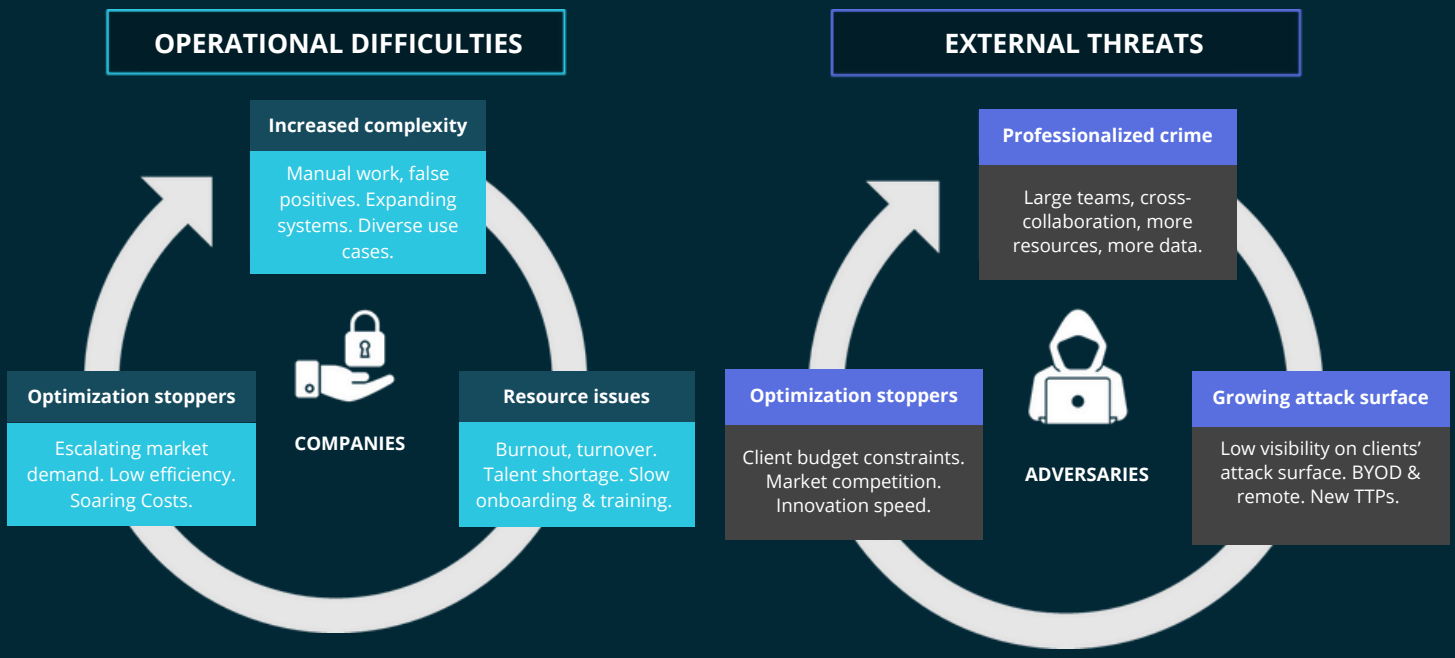
DOTLAKE

NEVER MISS A THREAT AGAIN

The Cyber Threat Intelligence solution that works for you

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 also access millions of pages from I2P, Tor and Freenet darknet networks. Dotlake enables users to access vital information effectively and safely.

RANSOMSITES I2P
CLOSED sources

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. This helps safeguard against potential risks.

Digital Survillance

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

Fraud Detection

Detect, prevent, and mitigate payment fraud to protect customers and business interests by identifying stolen credit cards, compromised bank information...

Brand Protection

Protect your brand from abuse and reputational risk. Minimize financial losses, mitigate potential damage to the brand, and regain lost customer trust.

Digital Forensic

Determine the chain of events leading to an incident with historical info from the time of the breach.

Risk Assessment

Enhance risk assessment with intelligence, identify emerging indicators, prioritize mitigation, and continuously monitor for improved accuracy.

Third party Analysis

Gain real-time visibility into the risk posture of third parties in order to safeguard the integrity of the business value chain.

Tactics, techniques & Procedures (TTPs)

Monitor new and trending TTPs and let red teams test them before they reach your systems.

info@dotlake.eu | dotlake.io