HORIZON3

How Virginia Tech Connected External Pentesting to Its Engineering Workflow

How can a ‘federated’ university serving more than 38,000 students with hundreds of independent departments manage security across a vast, complex attack surface? Virginia Tech solved this by using the Horizon3 NodeZero® GraphQL API to automate external pentests in GitLab and route findings into ServiceNow, giving security teams a repeatable path from attack validation to remediation.

CASE STUDY

Customer *snapshot*

CUSTOMER

Virginia Tech

INDUSTRY

Higher education, public research university

ENVIRONMENT

Large, multi-site environment spanning a 2,600-acre main campus with 213 buildings, plus academic and research operations across Virginia and the Washington, D.C., area

CHAMPION

Brad Tilley, Director, Security Architecture & Red Team

SOLUTION

Horizon3 NodeZero, GraphQL API, automated external pentest pipeline in GitLab, ServiceNow ticket routing

CHALLENGE

At Virginia Tech, security leadership must coordinate testing and remediation across a complex, distributed academic and research environment. Brad Tilley, the university's Director of Security Architecture & Red Team, describes it as "an organization of hundreds of organizations," with operations spanning Blacksburg, other parts of Virginia, and the Washington, D.C., area. Its systems are hosted across major cloud providers and local infrastructure, with public-facing assets distributed around the world. The security team also had a limited pentest staff and could not simply add headcount. That combination created a federated operating model, with technical responsibility spread across teams and subnet owners.

For the security organization, validating exposure across that environment required more than generating findings. Results had to reach the people responsible for the underlying systems, fit the university's established processes, and support follow-through after a test was complete. A highly segmented internal network also limited some testing paths, while password-audit work had paused as priorities shifted. The team needed a practical way to make external validation repeatable and connect discovery with remediation.

WHY NOW

From Testing Activity to Engineering Workflow

The first shift came when the team began treating NodeZero as an engineering component that could be integrated into its existing workflow. Brad Tilley built directly on Horizon3's GraphQL API and created an automated external pentest pipeline in GitLab. That moved testing from a separate security activity into a repeatable process the team could run through tools it already used.

Connecting Findings to Remediation

A second shift followed when the team connected those runs to ServiceNow. The need for that connection was explicit. As Brad explained, "We have to do these tests on a schedule automatically and then incorporate those into our ServiceNow instance." Findings could move into the university's established system for assignment and remediation tracking, giving subnet owners actionable results in a workflow they recognized. The security team gained a clearer path from discovery to follow-up, while technical owners could work from the same system they used for other operational responsibilities.

The value came from how the pieces worked together. GitLab handled orchestration, ServiceNow handled assignment and tracking, and NodeZero supplied the attack validation layer between them. For a federated institution, that connection reduced process friction and made it easier to treat testing and remediation as one continuous security practice.

WHY HORIZON3

Extensibility Without Process Friction

Virginia Tech needed a platform that could fit into its engineering workflow rather than create another disconnected process. NodeZero's GraphQL API gave the team the flexibility to build around GitLab and ServiceNow, while preserving the attack validation needed to understand real-world exposure.

A Reusable Security Workflow

That extensibility also aligned with an existing internal pattern. Virginia Tech has historically written software to drive vendor tools, collect reports, map systems to responsible owners, and open ServiceNow incidents. Instead of manually coordinating each external test and then translating findings into a separate tracking process, the team could automate the run and route the output into the system where remediation already happened. In a decentralized environment, that operational fit matters. A security platform has to make findings understandable, portable, and actionable for the owners who can address them.

VERIFIABLE RESULTS

A More Connected Operating Model

Virginia Tech's external testing program now has a more connected operating model:

- Automated execution: External pentesting is part of a GitLab workflow rather than an isolated testing activity.
- Direct remediation routing: Findings flow into ServiceNow for assignment and follow-up by subnet owners.
- Repeatable security operations: The university has a reusable process that connects attack validation, ownership, and remediation tracking.

The most important change is structural. Testing no longer ends when a report is produced. The workflow carries findings into the university's existing remediation process, helping the security organization maintain clearer accountability across a distributed environment.

LOOKING AHEAD

Virginia Tech's next opportunity is to deepen the connection between automated testing, remediation tracking, and broader coverage across its decentralized environment. The foundation is already in place: NodeZero validates exposure, GitLab orchestrates the work, and ServiceNow gives owners a clear path to act. Each automated run can now strengthen the university's ability to identify the next attack path and address it through a process built for repeatability. The team is now looking to expand this automated pipeline to cover internal assets and research-specific subnet environments.