**Position:** Technical Research and Support Specialist

Gravwell is an exciting startup driven by a mission to help organizations achieve their objectives by harnessing the power of unlimited data analytics. The company was founded in 2017 by security practitioners who were looking for a solution that could natively ingest large-scale, fully unstructured data quickly. No such tool existed, so Gravwell was purpose-built from the ground up to meet that need. Initial development was focused on creating a rock-solid product that would exceed customer expectations, and the company is now embarking on a growth stage to bring their robust platform to a wider audience.

Gravwell is seeking an experienced Technical Research & Support Specialist to assist with the implementation, management and support of our analytics platform, along with internal R&D efforts. The ideal candidate will be self-motivated and capable of working remotely on tasks which may be self-designated. Candidates are expected to be very comfortable working with many different log and data formats to rapidly extract, interrogate, and visualize data.

In other words, this job is about doing cool blue team stuff with all manner of data sources, supporting customers, and publishing content because there aren't *nearly* enough blue-team resources out there.

**Key Responsibilities *(3 main activity areas for this role)*:**

***Research & Development Activities:***

- Research and publish materials on defensive tactics, techniques, and strategies
- Utilize knowledge of security incidents to develop playbooks and procedures for use by Gravwell customers
- Create use cases for security operations and monitoring
- Develop Gravwell tools (queries, dashboards, Kits, etc.) for given use cases

***Developer Support Activities:***

- Provide feature suggestions - help us build a more awesome Gravwell!
- Offer subject matter expertise for cybersecurity
- Bug reporting

***Customer Success Activities:***

- Architecture planning / POC implementation - Work with Gravwell sales and field operations team to determine appropriate architecture and proof of concept (POC) implementation for customer
- Onboarding - Act as technical liaison as needed during onboarding process
- Technical support

**Location:** Remote (This is a remote position, but candidates must be authorized to work in the U.S. and reside within the contiguous 48 states)

**Required Background & Experience**

- 5+ years' experience installing and configuring SIEM and/or log management tools
- Log analysis (anything from firewalls to vmware to endpoint to Zeek - you name it, we collect it)
- Solid scripting skills (python, powershell, bash, etc.)
- Understand and be able to run network attack tools
- Clear understanding of network protocols
- Strong communications skills, both written and verbal (fluent in English)

**Preferred, but not required Skills**

- Software reverse engineering and protocol design (ability to reverse engineer a black box system or network stream and develop a decoder)
- Language experience (Assembly, Python, C#, C, C++, Java)
- Malware analysis

---

**APPLY TODAY:** Please send your resume and/or inquiries to careers@gravwell.io

**About Us:** https://www.gravwell.io/about-us

**Our Mission:**
Data is powerful. Today there are nearly infinite data sources leaving organizations struggling to make sense of it all. Gravwell is changing the shape of data by empowering organizations to collect everything, see everything, and know everything, instantaneously.