Signal Sciences

Cybrary: Real-Time Visibility and Modernization

CHALLENGE

Cybrary faced a variety of attacks across its APIs and web properties, but its legacy web application firewall (WAF) was failing to deliver usability and complete attack coverage.

Cybrary is an online training and career development platform preparing the next generation of IT and cybersecurity professionals. With a wide range of pages and training content to protect, Cybrary's two-person infrastructure team was tackling issues their legacy WAF could not address. "The model of blocking based on pattern matching such as a specific SQL-injection string won't work for us in the future. Signal Sciences provides more context and visibility at the app layer and makes more precise blocking decisions to stop bad web requests."

Cybrary's legacy WAF proved extremely difficult for the team to configure and debug issues without investing significant time and resources. It also provided incomplete attack coverage and blocked valid requests, with no real-time visibility, alerting, or a functional dashboard to monitor activity over time. And as security experts, Cybrary needed to maintain their brand identity and ensure their security practice was cutting-edge.

> "Working with Signal Sciences has been an excellent experience. Their openness and no-nonsense approach to solving our problems are refreshing compared to other vendors"
>
> **Mike Gruen,** VP Engineering / CISO

SOLUTION

Cybrary was searching for a modern, feature-rich WAF solution that can be easily configured, block attacks, natively work within Kubernetes containers, and provide real-time alerting without incurring heavy maintenance investment.

Cybrary chose to replace their legacy WAF with Signal Sciences after a successful two-week pilot where they evaluated the ease of use, performance, and availability of features required by the infrastructure team, including Slack integration, unified dashboard, all working seamlessly with Kubernetes.

After a five-minute installation, Signal Sciences provided immediate time to value during the pilot. "We deployed Signal Sciences behind our current WAF, and over one weekend we saw it block attacks our WAF was missing," said Jonathan Meyers, Principal Infrastructure Engineer. "The dashboards allowed us to easily see and track malicious activity in a way we couldn't with our old WAF."

Complete Protection Against OWASP Top 10

Even after extensive tuning and configuration, Cybrary's legacy WAF was still allowing attacks and web requests from bad IPs through. But Signal Sciences blocks attacks that Cybrary's legacy WAF missed and provides the security team with comprehensive protection capabilities. Using Power Rules, users can quickly define, monitor, and take action on any web application or API transaction without extensive tuning. Additionally, Cybrary can protect their WordPress site without using any additional plugins.

Maximize IT Staff Time and Resources

With a lean, two-person staff running infrastructure and security, the Cybrary team could not afford to spend time and deprioritize tasks navigating their legacy WAF's complicated interface. Signal Sciences focus on user experience empowers Cybrary to easily obtain the information they need without hiring an additional dedicated security employee.

Complete Visibility and Insight

Cybrary's legacy WAF was operating as a black box so the team could not easily see or evaluate malicious behavior. Even simple functions, such as searching through logs, were long and non-intuitive to complete. Signal Sciences provides Cybrary's team with a comprehensive dashboard and powerful search and alerting tools, significantly increasing visibility and insight into attacks. And with real-time alerts integration with Slack, the Cybrary team can now extend that visibility and oversight to their wider engineering team.

CYBRARY

> "Signal Sciences low-maintenance approach does its job very effectively and alerts us when something needs to be addressed."
>
> **Jonathan Meyers,** Principal Infrastructure Engineer