The Guide to Outsmarting Hackers

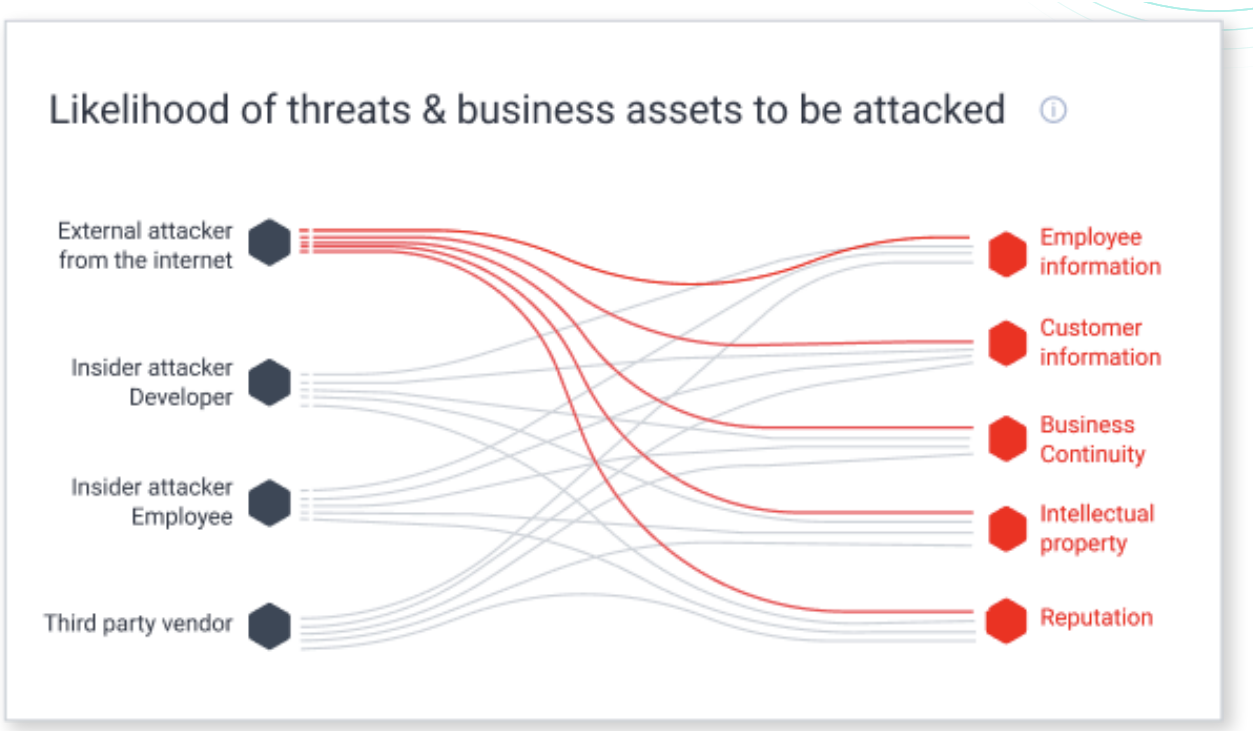
An overview of CYE's offensive approach to cybersecurity

The Challenge

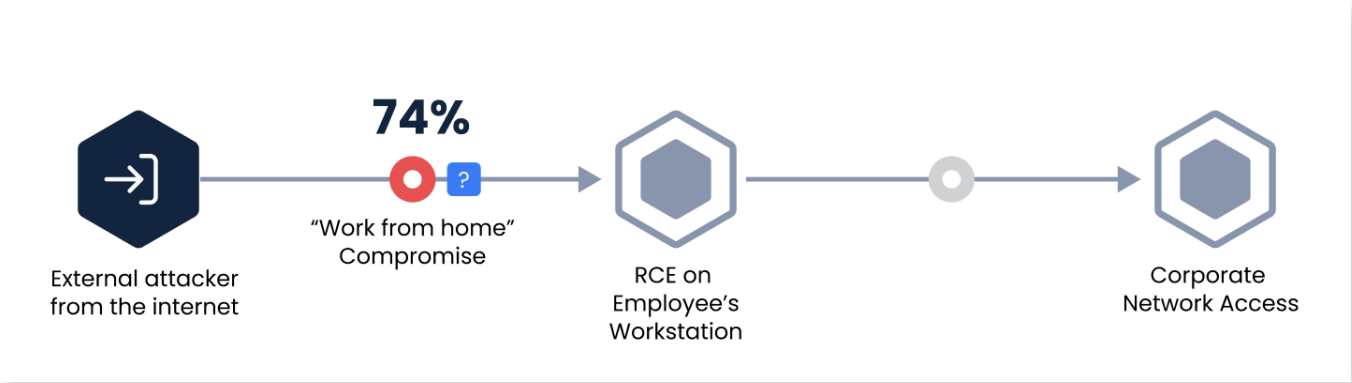
Organizations face an ever-evolving cybersecurity threat, which presents a constant risk to the organization's business critical assets that can negatively impact the business in numerous ways, including business continuity and reputation. In the past, security leaders were expected to always have a clear answer to the question of, "How secure are we?" Recently, however, that question has evolved to, "Are we optimizing our resources and investments effectively?"

The answer tends to be elusive. While attackers just need to identify and exploit a single vulnerable path, an organization needs to identify and defend all possible paths—a much more difficult task.

Minimizing this risk is also challenging because the attack surface of an organization is vast and ever-expanding, whether it's due to size and growth, technology stack, remote locations, or cloud presence. Focusing on the Internet perimeter—even though it's the first line of defense—is not enough, because threats can be originated from the inside as well, such as from a compromised employee's workstation or as part of a supply chain attack.



For example, an employee's workstation can be compromised when working from home by unintentionally downloading malicious files. Another example is a compromised personal home computer that is also used for work purposes, such as what occurred with the recent LastPass breach. These situations immediately bypass all internet perimeter measures and puts the attacker in a privileged position—the same as the compromised employee.



Assessing the organization can reveal a large amount of findings and vulnerabilities, but because of limited resources, security teams must decide where to prioritize efforts while considering cost, time, available personnel, and more.

Currently, many organizations use severity to prioritize their gaps, but this approach is missing the more complex context: determining how vulnerabilities can be exploited by an attacker and how this will impact the organization. This is not always a straightforward deduction.

The Data-Driven Approach

At CYE, we've developed an advanced, data-driven approach. Red teams assess organizations in a structured and methodology-based manner to anticipate attackers' steps. This is combined with additional vulnerability data collected by different tools, scanners, and connectors to the environment. Our cybersecurity optimization platform, Hyver, then models the security gaps of the organization into an attack graph, which is later analyzed using graph algorithms to suggest an optimized way to prioritize mitigation.

To outsmart hackers, Hyver prioritizes mitigation that reduces the overall risk, which directly results in decreased probability of attack routes being exploited. If we cut all routes and focus on the riskiest paths first, we systematically make it more difficult for attackers to breach the organization, cause them to spend more effort and resources on the attack, and encourage them to move on to more attractive and easier targets. This also gives the SOC (Security Operations Center) more time to catch the attackers.

Hyver's graph model (Figure 1) is built using "positions" and "edges." "Positions" are capabilities that an attacker gains while progressing deeper into the organization, and "edges" represent progress between these positions by exploiting different security vulnerabilities or the natural capabilities that result from them. Each edge also has "probability," which represents the probability of an attacker for exploitation and moving from one position to another. The probability is based on several parameters, such as attack complexity and its popularity.

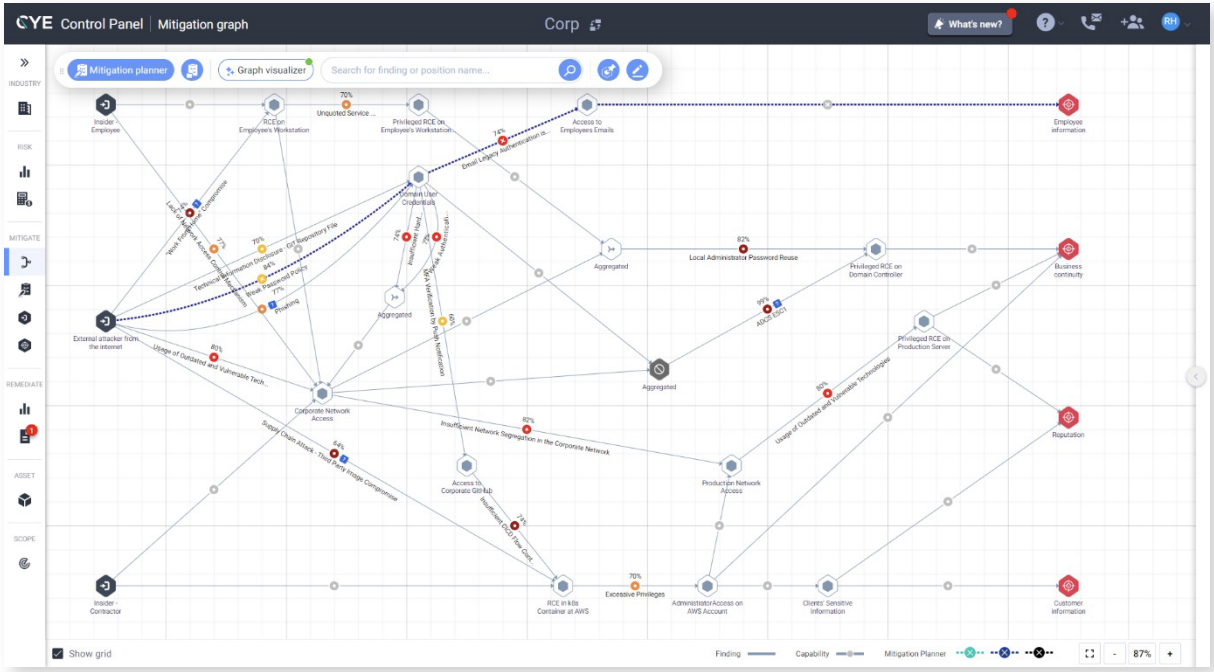


Figure 1 - Organizational attack graph

For example, an external attacker threat source gains “corporate network access” position, due to a vulnerability in the VPN, which is under the “usage of outdated and vulnerable technologies” finding. We can see in the image below how this is represented in the graph model. We can also see the recommendation to mitigate this issue, as it is part of a route which can result in negative business impact.

The initial attacker positions, depicted as black hexagons on the left of Figure 1, are defined by the organizational threat sources, which are both common (“External attacker from the internet”) and specifically designated to the assessed organization, such as contractors with custom privileges in the organization. The business-critical assets, which are depicted as red hexagons on the right of Figure 1, are the “targets” of the attacker that the organization wants to protect, and their compromise is connected directly to an impact on the organization, such as the clients’ privacy, the organization’s reputation, or its business continuity.

This model also includes recommendations for mitigation that can fix or minimize one or more edges on the graph, and each recommendation has cost and effort parameters based on cyber risk quantification.

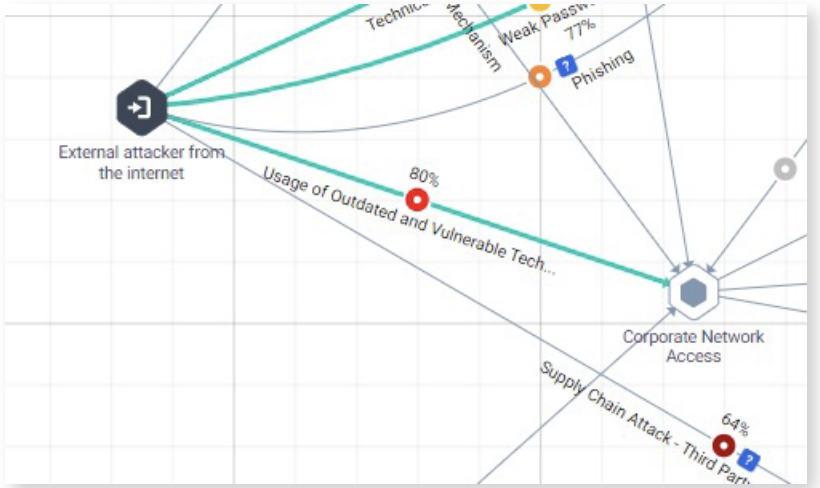


Figure 2 - An external attacker gains "corporate network access" position, due to vulnerability in the VPN product

Building this model takes a lot of effort. At CYE, we've defined several sources for this data:

- **Tactical edges,** representing actual findings/vulnerabilities that were identified and abused during an assessment.
- **Potential edges,** which are separated into different types:
    - Edges representing possible risks that needs to be taken into consideration as part of a risk management, such as possible compromise of an internet-exposed machine, due to a new vulnerability ("assume-compromised" approach)
    - Edges based on organizational observed "behavior"; for example, when observing Domain Admin sessions on specific organizational workstations, it is safe to assume that they can be found on other workstations as well.

- **Common paths edges,** representing high-level edges and paths on the attack graph, showing possible routes on non-assessed areas in the organization. These edges are based on:

    - Common vulnerabilities that were exploited in many engagements on similar environments.
    - Recent trends in cybersecurity (e.g., ADCS vulnerabilities)
    - TTPs (Tactics, Techniques and Procedures) of known APTs (Advanced Persistent Threats), which can be customized to the industry of the assessed organization.

The Hyver algorithm aims to cut all paths that lead threat sources to business-critical assets, while prioritizing mitigation by minimizing cost and effort with maximized overall organizational risk reduction.

The Result

One of the CISO's most important goals is to prioritize the mitigation that most effectively reduces cyber risk while optimizing available resources and achieving the highest return on investment. For example, DLP (Data Loss Prevention) may be hard to absolutely mitigate; it usually interferes with business operability and may require a considerable amount of organizational resources to implement. In such a case, it might make sense to spend these resources on a deeper defense layer, such as data compartmentalization, access control, and monitoring. This doesn't mean that the DLP vector should be ignored; it just means that it will be prioritized only when it's the most beneficial. When you can quantify the alternatives, it makes it easier to communicate such decisions to the board and to employees.

By representing the common routes, this same algorithm can also provide insights such as which areas to assess, harden, or monitor more thoroughly, based on common trends and threats.

In Figure 3, we see the recommendation to fix the findings, which will result in cutting all routes from threat sources to business impact.
By providing a clear understanding of organizational risk based on data, we can focus on prioritizing the right mitigation that provides the most benefit to organizational security posture while effectively utilizing existing resources. Using this approach, we protect organizations, optimize resources, and significantly reduce the likelihood of cyber incidents.

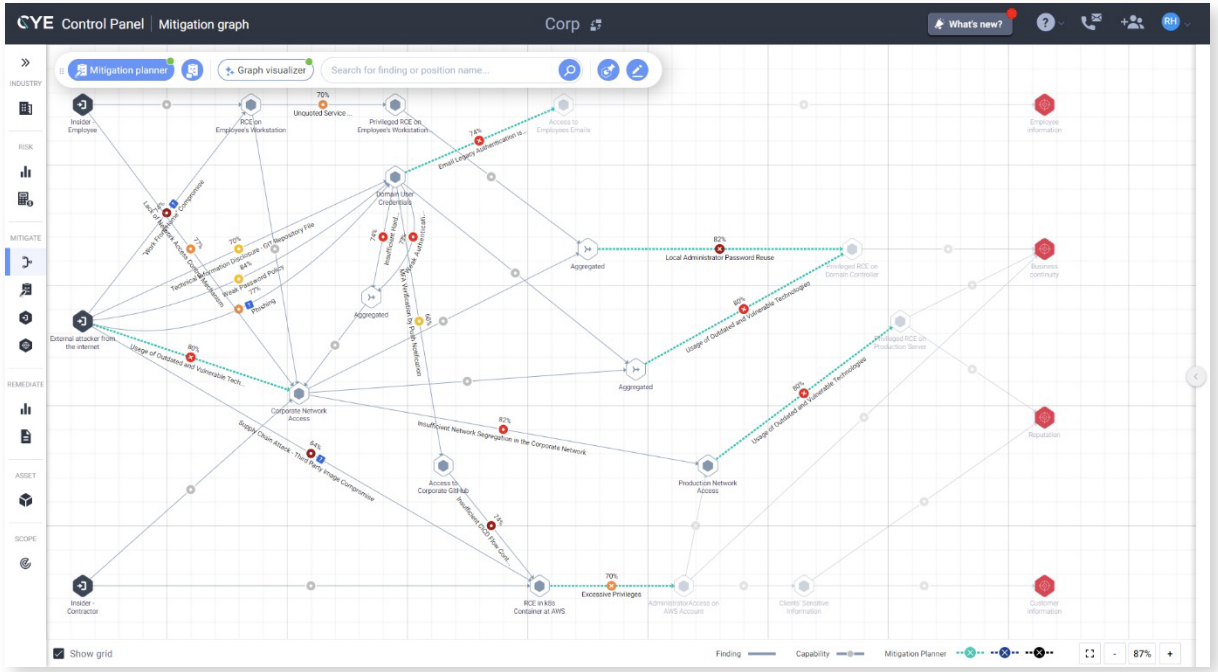


Figure 3 - "Critical-to-block" findings

Want to learn more about how CYE
protects organizations from cyberattacks?

Contact us

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 cutting edge technology with dedicated professional guidance and services provided by world-class 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 cyesec.com.