Trent Tucker,
M.S. CISSP, CMMC CCA, CCNA

Desired Location: Remote. United States. Overseas

Active Top Secret Security Clearance

Objective: Cyber Security Assessor/Auditor,FedRAMP Consulting, CMMC Readiness, CMMC Assessment Team Member (ATM), Information System Security Engineer

Technical Skills

Cloud Infrastructures(AWS, Azure)
BGP
OSPF
GRE/mGRE
MPLS
DMZ
IPSec
SSL/TLS
VPN
VRF
Vulnerability Scanning
TCP/UDP Packet Analysis
IDS/IPS

Cyber Security Standards and Frameworks

NIST 800-37 (RMF)
NIST SP 800-53 rev5
NIST SP 800-53a rev5
NIST SP 800-171 (CMMC)
CMMC Scoping Guide Level 1 and Level 2
CMMC Assessment Process (CAP)
NIST CSF 1.1
PCI-DSS 4.0
FedRAMP
ISO 27001:2022
ISO 27002:2022
DISA STIG
CIS Benchmarks

Cloud Services

Azure Firewall
Azure Security Center
Azure VPN Gateway
AWS VPC

Cyber Network Devices

Cisco Routers
Cisco Switches
Cisco ASA Firewalls
Palo Alto Firewalls
F5 Load Balancers

Professional Summary

Dedicated Sr.Cyber Security Leader that possesses an **ACTIVE TOP SECRET CLEARANCE** with expertise performing cyber security assessments, vulnerability scanning, implementing security controls based on cyber security standards, and configuring network security engineering solutions such as VPN and firewalls.

Certifications

Certified Information Systems Security Professional (CISSP) - DoD 8570 Information Assurance Manager Level III Certified
CompTIA Advanced Security Practitioner CE (CASP) - DoD 8570 Information Assurance Technical Level III Certified
CMMC Certified Assessor (CCA) – NIST 800-171 Level 2 Consulting and Assessment
CMMC Certified Professional (CCP) – NIST 800-171 Consulting and Assessment
DISA Assured Compliance Assessment Solution v. 5.3 (ACAS) - Nessus Vulnerability Scanner
Microsoft Azure Cloud Fundamentals Certified
Cisco Certified Network Associate (CCNA)
Palo Alto Firewall Accredited Configuration Engineer (ACE)
CompTIA Cyber Security Analyst (CySA) - DoD CND Certified
Qualys PCI DSS Compliance Foundation Certified
CompTIA Security+ CE - DoD 8570 Information Assurance Technical Level II Certified

Experience

T2 Square Solutions LLC
Montgomery, Alabama

Cyber Security Compliance Consultant (Information Systems Security Officer (ISSO, CMMC Assessor, and Security Control Assessor roles) (Jan 2022-Present)

- Serve as a Cyber Security Compliance Consultant in various roles such as Information System Security Officer (ISSO) and Cyber Security Control Assessor/Auditor based on NIST 800-37 (RMF), NIST 800-53,NIST 800-53a, NIST CSF 1.1, NIST 800-171 (CMMC Level 1 and Level 2 Practices), PCI-DSS 4.0, FedRAMP, CIS Controls 8.0, CIS Benchmarks, DISA STIG, and various additional standards and frameworks.
- Perform DoD Risk Management Framework (RMF) NIST 800-37 for various government agencies.
- Familiar with mapping controls for various different cyber security control frameworks.
- Function as a GRC Information System Security Officer (ISSO) to aid clients achieve compliance with security control frameworks,
- Prepare System Security Plans (SSPs), Cyber Security Policies, and necessary Cyber Security documentation to achieve compliance with industry standards
- Assess clients network enterprise environments as an auditor/assessor to determine the compliance with security controls
- Prepare Clients for NIST 800-171 compliance by reviewing vendor SSP and

identifying gaps prior to assessment.
- Perform network security firewall and VPN configurations.
- Review Vendors SSP documentation based on NIST 800-171 level 1 and level 2 practices and perform readiness assessment based on artifacts, implementation statements, diagrams depicting CUI and FCI assets, and any potential cloud FedRAMP inheritance.
- As a Cyber Security Consultant, tasks are completed based on the establishment of 1099, C2C, or subcontractor agreement.

Government Contractor (Independent Consultant/Subcontractor)
Cyber Security Authorization and Assessment (A&A) Team
Cyber Security Control Assessor (SCA)/Auditor (August 2022-Present)

- Serve as a Cyber Security Control Assessor to assess security controls across on premise network architectures as well as Cloud SaaS based on NIST 800-53 and FedRAMP.
- Perform cyber security assessments based on NIST 800-53a security control assessment procedures within enterprise network enclaves and provide comments based on evidence (examine, interview, or test) to determine whether the security control is satisfied according to NIST standards.
- Conduct vulnerability analysis via vulnerability scanners and assess scan results for vulnerabilities within network architectures.
- Provide technical guidance and configuration guidance to achieve credentialed compliance scanning within the enterprise network architecture of network infrastructure devices with vulnerability scanners.
- Evaluate FedRAMP packages with Agency or JAB ATO and review Cloud Service Provider's Security System Plan (SSP) and access results from the third party assessor organization's (3PAO) Security Assessment Report (SAR) to aid in tailoring specific controls and collecting relevant department artifacts for assessing customer responsible security controls to achieve department ATO.
- Define NIST security controls for the Common Control Provider (CCP) which is expected to be inherited by relevant system packages within the network enclave
- Provide specific recommendations on how to correct weaknesses or deficiencies in the security controls and mitigate vulnerabilities within system specific, hybrid, or common controls.
- Prepare Security Assessment Report (SAR) documentation which includes security assessment findings and recommendation to Authorizing Official (AO) to authorize or not authorize a system.

Gray Link Technologies, LLC
Gunter AFB Montgomery, Alabama
HNI/HNIB-Network Security Engineering Team
Cyber Security Network Advisor (May 2021-August 2022)

- Cyber Network Boundary Security Consultant serving Air Force Network Architecture and demilitarized Zone (DMZ) enclaves to define and mitigate enterprise network vulnerabilities, and produce cyber security engineering solutions.
- Initiate network enterprise security assessments by developing a cyber security baseline of performance and reviewing cyber network devices to define insufficient network security implementations within current network architecture.
- Discover cyber network vulnerabilities by accessing Network Security Event Monitoring Tools, Network Security Detection tools, and reviewing network device configuration to evaluate network performance for network security abnormality.
- Assess network security vulnerabilities discovered by Network Security Detection, Network Security Event systems, and Cyber Network devices and provide recommendations for network security performance optimization.
- Evaluate Firewall security policies and VPN solutions and determine areas of improvement to increase network enterprise security.

Cyber Security Assessment Tools
DISA STIG Viewer
Tenable Nessus Vulnerability Scanner and Security Center
AWS Inspector Vulnerability Scanner
Archer RMF/GRC Tool
eMASS RMF/GRC Tool
Nmap
Forescout CounterACT

Security Incident Event Manager (SIEM)
ArcSight
SPLUNK

Cyber Network Security Management System
Palo Alto Firewall Panorama
Forescout CounterACT

Network Sniffers
Wireshark
TCPDump

Network Security Detection Tools
InfoVista
Extrahop
Netscout
NetCool
Solarwinds
NetQoS

Training
Cisco 9000 Series Router Troubleshooting Course
Palo Alto Firewall PAN OS Version 8.0 Configuration and Troubleshooting Course
JRSS Network Operations (NetOps) Course
DISA Assured Compliance Assessment Solution (ACAS) Operator and Supervisor Course

MSM Technology, LLC
DISA Montgomery, Alabama
DISA-SEL86 Network Engineering Information Assurance Team
Information System Security Engineer(ISSE)/Cyber Vulnerability Security Assessor
(May 2020-May 2021)

- Cyber Network Security/Information Assurance Engineer operating DISA Out-of-Band (OOB) Management and Demilitarized Zone (DMZ) cyber network boundary enclaves, define enterprise network vulnerabilities, and produce cyber security engineering solutions.
- Conducted initial cyber network vulnerability analysis by evaluating network architecture, reviewing DISA STIGs and gaining access to required Cyber Network Devices and Cyber Assessment Tools.
- Scanned cyber network devices for vulnerabilities against Common Vulnerability Databases (CVES and NVD) and initiate false-positive analysis of vulnerabilities identified in cyber network devices
- Performed in-depth network security vulnerability assessments of network device configurations, via DISA STIG, to identify potential vulnerabilities within DMZ and OOB network boundary enclave.
- Review Firewall security policies, routing protocols, and VPN solutions to develop recommended configuration modifications for increased security and network boundary protection.
- Advised network engineers on securing network configurations for operational security maintenance and offered resolutions to mitigate security vulnerabilities and enhance OOB and DMZ cyber enterprise security posture.
- Provided support regarding Direct Tasking Orders (DTO) of Firewall vulnerabilities by developing procedure for evaluating each firewall, establishing comprehensive listing of each vulnerable Firewall and offering vulnerability mitigation strategy.
- Configured and troubleshot cyber security network engineering solutions for increasing enterprise cyber security posture and achieving DISA STIG compliance.
- Validated cyber security network engineering solutions to ensure DISA IAVM compliance by operating network vulnerability scanners and verify adherence to DISA STIGs through performing manual assessment of network device configurations.
- Developed Plan, Action, & Milestones (PO&AMs) document to address vulnerabilities and define a remediation strategy for vulnerability mitigation within a specified timeline.

Heptagon Information Technology, LLC
Gunter AFB, Alabama
JRSS Air Force Service Migration Team
Information System Security Engineer(ISSE)/Cyber Network Vulnerability Security Assessor (November 2018 – May 2020)

- Cyber Security Engineer on the NIPRNet JRSS Air Force Service Migration Team responsible for constructing network boundary protection solutions to ensure confidentiality, integrity, and availability which involved configuring network security devices, assessing current network architecture, and proposing recommendations to enhance network security posture.
- Developed network security engineering implementation plans for migrating AF bases to JRSS which involved identifying network security devices for modification, assessing network architecture, defining network security device configurations, and assuring compliance to DISA STIG guidelines within implementation approach.
- Implemented vulnerability mitigation by engineering network security optimization solutions and performing vulnerability assessments on Cyber Network Devices for AF Network Security Boundary Enclaves based on DISA STIG guidelines.
- Developed context-based Next-Generation Firewall security policy rules and Firewall routing configurations for establishing a Demilitarized Zone (DMZ) within JRSS for AF network traffic.
- Migrated AF bases to JRSS by configuring encrypted Site to Site VPNs which provided

data integrity, encryption, and authentication in accordance with DISA Security Technical Implementation Guide (STIG).
- Analyzed network traffic within Security Incident Event Managers (SIEMS), Network Sniffers, Network Security Management Systems, and Cyber Network Devices to define security related events that may impact network availability and confidentiality.
- Troubleshot AF JRSS network security enclave by evaluating dynamic routing protocols, VPN tunnels, next-generation firewall configuration, and VRF instances to identify source of issue and configure solution with least possible impact to network operations.
- Advise the 26th Network Operations Squadron (NOS) Boundary Protection Team regarding network security policy implementation within JRSS and provide technical insight for resolution of JRSS security enclave deficiencies.

26th Network Operations Squadron

Gunter AFB, Alabama
JRSS Air Force Service Migration Team
Cyber Security Engineer (October 2015 –November 2018)

- One of four lead network migration engineers on the Air Force Service Migration Team for migrating AFB bases to the Joint Regional Security Stacks (JRSS).
- Performed initial network security analysis before migration to determine potential vulnerabilities and collaborated with principal engineers to develop a plan of action for resolution.
- Identified network vulnerabilities within enterprise boundary devices and developed implementation plans to achieve DISA Security Technical Guide (STIG) Compliance.
- Assisted JRSS network support teams with testing connectivity through the enterprise platform by executing network sniffers to analyze network traffic.
- Examined network traffic within Security Incident Event Managers (SIEMS) and Cyber Network Devices to define security related events that may impact network availability and confidentiality.
- Resolved network and security related issues in JRSS by identifying root cause of issue and implementing an optimal course of action that will provide least possible risk impact for organization while maintaining confidentiality, integrity, and availability.
- Troubleshot eBGP,iBGP, routing issues, firewalls, load balancers proxies, and DMVPN infrastructures within Air Force Non-Secure Internet Protocol Router Network (NIPRNet) and Air Force Secure Internet Protocol Router Network (SIPRNet).

The CENTECH Group, Inc.

1763 Taliaferro Trail
Montgomery, AL 36117
Project Management Team (June 2011 to October 2015)
Cyber Security Network Support

- Cyber Security Network Support for the Project Management Team responsible for securing cyber host systems and network devices to ensure data protection and device availability.
- Provided maintenance of cyber systems and supported multiple IT contracts.
- Installed host systems and troubleshot network related issues for operational functionality.
- Implemented vulnerability mitigation with antivirus software and spyware on workstations.
- Performed local area network (LAN) support for Project Management Site and troubleshoot network related issues for availability.
- Enabled LAN accessibility by connecting users to active switch ports.

Education

Colorado Technical University
Masters of Science (M.S) Management Information Systems Security
GPA 3.9/4.0
IT635 Information Systems Auditing

- Established a network security assessment policy for an information technology company. NIST SP 800-53 was implemented as a security control evaluation criteria for identifying compliance in information systems. The network security assessment policy included reporting instructions for notifying customers of potential vulnerabilities found within the audit inspection.

CS654 Information Security Management

- Operated as an Information Systems Security Officer for an information technology company which involved developing a comprehensive information security management plan. The information management security plan included risk management, an employee acceptable use policy, and disaster recovery procedures for maintaining an operational security standard.

CS661 Information Assurance

- Analyzed potential security vulnerabilities of an enterprise network system, compared potential vulnerabilities against NIST SP 800-53 to assess security controls, and defined recommendations for achieving compliance.

CS662 Systems Security Certification and Accreditation

- Implemented Risk Management Framework (RMF) to perform information assurance throughout a network enterprise system, researched and evaluated legacy cyber security frameworks such as DITSCAP and DIACAP for identifying differences in security standard methodologies.

Alabama State University
Bachelors of Science (B.S.) Computer Information Systems
GPA. 3.8/4.0