CYE's Optimized Cyber Risk Quantification

A comprehensive solution to improve organizational maturity and reduce risk.

Customer Engagement Flow

General

As cyber breaches continue to escalate, ensuring robust cybersecurity has become a paramount concern for enterprises. CYE 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 will 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. **Technical interview**
   This phase aims 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, etc.

3. **IR engagement Readiness**
   In this session, we define the IR processes and the communication channels and protocols that will be used in case of a cyber emergency.

4. **Threat Modeling**
   Threat modeling process includes a threat intelligence led activity to identify the potential threat sources to the organization, the organizational protection objectives and business critical assets, and proactive prioritization of the threat actors and business critical assets. This process will be the foundation for the attack route discovery and attack graph construction.

5. **Data collection**
   In this phase, we collect the initial data and integrate with the customer technologies. This phase includes:

   a. Enabling some of the automation capabilities of the product
   b. Updating financial data with the "Cost of Breach" questionnaire product

6. **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.

Organizational Cyber Risk Assessment

The goal of CYE's comprehensive organizational cyber risk assessment is to determine the extent of cyber risk that an organization faces, as well as its likely business impact. The assessment includes several steps:

1. **Scoping meeting**
   a. Defining the goals, the scope, the targets, the use cases to be tested, and the approach of the assessment
   b. Defining communication channels and processes for communication
   c. Defining the rules of engagement

   All the above are summarized in a "scope sign-off document."

2. **Baseline assessment**
   In this phase, CYE's red team simulates the threat actors according to the plan, trying to detect vulnerabilities, exploit them, and demonstrate the potential impact on the organization.

   The duration of the assessment is about 6-8 weeks. During this period, we have ongoing meetings to sync about progress. Critical findings (which can be exploited from the internet) are reported immediately.

3. **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.

4. **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

5. **Maturity calculations**
   Based on the results of the assessments and based on 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.

6. **Mitigation optimization**
   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 make optimized mitigation decisions based on outcome. This stage includes:
   - Hyver recommendations: critical to block, immediate action
   - Expert mitigation workshop
   - Defining work plan and follow-ups

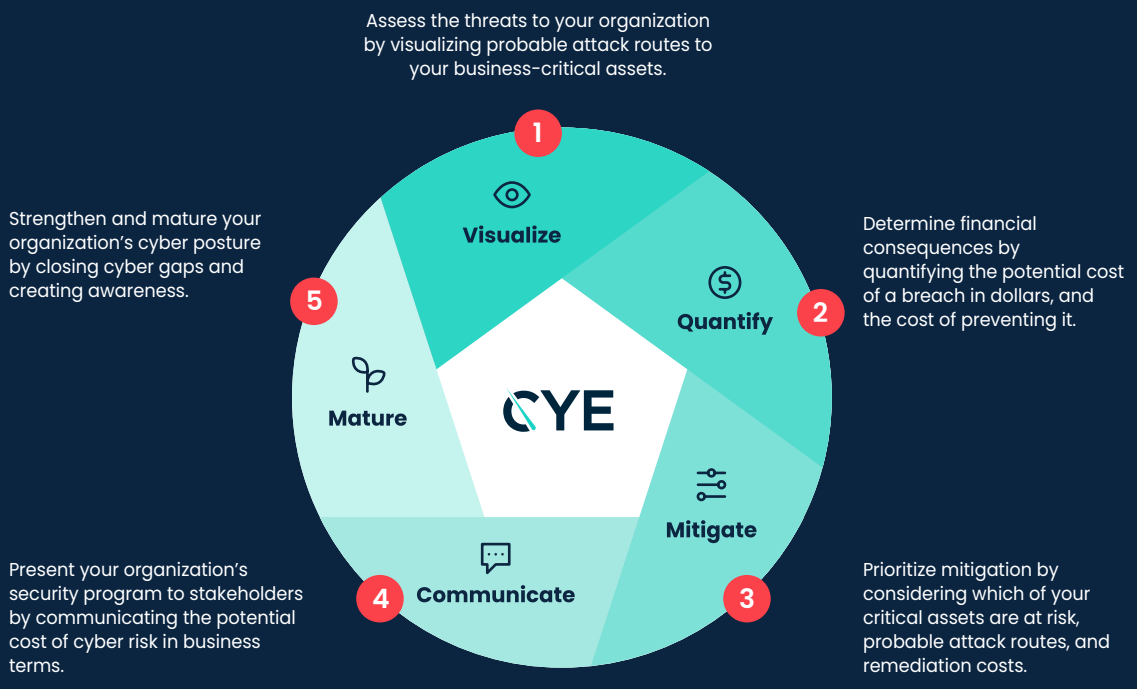
Ongoing

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.

Customer Engagement Flow

Summary

With CYE's comprehensive cyber risk assessment, organizations can visualize attack routes, quantify, mitigate, and communicate cyber risk, and mature their 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