Andrew Scharlott

CISSP, CISM, MSCS

ascharlott@gmail.com / 303.949.3486 / ascharlott.com

EXECUTIVE SUMMARY

Cybersecurity and Information Technology leader with a federal security clearance (TS/SCI) and more than seventeen years of expertise in building and maturing security programs, leading cross-functional teams, and developing and implementing innovative budget-conscious solutions to address complex business and technology challenges.

PROFESSIONAL EXPERIENCE

Principal Cybersecurity Architect [TS/SCI Clearance]

Ampsight

2024 - PRESENT

- Support numerous federal government (civilian, military, intelligence) and private-sector clients in multiple areas of cybersecurity, including: SOC operations; XDR/EDR/NGAV; cloud migrations, architecture, engineering, and security; Zero Trust Networking and Architecture.

Vice President of Information Security

Sylvan Road Capital

2022 - 2024

- As the company's first Information Security hire, built a comprehensive cybersecurity program from the ground up, including authoring foundational charters and key company policies (such as Incident Response procedures), and developing an enterprise-wide information security strategy and roadmap aligned with regulatory requirements and business objectives.
- Directed major IT and Cybersecurity projects including:
    - Cloud Migration: Completed a physical data center to cloud migration ahead of schedule, under budget, and with no unplanned downtime, minimizing the impact on operations
    - Endpoint Security: Replaced an old solution with a modern complete endpoint security suite, reducing the false-positive rate and identifying previously unknown threats.
    - Cloud Optimization: Analyzed and optimized the cloud architecture and resource utilization, resulting in a more than 20% reduction in ongoing operating costs
    - Vulnerability Management: Implemented a vulnerability management program that eliminated 100% of all high and critical exposed vulnerabilities on public-facing assets
- Evaluated, selected, and deployed solutions for numerous cybersecurity functions, including vulnerability assessment, patching, email security, and endpoint configuration management.
- Led cloud security efforts across our entire portfolio, leveraging the capabilities of Google Workspace, AWS GuardDuty, CloudTrail, and CloudWatch, and Microsoft 365 and Security Center.

- Collaborated with executives and business units to achieve company-wide and IT objectives, including those related to finance, legal, HR, software development, and IT operations. Lead compliance efforts in PCI, cybersecurity insurance, privacy (GDPR and CCPA), and SOC 2.

Chief, Cybersecurity Operations - Development and Delivery [TS/SCI Clearance]

U.S. Dept. of the Interior (DOI)

2020 - 2022

- Led team of two dozen managers, engineers, administrators, and analysts responsible for the oversight, deployment, and management of DOI's key cybersecurity technologies including: SIEM and related logging, dashboards, and reporting; Network Access Control (NAC); system and web (DAST) vulnerability scanning; advanced malware and intrusion detection; asset and inventory management and reporting; Data Loss Prevention (DLP); and EDR.
- Regularly briefed executive management across the agency and contributed as subject matter expert in various areas including incident response, cloud architecture and security, NAC, asset and inventory management, network segmentation, Zero Trust Architecture (ZTA), IPv6, Secure Access Service Edge (SASE), and vulnerability management.
- Supported multiple internal and external audit engagements (including those based on SOC standards and NIST requirements) by creating and providing documentation, being interviewed and answering questions, and giving demonstrations of tools and processes.
- Managed all aspects of team performance, including workforce planning, contract management, objective setting, performance reviews, and professional development. Developed and managed quarterly and annual budgets, negotiated with vendors, and reviewed and approved contracts and invoices to ensure fiscal responsibility.
- Worked closely with and advised many teams on cybersecurity functions and capabilities including those involved in privacy, governance, project management, risk management, infrastructure and systems administration, data center management, and end-user services.

Seamless Access Project Manager & Technical Lead [TS/SCI Clearance]

U.S. Dept. of the Interior (DOI)

2019 - 2020

- Led the DOI's high-priority *Seamless Access* project, with the stated goal of enabling the more than 75,000 DOI personnel to easily and securely connect to the enterprise network and access all needed resources at any of the more than 2,400 DOI office locations.
- Designed, deployed, and documented network and security technologies to enable secure access to enterprise resources. Developed and implemented policies, processes, and standards for VLAN and IP configuration, network routing, DNS, DHCP, endpoint security, firewall settings, captive portals, web filtering, troubleshooting, end-user support, and performance monitoring.

Cybersecurity Boot Camp Instructor

University of Denver (Contractor)

2018 - 2021

- Taught evening and weekend classes at the University of Denver's Cybersecurity Boot Camp.
- Developed and updated teaching materials including lecture presentations, lab activities, and homework assignments; reviewed and graded major projects and other student work.

- Topics covered in the course include: incident response, offensive security and penetration testing (including Kali Linux and Metasploit), web application architecture and security, networking and firewalls, system administration and hardening, Wireshark and packet analysis, forensics, cryptography, SIEMs and network monitoring (including Splunk, Snort, and ELK), cloud security and architecture, Bash shell and scripting, threat modeling and vulnerability assessments, governance and compliance, and risk management.

Information System Security Officer (ISSO) [TS Clearance]

U.S. Dept. of the Interior (DOI)

2015 - 2020

- Oversaw the continuous monitoring and information security controls for the DOI enterprise information security environment, including on-site and FedRAMP-certified cloud systems. Led a contract team that supported the continuous monitoring program, providing regular reporting and real-time alerting across multiple heterogeneous operational environments.
- Ensured accurate and updated documentation was in place to support the enterprise information security environment, including policies and plans, SOPs, BCP/DRPs, configuration guides, PIAs, POA&Ms, SAP/SARs, and A&A documentation.
- Supported numerous internal and external audit engagements and data calls based on FISMA, SSAE 18 SOC 2, and NIST requirements (including 800-53 and 800-37).

Security Operations Lead, Security Engineer, & Security Analyst [MBI Clearance]

U.S. Dept. of the Interior (DOI) - Contractor

2009 - 2015

- As Lead, managed the daily responsibilities of the Information Systems Security Operations team including security analysts, engineers, and administrators.
- Led incident response as a CSIRT lead analyst and incident manager, conducting security forensics on system logs, network traffic, and disk contents for malware infections, HR/management requests, and law enforcement investigations, following legal chain of custody requirements when needed.
- Architected, deployed, and managed the entire suite of information security capabilities, including SIEM, WAF, IDS/IPS, NAC, DLP, vulnerability scanners, and forensic analysis tools.
- Drove efforts to consolidate security technologies and optimize configurations and processes leading to savings of more than $100k/year
- Worked with internal (including the Inspector General) and external auditors in response to SSAE-16, FISMA, NIST controls, and other audit engagements and requirements.

EDUCATION

Master of Science in Computer Science - *Purdue University*

Bachelor of Science in Computer Engineering - *University of Missouri*

Bachelor of Science in Computer Science - *University of Missouri*

ACTIVE CERTIFICATIONS and RECENT TRAINING CLASSES

Certified Information Systems Security Professional (CISSP)
Certification # 472210

Certified Information Security Manager (CISM)
Certification # 1426392

Microsoft Azure Fundamentals
Certification # 989623039 (AZ-900)

Palo Alto Networks
Cortex XDR: Prevention and Deployment (EDU 260)
Cortex XDR: Investigation and Response (EDU 262)
Cortex XSOAR: Automation and Orchestration (EDI 380) [Pending 08/24]

AWS Cloud Practitioner Essentials & Security Fundamentals

Splunk Fundamentals 1 & 2

CURRENT VOLUNTEER POSITIONS

Vice President and Chief Technology Officer (CTO) - *Halo Girls Corp*

- *Halo Girls Corps* is a registered 501(c)(3) non-profit organization dedicated to helping girls and women of all ages discover their inner strengths and abilities through physical fitness and service to their community. We are an inclusive organization that welcomes girls and women of all races and religions. Our members work to improve the community around them by volunteering their services and their skills. We promote physical fitness, character development, and the importance of education. Halo strives to help girls understand that they are not limited by conventional stereotypes of what a girl can do, nor should they be afraid to be feminine.