Continued Vulnerability Management Activities with the Institute for Defense Analyses

A Professional Readiness Experiential Program (PREP) Project Effort

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

Navjot Singh is a student at George Mason University graduated with a bachelor's degree in Cybersecurity. He is currently pursuing a Master's in Digital Forensics through Mason's accelerated BAM (Bachelor's to Accelerated Masters) program. His academic background and recent internship experience have provided him with valuable knowledge in cybersecurity principles and vulnerability management.

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

Christopher Murphy
Enterprise IT Operations Manager
Institute for Defense Analyses

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

Brian K. Ngac, PhD
FWI Corporate Partner Faculty Fellow
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

During this project, PREP supported IDA's vulnerability management effort on their unclassified side. In the summer-fall, the primary focus was on identifying and addressing system vulnerabilities using Tenable Security Center then remediation of the vulnerabilities. This fall, we took it a step further and planned to automate the process of identifying and addressing vulnerabilities on end user's systems. A system was built for automated/AI Generated email notification to end user to remediate vulnerable software.

Business Challenge

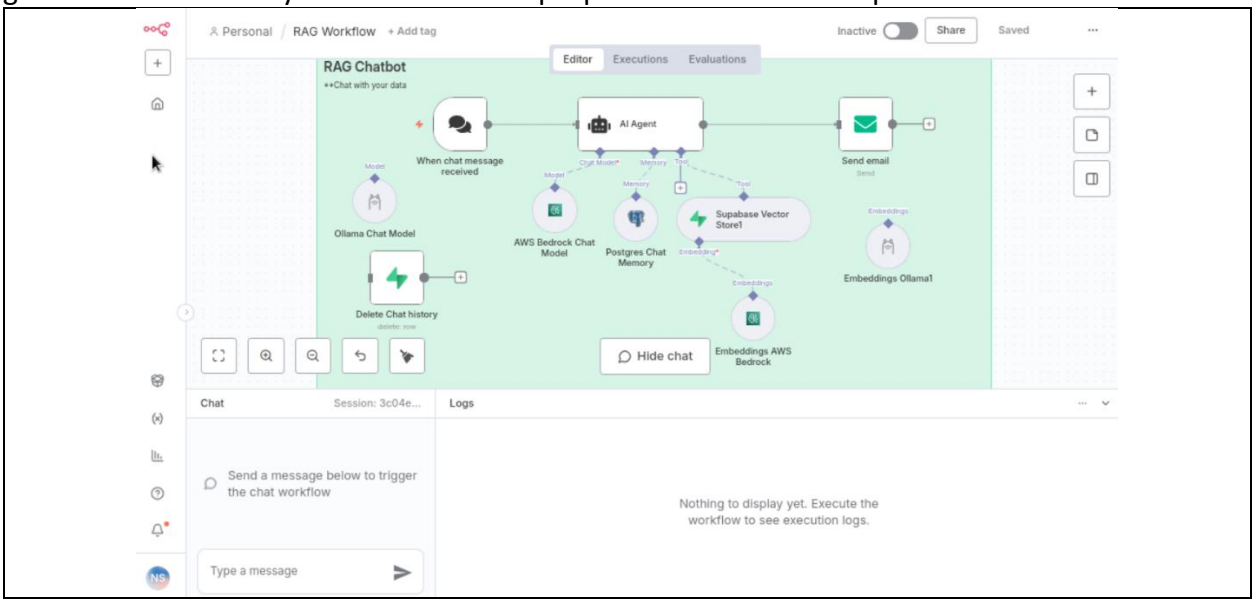
IDA was facing an increasing number of vulnerabilities across their systems and applications. These vulnerabilities ranged in severity, with some being critical or high risk, and posed a threat to the integrity and confidentiality of business operations. A major challenge was the lack of a streamlined process to ensure that findings from vulnerability scans were clearly communicated to the appropriate end users.

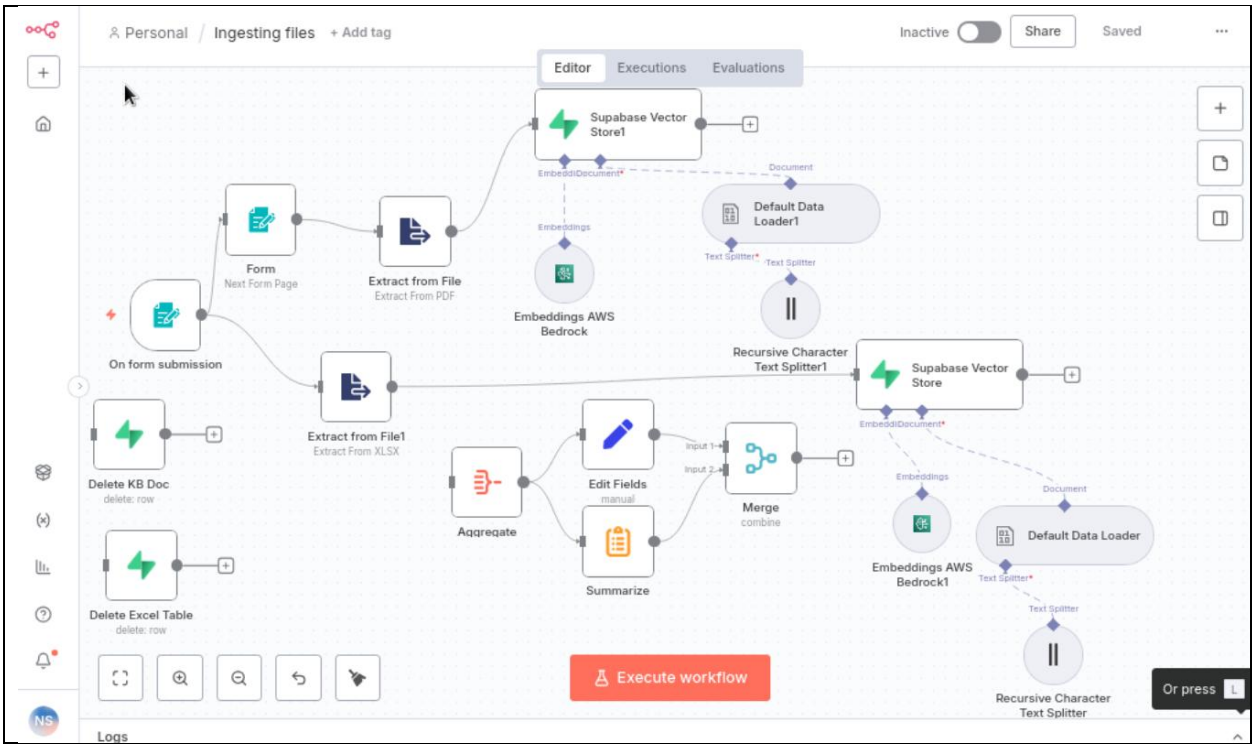
Activities Done to Address the Business Challenge

To address IDA's escalating vulnerability issues, the initiative was to develop an automated process which would pull the vulnerability findings from Tenable for end users and email each user the vulnerabilities found on their systems and the steps they need to remediate these findings.

Results & The Positive Impact

The automated notification system significantly improved the efficiency of vulnerability remediation efforts. By delivering clear, targeted remediation emails directly to end users, the system reduced the time required to communicate findings and eliminated much of the manual follow-up previously required by security staff. End users received actionable guidance tailored to their systems, which helped improve remediation turnaround time and consistency. Additionally, the automation framework provides a scalable foundation that can support future growth in vulnerability volume without a proportional increase in operational workload.





Email Example:

Vulnscansvc@ida.org
To Singh, Navjot [UNC]

Follow up. Start by Tuesday, October 7, 2025. Due by Tuesday, October 7, 2025.
We removed extra line breaks from this message.

Here is an example email:

Subject: Updating 7-Zip Application on SRV01

Body:

Hello Jane Doe,

To ensure you have the latest security patches and features for your 7-Zip application, we recommend updating to the latest available version.

Remediation Steps (retrieved from semantic database):

1. **Download the Latest Version**: Go to the official 7-Zip website (www.7-zip.org) and download the latest executable file for your operating system.
2. **Install the Update**: Run the downloaded executable file and follow the installation prompts to update the application.
3. **Verify the Version**: After installation, verify that you are running the latest version by checking the about box in the application.

Additional Recommendations:

* Regularly check for updates and install the latest version as soon as available.
* Consider configuring 7-Zip to automatically download and install updates when new versions become available.
* Ensure you have a backup of your important data before making any changes to the application.

If you encounter any issues during the update process, please reach out to the IT department for assistance.

Best regards,
[Your Name]

Note: The semantic database tool retrieved the following remediation steps:

* Download the Latest Version: `GET /7-Zip/updates/latest.exe`
* Install the Update: `RUN /latest.exe /install`
* Verify the Version: `CHECK ABOUT BOX IN APPLICATION`

This email was sent automatically with n8n https://n8n.io

Conclusion

This project demonstrated how automation and AI can enhance vulnerability management by bridging the gap between detection and remediation. By integrating vulnerability scan results with automated workflows and AI-generated guidance, the solution improves communication, reduces manual effort, and supports a more proactive security posture. The system can be expanded further to include additional data sources, ticketing integrations, or reporting capabilities, making it a valuable long-term asset for IDA's cybersecurity operations.

PREP Student Reflection

Through this project, I gained hands on experience in vulnerability management, automation, and applied AI within a real-world enterprise environment. I developed a deeper understanding of how security tools, data workflows, and end-user communication must work together to effectively reduce risk. This experience strengthened my technical skills while also highlighting the importance of designing solutions that are scalable, maintainable, and aligned with operational needs. The project reinforced my interest in cybersecurity and automation and provided valuable insight into how emerging technologies can improve existing security processes.