



## Resident Engineer and Systems Support Specialist

### Position Overview

The resident engineer position supports Gravwell's core product development and support system, which is responsible for the design, deployment, and integration of the Gravwell analytics platform. Well-suited candidates are self-motivated and capable of working remotely on tasks which may be self-designated and well-suited to directly interact with customers and partner engineering teams. The position is primarily remote but has immediate customer needs in Atlanta and surrounding areas. Travel will be minimal but onsite work with a local customer may be significant.

The core platform often acts as the integrator to many other 3rd party systems, including security sensors, network services, switching infrastructure, and endpoints. As a result the systems support specialist needs to be highly capable and willing to dig into internals of many other tools and products. When not directly supporting customer and 3rd party integrations the Systems Support Specialists are helping advance the core product and build state of the art interface systems on top of the core product. The position blends systems architect, SRE, and DevOps engineer.

### Duties and Responsibilities

- Design, deploy and integrate Gravwell on customer sites and with 3rd parties.
- Product documentation and training
- Testing and development of integration modules
  - Endpoint, network, and application
- Development of query and automations to be deployed to customer sites
- Use case development and customer success
  - Design and deploy customer specific integrations and detections

### Required Skills

A qualified candidate must be well versed in Linux systems, system administration, network debugging, system logging, and data broker systems. Gravwell is a full-stack analytics platform;

Systems Support Specialists integrate our product with everything from Linux and Windows logging to network capture sensors. Our customers use us to consume data from custom application stacks, cloud infrastructures, Kafka, RabbitMQ, and even some PCAP.

The position requires minimal travel outside of a local customer site. Occasional extended travel involving a week of onsite support and analysis for other large customers may be required. Extensive remote communications are required, and the candidate must have a quiet working environment and reliable means to interact with the rest of the remote team.

## Software Engineering Requirements

- Strong Linux fundamentals including but not limited to:
  - Process management
  - Network communications
  - Memory management
  - Kernel interfaces
  - Filesystems and file management
- 2+ years experience with any common scripting language
  - Shell, Python, Perl.
- Network and systems security
- Network communications
  - IPv4, IPv6, TCP, UDP
- Strong speaking and writing skills
  - Fluent in English
- Strong understanding of automated deployment technologies
  - Chef, Puppet, Satellite
- Experience with a log centralization system
  - ELK, Splunk, etc..
- SELinux and Redhat systems management

## Preferred but not required skills

- Low-level network debugging
  - Flow introspection and packet capture
- Log processing and query systems
- Kafka and data broker systems

## About Gravwell Inc.

Gravell Inc. is a data analytics and security company composed of people with extensive backgrounds in penetration testing, reverse engineering, analytics, incident response, and large scale virtualization. We are striving to push the boundaries of traditional I.T. security and analytics products by enabling high-speed binary compatible analysis. Our platform is built from the ground up--not a bolted-together conglomerate of disparate technologies--and we take pride in enabling customers to ingest, store, and analyze all of their data without compromise.

Gravwell's core mission is to enable teams in IT, OT, and marketing to perform hunt operations, which means enabling humans to identify and understand data features and emergent behaviors in IT operations, physical systems, security incidents, and marketing.