

# Attack Path Management Services

The XM Cyber platform

## Be one step ahead of the attacker – every single day

**Do you know for certain how secure your enterprise IT is? Or are you wondering whether there are attack scenarios that you haven't even considered yet or that you're not even aware of? When the press reports yet another security incident, are you afraid your company might be the next victim?**

With our Attack Path Management Services, there is no need to worry anymore. With XM Cyber, we provide you with a continuous real-time model of the security posture of your IT. With just one glance, you will be able to identify all possible attack paths and find out how critical they are. And even better yet, XM Cyber will also tell you how to fix your vulnerabilities.

### A new dimension of security

Without any doubt, you are already doing a lot in order to secure your IT infrastructure. You are using firewalls, VPN, encryption, authentication and many other mechanisms to protect your most valuable asset – your data. And in order to be absolutely sure your measures are effective, you run checks – penetration tests, security checks and regular audits.

But eventually, all that is not enough anymore! None of these measures will help you understand which path a hacker would take. Because all of these tests and analyses focus only on the isolated systems involved in the respective test. Therefore, they will never be able to provide you with an overall view of your IT landscape including the human factor.

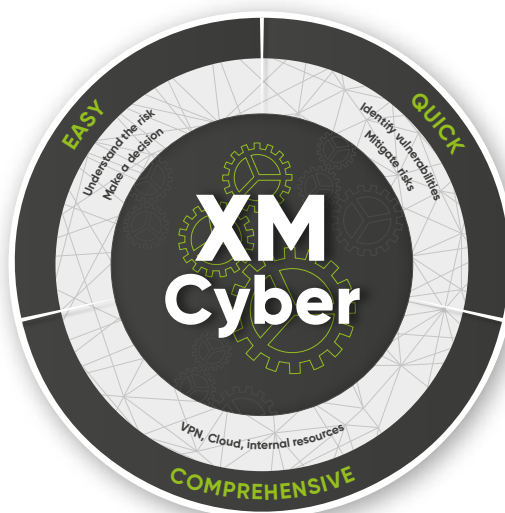
### See your IT through the eyes of a hacker

A hacker isn't interested in your individual systems. He is looking for the quickest and easiest way to the „core“ – your most valuable data. He often uses a combination of various mechanisms that become a vulnerability only by blending them together. The Attack Path Management platform identifies these exact combinations and shows you the choke points you need to fix to disrupt the attack path.

## Improve your security posture with us – step by step

Our experts at the Swiss IT Security Group will guide you through the implementation and operation of XM Cyber – on your first day of use as well as in your continuous effort to improve your security posture. We offer tailored service packages for Attack Path Management.\*

Together with our customers, we will get the system ready for use and perform a first check. But you will not have to take the next steps alone either. We will be in touch with you on a weekly or monthly basis to discuss the newest findings of XM Cyber, analyze the different options for fixing the vulnerabilities and assist you in planning the mitigation. If desired, we can even take care of the entire operation of the XM Cyber platform for you.



## Your benefits using our Attack Path Management Services



### About XM Cyber

XM Cyber brings the expertise of the world's leading IT security specialists to your door. XM Cyber has developed more than 15 patented technologies based on a proprietary set of algorithms that enable the continuous and automatic simulation of a hacker's techniques and methods.

The Swiss IT Security Group offers tailored service packages for XM Cyber. Our experts will not only help you find the perfect solution. We will also implement the system for you and make sure you get the best value out of it.

### About Swiss IT Security Group

The Swiss IT Security Group, headquartered in Wettingen (Switzerland), offers its customers comprehensive security services and solutions.

With over 600 employees, the company combines the know-how, resources and services of leading IT security experts in one single service provider and offers its customers overall IT security concepts based on the aspects of protection, detection and defense with the help of innovative solutions and technologies.

### Swiss IT Security Group

www.sits-group.ch  
CH: xmcyber@sits.ch  
GER: sales@sits-d.de

REQUEST NOW AND  
RECEIVE INDIVIDUAL  
ADVICE



\*A detailed overview of the content of our various service packages can be found on the corresponding datasheet.