City of College Station Utilities

City of College Station is at the heart of the Texas triangle and is the home of Texas A&M University. With its designation as a Land, Sea, and Space Grant institution, the university brings in a broad range of projects to the city that are funded by NASA, the NIH, the National Science Foundation, and the Office of Naval Research.

College Station Utilities
Reliable, Affordable, Community Owned

At a Glance

- Organization oversees critical infrastructure

- Industrial systems undergoing digital transformation

- Lean security team faced with noisy environment

"Darktrace helps us to have a complete picture into what is going on."

**Lead SCADA Analyst,
City of College Station Utilities**

Increasing Visibility into Critical Infrastructure

As a municipality overseeing critical infrastructure, City of College Station Utilities must maintain the availability and integrity of their utilities systems. Further, the city relies on a robust system to allow for remote operation and control of electrical system assets, and so their major security concerns include unauthorized network access and software use.

The city's largest security challenges were in local visibility in substation networks. Any traffic that crossed substation boundaries was typically visible, but internal traffic was not. Darktrace allows them to have visibility into the traffic in these remote locations and allows them to characterize the network traffic. For this use case, they had no prior capability and relied only on firewall tools for cross-substation or control center traffic.

After deploying the Industrial Immune System, City of College Station Utilities now has full visibility throughout their sensitive environments, granting peace of mind that their vital systems are secure. "Darktrace helps us to have a complete picture into what is going on," affirms Robert White, Lead SCADA Analyst at City of College Station Utilities. "It lets us know if a problem is brewing, which helps us to manage the risks and our overall security posture."

'Plug and Play' Deployment in Air Gapped Environment

With an air gapped environment, City of College Station Utilities chose a hybrid deployment of Darktrace. Self-Learning AI technology was installed on premise in their primary Control Center and OS based sensors also sent traffic from a network outside of the Control Center. With traffic sampled from an ICS control server and a domain controller, Darktrace characterized the only types of traffic that are supposed to be on the network.

"Even in our isolated environment, the Darktrace deployment was a snap," notes White. "The Darktrace system has greatly improved the visibility of traffic within our substations and within the local control centers."

Enabling Expansion and Transformation of Infrastructure

City of College Station Utilities' next major project is related to the expansion of their footprint to include two new substations and rebuilding existing older substations up to their new standards. Part of this is replacing non-connected equipment with centrally managed systems, which means also increasing their vulnerability footprint.

"The most secure network is no network at all," says White, "so whenever we get away from that, measurement, monitoring and securing actions are all needed to manage the security, and Darktrace helps provide that for us."

"Darktrace has helped us to keep our networks and devices honest about what they should be doing."

Lead SCADA Analyst, City of College Station Utilities

ROI: Unprecedented Visibility and Augmenting Human Teams

"Darktrace has given us a window into the activity on our network that no one really had before," notes White. Previously, the city knew generally when something would work or not, but now they have the on-site tools and capabilities to deep dive into what traffic is really on their network, and also what should not be happening.

Given the small size of the city's organization, they are leaning heavily on the Darktrace system and its model of their traffic to identify the problems and filter the noise. This allows the team to focus its limited personnel resources toward the issues that are most likely to be a problem.

In this way, Darktrace has freed up the city's limited personnel resources to focus on the actual high likelihood security events rather than investigating every incident of chatter, which is most often a misconfigured field device or an update to a new application. "With the Darktrace models, we can dedicate more resources to the incidents that are flagged," White confirms, "knowing that Darktrace is helping to separate the wheat from the chaff."

"With Darktrace, a full day task involving at least two employees previously is now about 30 minutes of work from a central location."

Lead SCADA Analyst, City of College Station Utilities

Darktrace's Industrial Immune System illuminates the entire cyber ecosystem.

For More Information

- Book a free trial
- Read: Defending OT Environments from Ransomware
- Visit our YouTube channel