Network Automation Project Improves **Security, Supportability, and Scalability**

Case Study

its co

The Background

As one of the world's largest oil companies, the subject of this case study is under almost constant attack by cyber criminals and state actors who wish to disrupt western economies for financial and political gain.

After a massive breach that affected their business network for several months and cost multiple-millions-of-dollars, our (soon-to-be) client mounted a massive effort to secure its network and improve its cybersecurity defenses across the company.

This effort included a review of vulnerabilities and the creation of remediation plans at every level of the network – from network architecture and device configuration standards, to network security policies and procedures.

As part of solving this complex puzzle, the client reached out directly to Red Hat for help because of its expertise in network automation. And through its relationships in the Red Hat Partner Network, ITSco was asked to work on this project. Specifically, we were asked to work with the client's internal resources to help setup a network automation infrastructure, integrate it with the existing enterprise resource management system and configure it to improve operational efficiency and security, drive standardization, detect irregularities, and lessen the potential for human error.

The client wanted results fast. They wanted proof that the solution would be effective. And they wanted to be confident that, at the end of the engagement, their personnel would be up-to-speed on the ongoing management of the platform.

The primary tool used for this project was Red Hat's Ansible Tower Automation Platform, a flexible automation toolset that can be used across diverse network devices, making it easier to automate entire networks and IT processes.

Case Study:
Security, Supportability, and Scalability

The Deliverables

- Provision of computing resources to provide a high-availability environment,
- Installation and configuration of Ansible Tower to support separate test and production environments,
- Integration of Ansible Tower with existing IT management infrastructure,
- Creation of initial Ansible "playbooks" to support network operations automation, including:
    - **Automated management of Firewall rules and ACLs**
    - **Automation of network segmentation initiatives**
    - **Network device configuration standardization and consistency checking**
- Full documentation, including recommendations for best practices
- Mentorship of client personnel on Ansible capabilities, configuration, and best practices

The Results

Deliverables were all met on-time and within budget. And because of our efforts, the client now has:

- **A fully functional Ansible Tower environment, integrated into the existing IT management infrastructure, that can support its network automation efforts, improve operational efficiency and scalability, drive standardization, validate configurations, detect irregularities, and lessen the potential for human error,**
- **A core set of Templates and Playbooks to support their most critical security projects,**
- **Internal resources who have been successfully mentored to take over the operation and extension of the system.**

Due to the sensitive nature of this project, our client must remain anonymous. At the same time, they were so pleased with the results, that they brought us back for an additional security engagement (an SSL Certificate Management System) almost immediately.