Case study

INFOVISION
#AccelerateDigital

VAPT and DAST assessment for a leading medical provider

Enhancing cybersecurity for a medical technology customer

InfoVision collaborated with a leading U.S. based medical technology company, specializing in cancer detection solutions, to enhance its security infrastructure. Through comprehensive Cloud VAPT *(GCP & Azure), on-premises infrastructure assessment, and DAST*, we significantly bolstered data protection, ensured HIPAA* compliance, and enabled secure service delivery. This partnership resulted in a robust security posture, mitigating risks across cloud and on-premises environments, and reinforcing the company's commitment to protecting sensitive medical data and maintaining operational integrity.

About the customer

The customer is a pioneer in medical technology, offering advanced cancer detection and therapy solutions. Their high-precision systems rely on secure, compliant environments to protect sensitive healthcare data and ensure uninterrupted services for patients and providers.

* Vulnerability Assessment and Penetration Testing (VAPT)
* Dynamic Application Security Testing (DAST)
* Health Insurance Portability and Accountability Act (HIPAA)

© InfoVision, Inc. All Rights Reserved.

Business need

Data breaches can have catastrophic consequences in healthcare. To strengthen its security posture and meet regulatory requirements, the customer sought to:

- Ensure HIPAA compliance and align with industry best practices.
- Secure on-premise (network devices and servers) and cloud infrastructure (GCP and Azure).
- Protect sensitive medical applications and patient data.
- Maintain uninterrupted service delivery for patients and healthcare providers.

Solution delivered

InfoVision implemented a robust security framework leveraging advanced vulnerability detection and remediation:

Hybrid vulnerability assessment

- Utilized a combination of automated scans and in-depth manual analysis for comprehensive coverage.

Comprehensive vulnerability analysis

- Conducted thorough VAPT on GCP and Azure cloud assets
- Performed DAPT on critical applications.
- Assessed on-premises infrastructure, including all network devices and servers.

Detailed reporting and prioritization

- Delivered executive summaries for leadership.
- Provided technical reports with prioritized vulnerabilities and actionable remediation steps.

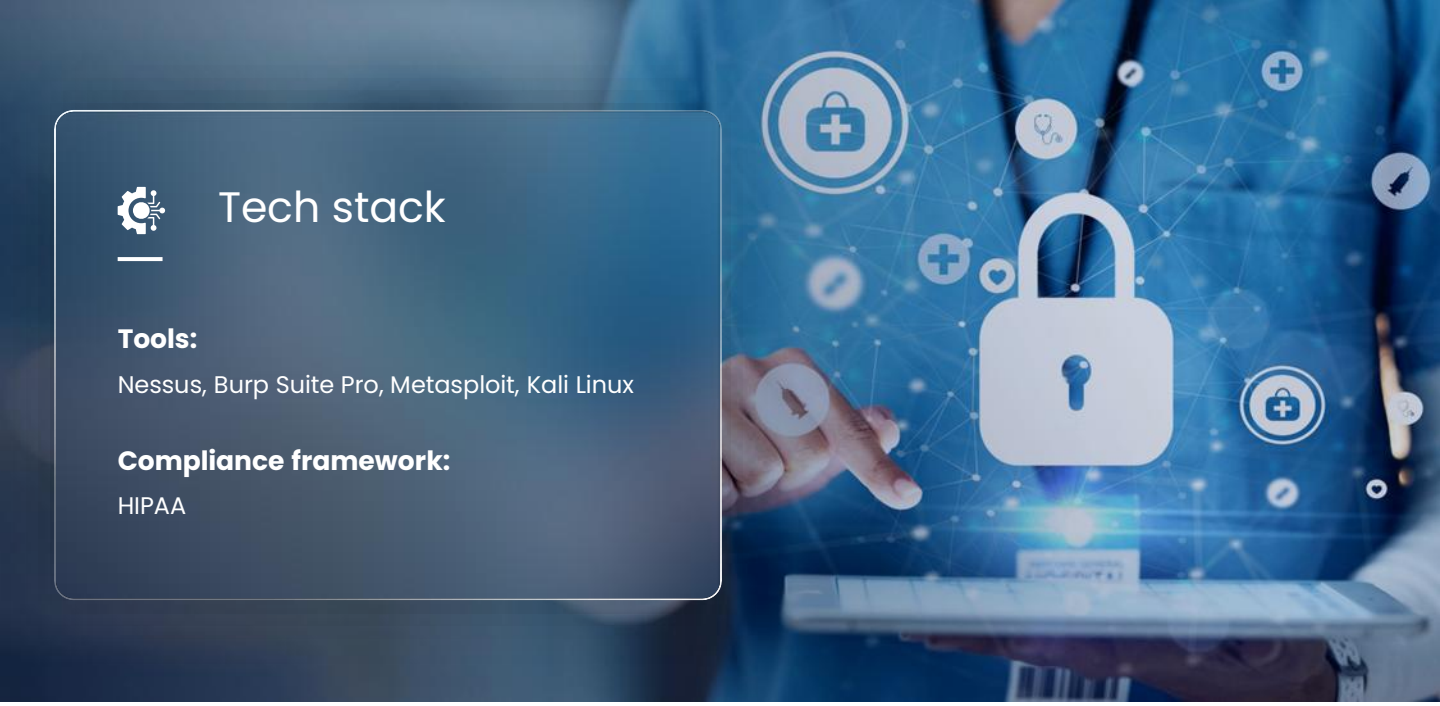
Collaborative remediation

- Engaged in brainstorming sessions with the customer's development teams.
- Offered guidance on vulnerability closure strategies.

Validation and assurance

- Conducted rigorous re-validation checks for all critical and high-risk vulnerabilities.

© InfoVision, Inc. All Rights Reserved.



Tech stack

Tools:

Nessus, Burp Suite Pro, Metasploit, Kali Linux

Compliance framework:

HIPAA

Key outcomes

Enhanced security posture: Prioritized critical vulnerabilities across cloud and on-premise assets.

Proactive risk mitigation: Uncovered potential threats during the testing phase, preventing future exploits.

Regulatory compliance: Ensured adherence to HIPAA and industry standards, protecting sensitive medical data.

Stakeholder confidence: Increased trust among patients, healthcare providers, and partners.

Operational resilience: Enabled the delivery of secure and uninterrupted medical technology services.

© InfoVision, Inc. All Rights Reserved.