TRUESEC

Threat Intelligence: Leak Detection and Mitigation

What Is Leak Detection and Mitigation?

Your organization's sensitive data can end up in the wrong hands in many ways. Once leaked, cybercriminals can buy and sell information such as credentials or vulnerabilities in your IT environment that can be used to gain further unauthorized access. Cybercriminals will also often steal data and threaten to release it on the Darkweb.

Truesec utilizes its in-depth knowledge of the cybercriminal ecosystem and infrastructure to search for signs of your organization's sensitive data being released by cybercriminals into the wrong hands. We then help you take the necessary steps to stop breaches and mitigate attacks.

The Truesec Promise

Truesec is a purpose-driven cybersecurity company with extensive experience in the field of cyber threat intelligence. We possess in-depth knowledge of how cybercriminals operate and where to find information on the Darkweb. Armed with the knowledge acquired through Truesec's Threat Intelligence: Leak Detection and Mitigation service, your organization will gain a new level of security.

Your New Capabilities

- Minimize the impact of breaches
- Predict possible future attacks
- Protect your IT environment from further intrusions
- Formulate a measured response if you have already been breached and criminals have threatened to release your data publicly
- Identify and mitigate infringements on your corporate brand

About Us

As a global cybersecurity company, we're proud to be at the forefront of protecting organizations and our society against cyber threats. Our purpose has been clear since day one: Creating safety and sustainability in a digital world by preventing cyber breach and minimizing impact. We never cease to challenge and reinvent ourselves to help defend your most valuable data assets every day.

TRUESEC

A Safe Digital Future

Sweden	Denmark	US
truesec.com	truesec.com	truesec.com
+46 8 10 00 10	+46 8 10 00 10	(904) 900-4532
hello@truesec.com	hello@truesec.com	hello@truesec.com

If You Are Under attack, call Truesec

+46 (0) 8 10 72 00
incident@truesec.com

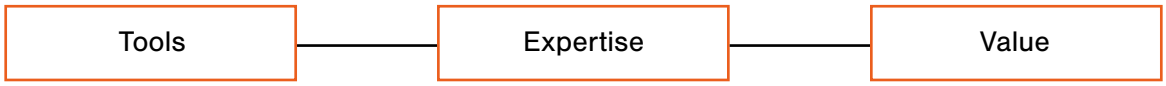
Delivery

Truesec firmly believes that tools are enablers of value; but to produce the expected outcome, they must be correctly configured and maintained, be utilized by trained operators, and put into skilled context. Threat Intelligence: Leak Detection and Mitigation is a fully managed service that combines the output of the following commercial and proprietary tools and capabilities, which we continuously develop and refine:

- **Recorded Future**
  Truesec works in close collaboration and partnership with Recorded Future, a global leader in providing automated and machine-based scanning of both the Internet and the Darkweb. They provide a rule-based, indexed crawler which will generate alerts that are then qualified and investigated by Truesec experts.
- **Truesec Darkweb Explorer**
  To further enhance capabilities, Truesec has developed its own engine for Darkweb hunting. It allows for a highly customizable target list based on your organization's specific context. It also enables Truesec to scan for customer related information without exposing you or your organization.
- **Brand Intelligence and Take-Down Service**
  Through collaboration with Recorded Future, we can further assist in identifying fraudulent or malicious behaviour where your organization's brand is misused for antagonistic purposes. If we find such occurrences, you can apply to have the site taken down, and if you meet the criteria based on an individual evaluation, Recorded Future will then assist in this service.

To ensure continuity, this service is monitored by our dedicated team of Security Operations Center (SOC) Threat Intelligence (TI) Analysts. The SOC TI Analysts will manually inspect all Threat Intelligence: Leak Detection and Mitigation alerts on a daily basis. They can also call upon the assistance of the Truesec Threat Intelligence Unit for more advanced analysis.

The Truesec Threat Intelligence Unit consists of highly skilled professionals leveraging a proprietary platform to collect and index all intelligence relating to threats and threat actors – independently of source or data format. The team employs some of the most well established and well-known names in the industry, with experience in both civilian and military intelligence.



What Is Included

	Included
Reporting of Leaked or Compromised Information Identified by Truesec Proprietary and Commercial Tooling	✓
Identification and Mitigation of Corporate Brand Infringements	✓
Truesec Threat Intelligence Unit Feedback and Analysis of Alerts	✓

Our Methodology

Our service is built around the knowledge of your organization's specific threat landscape.

Methodology

Implementation
Onboarding to the service is primarily achieved by mapping your organization's specific threat landscape and creating a relevant list of target sites and forums as well as keywords and other triggers. Special focus is given to any known ongoing situation or specific threat. These become rulesets in the various tools and platforms. The level of your involvement in the setup varies greatly based on Truesec's knowledge of your organization. The process is usually managed end-to-end within a week.

Process
This service is available individually and as an add-on service to the Detect and Disarm managed service; in either case, it integrates into the workflow of that service. As such, the tools are run (automatically and through manual interaction) 24/7 - generating alerts that are forwarded to the SOC. Specially trained operators receive the alerts, qualify them as needed to rule out critical events in need of immediate attention, and forward them as appropriate to the Threat Intelligence Analysts. After analyzing, incidents are raised as necessary and forwarded to you via the standard customer portal; if critical, warm handover will be performed.

- Monitoring and Scanning
- Alerts Qualified by SOC
- Alerts Investigated by Analysts
- Incidents Forwarded to Customer

Governance and Reporting
The operational management of the service exists in the same governance space as Detect and Disarm; any incident is reported as a specific incident and the service is maintained according to the same delivery governance model.

How Do You Begin to Benefit from Threat Intelligence: Leak Detection and Mitigation?

You start by talking to your Truesec sales contact. Together you will begin the journey to protect your organization's sensitive information and safeguard your corporate brand by scoping the assignment and determining what actions would benefit you most.

By having Threat Intelligence: Leak Detection and Mitigation as an ongoing service you will acquire the capability to rapidly detect whether information has leaked, without having to run your own internal department with cybersecurity threat intelligence experts.

TRUESEC
A Safe Digital Future

Sweden
truesec.com
+46 8 10 00 10
hello@truesec.com

Denmark
truesec.com
+46 8 10 00 10
hello@truesec.com

US
truesec.com
(904) 900-4532
hello@truesec.com