tylertech.com
P 800.772.2260
E info@tylertech.com

Case Study

Lowndes County

GEORGIA

Tyler Detect deployed to detect network threats

24 / 7

Malicious behavior found and corrected **immediately** following deployment

Visibility into all network activity is increasing awareness and driving risk mitigation solutions

Network Insight Delivers Peace of Mind

Tyler Detect has an immediate impact on Lowndes County's cybersecurity program.

Advanced cyber threat detection cannot happen by algorithm alone. Cybercriminals can evade traditional defenses compromising an infrastructure within minutes or hours. Study after study shows it can take organizations weeks, even months or years, to uncover an intruder.

Aaron Kostyu, director of technology for Lowndes County, Georgia, knew they needed better insight into what was happening on their network to defend against the growing number of cyberattacks threatening the public sector. But, like most entities, the county, which has a population of 115,000, didn't have extra technical resources on staff, much less a dedicated security expert to manage these tasks.

"Knowing that I have security experts monitoring my traffic 24/7 for any deviant behavior is an added bonus that gives me and the county's management team peace of mind."

— **Aaron Kostyu**
Director of Technology
Lowndes County, Georgia

TD-LCGA-CS-12929-1119

"Beyond knowing that Tyler Detect will now alert me of nefarious behavior and allow us to mitigate risks, the biggest benefit of the service is that we now have insight into all network traffic."

— **Aaron Kostyu**
Director of Technology
Lowndes County, Georgia

The Search

There are myriad options out there. According to Kostyu, they considered a SIEM, but it would have been too costly. Plus, a staff member would need to take on the event coordination and analysis, which is a time-consuming endeavor. That wasn't a viable option for the county.

Then they explored several managed threat detection services. Tyler Detect, from Tyler Technologies, quickly rose to the top of the list because its methodology includes analysis by security experts.

"We feel strongly that it takes human eyes and logic to be able to quickly and efficiently spot suspicious activity and defend against today's hacker activity that is constantly evolving to infiltrate systems," said Kostyu. "Tyler Detect was also a fraction of the cost of other solutions and, because of this, the county was able to roll it into their current budget to get immediate coverage."

The Find

On the day Tyler Detect was deployed, we uncovered a persistence mechanism within a scheduled task that looked suspicious. Upon further review by the Detect analyst, the activity was confirmed to be a type of malicious Trojan. Trojans act as a backdoor, often connecting to a command and control (C2) server that gives an attacker unauthorized access to the compromised computer.

The analyst immediately alerted the county's team and they removed the infected end user machine from their network. Upon investigation, the Trojan had been on the device since 2014, and the county's previous solution for monitoring end-user traffic had never alerted them to it.

"This really speaks to the thoroughness and effective methodology of the Tyler Detect service," Kostyu noted.

Added Benefits

"Beyond knowing that Tyler Detect will now alert me of nefarious behavior and allow us to mitigate risks, the biggest benefit of the service is that we now have insight into all network traffic," Kostyu went on to say. "This wasn't possible before."

The county runs many applications developed by third parties, and before implementing the Tyler Detect service, they had limited knowledge of the type of traffic being created on their network. The daily Tyler Detect reports have opened their eyes to all this communication and activity, allowing them to learn what normal behavior is. According to Kostyu, "Awareness of my network has increased 80% with Tyler Detect. Small things that are reported through Detect are making big differences in our actions.

"There is absolutely no way for a CIO or technology director to be aware of what is going on in their environment without a tool like Tyler Detect. Knowing that I have security experts monitoring my traffic 24/7 for any deviant behavior is an added bonus that gives me and the county's management team peace of mind."

CONTACT US

Phone
800.772.2260

Email
CybersecuritySales@tylertech.com

Website
tylertech.com/tylerdetect