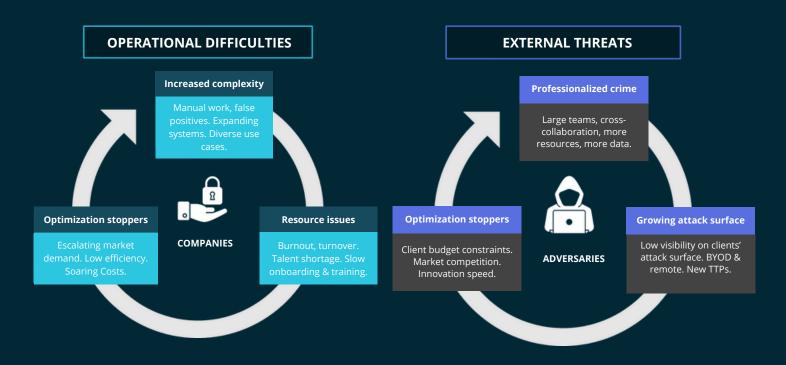


### Cybersecurity is getting harder

Security teams continuously face operational challenges, including excessive manual work, complex systems, and high false positive rates resulting in burnout and turnover. The difficulty in hiring and onboarding cybersecurity professionals hampers SOC optimization. Additionally, cybercriminals now operate with business-like strategies, demanding more resources and tools, while cybersecurity budgets remain stagnant. Consequently, Security teams must seek ways to optimize operations and safeguard an ever-expanding attack surface.



### Cyber Threat Intelligence is the key to prevent risks

#### Optimize MTTD and MTTR

Prioritize highly relevant alerts and correlate events with context-rich criminal information.

#### Reduce false positives

Enrich scoping and triage data to reduce noise and let analysts focus on genuine threats.

Connect the Dots
Built-in context: zero in on specific posts, threads and threat actors to uncover the full story.

## Dotlake: Exclusive open & deep web threat data

Dotlake provides real-time visibility to crucial criminal sources across the open and deep web, including ransomsites, fraud markets, telegram and invite-only forums.

Its advanced crawlers can access millions of darknet pages and its social engineering allows you to view the hidden contents of the forums **effectively** and **safely**.

Additionally, at Dotlake we have incorporated a series of **Addons** that provide you access to more than <u>66</u> billion of **Data Breaches** from the last 19 years to the current date.



**Immediate action:** Dotlake insights help you **avoid false positives** with built-in context and entity analytics that let you analyze and prioritize alerts more effectively.

A **flexible tool** that integrates with your existing workflow and lets you spot & manage the exposure of your digital assets in seconds.

## Access the data in 2 ways

#### **Easy-to-use API REST**

An API that integrates seamlessly with existing systems and allows the automation of reading results in a simple way through a structured JSON response.

#### **Dotlake Web Portal**

Users can access the full database through a web portal and use the query builder to retrieve data immediately.

- **Always on alerts:** DOT WATCH allows you to make automated queries to monitor your digital assets
- **Actor monitoring**: DOT PROFILING enables you to investigate and monitor actors that may pose a threat to your company.



### Use cases



#### Threat Hunting

Analyze threats against similar companies to prevent vulnerabilities.



#### Digital Forensic

Determine the chain of events that lead to an incident based on history from the time of the violation.



#### Digital Survillance

Monitor critical assets to detect exposures before they become a threat.



#### Risk Assessment

Continuously monitor for IOCs (credentials, IP addresses, domains, etc.).



#### Fraud Detection

Identify stolen credit cards, compromised banking information or logs with stolen credentials...



#### Third party Analysis

Get real-time visibility into the situation of your suppliers to safeguard your business.



#### **Brand Protection**

Protect your brand from abuse and reputational risk by minimizing financial losses.



# Tactics, techniques & Procedures (TTPs)

Monitor new TTPs and have your red team prevent attacks before they reach your systems.

