FORTRA®

Pen Testing Use Case - Hospital Network

Enhancing Hospital Cybersecurity with Automated Penetration Testing Software

Background

A major hospital system relies on a complex digital ecosystem—including a patient portal, Electronic Health Records (EHR), IoT-connected medical devices, and an internal clinical network—to support daily operations and patient care. With rising cyber threats targeting healthcare environments, the hospital needed a way to continuously assess weaknesses without disrupting clinical workflows.

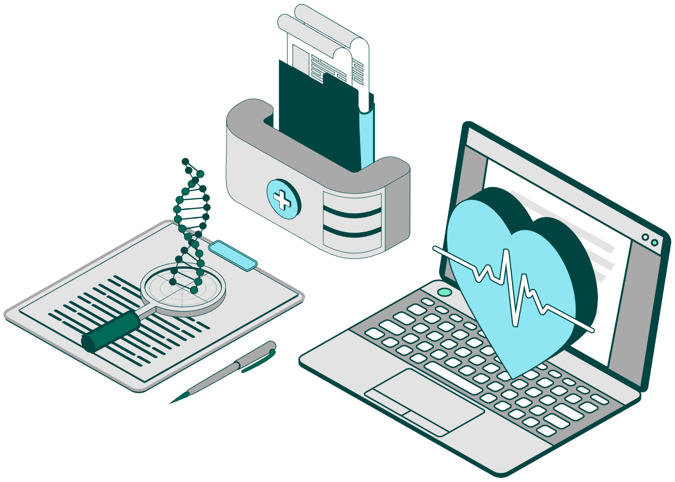
To achieve this, the security testing team used penetration testing software, such as Core Impact, to simulate real-world attack scenarios safely and efficiently.

Phase 1: Planning & Reconnaissance

Before executing any tests, the team defined a clear scope to avoid operational disruptions, particularly important in environments that support patient care.
Key reconnaissance tasks included:

- Mapping the hospital network and identifying interconnected systems such as EHR servers, medical imaging devices, IoT endpoints, and Wi-Fi access points.
- Identifying open ports, active services, and operating systems used across clinical and administrative devices.

By leveraging Core Impact, the team was able to automate early reconnaissance steps and streamline their testing workflow.



Phase 2: Scanning

With the scope established, automated scanning began across multiple systems:

- Network scanning to reveal outdated firmware, misconfigurations, and exposed services.
- Web application scanning to identify injection vulnerabilities associated with patient portals or internal web-based tools.
- IoT/medical device scanning to detect hardcoded credentials or unrestricted permissions.

Core Impact's ability to integrate scanning results from top vulnerability management solutions provided the team with a consolidated view of vulnerabilities, helping them prioritize by risk and clinical impact.

Phase 3: Gaining Access (Exploitation)

Once vulnerabilities were identified, exploitation testing was performed to validate risk levels:

- Running CVE-based exploits against outdated firmware on Wi-Fi access points, confirming the potential for remote code execution.
- Testing for hardcoded credentials on medical imaging systems.
- Attempting privilege escalation on compromised systems.
- Simulating ransomware propagation, helping the hospital visualize how fast an attack could spread.

Core Impact's certified exploitation capabilities proved critical for safely demonstrating real-world attack paths while maintaining hospital uptime.

Phase 4: Lateral Movement & Post-Exploitation

After initial access was achieved, the security team simulated internal attacker behavior:

- Mapping reachable clinical systems from compromised devices.
- Assessing whether PHI (Protected Health Information) was accessible due to misconfigured file permissions.
- Evaluating segmentation controls between administrative and clinical networks.

Core Impact's structured workflow enabled repeatable and safe post-exploitation testing across sensitive healthcare systems.

Phase 5: Reporting & Remediation

The automated penetration testing platform generated two levels of reports:

- Technical reports for IT teams, containing details on exploited vulnerabilities and recommended fixes.
- Executive summaries highlighting business impact, regulatory implications (HIPAA, NIST, ISO 27001), and prioritized action items.

Once remediation steps were completed, the team retest vulnerabilities and verify closure.

Outcome & Lessons Learned

At the outset, the hospital launched automated penetration testing to strengthen security and reduce risk across patientcare systems.

Identify Critical Vulnerabilities Before Attackers Could

Testing uncovered several high impact weaknesses—including outdated WiFi firmware vulnerable to remote code execution, hardcoded credentials on medical imaging systems, and misconfigured file permissions exposing PHI—giving the hospital early visibility into threats that could jeopardize operations and data privacy.

Support Compliance With HIPAA, NIST, and Internal Controls

Automated testing, enhanced through Core Impact, enabled continuous, scalable assessments, early detection of vulnerabilities across EHR, IoT, and network assets, and streamlined verification of remediation efforts to meet healthcare security standards.

Clarify Key Areas of Concern Across Clinical and Network Systems

With clear findings and compliance ready reports, the hospital improved its cybersecurity posture and established a recurring testing schedule to ensure ongoing risk reduction and operational resilience.

Advanced Penetration Testing Tools

With Fortra's Core Impact, healthcare organizations gain a powerful, multivector penetration testing platform designed to evaluate vulnerabilities across critical clinical systems, connected medical devices, and hospital networks. The solution delivers commercial grade, certified exploits within an automated framework—each exploit vetted internally, compatible with thirdparty modules, and subjected to routine testing to ensure reliability, stability, and the absence of hidden backdoors.

Core Impact's continually updated exploit library—expanded regularly—helps hospitals stay ahead of fast-evolving cyber threats. For environments where patient safety, PHI protection, and uninterrupted clinical operations are paramount, this makes Core Impact an ideal tool for maintaining strong, proactive cybersecurity defenses.

FORTRA®

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.