UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Case Study

Global Oil and Energy Provider Penetration Test

Industry:

Oil and Energy

Business Challenge:

Meeting compliance and regulation standards
Protecting employee and customer data

IT Environment:

Cisco Servers,
Windows Tech Stack

Solution:

Custom developed security roadmap, built post pentest to help meet compliance and regulations

Results:

- Met compliance standards
- Increased customer trust and retention
- Simplified internal and external security practices

Background:

One of the world's leading international oil and gas companies, providing fuel, energy, retail services and petrochemicals, best known to the public for its service stations and for exploring and producing oil and gas on land and at sea. Prominent in over 140 countries and territories and employing more than 112,000 people around the globe.

> *"UnderDefense stands out in the field of penetration testing because they understand the importance of security risks and are able to map it to the domain in which their client is operating. Their services are very much tailored to the particular application being examined. Simply using automated scanning tools is not a replacement for smart, intelligent people with a deep understanding of security related issues. UnderDefense takes penetration testing to the next level, using real people to test systems and interpret the results".*

CISO - Oil and Energy Company

The Challenge:

Holding a major global presence and continuously being targeted, our client understood the risks they faced on a daily basis. In order to meet compliance and regulation standards they engaged the Security Team at UnderDefense to conduct and full black-box Organizational pentest, to learn more about the vulnerabilities they have and how they can be remediated.
Additionally, the customer had a specific business continuity and compliance requirements, relating to its duty of care to maintain employees' and clients personal, and financial data . With a multinational
presence the pentest itself was conducted on multiple territories to ensure the highest level of results.

People, Process, & Technology:

Penetration testing can be conducted in many ways and methodologies. Usually we follow this process:

Test Planning	Vulnerabilities Identification	Vulnerabilities Exploiting	Post Exploitation	Reporting and Recommendation
Meetting with customer Allign test goals and scope Intelligance gathering	Potential vulnerabilities detection Threat modeling Business process analysis	Vulnerabilities testing Vulnerabilities validation Vulnerabilities research	Escalating privileges Infrastructure analysis Vulnerabilities research	Create report for system owner, including found vulnerabilities and recommendations how to eliminate them

For our client's specific requirements and geographical locations we agreed to pursue the following methods: black box tests, social engineering, email phishing, and onsite red teaming.

#	Standard/Methodology
1.	Penetration Testing Execution Standard
2.	OWASP Application Security Verification Standard
3.	Information Systems Security Assessment Framework (ISSAF)
4.	SANS: Network Penetration Testing and Ethical Hacking

With a team of 4 engineers and a duration of 4 weeks we were able to fully compromise not only the organizations infrastructure but also, web applications as well as expose critical data related to key organizational stakeholders.

The Result:

Penetration testing is often done for varying reasons. Two of the key goals we and our client aimed for, were to increase upper management awareness of security issues and to test intrusion detection and response capabilities. After conducting the pentests and compromising the organization UnderDefense engaged the client in a controlled offensive/defensive threat detection challenge, allowing the client several days to identify and remediate active threats within their systems. After this challenge was complete UnderDefense was commissioned to conduct training for the key internal security team as well as further advisory on remediation tactics. In the end our client was able to meet the highest level of compliance and regulation standards, develop better security practices and reassure their customers, employees, and board of their continued dedication to best business practices and continued growth.

Key Benefits:

Increase Business Continuity

Protect Clients, Partners and Third Parties

Help to evaluate Security Investments

About UnderDefense:

We at UnderDefense are dedicated to supporting organizations around the world in planning, building, managing, and running successful security operations programs, meeting and maintaining compliancy regulations and exceeding organizations abilities to run their businesses securely and confidently.

We don't just do;
we think, innovate, and create new security capabilities to
combat tomorrow's threats today.

USA, New York
375 Park Avenue, Suite 2800, NY
Tel: +1.929.999.5101
email: help@underdefense.com

Poland (EU), Wrocław
Rzeźnicza str. 28-31, 50-130
Tel:+48 792-229-273
email: help@underdefense.com

Ukraine, Lviv
Heroiv UPA 73 k.38, Lviv, 79014
Tel: +38 063-11-357-66
email: help@underdefense.com