Case Study

Comprehensive cybersecurity audit to detect critical vulnerabilities and implement protective measures

Client: A large telecommunications operator

Challenge

The client needed to evaluate IT security maturity and ensure the protection of sensitive corporate information. **Key challenges included:**

Data confidentiality: There was a risk that sensitive financial and operational data could be leaked.

Security maturity assessment: The client needed to evaluate the overall maturity of their IT security systems to understand potential gaps and risks.

Solution

ZONE3000 performed a focused cybersecurity assessment using:

Black-box penetration testing

Simulating real-world attacks without prior knowledge of the internal and external systems.

Red Teaming and remediation support

Providing specialists to directly address identified weaknesses and implement additional safeguards, including secure configuration of network and server systems.

Rapid analysis

Delivering actionable insights on high-risk areas of the client's IT infrastructure.

Results

The audit helped the client uncover critical vulnerabilities and improve security controls:

Critical access demonstrated

ZONE3000 gained access to the financial system with CFO-level privileges, highlighting gaps in protection.

Targeted remediation

Our specialized team conducted Red Teaming and implemented secure configuration of network and server systems, enabling the client to reduce the risk of future breaches.

The collaboration with ZONE3000 allowed the client to evaluate security maturity, remediate high-risk vulnerabilities, and strengthen protection of sensitive financial data across their organization through both assessment and active remediation.

Roman Dzvinka
Chief Revenue Officer

+380 67 505 72 96

roman.dzvinka@zone3000.net