TRUESEC

Security Vetting Interview

What Is a Security Vetting Interview?

Predict Prevent Detect Respond Recover

Security-sensitive roles or projects require that we know and can trust the individuals involved. A well-conducted security vetting interview is a crucial prerequisite for an accurate assessment of a person. It provides a valuable depth and nuance to information such as a CV, extracts from public registers, and financial records.

The objective of a security vetting interview (Swedish: “Säkerhetsprövningsintervju”) is to assess whether a person can be assumed to be reliable from a security perspective, loyal to interests that need to be protected, and to identify possible vulnerabilities that could potentially be exploited to gain access to sensitive information or operations.

Truesec Human Threat Intelligence (HTI) focuses on people. Truesec’s technical expertise combined with our expertise in HTI, offers a comprehensive 360-degree view and provides customers with holistic support in their cybersecurity work.

Examples of areas covered in a security vetting interview

- Current life situation and background.
- Education, training and certificates.
- Personal finances.
- Corporate engagements and intrests and potential conflicts of interest.
- Work related conflicts and breaches of obligations and responsibilities.
- Security awareness and approach to security.
- Internet presence and digital footprint.
- Discussion regarding threats and security risks, and advice on how to increase awareness.

(Note: These are examples, not a complete list. Security Vetting Interviews are often successfully combined with doing a Background Check)

Who It’s For

The value that security vetting interviews bring to an organization isn’t confined only to operations subject to the Protective Security Act. Security vetting interviews are an effective and proactive way to reduce the risks associated with insiders, fraud, theft, and other threats in the workplace, and benefit all organizations that manage sensitive information, assets, and knowledge.

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

The Truesec Promise

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

What We Have Learned

Trends indicate that nation-states and criminal organizations exploit human vulnerabilities to access systems and information using human intelligence and social engineering.

The threat posed by insiders is frequently reported to be one of the most significant factors in cases of successful data exfiltration.

The consequences of a successful insider threat can take a variety of forms, including data breach, fraud, theft of trade secrets or intellectual property, and sabotage. To prevent this growing threat, we need to not only understand how insider incidents happen, but also why. Employees are rarely disloyal from the start, when first hired. They don't join their organizations with the intent to do harm. This is (most of the time, at least), something that happens later, because of personal or work-related stressors. Most people who have access to secret or sensitive information could potentially steal this information or cause harm in some other way. Many people also have some type of motive. They may want more money or feel that management makes bad decisions. However, that doesn't mean that "most people" would betray their employer or country. Most of us have a moral compass and would never allow us to cross that boundary, however much we would like to have more money or dislike changes at work. It's those without a moral compass that we need to identify, to prevent them from having access to information so sensitive that it could cause damage.

When To Conduct a Security Vetting Interview

As mentioned previously, employees are rarely disloyal from the start. Almost no one joins their organizations with the intent to do harm. Therefore, vetting should be followed up on a regular basis with security interviews. This is about taking the temperature of the organization and caring for the employees' well-being to be able to preemptively identify changes. Additionally, security interviews should also be conducted when a person or consultant is in the process of being hired, changing roles in the organization, or entering a project with a higher security profile.

Cybersecurity and information security aren't just about IT and technique. Firewalls, virus protection, encryption, and separate systems are essential and important security measures. However, it doesn't help if someone on the inside "opens the door" to the attacker. Cliché or not – the weakest link is the human being. We humans are the ones handling the information and the security systems, and we are the ones that make mistakes – or our choices allow us to.

What we do

Security protection involves safeguarding information and operations considered critical for our security against espionage, sabotage, terrorism, and other threats. Security vetting interviews are among the requirements necessary for granting access to and conducting security-sensitive operations, and are an important instrument in obtaining knowledge about, and understanding, an individual. A thorough and well-conducted interview is essential to establish whether a person can be assumed to be loyal to interests protected under the Security Protection Act, whether the person can be considered reliable from a security point of view, and to investigate possible security vulnerabilities.

How We Do It

Our methodology for conducting security vetting interviews is based on extensive experience and thousands of interviews. Our interviewers have deep expertise in the field of personnel security and backgrounds in defense and/or risk management.

TRUESEC
A Safe Digital Future

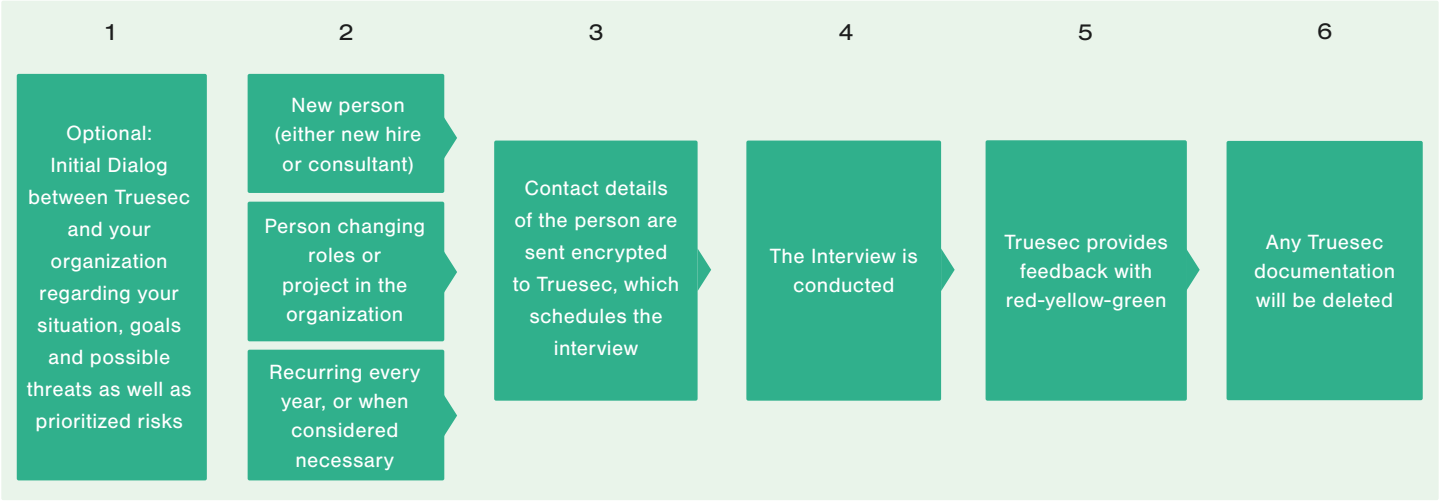
Sweden
truesec.com
+46 8 10 00 10
hello@truesec.com

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

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

The Partnership

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



1. Initial Dialog (Optional)

We begin with an initial dialog in which we discuss your organization's situation and goals, potential threats, and prioritized risks, particularly for organizations that are subject to the Protective Security Act or anticipate a large number of interviews.

2. Prior to Changes/Recurring Annually

A security vetting interview is often part of the employment process for a new employee, or when an external consultant is set to join an organization. However, it is equally important when an employee or consultant is assigned to a project with a higher security clearance than before, or if their roles change, or involve access to new assets and information in the organization. Vetting should also recur annually, to identify any changes in behavior or reliability.

3. Scheduling

We determine a time that suits all parties and schedule the interview/s.

4. Interview

The interview is conducted in a positive conversational climate characterized by reflection and dialogue. It is essential that the interviewee feels heard and respected and that the interview is not perceived as an interrogation.

5. Feedback

Upon completion of the interview, we provide the results of the risk assessment, which will be categorized as follows: Green (no relevant finding to discuss), Yellow (findings that require discussion), or Red (findings of a more complex nature that require discussion).

You hire us not only to gather information, but also to make assessments and subsequently provide recommendations. Therefore, you will not receive a lengthy report that requires you to have the necessary knowledge to interpret the content yourself. Instead, we will use our expertise and experience gathered over many years of conducting thousands of these interviews, and our in-depth understanding of the threat actors and how they act. We will determine on your behalf, whether a person can be assumed to be reliable from a security perspective, loyal to interests that require protection, and whether there are any identified possible vulnerabilities that could potentially be exploited to gain access to sensitive information or operations.

Our findings will be summarized and provided to you with a recommendation for the next step with the individual. Any findings that warrant further discussion will be communicated to designated contact persons within your organization.

6. Documentation

In accordance with our way of working, no written report will be produced concerning a completed security vetting interview, and no information pertaining to completed interviews is stored or saved.

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

If You Are Under Attack, Call Truesec

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

How Do You Begin to Benefit From Security Vetting Interviews?

You start by talking to your Truesec customer contact, or any of our experts. Together you will begin the journey to protect your organization's sensitive information and assets.

By conducting security vetting interviews, you will increase your capability to predict and manage risks, minimizing your exposure to cybersecurity incidents and similar threats.