Stuttgart, Germany | Sep 2021 – May 2025

Lead and coordinate Defensive Cyberspace Operations (DCO) and threat-hunting activities for a Combatant Command (CCMD) environment. Translate mission priorities, threat intelligence, and adversary TTPs into actionable detections, investigations, and risk decisions across endpoint, network, and cloud/identity telemetry. Focused on translating commander's intent into executable DCO and C4I/enterprise IT plans within a Combatant Command environment, coordinating across joint/coalition stakeholders.

Key Responsibilities

- Own the DCO planning and execution cycle: define priorities, scope hunts, coordinate collection/visibility, and track remediation to closure.
- Lead escalated investigations and incident response across multiple data sources (endpoint, SIEM, network telemetry, and cloud/identity logs), ensuring containment, eradication, recovery, and after-action reporting.
- Drive detection engineering: map threats to MITRE ATT&CK, develop/refine detection logic, tune alert fidelity, and reduce false positives through enrichment and correlation.
- Build and maintain threat-hunting playbooks (hypothesis-driven hunts, IOC/TTP pivots, validation criteria) and mentor analysts on repeatable hunt methodology.
- Coordinate purple-team and tabletop exercises to validate detection coverage and incident response playbooks; turn exercise findings into measurable improvements (MTTD/MTTR, coverage gaps).
- Provide cybersecurity governance support (RMF/ATO lifecycle, NIST 800-53 control status, POA&Ms, risk acceptance documentation) and communicate risk to leadership with clear decision options.
- Deliberate and crisis action planning support for cyberspace operations (JOPP-aligned), including cyber inputs to plans and orders.
- C4I / enterprise IT planning integration—secure communications architecture considerations for operational readiness and continuity.

Deliverables / Outputs

- Threat hunting playbooks and ATT&CK coverage mappings
- Detection rules / analytic queries, SIEM dashboards, and alert tuning documentation
- Incident timelines, evidence packages, and executive/technical incident reports
- ATO artifacts (SSP inputs, control implementation status, POA&Ms) and compliance reporting (e.g., eMASS-ready content)
- After-action reports and remediation plans from exercises and assessments

Selected Achievements

- 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.

Tools / Tech: SIEM/SOAR concepts and tooling (e.g., Splunk/ELK-style pipelines); EDR platforms (e.g., CrowdStrike/SentinelOne-style telemetry); Network analysis tools (e.g., Wireshark/flow analysis); Threat intel enrichment (OSINT, DNS/WHOIS/hosting pivots); MITRE ATT&CK mapping, YARA-style pattern logic, scripting/automation

Skills: Threat hunting; Detection engineering; Incident response; Forensics basics; Threat intelligence analysis; Risk management; RMF/ATO support; Security operations leadership; Stakeholder communication; Operational planning

Senior Incident Responder/Cyber Network Defender — US Army

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

Operate as a senior defender and incident responder for Army/DoD networks, combining hands-on incident handling with security hardening, monitoring improvements, and compliance support for mission systems and enclaves. Managed and delivered dozens of concurrent security projects while serving as a senior incident responder and cyber network defender in an enterprise DoD environment.

Key Responsibilities

- Perform triage and investigation of security events, identify root cause, and coordinate containment and remediation actions with system owners and administrators.
- Conduct threat hunting, log review, and basic forensic artifact collection to support incident response and improve defensive visibility.
- Support vulnerability management: coordinate scanning, prioritize findings, track remediation, and validate fixes through retest/verification.
- Implement and validate security controls (hardening/STIG-aligned baselines, account/access controls, logging requirements) and document evidence for compliance packages.
- Develop SOPs and train/mentor teammates on incident response procedures, reporting standards, and defensive best practices.

Deliverables / Outputs

- Incident response reports and evidence summaries
- Vulnerability scan summaries, prioritization/risk narratives, and remediation tracking
- Security SOPs, runbooks, and training materials

- Control evidence and documentation for compliance/authorization activities

Selected Achievements

- 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.

Tools / Tech: EDR/SIEM monitoring and alert triage workflows; Vulnerability scanners and configuration/hardening guidance (e.g., STIG concepts); Windows and Linux administrative tooling; Network troubleshooting and packet/log analysis

Skills: Incident response; Vulnerability management; Security monitoring; Defensive hardening; Log analysis; Documentation; Training/mentorship; Operational risk communication

Senior COMSEC Account Manager (Additional Duty) — US Army

HHC, 392nd Expeditionary Signal Battalion (ESB) | Baltimore, MD | Aug 2018 – Aug 2020

Manage a COMSEC account as an additional duty: safeguard and account for cryptographic keying material and COMSEC equipment, enforce policy compliance, and enable secure communications for supported units.

Key Responsibilities

- Maintain end-to-end accountability for keying material and cryptographic devices (inventories, issue/receipt, destruction, and incident reporting).
- Operate COMSEC management systems and workflows (KMI/LCMS-style processes), ensuring accurate records and audit readiness.
- Conduct internal inspections and prepare for external audits/assistance visits; correct discrepancies and implement procedural fixes.
- Train custodians and end users on secure handling procedures, reporting requirements, and day-to-day COMSEC operations.

Deliverables / Outputs

- COMSEC account records, inventories, and audit artifacts
- Keying material distribution/turn-in documentation
- COMSEC SOPs and training/checklists
- Corrective action plans from audits/inspections

Selected Achievements

- 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.

Tools / Tech: KMI/LCMS account workflows and reporting; Cryptographic equipment handling procedures; COMSEC incident reporting and audit preparation

Skills: COMSEC account management; Key management; Audit readiness; Policy compliance; Inventory control; Procedural training; Risk reduction

Senior COMSEC Account Manager/Cyber Network Defender — US Army

35th ESB, Cyber and Communications Security Branch | Fort Allen, Puerto Rico | Oct 2016 – Jul 2018

Blend COMSEC program management with cyber defense responsibilities—supporting secure communications while contributing to defensive security operations and incident response.

Key Responsibilities

- Perform COMSEC account manager duties (keying material accountability, audits, compliance) while supporting cyber defense functions for mission networks.
- Coordinate with S6/NetOps and security teams to align cryptographic support with operational requirements and security controls.
- Support incident response and defensive monitoring activities when needed, contributing to investigations and remediation.

Deliverables / Outputs

- COMSEC program documentation and audit artifacts
- Secure communications enablement for supported units
- Security support documentation and incident response inputs (as applicable)

Selected Achievements

- 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.

Tools / Tech: COMSEC management processes (KMI/LCMS concepts); Network operations coordination and documentation; Basic defensive monitoring workflows

Skills: COMSEC; Secure communications support; Compliance; Coordination with NetOps; Defensive operations support

Network Operations Specialist — US Army

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

Operate and maintain enterprise and tactical network services, ensuring availability, performance, and secure configuration of systems supporting mission operations.

Key Responsibilities

- Provide network operations support (monitoring, troubleshooting, service restoration) across routing/switching, transport, and server services.
- Administer user/services access (account provisioning, permissions, service continuity) and implement basic security controls (patching, configuration, logging).
- Support field/training exercises by planning and deploying communications packages and resolving outages under time constraints.
- Document network configurations, changes, and incident/problem tickets; coordinate with higher-level support and vendors as required.

Deliverables / Outputs

- Network diagrams and configuration documentation
- Troubleshooting records and root-cause summaries
- Change records and implementation notes
- Exercise communications plans and after-action notes

Selected Achievements

- 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.

Tools / Tech: Routing/switching administration and monitoring concepts; Windows/Linux server administration; Ticketing/change management workflows; Basic network analysis and troubleshooting tools

Skills: Network operations; Troubleshooting; Systems administration; Service availability; Documentation; Change management; Customer support

Information System Instructor — US Army

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

Deliver technical instruction and mentorship in information systems and cybersecurity topics to build operator and leader proficiency.

Key Responsibilities

- Develop and maintain lesson plans, practical labs, and assessment materials aligned to Army training requirements (TASS) and current security best practices.
- Instruct and evaluate students on secure system administration, troubleshooting, incident reporting, and foundational cyber defense concepts.
- Maintain training records and provide feedback/coaching to improve student performance and readiness for follow-on assignments.
- Ensure classroom and lab environments are configured safely and consistently to support hands-on learning.

Deliverables / Outputs

- Lesson plans and courseware
- Practical lab guides and checklists

- Student evaluations and training records
- After-action notes to improve future iterations

Selected Achievements

- 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.

Tools / Tech: Classroom/lab environments (Windows/Linux fundamentals); Virtualization and training lab images (conceptual); Network troubleshooting tools and exercises

Skills: Training delivery; Curriculum development; Technical communication; Cybersecurity fundamentals; Mentorship

Information System Team Chief — US Army

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

Supervise unit IT support activities, coordinating personnel and technical work to maintain service availability and enforce basic security practices.

Key Responsibilities

- Coordinate help-desk style support, user onboarding, troubleshooting, and service restoration.
- Support server/workstation maintenance, patching, and backup routines; assist with change and configuration management.
- Document equipment accountability, configurations, and recurring problems; brief leadership on operational status.

Deliverables / Outputs

- Troubleshooting logs and work summaries
- Inventory/accountability documentation
- Configuration notes and basic network diagrams (as required)

Selected Achievements

- 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.

Tools / Tech: Windows administration fundamentals; Ticketing/work order workflows (conceptual); Basic network troubleshooting tools

Skills: Team leadership; IT operations; Troubleshooting; Documentation; End-user support

Senior Local Area Network Manager — US Army

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

Maintain local network services and user support, ensuring reliable connectivity and basic configuration management.

Key Responsibilities

- Troubleshoot LAN connectivity, workstation issues, and peripheral problems; restore service and document actions taken.
- Support routine administration tasks (accounts, patching, configuration baselines) under supervision.
- Maintain inventories and basic documentation for network and endpoint assets.

Deliverables / Outputs

- Outage/incident notes
- Configuration and inventory records

Selected Achievements

- 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.

Tools / Tech: Network troubleshooting utilities (ping/traceroute, basic packet capture concepts); Windows OS administration fundamentals

Skills: LAN administration; Troubleshooting; Documentation; Customer support

Network Manager — US Army

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

Provide network and communications support for unit operations, sustaining connectivity and assisting with service restoration and documentation.

Key Responsibilities

- Assist with installation/configuration of network and workstation assets; troubleshoot outages and coordinate restoration.
- Perform basic systems administration tasks (accounts, configurations, maintenance) and document actions taken.

Deliverables / Outputs

- Configuration notes and hand-offs
- Incident/troubleshooting records

Selected Achievements

- 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.

Tools / Tech: Basic network troubleshooting tools and procedures; Windows OS and endpoint configuration concepts

Skills: Network operations; Communications support; Troubleshooting; Documentation

Information Systems Operator-Analyst (74B10) — US Army

Operation Iraqi Freedom (OIF) | Iraq | Jun 2004 – Nov 2005

Provide hands-on IT operations and user support in an operational environment, maintaining computers, networks, and communications systems and troubleshooting outages to keep mission services available.

Key Responsibilities

- Install, configure, and troubleshoot computer systems and local networks; perform basic maintenance and repair of hardware and operating systems.
- Support communications and data services in a deployed environment; coordinate restoration actions and escalate complex issues to higher support when needed.
- Apply basic information assurance practices (user access control, security procedures, incident reporting) in accordance with unit SOPs.
- Maintain technical documentation (system status, work orders, configuration notes) and assist with training users on systems and applications.

Deliverables / Outputs

- Work orders and troubleshooting documentation
- Configured endpoints and network devices ready for operations
- User support and training artifacts
- Basic security/IA compliance actions and records

Selected Achievements

- 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.

Tools / Tech: Windows operating systems and common productivity software; LAN and basic routing/switching concepts; Hardware maintenance/repair procedures; Operational reporting and documentation processes

Skills: IT support; Hardware/software troubleshooting; LAN fundamentals; Operational documentation; Security fundamentals; Customer service

Information Systems Specialist — US Army

Information Systems Support | Multiple Locations (incl. Fort Eisenhower) | Jun 2002 – Jun 2004

Perform foundational IT support and troubleshooting tasks, supporting users and maintaining basic system readiness.

Key Responsibilities

- Install and configure user workstations; assist with accounts and access under local procedures.
- Troubleshoot common hardware/software issues and document actions for escalation when required.

Deliverables / Outputs

- Trouble tickets/work summaries (as applicable)
- Basic configuration documentation

Selected Achievements

- 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.

Tools / Tech: Windows desktop support fundamentals; Basic network troubleshooting utilities

Skills: IT support; Troubleshooting; Customer support; Documentation

Education

SANS Technology Institute

Master of Science | Information Security Engineering | 2019-12-01 – 2022-10-10 | GPA 3.55

- Cumulative GPA 3.55 (37 credits awarded)

Selected Coursework

- {'course': 'ISE 6445: Cyber Threat Intelligence', 'term_start': None, 'term_end': None, 'credits_earned': 0, 'grade': 'CR'}
- {'course': 'ISE 5201: Hacker Tools, Techniques, Exploits, & Incident Handling', 'term_start': None, 'term_end': None, 'credits_earned': 0, 'grade': 'CR'}
- {'course': 'ISE 6901: MSISE Capstone', 'term_start': None, 'term_end': None, 'credits_earned': 0, 'grade': 'Waived'}
- {'course': 'ISE 6001: Implementing & Auditing CIS Critical Controls', 'term_start': None, 'term_end': None, 'credits_earned': 0, 'grade': 'CR'}
- {'course': 'ISE 6240: Continuous Monitoring and Security Operations', 'term_start': None, 'term_end': None, 'credits_earned': 0, 'grade': 'CR'}
- {'course': 'ISE 6715: Auditing & Monitoring Networks, Perimeters, & Systems', 'term_start': None, 'term_end': None, 'credits_earned': 0, 'grade': 'CR'}

- {'course': 'ISE 5401: Intrusion Detection In-Depth', 'term_start': None, 'term_end': None, 'credits_earned': 0, 'grade': 'CR'}
- {'course': 'ISE 5800: IT Project Management and Effective Communication', 'term_start': None, 'term_end': None, 'credits_earned': 0, 'grade': 'Waived'}
- {'course': 'ISE 5101: Security Essentials', 'term_start': None, 'term_end': None, 'credits_earned': 0, 'grade': 'CR'}
- {'course': 'ISE 5600: IT Security Planning, Policy, & Leadership', 'term_start': '12/01/2019', 'term_end': '01/15/2020', 'credits_earned': 1, 'grade': 'A'}
- {'course': 'ISE 5300: Managing Human Risk', 'term_start': '04/15/2020', 'term_end': '06/06/2020', 'credits_earned': 1, 'grade': 'A'}
- {'course': 'ISE 6300: NetWars Continuous Practicum', 'term_start': '06/16/2020', 'term_end': '08/06/2020', 'credits_earned': 1, 'grade': 'A'}
- {'course': 'ISE 5700: Situational Response Practicum', 'term_start': '01/22/2021', 'term_end': '02/16/2021', 'credits_earned': 1, 'grade': 'B'}
- {'course': 'ISE 6100: Security Project Practicum', 'term_start': '02/15/2021', 'term_end': '03/17/2021', 'credits_earned': 1, 'grade': 'B'}
- {'course': 'ISE 6200: Core Comprehensive Exam', 'term_start': '04/01/2021', 'term_end': '04/15/2021', 'credits_earned': 1, 'grade': 'Pass'}
- {'course': 'ISE 6255: Defensible Security Architecture & Engineering', 'term_start': '12/15/2021', 'term_end': '03/14/2022', 'credits_earned': 3, 'grade': 'B'}
- {'course': 'ISE 5501: Technical Research and Communication Practicum', 'term_start': '06/21/2022', 'term_end': '10/10/2022', 'credits_earned': 3, 'grade': 'A'}

SANS Technology Institute

Graduate Certificate | Cyber Defense Operations | 2023-03-01 – 2024-04-28 | GPA 3.33

- Cumulative GPA 3.33 (12 credits awarded)

Selected Coursework

- {'course': 'ISE 6240: Continuous Monitoring and Security Operations', 'term_start': None, 'term_end': None, 'credits_earned': 0, 'grade': 'CR'}
- {'course': 'ISE 6255: Defensible Security Architecture & Engineering', 'term_start': None, 'term_end': None, 'credits_earned': 0, 'grade': 'CR'}
- {'course': 'ISE 4450: Security Operations and Analysis', 'term_start': '03/01/2023', 'term_end': '06/18/2023', 'credits_earned': 3, 'grade': 'A'}
- {'course': 'ISE 6655: Cloud Security Attacker Techniques, Monitoring and Threat Detection', 'term_start': '08/15/2023', 'term_end': '11/13/2023', 'credits_earned': 3, 'grade': 'B'}
- {'course': 'ISE 6250: Purple Team Tactics & Kill Chain Defenses', 'term_start': '02/01/2024', 'term_end': '04/28/2024', 'credits_earned': 3, 'grade': 'B'}

University of Maryland Global Campus (UMGC)

Graduate Coursework | Cybersecurity | 2016-01 – 2016-05 | GPA 4.00

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

Selected Coursework

- {'course': 'CSEC 610 Cyberspace and Cybersecurity', 'credits': 6, 'grade': 'A'}
- {'course': 'UCSP 615 Orientation to Graduate Studies', 'credits': 0, 'grade': 'P'}

University of Maryland Global Campus (UMGC)

Bachelor of Science | Computer and Information Science; Digital Media and Web Technology (Double Major) | 2013 – 2015-12-30 | GPA 4.00 | Summa Cum Laude

- Degree GPA 4.000; Degree Honors: Summa Cum Laude

University of Maryland Global Campus (UMGC)

Associate of Arts | General Studies – Computer Studies Curriculum | 2013 – 2015-12-30 | GPA 4.00

- Degree GPA 4.000

Certifications

GIAC Defending Advanced Threats (GDAT) — GIAC

2024-04-28 | Expires: 2028-04-30 | active

Validates advanced understanding of how sophisticated adversaries operate (APT models and methods) and how to strengthen prevention, detection, and response across the attack lifecycle. Emphasizes purple-team thinking: offensive tradecraft awareness combined with defensive control validation and threat-hunting techniques.

Skills: Advanced threat (APT) models & methods; Adversary emulation; MITRE ATT&CK mapping; Kill chain / attack lifecycle analysis; Threat hunting; Detection engineering concepts; Incident response; Cyber deception concepts; Control validation & hardening; Post-exploitation detection

GIAC Open Source Intelligence (GOSI) — GIAC

2024-02-16 | Expires: 2028-04-30 | active

Validates the ability to collect, analyze, and operationalize open-source intelligence (OSINT) in support of investigations, threat intelligence, and security operations. Focuses on repeatable collection methods, pivoting, validation, and reporting.

Skills: OSINT collection & analysis; Web research & pivoting; Social media intelligence; Domain/IP/WHOIS research; Metadata analysis; Link analysis & attribution support; Data validation & source evaluation; Investigation reporting; Operational security (research OPSEC)

GIAC Cloud Threat Detection (GCTD) — GIAC

2023-11-13 | Expires: 2028-04-30 | active

Validates the ability to detect and respond to threats in public cloud environments by leveraging cloud-native logging, identity signals, and telemetry. Emphasizes detection use cases, alert triage, and investigation of cloud-centric attack techniques.

Skills: Cloud threat detection; Cloud logging & telemetry; IAM / identity signal analysis; Cloud incident response; Detection use-case development; CloudTrail / audit-log analysis; Threat hunting in cloud; Misconfiguration & exposure detection; Security monitoring

GIAC Certified Web Application Defender (GWEB) — GIAC

2023-07-23 | Expires: 2028-04-30 | active

Validates skills required to defend web applications by understanding common web vulnerabilities, secure design principles, defensive controls, and monitoring strategies. Focuses on preventing, detecting, and mitigating application-layer attacks.

Skills: Web application security; OWASP Top 10; Authentication & session security; Input validation & output encoding; Secure SDLC fundamentals; WAF concepts & tuning; Application logging & monitoring; Secure configuration; Vulnerability remediation

GIAC Security Operations Certified (GSOC) — GIAC

2023-06-18 | Expires: 2028-04-30 | active

Validates competence in modern security operations workflows, including monitoring, triage, escalation, and coordination of incident response and vulnerability management activities. Emphasizes operational rigor and measurable SOC practices.

Skills: SOC operations; Alert triage & escalation; Security monitoring; Incident response coordination; Use-case & playbook development; Operational metrics & reporting; Vulnerability management workflows; Continuous improvement / tuning

GIAC Assessing and Auditing Wireless Networks (GAWN) — GIAC

2022-05-23 | Expires: 2028-04-30 | active

Validates the ability to assess and audit 802.11 wireless networks, identify configuration weaknesses, and evaluate the security posture of wireless environments using offensive and defensive techniques.

Skills: Wireless security (802.11); Wireless auditing & assessment; WPA/WPA2/WPA3 concepts; Rogue AP detection; Wireless packet capture & analysis; RF threat awareness; Secure wireless configuration; Penetration testing (wireless)

GIAC Defensible Security Architect (GDSA) — GIAC

2022-03-14 | Expires: 2028-04-30 | active

Validates the ability to design and evolve defensible security architectures using threat modeling and practical security design patterns. Emphasizes building layered defenses, visibility, and resilience aligned to business requirements.

Skills: Security architecture; Threat modeling; Defense-in-depth design; Network segmentation; Secure design patterns; Logging & visibility architecture; Zero trust concepts; Security control selection; Risk-informed decision making

GIAC Web Application Penetration Tester (GWAPT) — GIAC

2021-08-06 | Expires: 2028-04-30 | active

Validates the ability to perform penetration testing of web applications, including discovery of common vulnerabilities, exploitation concepts, and reporting of actionable remediation guidance.

Skills: Web application penetration testing; OWASP testing methodology; Authentication/authorization testing; Input validation testing; Session management testing; Exploitation concepts; Testing documentation & reporting; Remediation guidance

GIAC Certified Project Manager (GCPM) — GIAC

2021-01-01 | Expires: 2028-04-30 | active

Validates practical project management skills for cybersecurity and IT initiatives, including planning, risk management, scheduling, communication, and delivery of measurable outcomes.

Skills: Project management; Scope / schedule / cost management; Risk & issue management; Stakeholder communication; Requirements management; Project governance; Documentation & reporting; Execution & delivery

GIAC Certified Windows Security Administrator (GCWN) — GIAC

2019-12-04 | Expires: 2028-04-30 | active

Validates the ability to secure Windows environments through hardening, configuration, monitoring, and response practices across endpoints and servers.

Skills: Windows security administration; Hardening & baselining; Active Directory security; Endpoint security concepts; Logging & monitoring on Windows; Privilege management concepts; Vulnerability mitigation

GIAC Security Leadership (GSLC) — GIAC

2019-08-09 | Expires: 2028-04-30 | active

Validates leadership-focused cybersecurity knowledge, emphasizing governance, risk, communication, and translating security requirements into operational and strategic outcomes.

Skills: Security leadership; Governance, risk, and compliance (GRC); Policy & standards; Security program management; Risk communication; Stakeholder management; Strategic planning

GIAC Certified Forensic Analyst (GCFA) — GIAC

2019-01-10 | Expires: 2028-04-30 | active

Validates advanced incident response and digital forensics skills, including evidence collection, timeline creation, and analysis of attacker activity to support containment, eradication, and lessons learned.

Skills: Incident response; Digital forensics; Evidence handling; Timeline analysis; Endpoint artifact analysis; Log analysis; Case reporting

GIAC Continuous Monitoring (GMON) — GIAC

2018-05-29 | Expires: 2028-04-30 | active

Validates the ability to implement and operate continuous monitoring and security operations practices, including log management, alerting, detection logic, and operational response workflows.

Skills: Continuous monitoring; Security operations; Log management; SIEM concepts; Detection use cases; Alert tuning; Operational response workflows; Security metrics

GIAC Cyber Threat Intelligence (GCTI) — GIAC

2018-05-16 | Expires: 2028-04-30 | active

Validates the ability to produce and operationalize cyber threat intelligence, including collection, analysis, production, and dissemination aligned to stakeholder needs and decision-making.

Skills: Cyber threat intelligence; Intelligence lifecycle; Collection management; Analytic tradecraft; Indicator evaluation; Reporting & briefing; Stakeholder requirements; Intelligence-driven defense

GIAC Critical Controls (GCCC) — GIAC

2018-04-27 | Expires: 2028-04-30 | active

Validates the ability to implement and audit the CIS Critical Security Controls, focusing on practical, prioritized security measures and governance of control effectiveness.

Skills: CIS Critical Security Controls; Security control implementation; Control auditing; Security measurement; Prioritization & roadmap planning; Program governance; Risk reduction planning

GIAC Certified Forensic Examiner (GCFE) — GIAC

2017-07-18 | Expires: 2028-04-30 | active

Validates foundational digital forensics skills for examining systems, acquiring evidence, and performing structured analysis to support investigations and incident response.

Skills: Digital forensics fundamentals; Evidence acquisition; Windows artifact analysis; File system analysis; Chain of custody concepts; Reporting

GIAC Systems and Network Auditor (GSNA) — GIAC

2017-07-06 | Expires: 2028-04-30 | active

Validates the ability to assess and audit systems and networks, focusing on control verification, configuration review, and identification of weaknesses and risk exposures.

Skills: Security auditing; Control verification; Configuration review; Risk assessment; Network security assessment; Audit reporting

GIAC Penetration Tester (GPEN) — GIAC

2017-06-17 | Expires: 2028-04-30 | active

Validates penetration testing skills across planning, reconnaissance, exploitation concepts, and reporting. Focuses on ethically identifying security weaknesses and communicating risk and remediation.

Skills: Penetration testing methodology; Reconnaissance & enumeration; Exploitation concepts; Privilege escalation concepts; Reporting & remediation guidance; Risk communication

GIAC Certified Intrusion Analyst (GCIA) — GIAC

2017-04-10 | Expires: 2028-04-30 | active

Validates network intrusion analysis skills, emphasizing packet-level investigation, IDS/NSM concepts, and structured detection and analysis of malicious activity.

Skills: Network intrusion analysis; Packet analysis; IDS/NSM concepts; Traffic baselining; Protocol analysis; Detection & investigation

GIAC Certified Incident Handler (GCIH) — GIAC

2017-03-23 | Expires: 2028-04-30 | active

Validates practical incident handling capability to detect, respond, and resolve security incidents. Emphasizes common attack techniques, vectors, tools, and defensive countermeasures.

Skills: Incident response; Attack techniques & vectors; Triage & containment; Eradication & recovery; Threat detection; IR documentation & reporting

GIAC Python Coder (GPYC) — GIAC

2017-03-14 | Expires: 2028-04-30 | active

Validates the ability to write and reason about Python code for automation and security use cases, including data handling, scripting patterns, and practical programming fundamentals.

Skills: Python scripting; Automation; Data parsing & manipulation; APIs & integrations (concepts); Debugging & testing concepts; Secure coding fundamentals

GIAC Certified Enterprise Defender (GCED) — GIAC

2017-02-17 | Expires: 2028-04-30 | active

Validates enterprise defensive skills spanning hardening, monitoring, and response across common operating systems and network environments.

Skills: Enterprise defense; System hardening; Detection & monitoring; Incident response; Windows/Linux security concepts; Network security

GIAC Security Essentials (GSEC) — GIAC

2017-01-20 | Expires: 2028-04-30 | active

Validates broad, hands-on information security knowledge beyond terminology, spanning core security concepts, networking, and practical defensive skills used in IT and security roles.

Skills: Security fundamentals; Networking fundamentals; Access control concepts; Cryptography fundamentals; Incident response basics; Security policy basics

SUSE Certified Linux Administrator (SUSE Linux Enterprise Server 11) — SUSE

2016-05-04 | completed

Validates administration of SUSE Linux Enterprise Server, including installation/configuration, user and service management, and operational troubleshooting.

Skills: Linux administration (SUSE); User & group management; Service management; System configuration; CLI proficiency; Troubleshooting

CompTIA Linux+ Powered by LPI (and LPIC-1) — CompTIA/LPI

2016-05-03 | completed

Validates foundational Linux administration across distributions, including command-line usage, file systems, networking basics, users/permissions, and troubleshooting.

Skills: Linux administration; Command-line operations; File system management; Permissions & ownership; Networking basics; Process management; Troubleshooting

EC-Council Certified Digital Marketer — EC-Council

2016-03-14 | issued

Validates knowledge of digital marketing fundamentals, including online strategy, content, SEO/SEM concepts, analytics basics, and campaign planning.

Skills: Digital marketing fundamentals; Campaign planning; SEO/SEM concepts; Content strategy; Web analytics basics; Audience targeting concepts

EC-Council Certified Ethical Hacker (CEH) — EC-Council

2015-09-22 | issued

Validates knowledge of ethical hacking concepts, common attack techniques, and foundational penetration testing methodology used to identify and remediate vulnerabilities.

Skills: Ethical hacking concepts; Penetration testing methodology; Reconnaissance & enumeration; Vulnerability assessment; Exploitation concepts; Reporting & remediation guidance

EC-Council Certified Network Defense Architect (CNDA) — EC-Council

2015-09-22 | issued

Validates defensive network security architecture concepts, including layered defense, secure network design, monitoring, and resilience planning.

Skills: Network security architecture; Defense-in-depth; Network monitoring concepts; Perimeter security concepts; Security controls design; Risk-informed design decisions

Cisco Certified Academy Instructor (CCAI) — Cisco

qualified

Validates capability to instruct Cisco Networking Academy curricula, including facilitation, lab delivery, and learner support aligned to Cisco Academy standards.

Skills: Technical instruction; Curriculum delivery; Lab facilitation; Student coaching; Networking fundamentals instruction

Cisco Certified Network Associate (CCNA) — Cisco

Expires: 2014-04-02 | expired (historical)

Validates foundational Cisco networking skills including routing/switching concepts, IP addressing, network troubleshooting, and core network services fundamentals.

Skills: Routing & switching fundamentals; IP addressing & subnetting; Network troubleshooting; Cisco IOS fundamentals; VLANs & switching concepts; WAN concepts

SANS Security Awareness Professional (SSAP) — SANS

issued (date not listed in source docs)

Validates foundational capability to build and run an effective security awareness program, including behavior change concepts, program execution, and measurement.

Skills: Security awareness program design; Training development; Phishing awareness concepts; Security communications; Metrics & reporting; Behavior change concepts

XM-Cyber Exposure Management Certification — XM Cyber

issued (date not listed in source docs)

Demonstrates understanding of exposure management concepts, including attack path modeling, control validation, and risk-based remediation prioritization to reduce overall exposure.

Skills: Exposure management; Attack path analysis; Security control validation; Risk-based prioritization; Vulnerability remediation planning; Continuous exposure reduction

CompTIA Security+ (CE) — CompTIA

2015-12-28 | recognized

Validates baseline cybersecurity knowledge (threats, attacks, controls, cryptography, identity/access, and risk management) commonly aligned to DoD workforce requirements.

Skills: Security fundamentals; Threats & vulnerabilities; Access control concepts; Cryptography basics; Risk fundamentals; Security operations basics

CompTIA Network+ (CE) — CompTIA

2015-12-28 | recognized

Validates foundational networking knowledge including TCP/IP, network operations, troubleshooting, and common network security concepts.

Skills: Networking fundamentals; TCP/IP fundamentals; Routing & switching basics; Network troubleshooting; Network operations; Network security concepts

CompTIA Security+ (historical) — CompTIA

2007 | historical

Historical attainment of CompTIA Security+ demonstrating early baseline cybersecurity knowledge (pre-CE/renewal era).

Skills: Security fundamentals; Threat awareness

CompTIA Network+ (historical) — CompTIA

2007 | historical

Historical attainment of CompTIA Network+ demonstrating early baseline networking knowledge (pre-CE/renewal era).

Skills: Networking fundamentals; Network troubleshooting

LPI LPIC-1 (Linux Professional Institute Certification) — Linux Professional Institute (LPI)

2016-05-03 | completed

Validates ability to perform maintenance tasks on the command line, install and configure a Linux computer, and configure basic networking.

Skills: Linux administration; Command-line operations; System configuration; Users/permissions; Networking basics; Troubleshooting

Certified Authorization Professional (CAP) — (ISC)²

None | Expires: None | self-reported

Credential focused on authorization and governance of information systems—risk management, control selection/assessment, and maintaining authorization packages (SSP, POA&M) for compliance-driven environments.

Skills: Risk Management Framework (RMF); Security authorization (ATO); System Security Plan (SSP); Plan of Action & Milestones (POA&M); NIST SP 800-53 controls; Security assessment & authorization (A&A); eMASS workflows; Continuous monitoring governance

Training & Professional Development

DoD Mission Assurance Assessment Course (GQ55000APCIL) — Defense Threat Reduction Agency (DTRA)

2022-09-19 – 2022-09-23 | 40 hrs | Certificate of Training

Mission Assurance Assessment course focused on planning and conducting DoD mission assurance / resilience assessments. Emphasizes identifying mission-essential functions, evaluating system and process vulnerabilities, assessing risk, and producing actionable mitigation recommendations and reporting artifacts.

Topics: Mission-essential functions (MEF) identification; Criticality analysis and dependency mapping; Assessment planning and stakeholder interviews; Vulnerability identification (people/process/technology); Risk characterization and prioritization; Mitigation recommendations and tracking; Assessment reporting and briefings

Skills: Mission assurance; Risk assessment; Vulnerability identification; Control assessment; Operational resilience; Criticality analysis; Continuity planning; Assessment reporting; Stakeholder interviews; Remediation planning; Security posture evaluation

Cyber Common Technical Core (CCTC) — US Army Cyber School (Cyber Center of Excellence)

2020-05-11 – 2020-07-14 | Certificate of Training

Common technical foundation for Army cyber professionals. Covers core cyber concepts, networking fundamentals, operating system administration concepts, scripting/automation fundamentals, and defensive cyber operations basics used across cyber MOS roles.

Topics: Networking fundamentals (TCP/IP, routing/switching basics); Windows and Linux operating system concepts; Scripting/automation fundamentals; Security fundamentals and defensive concepts; Cyber operations processes and terminology; Hands-on labs reinforcing core technical skills

Skills: Cyber fundamentals; Networking; TCP/IP; Windows administration; Linux administration; Scripting fundamentals; Cyber operations processes; Defensive cyber operations; Troubleshooting; Security controls awareness

Army Information Operations Planners' Course (AIOPC) — 1st Information Operations Command (LAND)

2020-01-06 – 2020-01-17 | Certificate of Training

Information Operations (IO) planning course covering the information environment, IO planning processes, integration of IO capabilities into operational planning (e.g., OPSEC, MILDEC, EW, cyberspace considerations), and development of IO annexes/products to support commanders' objectives.

Topics: Information Operations (IO) doctrine and planning; Information environment analysis; Target audience and effects-based planning concepts; Integration with OPSEC, MISO, EW, cyber, PA; Measures of effectiveness and assessment; IO annex/supporting products

Skills: Information Operations (IO); Operational planning; Information environment analysis; OPSEC; MISO/PSYOP integration; Electronic warfare (EW) awareness; Cyber IO integration; Target audience analysis; IO annex development; Campaign planning support

Joint Command, Control, Communications, and Computers Planners Course (Joint C4 Planners) (4C-F55/260-F15) — Joint C4 Planners (DoD)

2019-10-16 – 2019-11-13 | 160 hrs | Certificate of Training

Joint C4 planners course focused on communications planning for joint operations. Covers requirements analysis, interoperability considerations, satellite/terrestrial communications planning concepts, and coordination of C4 capabilities to support operational plans.

Topics: Joint C4 planning fundamentals (J6 context); Requirements and capability analysis; Interoperability and integration planning; SATCOM and network planning considerations; Architecture and communications planning products; Planning for exercises/operations

Skills: C4 planning; Communications planning; Interoperability; Requirements analysis; SATCOM planning; Network design concepts; Joint planning processes; Capability integration; Operational support coordination

AEHF Mission Planning Element Communications Tactical (4C-F72/260-F24 (CT)) — US Army Signal School

2019-08-12 – 2019-08-30 | Certificate of Training

Upon completion of the course, the student will be able to plan and design communication satellite installations; select and align satellite antenna configurations; evaluate communication bandwidth alignments for low and medium data rates; configure satellite communication system data and network connections; and troubleshoot satellite communication systems data and network connections.

Topics: AEHF SATCOM fundamentals and mission planning concepts; Link planning, bandwidth/frequency considerations; Crypto/keying material considerations for SATCOM; Terminal setup/configuration and troubleshooting; Mission planning products and coordination; Operational employment and readiness checks

Skills: Satellite Communications; Networking; Satellite communications; Bandwidth planning; Antenna alignment; SATCOM mission planning; AEHF operations; Network configuration; SATCOM troubleshooting

Antiterrorism Officer Basic Course (AT OBC) (Class #731-2019) — US Army

2019-03-18 – 2019-03-22 | 40 hrs | Diploma

Antiterrorism Officer Basic course focused on establishing and managing an antiterrorism program, performing threat/vulnerability assessments, implementing risk-based protective measures, and coordinating force protection training and compliance.

Topics: Antiterrorism (AT) program management; Threat assessment and terrorist tactics overview; Vulnerability assessment methodology; Risk management and mitigation measures; Force protection planning and compliance; AT training and exercise planning

Skills: Antiterrorism (AT); Force protection; Threat assessment; Vulnerability assessment; Risk management; Protective measures; Program management; Compliance; Training coordination

Master Leader Course (Class 14-19) — NCO Leadership Center of Excellence

2018-10-17 – 2018-11-27 | 112 hrs | Diploma

This course provides students with the knowledge to conduct practical applications of organizational communication and leadership skills. Students learn advanced leadership skills in the areas of negotiation, conflict management, leader-leadership styles, and methods of delegation. In addition, students learn to exercise strategic influence in an organizational

environment, build consensus in a diverse community using various communication strategies, and implement internal and external plans.

Topics: Senior NCO leadership and organizational stewardship; Operational-level thinking and problem solving; Training management and leader development; Communication, counseling, and mentorship; Ethics, command climate, and discipline; Planning and decision-making processes

Skills: Applied Leadership; Executive Communication; Leadership; Negotiation; Conflict management; Organizational communication; Strategic influence; Consensus building; Delegation; Leadership styles

Certificate of Appreciation (Cyber Center of Excellence NCO Academy) — Cyber Center of Excellence NCO Academy

Recognition

Recognition for contribution in support of Cyber Center of Excellence NCO Academy training mission (instructional support / leadership).

Topics: Recognition for support to NCO Academy mission; Instructional support / mentorship / operational assistance; Contribution to course delivery or student development

Skills: Training support; Mentorship; Leadership; Professionalism

Cyber Network Defender Senior Leader Course (SLC) 230-25D40-C46 (CP) — US Army Signal School

2018-04-09 – 2018-06-01 | Diploma

This course provides students with the skills to safeguard networks, systems and data through technical exercises consisting of auditing, hacking detection, system administration, networking, and perimeter defense. The course consists of a capstone summarizing these technical skills utilizing the SANS Institute "NETWARS" simulations interactive learning scenarios. The SANS AUD507: Auditing and Monitoring Networks, Perimeters certification is required to pass the course. In addition, this course prepares students to take the SANS SEC566: Implementing and Auditing the Critical Security Control In-Depth, and SEC511: Continuous Monitoring and Security Operations certification exams. The student will also be able to develop and deliver professional communications.

Topics: Defensive cyber operations leadership; Threat hunting and detection engineering concepts; Incident response planning and execution; Network security monitoring and analysis;

Risk management and security governance fundamentals; Training management and team leadership in cyber units

Skills: Communications; Hacking Detection And Prevention; Security Auditing; Security Monitoring And Operations; Hacking detection; Continuous monitoring; Security operations; Networking; Auditing; Security auditing; Perimeter defense; System administration; Network monitoring; Professional communications; NetWars simulation exercises; Continuous monitoring concepts; Critical controls familiarity

Key Management Infrastructure (KMI) Management Client (MGC) Operator Course (Spiral 2 / Spin 2) — KMI / DoD

2017-10-16 – 2017-10-27 | 80 hrs | Certificate of Training

KMI Management Client (MGC) operator training covering operation of the KMI client platform used to manage cryptographic keys and related COMSEC material. Includes key/account administration concepts, transaction workflows, and procedures supporting secure communications.

Topics: KMI architecture and roles; Account setup and key ordering workflows; Key distribution, issuance, and accountability; Audit reporting and compliance procedures; Troubleshooting and operational best practices

Skills: Key Management Infrastructure (KMI); Key management; COMSEC workflows; Cryptographic material handling; Account administration; Secure communications support; KMI MGC operation; Procedural compliance

Local COMSEC Management Software (LCMS) Workstation Operator (4C-F59/160-F39) — Signal School / Ft Gordon GA

2017-06-12 – 2017-06-23 | ACE-evaluated military course (JST)

Upon completion of the course, the student will be able to operate and manage the local communication security (COMSEC) management software (LCMS) workstation and associated platform for the purpose of encrypting data communications.

Topics: LCMS workstation setup and operations; Keying material generation and management; Account records, reports, and audits; Compliance and incident reporting procedures; Workflow troubleshooting and best practices

Skills: Credit Is Not Recommended; COMSEC; Local COMSEC Management Software (LCMS); LCMS operations; Key loading; Cryptographic support; COMSEC procedures; Secure communications

Cyber Network Defender 230-25D30 (CP) — US Army Signal School

2017-01-03 – 2017-04-13 | Diploma

Upon completion of the course, the student will be able to employ directed response actions; analyze digital forensic data; perform trend analysis; validate network security and alerts; deploy situational awareness tools; manage remote access; analyze suspicious software; identify attack techniques; analyze system and network vulnerabilities; perform trend analysis; validate network alerts and assess causes; monitor network resources to detect threats; verify wireless security postures; implement computer network defense systems; manage remote access solutions; validate cryptographic solutions; perform firewall host-based security validation; configure router validation; analyze suspicious software; monitor network resources to detect advanced threats; verify wireless security; deploy network sensors; evaluate Python code for penetration testing; build intrusion detection capability; analyze advanced IP packets; perform malware analysis; calculate, control, and mitigate risks; build risk management plans; outline a data classification program; manage data access; articulate data loss prevention concepts; identify data loss prevention solutions; identify vulnerabilities; perform materials disposition; handle materials transfer; provide physical material handling; perform materials transport; handle materials movement; document custodian inventory changes; perform semi-annual inventory; and perform special inventory tasks.

Topics: Network defense operations fundamentals; Intrusion detection and defensive tools; Vulnerability assessment and mitigation basics; Incident handling and response procedures; Digital forensics fundamentals; Security monitoring and reporting

Skills: Inventory Management; Materials Handling; Advanced Security Essentials - Enterprise Defender; Global Information Assurance Certification - Security Essentials; Hacker Techniques, Exploits, And Incident Handling; Risk Management; Intrusion detection; Digital forensics; Malware analysis; Packet analysis; Networking; Wireless security; Firewall administration; Router configuration; Cryptography / encryption; Risk management; Physical fitness; Defensive cyber operations; Alert validation; Trend analysis; Threat detection; IDS/IPS deployment; Python code review; Wireless security validation; Data classification; Data loss prevention (DLP); Inventory accountability

COMSEC Account Manager Course (CAMC) 4C-F22/160-F23 — USACyberCoE & Ft Gordon

2016-11-28 – 2016-12-08 | 70 hrs | Certificate of Training

Upon completion of the course, the student will be able to identify regulations, manuals, forms, publications, equipment, and materials required in the role of a Communications Security (COMSEC) account manager; identify the established policies and procedures for providing

effective security management; describe the security requirements for the overall security of a Communications Security (COMSEC) facility; perform the steps to close or move a security account; perform security account inspections and audits; and identify CryptoNet and associated security communications equipment.

Topics: COMSEC account manager duties and responsibilities; Keying material accountability and lifecycle; Cryptonet management and distribution; Physical security and incident reporting; Audit/inspection preparation and corrective actions

Skills: Network Administration; COMSEC; Auditing; Inspection / compliance; COMSEC account management; Keying material accountability; CryptoNet; COMSEC inspections & audits; COMSEC facility security; Policy compliance

Information Technology Specialist Senior Leader Course (SLC) 531-25B40-C46 — US Army Signal School

2016-08-02 – 2016-09-20 | Diploma

Upon completion of the course, the student will be able to provide leadership necessary to plan, supervise, and coordinate the deployment, operation, management, and maintenance of information technology in mobile and fixed environments; create personal development plans; administer personnel evaluations; develop and administer employee awards programs; implement components of a fitness and wellness program; perform installation and configuration of SQL server; configure network address translation and port address translation; plan, supervise, coordinate, and direct the operation and maintenance of information technology systems; perform integration of a Local Area Network into a Wide Area Network; plan a Local Area Network; perform SQL server installation; create databases to include tables, keys, and relationships; perform administrative tasks on SQL server; plan and implement an active directory infrastructure; perform installation of Windows server; implement active directory; and administer exchange server.

Topics: Senior-level IT operations leadership; Enterprise networking concepts (LAN/WAN); Server and directory services administration concepts; Planning, resourcing, and readiness management; Training management and leader development

Skills: Cisco Wide Area Network (Wan) Technologies; Server Administration; Database Management; Decision-Making; Leadership; Networking; Windows administration; Active Directory; Exchange Server; SQL / database administration; Database design & administration; Strategic IT planning; Personnel evaluations; Awards program management; Fitness & wellness program oversight; SQL Server installation; NAT/PAT configuration; Active Directory design; Windows Server installation; Exchange Server administration

Certified Authorization Professional (CAP-RMF/eMASS) (5 days) — Army in Europe ITT Program

Certificate

RMF / eMASS-focused training aligned to the Certified Authorization Professional (CAP) body of knowledge. Covers RMF steps, security control selection/implementation/assessment, authorization package development, POA&M management, and eMASS workflows.

Topics: NIST Risk Management Framework (RMF) steps; Security categorization and control selection; Control implementation and evidence collection; Assessment support and POA&M management; eMASS workflows and reporting; Authorization decision support

Skills: NIST RMF; eMASS; Authorization packages; Security controls; POA&M management; System categorization; Control implementation; Control assessment support; ATO process; Continuous monitoring governance

Signal Digital Master Gunner 531-F75 (CT) — US Army Signal Center and School

2012-08-08 – 2012-09-12 | 203 hrs | Diploma

Upon completion of the course, the student will be able to integrate, operate, and maintain LAN hardware and software; administer data servers; and troubleshoot and maintain workstation, gateways and VoIP systems.

Topics: Enterprise signal systems troubleshooting; Network operations and service assurance; Routing/switching and LAN integration concepts; Server/service administration concepts; VoIP fundamentals and troubleshooting; Training others on digital systems operations

Skills: Internetworking Basics; Network Systems Administration; Server Administration; LAN integration; Server administration; VoIP troubleshooting; Network operations; Enterprise troubleshooting

Structured Self Development (SSD) IV (1-250-C49-4 (DL)) — SGM Academy - Structured Self Development / Ft Bliss, TX

2011-11-02 – 2011-11-09 | ACE-evaluated military course (JST)

Upon completion of the course, the student will be able to evaluate and manage various military related activities; critique and validate various military related activities; and develop various military - related programs.

Topics: Senior leader self-development modules; Leadership and professionalism topics; Operational and organizational concepts; Army programs and administrative requirements

Skills: Leadership; Military Operations; Leadership development; Program evaluation; Operational management; Decision making

Structured Self Development (SSD) III (1-250-C49-3 (DL)) — SGM Academy - Structured Self Development / Ft Bliss, TX

2011-10-21 – 2011-11-01 | ACE-evaluated military course (JST)

Upon completion of the course, the student will be able to conduct various military related tasks; develop various military related programs; supervise various military related activities; and engage in various leadership activities.

Topics: Leader self-development modules (mid-career); Leadership foundations and problem solving; Army programs and administrative requirements; Preparation for advanced PME

Skills: Leadership; Military Science; Leadership development; Program supervision; Military staff processes; Training management

Honor Graduate Letter (Class 25B-018-11, ALC) — Noncommissioned Officer Academy

Recognition

Recognition for graduating as Honor Graduate (top performer) for the referenced course/class.

Topics: Formal recognition for top performance in ALC; Indicates academic excellence and leadership potential

Skills: Academic excellence; Discipline; Technical mastery; Professionalism

Information Technology Specialist Advanced Leader Course (ALC) 531-25B30-C45 — US Army Signal Center and School

2011-08-23 – 2011-10-19 | 578 hrs | Diploma

Upon completion of the course, the student will be able to supervise the deployment, operation, management, and maintenance of information technology (IT) systems in mobile and fixed facilities; serve in a leadership role for IT operations and maintenance; and supervise a field training exercise.

Topics: Supervision of IT operations and maintenance; LAN/WAN and network security concepts; Leadership, supervision, and management; Planning and executing field training exercises; Troubleshooting and readiness management

Skills: Cisco Lan Switching And Wireless; Cisco Wide Area Network (Wan) Technologies; Introduction To Management; Network Security; Supervision; Leadership; Training development; IT operations supervision; LAN/WAN design; Wireless networking; Field training exercise leadership; Network security; Team leadership

Army Basic Instructor (5K-SI5K/012-SQI8) — PS - Personnel Services BDE / US

2010-10-30 – 2010-11-08 | ACE-evaluated military course (JST)

Upon completion of the course, the student will be able to develop classroom lesson plans with the analysis, design, development, implementation, and evaluation (ADDIE) model in mind; to demonstrate effective management techniques for classroom instruction; to understand various learning theories; adult learning styles; and Bloom's taxonomy; and to understand formal and informal evaluation techniques. Teaching or Classroom Management for Teachers

Topics: Instructional design (ADDIE); Adult learning principles and learning theories; Lesson plan development; Facilitation and classroom management; Evaluation and assessment techniques

Skills: Introduction To Teaching And Learning or Principles Of Learning And; Instructional design; ADDIE model; Bloom's taxonomy; Lesson plan development; Adult learning principles; Classroom facilitation; Student assessment; Learning theories

Warrior Leader (Modified) (600-WLC (MOD)) — NCO Academy / Ft Sill OK

2010-01-07 – 2010-01-22 | ACE-evaluated military course (JST)

Upon completion of the course, the student will be able to function as a junior level leader with essential skills in leadership, training, warfighting and administration

Topics: Junior NCO leadership foundations; Training management and small-unit leadership; Warfighting fundamentals and discipline; Army administration and counseling

Skills: Leadership Principles; Military Science; Leadership; Training development; Small unit leadership; Training management; Warfighting fundamentals; Army administration; Counseling & mentorship

Computer Network Defense (921-640) — Readiness Training Center / Ft McCoy, WI

2007-02-26 – 2007-03-09 | ACE-evaluated military course (JST)

Upon completion of the course, the student will be able to demonstrate an understanding of the legal and ethical issues of intrusion defense, demonstrate an understanding of common computer security flaws, implement encryption in the network, execute post-intrusion actions, demonstrate an understanding of the methodologies of computer intrusions, and utilize network perimeter defense tools.

Topics: Legal and ethical considerations in defense; Common computer/network security flaws; Encryption and secure communications concepts; Post-intrusion actions and incident handling; Network perimeter defense tools and methodologies

Skills: Computer Security; Networking; Cryptography / encryption; Intrusion defense; Legal & ethical considerations; Perimeter defense tools; Network encryption; Post-incident actions; Vulnerability awareness

Information Systems Operator-Analyst (531-74B10) — Signal School / Ft Gordon GA

2003-09-29 – 2004-02-02 | ACE-evaluated military course (JST)

Upon completion of the course, the student will be able to demonstrate a basic working knowledge and understanding of microcomputer software, computer operating systems, software utilities, assembly/disassembly of microcomputers, data communications, local area networks, problem solving using structural design techniques, data base system design, develop and error recovery and security. Students will be able to use personal computer hardware and basic computer applications software.

Topics: PC hardware assembly/disassembly and maintenance; Operating systems fundamentals (desktop/server concepts); LAN fundamentals and data communications; Software utilities and application support; Database fundamentals and problem-solving methods; Basic security and error recovery procedures

Skills: Cisco Router Fundamentals; Computer Applications; Computer Hardware Repair; Computers And Communications; Network Fundamentals; Windows Desktop Operating Systems Administration; Windows Server Administration; Networking; PC assembly/disassembly; Operating systems fundamentals; LAN administration; Data communications; Database design; Troubleshooting; Security fundamentals; Technical documentation

Basic Combat Training (750-BT) — Joint Services Transcript (JST)

2003-06-13 – 2003-08-14 | ACE-evaluated military course (JST)

Upon completion of the course, the student will be able to demonstrate the skills necessary for survival in a combat environment including marksmanship, physical conditioning, navigation, and combat techniques.

Topics: Soldier fundamentals and discipline; Marksmanship and weapons safety; Physical conditioning and fitness; Land navigation and fieldcraft; Basic tactical and combat skills; First aid and combat lifesaver basics

Skills: First Aid; Marksmanship; Physical Conditioning; Land navigation; Physical fitness; Combat techniques; Weapons safety; Fieldcraft; Teamwork; Discipline; Small-unit tactics

AMEDD Field Sanitation Team Certification Course — US Army AMEDD / Preventive Medicine

DD214-listed military education

Field Sanitation Team (FST) certification trains Soldiers to identify, prevent, and mitigate health threats in field environments. Focuses on hygiene, water and food safety, waste management, disease prevention, and environmental risk controls to reduce non-battle injuries and maintain unit readiness.

Topics: Field hygiene and disease prevention; Water testing, purification, and distribution controls; Food service sanitation and inspection basics; Waste disposal and vector control; Heat/cold injury prevention; Risk assessment and reporting for field health hazards

Skills: Preventive medicine basics; Environmental health awareness; Water/food safety fundamentals; Risk identification and mitigation; Operational readiness support; Inspection and reporting

Blue Force Tracker (BFT) Leader Network Course — US Army / Mission Command Systems Training

DD214-listed military education

Leader-focused training on Blue Force Tracking (BFT) / tactical mission command tracking systems. Emphasizes system setup, message traffic, situational awareness, network connectivity, and troubleshooting to support operational reporting and common operating picture updates.

Topics: System setup and configuration; Position reporting and situational awareness; Message composition and routing; Network connectivity and troubleshooting; Operational reporting workflows

Skills: Tactical mission command systems; Operational reporting; System configuration; Troubleshooting; Communications interoperability

Joint Planning Course — Joint Staff / Joint Professional Military Education (JPME)

DD214-listed military education

Joint Planning instruction on the Joint Planning Process (JPP) and operational planning fundamentals used across Combatant Commands and joint staffs. Covers mission analysis, course of action development, orders production, and briefing techniques aligned to joint doctrine.

Topics: Joint Planning Process (JPP) overview; Mission analysis and problem framing; COA development and comparison; Orders and briefing products; Operational art and design basics; Staff integration and battle rhythm

Skills: Operational planning; Mission analysis; COA development; Staff coordination; Briefing and communication

Senior Enlisted Joint Professional Military Education II (SEJPME II) — Joint Knowledge Online (JKO) / Joint Staff

DD214-listed military education

Senior enlisted joint education focused on joint operations, strategic context, interagency/coalition integration, and senior-enlisted leadership responsibilities in joint environments.

Topics: Joint functions and joint operations overview; Strategy-to-task linkage and theater context; Interagency/coalition integration concepts; Senior enlisted roles in joint staffs; Operational-level communication and leadership

Skills: Joint operations literacy; Strategic awareness; Interagency coordination; Senior enlisted leadership; Professional military education

SHARP (Sexual Harassment/Assault Response & Prevention) Course — US Army

DD214-listed military education

SHARP training focused on prevention, reporting procedures, victim advocacy concepts, leader responsibilities, and creating a professional command climate that prevents harassment/assault and supports reporting and response.

Topics: Prevention and bystander intervention concepts; Reporting options and response processes; Leader responsibilities and command climate; Victim advocacy basics and resources; Policy and compliance fundamentals

Skills: Program compliance; Professional climate leadership; Reporting process awareness; Prevention mindset

COMSEC Manager Course — US Army / COMSEC Training

DD214-listed military education

Advanced COMSEC program management training for supervising COMSEC accounts, enforcing cryptographic security policies, and managing audits/inspections. Builds on custodian skills with emphasis on program oversight, risk management, and corrective action planning.

Topics: COMSEC program oversight and governance; Keying material lifecycle management; Cryptographic incident reporting; Audit and inspection preparation; Corrective action planning and training

Skills: COMSEC program management; Audit readiness; Policy enforcement; Risk mitigation; Training management

Standardized Communications Security Custodian Course — US Army / COMSEC Training

DD214-listed military education

Custodian-focused course covering COMSEC fundamentals: safeguarding keying material, maintaining accurate account records, physical security requirements, and compliance with handling, issue/receipt, and destruction procedures.

Topics: COMSEC fundamentals and responsibilities; Keying material control and accountability; Physical security standards for COMSEC; Records management and reporting; Audit readiness basics

Skills: COMSEC custody; Accountability; Records management; Physical security compliance; Procedural discipline

System Administrator / Network Manager Security Course — US Army / Signal Training

DD214-listed military education

Security-focused systems administration and network management instruction emphasizing secure configuration, access control, patching, logging, and basic defensive practices for maintaining mission IT services.

Topics: Secure configuration and baseline management; Account/access control fundamentals; Patching and vulnerability awareness; Logging and monitoring fundamentals; Incident reporting basics

Skills: System administration; Secure configuration; Access control; Operational hardening; Security monitoring fundamentals

Computer Network Defense (Level 3) Course — US Army / Signal or Cyber Training

DD214-listed military education

Advanced or follow-on computer network defense training (as listed on DD214) building on intrusion defense fundamentals. Focus typically includes defensive tool usage, incident response actions, and deeper understanding of attacker techniques.

Topics: Intrusion detection/defense concepts; Defensive tools and procedures; Incident response actions; Attacker methodology awareness; Network perimeter defense

Skills: Network defense; Intrusion defense; Incident response fundamentals; Perimeter security

CompTIA Advanced Security (CASP) Course (prep) — US Army / Commercial training (as listed on DD214)

DD214-listed military education

Preparation course aligned to CompTIA Advanced Security Practitioner (CASP) objectives—advanced security architecture, enterprise security operations, risk management, and integration of security solutions.

Topics: Enterprise security architecture concepts; Advanced risk management; Security operations and incident response; Integration of security controls and tools; Identity and access management concepts

Skills: Security architecture; Risk management; Security operations; Control integration

Security+ (Level 2) Course (prep) — US Army / Commercial training (as listed on DD214)

DD214-listed military education

Baseline cybersecurity training aligned to Security+ objectives—confidentiality/integrity/availability principles, network security basics, risk concepts, and foundational incident response/security operations terminology.

Topics: Security fundamentals (CIA triad); Network security basics; Threats, vulnerabilities, and controls; Identity and access management basics; Incident response fundamentals

Skills: Security fundamentals; Network security; Risk concepts; Security operations basics

Linux+ Course (prep) — US Army / Commercial training (as listed on DD214)

DD214-listed military education

Linux administration fundamentals aligned to Linux+ objectives—shell usage, filesystem management, basic services, permissions, and troubleshooting.

Topics: Linux command line and shell basics; User/group and permissions management; Filesystem and process management; Basic networking on Linux; Troubleshooting and log basics

Skills: Linux administration basics; Command line proficiency; Troubleshooting; Permissions management

Certified Information Systems Security Professional (CISSP) Course (prep) — US Army / Commercial training (as listed on DD214)

DD214-listed military education

CISSP-aligned preparation covering security management, asset security, security architecture/engineering, communications/network security, IAM, security assessment/testing, security operations, and secure software development concepts.

Topics: Security and risk management concepts; Security architecture and engineering basics; Network security concepts; Identity and access management basics; Security operations and incident response concepts; Assessment/testing fundamentals

Skills: Security program fundamentals; Risk management; Security operations; Security architecture concepts

Publications

Automating RMF Steps Using Lightweight Scripts and Tools

SANS | 2022-10-14

Link: https://www.sans.org/white-papers/automating-rmf-steps-using-lightweight-scripts-and-tools/

Awards & Recognition

Award

2019-08-30

Named Honor Graduate for top academic/performance standing in the course cohort; reflects mastery of AEHF SATCOM mission planning and rapid application to unit readiness improvements.

Award

2011-10-19

Honor Graduate recognition awarded to a top-performing student in an NCO professional military education course focused on advanced IT operations and leadership.

Award

2018-05-11

Certificate of appreciation recognizing meaningful contributions/support to an Army NCO Academy mission (e.g., instruction, mentorship, or operational support).

Award

2019-11-22

Top-box potential rating used in the Army's NCO Evaluation Report system. Indicates the Senior Rater assessed performance/potential as among the very best compared to peers in the grade.

Award

2020-09-24

High potential rating used in the Army's NCO Evaluation Report system. Indicates strong performance and potential relative to peers.

Award

2020

Selection to represent/advise on Communications Security (COMSEC) matters at an Army-wide level based on technical expertise and credibility.

Award

Latin honors designation reflecting exceptional academic achievement for an undergraduate degree program.

Award

None

Selected to serve on the GIAC Advisory Board—typically indicates recognized expertise and contribution to the GIAC/SANS certification community (e.g., feedback on certification/program direction).