Case Study for

Frictionless efficiency in TAC

iOPEX delivers frictionless efficiency in TAC with 60% of cases resolved through auto-remediation for a security & network solutions provider through operational expertise and AI engineering.

Industry
Cybersecurity

Services
TAC

iOPEX handles **Enterprise Technical Services** operations for the customer and manages close to 50% of all their global support & end customer interactions from Global Delivery Centers in US, Canada, India and Poland. This includes L2-L4, TAM, Expert Support, Engineering Support, Customer Success, Partner Success etc. iOPEX handles network administrators, security administrators, IT administrators from enterprises who have invested customer's solutions for their enterprise mission-critical infrastructure.

The Client

North America headquartered, leading provider of platform solutions for Network Security, Cloud Security and Security Operations through multiple product categories.

Business Challenges

As part of continuing enhancement to the products & services, client identified potential vulnerabilities and exposures were identified in their flagship product. This vulnerability posed a risk to the security of their customers' networks and client wanted to address the issue proactively and manage the increase in volume of support cases from concerned customers seeking assistance in securing their systems against potential threats. Such a proactive approach improves the confidence of enterprise customers in client's solutions.

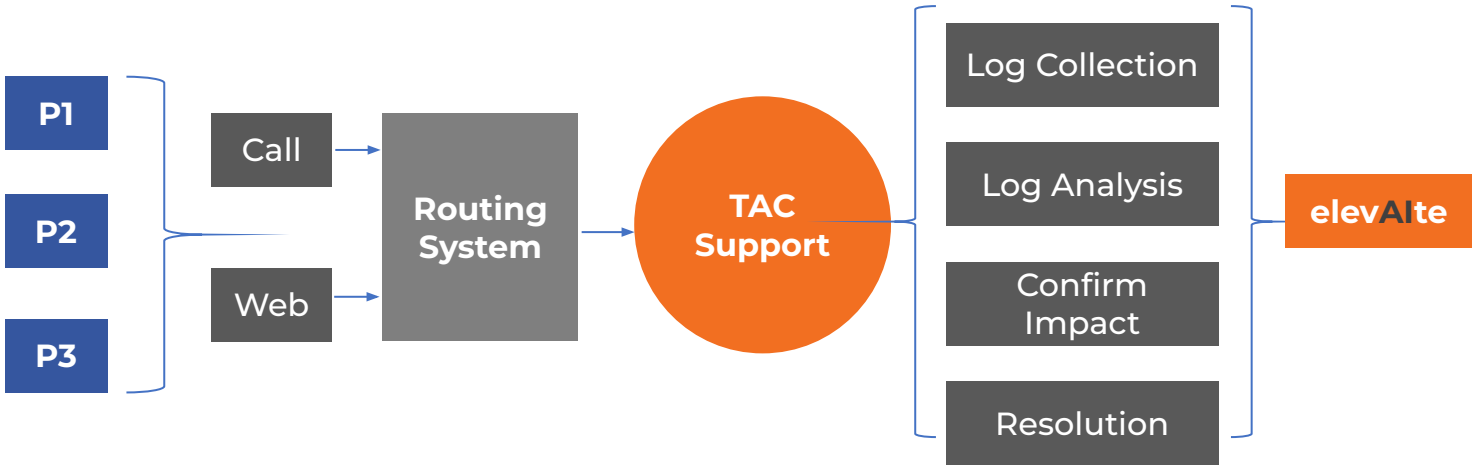
The business need was clear - A scalable and efficient solution to address proactive & incoming support cases while ensuring that their customers' networks remained secure and protected from potential vulnerabilities.

Our Solutions

The solution is a combination of AI Engineering and Operational expertise. iOPEX closely collaborated with the client to implement a revised remediation model that included Generative AI framework (Development, Deployment, Production and Monitoring) & iOPEX's AI operations team that could automatically parse through vast amounts of firewall logs and identify potential instances of vulnerabilities across customer base.

The AI system was trained to analyze firewall logs, identifying patterns indicative of the vulnerabilities presence. By processing large volumes of data rapidly, the AI solution could pinpoint affected systems with a high degree of accuracy, enabling the support team to prioritize support cases based on the severity of the vulnerability and proactively reach out to impacted customers.

Furthermore, the AI system was integrated with the support ticketing system, allowing it to automatically generate and send tailored solutions to customers' support cases. These solutions included step-by-step instructions for patching the vulnerability, recommended configuration changes, and best practices for enhancing network security. With automation of the resolution process, the strain on the support team was alleviated while ensuring that the customers received proactive and effective assistance in securing their networks.



Business Benefits

The implementation of the AI solution, coupled with AI operations, yielded significant improvements in support efficiency and customer satisfaction.

Streamlined Support Workflow:

The AI system significantly reduced the burden on the support team by automating the analysis of firewall logs and generation of solutions. This allowed support staff to focus their efforts on more complex cases requiring human intervention, thereby improving overall productivity and response times. Brought the waiting interactions down by **75%.**

Proactive Customer Engagement

By leveraging AI to identify and address vulnerabilities proactively, the client was able to reach out to customers before they even reported issues, demonstrating their commitment to customer security and satisfaction. This proactive approach fostered greater trust and loyalty among Chennai Firewall's customer base.

Enhanced Security Posture:

The AI solution the client to rapidly identify and mitigate potential security risks across their customer network, minimizing the impact of the CVE and reducing the likelihood of security breaches.

The project was successfully implemented with careful monitoring for any customer impacts and risks. Following is the summary of results:

Phases	Before Gen AI	After Gen AI (elevAIte)	Improvement
Log Error Analysis	1 – 2 days	3 hrs.	75%+
Identification Process	3 – 5 days	4 hrs.	90%+
Interactions waiting	600	100	75%+