Earn continuing education units with these free, on-demand webinars.

Having trouble viewing this email? Click here to view in a browser.

Maintain Cybersecurity Certifications with On Demand Continuing Education

AFCEA's continuing education program is specifically targeted to support maintenance of cybersecurity certifications related to DoD 8570.01-M compliance. See tips for preparing continuing education documentation under FAQ #4.

Please note, if you haven't previously registered for a webinar, you will need to do so first to access the on-demand link.

CROWDSTRIKE

Time To Modernize Enterprise Cyber Threat Hunting

Approved for 1 CompTIA CEU for A+, Network+, Security+, Linux+ and Cloud+, 1 GIAC CPE and 1 CertNexus CEC for CyberSec First Responder (CFR).

With so many sources of cyber threat intelligence, both commercial and opensource, including advances in automation, specifically AI/ML and the latest dialog

around generative AI as another emerging threat vector, it begs the question do cyber defenders need to re-evaluate how cyber threat hunting is performed across an enterprise? For far too long the cyber threat hunting model has been reactive.

This webinar explores how cyber defensive teams can become more proactive and leverage the latest in automation, tools and techniques to look around corners and get a head start on the adversary.

Access Webinar

Resilient Networking for the Tactical Edge

Approved for 1 CompTIA CEU for A+ and Network+.

Networks of the future will self-configure for high bandwidth communications, but will function with low bandwidth alone and they will be tolerant of transports with various latency and capacity (cellular, satellite communications (SATCOM), direct line of sight, free space optic, tactical data links). These resilient tactical networks will enable automatic primary, alternative, contingency, emergency (PACE) communications between all available transports and manage capacity to ensure quality of service across the network. Commercial software-defined wide area networking (SD-WAN) technologies have the potential to bring critical capability in enabling the much-needed revolution towards resilient tactical networking, however, these solutions are limited by a focus toward fixed enterprise networks.

This webinar explores how SD-WAN can be augmented to meet the unique challenges of the tactical edge network including latency and throughput disparity, heterogenous networks, encryption, disconnected operations, efficient authentication methods and centralized orchestration.

Access Webinar

Optimize Network Access at the Tactical Edge with Software-Defined Wide Area Networking

Approved for 1 CompTIA CEU for A+, Network+, Security+, Linux+, Cloud+, PenTest+, CySA+ and 1CertNexus CEC for Cybersecurity First Responder (CFR).

Software Defined Wide Area Networking can help address the connectivity challenges and provide access to critical data and networks rapidly and reliably, even in the most isolated and austere environments. Software Defined

Networking, deployed to the tactical edge, can ensure that you automatically make the most of the transport options that are available in any given location, such as SATCOM, 4G/5G or even fixed infrastructure without relying on predefined PACE (Primary, Alternate, Contingent, Emergency) plans.

Availability is a key part of cybersecurity. Join experts in this educational webinar exploring how cutting-edge SD-WAN technologies can ensure that you have the fastest and most reliable access to your data.

Access Webinar

Securing Communications at the Tactical Edge Using Hardware Security Modules

Approved for 1 CompTIA CEU for A+, Network+, Security+, Linux+, and Cloud+ and 1 GIAC CPE.

Today's warfighters and the network architects who design the communications networks they rely on are faced with adversaries that are increasingly sophisticated. It's critical that sensitive and classified information is secured while in transit and at rest.

Public key cryptography plays an essential role in securing this data, whether it is CUI data used throughout the federal government or secret and top secret data secured through the NSA's Commercial Solutions for Classified (CSfC) program. Turnkey solutions for a PKI environment are crucial in delivering secure data to warfighters at the tactical edge and remote workers around the globe.

Learn about factors in selecting and using Hardware Security Modules (HSM) for secure generation and storage of private key data and how this plays a critical role in data security and integrity.

Access Webinar

Cross-Domain and Secure Remote Access Solutions at the Edge

Approved for 1 CompTIA CEU for A+,Network+, Security+, Linux+ and Cloud+ and1 GIAC CPE.

In today's rapidly evolving defense landscape, expeditionary teams require secure, fast and efficient access to multiple networks and data sources from varying security levels. This is essential to maintain situational awareness and provide robust decision support. To meet these demands, it is crucial to minimize

the size, weight and power (SWaP) of deployed solutions for optimal performance at the tactical edge.

Chris McCloskey, Sales Engineer from Forcepoint and Dominic Perez, CTO at Curtiss-Wright Defense Solutions, discuss the challenges and best practices for deploying cross-domain solutions (CDS) in accordance with the latest Raise the Bar (RtB) requirements from the National Cross-Domain Strategy Management Office (NCDSMO) for securing remote access to classified networks.

Access Webinar

How To Leverage Defense-in-Depth to Minimize Risk

Approved for 1 CompTIA CEU for A+, Network+, Security+, Linux+, and Cloud+, 1 GIAC CPE and 1 CertNexus CEC for CyberSec First Responder (CFR).

Federal agencies are not immune to security attacks, even if their controls and processes are as tight as Fort Knox. Some of the world's most technologically advanced enterprises have faced security incidents and were exposed to risk.

Many of these successful cyber attacks did not start with hackers fighting their way through firewalls and intrusion prevention systems or executing zero-day exploits. Instead, threat actors compromised user credentials, took over legitimate user identities and gained access to internal systems and resources.

Learn about use cases that illustrate identity security and defense-in-depth strategies.

Access Webinar

How To Meet Zero Trust and Other High-Level Government Security Standards

Approved for 1 CompTIA CEU for A+, Network+, Linux+ and Cloud+, 1 CertNexus CEC for CyberSec First Responder (CFR) and 1 GIAC CPE.

Developers and security experts are now tasked with extending Kubernetes' built-in security to effectively protect against more complex, volatile and frequent cyber attacks. The previous "trust but verify" approach has often proven ineffective for the complex distributed nature of cloud

computing, so Kubernetes security is being elevated to the "never trust, always verify" ideology of the zero-trust model to provide greater protection to organizations.

Key takeaways include basic concepts of the zero-trust model, three best practices, optimizing software configuration and more.

Access Webinar

---

opentext™

Defending Sensitive Government Data Against Modern Cyber Threats With Network Detection and Response (NDR)

Approved for 1 CompTIA CEU for A+, Network+, Security+, Linux+, Cloud+, PenTest+, CySA+, and CASP+, 1 CertNexus CEC for CyberSec First Responder (CFR) and for 1 GIAC CPE.

Network detection and response solutions can help detect potential breaches and prevent attackers from disrupting operations or exfiltrating data. Learn how to sort the signal from the noise when analyzing massive volumes of network events. By minimizing false positives, analysts can focus on the most serious threats—helping to drive down response times.

Learn how you can identify and eliminate the blind spots in your network to detect highly evasive attackers in fast-evolving infrastructures. In this webinar, security experts from OpenText and MAD Security discuss case studies, best practices and the methods NDR supports to identify malicious behavior on the network and how to detect unknown threats that other technologies miss and investigate and respond to them faster with NDR.

Access Webinar

PESA

PESA SECURA VDS - The Secure Eyes and Ears of Command and Control, C5ISR and JADC2 Applications

Approved for 1 CEU for CompTIA A+.

Secure video and audio, along with other types of data, enables warfighters to make faster and better decisions with real-time video input. AV/IP data also flow into artificial intelligence algorithms and data analysis engines to rapidly identify, assess and take action against adversaries. SECURA's certified secure AV/IP was developed specifically for optimal security and scalability of command and control centers, Navy combat information centers, briefing rooms, watch rooms and operations centers.

SECURA can be implemented virtually and securely in a single C2 room, across multiple C2 rooms in one building, across multiple buildings in one campus or base, across multiple locations CONUS and OCONUS, from on-premise to the cloud and all the way to the edge of the cloud using Kubernetes.

SECURA video distribution system (VDS) applies to other JADC2 implementations, such as ABMS (Air Force), Project Overmatch (Navy), Project Convergence (Army), FNC3 (OSD) and Mosaic Warfare (DARPA). In one system, SECURA delivers a highly secure VDS and keyboard, video, mouse (KVM) system with Multiple Independent Levels of Security (MILS). With end-to-end AES 256 encryption, dynamic keys, multifactor authentication and mutual authentication, SECURA was designed at its inception for the zero-trust environment.

Access Webinar

Leveraging Cloud and Edge-Based Video Distribution Systems (VDS) To Realize the JADC2 Vision for Command and Control

Approved for 1 GIAC CPE.

The Defense Department's future battlefield network needs the cloud to increase command and control capabilities, to provide global accessibility and to directly support the warfighters at the tactical edge. Lessons learned in Ukraine highlight the importance of unified command and control between the U.S. military and its allies, the ability to rapidly and securely share massive amounts of data from a growing number of sensors and satellites and the need to link sensors and warfighters to achieve their missions.

The Video Distribution System (VDS) provides the mission-critical "eyes" (video) and "ears" (audio) for all C2 centers. For JADC2, the VDS must support the cloud and the cloud edge to meet the mission. The strategy needs a VDS that is certified-secure, cloud-architected and highly scalable AV/IP VDS, with multiple independent levels of security (MILS) and end-to-end AES 256 encryption, architected for zero-trust environments.

This type of VDS is also needed for field commands, intelligence surveillance reconnaissance (ISR), combatant commands, multi-domain, multiple geographical locations, ABMS, Project Overmatch, Project Convergence and future JADC2 centers. It should leverage the infrastructure of any of the leading cloud vendors and must operate on-premise, in the cloud and at the cloud edge to support current and future missions.

Access Webinar

Zero Trust: Take Your Cybersecurity Back to the Future

Approved for 1 CompTIA CEU for A+, Network+, Security+, Linux+ and Cloud+, 1 GIAC CPE and 1 CertNexus CEC for CyberSec First Responder (CFR).

Zero trust insists we trust no one and verify everyone before they come through the locked door into our secure room or segmented network. It goes back to identity-based authentication and access controls so that bad actors can't exploit easily compromised credentials to gain privileged access, move around the network and steal sensitive data. The future of cybersecurity demands it and the zero-trust architecture simply defines it.

This webinar discusses the challenges of this journey and guidance on ways to ease it.

Access Webinar

Layering Public Records and Blockchain Analytics to Enhance Cryptocurrency Investigations

Approved for 1 GIAC CPE, 1 CertNexus CEC for CyberSec FirstResponder (CFR) and 1 CompTIA CEU for A+.

From sanctions evasion and large-scale fraud to drug trafficking and terrorist financing, illicit actors are increasingly turning to cryptocurrencies to carry out their illegal activities. And while threat actors largely use virtual currencies to remain anonymous, investigators can better unmask and target these networks with access to the right data and technology.

This masterclass from Sayari and Chainalysis shows how pairing public records with blockchain analytic scan drive more effective investigations into crypto-related fraud and money laundering.

Topics include:

- Money laundering via cryptocurrencies—a 30,000-foot view
- Types of on-chain entities used to facilitate crypto-related illicit finance
- Illicit funds statistics in cryptocurrency
- A case study analyzing the Hash Flare crypto fraud and money laundering network

Access Webinar

TechNet Augusta 2022 Webinar Series
Game Changer: Operationalizing Cybersecurity

Approved for: 1 GIAC CPE, 1 CertNexus CEC for CyberSec First Responder (CFR) and 1 CompTIA CEU for A+, Data+, Network+, Security+, Linux+, Cloud+, PenTest+, CySA+, and CASP+.

The Army Unified Network Plan (AUNP) addresses Army information technology and the network in a comprehensive approach to enable Multi-Domain Operations (MDO). The AUNP establishes five lines of effort (LOE), number three specifically being Security and Survivability—Commander's Freedom of Action in Cyberspace. To support LOE 3, it was imperative to reform and operationalize cybersecurity processes and the way the Army manages risk. Operationalizing cybersecurity is being implemented through the Army's Risk Management Framework (RMF) 2.0.

Presenters explain how RMF 2.0 shifts from a culture of compliance to a culture of defend and react by monitoring the current cybersecurity posture by focusing on the right controls versus all controls. They will show how the Army has set up the Army Cyber Risk Management Council (ACRMC) to look at high- and very high-risk systems and bring these decisions from current authorizing officials to Army senior leaders.

Access Webinar

AFCEA Solutions: Making the Case for a Federal Bureau of Statistics

Approved for 1 CertNexus CEC for CyberSec First Responder (CFR) and 1 CompTIA CEU for A+, Network+, Security+, Linux+ and Cloud+.

The Cyberspace Solarium Commission recommends creating a federal bureau of statistics to support a broad range of needs, as well as public and private sector users. Such a bureau's work would be useful to U.S. national and economic security, as well as to government, critical infrastructure and private businesses.

During this *SIGNAL* Media Webinar, cybersecurity experts tackle how professionals, the public, policymakers and decision-makers suffer from anecdotes masquerading as data, and discuss the trends lines drawn from highly visible incidents that can lead to effective processes, safeguards and trust for cyber data collection and sharing.

Access Webinar

AFCEA Solutions: 'Digital Chatter' — The Growing Challenge of Mis/Disinformation

Approved for 1 GIAC CPE and 1 CertNexus CEC for CyberSec First Responder (CFR) and 1 CompTIA CEU for A+, DataSys+, Network+, Linux+ and Cloud+.

Cyber threats related to mis/disinformation are rapidly evolving. Artificial intelligence (AI), deep fake technology and machine learning have the potential to greatly expand the capabilities—and the reach—of mis/disinformation. New language model technologies have the potential to generate extensive amounts of mis/disinformation—much of which may be distributed without fact-checking resolution.

Enemy states and terrorist groups may use these developing technologies to deliver cognitive attacks that potentially damage community, organizational and national security on a larger scale than previously observed. The same communication tools that improve our quality of life may be used to destroy it, if left unchecked. Across the globe, there has been much discussion on increasing legislation and regulations on social media platforms, AI tool sand related technologies.

Cyber experts explore how best to counter these emerging cyber threats and the required innovative solutions that understand the evolving impacts of social media on our society, along with the rapidly changing capabilities of technologies that support the irresponsible and malicious spread of mis/disinformation across the internet.

Access Webinar

Accelerating Mission Success Through Enterprise Analytics

Approved for 1 GIAC CPE.

Maintaining superiority, readiness and operational advantage requires a transformational approach to leveraging data as a strategic asset. Amid a range of emerging threats and disruptors, enterprise self-service analytics are imperative for faster and more informed mission and business decisions. By implementing data strategies and modernizing data governance, processes,

technologies and architectures, organizations are improving data access and capabilities for users. However, enterprise-wide adoption and data-driven decision-making at scale remain a challenge.

During this webinar, data leaders share perspectives and examples on how organizations can overcome this challenge while cultivating a data culture and bolstering the workforce's data literacy and analytics skills. Learn how enterprise data and analytics platforms are optimizing performance and accelerating mission outcomes.

Access Webinar

Zero Trust-based Remote Access for Operational Cybersecurity

Approved for 1 GIAC CPE and 1CertNexus CEC for CyberSec First Responder (CFR), and 1 CompTIA CEU for A+, Network+, Security+, Linux+, Cloud+, PenTest+, CySA+ and CASP+.

Zero Trust Network Access (ZTNA) solutions brought simplicity, scalability and more security for IT remote access use cases. This is long overdue for industrial cybersecurity. Traditional IT security approaches such as VPNs and Jump servers as well as IT security-oriented ZTNA solutions have several limitations and complexity when it comes to providing streamlined and fully secure remote access for an Operational Technology (OT) environment where policies must be enforced for OT assets at the lowest level of the network.

During this webinar, U.S. Space Force and Xage Security experts explore how a Cybersecurity Mesh-based approach combined with zero-trust principles can enable secure access to OT assets at different levels without compromising security measures like opening up RDP and VNC protocols through firewalls. They also discuss how the distributed enforcement of security services on a per-asset basis with least privilege access and distributed data protection services can improve resiliency across various systems.

Access Webinar

STAY CONNECTED:

AFCEA International
4114 Legato Road, Suite 1000, Fairfax, VA 22033-4002
703-631-6100

Email Preference Management
Unsubscribe