SHINE A LIGHT ON YOUR ATTACKERS AND YOUR SECURITY POSTURE

Computacenter's Cyber Defence Maturity Assessment puts attackers classes, attack methods and protection controls under the microscope

Be it script kiddies, financially motivated cyber criminals or politically motivated actors: companies today are being targeted by a wide variety of attackers – and every group has developed its own methods.

To combat these increasingly sophisticated attacks, companies have to be aware of, understand and prepare for, these new attack techniques. That is the only way they can fend off threats, detect incidents and respond to them adequately. In practice, however, few organisations can really do this.

Since many companies simply do not know which attack methods they need to protect themselves against and whether their existing controls are even effective, they can neither assess their security level nor implement the correct controls to improve it.
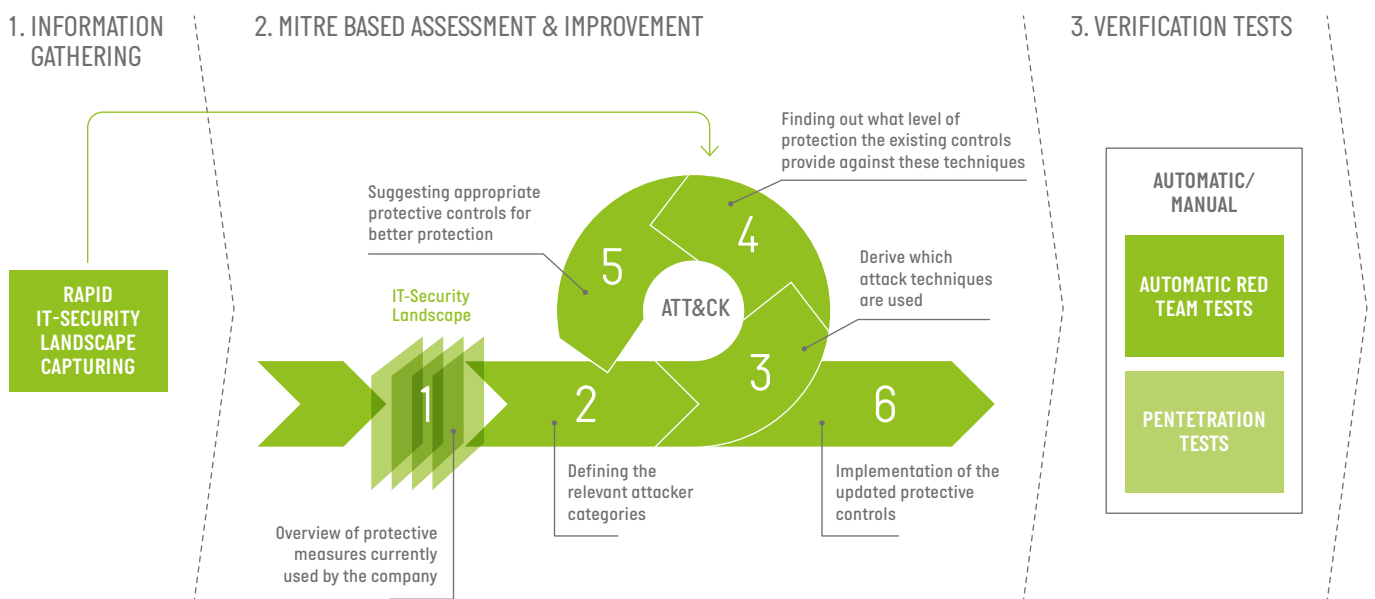
With Computacenter's 'Cyber Defence Maturity Assessment', we help companies understand if they are vulnerable to these new attack types and if their existing solutions are effective. As part of the assessment, we will provide answers to questions like:

- Which attackers are interested in my company?
- What attack techniques do these attackers use?
- How well do my protective controls detect and prevent these techniques?
- Which attack techniques are my protective controls unable to detect?
- Which of my protective controls have become obsolete?
- How can my company effectively close any gaps?

GAIN REAL INSIGHT: COMPARISON OF ATTACK TECHNIQUES AND PROTECTIVE MEASURES
We have developed a methodology for assessing the resilience of IT infrastructures, based on the MITRE ATT&CK™ knowledge database. MITRE ATT&CK™ is constantly updated and collates all known attack techniques, attack vectors and typical attacker categories according to the phases of a cyberattack.

We use our Cyber Defence Maturity Assessment to individually assess how effective your existing protective measures are against over 230 MITRE attack techniques. We look specifically at detection and prevention measures as well as your company's ability to respond to differently motivated and technically savvy attacker categories.

1. INFORMATION GATHERING
2. MITRE BASED ASSESSMENT & IMPROVEMENT
3. VERIFICATION TESTS

RAPID IT-SECURITY LANDSCAPE CAPTURING

Suggesting appropriate protective controls for better protection

Finding out what level of protection the existing controls provide against these techniques

IT-Security Landscape

5

4

ATT&CK

Derive which attack techniques are used

1

2

3

6

Overview of protective measures currently used by the company

Defining the relevant attacker categories

Implementation of the updated protective controls

AUTOMATIC/ MANUAL

AUTOMATIC RED TEAM TESTS

PENTETRATION TESTS

HOW DO WE DO THIS?

Our methodology is divided into three phases: evaluation of the current state based on MITRE ATT&CK and verification tests.

In the first phase, "evaluation of the current state", we identify what technical security controls are used in your company by running an audit which allows us to gather all the necessary information within a short period of time – even for large, international companies with many sites.

In the second phase, we conduct the actual assessment. We do this in six steps:

1. Defining the relevant attacker categories
2. Working out which new attack techniques need protecting against
3. Finding out what level of protection the existing controls provide against these techniques (Which technique is covered and how well is it covered?)
4. Suggesting appropriate protective controls for better cover

In the third phase, verification, we test the company's security controls against attack techniques. The tests focus on the attack techniques for which cover cannot be 100 percent assured due to lack of information at the time of the assessment or which have since been improved.

WHERE ARE THE EXISTING PROTECTIVE MEASURES EFFECTIVE?
WHICH ATTACK TECHNIQUES ARE FULLY COVERED, PARTIALLY COVERED OR NOT COVERED AT ALL?

Our Cyber Defence Maturity Assessment provides information about where attackers have easy targets and where improvements are required.
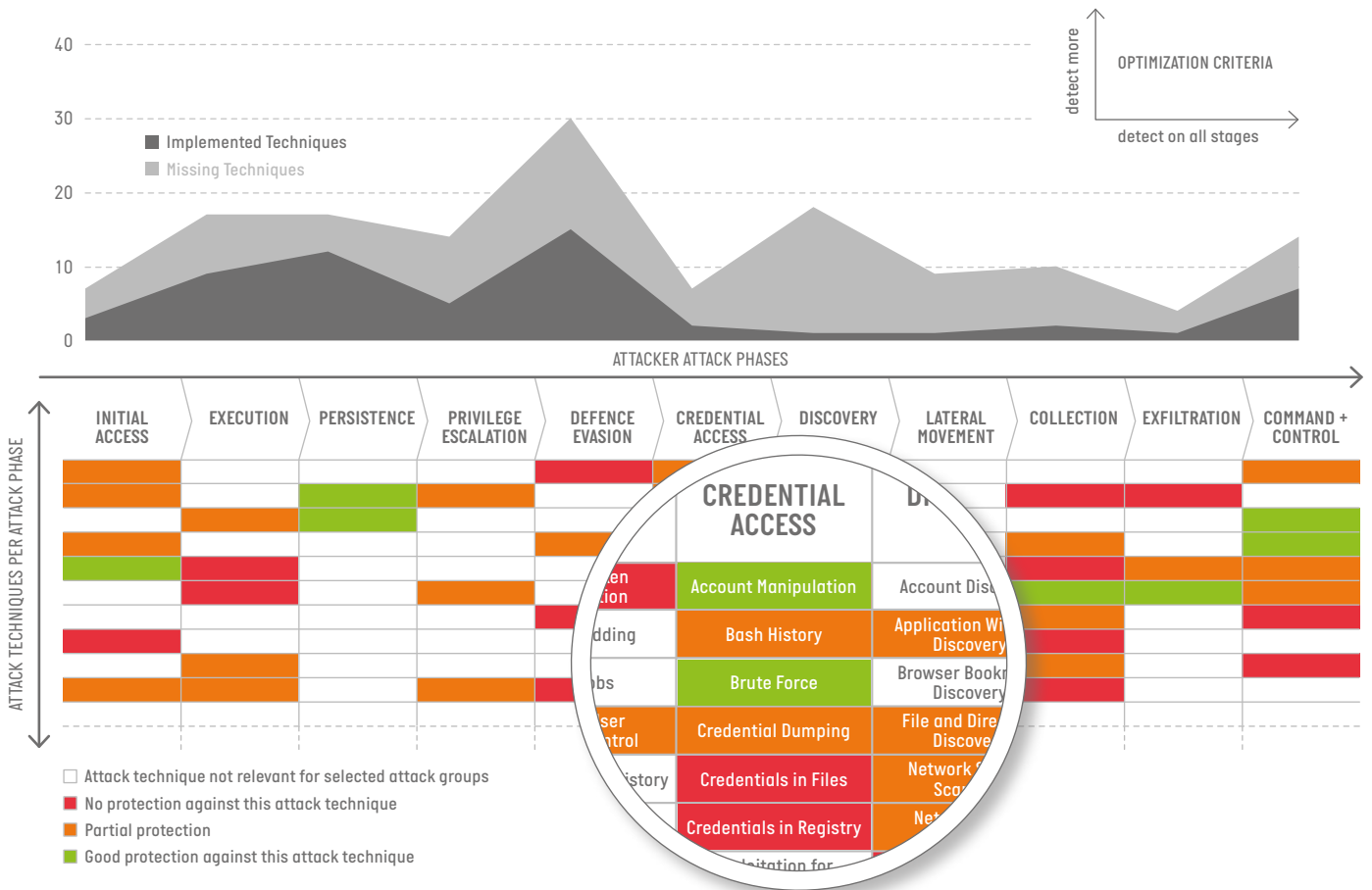
A SOLID BASIS FOR MAKING INVESTMENT DECISIONS

This process helps us to systematically identify the protection gaps in your IT. You get a clear picture of where your IT is well protected and where there are gaps that need closing. In addition, we can show how you compare with other organisations in the same industry segments, whilst also providing you with specific recommendations as to how you could improve your security level. Our Cyber Defence Maturity Assessment provides not only a realistic assessment of your security level, but also a solid and quantifiable basis for making investment decisions regarding your IT security.

GET IN TOUCH

To find out how Computacenter can help you master business security, please contact your Computacenter Account Manager. You can also visit our Solutions Center to discover how our security services will enable you to deliver better, more secure business outcomes.

www.computacenter.com/de/security

Computacenter is a leading independent technology partner, trusted by large corporate and public sector organisations. We help our customers to source, transform and manage their IT infrastructure to deliver digital transformation, enabling users and their business. Computacenter is a public company quoted on the London FTSE 250 (CCC.L) and employs over 15,000 people worldwide.