COLORTOKENS

CASE STUDY

Critical Infrastructure Powered Up, Securely

INDUSTRY: Electric Utility

HEADQUARTERS: Mexico

Overview

The electric utility company is one of the leading providers of electricity for Mexico City's public lighting, covering approximately 18 million inhabitants. It operates 5 hydroelectric plants and monitors water levels across major dams in Mexico using a critical infrastructure application.

The Challenge

Having the electric utility company's IT network infrastructure newly separated from its parent company, security stakeholders were looking for a solution to improve the organization's security posture and provide proactive protection against advanced attacks.

Having possession of data records of major dams and hydroelectric plants in Mexico made the utility provider vulnerable to ransomware and cyberattacks. Stakeholders were concerned that a breach would go undetected, giving bad actors opportunities to access critical data and disrupt the functioning of dams and hydroelectric plants. The critical infrastructure threat landscape in Mexico is getting increasingly hostile. A breach instance can have widespread consequences beyond financial and reputational loss, by potentially impacting the fundamental functionality of civil society.

With the electric utility's employees working remotely, the organization wanted a solution that offered comprehensive visibility into its network traffic, applications and potential blind spots, that defended against an unpredictable threat environment without disrupting its end users.

The Approach

ColorTokens brought under its scope approximately 250 critical assets and deployed its platform based on a foundation of Zero Trust architecture. ColorTokens recommended and implemented three core solutions: Xshield, Xprotect and Xassure, with each fulfilling a distinct purpose. Xshield, which was designed to protect the electric utility's IT network, endpoints and sensitive client, offered complete visibility with a simplified zero trust microsegmentation approach.

The electric utility company implemented Xprotect for highly granular security controls in order to restrict unauthorized access to endpoints and enable dynamic whitelisting for endpoints in remote locations. This approach allowed ColorTokens to create a Zero Trust posture for electric utility company where least privilege access was granted on role-based credentials, and not locations or specific hardware. And lastly, ColorTokens applied Xassure, which allowed electric utility company to leverage integrated dashboards, threat intel feeds and threat detection rules to quickly sound the alarm on any anomalies and/or suspicious traffic or processes.

> "What ColorTokens offered us was the most comprehensive solution we have come across. Initially, we were worried that the Zero Trust implementation would need significant time and resources. But, ColorTokens alleviated those concerns and installed agents without any disruption to our end users."
>
> - IT Planning and Control Manager, Electric Utility Provider

Results and Benefits

With ColorTokens' Xtended ZeroTrust™ Platform, one of Mexico's leading electricity providers implemented a proactive cybersecurity approach across their organization. But even with an elevated security posture, it did fall under the radar of threat actors.

In February 2021, intrusion attempts were made to penetrate inside its webserver environment hosted on Azure cloud through 600+ malicious IP addresses from suspicious geo locations.

ColorTokens' threat monitoring team detected these network anomalies and sent security alerts related to brute force attempts and botnet connections. Using Xshield's Skyview visualizer console, security stakeholders gained a deeper understanding of the attack scenario in real time and successfully blocked those connections in less than 24 hours.

This led to **a potential savings of $1M** that the organization would have spent to eradicate the infection had it materialized. In such challenging times when the threat landscape is evolving every day, the **organization realized rapid time-to-value with ColorTokens' solution set within 6 months** and is prepared to fight against advanced threat attempts proactively.

Conclusion

Overall, ColorTokens provided a leading Mexican electric utility company with security before, during and after an attempted breach of their webservers. A breach of this size could have potentially caused mass disruption, and instead, due to having comprehensive visibility into network traffic and blindspots and proactive endpoint protection for all end-user systems and remote workstations, a costly disaster was avoided. The electric utility company now has zero disruption to business operations, as there are no longer hardware or infrastructure dependencies. They now have platform-generated policy recommendations that reduce the security team's efforts and time and receive real-time alerts with managed threat detection along with response services with qualified insights.

Simplifying Your Journey to Zero-Trust Architecture

ColorTokens is a leader in delivering innovative and award-winning zero-trust cyber security technology solutions such as network micro-segmentation, endpoint hardening and whitelisting, cloud and container security, and zero-trust network access. ColorTokens is a US corporation headquartered in Silicon Valley, and has approximately 400 employees world-wide, with offices in the United States, the United Kingdom, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please visit **colortokens.com**