novacoast

SECURITY ASSESSMENT

Case study: **External infrastructure**

Industry	Business	Company size	Reason for assessment
Insurance	**Insurance Brokerage**	**10,000+**	**Regulation required compliance testing**

Situation: An employee's credentials are leaked

Passwords are intended to protect networks—but used incorrectly, they can become a ready key for bad actors. It's not uncommon for employees to use the same password across third-party sites and workplace access points, making the organization vulnerable to credential stuffing attacks. With this approach, an attacker uses leaked account credentials to access an organization's appliances, email, or VPN—often gaining access to the entire network.

Read how one insurance firm partnered with Novacoast in penetration testing, revealing a previously unknown security risk due to numerous leaked employee credentials.

Novacoast assessment: External infrastructure

As part of a routine Novacoast security assessment, the team performed a penetration test. The full-spectrum test allowed the team to gain clarity on the environment and situation as they cataloged every potential point of entry for the firm, including Open Source Intelligence (OSINT) reconnaissance.

Solution: Gained access to internal network with leaked credentials

In their assessment, the Novacoast team identified a set of employee email credentials that had been leaked on the Darknet—the result of a third-party breach. Using one of these credentials, the team accessed the employee's desktop via an external Citrix appliance. With a foothold in the internal organization network, they proceeded to hunt for additional vulnerabilities, ultimately gaining domain administrator privileges.

Outcome: Short-term remediation, long-term security strategy

Previous pentesting companies had deemed this insurance firm secure, where Novacoast was able to penetrate their internal network and gain access to sensitive information. The final Novacoast security assessment documented the firm's weak entry points, outlined a plan of action to address immediate network vulnerabilities, and provided a long-term strategy to improve the firm's overall security posture.

Ask yourself—are your systems reliably secure?

- ✓ Are there strong password policies in place?
- ✓ Are your employees' credentials securely managed?
- ✓ Do you have 24/7/365 access and behavior monitoring?
- ✓ Is MFA enabled on all critical services?