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

Cybersecurity & IT Professional, 12+ 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 Information Security & Assurance, IT & Network Management, Defensive Cyber Operations (DCO), Project & Program Management, Risk Management, 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

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

- Cyber Technical Director managing the US Air Force unclassified and classified networks through the entire CIA triad; lead technical adviser and chief of staff for the organization of 180 personnel
- Responsible for Cyber incident response, enterprise program management, risk management, crisis action planning, process improvement, and continuous monitoring for an 800,000-user enterprise
- Leads 100 personnel of five distinct cross-functional enterprise teams for vulnerability management, cloud & storage, network operations, endpoint security, and identity & access management
- Hyper-focused Governance, Risk, & Compliance (GRC) & risk management strategy; performed risk assessments for projects, change requests, and emerging technologies/risk
- 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 – April 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, and continuous monitoring to deter adversaries
- Managed a team of 5 Incident Handlers, 5 Cybersecurity Analysts, and 5 Threat Hunters; planned and directed all incident handling, threat hunting, monitoring, and external missions
- 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 Cyber Threat Intelligence into operations turning data into actionable IOCs
- 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 supply chain & third-party security program; oversaw all third-party vendors, secure facilities (100+), and projects encompassing systems, networks, and applications
- Responsible for third party InfoSec risk assessments for existing and emerging risks to business processes; conduct end-to-end management to identify, measure, monitor, and control risks
- Conducted 150+ InfoSec on-site Audits, discovered 500+ critical third-party InfoSec 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

Digital Product Manager (User Experience & Design), *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 IT Ops & Security*, April 2020 - Present*

- IT Director for an 800-user organization providing planning for long-range communications across NATO & EU countries utilizing a host of tools and systems; maintains a two decentralized IT networks
- Responsible for a 20-personnel and over $5 million of IT hardware and equipment
- Rapidly innovated to solve a Reserve-wide attendance problem my creating an Army-wide 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 weapons ranges, cyber capture-the-flags, programming/mark-up language overviews, Bash CLI & Kali Linux overviews
- Lead operational planner, process developer, and technical order writer

US Army **March 2010 – September 2016**

Information Systems Manager*, February 2014 – September 2016*

- IT Manager for 800 users responsible for network operations, security, systems integration, project & program management, 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 compliance
- Operational leader responsible for various IT and logistics missions with the ability to globally deploy; responsible for 40+ personnel and over $50 million+ of hardware and equipment

EDUCATION

M.S. in Cybersecurity & Information Assurance, Western Governors University, 2019
B.A. in History, James Madison University, 2009
Cyber P3i Program National Security Agency (NSA), University of Texas San Antonio, 2017

CERTIFICATIONS

CISM, PMP, CEH, CySA+, CHFI, CNDA, Security+, ITILv3, Microsoft Certified: Power Platform, Top Secret Security Clearance (TS/SCI)

SKILLS & SOFTWARE

- **Tools**: Nmap, Metasploit, Wireshark, ArcSight, Blue Coat, IDS/IPS, Nessus, Active Directory, PowerShell/Bash, Tanium, Big Data Platforms, PuTTY/SecureCRT
- **Languages**: HTML, CSS, PowerFX/Honeycode, VBA, JSON, JavaScript (novice), jQuery (novice)
- **Niche Functions**: Web & User Experience Design, Incident Response Management, GRC, Auditing, Regulatory Compliance (GDPR, FINRA, GLBA, etc.), Automation, SharePoint Designer/Admin
- **Platforms/Software**: MS Power Platform (PowerApps/BI/Automate), SharePoint, AWS/Azure, Jira, MS Visual Code, Adobe Analytics, InVision, Axure, Balsamiq, VMware, Salesforce, Service Now/Remedy, Asana, Metric Stream, Archer