



Assess, quantify, and mitigate your cyber risk

# CYE Creates Optimized Cybersecurity Program for a **Global Telecom Company**

## **CHALLENGE**

Build a unified comprehensive security program for a global organization

## **SOLUTION**

Thorough security assessment with Hyver, red teams, and data science expertise

## **VALUE**

Quality, accurate insights at scale, driving mitigation efforts

# COMPANY

A telecommunications, information technology, and communications equipment manufacturer

**100K**

Employees

**120**

Sites

## THE CHALLENGE

### BUILD A UNIFIED COMPREHENSIVE SECURITY PROGRAM FOR A GLOBAL ORGANIZATION

The engagement with the company started with a limited scope of the main network infrastructure and connected sites. The company network architecture comprised multiple networks and several independent domains with connectivity traversing multiple countries. Over and above the core infrastructure, there were several locations and companies that were added to the group via M&A that were disconnected or have independent networks.

As the engagement progressed, CYE was tasked with including additional locations and their respective network structures. Consequently, the overall organizational maturity and risk profile of the organization was duly expanded and updated accordingly.

#### The engagement had several objectives:

- Gain clear visibility into the technical risk profile of the organization (based on the scope) as a baseline. The risk profile needed to be validated with evidence of the risk items and vulnerabilities.
- Draw a map with detailed steps connecting the business-critical assets and crown jewels to potential threat sources.
- Assess and quantify the cybersecurity business risk.
- Optimize the cybersecurity program based on the findings.
- Reassess the organizational maturity and the organizational reflected risk after initial mitigation.

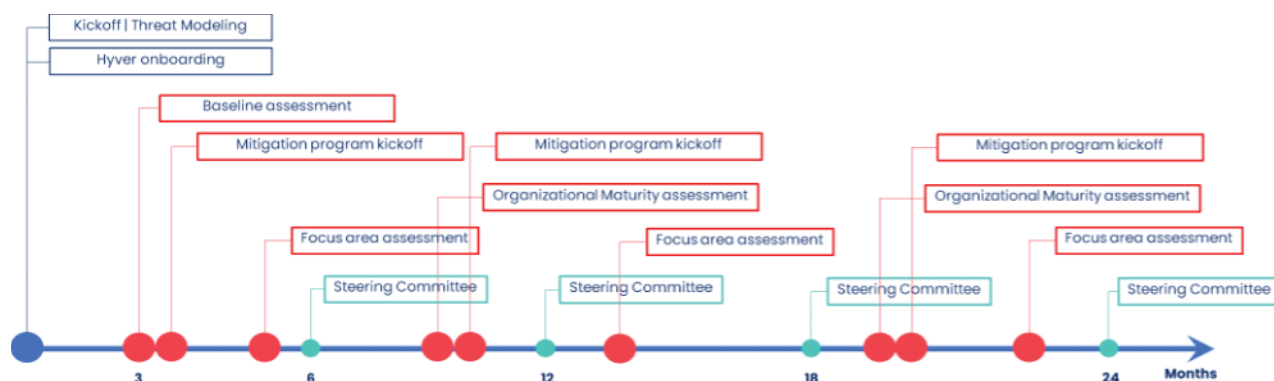
# THE SOLUTION

## THOROUGH SECURITY ASSESSMENT WITH HYVER, RED TEAMS, AND DATA SCIENCE EXPERTISE

The activity was performed using CYE's cybersecurity optimization platform, Hyver, and CYE's unique, professional red team services, data science expertise, and security assessment methodology. The method includes a smart sampling approach in which CYE collects the relevant evidence and executes attacks on environments. This obtains a clear technical risk profile, while also demonstrating the potential exposure to the business. CYE's methodology and tools are integrated into the Hyver platform.

# PROGRAM EXECUTION

The program included the following activities over a 24-month program:



The initial baseline duration was 10 weeks. The activity was conducted to mimic two types of threat sources simultaneously:

### External threat sources

- Passive and active external reconnaissance and rapid risk assessment of the organization and the group entities.
- External "black box" approach to impersonate the external threat of the organization, with a specific focus on the desired entities as mentioned in the scope, where the crown jewels are present. In this stage, the team used different techniques to obtain access to the organization in order to elevate privileges and compromise business critical assets.

### Internal threat sources

- Grey box approach in which the team obtained access to the network as a regular employee (the network access and privilege level) and tried to escalate access and privileges towards the predefined targets.
- This was executed using remote VPN access with a regular, non-privileged domain user.

# THE VALUE

## QUALITY, ACCURATE INSIGHTS AT SCALE, DRIVING MITIGATION EFFORTS

During the engagement, all the predefined objectives were fully achieved. By leveraging Hyver, the company was able to receive quality, accurate insights at scale that drove effective mitigation efforts and resource allocation. In addition, the following items were identified by the company as high-value outcomes:

- Clear visual representation of the organizational risk profile that can be easily communicated to executives and board members.
- Clear scientifically supported reasoning for budget requests and cybersecurity initiatives, while improving ROI.
- Agility in developing and maintaining cybersecurity programs, while balancing strategic initiatives and reaction to tactical risks.
- Optimized cybersecurity program that is achievable and measurable.

### ABOUT **CYE**

CYE's cybersecurity optimization platform enables businesses to assess, quantify, and mitigate cyber risk so they can make better security decisions and invest in effective remediation. CYE combines this with dedicated professional guidance and advice provided by established cybersecurity experts. The company serves Fortune 500 and mid-market companies in multiple industries around the world. With headquarters in Israel and offices in New York and London, CYE is funded by EQT Private Equity and 83North. [Visit us at cyeseccom.com](https://www.cyeseccom.com)



Want to learn more about how CYE can help protect your company from cyber threats?

[Contact us](#)