Verodin Job Posting –Security Analyst, Behavior Research Team

Who We Are

Verodin is reshaping how organizations measure, manage and improve cyber security effectiveness. Evangelizing a technology movement takes more than just a good sales pitch. As a team, we obsess over helping our customers:

- Assess their current state and expose true security gaps
- Establish a means to measure security effectiveness and demonstrate improvement over time
- Realize the maximum potential of existing security investments
- Raise the bar for the entire security organization

If you're passionate about security, have the core competencies outlined below and are looking to join a team on a mission, Verodin is the place for you.

The Team and The Role

The Verodin Behavior Research Team (BRT) identifies adversarial tactics and techniques. The BRT creates content that demonstrates weaknesses in identified tactics and techniques, enabling customers to empirically measure and improve their defenses.

The BRT is currently seeking a Security Analyst to join our team at Verodin Headquarters in Virginia. Are you a sharp mind who lives to employ analytical skills to help organizations stay one step ahead of the adversary? Do you love learning and having an never ending supply of new things to figure out? If so, the BRT is looking for you.

Job responsibilities include:

- Collection and analysis of artifacts including malicious executables, scripts, documents, and packet capture.
- Research and reproduction of hacking tools and techniques, including any and all information sources
- Creation of Verodin Behaviors incorporating new and existing research
- Communication of technical concepts to a broad audience including Verodin customers both in writing as well as in direct engagement

Desired qualifications include:

- A deep understanding of network protocols including TCP/IP, UDP, and HTTP
- The ability to read, process and understand network packet capture. Proficiency with wireshark, tcpdump and bro expected.
- A proven ability to author, tune, and understand signatures from multi-vendor security products including Snort, Yara, Palo Alto, Cisco Firepower, ESA, WSA and others
- Crystal clear understanding of network exploitation tactics, techniques, and procedure modeling including the Cyber Kill Chain, MITRE ATT&CK, CVE and others
- Extensive experience operating a variety of network defense equipment (NGFW IDS/IPS) including Palo Alto, Proofpoint, Fidelis, FireEye, Sourcefire, Snort, Cuckoo and others
- Familiarity with hacking, penetration testing, and vulnerability scanning tools such as NMAP, Kali Linux, Metasploit, CORE Impact and others
- Knowledge of command line interaction with Linux and Windows shells.
- Demonstrated proficiency in reviewing and authoring regular expressions (regex)
- A self-starter who values working in and with a team, who's willing to challenge assumptions and be challenged in a constructive group environment
- Significant experience in fast-paced operational (e.g. Security Operations Center) or startup environments a huge plus

To apply for this role, please send your CV/resume and a detailed cover letter describing why you're a fit to careers@verodin.com.

Verodin is an equal-opportunity employer.