CASE STUDY

Secureworks®

SECUREWORKS TEAMS UP WITH CITY OF AMARILLO TO PREVENT COSTLY DATA BREACHES

Why the largest city in the Texas Panhandle chose Secureworks Incident Response to help defeat threats

CHALLENGE

Security was a hot topic to leaders and administrators in the City of Amarillo, Texas. A massive and devastating ransomware attack had recently struck a neighboring county, and as a result, the city of Amarillo was upgrading its IT infrastructure with cybersecurity as a primary focus.

City of Amarillo Chief Information Officer Rich Gagnon and his team had completed segmentation and were in the process of rolling out Zero Trust when they discovered the Log4J vulnerability on the city's Horizon servers prior to a patch release that was meant to address the vulnerability. The city's team drew upon their incident response documentation and reacted quickly to the vulnerability when they spotted lateral movement. Acting swiftly, they prevented the potential breach by evicting the threat actor. Fortunately, the city did not suffer any loss of data.

CITY OF AMARILLO®
OPEN SPACES ★ ENDLESS OPPORTUNITIES

Name: City of Amarillo
Industry: Local Government
Country: United States
Employees: 2,400

CHALLENGES:

- The city's internal team experienced an attempted security breach
- Security upgrades were in progress when attempted breach was detected
- City's internal security team was strong, but needed additional training

SOLUTION:

Secureworks® Emergency Incident Response provides organizations with:

- 24/7 Incident Response Hotline, with thorough scoping by IR experts and immediate deployment of resources
- Rapid, complete investigation, analysis, and remediation of cyberattacks
- Vital incident command, specialized technical expertise, and remediation guidance
- Tangible benefit of real-world training with seasoned threat experts and researchers
- Direct collaboration with internal teams to strengthen future IR capabilities

BENEFITS:

- City gained third party validation and experience working with IR experts
- City reduced cyber risk and created long-term knowledge sharing, based on insights and best practices from thousands of IR engagements
- Customer enabled rapid remediation while expediting rollout of upgrades

"We went into incident response mode immediately when we saw the indications that this was Log4J," Gagnon said. "We turned off access, put out an emergency notice, and shut down internet access. We needed to see how bad this was."

Gagnon had been in conversation with Secureworks to learn about available security solutions and saw an opportunity to tap into the company's vast expertise in incident response, while providing his team with valuable, real-world training.

"I wanted to have assistance as we went through the incident," Gagnon said. "Speed was important, and it also was a great chance for a young team to watch an experienced team of security experts go through incident response. We could not get this wrong. This had to be done right."

SOLUTION

Secureworks Emergency Incident Response provides cross-functional expertise for full-scale, rapid investigation, analysis, and remediation of cyberattacks. Secureworks Emergency Incident Response service is certified by the National Counterintelligence and Security Centre's (NCSC) Cyber Incident Response (CIR) scheme and the NSA's Cyber Incident Response Assistance (CIRA) program.

Secureworks Incident Response team features experienced responders with backgrounds spanning military, police, and intelligence agencies, as well as Computer Security Incident Response Teams (CSIRTs). Secureworks Incident Response team members combine hands-on understanding of advanced cybersecurity practices with front-line incident response experience, supplemented by access to the entire network of Secureworks experts and threat intelligence and security analysts to accelerate investigations and help customers recover with confidence.

Secureworks

"The city of Amarillo was fantastic to work with," Secureworks senior consultant Kevin Walsh said. "They fully embraced the team concept of the engagement from the start. They were not only incredibly dedicated, but they also were eager to learn, collaborate and work together with us from start to finish, which led to a successful engagement."

BENEFITS

One key area of emphasis for Gagnon is continuously educating his team to be ready for the next security incident. Working through a real incident is different from reviewing incident response policies. That's why Gagnon says Secureworks provided tremendous value in showing the city of Amarillo's team best practices, from investigating the incident to remediation planning and guidance.

"This is education that most of my team has gone through in more of a classroom setting," Gagnon said. "It's different in real life, and the Secureworks incident response team gave our people a lot of practical knowledge. The Secureworks team did a great job of letting my engineers see behind the curtain. They explained, 'Here is what we're searching for. We see these indicators. Here are the processes we are looking for.'"

Gagnon highlights the value of the ongoing and always-on communication with the Secureworks team throughout the engagement, as well as the expertise of the Secureworks Incident Commander. Incident Commanders are experts with decades of incident response experience who provide a combination of technical, executive communication, and relationships skills during business-critical incidents.

"Through multiple conversations every day, we knew exactly what was being investigated, what systems were suspect, and what impact it might have," Gagnon said.

While Secureworks focused on incident documentation and follow up, Gagnon's team was free to complete the city's Zero Trust rollout. The team had been about 25% of the way through that implementation when they initially discovered the Log4J vulnerability. With the assistance of the Secureworks incident response team, and the support of Secureworks professionals in areas such as Active Directory assessments, Gagnon said the city "essentially did six months of work in 10 days" by fast-tracking the Zero Trust rollout with Secureworks support.

"Knowing that we had an extra set of eyes watching to make sure we didn't miss anything, it gave us the security to get our staff out of the building, get them rested," Gagnon said. "We always had fresh eyes and rested engineers working the incident at all times. It also gave us time to focus. We knew the Secureworks team was keeping an eye on the incident side of the house, so my team could shift to completing our zero-trust roadmap. We did it a lot faster with their help."

Amarillo is the largest city in the Texas panhandle, a region where many municipalities lack a wealth of in-house security experience. Gagnon said he hopes the best practices and lessons learned from Secureworks can cascade to his surrounding communities.

"We are putting together a regional learning session with all of these smaller communities and largely due to this engagement, we've captured those best practices," Gagnon said. "We're going to share those out, share the toolsets, and go through some fundamental things that these smaller communities can go home and do today."

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist
secureworks.com

About Secureworks
Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Secureworks®