Red Team Engagements.

Improve IT security – prevent advanced persistent threats and professional attacks with realistic simulations.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

OUR SERVICE

- In an intensive planning phase, together with our experts you identify critical attack vectors of real-life hackers – for your IT environment as a whole and for your personnel.
- In the implementation phase our red team simulates attacks by cyber criminals or APT groups. Various techniques are deployed within a preset framework: from attacks on the technical infrastructure and available services via spear phishing campaigns to physical attacks on your premises. If access is gained, the red team tries to achieve the set goals, such as stealing development data without alerting the IT security department in the process. Security issues are thus revealed that would otherwise rarely be identified in normal penetration tests.
- Finally, we recommend comprehensive and strategic improvements for your IT security and show you how to eliminate critical vulnerabilities.

YOUR ADVANTAGES

- Holistic view of your IT landscape: From the point of view of highly qualified and best equipped hackers launching an attack in real-life conditions. You decide in advance how far TÜV Rheinland may and should go.
- Detailed report: Which attack vectors were used? Where do weaknesses lie in organizational processes, IT systems and user awareness? How can you remedy them?
- TÜV Rheinland reveals whether existing IT security solutions and their configurations comply with security requirements and where optimization potential can be tapped.

OUR COMPETENCE

- One of the largest German-speaking security-testing services teams draws on its experience from around 1,000 penetration tests annually in all imaginable security fields: IoT, group-size office networks or applications. We use this comprehensive know-how In our red team engagements to match the expertise of global hacker groups.
- As one of the world's leading independent providers of cybersecurity services, we have teams at all key locations, including in Europe, USA, China, India, Singapore and Oman.

Red Team Engagement Elements

THREAT MODELING

With your help, we design a scenario to suit the attack scheme that is typical for your organization: Are we aiming at stealing development data or accessing a specific system? Is the IT department going to be involved or not? Is the attack going to be conducted as an "expected breach" scenario?

ATTACK PHASE

In a classic red team engagement, TÜV Rheinland uses all available attack methods. An even higher level of realism can be achieved by a black team scenario: In this case, only an approximate time frame is agreed, for instance six months, during which the attack is to take place. This effectively prevents the IT security department preparing for it.

If the main focus is on checking data security in the internal network, a bridgehead in the corporate network can be mounted in a so-called "expected breach" scenario. TÜV Rheinland uses it to directly access the internal network and try to achieve defined goals. Time-consuming searches for access to the internal network are eliminated, which can reduce costs substantially. Other sub goals can also be realized as independent projects.

If you wish, TÜV Rheinland will stay in close touch with your project manager and coordinate attack targets and next steps with them – so effective, well-oiled running is guaranteed.

REPORTING

Any relevant vulnerabilities are classified, placed in overall context and submitted to the customer in the form of a TÜV Rheinland test report. In it,we show you the damage a successful hacker might cause in your organization and suggest appropriate countermeasures for you to adopt.

Simply ask us!

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Cologne Germany
Tel. +49 221 806-0
cybersecurity@tuv.com

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

® TÜV, TUEV and TUV are registered trademarks. Their use must be approved beforehand. DE18_D01_1800022 11/2018