RESCANA

Case Study: Strengthening Telco Cybersecurity with Rescana's AI-Driven Risk Management

Customer Overview

A leading Israeli telecommunications provider with millions of subscribers sought to enhance its cybersecurity posture amid rapid 5G expansion, digital transformation, and intensifying cyber threats. Like many telcos facing challenges such as sophisticated DDoS assaults and state-sponsored intrusions, the customer needed to secure not only its network and IT infrastructure but also its supply chain and partner ecosystem.

Challenges

Limited Asset Visibility Across a Complex Digital Footprint

The provider lacked a full understanding of its external attack surface, including cloud resources, legacy data centers, exposed services, and an expanding IoT ecosystem. Gaining real-time visibility was critical to identifying potential security gaps.

DDoS Readiness Assessment

With repeated DDoS attacks targeting critical infrastructure, the telco required an effective assessment of its exposure. It needed insights into whether protective measures—such as WAF and CDN configurations—were adequately deployed and optimized.

Exposure of Web-Facing Applications

The telco sought to understand its exposure to web application vulnerabilities, particularly those related to outdated software, misconfigurations, and potential exploits—without the overhead of performing active penetration testing.

RESCANA

Data Leak & Call Detail Record (CDR) Exposure

Highly sensitive subscriber data, including CDRs, posed regulatory and reputational risks if leaked. The provider needed continuous monitoring for indications of data exposure on the deep and dark web.

Third-Party & Supply Chain Risk

With a vast network of resellers, service providers, and technology partners, third-party risk was a major concern. The telco required a scalable and objective approach to evaluating vendor security postures and potential weak links in its supply chain.

Solution: Rescana's AI-Powered External Attack Surface and Risk Management Platform

Rescana provided a passive, AI-driven cybersecurity platform that enables continuous monitoring and external risk assessments without intrusive scanning or active testing.

Key Features & Capabilities

✅ Continuous External Asset Discovery & Risk Assessment
Using OSINT methodologies and AI, Rescana mapped the telco's publicly exposed digital assets, identifying unpatched systems, misconfigurations, and potential vulnerabilities. This provided near real-time visibility into the organization's external risk landscape.

✅ DDoS Risk Insights
Rescana analyzed the telco's infrastructure to detect the presence and configuration of DDoS mitigation measures, such as WAF coverage, CDN usage, and public exposure of critical assets. The platform highlighted weak points that could be exploited in an attack.

✅ Web Application Security Monitoring
Without requiring active testing, Rescana flagged outdated web-facing applications, configuration issues, and potential entry points for attackers. This enabled the telco's security team to prioritize necessary remediations.

RESCANA

✅ **Dark Web & Data Leak Monitoring**
By continuously scanning deep and dark web sources, Rescana provided early warnings of leaked credentials, exposed CDRs, and other sensitive data, enabling proactive risk mitigation.

✅ **Third-Party Risk Management**
Rescana automated vendor risk assessments, combining OSINT-based security evaluations with compliance questionnaire analysis. This allowed the telco to enforce security benchmarks across its partner ecosystem.

Results & Impact

📌 **Enhanced Asset Visibility**
The telco achieved a 360-degree view of its external digital footprint, reducing blind spots and unmonitored attack vectors.

📌 **Improved DDoS Resilience**
Insights from Rescana allowed the telco to optimize its WAF and CDN deployment, strengthening its ability to mitigate high-volume DDoS attacks.

📌 **Stronger Web Application Security Posture**
The telco identified and prioritized vulnerabilities in its web-facing applications, significantly reducing the risk of exploitation.

📌 **Proactive Data Leak Prevention**
Early detection of leaked credentials and sensitive records enabled rapid response, mitigating regulatory and reputational risks.

📌 **More Secure Supply Chain**
Automated vendor security assessments standardized third-party risk management, reducing exposure from compromised suppliers.

RESCANA

Balanced Perspective & Lessons Learned

The implementation of Rescana's platform provided the telco with a non-intrusive, continuous, and AI-driven approach to cyber risk management. However, early adoption required refining OSINT-based monitoring to align with specific industry concerns. Additionally, while automation reduced manual workload, ongoing security awareness and policy enforcement remain essential to long-term resilience.

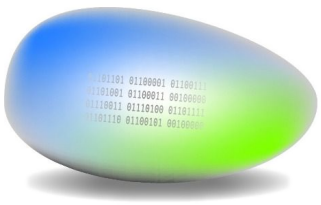
By leveraging AI-powered external risk intelligence and third-party risk automation, the telco significantly strengthened its cybersecurity posture without intrusive testing or active remediation.

About Rescana

Rescana is a leader in AI-powered cyber risk management, specializing in external attack surface monitoring and third-party risk assessment. The platform provides passive, OSINT-based visibility into an organization's security posture, helping enterprises anticipate, detect, and mitigate cyber threats without active scanning or intrusive checks.

👉 **Learn more: www.rescana.com**

Contact: raviv@magicstone.nl



Partner of

MAGIC STONE