Cybersecurity Incident Response

What's Cybersecurity Incident Response?

Predict Prevent Detect Respond Recover

Your organization has become the latest victim of a cyber attack and your internal IT environment has been breached. What should you do? Contact Truesec!

Cyber attacks are a far too common occurrence in today's connected world. Threat actors are constantly evolving, and the degree of intrusion and damage can vary greatly from case to case.

If your organization is the victim of a cyber attack, you can rely on one of the most sophisticated and experienced incident response teams in the industry, Truesec Cybersecurity Incident Response Team (CSIRT) to assist you. We'll put our experts to work to help your organization through the incident, stop the cyber attack, mitigate damage, and speed recovery time.

What should you do if you're under attack?

- Contact IT security experts - CALL TRUESEC!
- Don't touch anything!
- Secure your backups.
- Create a timeline of events.

(Read more on Page 4)

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

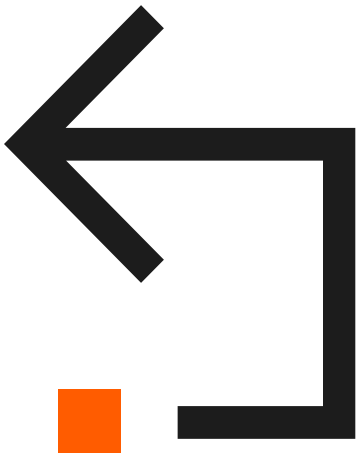
truesec.com hello@truesec.com

Truesec CSIRT Is Here to Help

We're here to help you when the breach is a fact.

The Truesec CSIRT Team

Being hit by a cyber attack can seem devastating, and indeed, if not resolved quickly, it can be. Truesec CSIRT has extensive experience responding to cybersecurity incidents worldwide, conducting forensic investigations, and tackling threat actors head-on. We stay ahead of the curve by continually expanding and refining our knowledge base, and by utilizing some of the most advanced tools on the market.



Our assignments have included attacks such as advanced ransomware campaigns, cyber espionage, and theft of digital assets. We have the capacity to rescue data from encrypted files and successfully disarm advanced cyber threat actors. Such experience has provided us with comprehensive knowledge on how to instantly minimize impact, immobilize threat actors, and provide you with strategic advice moving forward.

Delivery

Our primary goal in responding to an incident is to help organizations return to normal operation as quickly as possible, with no data loss during ongoing security incidents.

Truesec CSIRT follows a proven, well-defined process in close collaboration with your organization's representatives. The work will be divided into multiple workstreams with specialized experts to ensure efficiency.

Depending on the nature of the incident, such experts may include:

- Forensic Experts
- Data Recovery Experts
- Reverse Engineering Experts
- Threat Intelligence Unit
- Incident Management
- Legal and Crisis Management

Contact Us
truesec.com
hello@truesec.com

Our CSIRT Operations Methodology

Our method builds on the seven steps described below.

What We Do

1. Initial Contact/Start Up Meeting

Truesec's Incident Manager together with your IT personnel, will help to quickly establish what occurred, the extent of the intrusion, and develop an action plan. We'll also assist you in establishing alternative communication channels, as your email will most likely be compromised.

2. Preparation

Our experts will begin the investigation by doing the preparation needed in the environment to collect information to understand the environment and the incident at hand. This will involve interviews and data collection. Any information can be crucial, so it's imperative to secure evidence for later analysis.

3. Containment

In the containment workflow we perform activities to limit the damage/breach. At an early stage, we'll initiate active security monitoring by the Truesec Security Operations Center (SOC) during the incident response to ensure visibility into the environment. This is beneficial if the threat actor tries to breach or move around within the environment.

4. Forensic Analysis and Investigation

In this workflow we initiate a forensic investigation to secure traces of the threat actor, determine if any company or personal data has been breached or exfiltrated, and what the threat actor has done within the environment. This determines in exact detail how the threat actor breached the system. We also conduct Threat Intelligence on the attackers by analyzing the Darkweb and locating other relevant leaked information.

5. Eradication

Based on the forensic investigation results, exact measures will be taken to eradicate the threat actor from the environment. This is aimed at removing any remaining artifacts associated with the threat actor, and at restoring the environment back to a clean state.

6. Recovery

In the recovery workflow the activities are aimed at recovering operational capacity in the most effective, yet secure way possible. If required, we can also help rebuild systems that cannot be restored.

7. Final Report/Post Incident

Following the incident response and recovery, Truesec CSIRT will finalize an Incident Report and provide a debriefing, ensuring your organization's operational procedures and incident response plans can be updated to reflect the knowledge gained from the incident. Truesec can also provide active security monitoring for a predetermined time to ensure a smooth return to normal operation.

Contact Us
truesec.com
hello@truesec.com

If You're Under Attack, Call Truesec

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

What's Included	Included	Optional
Truesec proven CSIRT methodology.	✓	
Truesec Threat Intelligence Unit analysis.	✓	
Truesec proprietary Threat Intelligence platform.	✓	
Retrieval of data from encrypted files whenever possible.	✓	
Final Report/Post Incident.	✓	
Active Security Monitoring by Truesec SOC (Security Operations Center) during incident.		✓
Active Security Monitoring by Truesec SOC (Security Operations Center) post incident (typically 3-6 months).		✓
Crisis and communications management.		✓
Rebuild of unrestorable systems post incident.		✓

What To Do if You're Hit by a Cyber Attack

If you're being attacked, immediately follow these basic steps to mitigate damage:

Contact IT Security Experts - CALL TRUESEC!

Get professional help immediately to stop the attackers. Wait for the IT security experts to start their investigation to avoid forensic data loss.

Don't Touch Anything!

Don't turn off computers, pull out power cords, shut down accounts or make any changes to the environment. Consider the situation a crime scene.

Secure Your Backups

Secure your backups so they're not on any network. Critical systems can be disconnected from the network - but don't switch them off.

Create a Timeline of Events

Create a timeline of how you experienced the incident – record the who, what, when, where, and why of the incident. Every detail counts.