Automating Cybersecurity Compliance by Enhancing Security Frameworks with Ansible at Chameleon Consulting Group

A Professional Readiness Experiential Program (PREP) Project Effort

----- ***Authors / Student Project Team Members*** -----

Jeewoo Lee

Layth Rishmawi

Khalil Jebsi

----- ***Industry Participant / Mentor*** -----

Jess Ingison
Director, Cybersecurity
Chameleon Consulting Group

----- ***Faculty Member*** -----

Brian K. Ngac, PhD
Instructional Faculty & Dean's Teaching Fellow
George Mason University's Costello College of Business
bngac@gmu.edu

Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!

Introduction

The internship at Chameleon Consulting Group (CCG) provided an opportunity for interns to work on cybersecurity automation and compliance. Over the 12-week program (which was reduced to approximately 8 weeks due to environmental setup issues), the interns collaborated with the engineering department to develop an automated system for implementing security controls. The experience introduced them to real-world cybersecurity frameworks, tools, and challenges while enhancing their technical and teamwork skills.

Business Challenge

One of the major tasks was automating the implementation of security guidelines for new virtual systems based on the NIST 800-53 control set. The challenge was to create an **Ansible playbook** capable of automatically configuring systems to comply with these strict security controls.

The second challenge was compiling the project outputs into an **OSCAL (Open Security Controls Assessment Language)-compliant document**, which would structure security controls, baselines, and assessment results in a standardized format (XML, JSON, YAML). However, due to technical difficulties and time constraints, this aspect remained incomplete.

Activities Done to Address the Business Challenge

For the first project, the interns performed a variety of activities related to automating security compliance for CCG. They worked with Ansible, an open-source automation tool, to implement security frameworks. They Accessed the company's environment using SSH via Putty to configure security settings remotely. They developed Ansible playbooks that structured security tasks into high, medium, and low-priority categories. They created YAML-based configurations to push changes to remote devices following NIST 800-53 security standards. And finally, they designed a main playbook architecture that called multiple YAML tasks to apply security settings efficiently.

For their secondary project, the interns performed a variety of activities related to OSCAL-Compliant Documentation. They gained an understanding of OSCAL as a machine-readable format for security controls. Following that, they attempted to structure security configurations into XML/JSON/YAML for documentation compliance. However, the interns faced technical challenges and time constraints that prevented full completion.

Results & The Positive Impact

The work resulted in four major positive impacts for CCG:

- Enhanced Security Automation: The Ansible playbooks allowed for efficient, repeatable security configuration, reducing manual effort and improving consistency.
- Improved Compliance with NIST 800-53: Systems were configured to meet federal security standards, strengthening cybersecurity defenses.
- Real-World Cybersecurity Experience: Interns gained hands-on experience in Ansible, YAML scripting, remote system access (SSH), and NIST compliance frameworks.

- Stronger Understanding of IT Workflows: Exposure to an enterprise-level IT environment improved their ability to troubleshoot, document, and deploy security solutions.

Conclusion

This internship provided invaluable experience in cybersecurity automation and compliance. The interns developed technical skills in security frameworks, scripting, and remote system management while also learning about teamwork and problem-solving in a professional IT setting. Though they faced challenges such as setup delays and technical difficulties, the experience deepened their understanding of cybersecurity best practices and prepared them for future careers in the field.

PREP Student Reflection

In their final presentation to CCG, the interns reflected on their experience as follows:

- Learning Ansible & YAML from Scratch: Interns had to quickly self-teach these tools, reinforcing the importance of independent learning in cybersecurity.
- Overcoming Communication Barriers: Initial team coordination issues improved over time, teaching them the value of effective collaboration.
- Understanding Real-World IT Operations: The experience provided insights into remote IT work, security implementation, and industry workflows.
- Handling Project Hiccups: Encountering unexpected challenges (setup delays, debugging issues) taught resilience and adaptability in an enterprise environment.