



Backend Software and Systems Engineer

Position Overview

The backend software and systems engineer position supports Gravwell's software engineering and systems development group, which is responsible for the design, development, and testing of the core Gravwell analytics platform. Well-suited candidates are self-motivated and capable of working remotely on tasks which may be self-designated. The position is remote, but candidates must be resident in the United States.

The core platform is a highly concurrent distributed system designed to ingest and analyze all manner of data, including text, network traffic, executables, audio, and video. Candidates are expected to be competent in Go and concurrent programming, comfortable on a Linux platform, and capable of debugging and designing distributed concurrent systems.

Duties and Responsibilities

- Design, development, and testing of Gravwell's Go-based analytics and storage systems
- Software development, system architecture, and API interfaces
- Product documentation and training
- Testing and development of remote ingest modules
 - Deployment platforms include BSD, OSX, Windows, and embedded systems
- Development of data extraction, processing, and storage systems
- Continuous integration and automated testing
 - Docker, Drone, etc.

Required Skills

A qualified candidate must be well versed in Unix process flow, task management, concurrent program design, distributed systems, and system security. Gravwell is a full-stack analytics platform; developers and engineers are responsible for data from generation to cold storage. The senior position requires a candidate that takes ownership of the platform, identifying and doing what is necessary to improve the team, the product, and the company at their own initiative.

The position requires minimal travel. Occasional extended travel involving a week or more of onsite support and analysis for 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 Unix fundamentals including but not limited to:
 - Process management
 - Network communications
 - Memory management
 - Kernel interfaces
 - Filesystems and file management
- 5+ years experience with statically-typed systems languages
 - Any combination of C, C++, Rust, Go
- 2 years experience with Go
- Network and systems security
- Network communications
 - IPv4, IPv6, TCP, UDP
- Operating systems
 - Linux, Windows, MacOS
- Parallel processing and concurrency
 - Resource locking and mutual exclusion
 - Deadlock and livelock
- Strong speaking and writing skills
 - Fluent in English

Preferred but not required skills

- Software reverse engineering and protocol design
 - Able to reverse engineer a black box system or network stream and develop a decoder
- Language experience
 - Assembly, C, C++, C#, Rust, Python, Java
- Lexing and grammar parsing for high speed data dissection
- Cryptography fundamentals and code protection
- Distributed system design
 - Federated data storage
 - Fault tolerant design and recovery
- Web interfaces
 - REST, websockets, API design
- Penetration testing and incident response

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.