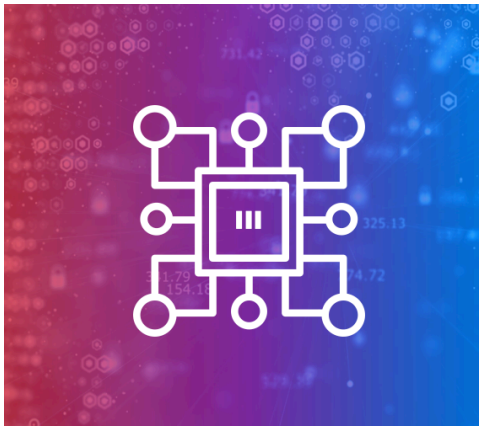
DarkDefense. XM CYBER

Cyber Risk Analysis

Measure, prioritize and improve your overall cyber security posture

In our digital business world, there are three questions every CISO should be able to answer: (1) are my critical assets and the digital infrastructure protected against cyber threats, (2) where should I prioritize my team and (3) are my security strategies working as expected?
These three questions can be answered quickly, easily and effectively using the darkdefense attack exposure analysis service based on the innovative XM Cyber-attack simulation platform. And there is not only the benefit of improving the day-to-day work of the security team, but also to be able to report to the management the security posture of the organization in a clear and meaningful way.

The Problem



Risk Management
how can my critical assets be compromised?

Prioritization
Where do we start?

Validation
Have we closed the risk?

Technology

The technology is based on passive sensors with a small footprint, which are installed on the endpoints, totally safe with no impact on the production environment. The systems collects metadata from the IT Infrastructure, which are analyzed using advanced ML algorithms – Simulating a variety of attack methods uncovers exploitable vulnerabilities or mis-configurations and shows possible attack paths.

The simulation looks at your IT Infrastructure with the eyes of an adversary and simulates starting from endpoints, how an attacker can spread into the network to reach critical assets or disrupt operations. As a result, you will get prioritized Information and recommendations to remediate significant vulnerabilities, wrong configurations and process-gaps.

DarkDefense.

APT Simulation

Advanced Persistent Threat (APT) today represent a major cyber risk for all organization of all sizes. Advanced Persistent Threats jeopardize enterprises by combining the best in stealth hacking techniques with patience and time. Waiting for the right next step, these techniques move laterally within an organization hunting for the most valuable data to steal.

Most security technologies that are used today are reactive and work well for some attack methods. Unfortunately, they are not sufficient for complex and advanced cyber-attacks.

To defend against an APT, you need countermeasures that are themselves advanced and persistent. APT simulations identifies and exposes attack paths that were previously unknown or considered impossible.

Key attributes of a successful APT Simulation include:

- APT simulations must rely and be updated by the most advanced techniques available.
- be persistent, waiting for changes in the network that can be exploited.
- a holistic view of the enterprise, combining opportunities like cached credentials and misconfigurations into new attack paths.
- constant search for blind spots and holes in your network and infrastructure security posture, running 24/7

Our Technology-Partner

XM CYBER

XM Cyber is the global leader in Attack-Centric Exposure Prioritization, which is also known as Risk-Based Vulnerability Management (RBVM). The XM Cyber platform enables companies to rapidly respond to cyber risks affecting their business-sensitive systems by continuously finding new exposures, including exploitable vulnerabilities and credentials, misconfigurations, and user activities. XM Cyber constantly simulates and prioritizes the attack paths putting mission-critical systems at risk, providing context-sensitive remediation options. XM Cyber helps to eliminate 99% of the risk by allowing IT and Security Operations to focus on the 1% of the exposures before they get exploited to breach the organization's "crown jewels" – its critical assets.

- **Persistent APT Simulation**: Performs continuously and safely in your production environment with the full range of virtual hacker capabilities
- **True Hacker Techniques:** Uses previously collected information and its current network posture to simulate an extremely realistic adversary
- **IT-Hygiene:** Continuously identify and respond to new exposures such as misconfigurations, undermanaged credentials, exploitable vulnerabilities and user error **MITRE ATT&CK:** Relies on the most advanced techniques available, including the MITRE ATT&CK knowledge base

Platform

The patented platform continuously simulates known and unknown attack vectors, using a hacker mindset to demonstrate what could happen. By continuously identifying new exposures from misconfigurations, poorly managed credentials and exploitable vulnerabilities, the platform shows your IT and SecOps teams what needs to be remediated, what the risk is to the rest of the network, and what steps need to be taken to fix the problem. More importantly, the platform also prioritizes the remedial activities based on risk factors associated with your most important, business-critical systems and data.

The risk-free platform delivers context to cyber security remediation programs, allowing your security and IT operation teams to achieve higher security posture and operational efficiency. You can now eliminate 99% of the risk to your critical systems by focusing on 1% of the exposures that can be exploited.

The XM Cyber platform can be used as SaaS, on-premise or managed service provided by Darkdefense. The installation is without integration efforts and the solution can be used immediately. Darkdefense offers a one-time assessment service to analyze the existing security architecture, which takes two to four weeks.

Cyber Risk Analysis use cases

Attack Simulation
- Breach & Attack
- Red Teaming
- Auto Pen Testing

Security Posture Visibility
- Risk Management
- Resource Management
- Compliance Support

Vulnerability Prioritization
- Vulnerability Scan
- Patch Management
- IT Hygiene

Cloud Security Posture Management
- AWS
- Azure

ECO System
- Integrations
- Service Partner
- Alliance Partner

Darkdefense offers consulting, solutions and managed services to strengthen the cyber resilience of our customers. Based on our automated intelligence driven platform, we enable companies of all size to quickly and efficiently identify relevant vulnerabilities, detect threat actors in their digital infrastructure and take appropriate remediation actions.

DarkDefense.

Contact: sales@darkdefense.ai, +49 721 66998507
Herzstrasse 14, 76187 Karlsruhe