WOOLLEMIA INFOSEC

WOOLLEMIA INFOSEC

Case Study

Comprehensive Network Security Assessment for a Multi-Campus Educational Institution

Industry	Higher Education
Environment	On-Premises Campus Network with Multi-Building Wired & Wireless Infrastructure
Assessment Type	Internal & External Network Security Assessment
Technology Landscape	Enterprise LAN/WAN, Wireless Infrastructure, Campus Servers, Active Directory, Firewalls, Network Segmentation
Core Services Delivered	Network Vulnerability Assessment, Internal Penetration Testing, Wireless Security Assessment, Firewall & Segmentation Review, Active Directory Security Review, Configuration Hardening Review

Executive Summary

Educational institutions increasingly rely on large, distributed network environments to support academic operations, research activities, administrative functions, and student services across multiple buildings and campuses. As these networks grow in scale and complexity, they become an attractive target for cyber threats seeking to exploit weak segmentation, outdated configurations, and exposed services.

A leading educational institution engaged Woollemia Infosec to conduct a comprehensive Network Security Assessment of its campus-wide network infrastructure, encompassing wired and wireless environments across multiple academic and administrative buildings. The institution sought an independent evaluation to confirm that its network could reliably support day-to-day academic operations while protecting student records, research data, and administrative systems from unauthorized access.

Woollemia Infosec performed a structured assessment covering perimeter defenses, internal network segmentation, wireless infrastructure, Active Directory configuration, server and endpoint exposure, and network device hardening. The engagement combined automated discovery with extensive manual validation to uncover real-world attack paths that automated tools alone would miss.

The assessment enabled the institution to strengthen its network security posture, close critical exposure points, and establish a prioritized roadmap for long-term infrastructure hardening.

Client Overview

The client operates a multi-building campus network supporting thousands of students, faculty, and staff across academic departments, administrative offices, libraries, hostels, and research facilities. The network infrastructure includes wired connections in classrooms and offices, campus-wide wireless coverage, centralized authentication services, file and print servers, and internet-facing systems supporting remote access and online learning platforms.

Day-to-day operations depend on reliable connectivity between academic buildings, administrative systems, and centralized services including student information systems, learning management platforms, and internal communication tools.

As the institution expanded its digital footprint and introduced additional connected devices and services, it recognized the need for an independent, structured assessment of its network security posture.

Business Challenge

The client's network had grown organically over several years as new buildings, departments, and services were added, resulting in a complex mix of legacy and modern network equipment, inconsistent segmentation practices, and varying levels of configuration hardening across devices.

The institution required assurance that its wireless infrastructure, internal segmentation, and perimeter defenses could withstand both external threats and risks originating from within the campus network itself, including compromised endpoints or unauthorized devices connecting to campus networks.

Because the network carried sensitive student and staff data, research information, and administrative records, any weakness in network security controls could potentially disrupt academic operations, expose confidential information, or damage institutional reputation.

The client also wanted to verify that wireless networks were appropriately isolated from critical administrative systems, and that unauthorized devices could not gain a foothold that would allow lateral movement toward sensitive infrastructure.

Our Understanding

Woollemia Infosec recognized that securing a large educational campus network required more than scanning for known vulnerabilities. Academic environments present a distinctive challenge: open, accessible networks must coexist with sensitive administrative and research systems, and the population of connected users and devices changes constantly.

Our team understood that weaknesses in wireless security, network segmentation, or device hardening could allow an attacker with only physical proximity to the campus to pivot toward critical systems. Rather than relying solely on automated scanning, our assessment combined manual internal and external penetration testing, wireless security evaluation, segmentation validation, and configuration review to build a realistic picture of the institution's actual exposure.

Our Solution

Network Discovery and Architecture Review

The engagement began with detailed reconnaissance of the client's network topology, including building-to-building connectivity, VLAN structure, wireless deployment, server locations, and perimeter architecture, establishing a complete map of the attack surface.

External Perimeter Assessment

Our consultants assessed internet-facing systems and services, identifying exposed ports, outdated software versions, weak or default credentials, and misconfigurations that could be leveraged by external attackers to gain an initial foothold.

Internal Network Penetration Testing

Simulating a threat actor already present within the network, our team evaluated internal segmentation, lateral movement opportunities, exposed internal services, shared credentials, and privilege escalation paths across the wired campus network.

Wireless Security Assessment

Our consultants evaluated the security of campus wireless networks, including encryption strength, authentication mechanisms, network isolation between guest, student, and administrative wireless segments, rogue access point exposure, and resilience against common wireless attack techniques, all performed strictly within the pre-agreed scope and authorized testing windows.

Active Directory and Identity Infrastructure Review

Given the central role of directory services in the institution's operations, our team reviewed domain configuration, privileged account management, group policy settings, credential storage practices, and common misconfigurations frequently leveraged for privilege escalation.

Network Device and Firewall Configuration Review

Our consultants reviewed the configuration of routers, switches, and firewalls supporting the campus network, evaluating access control lists, management interface exposure, firmware currency, and adherence to secure configuration baselines.

Segmentation and Access Control Validation

The assessment validated whether academic, administrative, wireless, and guest network segments were appropriately isolated from one another, confirming that a compromise in one segment could not easily extend into sensitive administrative or research systems.

Manual Validation and Exploitation Testing

Every finding identified through automated discovery was manually validated by experienced consultants, with proof-of-concept testing performed in a controlled manner to confirm real-world exploitability without disrupting campus operations.

Reporting and Remediation Guidance

Woollemia Infosec delivered a comprehensive technical report together with an executive summary, providing business impact analysis, risk prioritization, and practical remediation guidance for the institution's IT and security teams.

Business Value Delivered

The Network Security Assessment gave the institution comprehensive visibility into the security posture of its campus-wide infrastructure, highlighting real attack paths rather than a simple list of theoretical vulnerabilities.

The engagement strengthened confidence in the institution's ability to protect student and staff data, maintain uninterrupted academic operations, and support the continued growth of connected campus services.

By identifying and prioritizing remediation of network segmentation gaps, wireless weaknesses, and configuration issues, the client significantly reduced its exposure to both external attackers and threats originating from within the campus network.

Why Woollemia Infosec

Woollemia Infosec delivers comprehensive network security assessments designed to uncover real-world attack paths across complex, distributed environments.

Our consultants combine deep expertise in network penetration testing, wireless security, Active Directory hardening, and infrastructure security to help organizations understand and reduce their true security exposure, always within a clearly authorized and agreed scope.

Conclusion

This representative engagement demonstrates Woollemia Infosec's ability to perform comprehensive Network Security Assessments for large, distributed campus environments.

By evaluating perimeter defenses, internal segmentation, wireless infrastructure, identity services, and device configurations, we helped the client establish a stronger security foundation to protect its academic community and critical operations.