



# Case Study



## Client Profile

The Midwest Independent Transmission System Operator, Inc., also known as “Midwest ISO” or “MISO”, is the nation's first Regional Transmission Organization (RTO) approved by the Federal Energy Regulatory Commission (FERC). The Midwest ISO is based in Carmel, Indiana, and is responsible for monitoring the electric transmission system that delivers power from generating plants to wholesale power transmitters (the entities that deliver power to distribution companies that, in turn, deliver power to residential and commercial customers). The Midwest ISO's role is to ensure equal access to the transmission system and to maintain or improve electric system reliability in the Midwest.

## Executive Summary

The scope of work provided by DYONYX consisted of a number of specific Tasks as described below:

- Task 1: Given a set of IP address ranges and phone number listings, determine what hosts or devices are visible externally to Midwest ISO and what phone lines have devices that are set to auto answer; additionally, through a search of the Internet for any documents published by Midwest ISO posted on Internet search engines, forums, blogs, or any other miscellaneous websites, identify any confidential or sensitive documents that may be published or cached on public Internet sites;
- Task 2: Conduct penetration testing to determine vulnerabilities that were not detected in Task 1;
- Task 3: Drill down into key systems identified in prior phases to discover vulnerabilities to these systems and devices; explore possible vulnerabilities at several levels including but not limited to the networking, operating system, server, security and application levels; and,
- Task 4: Provide a comprehensive and detailed report of the findings discovered in the previous phases.

The DYONYX team delivered a comprehensive report detailing the findings listed above. Subsequent to the completion of these Tasks, DYONYX provided a detailed vulnerability assessment of the Midwest ISO Market Portal System. Considerable insight was provided concerning the development processes and techniques to remove the existing vulnerabilities.

