CONSISTENT SYSTEM BRACES UP A GLOBAL IT SERVICES COMPANY TO STAY AHEAD OF CYBER ATTACKS

CERT-In Compliance Testing | Case Study

ABOUT THE CLIENT

The Client is a global information technology consulting and cloud services company that delivers result-oriented and cost-effective cloud services and business IT solutions to help companies across various industries maximize their revenue and growth.

BUSINESS REQUIREMENT

The client required a rigorous security assessment of their critical enterprise application. Involved evaluating the cyber resilience across network, application, API layers, with the ultimate goal of achieving CERT-In certification, a very stringent security standard.

AUTOMATED TESTING UTILITIES

- Nmap
- Nessus
- Rapid 7
- Qualys
- Kali Linux
- Burp Suite Pro
- OWASP ZAP
- Acunetix
- Microsoft Threat Modelling Tool
- Threat Dragon
- Wireshark
- SSLScan
- SQLMap
- Postman

50% Faster Results

40% Lesser Costs

Full coverage on OWASP, CERT-In Standards

OUR APPROACH



Engaged experienced security professionals for a comprehensive assessment of the enterprise application.



Utilized top tools & methodologies to identify vulnerabilities across network, application, and API layers.



Conducted network testing to remediate weaknesses in configurations, access controls, and data transmission.



Performed application-level testing to uncover injection attacks, authentication bypass, and data exposure.



Assessed API security focusing on authentication, access controls.



Aligned assessment with CERT-In regulatory standards.

OUTCOMES ACHIEVED

- Thorough Security Assurance: Ensured the application's resilience against diverse threats through comprehensive tests.
- CERT-In Certification: Achieved certification by meeting CERT-In's stringent security standards.
- Enhanced Security Posture: Strengthened overall security by implementing recommended controls and remediating identified vulnerabilities.