



FORTIFY WITH THREATCOP

OIL & GAS INDUSTRY

CASE STUDY

www.threatcop.com

Introduction

The company is an integrated oil and gas company with operations across the entire value chain, from exploration and production to refining and marketing. It is the largest oil and gas company in the country, with a strong presence in both upstream and downstream sectors. The company has a diversified portfolio of assets, including oil and gas fields, refineries, pipelines, and marketing terminals. It is a major player in the Indian energy sector, and it is committed to meeting the growing energy needs of the country. It is a trusted partner of the government, and it is committed to the development of the country.

The company is committed to providing safe, reliable, and affordable energy to its customers. It is also committed to protecting the environment and to operating sustainably. The company is a responsible corporate citizen, and it is committed to making a positive contribution to the communities in which it operates.

Company Details

Employee Size: 20,000+

Annual Revenue \$133.12 billion

Market Capitalization \$119.62 billion

Cybersecurity has become a paramount concern for organizations across all industries, particularly in the oil and gas sector. The oil and gas industry plays a crucial role in powering the global economy, and any disruptions to its operations can have severe consequences, ranging from financial losses to environmental disasters. As a result, cybersecurity has emerged as a critical component of risk management for oil and gas companies.

Common Challenges Faced by the Oil & Gas Industry

1. Human Risk Management: Addressing the Human Element

In today's increasingly digital world, people remain the weakest link in the cybersecurity chain. Phishing attacks, for instance, often rely on social engineering tactics to manipulate employees into clicking on malicious links or revealing sensitive information. Effective human risk management is therefore essential to minimize vulnerabilities and enhance cybersecurity posture.

2. DMARC (Domain-based Message Authentication, Reporting & Conformance): Protecting Brand Reputation

DMARC is an email authentication protocol that helps protect organizations from email spoofing attacks, where scammers impersonate legitimate senders to trick recipients into divulging sensitive information. By implementing DMARC, oil and gas companies can safeguard their brand reputation from phishing attacks and maintain trust among their customers and partners.

3. Phishing Incident Response: Addressing Phishing Attacks Swiftly and Effectively

Phishing attacks are a common threat to oil and gas companies, and having a robust phishing incident response plan is crucial to minimize their impact. This plan should include clear procedures for identifying, investigating, and remediating phishing attacks, as well as effective communication strategies to inform employees and stakeholders.

4. Phishing Simulation: Educating Employees through Simulated Attacks

Phishing simulations provide a valuable tool for educating employees about phishing attacks and raising their awareness of cybersecurity risks. By conducting simulated phishing attacks, companies can assess their employees' susceptibility to phishing and provide targeted training to improve their ability to identify and avoid phishing scams.

People Security Management: Empowering Employees

Cybersecurity awareness training is essential for equipping employees with the knowledge and skills to protect themselves and the organization from cyber threats. This training should cover topics such as phishing attacks, password management, social engineering techniques, and secure online behavior.

Challenges being faced by the customer:

- Phishing attacks by impersonation.
- Social engineering
- Unintentional Errors by Employees
- Email spoofing
- Domain abuse
- Lack of visibility.
- Delayed detection
- Difficulty in containment
- Inadequate communication
- Insufficient feedback and follow-up training

Potential risks and consequences of these challenges

- Data breaches:** Phishing attacks and human error can lead to data breaches, exposing sensitive customer, financial, and operational information. This can result in reputational damage, regulatory fines, and financial losses.
- Financial fraud:** Phishing attacks and social engineering can lead to financial fraud, such as wire transfers or fraudulent account access. This can result in substantial financial losses for the company.
- Disruptions to operations:** Cybersecurity incidents stemming from human factors can disrupt critical oil and gas operations, leading to production delays, supply chain disruptions, and safety hazards.

Outcomes and improvements observed after Implementing Threatcop

Threatcop Phishing Simulation Implementation Report

1. Purpose

This report highlights the measurable outcomes and improvements observed in oil & gas company's cybersecurity posture after the implementation of Threatcop, a comprehensive cybersecurity solution designed to enhance threat detection, response times, and overall security resilience.

2. Implementation Overview

After the phishing simulation campaign results, oil & gas company undertook the following measures to strengthen its security posture:

3. Security Awareness Training:

Conducted targeted security awareness training programs for employees to enhance their ability to identify and mitigate phishing threats.

4. Awareness Enhancement:

Improved awareness and messaging to provide more detailed guidance on recognizing and avoiding phishing attacks.

Measurable Outcomes and Improvements

1. Email Open Rate:

Post-ThreatCop implementation, the email open rate decreased significantly to 6.28%, showcasing a substantial improvement in employees' resilience to phishing attacks.

2. Click-Through Rate:

The click-through rate dropped to 2.1% after ThreatCop implementation, indicating a notable reduction in employees' susceptibility to clicking on malicious links.

3. Phishing Link Clicked:

The number of employees clicking on phishing links reduced to 7.8% post-ThreatCop implementation, demonstrating a significant improvement in employee vigilance.

4. Threat Detection:

Threatcop's advanced threat detection capabilities led to an 80% increase in the identification and blocking of phishing emails compared to pre-implementation levels.

5. Response Times: The response times to identified threats improved by 50%, showcasing the efficiency of ThreatCop in enabling swift and effective responses to potential cyber threats.

6. Awareness Page Impact:

The enhanced awareness page contributed to a 30% decrease in repeat phishing attempts, indicating improved employee awareness and response to phishing simulations.

Before-and-After Scenarios

<u>Threatcop</u>	<u>Before</u>	<u>After</u>
Open Rate	28.03%	6.28%
Click-Through Rate	28.03%	2.1%
Phishing Link Clicked	28.03%	7.8%
Response Time	Moderate	Rapid

Ransomware Simulation & Awareness Program Outcomes

Purpose

This report outlines the measurable outcomes and improvements observed in oil & gas company's cybersecurity posture after the implementation of Threatcop, a comprehensive cybersecurity solution designed to enhance threat detection, response times, and overall security resilience.

Implementation Overview

Following the ransomware simulation campaign results, the company undertook the following measures to fortify its security posture:

Security Awareness Training:

Conducted regular security awareness training programs for employees to enhance their ability to identify and mitigate phishing threats.

Multi-Layered Security Solution:

Implemented Threatcop, a robust multi-layered security solution comprising advanced email filtering, firewalls, and intrusion detection systems.

Data Backup and Recovery Plan:

Established and implemented a comprehensive data backup and recovery plan to ensure the organization's ability to recover from ransomware attacks without succumbing to ransom demands.

Measurable Outcomes and Improvements

Email Open Rate:

Post-ThreatCop implementation, the email open rate decreased significantly to 15.2%, showcasing a substantial improvement in employees' resilience to phishing attacks.

Click-Through Rate:

The click-through rate dropped to 5.7% after ThreatCop implementation, indicating a notable reduction in employees' susceptibility to clicking on malicious links.

Infection Rate:

The infection rate decreased dramatically to 2.1%, demonstrating a substantial improvement in IT's ability to prevent successful ransomware attacks.

Threat Detection:

Threatcop's advanced threat detection capabilities led to a 75% increase in the identification of phishing emails and malicious links compared to pre-implementation levels.

Response Times:

The response times to identified threats improved by 60%, showcasing the efficiency of ThreatCop in enabling swift and effective responses to potential cyber threats.

Overall Cybersecurity Posture:

IT's overall cybersecurity posture witnessed a significant enhancement, with ThreatCop contributing to a 40% reduction in successful cyberattacks and an increased level of resilience against evolving threats.

Before-and-After Scenarios

<u>Threatcop</u>	<u>Before</u>	<u>After</u>
Open Rate	55.6%	15.2%
Click-Through Rate	43.4%	5.7%
Ransomware Infec. Rate	12.9%	2.1%
Response Time	Moderate	Rapid

Threatcop DMARC Implementation Report

Purpose

This report outlines the measurable outcomes and improvements observed in oil & gas company's email security posture after the implementation of Threatcop's DMARC (Domain-based Message Authentication, Reporting, and Conformance) solution. The focus is on enhancing email authentication, reducing phishing risks, and fortifying overall email security.

Implementation Overview

Following the DMARC data analytics, the company implemented Threatcop's DMARC solution to strengthen email authentication and combat phishing threats. The key focus areas included:

1. DMARC Configuration:

Configured DMARC policies to ensure strict authentication of email senders and prevent unauthorized use of oil & gas company's domain.

2. Email Sender Authentication:

Implemented SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) authentication mechanisms to enhance the validation of legitimate email senders.

3. Threat Detection and Reporting:

Leveraged Threatcop's threat detection capabilities to identify and mitigate potential email threats, including phishing attempts.

Measurable Outcomes and Improvements

1. DMARC Implementation:

Achieved a DMARC adoption rate of 90%, indicating a substantial improvement in email authentication and domain protection.

2. SPF and DKIM Authentication:

Improved SPF authentication to 86% and DKIM authentication to 55%, enhancing the overall validation of legitimate email senders.

3. Failed Authentication Rate:

Reduced the failed authentication rate to 10%, showcasing the effectiveness of DMARC, SPF, and DKIM in preventing unauthorized email senders.

4. Email Volume and Threat Sources:

Effectively managed an email volume of 10.4 million, with identified threat sources reduced to 5 key domains, demonstrating enhanced threat visibility and control.

5. Geolocation Monitoring:

Monitored email sources across geolocations, with a notable reduction in threats originating from certain regions, ensuring a more secure email environment.

Before-and-After Scenarios

<u>Threatcop</u>	<u>Before DMARC</u>	<u>After DMARC</u>
DMARC Adoption Rate	NA	90%
SPF Authentication	NA	86%
DKIM Authentication	NA	55%
Failed Authentication Rate	NA	10%

Conclusion:

The implementation of ThreatCop has been instrumental in elevating the cybersecurity postures of both the Oil and Gas Industry. Both organizations witnessed a significant reduction in susceptibility to phishing attacks and ransomware, coupled with enhanced threat detection and improved response times. Threatcop's efficacy was particularly evident in mitigating cyber risks and fortifying defenses against evolving threats, underscoring its pivotal role in cybersecurity strategies. Continuous monitoring, periodic assessments, and ongoing employee training were identified as critical factors for sustaining and further improving the organization's cybersecurity resilience. In the context of email security, Threatcop's DMARC solution demonstrated remarkable success, achieving a high adoption rate, enhancing SPF and DKIM authentication, and substantially reducing the failed authentication rate. Ongoing optimization of DMARC policies and vigilant monitoring were identified as crucial for sustaining and improving email security resilience, ensuring organizations are well-equipped to defend against phishing attempts and unauthorized email sources.