

Agile Security

What's Agile Security?

Performing continuous penetration testing of your applications, systems, and infrastructure is vital to surviving in the digital era.

With seamless teamwork between pentesters, developers, and IT staff, our customers receive increased value for investments with relevant findings and continuous development of their cybersecurity resilience.

What We Do

The Agile Security service from Truesec is a subscription-based service, delivering focused penetration testing of systems, applications, and infrastructure.

By working closely with stakeholders, developers, and IT staff, we ensure a tight and effective collaboration between Truesec and you, as a customer.



Predict



Prevent



Detect



Respond



Recover

The Agile Security service will provide you with the following:

- Risk-based penetration testing.
- Relevant findings and insights into solving the actual problem, not the fallout.
- Risk-based approach based on workshops.
- Findings reported directly to stakeholders.
- Optimized reporting to management.
- Minimized lead times between requirements and actual penetration testing.
- Continuous improvement to cybersecurity resilience.
- Access to Truesec cybersecurity experts.



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

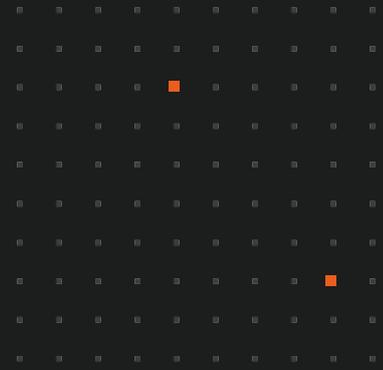
Contact Us

truesec.com

hello@truesec.com

If You're Under Attack, Call Truesec

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



How We Do It

We begin with a workshop identifying the most relevant systems, applications, or infrastructure belonging to a company. By identifying the critical IT infrastructure and focusing the penetration testing in these areas we ensure a proactive, as well as risk-based, approach to the penetration testing.

Assets identified as critical are added to the ticket system for easy oversight and collaboration. It also enables the customer to measure progress. Tickets are created to order a penetration test of a specific asset. Whenever a vulnerability is identified, the vulnerability is added to that ticket.

Each test period begins with the team reviewing the current tickets with the customer and verifying the priorities. During testing relevant stakeholders are contacted immediately depending on the severity of the vulnerability.

The penetration testers are always available for discussions regarding the specifics of a finding and its proper remediation.

At the end of each test period, the overall results are described to stakeholders and, if required, existing tickets and remediation actions are reprioritized.

Given the nature of this approach, the efficiency of the penetration testing and the resulting values will be significantly higher compared to regular one-off tests performed once a year.



What's Included

Included

Penetration Tests of Applications



Penetration Tests of Systems



Penetration Tests of Infrastructure



Continuous Reporting



Risk-Based Approach to All Penetration Testing



Relevant and Actionable Findings



Contact Truesec to begin increasing your cybersecurity resilience level today.

