Scott Ardis, PMP, CISM, CEH, CySA+, CNDA, CHFI, Sec+

Cybersecurity & IT Professional, 14+ Years of Experience, Master's Degree

Contact: ardisst@gmail.com, 804-590-6510
My Website: https://ardisst.github.io/resume/

Cyber & IT Professional with a background in Project & Program Management, Cyber Incident Response, Vulnerability Management, Defensive Cyber Operations (DCO), Governance Risk & Compliance (GRC), and User Experience Design. My work ethic, enthusiasm, attention to detail, and process driven mindset are my greatest strengths. I have a passion for leading people and engaging in customer-focused missions.

MY EXPERIENCE

Booz Allen Hamilton (BAH) **August 2022 – Present**
Cyber Risk Expert

- Cyber Risk Expert for BAH supporting the US Postal Service (USPS) managing the enterprise cyber risk management program & cyber risk register for a 600,000-user network.
- Responsible for daily strategic and tactical management of enterprise cyber risks, remediation, mitigation, and associated vulnerability management; liaison between mitigation stakeholders & executive leaders.
- Reduced overall enterprise risk landscape by 50%, reduced over 10 strategic risks & 40 tactical risks into executive appetite acceptance, conducted 50+ assessments, and exceed team KPIs every fiscal year.
- Revamped the entire cyber risk program by eradicating manual processes, building a cyber risk application, using automated workflows, and creating executive level cyber risk dashboards.
- Advocated & helped integrate cyber threat intelligence (CTI) into the cyber risk program by linking cyber risk to threats, threat actors, and adversary techniques.
- Acts as temporary project manager for mitigation efforts without PMs, establishing project foundation.

US Air Force Civilian Service **July 2020 – May 2022**
Cyber Technical Director

- Cyber Technical Director managing the US Air Force strategic networks; lead technical advisor and chief of staff for an organization of 140 personnel in a NOC/SOC environment for an 800,000-user enterprise.
- Led analysts and engineers across five cross-functional enterprise teams for vulnerability management, cloud computing, network operations, endpoint security, and identity & access management.
- Lead planner and director for business continuity & disaster recovery for the entire European enterprise network involving over a hundred thousand customers.
- SharePoint Administrator and web designer to include MS Power Apps; created and managed 20+ unique webpages, 50+ Power Automate flows, numerous dashboards, and 5 applications.
- Solely created and managed over 5 PowerApps applications; one deployed as an enterprise application to over 50 organizations streamlining processes for 30,000+ users.

US Army Cyber Command, Regional Cyber Center-Southwest Asia **March 2019 – May 2020**
Defensive Cyber Incident Response Lead

- Team lead for the Southwest Asia, Security Operations Center (SOC) Defensive Cyber Operations team handling cyber incident response, CTI, active defense, and continuous monitoring for 100,000 users.
- Managed a team of 5 Incident Handlers, 5 Cybersecurity Analysts, 5 Threat Hunters, and 10 engineers; planned and directed all incident handling, threat hunting, monitoring, and vulnerability management.
- Utilized a ArcSight/Splunk, IDS/IPS sensors, web proxy, firewalls, and Tanium to create an active defense-in-depth for 24/7 continuous monitoring, incident response, and threat hunting.
- Dual-hatted as lead project manager for IT & security infrastructure; led numerous projects for network architecture, sensor installation, and firewall & IDS upgrades across numerous hostile countries.
- Created an extensive SharePoint with automation and responsive design for managing enterprise IT programs; integrated into Army's first ever "Report Phishing" process via an automated Outlook button.

USAA (United Services Automobile Association) **September 2016 – March 2019**

Information Security Advisor & Auditor, *December 2017 – March 2019*

- Advisor and auditor for the cyber third-party security & risk management program; oversaw all third-party vendors, secure facilities (100+), and projects encompassing systems, networks, architecture, & apps.
- Responsible for third party cybersecurity risk assessments for existing and emerging risks to business processes; conducted end-to-end management to identify, measure, monitor, mitigate, and control risks.
- Conducted 150+ cybersecurity on-site Audits, discovered 1000+ critical third-party audit findings and remediated 100% of all findings on-time; used the data to conduct trend analysis to determine risk levels.
- Created comprehensive risk assessments on applications, cloud solutions and infrastructure; key stakeholder for third party cyber risk advising on all enterprise network & cloud projects.
- Responsible for the third-party cyber risk program encompassing audit & assessment projects.

User Experience Designer, *September 2016 – December 2017*

- USAA.com & mobile application experience manager & designer for Annuities & Survivor Relations; responsible for user interface & human design, continuous agile delivery, and project management.
- Heavily utilized Axure, Balsamiq, and InVision to wireframe and prototype experiences for stakeholders and testing; built with a 'member first' mindset while ensuring security and quality at the foundation.
- Key designer in experiences that are live today for annuities & survivorship; leveraged data analytics through Adobe Analytics, Google Analytics, and heat mapping to drive decisions and meet key metrics.
- Managed over 15 web pages with 100,000+ annual user traffic and engagement; created over 1500+ requirements & user stories across multiple projects & experiences on USAA.com & mobile.

US Army Reserve **September 2016 – Present**

Director of Information Technology Operations & Security*, April 2020 - Present*

- IT Director for an 800-user organization providing planning for long-range communications across numerous states using a host of tools and systems; maintains two decentralized IT networks.
- Responsible for a 20-personnel & overall organization IT & security program to include infrastructure projects, vulnerability management program, and business continuity/disaster recovery.
- Rapidly innovated to solve a Reserve-wide attendance problem my creating an Army-wide MS PowerApp; distributed the app and guide to hundreds of admins enabling 10,000+ users to utilize.

Cyber Network Defense Manager (Blue Team Lead)*, September 2016 – April 2020*

- Blue Team Lead for 15-person deployable Cyber Protection Team (CPT) providing active defense, scanning/reconnaissance, vulnerability assessments, and conducting "Blue Hunt" activities.
- Chosen to lead numerous Cyber & operational training events to include cyber capture-the-flags, programming/mark-up language overviews, Bash CLI & Kali Linux overviews, & mentor development.
- Lead operational planner, cyber range project manager, and cyber training program manager.

US Army **March 2010 – September 2016**

Information Technology Manager*, February 2014 – September 2016*

- IT Manager for 800 users responsible for network operations, vulnerability management, project & program management, and strategic planning; managed a 25-personnel cross-functional IT team.
- Responsible for $20 million in hardware and equipment; managed, designed and created a Secure Operations Center (SOC) supporting mission planning, SharePoint development, and orders program.
- Designed & created the organization's first SharePoint collection increasing overall productivity.

Technical Project Manager, *March 2010 – February 2014*

- Led and completed over 100+ critical projects to enhance unit capability though systems & hardware implementation, lead planner for operational orders, technical orders, and risk management.
- Operational leader responsible for various IT and artillery missions with the ability to globally deploy; responsible for 40+ personnel and over $50 million+ of hardware and equipment.
- Successfully completed a combat deployment in support of Operation Enduring Freedom (2012).

EDUCATION

M.S. in Cybersecurity & Information Assurance, Western Governors University, 2019
B.A. in History, James Madison University, 2009

CERTIFICATIONS *(**All Certifications are Active**)*

PMP, CISM, CEH, CySA+, CHFI, CNDA, Security+, ITILv3, MS Certified: Power Platform, MS Certified: Azure, MS Certified: Security Compliance & Identity, MS Certified: Dynamics 365 CRM, Top Secret Security Clearance (w/SCI)

SKILLS

- **Functions**: Project & Program Management, Software Development Lifecycle (SDLC), DevSecOps, Incident Response, Strategic Leadership, Cyber Risk Management, & Vulnerability Management.
- **Familiar Project Management Tools**: MS Project, Asana, Aha!, Jira.
- **Familiar IT & Security Tools**: Azure, Power Platform, SharePoint, SIEM (ArcSight & Splunk), Domain Services (Active Directory/Entra ID), VMWare vSphere & Aria, IDS (Cisco FirePower), Tanium.
- **Familiar GRC Tools**: Archer, Diligent, Metric Stream, ServiceNow.