

Detect and Disarm

What's 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 Detect and Disarm service is:

- A capability-centric MDR operation rather than tool 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 – allows our MDR team to become an extension of your organization.

The Truesec Promise

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

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

Contact Us

us.truesec.com

us@truesec.com

The Truesec Promise

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



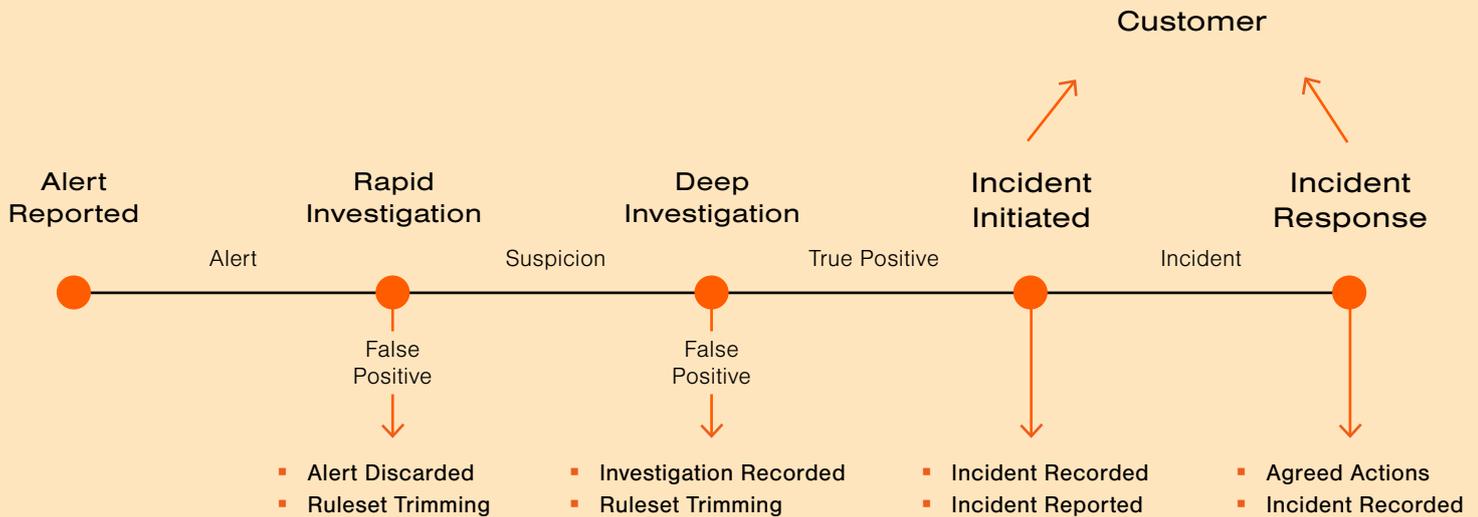
How We Do It

For each client, we customize a combination of capabilities and tooling, tailored to prevent and stop cyber attacks 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 tool 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 cyber attack 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.

After the structured onboarding of the service in your environment you'll get the benefit of Truesec's combined strengths including components of our Secure Operations Team, Incident Response Team, and Threat Intelligence Unit.



How We Keep Our Edge

- Truesec carries a large amount of intrusion investigations across the globe giving us unique insights into relevant threat actors, as well as their methods. This information feeds the rulesets in the Detect and Disarm managed service.
- Truesec's dedicated department for active threat intelligence is led by our most experienced specialists.
- We offer both threat intelligence analyses and assessments.
- Truesec's specialists can work closely with you for your future needs within cybersecurity, infrastructure, and development.



If You're Under Attack, Call Truesec

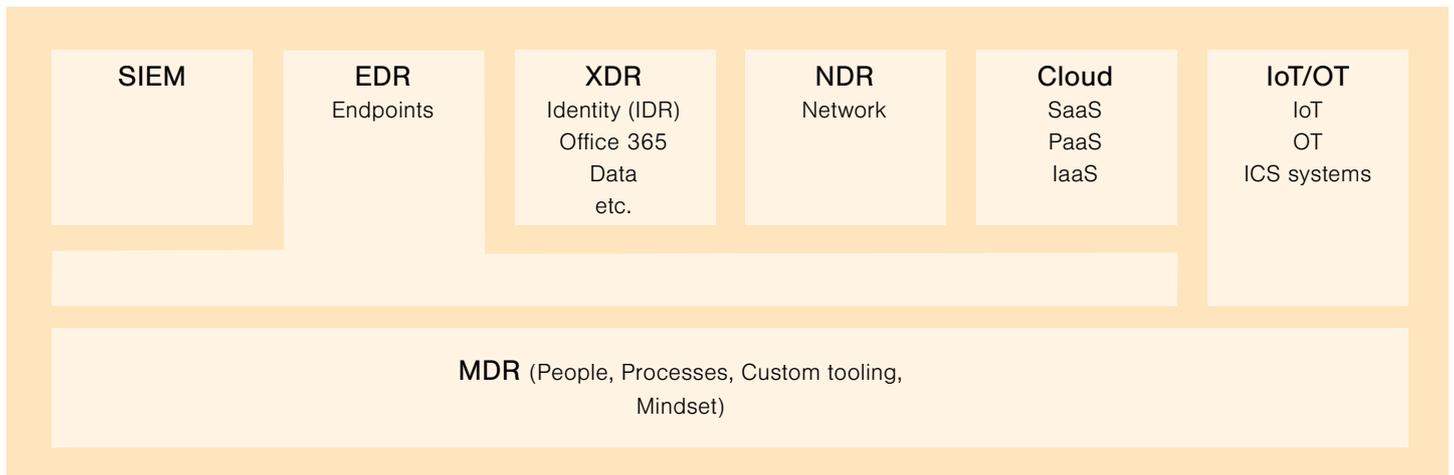
+1 904 323 3906

incident@truesec.com

Technologies

Truesec delivers Detect and Disarm capabilities based on the technologies and suppliers at the forefront of the security field; we tailor the capabilities to our client's needs but typically base the delivery on endpoint detection and response (EDR). Truesec's primary focus is to prevent cybercrime; therefore, we concentrate on helping our clients detect and prevent attacks in real time. To do this, client infrastructure requires tooling with response capabilities. An endpoint detection and response solution, or EDR, is the most

effective tool to ensure you're monitoring your endpoints while still being able to respond to any attacks or suspicious behavior. Expanding technologies in our client environments can also include extended detection and response (XDR), network detection and response (NDR), and security information and event management (SIEM) tools. With these tools, we can deliver a tailored and highly capable detection and response service with a holistic view of our client's network traffic, servers, cloud, and clients.



More Than Just a SOC

We regard our work as not merely a SOC or an MDR service, but a transparent and collaborative partnership in cybersecurity.

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 cyber attacks – 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, monthly tactical 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 can be proactive and preventive in trimming your cyber defenses.
- Build mutual trust and become your advisor in all things related to cybersecurity.

TRUESEC

A Safe Digital Future

Contact Us

us.truesec.com
us@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.

What's Included

	"Just an MDR"	Truesec MDR
Collection of logs and checks against general IOCs (Indicators of Compromise).	✓	✓
Conduct 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 incidents.	Sometimes	✓
Tool agnostic – working with the best tool for the customer's environment (not "the tool we like").	Rarely	✓
Threat hunters look for threats and create custom IOCs for each customer's environment.		✓
Threat intelligence team feeds tools and people with new knowledge of current threats to update awareness and knowledge and to create custom IOCs.		✓
Security recommendations for improving customers' security stance.		✓
Tools and people in the SOC obtain feedback and findings from Truesec-led CSIRT operations, red team exercises, 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, conduct better and quicker investigations, and work with custom IOCs.		✓
Dedicated teams – specialists in the SOC that know the customer environments.		✓

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 responsibility for the contract and relationship; manages any contractual disputes and commercial aspects of the delivery.

How To Get Started

Start by talking to your Truesec sales contact. Together, we'll determine the length of time your organization will subscribe to the service, the number of devices you have, what requirements and other conditions your organization has that will affect the choice of tool and deployment method.

During the implementation, together we'll implement the rulesets from the tool supplier, and add our own intelligence and rules based on feedback from our Secure Operations Team, Threat Intelligence Unit, and Incident Response Team.

After the structured onboarding of the service in your environment you'll receive the benefits of Truesec's combined strengths including components of our Secure Operations Team, Incident Response Team, and Threat Intelligence Unit.