PRODAFT

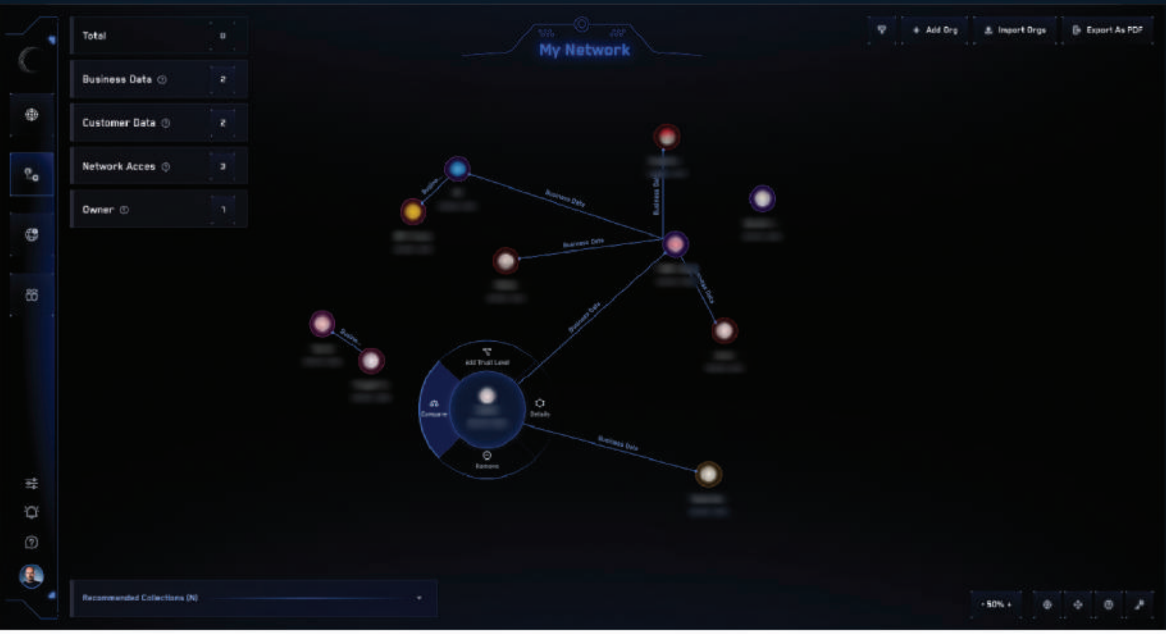
BLINDSPOT

THE ART OF ANTICIPATION

ABOUT PRODAFT

PRODAFT is a pioneering threat intelligence company reframing the approach to proactive cybersecurity since 2012. With our focus on creating a difference through long-lasting expertise enhanced by timely insights, we have aced our solutions to empower you with actionable intelligence that is tailored to fit your unique needs.

With our unmatched understanding of the adversarial landscape spanning over decades, we keep serving various industries and brands across the globe. By bringing in more accurate intelligence and taking away your team's workload, we ensure all challenges are addressed beforehand. Simply put – successful mitigation before any detrimental compromise.



WHAT IS BLINDSPOT?

BLINDSPOT is a **next-generation risk intelligence platform** that has been created with the goal of providing the user with a holistic assessment of any organization's cyber risk level. Supply chain attacks have been steadily on the rise, putting companies globally in a difficult position. Cybercriminals always want to find the least time-consuming path to execute their attacks, and in their quest to do so, they tend to compromise the suppliers of the targeted company first. However, companies cannot monitor their suppliers' security easily and comprehensively due to the nature of infrastructure and cloud complexities. And that means one thing: **unwillingly handing the threat actors an unobstructed path to move forward.**

To minimize these cybersecurity risks and ensure the full protection of the supply chain, the EU adopted the **NIS2 directive**. Aimed at improving the resilience and cybersecurity capabilities of EU Member States, the directive needs to be transposed into national law by October 2024. The management bodies of essential and important entities oversee the implementation of this directive and can be held liable for its violation and non-compliance. This reality prompts many organizations to ramp up their cybersecurity forces yet leaves them unsure about **how to efficiently comply with the regulation.**

BLINDSPOT gives you the **capability to smoothly tackle both issues**: the looming threat of supply chain attacks and much-needed compliance. Developed to equip you with a proactive upper hand, the platform allows you to monitor contemporary incidents and predict subsequent adversarial activities. By preventing software and physical supply-chain attacks and detrimental breaches, you ensure your security stays intact.

With BLINDSPOT's **unmatched coverage of cyber incidents** acquired right from the source, you can get instant visibility into an international supply chain and the intricate connectivity of all organizations globally. Effortless and concise, BLINDSPOT encompasses all the relevant insights you need for a **timely response to adversarial plotting** and to check the required resilience of your partners, buyers, or vendors.

KEY BENEFITS OF BLINDSPOT

1. **RISK ASSESSMENT BASED ON FACTS AND REAL-LIFE INCIDENTS**

   BLINDSPOT's next-generation AI can pinpoint the cyberattacks' root cause, providing you with an advantage over the defenders and affected organization's supply chain network – instead of facing any catastrophic consequences of an executed cyberattack.

2. **A FULLY COVERED THREAT LANDSCAPE**

   Every notorious adversary or other advanced persistent threat (APT) is instantly visible in the system, accurately calculating and adjusting the victims' risk value. The available information precedes the action, unveiling potential risk value even before any attack takes place.

3. **ACCURATE DISPLAY OF BLIND SPOTS AND NEVER-SEEN-BEFORE OBSERVABLES**

   Weak links, technology-related vulnerabilities or any blind spots that normally go unnoticed will be available for you to see. By leaving nothing to chance, you can easily map out all connections and exposed weaknesses in your business circles, ultimately ensuring your resilience on all fronts.

4. **COMPREHENSIBLE AND TIMELY RISK VALUES**

   All the risk values are thoroughly explained, providing our clients with clear and concise data, not any generic information. By sharing valuable details on why, what and when we empower the users with 3A intelligence – accurate, agile, and actionable. Ensuring compliance by first-class resilience has never been easier.

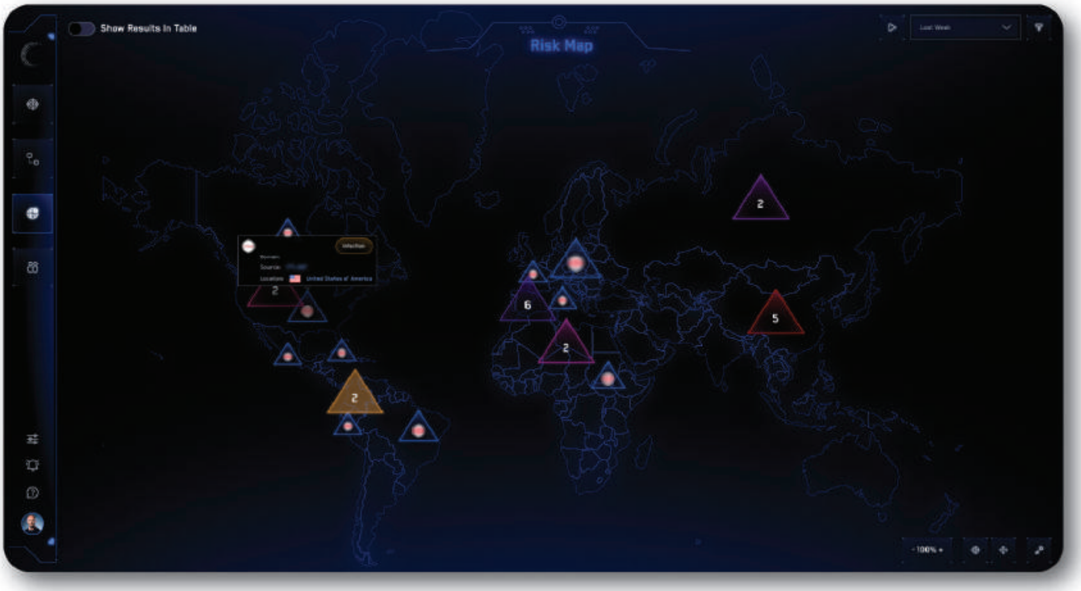
5. **EARLY WARNING SYSTEM**

   Distribution of an early warning regarding future attacks within the platform ensures that you are well-informed about any compromise headed your way. Instead of dealing with the ramifications of cyberattacks and preparing lengthy NIS2-compliant incident reports, you can mitigate next-generation threats in advance.

WHAT MAKES BLINDSPOT UNIQUE?

Unlike other cyber risk quantification platforms doing port scanning, technology tracking, or deriving information from basic compliance checks, BLINDSPOT gives you the ability to **see actual infections in real time**. Instead of conducting a vulnerability assessment or Attack Surface Management (ASM), the risk values are calculated based on facts – not mere assumptions or vulnerabilities that cannot determine the full picture.

With the **power to predict the next moves of your adversaries**, you don't need to be afraid of weaknesses that could cause you irrevocable damage or compromise your compliance with the NIS2 Directive. Instead, BLINDSPOT allows you to see an already-established connectivity graph with the risk networks that are relevant to your organization. You can always adjust the intelligence sources via your Priority Intelligence Requirements, depending on your unique needs and objectives.

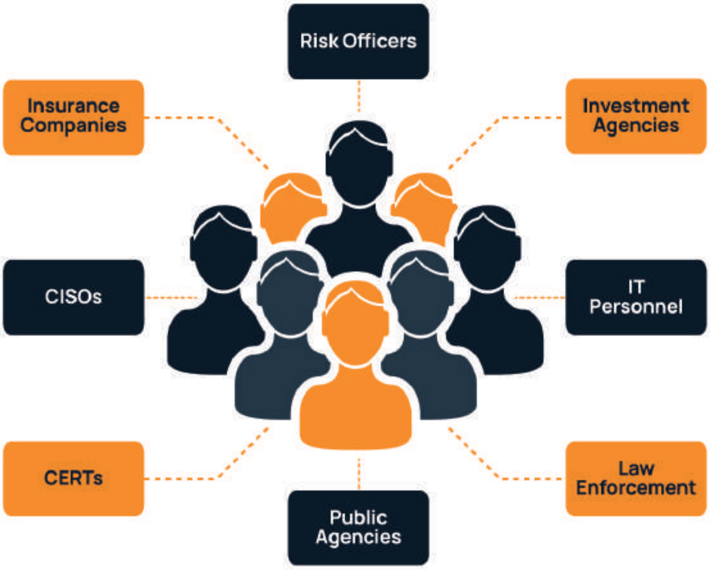


WHO IS BLINDSPOT MEANT FOR?

Providing game-changing insights, BLINDSPOT can calculate the risk values of **enterprises, governments, NGOs, educational institutions, vendors and suppliers, or their customers.**

Are you an **essential or important** service provider in the European economy? If you fall in any of these categories, then you're aware that your compliance with the NIS2 Directive is mandatory - meaning BLINDSPOT would be a great fit for you.

The platform is meant for a wide variety of stakeholders, such as (but not limited to):



The platform allows you to scrutinize your business supply chain partners' (and their suppliers') exposure to cybercrime - with immediacy and a precise threat-actor coverage ratio.

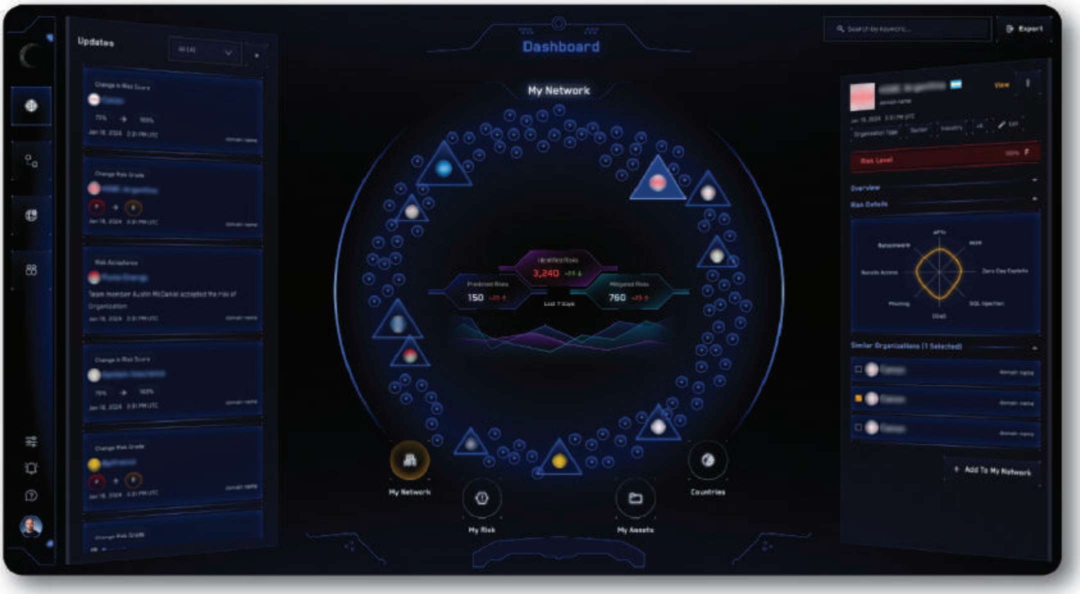
With BLINDSPOT you no longer need to calculate the company risk based on external information – oftentimes outdated and inaccurate nevertheless – but assess the risk based on relevant variables. We believe that factors such as infection rates, malspam campaigns or ransomware efforts provide more valuable information **to understand your or third party's exposure to serious cyber risks**, allowing you to better address those challenges within one solution.

WHAT ARE THE CORE TECHNOLOGIES OF BLINDSPOT?

Our sources present a mixture of human, communication, and open-source intelligence, along with various intelligence-gathering tools and mechanisms. They allow us to monitor the adversarial infrastructures and communication platforms of cybercriminals.In this way, we can provide our clients with the most timely and relevant information right from the source.

Our core technologies are:

- **Incident Prediction Engine (Oracle)** – ability to predict the incident using prior (precursor) events
- **Risk Propagation & Calculation Engine** – ability to propagate the individual risk within the connected entities
- **Attribution Engine** – ability to attribute incidents to organizations
- **What-if Analysis** - ability to compare various entities based on risk timeline
- **Trend Monitoring** - overseeing the trends of the threat actors and providing sectoral and regional insights



PRODAFT

RUINING THE SURPRISE OF CYBERCRIMINALS