Check out these free, on-demand continuing education-approved webinars.

.

Earn Continuing Education Units for Cybersecurity Certification Maintenance

AFCEA's continuing education program is specifically targeted to support the Department of Defense Cyberspace Workforce Qualification and Management Program. 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.

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

CURTISS-WRIGHT

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 1 CertNexus 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

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

REDSEAL

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

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

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

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

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

---

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 will 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

---

xage SECURITY

Zero Trust-based Remote Access for Operational Cybersecurity

Approved for 1 GIAC CPE and 1 CertNexus 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. We will 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

Classified Mobility Solutions: Streamlining Implementation and Operations

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

Join Gary Markham, vice president of technology, IGS, and John Glover, senior software engineer, Curtiss-Wright, in an in-depth exploration of challenges in deploying enterprise-scale classified mobility and how large-scale defense and federal organizations can overcome challenges using automated provisioning and management.

Access Webinar

Configuring Tactical Hardware In Minutes, Not Hours: A Practical Guide to Desired State Configuration at the Edge

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

Will Lester, VP of Engineering at NexTech Solutions, and Dominic Perez, CTO at Curtiss-Wright Defense Solutions discuss how automation can bring our battlespace into a cloud-native landscape operating alongside legacy and virtualized applications to maximize situational understanding and improve warfighter effectiveness.

Access Webinar

DoD CIO Presents: Software Modernization

Approved for 1 CertNexus CEC for CyberSec First Responder (CFR).

The Software Modernization Senior Steering Group (SW Mod SSG) is leading the strategy and delivering an implementation plan. It is tri-chaired by the Offices of the DoD Chief Information Officer (CIO), the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), and the Under Secretary of Defense for Research and Engineering (OUSD(R&E)).

Technical implementation is delegated to the Action Officer Working Group, with chairs appointed by the SSG to identify and prioritize activities, convene working groups, and provide metrics for tracking progress advancing the creation of DoD software. The three AOWG chairs discuss the implementation plan and the activities they are leading and monitoring to move the Department forward and deliver on the Software Modernization Strategy goals:

- Accelerate the DoD Enterprise Cloud Environment
- Establish Department-wide Software Factory Ecosystem
- Transform Processes to Enable Resilience and Speed

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 from this webinar include:

- Basic Concepts of the Zero-Trust Model
- Three Best Practices for Zero Trust
- Optimize Software Configuration, Access Permissions Log and Monitor Data
- Focus on People and Process Management
- How to Create a Zero Trust Security Culture

Access Webinar

STAY CONNECTED:

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