Case Study

University Services Provider Achieves Full Visibility of Its External Attack Surface

THE CHALLENGE

Grand Canyon Education (GCE) is a shared services provider that serves colleges and universities. The company employs thousands of people with revenues near $1 Billion. GCE's high visibility as a cyber and technology education leader and its relationships with respected affiliations were key drivers behind its focus to stay ahead of a rapidly evolving threat landscape. The security team's primary goals were to reduce the attack surface of the organization, elevate the efficacy of security controls, and improve and contextualize response efforts.

To achieve these goals, GCE knew it needed expanded visibility and dynamic discovery of its assets since growth by any method—organic or via acquisition—can lead to the accumulation of information systems that did not evolve through the normal established process. Finding new and acquired assets was not enough; what was needed was continuous attack surface mapping and vulnerability analysis.

The GCE team understood how legacy applications and infrastructures created a significant attack surface that malicious actors may attempt to exploit. Time is always a factor in preventing cyberattacks that may disrupt business operations and services. Recent attacks utilizing Ransomware as a Service or Affiliate models are cascading into the domain of conventional cybercrime via highly optimized distribution and information sharing models.

With a dynamic and rapidly unfolding threat landscape, the GCE team sought a solution that would automate preventative activities, while providing complete visibility over the full external attack surface. The team needed a solution that was simple, intuitive and easy to leverage across the entire enterprise.

Challenge

- Prevent operational disruptions due to cyberattacks for a shared services provider to the education market

Solution

- Achieve complete visibility of the external attack surface, including IT assets inherited through acquisitions

Outcomes

- Reduced overhead/overtime through automated discovery and mapping of IT resources
- Prevented operational disruptions, data loss, and ransomware attacks through proactive identification, mitigation, and remediation of vulnerabilities

"Cyberpion provides us the strategic advantage of seeing our external attack surface, dynamically, in the same way attackers see it."

Mike Manrod, CISO - Grand Canyon Education

THE SOLUTION

While investigating solutions to support this initiative, GCE identified Cyberpion's Ecosystem Security platform as a strong candidate. Exploring Cyberpion's capabilities included a full Proof-of-Concept (PoC) product demonstration. Cyberpion's solution is delivered as a web-based SaaS portal and requires no installation, configuration, or modification to GCE's existing IT. Because of the speed at which the PoC was deployed, GCE gained immediate actionable insights into its attack surface.

Grand Canyon Education understood that an intractable problem for many cyber security teams with limited resources is figuring out the organization's complete external web footprint, including shadow IT and unauthorized projects.

During the PoC and product deployment, Cyberpion provided immediate value in terms of asset discovery. In particular, GCE had recently acquired a number of third-party resources and Cyberpion was able to discover and assess these resources automatically.

THE OUTCOME

Mike Manrod, GCE's Chief Information Security Officer, saw the value in reducing the overall external attack surface for the organization. By uncovering unknown assets and vulnerabilities, GCE's vulnerability management and penetration testing teams were able to begin achieving Mike's goal of finding and resolving critical security flaws.

The increased visibility provided by Cyberpion's platform has allowed GCE's cyber security team to continue to pre-emptively discover and act on vulnerabilities. By acting before hackers are able to exploit these vulnerabilities, GCE continues to prevent significant damage in terms of dollars, brand reputation, operational disruptions or Ransomware attacks. GCE's high profile continues to make it a target of attempted cyberattacks. However, by reducing the number and criticality of attack vectors, GCE is able to stay one step ahead.

"Cyberpion was an absolutely amazing discovery—the platform helped us to find applications, infrastructure and the associated vulnerabilities we needed to catapult our vulnerability management program ahead of the leading edge of corporate growth. We have since protected many information assets, informed by the reporting from the Cyberpion dashboard."

— Cameron Kownack,
Incident Response Analyst
Grand Canyon Education

Cyberpion™

US: 971.702.3850
Intl: +972 33752005
sales@cyberpion.com

Learn more online
cyberpion.com

Cyberpion, the Ecosystem Security™ company, is a pioneer in the new ecosystem cybersecurity paradigm, defending the new and vast attack surface created by online ecosystems. Cyberpion enables organizations to see and manage their online ecosystem and protect them from vulnerabilities as it continues to expand. The Cyberpion platform systematically tracks, analyzes and maintains the vast inventory of known and unknown assets and their connections throughout an organization's far-reaching ecosystem, to continuously identify and neutralize vulnerabilities before attackers can exploit them. To learn more, visit cyberpion.com. © 2021 Cyberpion, Inc. All rights reserved. Cyberpion, Ecosystem Security, and Connect with Confidence are trademarks of Cyberpion, Inc. Information subject to change without notice.