Chris Caraccioli

Phoenix, AZ
480-406-5447 ● chris@caraccio.li

Certifications

- PMI Project Management Professional (PMP)
- ISACA Certified Information Security Manager (CISM)
- (ISC)² Certified Information Systems Security Professional (CISSP)
- (ISC)² Certified Cloud Security Professional (CCSP)
- GIAC Security Leadership (GSLC)
- GIAC Defensible Security Architecture (GDSA)
- GIAC Python Coder (GPYC)
- AWS Certified Solutions Architect Professional (AWS-SAP)
- AWS Certified Security – Specialty (AWS-SCS)
- Microsoft Certified Azure Security Engineer Associate
- Red Hat Certified System Administrator (RHCSA)
- Splunk Core Certified Power User
- Zscaler Internet Access (ZIA) Administrator
- Zscaler Private Access (ZPA) Administrator
- Swimlane Certified SOAR Administrator
- Swimlane Certified SOAR Developer
- CompTIA PenTest+
- CompTIA CySA+
- EC-Council Certified Ethical Hacker (CEH)

Experience

Accenture Federal Services

Cyber Defense Engineering Manager, 05/2019 – Present

- Manage, mentor, and support a team of security engineers.
- Act as the subject matter expert for SIEM, SOAR, Linux, and AWS engineering.
- Integrate security information and event management (SIEM) and SOAR platforms across security disciplines such as incident response; penetration testing; identity and access management; and governance, risk, and compliance.
- Develop Python, Bash, and PowerShell scripts to automate management tasks, integrate APIs, and enhance security tool capabilities.
- Install and configure Splunk applications to onboard data sources into Splunk.
- Collaborate with application owners to create or update Splunk monitoring for applications and systems.
- Create and maintain Splunk reports, dashboards, forms, visualizations, alerts, and data models.
- Implement, tune, and create Swimlane security orchestration, automation, and response (SOAR) platform use cases to increase security operations center (SOC) efficiency and eliminate repetitive and time-consuming processes.
- Develop long-range strategies for security systems to anticipate, identify, and mitigate security risks associated with system vulnerabilities.
- Use vulnerability scanning tools such as Tenable and OpenSCAP to identify and remediate security vulnerabilities and develop hardened operating system images for use in AWS, Azure, and VMWare environments.
- Implement high-level security requirements for operating systems and software to meet compliance with the Federal Information Security Modernization Act (FISMA), as well as other applicable laws, regulations, and presidential directives.
- Configure, tune, and implement auditing solutions (Sysmon/auditd) to enhance organizational security posture.
- Provide technical analysis of emerging and observed cyber threats to develop detection methods.

Security Operations Center Team Lead, 08/2018 – 05/2019

- Coordinated and managed mentoring and development of security operations center (SOC) personnel.
- Acted as subject matter expert for incident handling and cyber risk analysis and mitigation.
- Performed routine auditing of security operations center ticket activity and incident handling to ensure compliance and identify process improvements.
- Delegated and prioritized SOC workload and workflow based on current threat levels and activities.
- Prepared briefings and risk assessments for federal management.
- Active threat hunting and risk assessment using tools such as Splunk, Tanium, and McAfee ePO.

U.S. Army

Logistics Manager, 07/2014 – 07/2018

- Certified Small Group Instructor
- Supported a military unit of over 200 personnel with equipment issue, food service, and other logistical needs.
- Asset management of over $20 million of organizational equipment.
- Provided direct leadership for 4-6 junior enlisted Soldiers.
- Responsible for compliance with physical security regulations.

Logistics Assistant, 09/2012 – 07/2014

- Responsible for resourcing and managing battalion logistics operations.
- Assisted in management of logistical operations to support over 600 personnel.
- Conducted physical security auditing functions, to include analysis, documentation, remediation, and follow-up audits.
- Document management, physical security audits, and logistical support to subordinate organizations.
- Implemented all-digital storage system to streamline and improve previous hard copy document management.
- Managed departmental SharePoint resources.

Chas Roberts
Network & Systems Administrator, 04/2012 – 10/2012

- Identity and access management within Microsoft Active Directory.
- Implementation and management of VMWare ESXi v5 platform to support server virtualization.
- Maintained accountability of all technology assets, to include servers, workstations, and networking equipment.
- Endpoint security administration (Symantec EPM).
- Automated commonly performed administrative functions with PowerShell.
- Configured and managed IPSEC VPN appliance and VPN user accounts.
- Firewall configuration, patch management, server & workstation security/hardening.

AZ Army National Guard
Transportation Specialist (IT), 10/2011 – 04/2012

- Implementation of RFID tracking system for military and government-owned vehicles throughout Arizona.
- Liaised with civilian contractors, military personnel, AZ state government employees, and Department of Defense civilians to implement technology solutions.
- Setup and deployment of Very-Small-Aperture Terminal (VSAT) systems to support satellite-based data transmission.
- Administration of VMWare vSphere virtual servers to feed data to systems state-wide via VSAT satellite communication systems.
- Assisted in management of project goals and timelines.

Sun Valley Technical Solutions
Field Systems Engineer, 10/2010 – 10/2011

- Installed and configured call center recording technologies in Windows & Linux environments.
- Implemented and managed Verint/Witness and Avaya recording software (Quality Monitoring, Avaya Contact Recorder, Contact Store for Communication Manager, Viewer).
- Experienced with RSA Key Manager for encryption of data at rest.
- SSL/TLS implementation in IIS and Apache Tomcat environments to secure data in transit.
- Installation and administration of Microsoft Dynamics CRM for internal use.

U.S. Army
Logistics Specialist, 07/2009 – 09/2012

- Military Basic Training, Advanced Individual Training, and National Guard Service

Pearson Education
Product Support Lead, 07/2008 – 06/2009

- Handled product escalations requiring in-depth troubleshooting or research.
- Troubleshot/analyzed incoming customer calls related to software and hardware issues.
- Determined escalation path and provide alternative solutions to meet customer needs.
- Analyzed/tested data and software to determine the customer-facing issues (software bugs, client set up, corrupted data, etc.).

A.T. Still University
Computer Technician, 05/2006 – 05/2008

- Supported over 15,000 on-site and remote faculty and students in person, through email, and on the telephone.
- Responsible for Novell identity management, software issues (configuration/installation issues), and hardware issues (replacement/upgrades).
- Ensured all computer hardware was licensed, updated, and properly maintained.
- Created and revised technical documents and technology newsletters.

Education

- *Master of Professional Studies in Cybersecurity Management*
  Tulane University – 2021
- *Bachelor of Science in Cybersecurity & Information Assurance*
  Western Governors University – 2018