CYE's Optimized Cyber Risk Quantification

A comprehensive solution to improve organizational maturity and reduce risk.

Hyver Customer Engagement Flow

General

As cyber breaches continue to escalate, ensuring robust cybersecurity has become a paramount concern for enterprises. CYE's Hyver offers a cybersecurity maturity program that includes comprehensive security assessments, security expertise, and an innovative advanced platform.

We provide completely tailored solutions aligned with our customers' specific requirements. Our cyber expert account managers orchestrate the workflow, establish timelines, and outline the scope of work prior to onboarding, ensuring solution optimization.

This document describes a high-level flow of the engagement.

Customer Onboarding

The onboarding process takes about 3-4 weeks. During this period, we get to know the organization from both business and technical perspectives.

The onboarding process includes a few phases:

1 Kick-off session

The purpose of this session is to introduce the teams to each other, create communication channels, and align expectations. During the session, we meet the stakeholders and define targets and objectives.

2 Data collection

In this phase, we collect the initial data through an organizational security review and integrate with the customer technologies. The objective is to get to know the technical environment – the IT organization, the main crown jewels, the network architecture, the security controls in place, known security gaps, and more.

This phase includes enabling some of the automation capabilities of the product and updating financial data with the "Cost of Breach" questionnaire.

The organizational security review aims to provide the initial organizational data gathering used to identify cybersecurity risks and maturity gaps. The data is collected, analyzed, and documented in Hyver, which enables the user to use Hyver's many features, such as an attack graph and mitigation optimization, NIST maturity scoring, assets identification, and more.

Typically, the activity is done using a white-box approach, i.e., system access, privileges, and data are available to CYE's team during the review. This ensures a comprehensive analysis of the organization's current status and focuses on identifying risks and gaps rather than mimicking a single attacker scenario.

The organizational security review is not an assessment. It is a white-box approach data gathering activity, done by hackers and security architects, which aims to create a graph and enable the risk and maturity calculations as fast as possible, presenting the client with Hyver's value within a month.

3 Hyver training

The purpose of this phase is to create a dedicated tenant on Hyver and invite the customer to start using the platform, define permissions, set the needed reports and alerts, and more. In this phase, the customer will will be trained about the the main modules and their functionalities.

Activity Results

1 Attack route visualization

In the attack route visualization phase, we create a graph that depicts the probable attack routes of potential threat actors by collecting and mapping vulnerabilities and potential vulnerabilities from different data sources.

Most customers purchase a package that includes manual assessments, enabling us to create and enrich the visualization

2 Cyber risk quantification

Based on the attack graph and the expected cost of breach, Hyver calculates:

- Probable exposure of the organization and resulting business impact
- Benchmarking against industry competitors
- Risk over time and maturity of the organization

3 Maturity calculations

Based on the results of the review and the questionnaire filled in by the customer, the platform determines the cybersecurity maturity score of the organization. The scoring is based on the NIST cybersecurity framework.

4 Mitigation optimization (add-on)

Once concluded, the findings and the graph are reviewed with the customer, and mitigation activities are proposed and prioritized through a mitigation workshop and later in the ongoing phase. You will be able to prioritize your remediation strategy according to risk and outcome.

This stage includes:

- Hyver recommendations: risk reduction through mitigation and prioritization
- Defining work plan and follow-ups

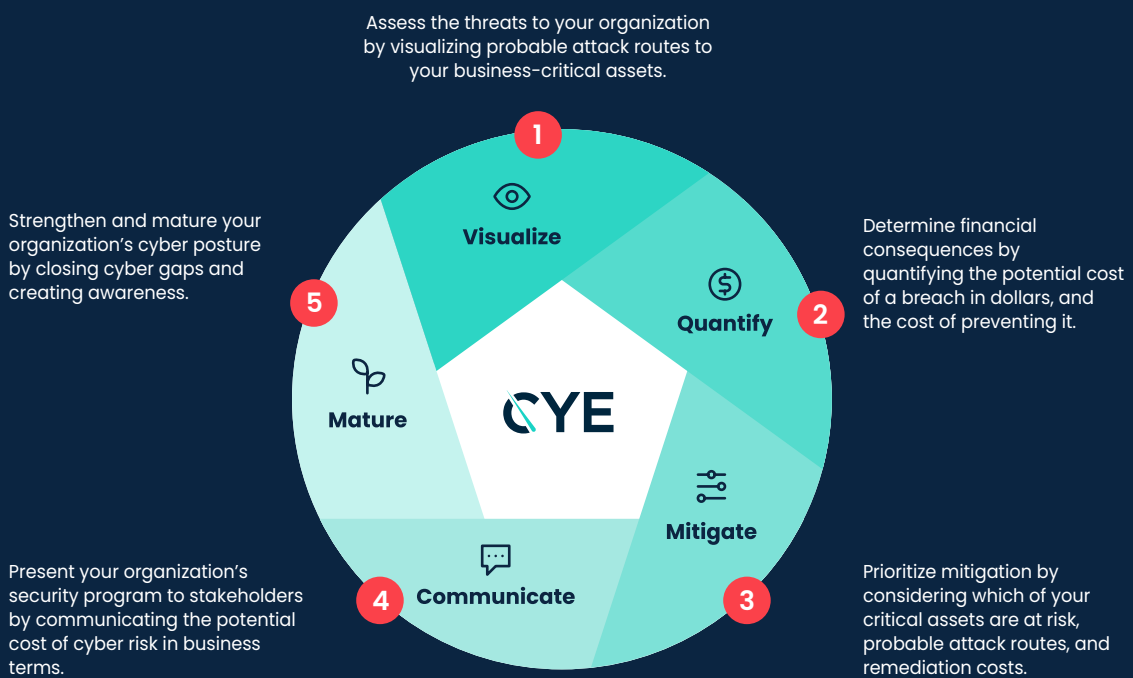
Ongoing

During the entire engagement time, we will have weekly or bi-weekly sessions to plan the activities and sync about the progress. In addition, we will have quarterly or bi-annually strategic meetings to follow the improvement in the organization's maturity and the reduction in the security risk.

Hyver Customer Engagement Flow

Summary

With CYE's comprehensive cyber risk assessment, organizations can visualize attack routes, quantify cyber risk, create mitigation plans, improve communication, and mature organizational cybersecurity posture.



About CYE

CYE's optimized cyber risk quantification platform and expert guidance transform the way organizations manage cybersecurity. Using AI, machine learning, and innovative technology, CYE visualizes attack routes, quantifies, mitigates, and communicates cyber risk, and matures organizational cybersecurity posture. In doing so, CYE provides clear and relevant insights that empower companies to make effective cybersecurity decisions. The company serves organizations in multiple industries globally. Founded in 2012, with headquarters in Israel and operations around the world, CYE is funded by EQT Private Equity and 83North.

Visit us at **cyesec.com.**

www.cyesec.com | info@cyesec.com