CASE STUDY: Delivering Talent for a DoD AWS Rollout

THE CLIENT

Department of Defense

Our Systems Integration partner was supporting a Department of Defense (DoD) project to standardize, streamline, and share critical data across the Army, DoD, and industry partners. Our partner was selected to modernize the DoD's financial system for sensitive activities of financial management transactions.

Our partner's project goal was to develop a SIPRNET installation of a cloud-based financial system that utilizes state-of-the-art technology to partition financial transactions by a user's need to know. Since this effort would require specialized AWS and DoD Network Security Specialists, our partner turned to our team at The Squires Group for help.

THE SUPPORT

- Amazon Web Services (AWS)
- Infrastructure as a Service (IaaS)
- AWS Identify and Access Management
- Secure Cloud Computing Architecture (SCCA)
- Cloud Security Requirements Guide (SRG)
- Unix/ Linux
- Firewalls (Palo Alto Networks, F5 Networks, Cisco Systems)
- Intrusive Detection System (IDS) and Intrusion Prevention System (IPS)
- Reverse Proxies
- Virtual Private Network (VPN)

THE CHALLENGE

This project initiative was designed to operate in a secure and classified environment. In addition, it would extend the functionality of the current SAP financial system to the special operations community. Finally, it will be designed to integrate seamlessly with the SAP financial system and provide secure, web-based, real-time data accessible by the special operations teams and other classified, intelligence, and special access program teams.

One of the key initiatives was the migration of various SAP applications to the AWS cloud. Given the stringent SIPRNET requirements (based on the sensitivity of the data), it was critical to bring in an experienced AWS team with in-depth knowledge of security administration. The project would also need a group of network security specialists who had a strong background in the DoD space.

The fact that all members of our consulting team were required to have an active DoD clearance added to the complexity of the staffing challenge.

THE SOLUTION

Our senior recruiting team accepted the challenge and divided our search into two projects – locating AWS Cloud Security specialists and experienced DoD Network Security specialists.

By surveying the AWS market, our team identified a similar DoD AWS project nearing completion. Bill Hill, one of our Senior Resource Managers, conducted an extensive search to identify the right resources from that project. Bill identified several candidates whose background and technical experience matched the requirements for the AWS Security Administrator.

After interviewing and screening potential candidates, Bill selected one senior resource with prior DoD experience working with AWS. We presented them to our partner, and they interviewed and on-boarded our consultant immediately.

To search for the AWS Network Security consultant, we adopted a slightly different approach since that talent is scarce in the Mid-Atlantic region. Jeremy Sullivan, one of our Resource Managers, researched candidates with deep Splunk experience and prior experience testing security on cloud deployments.

Through that process, he identified and interviewed a consultant with prior DoD AWS experience, utilizing Splunk to test AWS networks. We presented our consultant to our partner, who interviewed them immediately. Their team was so impressed with our consultant’s network security experience that he was added to the existing team to support them on a contract basis.

THE SUCCESS

Our AWS Cloud Security Architect continues to play a critical role in setting up the AWS environment for the SAP application. They are responsible for the AWS security while setting up the Infrastructure as a Service (IaaS). The key contribution has been in the area of providing guidance to ensure that the AWS setup follows all the DoD security guidelines. They are also responsible for AWS Identity and Access Management (IAM).

Our Network Security expert has been supporting the AWS cloud environment within the UNIX/ Linux landscape. They have been primarily responsible for the installation and configuration of firewalls, IDS, IPS, reverse proxies, and VPN. Our expert is responsible for installing and maintaining next-generation firewall applications from Palo Alto Networks, F5 Networks, and Cisco Systems.

Our AWS Cloud Security Architect and Network Security expert continue to play a major role in the rollout of AWS on this important project initiative. Their prior DoD experience continues to be an asset to the implementation team.