Summary

- 15 years worth of experience in Cyber Security/Project Management/Cyber Counterintelligence /Network Security Architecture/Malware Reverse Engineering
- Subject matter expertise in:
- Project management for large cyber security projects utilizing advance methodology (e.g. Six Sigma).
- Developing strategies to enhance overall cyber security program. Maintaining and improving security posture for IT governance.
- Advanced Persistent Threat (APT)/ Cyber CI (Counterintelligence)
- Cyber Security Forensic (malware analysis/ identifying intelligence related activity)
- Cyber security for critical infrastructure Nuclear, Oil, & Gas (SCADA/NERC CIP)
- Cyber security (FISMA) for US Government DoD (DIACAP), Civilian (NIST)
- Advanced cyber intrusion analysis/detection/forensic (rootkit, malware, etc.)
- Penetration Testing for large enterprise networks.

EXPERIENCE

03/2011 - Present Confidential
Lead Cyber Security Analyst (Cyber Counterintelligence/Malware RE)

- Applied PMI processes for all Cyber Security projects, redesigned cyber security processes through BRP, and used Six Sigma for quality enhancement on multiple cyber projects.
- Performed static & dynamic analysis of malware (APT) and its delivery mechanism (malicious documents e.g. pdf, doc, etc.).
- Extracted TTP, exploit, author attribution, C2, and more. Utilized custom sandbox to isolate malware, unpack malware, monitoring registry changes, and identifying malware communication channels.
- Analyzed high-level language constructs (branching statements, looping functions, network socket code, and more) of malware/APT.
- Performed digital fingerprinting to determine foreign adversary/actor behind malware/spear phish, and correlated the data back with the Intelligence community.
- Used malware (APT) analysis to develop IDS signatures (Snort), FW rules, AV signatures, NetWitness Meta, and create ArcSight channels/reports for APT specific threats

- Produced reports & briefings to provide an accurate depiction of the threat landscape that impacted the US Congressional resource. Liaison for Cyber Threat Analysis entities such as Joint Cyber Threat Working Groups, Law Enforcement, DOD and the Intelligence Community. Developed Tactics, Techniques and Procedure (TTPs) reports.
- Conducted Cyber CI (Counterintelligence) assessments, operations, and investigations for congressional programs. Assessed the effectiveness of Cyber CI related activities across the organization. Identified problems that directly affect the accomplishment of Cyber CI program goals and objectives and created alternatives and corrective actions.
- Developed and coordinated proactive Cyber CI projects and activities to detect attempts by foreign intelligence services to target Congressional resources (technology and personnel).

- Provided assessments on cyber capabilities and activities of foreign intelligence, security services, and potential threats to and impact on Congressional information systems and operations. Conducted open and classified source research in support of Cyber CI initiatives. Created and updated threat profiles for congressional programs and its asset to be used for threat modeling for potential cyber attack/spear attack.
- Served as a Cyber CI investigator for reports of CI anomalies or allegations of espionage. Documented investigative activity by preparing detailed written reports. Maintains liaison contacts throughout the intelligence community.
- Reviewed the security architecture of the organization to find gaps that impact the enterprise. Provided comprehensive solutions to enhance the security architecture.

04/2007 - 03/2011 Confidential
Cyber Security Consultant

- Managed various IT security projects to ensure project were in scope, budget, and time. Managed staff members on various cyber security projects.
- Conducted data exfiltration/leakage assessment (Advanced Persistent Threat /APT).
- Performed malware analysis using various tools (e.g. Encase, HBGary FireEye, NetWitness, IDA Pro). Conducted analysis on captured user, computer, and network security events, in a near-real time environment, to determine security vulnerabilities, policy violations, and malicious behavior.
- Identified user behavior that may be indicative of potential malicious or counter intelligence related activity.
- Performed IT auditing services (C & A) for various government agencies using NIST, NERC CIP, SCADA & DoD (DIACAP) guidelines.
- Implemented risk management framework for organizations, and developed affective strategy for continuous monitoring. Developed secure guideline for cloud computing, worked on projects integrating IT governance controls in cloud computing.
- Performed penetration testing & vulnerability assessment for compliancy assessment.
- Developed documentation for security authorization package/certification packages (e.g. ST & E, POA & M, security plans, business continuity plans/disaster recovery plans, risk assessments and more,

- Developed IT security policies, guidelines, baselines, and procedure for various organizations (government, banking, commercial, and more) to reflect their respected IT governance adherence (e.g. FISMA (NIST/DIACA), SOX, PCI, SCADA, NERC CIP and more).

- Assist in the writing and review of organizational security policies to support internal control (access management, contingency planning & testing, Security Awareness, intrusion detection, Patch Management, Anti-Virus, etc.)
- Developing IT security internal control for SOX environment (section 302 & 404). Auditing for Internal control for IT governance project (FISMA/SOX). Auditing domains such as Change Management, Access Management, and Operations for SOX [section 404],

08/2003 - 03/2007 Confidential
Cyber Security Manager

- Utilized various project management methodology & PMI process to enhance various cyber security programs within the Department. Managed the 24x7 DoT SOC/CIRT.
- Developed reports for CIO, CISO, and other executives (Dept. Secretary) about IT security posture across the department. Developed daily cyber security situation awareness reports from various sources (advisories, SIEM, Intel briefing, etc.). Advised in IT risk management for the department.
- Lead liaison for cyber security for the Department. Incident response liaison between the department and other government organizations (DHS US-CERT, DC3, NSA). Represented the department in government wide initiatives Cyber Storm, GFIRST, NCRCG, Federal Law Enforcement, JointCyber Threat Working Groups, DOD and the Intelligence Community.

- Analyze Cyber Intelligence threats (advanced persistent threats) by investigating of cyber security incidents, assisting the DOT Inspector General, FBI, NSA, ARL (Army Research Lab), AFRL (Air Force Research Lab), and other law enforcement agencies with forensic analysis (Malware/shellcode analysis via. tools Encase, IDApro)
- Designed & implemented the department SIEM (Arcsight) to monitor the DOT enterprise (over 20,000 assets). Administration of the DOT security infrastructure consisting of IDS/IPS systems (Snort, ISS, IDSM2, IPS, NFR, Checkpoint IPS1), Vulnerability Assessment tools (Foundscan and Nessus).
- Creating IDS signatures to detect undesired or malicious network activity (i.e. APT, worm scanning and payload propagation).
- Assist in the writing and review of Departmental security policies (Security Awareness, IDS, Patch Management, Anti-Virus, etc.)
- Ensuring that systems were compliant with departmental rules, OMB mandates & FISMA (NIST guidance).
- Developed C & A (certification and accreditation) documents (System Security Plans, Security Test & Evaluation Plans, Risk Assessments, Contingency Plans) on major systems using NIST guidelines (NIST 800-18, NIST 800-30, 800-53, and more). Managed the continuous Monitoring phase, which included monitoring and mitigating POAM, conducting

self-assessments.

- Assist in authoring OMB Exhibit 300 Capital Asset Plan and Business Cases and related content to include performing and documenting analyses of alternatives (AOA), cost benefit analyses, risk analyses, developing performance goals and measures, and authoring related CPIC life cycle documentation to the OMB Exhibit 300 for the IT security portfolio. Inspected and approved information assurance aspect of OMB Exhibit 300.

02/2003 - 08/2003 Confidential
Senior IT Security Engineer

- Provided network security expertise and guidance in support of security assessments for government (FISMA DIACAP & NIST) and commercial clients (SOX, PCI, HIPAA). Performed network risk assessments, vulnerability assessments, and penetration testing. Evaluated and recommended security technology such as network and host based intrusion detection systems (IDS), virus protection capabilities, and virtual private network solutions.

- Reviewed security logs to ensure compliance with policies and procedures and identifies potential anomalies.

09/2002 - 11/2002 Confidential
Computer Security Analyst

- Performed network scans in search of vulnerability across DISANet. Conducted physical security inspections of classified area. Monitored IDS for potential threats and vulnerabilities. Researched foreign software before they were deployed on the DoD Environment.

09/1999 - 11/2001 Confidential
Network Security Engineer

- Monitored security logs from Firewalls (Checkpoint, Gauntlet, and Cisco Pix) and IDS (ISS, Dragon, and Snort). Installed and supported IDS (Snort/ISS). Collected forensic evidence from compromised machines, network logs and more. Responsible for researching and identifying security vulnerabilities on the networks and systems. Also responsible for patching security holes.

Clearance:
TOP SECRET

Certifications:

- **CISSP**
- **PMP**
- **CEH** (Certified Ethical Hacker)
- **Network+**
- **Security+**

SKILLS

IDS/IPS: ISS, Snort, Sourcefire

SIEM: Cisco Mars, Arcsight (Logger, ESM, Express)

Vulnerability & Penetration Testing Tools: Nessus, ISS, Foundscan, Nmap, Retina, GFI Languard, MetaSpolit, Core Impact, nmap, BackTrack

Forensic/Malware:
Encase, FireEye, NetWitness, IDA Pro, Helix, Wireshark

Security Standards/Guidelines: FISMA, NERC CIP, BASEL II, SOX, PCI, GLBA, HIPAA, and more.

Development Language: Ruby on Rails, C, Perl, BASH,

Education:

B.S. Information Technology (Concentration Information Security)