Research University

GUIDEPOINT® SECURITY

Company **Overview**

Founded in 1902, this research institution is centered in Washington, DC., and comprises eight schools and colleges with diverse disciplines, each of which rank within the top twenty in several categories nationally. They pride themselves on having a reputation for creating meaningful change in the world. It follows necessarily as part of their mission that the university must maintain a secure, compliant IT environment to protect its data and ensure uninterrupted operation.

Cybersecurity Team and Environment

Cybersecurity **Challenges**

The university's foremost challenge is maintaining an up-to-date security posture against evolving threats. They have been addressing this through annual external security evaluations, including penetration testing and red teaming. To ensure a fresh perspective each year, they retain a different security company to help them perform these evaluations.

Each year for the past 10 years, the university has performed a thorough security evaluation of their environment, technology, personnel, and processes. Typically that approach emphasizes penetration testing, but over time it has grown to include red teaming. This includes not just scanning from the outside, but working within the university's network to determine what a malicious attacker might be able to leverage.

They reached out in 2023 after hearing a George Washington University official speak highly of their experience with GuidePoint Security. But it was the red team exercise that was the deciding factor. The ability to problem solve in a theoretical exercise using the same toolkits as malicious actors promised to be an excellent means of exposing weaknesses so that they could take immediate action to close those gaps.

One of the particular areas of concentration was on the university's wireless access points. Previously, the organization had two types of internal access points: one for more secure practices, and one that was more open (or the "free love Starbucks coffee" type as they call it) which they had outsourced. The organization asked GuidePoint Security to "red team" or emulate a malicious actor: put up an access point with an identical name to masquerade as legitimate. GuidePoint determined that they could, but the real issue was in the notification that such a transgression had occurred.

As a result, wireless access point security became one of the number one areas of concentration that they asked for in their 2024 security review.