Michael R. Hannah

Palmdale, CA | C: (661) 618-3677 | E: endcaptex@gmail.com | LI: https://www.linkedin.com/in/michael-hannah-u-aab835120

OBJECTIVE: Targeting an FTE role in Cyber Security, IT/OT Management, Project Management, Threat Intelligence, SCADA Management, IT Security Engineer, Safety, Governance, and Compliance Integrator. A recognized Honorably Discharged, U.S. Army Veteran with an Active DoD T3/5 Security Clearance including sixteen+ (16) overall years of demonstrated experience. And a critical member, responsible for managing a diverse range of local and Diversity, Equity, and Inclusion in the Workplace with several Fortune 500 companies.

KEY ACCOUNTABILITIES:

- Accomplished commissioning of the first diverse classified information objectives based on the NIST Cybersecurity Framework and other applicable security risk assessment standards that included the Special Access Programs.
- Accountable for division's overall performance/success in terms of finances, growth, personnel success/growth, quality of work, creation, and enforcement of team policies, compliance with company standards and policies, and individual project success where OT/Cyber team is involved in the project team.
- Contributed to the leadership and development to bridge large complex, federated organizational security assessments, processes to proactively monitor and govern the effectiveness of Governance Cybersecurity Risk and Compliance controls and services and ensuring the implementation of Cybersecurity Policies within Teneable.sc Vulnerability Monitoring reporting.
- Delivered meticulously integrated data protection via DLP, E-DRM integrated multiple Government information security policies and regulations Risk Management Framework (RMF), ICD-503, JSIG, and NIST 800 series special publications including proficiency in writing RMF authorization packages, incident response, disaster recovery, and forensics principles, design of computing hardware and networking, security-relevant tools, systems, DoD collateral processes, Cloud Security, ACAS - NESSUS, ACAS, DISA STIGs, SCAP, and HBSS.
- Driven to build something from the ground up. Knows when to ask questions and for support, but comes with ideas and solutions. Who can work autonomously and with minimal supervision, and can build a cohesive team made up of a variety of skill sets. A Top-Notch communicator in all mediums (face-to-face, email, presentations, reports, etc.), and can be hands-on and wants to be. Not some faceless person behind a computer.
- Lead threat modeling activities during Secure Development Lifecycle (SDL) to execute the IT vision and goals (Infrastructure Design & Optimization, BIA, Assessment, Strategy, and Framework and Managed oversight of the IT/OT infrastructure).
- Proven autodidact experience in problem-solving skills, Security Assessments, Vulnerability Scans, Security Health Checks, Roadmaps, Remediation, and Compliance Assessments under GDPR, CCPA, PCI, NIST RMF, HIPAA/HITECH, DAAPM, NISPOM, GLBA, PCI, FERPA, FedRAMP, FISMA regulatory requirements.
- **VOLUNTEERED:** Homes4Families – Veteran Home Ownership Affordable Sale Program

Responsible for several internal services including but not limited to:

- ACAS - NESSUS, SPLUNK, SCAP, POA&Ms
- Agile & Six Sigma Framework
- BIA, Assessment, Strategy, Framework
- CIA Triad for Information Systems Assets
- COMSEC Real-world - Contingency Planning
- GDPR Governance Risk and Compliance
- Network TAP/SPAN Cisco Nexus with Data Broker
- APT, HBSS, STIG, HIPS, Gigamon
- IA Vulnerability Analysis Management & Exploits

TPRM Endpoint Security & Encryption
HACS SIN - Oral Technical Evaluation
COBIT, HIPAA/HITECH, FedRAMP
SOX, GLBA, PCI, FERPA
NIST 800 53, DAAPM, NISPOM
QRADAR SIEM Threat Detection
RMF Package Development
Server Virtualization / Cloud experience
Teneable.sc Vulnerability Monitoring

MRHannah

Michael R. Hannah

CompTIA
Michael R Hannah
CompTIA
Security+

PROFESSIONAL REFERENCES: AVAILABLE UPON REQUEST

QUANTIFIED WORK HISTORY:

Freelance Cyber Security Consultant **7/2020 – Present**

Project w/DCS Corp. - F-35 Classified Cyber Security Analyst IV (Sr. ISSO) DoD Contractor

- Certified plans of action and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
- Created, deployed, and managed custom HBSS signatures, monitored HBSS for intrusions, failures, and other issues.
- Delivered technical guidance focused on information security architecture, and directed appropriate senior leadership Authorizing Officials of changes affecting the IA posture of the organization and its programs.
- Identified security requirements specific to an IT system in all phases of the System Life Cycle and initiated requests for temporary and permanent exceptions, deviations, or waivers to IA requirements.
- Implemented Governance and Compliance SCAP/ACAS - NESSUS scanning, policies, and procedures to ensure the protection of critical infrastructure (as appropriate).
- Maintained SIPRNet accreditation packages through the RMF process ensuring timely receipt of Authority To Operate (ATO) documentation
- Managed and conducted approved development efforts that leverage discovery tools ensure that baseline security safeguards are appropriately installed to identify potential threats and vulnerabilities, and risk analysis in the decision-making process.
- Monitored HBSS software to ensure improvement upon system hardening practices to reduce the attack surface and safeguard against emerging threats, and provided system requirements development.
- Performed troubleshooting of local and remote installation of HBSS components and deployments of HBSS products and policies, and installed updates to McAfee software as released and in compliance with STIG requirements
- Responsible for installing, managing, maintaining, and configuring the Host-Based Security System (HBSS) and associated agents and endpoint products.

Project w/City of Hope c/o KORE1, Remote Contractor

- Accountable for information security across multiple departments system-wide and requires interaction at all levels of staff and management.
- Certified disaster recovery and business continuity plans were implemented monitored, and updated on a recurring basis.
- Directed multiple work functions and major projects/programs with broad scope and strategy of business impact.
- Ensured security incidents are resolved timely and appropriately and oversaw strategic planning, budget development, and management for a single large or multiple cost center, contract compliance, and any necessary integration of government regulatory requirements.
- Established and maintained collaborative relationships with key business partners including Technology Plan and Forecast for enterprise applications, enterprise-wide tools, infrastructure, and center equivalent in scope domains and complexity.
- Interfaced with key Information Technology (IT) solution vendors Develops strategies and facilitates performance measurement plans to optimize vendor and associate performance and outcomes.
- Managed and conducted multiple, complex, and inter-dependent risk analyses of the company's information security architecture, focusing on threats and vulnerabilities affecting the company's hardware and software components, with the objective of proactively mitigating threats throughout our infrastructure.
- Managed domain/suite of applications (or the equivalent capital and/or level of responsibility), including overseeing the processes and outcomes for multiple interrelated security incidents, recoveries, breaches, intrusions, and system abuses.
- Planned and executed annual projects while maintaining profit and loss (P&L) responsibility.
- Proactively initiated security reviews, evaluations, and risk assessments, leading the development and implementation of appropriate recommendations.
- Responsible for leading and managing the direction of information system and programming activities, and leading the enterprise vulnerability management program.
- Served as project manager/project leader for information security projects, including the development of project scope requirements, budgeting, and project planning.

Project w/Softek International, Inc., Remote Contractor

- Delivered direction, oversight, and recommendation to senior management in passing GSA Oral for HACS SIN Evaluation.
- Validated Team HACS Oral Technical Evaluation consisted of questions related to the 3 subcategories of, High-Value Asset Assessments Including Security Architecture Reviews (SAR) and Systems Security Engineering (SSE).
- See Cover Letter for complete details.

CompTIA

Michael B Hannah

CompTIA
Security+

Sr. ISSO/Regional Lead DoD Contractor 12/2019 – 7/2020
ManTech International Corp. Edwards AFB, CA

- Appointed Regional Lead and management of activities to resolve problems and challenges to ensure sound execution of contracted efforts for both technical and non-technical personnel and lower-level managers, and all aspects of a large-scale, complex contract to include subcontractors, personnel, schedule, and financial performance of the West Region facilities: AZ: Davis-Monthan AFB, Luke AFB. CA: Beale AFB, Edwards AFB, Los Angeles AFB, NH Camp Pendleton, NH Twenty-Nine Palms, Presidio of Monterey, Travis AFB, and Vandenberg AFB. NV: Nellis AFB.
- Synchronized, planned, developed, finalized, and reviewed key deliverables at each stage of the Certification and Authorization (C&A) process using applicable DoD and DHS tools and guidance, and reviewed all systems test plans, and implemented each task within the six phases of the Risk Management Framework (RMF) and following the processes and procedures for the Air Force implementation of RMF within the Enterprise Mission Assurance Support Service (eMASS).
- Directed risk and vulnerability assessments of information systems to identify vulnerabilities, risks, and protection need using DISA SCAP Compliance Checker and ACAS - NESSUS in conjunction with hands-on manual STIG assessment as necessary, established, updated, and reviewed RMF documentation to include Security Plans, Implementation Plans, Plans of Action and Milestones (POA&Ms), and Risk Assessment Reports.
- Established goals and evaluated employee performance reviews, tracked productivity to determine worker and process weaknesses and ISSM POC for technical, D2D, and DHA questions and concerns, best practices for 14 direct reports across these facilities in CA, AZ, and NV.
- Systematized the transitioning to a single enterprise network via the D2D Program and other IT initiatives the 412th MTFs site with, consolidating and integrating this effort to ensure the D2D filled requirement gaps; met current and future mission needs; and reached the goals of the Department of Defense (DoD) leadership. This effort centered on providing needed support at the different MTF site locations throughout the MHS Genesis rollout in compliance with the National Defense Authorization Act (NDAA) to implement electronic health and benefits records.

Classified Cyber Security Analyst DoD Contractor 11/2018 – 8/2019
Brandes Associates, Inc., Point Mugu, CA

- Coordinated with the Defense Intelligence Agency and other elements of the U.S. intelligence community on inspections, reviews, investigations, and other reportable issues; coordinates with the Defense Security Service (DSS) and Department of Defense sponsors on inspections, reviews, investigations, and other reportable issues.
- Implemented CS compliance SCAP/ACAS - NESSUS scanning and management of new requirements of Windows 10, manual STIG testing, technical analysis of scan of JMPS MPEs while maintaining eMASS fully integrated cybersecurity management, and the generation of RMF for DoD IT and DAAPM Package Reports.
- Investigated A&A artifacts to achieve A&A for the Joint Mission Planning System, JMPS, IAW the DODI 8510.01, RMF for DoD IT, JMPS/Cyber.

Technical Training Consultant 8/2018 - 11/2018
LMU c/o TEKsystems, Los Angeles, CA

- Maintained state-of-the-art developments in INFOSEC standards, principles, and policies supporting the enterprise security posture of Vulnerability assessment, IPS/IDS, Access control and authorization, Policy enforcement, Application security, Incident response, Encryption, Email/Web-filtering, and Advanced Threat Protection/Detection.
- Monitored security tools and technologies: Azure AD, McAfee EPO/Email/Web Gateway, Splunk, Barracuda Spam filter, EDR, Proofpoint Email Protection, Digital Guardian DLP, Protected Trust Encrypted Email covering NIST SP 800-53 controls, FedRAMP and FISMA.

Systems Administrator/Cyber Security Analyst 7/2016 - 8/2018
Northrop Grumman Corp., Palmdale, CA

- Directed AD, IIS, and MS Windows Server 2K8, 2K12, and 2K16 while maintaining VMWare ESXi environment and components including VDI SME for IS unclassified processing by various scanning tools and STIGs.
- Contributed to the DFARS Technical Solution, with NIST SP 800.171 Compliance for IAL/F-35 Program Assisted enclave and system accreditations, and provide corrective actions to resolve or mitigate vulnerabilities that are identified.
- Organized security HW/SW administration and technical support for life cycle management, extended file security administration, file system creation and configuration, special backup and recovery services; manage file systems and disk space; manage virus protection system and update virus definitions on a routine basis, special off-Site storage handling (non-IT DCO/RAM systems).

CompTIA
Michael R Hannah
CompTIA Security+

McAfee ePO Administrator Consultant 2/2016 – 7/2016

St. Josephs Health Systems, C/o Peak17 Consulting, Anaheim, CA

- Collaborated endpoint security and implemented and administered (HIPAA, COBIT, PCI-DSS, and ITIL), McAfee ePO McAfee endpoint security technologies: Drive Encryption (DE) and Enterprise Encryption for PC (EEPC), VSE, MOVE-AV, Host Data Loss Prevention, Endpoint Protection for Mac, Management of Native Encryption (HIPAA, COBIT, PCI-DSS, and ITIL).
- Managed configured and managed Palo Alto Network Traps that prevented advanced persistent threats and zero-day attacks

Threat and Vulnerability Analyst Consultant 10/2015 – 2/2016

MUFG/Union Bank, C/o Genuent, Monterey Park, CA

- Centralized dynamic and static malware analysis of potentially malicious files identified from CND and Focused Operations personnel, while deploying and maintaining a malware analysis lab.
- Managed daily monitoring systems SIEM Splunk Arc Sight Agari/DMARC Threat Vulnerability Events used to detect and report security violations and analyzed the business risk and apply necessary security controls while minimizing the impact.

McAfee ePO Administrator Consultant 11/2014 – 10/2015

MLK JR Community Hospital, C/o CareTech Solutions, Inc., Los Angeles, CA

- Managed daily monitoring systems of McAfee: Advanced Threat Defense 3.2, Drive Encryption (DE), Agent, Go, Windows PC (EEPC), Email Gateway 7.6, Endpoint Protection for Mac, ePO Deep Command Client, Discovery and Reporting Plugin, FireScope, Host Data Loss Prevention, IPS/IDS, HIPS, Management of Native Encryption Behavior Analysis, MOVE-AV, NDLP, NSM, Product Coverage Reports, Quarantine Manager 7.0, SaaS Portal/Email Cloud Protection, SEIM 9.4, Site Advisor Enterprise Plus, Splunk, VirusScan Enterprise, Vulnerability Manager 7.5, Web Gateway 7.4.2.

SCCM Administrator Consultant 11/2013 – 12/2014

Health Net, C/o Cognizant, Woodland Hills, CA

- Managed day-to-day supervision, desktop operations team, support, planning, installation, integrated App-V Infrastructure, device testing, System Improvements, Client Health, Remote Tools, Wise, VB, Batch, and Shell scripting that featured parity of SCCM 2K7/2K12 environments.

Network Administrator/Security Analyst Consultant 8/2013 - 12/2013

Peak Performance MS/Affinitiv, Calabasas, CA

- Managed Assessment/Analysis/Compliance, Enterprise Architecture/Mitigation, documented findings, suggested remediation on problems consisting of 250+ Servers, 400+ workstations and 80+ network printers, IP Network, WAN and LAN free (SAN/NAS NetApp) based data backup design and configuration storage solutions, Citrix /XenApp server/client, ITIL best practices.

Systems Administrator Consultant 1/2013 - 7/2013

Chevron SJVBU, C/o Collabera, Bakersfield, CA

- Administrated, BMC Service Request Management Administrator, Citrix Presentation Server, Citrix server/client, DameWare NT Utilities v7.5.9.0, Microsoft Lync Server, Microsoft Lync 2010, SolarWinds-Orion Monitoring Management Tool, and Sophos Endpoint Security and created, maintained server desktop images, Hyper-V Manager, VMware vCenter Server 4.1.0, vSphere Client 4.1.0, Volume Activation Management Tool.

Systems Administrator Consultant 11/2012 – 1/2013

Union Bank, C/o Robert Half, Monterey Park, CA

- Administered support systems integration/test of enterprise application workload-centric management, IT Prep Phase Migration, Scheduled UAT's, Implemented application packaging with maintenance, inventory, packaging, and upgrades of UAT (User Acceptance Test), tested and certified vendor updates, maintenance, and general ownership of the application.

Systems Administrator DoD Contractor 4/2012 - 11/2012

USAF, 412th FSS/FSMCS, Edwards AFB CA

- Administered AD Server, TCP/IP, VPN, SSH, Public Key Infrastructure (PKI), VLAN, Allied Telesis Layer2/3 Switches, CAT5/6, Access, ethereal, PCAnywhere, Wireshark, Cisco ASDM, Citrix /XenApp server/client, ITIL best practices. ESX/ESXi, VMware High Availability, VMware Distributed Resource Scheduler, and virtual machine power-on problems.

CompTIA

Michael B Hannah

has successfully completed the requirements to be recognized as

CompTIA Security+

PROFESSIONAL REFERENCES: AVAILABLE UPON REQUEST

ISSO Security Administrator DoD Contractor 2/2011 – 4/2012
Raytheon SAS, El Segundo, CA

- Mitigated weekly Audits for DoD DAAPM packages and NAC through IA Controls, POA&M following NISPOM Chapter 8 compliance for DoD LAN/WAN, Standalone environments UNIX/Window servers, workstations, system categorization, SSPs, Risk Assessment Reports, SARs, Security Authorization, and ISCM, CP, and POA&M for review and approval by Authorization Official.

Infrastructure Mgr. Consultant 6/2010 - 10/2010
LBI Eyewear/Atlantic Optical, Chatsworth, CA

- Managed oversight of the IT infrastructure, Avaya telephony systems, PBX servers, 2K3 Server Platforms / OS: XP Pro, Vista, Windows 7, Server 2K3, P2V, ESXi Servers, 2K3 RC2, Citrix XenApp, XenDesktop), Terminal Server, and DOS, Crystal Reports Server, Pervasive/ Btrieve Database, Power Flex Software, Citrix XenApp secure gateway/web interface, VMware vSphere.

Network Administrator DoD Contractor 2/2010 - 4/2010
Jacobs Technology, Inc., Ridgecrest, CA

- Acknowledged new security threats by conducting continual monitoring, penetration testing, vulnerability assessments, and log analysis.
- Administered LAN setup, and performance issues of Cisco Routers, Switches, ASA firewalls, ISP, VPN, network cabling, day to day operation of network Intranet, Internet, Citrix Provisioning Server, Citrix server/client, Citrix XenApp, Web portal, and configured and administered Cisco AnyConnect and RSA two-factor authentication, and the Anti-Virus (AV) protection program.
- Applied cloud-based APIs to develop network/system-level tools for securing cloud applications.

ADDITIONAL CONSULTING PROJECTS 11/2000 – 2/2010

- AVAILABLE UPON REQUEST

VOLUNTEERED:

Homes4Families – Veteran Home Ownership Affordable Sale Program

EDUCATION:

• Purdue Global University, BS Cyber Security	In-progress
• Military Education, U.S. Army	Primary Leadership & Development

- Vulnerability Management, Information Security Governance, Risk Management, Security Incident Management, Security Program Development Management, Information Systems Operations, and Business Resilience, Data Privacy, and Protection.

CERTIFICATION & TRAINING:

• GIAC GICSP Certification	In-progress
• CISSP DOD 8570 IAM level II/III	In-progress
• ISACA Leadership and Governance Professional Credentialing	In-progress
• DHA CoA: eMASS/RMF/ACAS- NESSUS/POAM/HIPAA	2020
• DoD eMASS Certification	2020
• DoD CSSP: Analyst, Infrastructure Support, Incident Responder, Auditor	EC Council: C|EH
• DoD 8570 IAM Level I	Comp TIA Security+ ce
• McAfee University	Email and Web Gateway Systems
• Six Sigma Certification	Green Belt

PROJECTED CERTIFICATION & TRAINING: 2021 - 2022

• Certified Chief Information Security Officer (C|CISO).	Global Industrial Cyber Security Professional (GICSP).
• Certified in Risk and Information Systems Control (CRISC).	Project Management Professional (PMP).
• Certified in the Governance of Enterprise IT (CGEIT)	Certified Information Security Manager (CISM).
• Certified Information Systems Security Professional (CISSP).	Certified Information Privacy Professional (CIPP).

CompTIA
Michael B Hannah
has successfully completed the requirements to be recognized as
CompTIA Security+ ce

PROFESSIONAL REFERENCES: AVAILABLE UPON REQUEST