Ball State University Partnering to Provide 24/7/365 MDR Protection

PONDURANCE

CASE STUDY

Ball State University is home to more than 22,000 students, approximately 3,000 full-time faculty and staff and seven academic colleges. Protecting all of the people and assets that make BSU special is a big job. From a cybersecurity standpoint, all colleges and universities have a lot to protect: from the personally identifiable information (PII) of its students, faculty and staff, to unique teaching curricula, to intellectual property generated through research and more. Like their counterparts at other higher ed institutions, the team protecting BSU's digital infrastructure must constantly be concerned about ransomware, stolen credentials and phishing attacks, as well as other potential threats that could compromise the university and even the safety of its people.

BALL STATE UNIVERSITY

THE CHALLENGE: THE NEED FOR 24/7/365 THREAT DETECTION AND RESPONSE

Like so many higher ed institutions, Ball State has a relatively small but mighty cybersecurity team. Part of a centralized IT organization providing services for the whole university, the security team runs an internal security operations center (SOC), but staffing limitations mean they can only run it during business hours. Understanding that around-the-clock monitoring and response is essential for protecting the university from cyberattack, the BSU team brought in Pondurance to provide managed detection and response (MDR) services and extend those SOC working hours to 24/7/365.

Even before engaging Pondurance for MDR services, the BSU team hired Pondurance to supplement their vulnerability assessment capabilities with additional penetration and Red Team testing services.

THE SOLUTION: AN EVOLUTION FROM PENETRATION TESTING TO MDR SERVICES

"We started with one service, then progressed to two and then three and we keep expanding. It is important to feel like this relationship is an extension of our internal team," said Tobey Coffmann, Director of Information Security Services at BSU.

Following the successful collaboration around pen testing, the BSU team engaged Pondurance for threat hunting and response help, even before Pondurance formalized these capabilities (and more) into what are now the company's full MDR offering. "Having another set of eyes on our network traffic and data is critical," said Coffmann. "We're able to locate and mitigate issues that we wouldn't have found on our own."

> "We truly have middle-of-the-night visibility and the peace of mind that comes from knowing that someone is still looking at our data even after our analysts have gone home at the end of the day. Let's face it: Bad guys don't care about business hours. If something happens at 2:00 am, it's important to have the confidence that our vendor enables us to get on it right away."
>
> ***Tobey Coffmann,***
> ***Director of Information Security Services, Ball State University***

Ball State University Partnering to Provide 24/7/365 MDR Protection

PONDURANCE

CASE STUDY

Most recently, the BSU infosec team added log monitoring and SentinelOne for endpoint detection and response (EDR) to the services being provided by Pondurance. Coffmann added, "We truly have middle-of-the-night visibility and the peace of mind that comes from knowing that someone is still looking at our data even after our analysts have gone home at the end of the day. Let's face it: Bad guys don't care about business hours. If something happens at 2:00 am, it's important to have the confidence that our vendor enables us to get on it right away."

THE RESULTS: A PARTNERSHIP BASED ON COMMUNICATION AND COLLABORATION

Starting with penetration testing services in 2014, the teams have worked together to expand the University's SOC capabilities and ensure that BSU benefits from the 24/7/365 protection that Pondurance MDR services provide.

The greater diversity of threat intelligence that the Pondurance SOC team monitors also means that potential threats are found and can be responded to more quickly.

THE CHALLENGE	• Need to supplement in-house vulnerability assessment capabilities with additional penetration testing and Red Team services • Limited staff unable to provide 24/7/365 SOC coverage
THE SOLUTION	• Pondurance Managed Detection and Response Services, including log, network and fully-managed SentinelOne for endpoint monitoring • Pondurance Penetration and Red Team Testing Services • Pondurance Digital Forensics and Incident Response Services
THE RESULTS	• 24/7/365 SOC coverage and "the peace of mind that comes from knowing that someone is still looking at our data even after our analysts have gone home at the end of the day."

BSU QUICK PROFILE

- Founded: 1918
- Location: Muncie, Indiana
- Total enrollment: >22,000
- ~3,000 faculty and staff
- ~120 undergraduate majors
- >100 master's, doctoral, certificate and specialist degrees
- Rated "one of the best universities in the Midwest for 2022" by the Princeton Review; consistently earns high ratings as a top university in the U.S. and internationally.

ABOUT PONDURANCE

Pondurance delivers world-class managed detection and response services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals and compliance and security strategists who provide always-on services to clients seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

For more information, call 1-888-385-1702 or email us at info@pondurance.com.

pondurance.com