Project Overview:

Douglas Financials Inc (DFI from here forward) has experienced successful growth and, as a result, is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI, we are happy to bring you on as our first InfoSec employee!

Once you are settled in and finished orientation, we have your first 2-Weeks assignments ready.

- **Week 1**: Your first set of tasks is to perform an analysis of Windows server using Defense in Depth principles, as well as the concept of Least Privilege, and provide a report with recommendations on OS hardening, compliance issues, encryption, and network security.

- **Week 2**: You'll next be asked to recommend mitigation steps from your analysis of firewall reports (and new connections) in the form of creating sample firewall rules. Similarly, you will analyze threat intelligence and craft sample IDS signatures. You'll also encrypt several files and folders in preparation for transport to a client.

Connecting, Reporting and Analysis

Criteria
Demonstrate the ability to connect and navigate within the provided computing environment.
Demonstrate understanding of security frameworks and best practices by analyzing the server's security configuration.
Demonstrate understanding of appropriate encryption methods for data in transit.
Demonstrate the ability to identify opportunities for security automation within an organization.

Firewalls and IDS Configuration

Criteria
Demonstrate understanding of firewall concepts and rule creation using proper syntax.
Demonstrate understanding of intrusion detection concepts and rule creation.
Demonstrate the ability to analyze firewall logs and recommend appropriate mitigation strategies.

Encryption, Hashes and Linux

Criteria
Demonstrate the ability to verify file integrity using cryptographic hashes.
Demonstrate understanding of Windows security event logging and analysis.
Demonstrate understanding of Linux file system permissions and user management.
Demonstrate the ability to communicate technical work to non-technical management.
Demonstrate understanding of file encryption for secure data transfer.