UNCOMMONX

UncommonX Helps An Electrical Provider Recover After Two Ransomware Attacks

Incident

A premier electrical and communications services provider (“Electrical Provider”) suffered from a major data security breach in 2019, resulting in a ransomware attack that encrypted all their files and systems. Their IT team was able to restore access to their systems over time, but then they were hit again in late 2020. That attack affected multiple workstations, directories, and domain controllers. At that point, the Electrical Provider realized they needed help containing and recovering from the incident.

Response

The Electrical Provider contacted us through one of our partners. They explained they needed help recovering from the ransomware. They also wanted to improve their overall security maturity to prevent future attacks, but it needed to align with regulatory requirements and guidelines. Our Security Operations Center (SOC) team used our BOSS (Business Operations Security Suite) next generation cyber threat management and intelligence platform to run an in-depth assessment. They discovered the impact was limited to the systems that were reported and the ransomware was no longer propagating in the environment.

Forensic images of the impacted systems were taken, recovery via backups was started, and they were back online quickly. We began monitoring logs, events, and suspicious traffic from all feeds remotely. In addition, we provided triage services for the alarms that come in from the customer’s systems to filter out false positive alerts, and we provided alerting and intelligence so the Electrical Provider could

respond to any future threats and prevent severe damage.

Finally, we fortified their security set up to protect them from further assaults. At the same time, we created a common architecture that allowed the easy assimilation of newly acquired technologies, businesses, or organizations.

Results

By giving the Electrical Provider better visibility into their entire environment, identification, and remediation efforts, and helping them deploy the necessary tools where needed in their network, their security posture has increased substantially.

They haven't suffered another ransomware or any other type of cyber attack since. Our vigilant SOC team continues to deliver reliable situational awareness through our BOSS platform and security monitoring.

Solutions Provided:

- Managed Services
- BOSS Security Suite
- 24/7 SOC Support
- Security Assessment
- Security Monitoring
- Triage and Referral

Ready for the Security You Deserve? Let's Talk.

Talk to our experts today about your specific needs. Call **866-405-9156**, email us at **sales@uncommonx.com** or visit us at **uncommonx.com**.