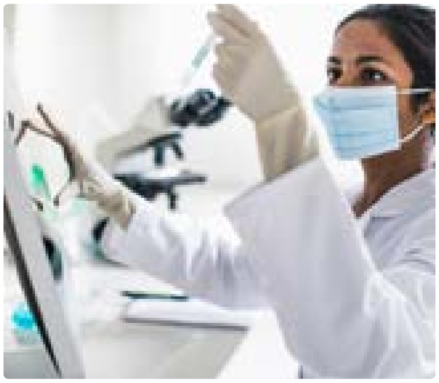
MANDIANT
NOW PART OF Google Cloud

MANAGED SERVICES
CUSTOMER STORY

Mandiant Managed Defense at Penn State Health

Industry
Healthcare



Mandiant Managed Defense fills a critical role for us by extending our existing incident response capabilities.

— Matthew Snyder, Senior Vice President, Chief Information Security and Privacy Officer, Penn State Health

Balancing cyber security costs and risks is a critical priority for healthcare providers like Penn State Health. Cyber attacks potentially disrupt the provider's operations, place unneeded strain on clinicians, staff and patients, or cause sensitive data to be stolen or lost.

Penn State Health has therefore invested significantly in growing its cyber security capabilities. It first established a security operations center (SOC) and implemented a suite of security tools. As the threat landscape evolved and Penn State Health grew, it increased its security funding; its SOC staff has increased in recent years as the provider added more security talent to the team.

While this investment in cyber security is mission-critical, Penn State Health has other fiscal priorities. Its reputation as an industry leader is based in part on its commitment to cutting-edge, capital-intensive healthcare technology, research, clinical facilities and patient-centered services.

The provider therefore welcomes opportunities to achieve its cyber security objectives in a cost-effective way, which is why Mandiant Managed Defense is a critical component of its cyber security program. This service has Mandiant experts extending the internal SOC's capabilities by providing continuous 24x7 Level 2 defensive cyber operation services which counter attacker-behind-keyboard activities during off-hours. It also augments the in-house team with detection and response experts 24x7. This ensures Penn State Health's systems are constantly guarded by hands-on security experts at a lower cost than what it would be to fully staff its SOC.

Read the full case study **here**.

Google Cloud

For more information visit cloud.google.com