Innominds
Powering the Digital Next

Case Study

Fortifying Telecom Infrastructure with Future-Ready Defense Systems

Conducted comprehensive security assessments to identify and mitigate critical vulnerabilities across diverse infrastructure platforms.

Acquired stakeholder and client's confidence by enhancing the security posture.

Success Highlights

Adhered to regulatory compliance and followed industry-standard protocols.

Implemented DevSecOps practices to streamline security processes.

Problem

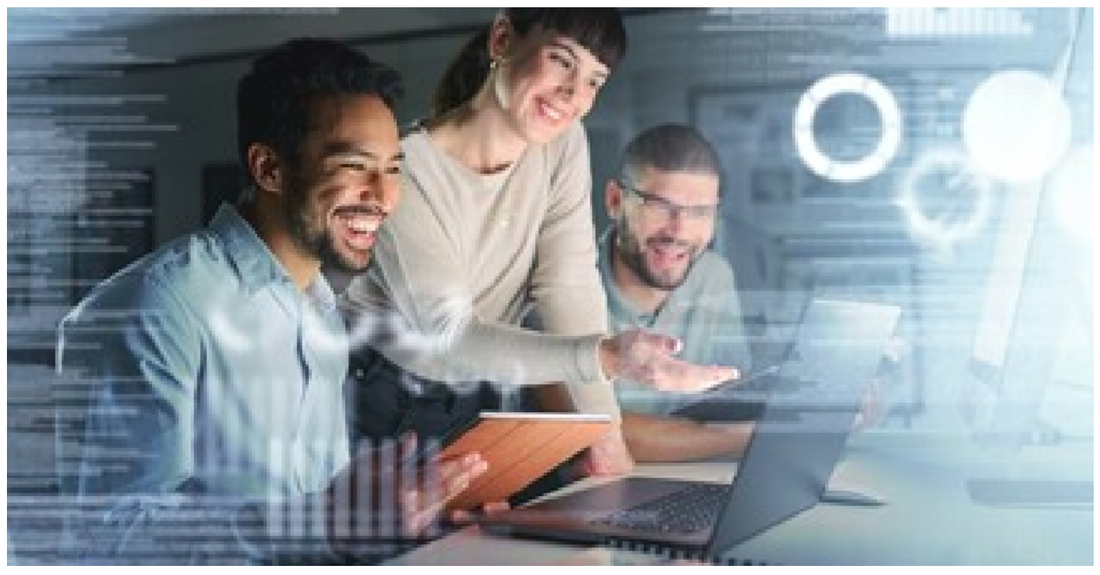
Our telecom industry client faced constant threats to their infrastructure security. Their ecosystem comprises on-premises infrastructure, GCP services, internally developed web and REST APIs, and third-party applications. With such an intricate and diverse setup, keeping the security strategy constantly updated was challenging. They were dealing with the risks of misconfigurations, vulnerabilities, and strict regulatory requirements. These security gaps opened them up to the possibility of cyber-attacks and threatened their data privacy. Their goal was to implement comprehensive end-to-end security solutions to strengthen their infrastructure, ensure regulatory compliance, and allow them to operate securely and confidently in a highly competitive and risky environment.

Challenges

The project faced numerous challenges across several dimensions

Operationally

The team had to work across multiple internal groups, including IT, security, development, and operations, each with its own priorities and methodologies. This made the distribution of resources, such as personnel, time, and budget, particularly complex while trying to maintain the current operations flow.



Technically

Identifying vulnerabilities and misconfigurations was a significant hurdle. Integrating multiple security tools into the existing CI/CD pipeline and ensuring the seamless integration of diverse technologies added to the complexity.

Human

Resistance from stakeholders accustomed to the established framework. Additionally, there was a need to narrow skill gaps among the client’s operation and development groups to ensure effective implementation.

External Factors

The necessity to adhere to advanced regulatory standards specific to the telecommunications industry and keep pace with rapid technological advancements and emerging threats. The risks associated with inadequate defense systems were severe, potentially exposing the client to significant financial losses. These risks included increased chances of data breaches, system downtime, regulatory fines, and reputational damage, leading to direct financial losses from remediation costs, legal fees, and compensation to affected parties. Moreover, the long-term financial repercussions due to the loss of customer trust and damage to brand reputation could result in decreased revenue and market share.

Approach

Innominds applied a structured approach to enhance client security.

Initial Analysis

Innominds began the engagement by conducting a thorough advisory assessment to understand the client's infrastructure and security posture comprehensively. This process started with a collaborative two-day workshop involving various client teams to gather detailed insights into the client's environment, including on-premises infrastructure, Google Cloud Platform (GCP) services, in-house developed web and REST APIs, and third-party applications.

Strategy Development

After an initial assessment, Innominds clearly outlined the extent of security requirements. The security landscape of the client was revealed, and areas demanding immediate action were identified, including:

Task Prioritization

Security measures were categorized by their relative priority, risk level, and overall security posture. The top two highest-risk factors were prioritized to minimize risks and address the most critical issues.

Assessment Types and Tools

A detailed framework included security audits, vulnerability scans, and risk evaluations. Each operation was assigned a specific tool and methodology to ensure thorough and accurate evaluations.

Timeline and Milestones

A timeline was established to capture the chronology of events and milestones, ensuring disciplined project progression checked frequently against plans.

Innominds after conducting a detailed analysis and development of the plans ensured a marked improvement in security standards for the client. The main threats were quickly identified and eliminated, and work was carried out to systematically address high-priority risks. Security concerns were reduced by the implementation of a systematic framework that included regular assessments, risk identification, and management. This strengthened the client's infrastructure while also mapping out a timeline of further enhancements to align with the client's operational goals and objectives while maintaining security resilience.

Implementation Plan

The implementation plan was executed across multiple levels, focusing on immediate and future security enhancements.

1. Gcp Cloud Security:

Security Audit: A comprehensive security audit of the client's GCP infrastructure was conducted to identify misconfigurations and vulnerabilities.

Risk Register and Reports: Risk registers and security reports detailed identified threats, risk ratings, descriptions, and strategies.

Method of Procedures (M.O.P.s): M.O.P.s were designed for quick resolution of medium and high-risk items, with operational team members addressing issues related to their teams.

Support for Deployment: Fixes were implemented at lower levels, and proper aid was given to projects implementing these fixes into production environments.

2. Application Security:

Grey Box Security Assessments: Conducted end-to-end grey box security assessments on in-house-built applications and microservices using OWASP, SANS, and WASC guidelines.

Review and Mitigation: Prepared a detailed vendor application risk assessment and a risk register with mitigation strategies.

Stakeholder Engagement: Held walkthrough sessions with stakeholders to explore identified risks and prevention mechanisms, ensuring clear communication and understanding.

Support for Security Fixes: Assisted the development team in fixing minor and major security issues.

The client's security was strengthened in many aspects because of the execution of the implementation plan. Important and potentially harmful vulnerabilities were discovered during the security audit of the GCP infrastructure and grey box evaluation of the apps. These concerns were subsequently resolved, and risk registers and reports were used to limit risks. High Risk Issue addressed through Method of Procedures (M. O. Ps) were resolved quickly and effectively, while targeted support for deployment helped ease the process of integration of fixes within the producing arenas. Engagement and support of stakeholders for security fixes improved the relationships with vendors and supported security work, providing a solid foundation for continued improvements in security.

3. IT Security

Evaluation of Security Controls: Reviewed security controls such as firewalls, routers, VPNs, and endpoint security tools.

Employee Process Assessment: Assessed compliance and security requirements for employee onboarding and off-boarding processes to identify security loopholes.

Detailed Reporting: Provided a report summarizing proposed security gaps and mitigation strategies.

Implementation Support: Supported teams in implementing recommended security fixes.

Threat Detection and Response: Implemented Gen AI to enhance threat detection and analysis, formulating effective responses to identify and mitigate irregularities and security threats.

4. Devsecops Integration

Tool Identification and Integration: Identified security tools for integration into the client's CI/CD pipeline to enable automated security checks.

Workflow Development: Developed comprehensive workflows and process documents to incorporate security checks within CI/CD processes.

Hardening Documentation: Created documentation for enhanced security measures to guide ongoing security practices.

Evaluation of Tools: Evaluated cloud-native and third-party tools for automated security assessments, including configuration reviews, container security, vulnerability assessments, patch management, endpoint security, SIEM, and SOC.

Proof of Concepts (P.O.C): Conducted P.O.C.s with various tools to assess features and budget considerations, ensuring selection of the most effective and cost-efficient solutions.

Innominds strengthened the client's telecom network by comprehensively analyzing security vulnerabilities and providing state-of-the-art security measures. The outcomes included identifying and mitigating critical misconfigurations and vulnerabilities across on-premises infrastructure, GCP services, web and REST APIs, and third-party applications. Consequently, the client achieved increased regulatory compliance and a more robust security position, enabling them to operate in a more secure and resilient environment.

Ensuring the firm met industry standards and regulatory requirements strengthened the trust of stakeholders and customers. With the implementation of DevSecOps practices in their security process, security checks are now automated and run continuously in the CI/CD pipeline. Finally, the client gained expertise in the complex telecom infrastructure ecosystem through enhanced assurance, reduced risk exposure, and a durable foundation for leadership in security.

Innominds' comprehensive assessment and strategic implementation of security measures have empowered the client to navigate the intricate telecom infrastructure landscape with resilience. Through collaborative efforts and expertise, we have safeguarded their assets, mitigated risks, and laid a foundation for sustained security excellence. By addressing operational, technical, and human challenges head-on, we have enabled the client to achieve enhanced regulatory compliance, fortify their security posture, and instil confidence among stakeholders. Continuous collaboration and periodic security reviews will be essential to maintaining and further enhancing the security posture of the client's infrastructure. Innominds remains committed to supporting our client's journey toward security excellence, providing innovative solutions and expertise to address emerging threats and challenges in the dynamic telecom industry.

About Innominds

Innominds is a leading digital transformation and product engineering company headquartered in San Jose, California.

Driven by the idea of "Engineering Intelligence. Responsibly," Innominds partners with cutting-edge companies to co-create products and solutions across various technological areas, from devices and embedded systems to AI-powered applications.

In addition, our expertise helps businesses navigate the complexities of digital transformation and achieve more with less. To learn more about our services, visit us at www.innominds.com.

www.innominds.com | USA | 99 Almaden Blvd, Suite 710, San Jose, CA 95113 | Ph: +1 408-434-6463