PRODAFT

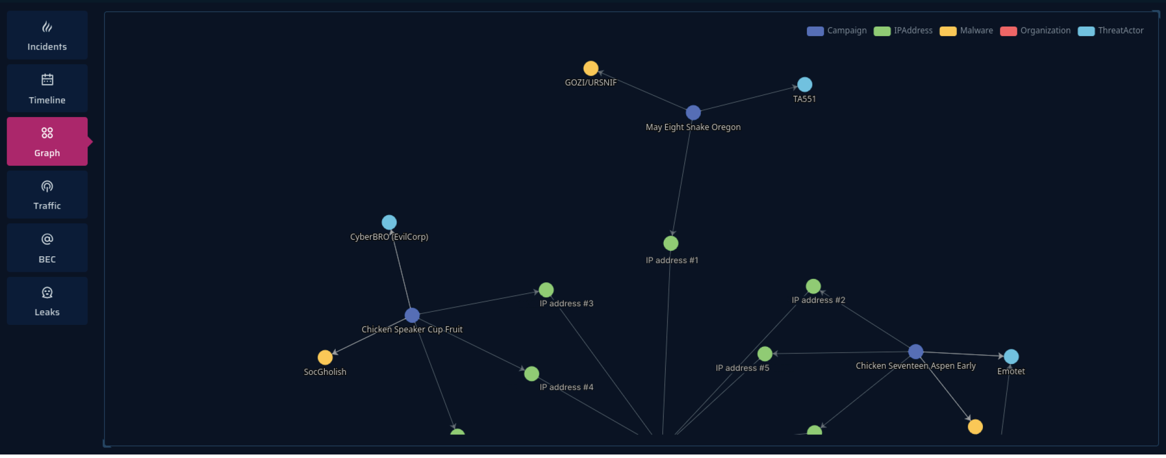
# BLINDSPOT

## 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.



# BLINDSPOT RISK INTELLIGENCE PLATFORM

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. Cybercriminals always want to find the least time-consuming path to execute their attacks, and in their quest to do so, they tend to 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.**

With the growing need to oversee these interconnected systems, BLINDSPOT was developed to equip you with a proactive upper hand. By monitoring contemporary incidents and predicting subsequent adversarial activities, our platform prevents software and physical supply-chain attacks and detrimental breaches worldwide

With BLINDSPOT's unmatched coverage of cyber incidents acquired right from the source, you can get instant visibility into an international supply chain and into 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.

# WHAT ARE THE KEY BENEFITS OF BLINDSPOT?

## 1 RISK ASSESSMENT BASED ON FACTS AND INCIDENTS IN REAL TIME

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 NEVER-SEEN-BEFORE OBSERVABLES

Weak links, Proof of Compromise (POC), breaches or 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.

## 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.

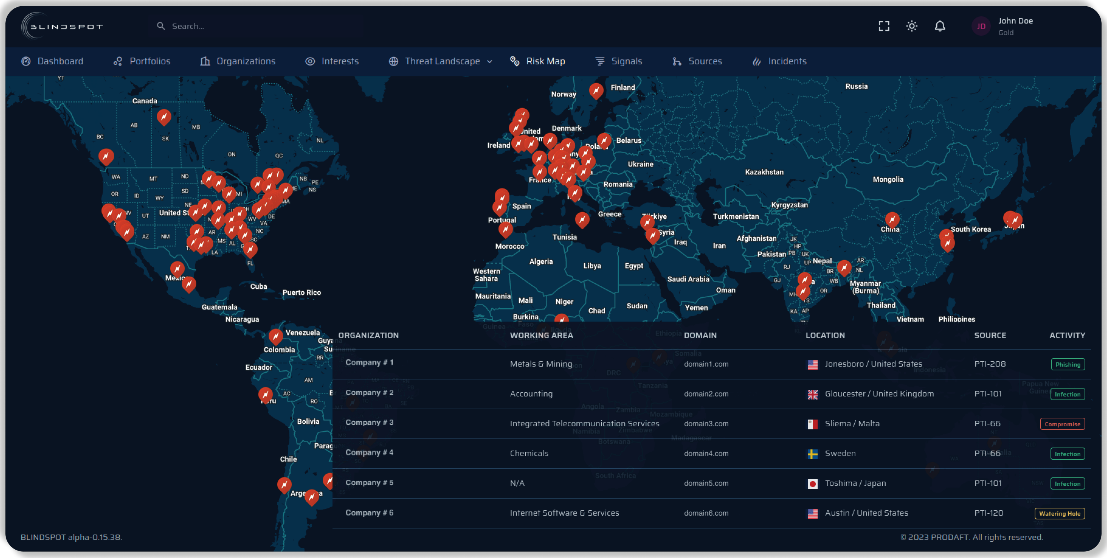
## 5 EARLY WARNING SYSTEM

Distribution of an early warning regarding future attacks within the platform ensures that you are well informed about any compromise headed your way. BLINDSPOT has been proven to warn users on average 2 weeks (up to 1 or 2 months) before the extortion takes place.

# 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. 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.



| ORGANIZATION | WORKING AREA | DOMAIN | LOCATION | SOURCE | ACTIVITY |
|---|---|---|---|---|---|
| Company # 1 | Metals & Mining | domain1.com | Jonesboro / United States | PTI-208 | Phishing |
| Company # 2 | Accounting | domain2.com | Gloucester / United Kingdom | PTI-101 | Infection |
| Company # 3 | Integrated Telecommunication Services | domain3.com | Sliema / Malta | PTI-66 | Compromise |
| Company # 4 | Chemicals | domain4.com | Sweden | PTI-66 | Infection |
| Company # 5 | N/A | domain5.com | Toshima / Japan | PTI-101 | Infection |
| Company # 6 | Internet Software & Services | domain6.com | Austin / United States | PTI-120 | Watering Hole |

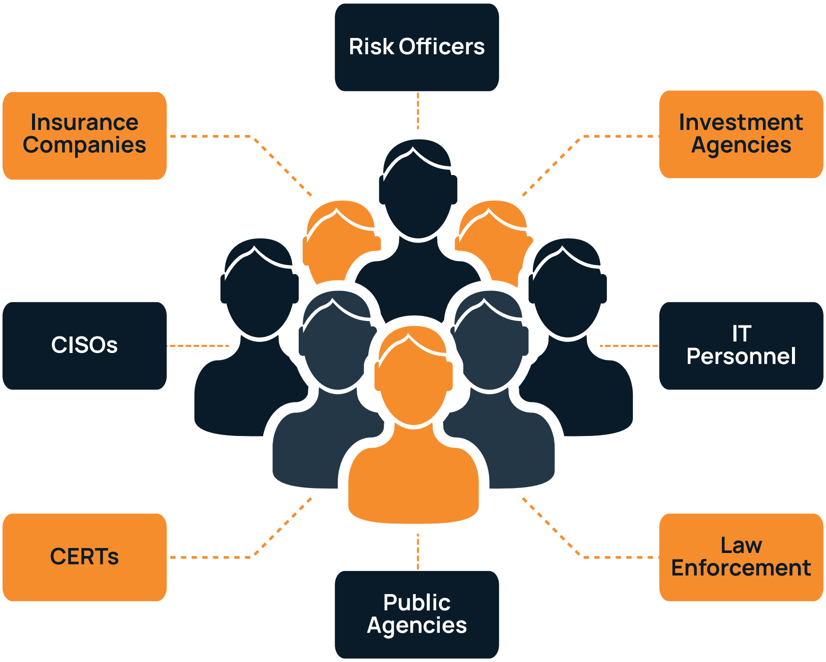
BLINDSPOT alpha-0.15.38.

© 2023 PRODAFT. All rights reserved.

# 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.**

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



Risk Officers

Insurance Companies

Investment Agencies

CISOs

IT Personnel

CERTs

Law Enforcement

Public Agencies

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.

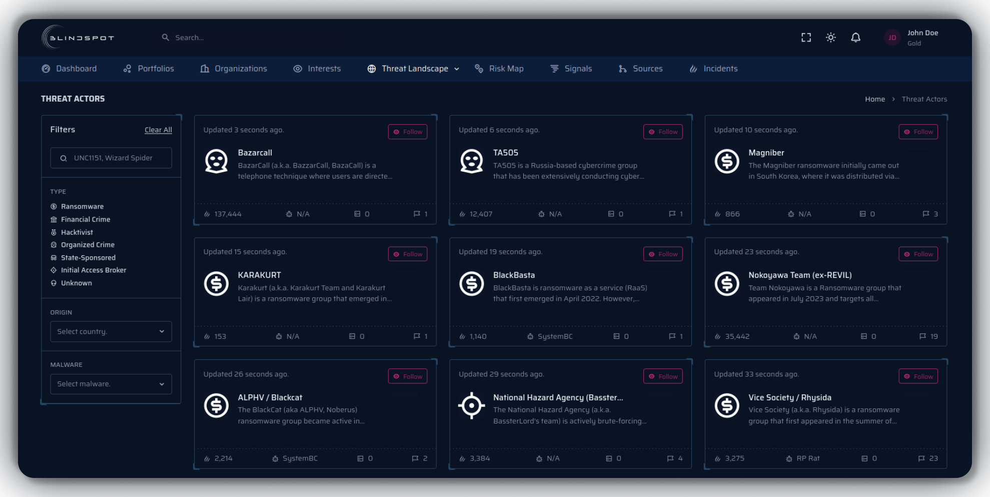
With BLINDSPOT you no longer need to calculate the company risk based on external information – oftentimes outdated and inaccurate nevertheless – but assess the risk based on relevant variables. We believe that factors such as infection rates, malspam campaigns or ransomware efforts provide more valuable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

# 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



Updated 3 seconds ago. Follow
Bazarcall
BazarCall (a.k.a. BazzarCall, BazaCall) is a telephone technique where users are directe...
137,444 N/A 0 1

Updated 6 seconds ago. Follow
TA505
TA505 is a Russia-based cybercrime group that has been extensively conducting cyber...
12,407 N/A 0 1

Updated 10 seconds ago. Follow
Magniber
The Magniber ransomware initially came out in South Korea, where it was distributed via...
866 N/A 0 3

Updated 15 seconds ago. Follow
KARAKURT
Karakurt (a.k.a. Karakurt Team and Karakurt Lair) is a ransomware group that emerged in...
153 N/A 0 1

Updated 19 seconds ago. Follow
BlackBasta
BlackBasta is ransomware as a service (RaaS) that first emerged in April 2022. However,...
1,140 SystemBC 0 1

Updated 23 seconds ago. Follow
Nokoyawa Team (ex-REVIL)
Team Nokoyawa is a Ransomware group that appeared in July 2023 and targets all...
35,442 N/A 0 19

Updated 26 seconds ago. Follow
ALPHV / Blackcat
The BlackCat (aka ALPHV, Noberus) ransomware group became active in...
2,214 SystemBC 0 2

Updated 29 seconds ago. Follow
National Hazard Agency (Basster...
The National Hazard Agency (a.k.a. BassterLord's team) is actively brute-forcing...
3,384 N/A 0 4

Updated 33 seconds ago. Follow
Vice Society / Rhysida
Vice Society (a.k.a. Rhysida) is a ransomware group that first appeared in the summer of...
3,275 RP Rat 0 23

PRODAFT

RUINING THE SURPRISE OF CYBERCRIMINALS