JOSHUA WEATHERS, CISSP, CISM, PMP

Email Address | Phone Number

CYBER SECURITY | CLOUD

Certified Project Management Professional with extensive experience leading security programs within various enterprise-wide organizations. Enterprise IT experience includes private, public, and federal sectors. Experience in FISMA and FedRAMP compliance and NIST-800-53 security specifications. Adept in evaluating gaps within the current technology landscape and implementing best practice methodologies that reduce costs, improve business functionality, and enhance its IT culture. Expert security analyst experience in multiple security areas, including network security, application security, server compliance, policy and standards management, and identity management. Military experience includes time in the US Air Force serving as a Project Manager.

- Excellent oral and written communication skills and interpersonal skills.
- Strong analytical skills, including the ability to collect, extract, synthesize, and summarize applicable data, perform root cause analysis, and implement recommended scalable solutions.
- Proven ability to quickly assess issues and challenges, utilize applicable data and innovative methodologies, and develop solutions in the best interest of long-term gain for the client/customer.
- Extensive experience in developing and nurturing relationships through collaborative engagements with executive leadership, operations management, peers, and clients.
- **Areas of Expertise**: Information/Cyber Security, Vulnerability Assessment, Firewalls/Network Security, Release Note Preparation, Code/User Guide Writing, Virtual Private Networks, Infrastructure Management, Risk Assessment/Reduction, Intrusion Detection Systems, Data Analysis/Security, Incident Management, Operations Management, Department Leadership, Workflow Analysis, Data Flow Diagrams, Project Management, IT Management, Leadership, Vendor Management, Integration, IT Strategy, Process Improvement, Disaster Recovery, Business Continuity, Enterprise IT Strategy & Development, Customer Service, Business Relationship Management, Process Improvement, Agile Development, Business Management, SDLC, Host-Based Security System (HBSS), Assured Compliance Assessment Solution (ACAS)

CERTIFICATIONS

CISSP – Certified Information Systems Security Professional
CCSP – Certified Cloud Security Professional
CISM – Certified Information Security Manager
AWS CCP – Certified Cloud Practitioner
PMP – Project Management Professional
CEH – Certified Ethical Hacker
CNDA – Certified Network Defense Architect
CompTIA A+, Network+, Security+, CySA+
CIW Web Security Associate
ITIL v3 Foundations

PROFESSIONAL EXPERIENCE

CYBER SECURITY SPECIALIST
SUGPIAT DEFENSE LLC **Dec 2020 - Current**

Cyber security specialist as part of a government/ contractor team with US Army DEVCOM DAC. Responsible for gray-box pentest and vulnerability assessments for DoD suppliers, engineers, and research and development partner as well as provide risk matrixes and offer mitigations.

- Point-in-time assessments tested to certify systems that are looking for formal acceptance into DoD networks and systems prior to deployment as well as testing of online systems to certify ongoing functions.

CYBER SECURITY ANALYST
APEX SYSTEMS **Jul 2020 - Dec 2020**

Cyber security intelligence analyst with DISA, Defense Information Systems Agency. CND experience within a Computer Incident Response Organization or Security Operations Center. Protect, Detect, Respond, and Sustain. Followed federal and local guidance from USCYBERCOM, DISA, and DoD regarding the CSSP Mission, Cyber Security Service Provider.

- Real time analyst for DoD using open-source intelligence for threats to compare against the supplied dashboards and raw logs.
- Identify indicators of compromise (IOCs) and integrate those into sensors and SIEMs with rules and updates.
- Triage alerts to identify malicious actors on customer networks as well as incidents over time to detect APT indicators.
- Report incident to customer and USCYBERCOM through JIMS, Joint Incident Management System, and TIPPERs for non-customers.

ASSOCIATE CONSULTANT
THREAT ANGLER **May 2020 – Dec 2020**

Evaluating system vulnerabilities to recommend and implement secure solutions in adherence to business processes and alignment with network design and infrastructure.

IT SECURITY ENGINEER
PERATON **Aug 2019 – Feb 2020**
Strategically analyzed and administered security controls for information systems. Introduced company security policies and ensure compliance. Delivered incident response, analysis, and reporting according to policies and procedures and Improved security posture of information systems by reviewing, assessing, and documenting vulnerabilities. Maintained all documentation on Security Policy and Procedures. Managed Information Security perspective for all incoming engineers and change requests for the station in accordance with NIST, FIPS, NASA, and Local Directives.

- Proposed, designed, and implemented various Information Security related projects, such as vulnerability assessments, remediation, intrusion detection, border security, and patch management
- Researched and evaluated the latest security technologies, provided implementation plans, and deployed security controls
- Administered firewalls and provided support for VPN concentrator. Performed quarterly firewall audits to identify open ports and services, compared those findings with approved change requests, and initiated the remediation of those findings
- Tenable Administrator for Tenable Security Center scheduled scans and Nessus ad hoc scans for systems acceptance.
- Administrator for multiple devices on the station, including CounterACT ForeScout, VMWare Hypervisors, Docker labs, and Redseal.

vSOC ANALYST
DEEPWATCH **Jun 2019 – Aug 2019**
Triaged security events and react according to criticality. Monitored Splunk Enterprise Security SIEM for suspicious or anomalous activity. Documented and managed incident cases in ServiceNow ticketing systems.

CYBERSECURITY ANALYST
ABACODE **Dec 2018 – Jun 2019**
Conducted base-level analysis to determine the legitimacy of files, domains, and emails using tools such as Wireshark and a Linux Toolkit as well as online resources such as Virus Total, URLVoid, IPVoid, and Robtex. Monitored a worldwide network for cybersecurity events and anomalies using various tools such as Site Protector, Net Witness, and Splunk.
Provided high-level analysis of security data to identify significant activity.

- Developed coordinated, implemented, and maintained standards and procedures to protect the security and integrity of information systems and data. Observed and analyzed traffic to learn valuable lessons from known malicious actors and determine countermeasures against such threats.
- Interacted with cyber intelligence analysts conducting threat analysis operations as well as numerous IT professionals performing varying technical roles within the client organization.

TECHNICAL SUPPORT ANALYST
GEOGRAPHIC SOLUTIONS INC **Apr 2018 – Dec 2018**
Monitored scheduled jobs in SQL, delivered SFTP files, completed SSIS packages, and provided escalation. Monitored, reported, and troubleshooted Cisco switches, routers, and firewalls, as well as DNS, IDS/IPS, and other utility applications.

HELP DESK TECHNICIAN II
PHYCISICAN BUSINESS SERVICES **May 2016 – Apr 2018**
Diagnosed, troubleshooted, and resolved a range of software, hardware, and connectivity issues—Excelled in asking probing questions and researching, analyzing, and rectifying problems, collaborated with Tier II and Tier III help desk peers to resolve complex issues that required escalation. Provided detailed descriptions of issues in the trouble ticket system and followed up diligently to ensure swift resolutions. Served as the point of contact for Technical Support for Dragon deployments, VDI's, Network troubleshooting. Primary technical trainer for new Helpdesk employees, directing the training path based on each person's strengths.

- Collaborated with the Helpdesk Manager with overall ticket tracking, projects, and keeping track of SLA requirements.
- Partnered with 3rd party Helpdesk personnel to find resolutions to various problems throughout the organization. Expediting solutions for all personnel. VPN, Citrix apps, 3rd party software.
- Managed dispatched technicians to oversee office repair and resolution of offices in need. Triaging repairs and personnel to have the most significant impact on the organization.
- Advised on new technologies and techniques that resulted in cost savings and produced effective productivity for the Helpdesk/ company.
- Resolved over 4500 help tickets total, far exceeding the Service Level Targets (SLT) and accounting for 40% of the total satisfied ratings on the Help Desk. Repaired and replaced components on failed machines in short periods to maximize work productivity.
- Improved corrective actions through resolution and follow up. Streamlined specific processes for faster resolution as a team to improve throughput. Reorganized department files and software suites for faster resolution and production.

EDUCATION

BS Information Warfare and Security Management, Norwich, Jun 2021 Ant. Grad
SecureSet Academy – CORE Program – Security Engineer Focus – BetaWolf Award High Performer
Digital Animation and Visual Effects School – Certificate of Completion