Technical Paper

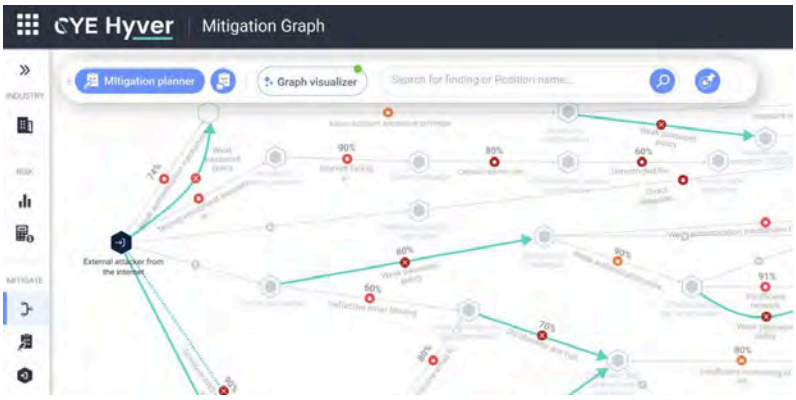
Calculating Edge Probability in CYE's Mitigation Graph

CYE's Mitigation Graph

At CYE, we use a mitigation graph to illustrate an organization's exposure to different threat scenarios. The graph outlines all the possible attack routes that may be exploited by an attacker to gain access and control of critical business assets in the organization.

A key feature of CYE's mitigation graph is the prioritization of threats, based on the probability of their occurrence, along with the impact of compromising an asset. This reflects the basic nature of risks and exploitation: Hackers are opportunistic and will find and attack through the path of least resistance, and this translates to our threat prioritization model.

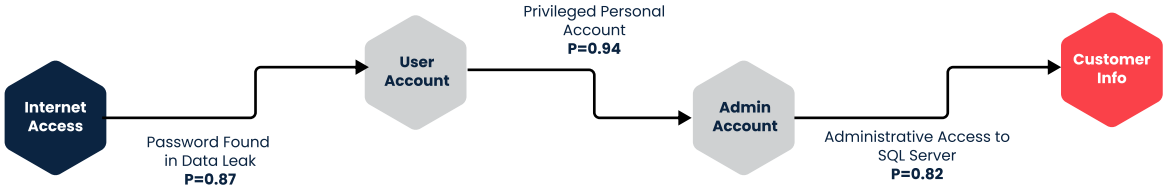
The probability of an attacker's route is calculated according to the findings that would be exploited on that route.



Attack route example:

Attack flow:

- An external attacker initiates the attack from the internet
- Access through an employee's password, which was obtained from a previous data leak
- Gains access to a user account
- Leverages high privileges of the user
- Reaches an SQL server
- Gains access to private customer information



Route probability calculation:

The overall probability of the route is a product of the probability of the findings; i.e., 0.87 x 0.94 x 0.82 = 0.67. This probability, along with the business impact of a compromised "customer info" asset (be sure to ask us how we calculate the cost of a breach), is used to prioritize the mitigation of findings on that route.

Therefore, if our optimized mitigation algorithm determines that mitigating the "privileged personal account" finding will produce the most overall decrease in organizational risk, it will suggest it as a high priority mitigation action that will disconnect the entire route.

CVSS is Impractical for Assessing Organizational Risk and Prioritizing Mitigation

The Common Vulnerability Scoring System (CVSS v.3.1) is often referenced as a means for quantifying the severity of vulnerabilities and the risk they pose. However, it was designed as a standard for communicating the characteristics and severity of software vulnerabilities specifically. Despite featuring some factors which are useful in quantifying risk, it is an impractical approach for assessing organizational risk.

CVSS is meant to classify and rate individual vulnerabilities for specific assets. For the example in Fig. 1, if we try and use CVSS to assess risk, we would need to produce a vector string for each of the three findings (e.g., CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) and then attempt to chain them together by identifying recurring metrics like attack vector or confidentiality, remove them from each of the vectors and reason about where they should be placed, and whether they need to occur more than once. The issue is exacerbated in cases where some aspect or metric of the chain of vulnerabilities changes (which is often the case in a rapidly changing threat landscape), requiring the analyst to repeat the entire process. Ultimately, the concept of a multi-stage attack is not well defined in CVSS, making it an impractical tool in this setting.

Another drawback is the inability to effectively reason over impact to business-critical assets. CVSS eventually produces a number ranging from 0-10, which is completely detached from the organization's business context for the asset being compromised in the attack. This often results in wrong mitigation prioritization, as the most severe vulnerabilities are almost always addressed first, instead of the most impactful ones.

Mitigation Graph Edge Probability

A key pillar of our methodology is the specific finding probability. We must be able to accurately quantify the likelihood of a finding, which is akin to assessing the overall probability of it being exploited, to produce a truly optimized mitigation plan.

Probability Estimation Factors and Models

Our model for computing finding probability relies on various internal factors such as in-house CYE knowledge, threat analysis and tools; and external factors such as global cybersecurity trends, community knowledge, exploits publication, etc. To illustrate approach, here are some of these factors (specifically those that are partially based in CVSS):

Factor Name	Description
Finding Complexity	The amount of effort and general level of know-how required for successfully exploiting the finding.
User Interaction	Does the attack require any sort of user interaction, whether it be passive (i.e., requires an operation that is routinely performed) or active (i.e., actively engaging the user)?
Exploitability	The availability and readiness of external tools and exploits required for successful exploitation.
Finding Popularity	Are we seeing high usage level, or a trend indicating the finding is on the rise?

Each probability factor is approximated using our data models. It's important to note that the approximation is continuous, thus at any given moment the mitigation graph contains the most up to date probability of each finding.

Conclusion

CYE's mitigation graph algorithm is a simple yet powerful way of prioritizing mitigation. It is based on well-known and established public methodologies, as well as tried and tested techniques and data gathered over years of security assessments performed by CYE.

Want to learn more about how CYE can help you with cyber risk quantification and mitigation optimization? Contact us.

About CYE

CYE's exposure management platform, Hyver, transforms the way security teams protect their organizations. With CRQ at its core, the platform reveals enterprises' exposure in financial terms, visualizes the most exploitable attack routes to critical business assets, and creates mitigation plans tailored to each business. CYE's customized reporting enables the sharing of vital board-level metrics and validating exposure reduction over time. In addition, CYE improves cybersecurity maturity by mapping weaknesses and defining targets based on industry frameworks. Founded in 2012 in Israel with operations around the world, CYE has served hundreds of organizations across industries globally. Visit us at cyesec.com.

© 2025 CYE, All rights reserved. www.cyesec.com | info@cyesec.com
1000 North West Street, Suite 1410, Wilmington DE 19801, United States
1 Ballards Lane, London N3 1LQ, UK | Abba Eban 10, Herzliya 4615200, Israel