Trusted CI Success Story
Gemini Observatory

Trusted CI creates roadmap to ensure data integrity for Gemini Observatory

The Gemini Observatory IT staff members weren't going to take any chances. After thwarting minor intrusion attempts into their infrastructure in 2015, they decided to contact Trusted CI to make sure they had robust systems in place to protect the research mission.

With two large ground-based optical/infrared telescopes located high in the mountains near Vicuña, Chile, and Hilo, Hawai'i, the Gemini Observatory probes the universe from the southern and northern hemisphere. The duo telescopes provide astronomical research for six participant countries, Chile, Brazil, Argentina, South Korea, Canada, and the U.S. In addition to financial support, each country also contributes significant scientific and technical resources.

The National Science Foundation (NSF) funds the U.S. portion of the Gemini Observatory, now part of the National Optical Infrared Astronomy Research Laboratory (NOIRLab). The NSF also funds Trusted CI, the NSF Cybersecurity Center of Excellence.

The IT team at the Gemini Observatory has a far-reaching mission. "We protect physical access to the telescope domes and their controls along with the IT systems and infrastructure that guarantee the astronomical data is secure and available to researchers. We also ensure we meet the IT standards required by the host countries, the U.S. and Chile, and we handle technical support and cyber training for observatory end users," explained Chris Morrison, head of IT operations for NOIRLab.

Laser and star trails over Gemini North, located in Hawaii.

One of the biggest hurdles to IT security, said Morrison, is the remote location of the telescopes. "Building infrastructure and getting data to and from the telescopes is complicated along with making sure we provide system redundancy," said Morrison. "We want to make sure that the data coming from the telescope is what the astronomer is receiving, that nothing is affecting the telescopes or control systems. Integrity is vital. Our data must be confidential, reliable, and available."

Annual attendance at the NSF Cybersecurity Summit prompted the observatory to work with Trusted CI on engagements in 2015 and 2016. "We got exactly what we needed, a wonderful roadmap for how to proceed with policies, control systems, network redundancy, data backups, and cybersecurity training," explained Morrison.

Since there were not enough staff members to execute all of the recommendations at the same time, Morrison's team created a weighted scorecard and drew a water line. Everything under the water line was already in progress or didn't need to happen right away. The water line still guides the IT team as they decide what to implement next.

Since the engagement, Morrison's team trains staff and end users that cybersecurity is everyone's responsibility. IT experts host cybersecurity brown bag sessions and conduct phishing tests. Those that don't pass get additional training. With so many working from home during COVID-19, observatory users are much more aware of security threats.

"We make sure our systems are available independent of events," Morrison added. "Trusted CI is a big part of how we do things now. I couldn't be happier with the support we got from Trusted CI."