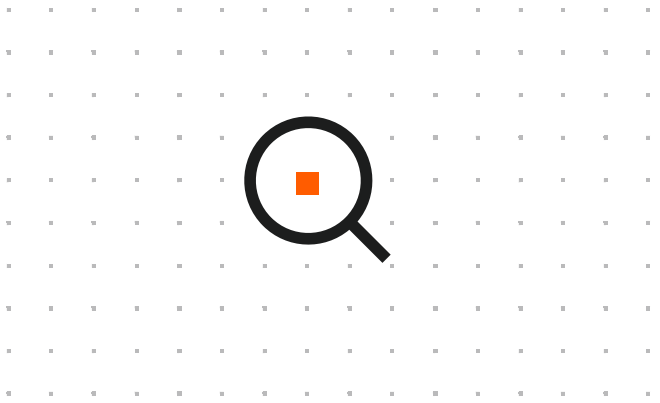
TRUESEC

Detect and Disarm

What is Truesec Detect and Disarm?

The perfect cybersecurity defense is very difficult to create and can also take considerable time to establish. For most organizations, the quickest, and most effective way towards achieving this, is to acquire state-of-the-art detection capability. This provides an organization with actionable alerts, information when a malicious event occurs, and the capability to stop an attack in real time. At the core of the Truesec Detect and Disarm managed service is a security analysis team that conducts 24/7 attack monitoring, threat hunting, threat intelligence analysis, and threat remediation. The team analyzes alerts, eliminates false positives, and in the event of an IOA (Indicator of Attack), immediately notifies your team and/or takes action to mitigate the attack, contain the threat, and protect your data. This saves you valuable time to focus on increasing your organization's proactive cybersecurity defense.



Predict Prevent **Detect** Respond Recover

The Truesec promise

At Truesec, purpose and value are at the helm of what we do; to prevent and stop cyberattacks, to protect data, and minimize the consequences of a breach. Like all our endeavors, our 24/7 SOC (Security Operations Center) service, Detect and Disarm, is crafted with this simple purpose in mind.

The Detect and Disarm service is:

- Capability-centric SOC operation rather than tools-centric.
- Scalable - capabilities can be upgraded or downgraded as you go.
- 100% transparency - verifiable delivery.
- No lock-in. Cyber is evolving - tools can be replaced when needed.
- Customer-focused and collaborative - letting our SOC team become an extension of your organization.

About us

Truesec is a highly regarded company that focuses on cybersecurity, IT infrastructure, and secure development. Our company was established in early 2005 and quickly assumed a key position in the Swedish market. We have made a concerted effort to assemble a team of the top experts in each field. Over time, we have created a strong reputation internationally. Today, the Truesec team has assignments all over the world.

TRUESEC

Together we make a difference

Sweden

truesec.se
+46 8 10 00 10
hello@truesec.se

US

truesec.com
+1 (425) 818-8044
info@truesec.com

The Truesec promise

We always strive for the best results for our customers.
That is a Truesec promise.

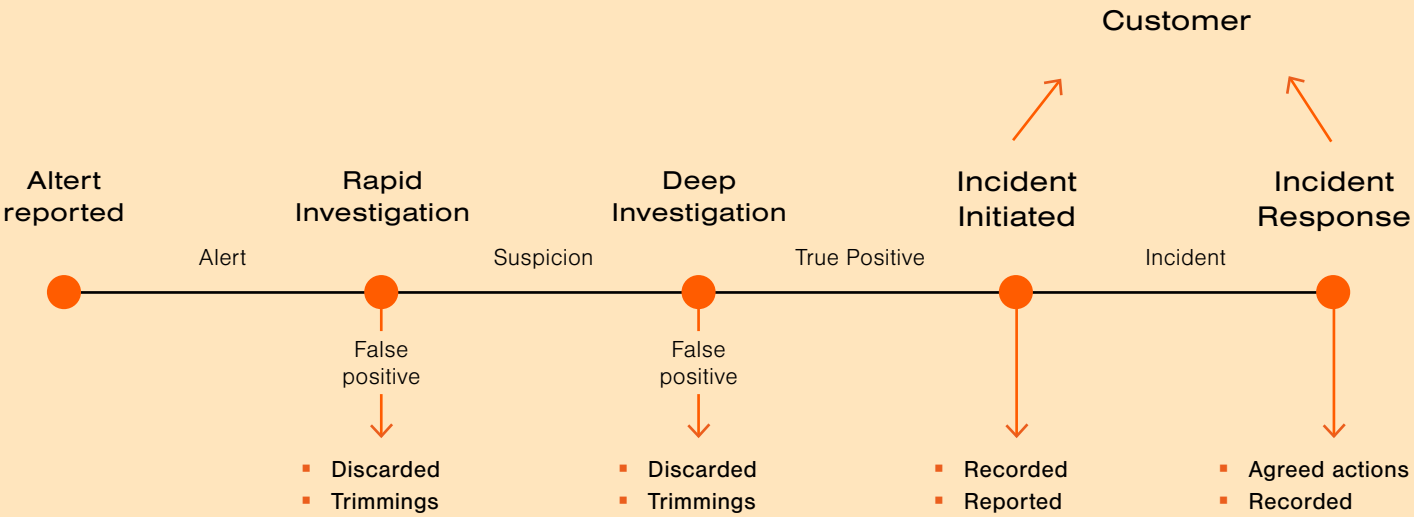
How we do it

For each client, we customize a combination of capabilities and tooling, tailored to stop and prevent cyberattacks in the most efficient way for each particular customer, based on their specific requirements such as threat exposure, budget, and risk appetite.

We are capability centric and tools agnostic. All capabilities may be combined in a custom fashion, as well as scaled up and down as you go. The capabilities we offer are designed to counteract every stage of a cyberattack event chain, as well as controlling its entirety; this includes active 24/7 attack monitoring and remediation, proactive threat hunting, preventive threat intelligence, and counteractive incident response and recovery. on that, help you plan for the next step from an operational, tactical, and strategic point of view.

The format also gives you the benefit of identifying a lot of areas where you as an organization are not in full sync. By taking your own notes during the workshop you will, besides the official assessment, also identify several areas and processes that need clarity and can be improved.

After the structured onboarding of the service in your environment you will get the benefits of Truesec's combined strengths including parts of the Secure Operations team, Incident Response team, and Threat Intelligence team.



How we keep our edge

- Truesec carries out most intrusion investigations in Sweden and has a unique insight into relevant threat actors, as well as their mode and that information feeds the rulesets in the Detect and Disarm service.
- Truesec's dedicated department for active threat intelligence is led by Sweden's most experienced specialists.
- We offer both threat intelligence analyzes and assessments
- Truesec has local specialists who can work closely with you for your future needs within Cyber security, infrastructure, and development.

TRUESEC
Together we make a difference

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

US
truesec.com
+1 (425) 818-8044
info@truesec.com

The Partnership

We see our work with our customers as a partnership.
We work together to get the best results and prevent incidents.

More than just a SOC

We regard our work as not merely a SOC-service, but a transparent and collaborative partnership in cyber security.

To form such a partnership it becomes crucial that we as the service provider and the customer consistently seek to align on challenges and targets, working in close collaboration towards the same goal and with shared interest.

Moreover, a collaborative framework and common mindset is essential for reaching and upholding the desired effect of the service; to protect you from cyberattacks, whatever the cost. To that end, our service is a commitment to help cultivate collaboration in many areas including:

- Constant reporting and dialogue (operational alert reporting, tactical monthly reporting on past months' activities and strategical reporting on trends, threat intel, and security posture).
- Close cooperation with your own CSIRT, DevOps and other IT staff to gain deep understanding of your infrastructure, security posture, and threat landscape to improve our detection capabilities, efficiency, and relevancy.
- Form personal relationships across your ecosystem – our team will know you and your environment; you will know our team.
- Embedment – by understanding your strategic choices and challenges ahead we may be proactive and preventive in trimming your cyber defenses.
- Build mutual trust and become your advisor in all things related to cybersecurity.

What is included	"Just a SOC"	Truesec SOC
Collection of logs and check against general IOCs (Indicators of Compromise)	✓	✓
Make rapid investigation on alerts	✓	✓
Record and report true positives	✓	✓
Escalation and activation of battle proven Cybersecurity Incident Response Team (CSIRT) in case of breach	Sometimes	✓
Activation of forensic specialists in case of suspected incident	Sometimes	✓
Tool agnostic - Working in the best tool for the customers environment, not "the tool we like"	Rarely	✓
Threat hunters looking for treats and creating custom IOCs for each customers environment		✓
Threat intelligence team feeding tools and people with new knowledge of the current threats. To update awareness and knowledge and to create custom IOCs		✓
Security recommendations for improving customers security stance		✓
Tools and people in SOC getting feedback and findings from Truesec-led CSIRT operations, Red Team engagements, forensic assignments and intelligence gathering activities. To update awareness and knowledge and to create custom IOCs		✓
Team creating internal tools for Intelligence gathering to increase knowledge, make better and quicker investigations and work with custom IOCs		✓
Dedicated Teams - Specialists in SOC knows the customer environments		✓

TRUESEC
Together we make a difference

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

US
truesec.com
+1 (425) 818-8044
info@truesec.com

If you are under attack, call Truesec

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

Continuous cooperation

As a framework for our customer collaboration, when required, we have the capacity to deploy a dedicated delivery governance team for each client which can include:

Service Delivery Manager - Operationally responsible for the daily delivery according to contract. Main escalation and contact point for customer/supplier interactions and driver of continuous service improvement, responsible for reporting and more.

Technical Account Manager - The customer's (technical) area specialist, responsible for best practice alignment of solutions, technical understanding of customer environment, service development and general advice.

Account Manager - Overall responsible for the contract and relationship; manages any contractual disputes and commercial aspects of the delivery.

How do I obtain the benefits of the Detect and Disarm service?

You begin by talking to your Truesec sales contact. Together, you will determine the length of time your organization will subscribe to the service, how many devices there are, what requirements and other conditions do your organization have that will affect the choice of tool and deployment method. During the implementation we will then together implement the rulesets from the tool-supplier, and add our own intelligence and rules based on feedback from the Secure Operations team, the Threat Intelligence team and from our Incident Response team.

After the structured onboarding of the service in your environment you will get the benefits of Truesec's combined strengths including parts of the Secure Operations team, Incident Response team, and Threat Intelligence team.