JIM HAIGHT

Round Rock, Texas | James@JamesHaight.com | https://www.linkedin.com/in/jameshaight/

SECURITY ANALYST

SECURITY ARCHITECTURE DESIGN | DIGITAL FORENSICS | LOG ANALYSIS | GCIA CERTIFIED

Accomplished Cybersecurity Analyst eager to leverage 5+ years of success configuring and monitoring intrusion detection systems. Proven track record reading, interpreting, and analyzing network traffic and related log files**.** Wide-ranging skill set includes network and host monitoring, traffic analysis, and intrusion detection. Keen grasp of the fundamentals of network forensics, abnormal conditions for common network protocols, the process and tools used to examine device and system logs, wireless communication, and encrypted protocols. Qualified to perform examinations employing network forensic artifact analysis. Demonstrated exemplary performance on GIAC exams. Subject-matter expert for content-related issues in various GIAC program needs.

CORE COMPETENCIES

Intrusion Detection Systems | Network Log Analysis | Incident Handling | Vulnerability Assessment | Innovative IT Solutions
Troubleshooting | Problem Solving | Operational Streamlining | Project Lifecycle | Process Improvement | Project Management
Network Forensics | Strategic Solutions | Documentation/Review | Deployment Roadmaps | Risk Analysis

PROFESSIONAL DEVELOPMENT

Certifications: **GCIA** March 2016 – Present **GNFA** December 2017 – Present
Present Recognition: GIAC Advisory board – December 2017 – Present

RELEVANT SKILLS

Programming: C++, Python, Perl, bash, PowerShell
Packet Analysis Tools: Wireshark, ngrep, tcpdump, snort, bro, SiLK
Network: Network administration and administration of network-based security devices;
common network protocols, both theoretical and practical

PROFESSIONAL EXPERIENCE

SECUREWORKS INC., Lisle, Illinois
Operational Security Strategy Advisor | June 2018 – Present
- Intermediary between operations staff and development staff.
- Guides development to operations needs, as well as to overarching, company-wide goals.

Senior Security Analyst | Jan 2015 – June 2018
- Ensured timely analysis of incoming alerts from a wide variety of security controls; packaged actionable incident tickets for escalation to clients.
- Triaged incoming client requests for additional investigation, configuration changes on managed devices.
- Fine-tuned SecureWorks' event processing engines on a per-client level.

Shift Point | March 2016 *forward*
- Assumed key leadership role during shifts when no managers were present.
- Maintained frontline analysis workflow, ensured that shift resources were allocated appropriately to cover operational load across the various workload buckets utilized by the security analysis team.

Advanced Analyst Apprentice | Jan 2018 *forward*
- Formalized peer mentor role of Advanced Analyst Apprentice taking on responsibilities of the Advanced Analyst role, including advanced single-client tuning, some cross-client event tuning, and triage of alert floods when no Advanced Analysts were on-shift.

EDUCATION

B.S. Information Security and Forensics,
Rochester Institute of Technology, Rochester, New York | 2015