Compound risk metrics

Explore this new metric type in the Panaseer platform. They combine metrics from across multiple security domains to identify and fix toxic combinations.

92% of security leaders agree that toxic combinations are a cause for real concern.

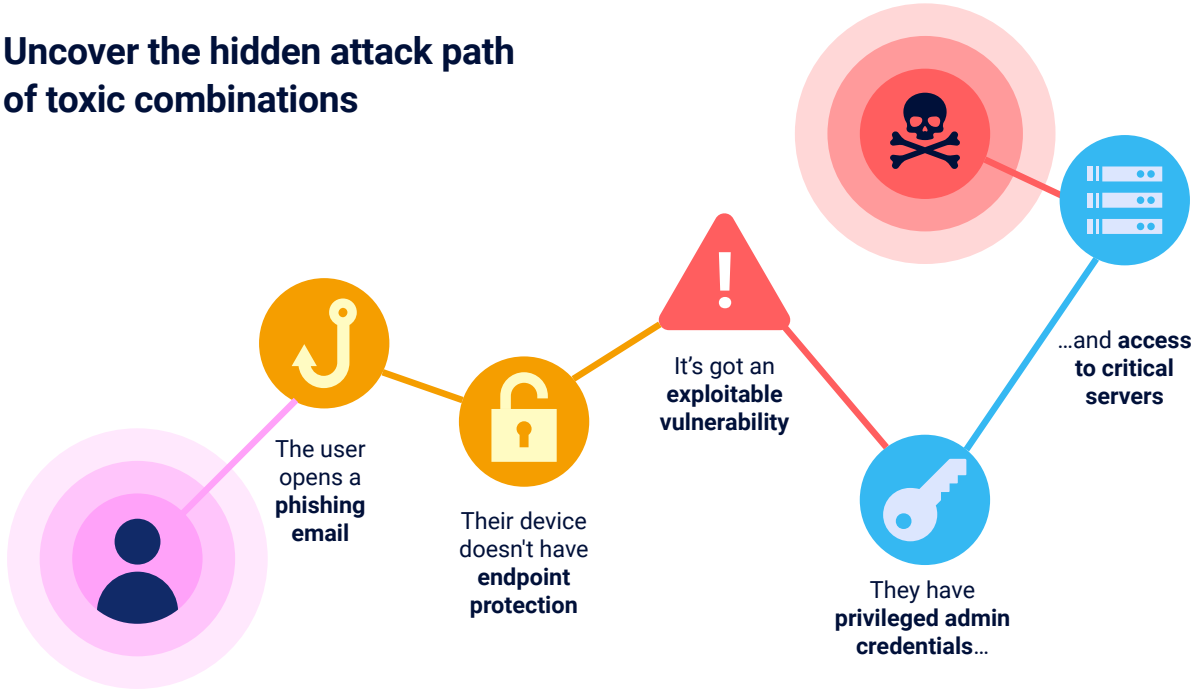
Panaseer 2025 Security Leaders Peer Report

What are toxic combinations?

The term “toxic combinations” originates in pharmacology, where two drugs can combine to inadvertently harm the patient. In the context of cybersecurity controls, it means a combination of control gaps relating to the same asset. Alone, each control gap is a small risk, but combined, they can be a major cause for concern. This is exactly the kind of thing threat actors will look to exploit.

The threat actor can craft and send a convincing phishing email that the user clicks, inadvertently executing malware that takes advantage of the unpatched vulnerability. The attacker can then use the elevated privileges the user has to disable security tools, modify configurations or access sensitive files.

Uncover the hidden attack path of toxic combinations



Operational challenge: The current approach

Most security teams prioritize based on severity within individual tools. They struggle to identify, let alone address toxic combinations that span multiple security domains.

They would typically need to analyse data from multiple tools across security domains and apply that to attack paths while factoring in how assets interact across the network. This is typically a slow, labor-intensive, manual process.

The solution: Compound risk metrics

Compound risk metrics enable users to combine analysis from across multiple security domains. This allows them to identify toxic combinations and prioritize them for remediation.

- Get actionable analysis across multiple security domains.
- Prioritize remediation to identify risky users and at-risk assets.
- Measure effectiveness of compensating controls to cover known control gaps.

Compound risk metrics use cases

Device focus
The most common use case for compound risk metrics is identifying vulnerabilities on devices that are missing from individual tools, usually a combination of EDR, AV, and CMDB. This data is drawn from multiple tools across domains, so isn't readily available in a typical tool. In Panaseer, these metrics are out-of-the-box.

People focus
Identify toxic combinations on devices owned by people who have recently failed phishing tests. Combine data from vulnerability management, endpoint management, and user awareness domains to uncover these hidden risks.

Business focus
Combine data from device and application domains to identify all your devices that are hosting business critical applications. By prioritizing these devices for protection and remediation, you can focus your resources on securing the devices that are most crucial to your critical business applications and processes.

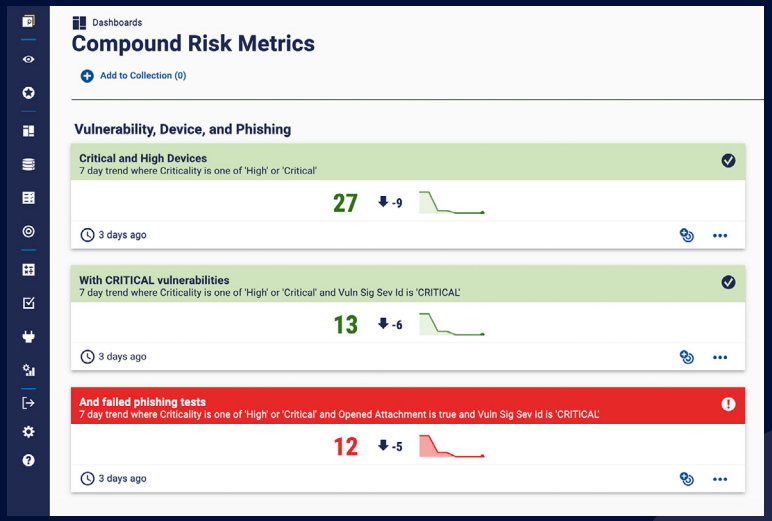
Compensating controls

Security tools can't always provide complete coverage. If a device doesn't have one particular protection in place, it must have another to compensate for the risk. In this scenario it's critical to understand how well other cyber controls are helping to protect those assets.

Compound risk metrics give you the ability to measure how many of these assets aren't covered by other controls. An organization might measure compensating controls as a compliance or policy metric. For example, this could be aiming for non-EDR compatible devices to be 100% covered by a combination of compensating controls.

For example, you can use compound risk metrics to answer this question: *"For assets where we cannot install CrowdStrike, how many are covered by a recently authenticated Tenable scan and have no detections?"*

Empower your dashboards



These metrics are automated, which means reduced manual effort and time saved for your security team. Like all metrics in the Panaseer platform, these metrics are actionable, so a few clicks can start the process of fixing the problem.

Compound risk metrics are designed to empower your existing security dashboards in Panaseer. For example, you can add value to your vulnerability management dashboard with contextual data on endpoint, inventory, patching, user awareness, or privilege.

While this example dashboard focuses on compound risk metrics, you can add them to any other dashboard. For example, you can empower your vulnerability dashboard with context from your user awareness program. And vice versa.

To learn more about compound risk metrics, get a personalized demo at panaseer.com/book-a-demo