Scott Ardis, CISM, PMP, 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 IT Management, Cyber Incident Response, Vulnerability Management, Defensive Cyber Operations (DCO), Project & Program Management, Governance Risk & Compliance (GRC), and User Experience Design. My work ethic, attention to detail, and enforcement of standards & processes 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

- Expert Cyber Risk Analyst for BAH supporting the US Postal Service (USPS) managing the enterprise cyber risk management program overarching a 600,000-user network of IT & OT infrastructure.
- 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 15 strategic risks & 65 tactical risks into executive risk appetite, conducted 100+ assessments, and exceeded team KPIs every fiscal year.
- Revamped the entire program by eradicating many manual processes by building a cyber risk application, Power Automate workflows, and creating executive level cyber risk PowerBI dashboards.
- Spearheaded the cyber risk register overhaul from tactically focused to strategic with integration of risk quantification (financial impact) and business continuity & disaster recovery planning.
- Integrated cyber threat intelligence (CTI) into the cyber risk program by linking risk to threats, threat actors, adversary techniques, and increasing researching with implementation of the Analyst1 platform.
- Consistently sought to brief executive leaders (C-Suite) on cyber risks to enable decision-making.

US Air Force Civilian Service, 691st Cyberspace Operations Squadron **July 2020 – May 2022**
Cyber Technical Director

- Cyber Technical Director for IT & OT Infrastructure managing the US Air Force strategic network; lead technical advisor and chief of staff for the organization of 140 personnel in a NOC/SOC environment.
- Responsible for incident response, vulnerability management, risk management & mitigation, crisis action planning, engineering systems, process improvement, and monitoring for an 800,000-user enterprise.
- Leads 140 personnel of five distinct enterprise teams for engineering, vulnerability management, cloud computing, network operations, endpoint security, and identity & access management.
- Hyper-focused technology governance and risk management strategy; performed risk assessments for projects, emerging technologies/risk, and created enterprise-wide Cyber policy to include KRI/KPIs.
- Infused cyber threat intelligence (CTI) to increase threat hunt to protect critical infrastructure for data centers, ICS, SCADA, internet of things (IoT), and life support systems.
- Lead strategic planner and director for the business continuity & disaster recovery for the entire European enterprise network include lifecycle, innovation, compliance, and new solutions.
- SharePoint Administrator and lead web designer to include the MS PowerApps, Power Automate, and Power BI; reduced manual operations by over 50% across 25+ processes.
- Created and managed 20+ unique webpages, 50+ Power Automate flows, numerous dashboards.
- 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) DCO team handling cyber incident response, threat management, active defense, GRC, and continuous monitoring for 100,000 users.
- Managed a team of 5 Incident Handlers, 5 Cybersecurity Analysts, and 5 Threat Hunters; planned and directed all incident handling, threat hunting, monitoring, and vulnerability management.

- Utilized a SIEM, IDS/IPS sensors, web proxy, Big Data aggregation, and Tanium to create an active defense-in-depth for 24/7 continuous monitoring, incident response, and threat hunting.
- Managed and assisted in identifying over 10,000+ threats and remediating all issues upon discovery; fused CTI into operations turning data into actionable indicators.
- Created strategic approach to protecting critical ICS, SCADA, and data center systems through continuous monitoring, active defense (Blue Hunt), and curated signatures.
- 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; process creator enabling over 20+ new and overhauling 10 existing processes increasing team efficiency.
- Managed numerous security tools including firewall whitelists, active directory, company data warehouse, GRC Tools, and Service Now platform; developed metrics and drove KRI/KPIs.
- Utilized assessment data and enterprise vulnerabilities to correlate probability of attack; data used to support funding for remediating identified issues and non-compliance.

User Experience Designer, *September 2016 – December 2017*

- USAA.com/Mobile experience manager & designer for Annuities & Survivor Relations; conducted User Interface & human design to build the foundation for the experiences, always putting the member first.
- 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.
- Used testing to enable data driven decisions such as user, A/B, quality, acceptance, and regression.
- Managed over 15 web pages with 100,000+ annual user traffic and engagement; created over 1500+ requirements across multiple projects & experiences for flows, calculators, pages, and product offerings.
- Built and managed team SharePoint automating numerous processes with SharePoint designer.

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, over $5 million of IT hardware and equipment, organization-wide vulnerability management program, IoT & engineering system maintenance, and BCP/DRP.
- Rapidly innovated to solve a Reserve-wide attendance problem by 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, process developer, technical order writer, and lead GRC officer.

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, GRC, and strategic planning; managed a 25-personnel cross-functional IT team.

- Responsible for $20 million in hardware and equipment; 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 GRC.
- Delivered hands-on execution of system hardening & patching, completion of Cyber Tasking Orders (CTO), assessing security controls for projects, and Q-TIP scanning for network security compliance.
- 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) providing rocket & missile fire support within US Army Central Command's Joint Area of Operation.

EDUCATION

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

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

CISM, PMP, 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 & SOFTWARE

- **Tools**: Nmap, Wireshark, ArcSight/Splunk, Blue Coat, IDS/IPS, Nessus, Active Directory/Azure AD, PowerShell/Bash, Tanium, Big Data Platforms, PuTTY/SecureCRT
- **Languages**: HTML, CSS, PowerFX, PowerBI DAX, JSON, jQuery
- **Niche Functions**: Web & User Experience Design, Incident Response Management, GRC, Auditing, Regulatory Compliance (GDPR, FINRA, PCI, SOX, GLBA, etc.), Frameworks (NIST, ISO, etc.)
- **Platforms/Software**: MS Power Platform (PowerApps/BI/Automate), SharePoint Administration, Azure/GCP/AWS, Jira, MS Visual Code, Adobe Analytics, InVision, Figma, Axure, Balsamiq, VMWare Suite, Salesforce, Service Now/Remedy, Asana, Metric Stream, Archer