STREAMLINING SOC REPORTING: A CASE STUDY IN AUTOMATING DATA EXTRACTION AND COMPILATION

Efficient management of Security Operations Centers (SOC) is essential for IT service providers to ensure accurate monitoring and reporting of security incidents. Customized reports are vital for maintaining transparency and meeting specific client requirements. However, manual report generation can be time-consuming and prone to errors, necessitating innovative solutions for optimization and accuracy.

This case study underscores the significant benefits of adopting RPA in IT service management, particularly in enhancing the reliability and efficiency of SOC operations.

Client Profile:

Our client began operations in 2005 with a vision to surpass client expectations in IT infrastructure managed services and support, leveraging deep technical expertise and a uniquely personalized approach to customer service.

The Challenge:

Our client, a US-based IT service provider, faced significant challenges in managing SOC operations for its clients. The primary task involved generating custom SOC reports tailored to each client's requirements. These reports generated was a customs report which combined data from Word, Excel, and PowerPoint, being sent via email and included about 500 data points. The data was extracted live from systems like Rapid7 and Salesforce (SFDC), often amounting to millions of records. The manual process of report generation required SOC personnel to spend 3-4 hours per report, during which human errors such as copy/paste mistakes were common, leading to embarrassing inaccuracies in the reports sent to clients.

The Approach:

Ahana adopted a meticulous, phased approach to implement Robotic Process Automation (RPA) for the client's SOC report generation process. This approach ensured a smooth transition from manual to automated processes:

- **Planning & Setup Readiness**: Initial phase focusing on readiness and strategic planning.
- **Process Walkthrough**: Detailed demonstration by the client's teams to explain processes to be automated.
- **Script Development**: Creation of automation scripts tailored to the client's needs.
- **User Acceptance Testing (UAT)**: Testing the scripts in a real-world environment to ensure they meet all requirements.
- **Go Live & Refine Script**: Implementing the scripts and refining them based on initial feedback and performance.

Each phase included well-defined deliverables, key tasks, and roles for both the client and Ahana teams. Templates were used to standardize tasks and activities, ensuring consistency and clarity throughout the implementation process.

Ahana's Solution:

Our team utilized an RPA tool to automate the manual SOC report generation process.
The automation process included:

- Extracting data from Rapid7 and SFDC.
- Compiling data into a SOC Word document.
- Generating detailed reports including Alerts Generated, Finding Reports, Gauge Graphs for Closed Alerts, Endpoint Agents, Active Users & Administrators, and User & Service Accounts with Non-Expiring Passwords.

Business Impact:

The implementation of the RPA solution had profound impacts on the client's SOC operations:

1) Time Efficiency: Report generation time was reduced from 3-4 hours to just a few minutes - **Reduced TAT upto 80%**.

2) Accuracy and Error Elimination: The automated system produced error-free reports, eliminating the human errors previously associated with manual report generation. - **Error reduced upto 100%**.

3) On-Demand Report Generation: Reports could now be generated on demand and in real-time, significantly improving responsiveness to client needs.

4) Cost Optimization: The automation reduced the time and resources required for report generation, leading to substantial cost savings - **Cost savings upto 80%**.

5) Elimination of Human Effort: SOC personnel were freed from the tedious task of manual report generation, allowing them to focus on more critical activities.

Conclusion:

Ahana's RPA solution transformed the client's SOC report generation process, enhancing accuracy, efficiency, and cost-effectiveness. By automating a previously manual and error-prone task, Ahana enabled the client to deliver high-quality, timely reports to their customers, thereby strengthening client relationships and operational performance.

About Ahana Systems and Solutions:

Ahana Systems & Solutions is a leading IT Infrastructure Management Services and Digital Transformation company based in Bengaluru, India. Our expertise extends to a wide range of solutions, including Cloud, RPA, DB & EDW, BI & Analytics, and Application Development. Our 100+ roster of clients relies on us for our deep domain expertise, skilled resource base, and proven partnership with the best technology providers.

Contact Us:

sales@ahanait.com | info@ahanait.com | +91 9148724605