LSUA

At a Glance

- Ransomware a key security concern
- Darktrace AI responds to emerging attacks around the clock
- Malicious crypto-mining campaign uncovered

Louisiana State University of Alexandria (LSUA) is a publicly supported institution that provides undergraduate level college education to the citizens of Central Louisiana.

The Cyber Security Threat to Education

Educational organizations make favorable targets for threat actors hoping to exploit their device-laden networks and masses of sensitive data, while the size of the student body increases the chance of network users inadvertently opening up vulnerabilities.

“Security concerns in higher education are widespread. We had daily concerns about email phishing, student data privacy, and malware,” said Richard Robinson, Network Administrator at LSUA.

The greatest of these concerns was ransomware, which has increasingly targeted educational institutions in recent years. The impact of a successful attack – from the potential ransom payment itself to the disruption caused by network shutdowns – could be devastating.

The security team had already taken measures to mitigate this threat, including security awareness training for both staff and students, creating and storing backups, and implementing strong password requirements. But they recognized that there is no silver bullet to stopping ransomware attacks, and that another layer of defense was needed.

> “We had daily concerns about email phishing, student data privacy, and malware.”
>
> Richard Robinson, Network Administrator, LSUA

LSUA

Autonomous Response Elevates a Small Team

The LSUA security team had limited capability for defending against ransomware without Darktrace. With only three IT professionals working on the organization’s security, a targeted, out of hours attack could have caused serious damage before a response could be organized.

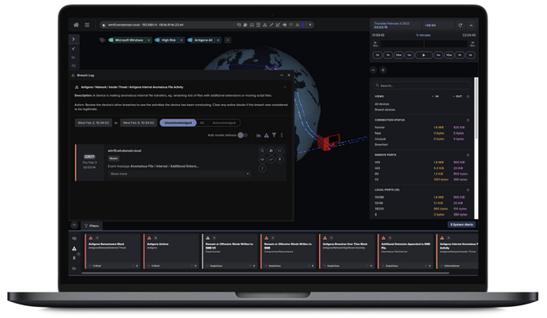
Autonomous Response now defends LSUA from ransomware 24/7, responding to the early signs of an attack, regardless of the malware used or the method of delivery. It constantly revises its understanding of ‘normal’ for the digital estate, and therefore does not require updates or substantial maintenance from Robinson and his colleague. Any action taken by the AI is calculated to avoid disrupting the university’s normal operations. Robinson, as well as all of campus, can therefore continue working uninterrupted as potentially fatal attacks are neutralized.

Revealing Malicious Activity with AI

In addition to responding to serious emerging threats, Darktrace brings a new layer of visibility across the digital estate. Robinson now has oversight across suspicious external connections which had previously passed by unnoticed, and has even caught students exploiting the university network to conduct crypto-mining.

With a new level of oversight across the digital estate, and Darktrace AI autonomously finding and prioritizing serious incidents for review, the security team are able to spend their time being proactive rather than reactive, and help the university operate productively without risk.

“Darktrace has given us a new level of visibility into our own network which we never had before,” explained Robinson. “And we feel safer knowing that the AI technology is monitoring and responding to all of these findings even when our team is unavailable.”



Darktrace’s findings and autonomous actions are shown in the Threat Visualizer

> “We feel safer knowing that Autonomous Response is monitoring and responding to all of these findings even when our team is unavailable.”
>
> Richard Robinson, Network Administrator, LSUA