## CYBER SECURITY PROFESSIONAL

Experienced cyber security professional with expertise directly supporting Federal, State, Local, and Educational (SLED) cyber operations. Seasoned advisor with knowledge of cyber threat management, incident response, network defense, customer success relations, and business development. Extensive experience in cybersecurity assessment and consultation operations helping defend SLED entities. Proven record of mission success while conducting over 100 cyber engagements for SLED entities throughout California. Consistent ability to develop tailored security strategies, identify security weaknesses and enhance threat management plans. Exceptional ability to communicate and collaborate with governments entities, law enforcement, private sector partners, education institutions, and critical infrastructure stakeholders during fast-paced and high-pressure cyber operations. Demonstrated leadership ability while leading cybersecurity and consultation operations and customer success activities with limited guidance, resources, and support.

**Core Competencies*:***

|  |  |  |
| --- | --- | --- |
| * Penetration Testing | * M365 | * Project Management |
| * Threat Management | * GitHub | * Threat Intelligence |
| * Network Defense | * Customer Success | * Security Operations |

### Professional Experience

SomeOrganiztion - City, State 09/2016 to present

**JobTitle**

Serve as ***Some Job Title*** for Some ***Organization*** assisting other entities with vulnerability assessments and security posture.

* Conduct professional quality penetration tests of all state agency networks and select Educational Institutions, simulating current real-world attacker tactics, techniques, and procedures.
* Conduct detailed In-Briefs detailing customer expectations, scope of work and rules of engagement.
* Conduct detailed and technical Out-Briefs regarding identified vulnerabilities and our associated paths to compromise, discussing remediation within the context of business functions.
* Generate custom recommendations for identified vulnerabilities with context to business needs and functionality, including estimated cost and time to implement.
* Perform as a member of ***Some Organization*** IR team, responding to intrusions, anomalous activities, and malware to perform network and host hunting and provide correlated recommendations, and assist in remediation.
* Train, mentor, and lead 15 junior security analysts and penetration testers within the organization.
* Provide mentorship to Information Technology and Security departments to assist organizations in increasing their security posture.
* Develop and implement plans for hardening of infrastructure using DoD Security Technical Implementation Guides(STIG).
* Build and deploy security measures to shield company data from unauthorized access, leaks, or misuse.

SomeOrganiztion - City, State 04/2015 to 09/2016

**JobTitle**

Serve as the senior security analyst for ***Some Organization***.

* Develop, test, and refine collection TTPs for all cyber security assessment metrics with regards to applicable regulatory standards (NIST, ISO).
* Train, mentor, and manage junior analysts and other team leads.
* Conduct detailed In-Briefs detailing organization expectations, scope of work and rules of engagement.
* Conduct detailed and technical Out-Briefs regarding identified vulnerabilities, IT management and operations, discussing remediation within the context of business functions.
* Conduct network vulnerability assessments using tools to evaluate attack vectors and identify system vulnerabilities in accordance with current standard operating procedures.
* Create risk and analysis reports and prepare them for organization management.
* Analyze network topologies and network traffic to identify anomalies and potential threats.
* Research potentially identified risks and evaluate findings based on research.
* Assist entity information technology teams in understanding the procedures within the scope of the type of security assessment being performed.
* Review entity policies including incident response procedures to assess compliance with state Chief Information Office’s requirements and best business practices.

SomeOrganiztion - City, State 9/2001 to 4/2015

**JobTitle**

Serve as the senior administrator for the ***Some Organization***.

* Lead administrator for 3000 windows clients, 100 windows servers.
* Train and mentor 9 system and network administrators.
* Instrumental in moving the organization to a VMware environment from bare metal installations.
* Completed multiple directory migrations from NT4.0 – Active Directory 2003.
* Completed migration of analog phone system to VoIP across 120 remote sites, to include E911 services.

### Education and Technical Certifications

* List of education
* List of certifications

### Repositories

* Some GitHub Repository
* Some other GitHub Repository