Case Study

CyScope's Bug Bounty Program for a Telecommunications Operator

CyScope

CyScope

Case Study

CyScope’s Bug Bounty Program for a Telecommunications Operator

Challenges and Needs

- Reducing the risk level of their external perimeter.
- Centralizing results on an intuitive and transparent platform.
- Maintaining their reputation

How Can CyScope's Bug Bounty Programs Safeguard a Telecom Company?

Telecommunications operators face a significant challenge due to their extensive attack surface and a high number of exposed assets. They need to continuously assess the security of their systems and services in an agile, efficient, and effective was to lower cyber risk and uphold their reputation.

Results and Insights

Over the course of 4 years collaborating with the CyScope team, the client has launched 15 programs, receiving more than 700 security reports from our ethical hacker community, paying between $50 and $500 per report depending on the severity of each finding.

CyScope’s continuous penetration testing has helped the client understand and assess the knowledge of their DevSecOps teams, identify new external threats, and address them effectively.

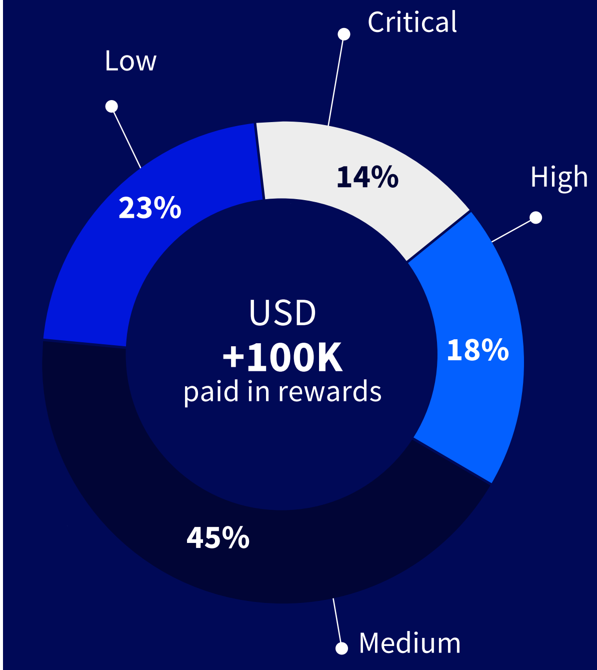
CyScope offers an intuitive and transparent workspace to manage security vulnerabilities proactively, streamlining the mitigation process for improved internal operational efficiency.

cyscope.ch

Client Profile

- One of the Top Telco Companies in its operating country
- +4 years collaborating with CyScope
- More than 15 bug bounty programs launched
- Average Annual Reward Budget: 50.000 USD

Web and Mobile Program Overview*



+200 domains audited.
+700 security reports received.
+160 active hackers engaged.
Reward amounts ranging from **$50-$500 USD.**
Payment per valid report.

*Published on August 2023