Red Sentry
x Energy Company

CASE STUDY

Defeating the Russians through **Cybersecurity**

A large US energy company partnered with Red Sentry to protect itself from Russian hacking trends.

INTRODUCTION/OVERVIEW

The 2022 Russia-Ukraine Conflict created new threats to cybersecurity, not just abroad, but in the US as well.

An energy company (who's real name is kept private for security reasons) sought out **Red Sentry**'s help to test their cyber environment and stay secure from the most common vulnerabilities Russian hackers were using.

CHALLENGE

In early 2022, Russian state-sponsored hackers began specifically targeting US energy companies, which posed a serious threat to American infrastructure.

The FBI and other government entities warned these companies of **DDoS attacks** (distributed denial-of-service), which interrupt services and are especially detrimental to companies in the energy, gas and oil industries.

20%
of all companies will suffer a cybersecurity breach in the next year.

At the same time, organizations like our client have a hard time finding offensive cybersecurity companies they can trust because of the sensitive nature of their data.

SOLUTION

The energy company engaged with Red Sentry and other providers to find the best partner for them, and after thorough due diligence decided that they wanted to entrust Red Sentry with this large penetration testing project. Red Sentry was scanned through BitSight and found to be a secure vendor option.

Red Sentry conducted a penetration test of their entire environment to identify vulnerabilities and weaknesses.

167 TOTAL FINDINGS
were uncovered by our team of experts.

Among numerous other findings, Red Sentry was able to gain access to all phones and conference sessions within the organization. The findings have since been remediated and retested, suring up the environment and hardening the target from external hackers.

HIGH-SEVERITY FINDINGS

- Default Administrative Passwords within Sensitive Systems
- SQL Injection
- Anonymous FTP Login Enabled

BENEFIT

With attacks coming from all angles, it's hard to gain peace of mind in this era. Our client can now feel secure knowing that they have a strong environment, and continue to focus on serving the public with the energy they need.

RESULT

Not only did the organization get a thorough penetration test that led them to find and remediate vulnerabilities, but they're now using Red Sentry's continuous vulnerability platform on a daily basis, so that if a new vulnerability pops up, they'll be ready.

Red Sentry is quickly becoming the partner of choice for growing businesses.