

Case Study #2

How **HackGRC** saved the technology from the humans.

During this engagement, VULSEC acted as the Chief Information Security Officer. During this time we were able to bridge the gap between the Corporate and production divisions within the company.

We discovered risks through our External Network Security Assessments, Internal Network Security Assessments, Social Engineering, Information Security Program development, and Web Applications Security Assessments.

Natural Gas Pipeline had a technical problem.

Their technology was configured by employees who did not understand technology.

So VUISEC performed technical analysis to understand the risks within 20 remote locations mapping to an overall corporate risk ranking.

1. RESEARCH

First performed various assessments around external and web applications assessments to discover risks within critical assets and client portals. VULSEC then performed an internal assessment to assess the micro level of the organization. After we gathered the technology risks we create the Information Security Program towards NIST and SANs critical controls. Then we mapped to specific regulations like NERC CIP 6, INGAA, and TSA.

2. IMPLEMENTATION

By focusing on the technical risks within the organization we were able to correlate both on a macro and microlayer of the organization to determine holistic risks. After these VULSEC create a blueprint in specific ways to reduce the most amount of risk at the most cost effective price. VULSEC then brought in partners through our CISO marketplace to speed up remediation.

3. THE RESULTS?

- Discovered DDoS vulnerability within Checkpoint Firewalls during scans because of improper network architecture.
- Through CISO marketplace we implemented a Syslog, SIEM, Threat Intelligence, and 24x7 Security Operation Center with active mitigation.
- Through CISO marketplace we implemented an endpoint protection solution that protects the users and mobile devices.
- Conduct social engineering against employees through remote ways. Provided user education seminars for the organization to understand information security within their industry.
- Information Security Coach to provide bi-weekly community updates, assessment updates, and provide roadmap feedback.