MICHAEL CALLAHAN

123 Newberry Drive, Lee, VA ● 123-456-7890 ● mcallahan@email.com

MALWARE ANALYST

- Senior Malware Analyst with over a decade of experience in the examination, identification and understanding of cyber threats such as viruses, worms, bots, rootkits and Trojan horses.
- Proactive in preventing and containing malware infestation to protect network software and hardware integrity as well as proprietary data.
- Proficient with interpreted and compiled programming languages with a keen understanding of both reverse engineering and software development to recover any potential damage.
- Honed leadership skills developed through numerous supervisory positions within the intelligence community and collaborations with Department of Defense (DoD) organizations.

CORE COMPETENCIES

Computer Forensic & Malware Analysis ● Vulnerability Research ● Reverse Engineering ● Signals Intelligence (SIGINT) ● Software Development ● Cybersecurity ● Information Operations ● Computer Network Operations & Security ● Information Assurance ● Technical Writing ● EnCase ● Intrusion Detection Systems (IDS) ● FTK ● Intel X86 Assembly Language ● OllyDbg ● VMware ● C++ ● SNORT ● Windows Internal ● Windows Kernel Debugging (Windbg) ● IDA Pro ● Linux ● FreeBSD

CERTIFICATIONS

CERTIFIED ETHICAL HACKER (CEH) – *EC-Council, 2010*

CERTIFIED COMPUTER FORENSICS EXAMINER (CCFE) *– Infosec Institute, 2009*

PROFESSIONAL EXPERIENCE

CSC, Manassas, VA 2011 – Present

Malware Analyst

Analyze malicious code by conducting reverse engineering techniques and employing tools and scripting languages as well as virtual machine and networking software. Identify the methodology of hackers posing a potential threat to customer networks and systems. Document results in time-sensitive reports, presentations and analyst exchanges.

Select Accomplishments:

- Selected to lead a cross-functional government contractor team to develop and implement system software and policies to upgrade network security. Finished project on budget and on time, ensuring compatibility with the fast-paced civilian sector.
- Developed a reputation for proactively researching high impact, emerging and complex malware threats to enact safeguards prior to possible infection.

RAYTHEON, Alexandria, VA 2008 – 2011
Forensic & Malware Analyst
Performed computer forensics including detailed technical analysis and reverse engineering of malware, malicious code and media such as hard drives and USB drives of compromised systems in support of Army Computer Network Operations (CNO) and Computer Network Defense (CND) efforts. Drafted technical reports detailing analysis results to US Army staff and leadership.

Select Accomplishments:

- Analyzed over seventy pieces of malicious software utilized to attack and exfiltrate data from systems operating on the Department of Defense's Global Information Grid.
- Supported the DOD Computer Network Defense Mission by authoring vital forensics and malware technical analysis reports.

KMPG, Bethesda, MD 2006 – 2008
Incident Response Analyst
Responded to enterprise computer security incidents, recording and reporting incidents through monitoring and analysis of IDS. Communicated intrusion alerts and compromises of network infrastructure, applications and operating systems to appropriate agencies. Created and maintained standard operating procedures (SOPs) and other similar documentation.

Select Accomplishments:

- Implemented daily systems health checks as preliminary forensic evaluations of internal systems.
- Ensured the integrity and protection of networks, systems and applications by technical enforcement of organizational security and policies.

PREVIOUS POSITIONS as ***Vulnerability Researcher*** and ***Security Analyst*** for Conway, Inc.

EDUCATION

GEORGE MASON UNIVERSITY, Fairfax, VA
Bachelor of Science in Applied Computer Science