XM Cyber

Establishing a Modern Exposure Management Program

Table of Contents

Introduction:
Critical Vulnerability Does Not Necessarily Equal Risk

Managing vulnerabilities is a challenging task. Today's ever-changing environment creates a situation where new critical vulnerabilities emerge on a daily basis. Keeping up with the technologies that we use and monitoring the vulnerabilities associated with them is difficult and overwhelming.

But the mere existence of a vulnerability doesn't necessarily mean that it poses a real risk. When it comes to managing vulnerabilities, many organizations focus on metrics such as CVSS score or the number of vulnerabilities. But this approach is lacking; it fails to provide business context around issues, it doesn't enable sufficient prioritization, and it fails to understand the opportunity presented – or not presented – to attackers. Furthermore, vulnerabilities are just a small part of the exposure surface attackers leverage.

This whitepaper dives deep into why a critical vulnerability does not equal risk, the different types of exposures that can impact an organization's security posture, and the key fundamentals of a modern exposure management program designed for an evolving risk landscape.

The Evolution of Vulnerability Management

The field of vulnerability management in cyber security has undergone significant transformation over the years. Initially, organizations used manual methods like verifying software versions and applying patches to address known security weaknesses. However, as technology and cyber threats evolved, the need for a more automated and comprehensive approach to managing vulnerabilities became apparent.

Legacy vulnerability management tools and programs were primarily designed for compliance and not to address an organization's security needs. While modern tools can identify vulnerabilities, there is often a gap between what is found and what is fixed, due in part to prioritization challenges and limited resources. In addition, managing vulnerabilities in a dynamic and agile cloud environment is difficult due to the existence of vulnerabilities in various areas such as infrastructure and different stages of the development lifecycle. This can make scanning for and patching vulnerabilities a difficult task.

Nowadays, modern vulnerability management integrates a variety of security tools, such as vulnerability scanners, threat intelligence, and remediation workflows, to provide a more efficient and effective solution to protect against security risks. But despite these advancements, organizations still face numerous challenges when it comes to vulnerability management:

A constantly growing list of vulnerabilities makes it difficult to prioritize and address them promptly.

Broken communication between IT and security teams leads to misalignment of priorities and resources.

Lack of context in vulnerability assessments often leads to inaccurate prioritization.

Lack of coverage and unified view of risk makes it difficult for organizations to get a complete picture of their security posture.

It is clear vulnerability tools just aren't aligned to the modern attacker and lone wolf type of attacks that are affecting organizations today as vulnerability management tools originally looked for exploits in their software not associated with the techniques leveraged by attackers. According to the 2022 Verizon Data Breach Investigations Report (DBIR), 82% of breaches involved the human element. Whether it is the use of stolen credentials, phishing, misuse, or simply an error, people continue to play a very large role in incidents and breaches alike. While only 7% of breaches came from an exploited vulnerability while nearly 50% came from credentials.[1]

Exposures Are More Than Just Vulnerabilities

An exposure is much wider than a standard Common Vulnerabilities and Exposures (CVEs). "Exposure extends beyond vulnerabilities. Even taking a risk-based vulnerability management (RBVM) approach might not be sufficient." Gartner®; Implement a Continuous Threat Exposure Management (CTEM) Program, 21 July 2022[2]

Exposures can be anything from: a missing security control, a human error wherein the wrong checkbox was selected, a security control not defined properly, to poorly designed and unsecured architecture, etc.

Identities	Vulnerabilities	Misconfigurations	Security Controls
Group membership issues	Follina CVE-2022-30190	Publicly Exposed S3 Bucket	Disabled Endpoint Protection Platforms
Excessive write permissions	PrintNightmare CVE-2021-34527	SMB Signing disabled	Multi-Factor Authentication not configured
Cached Credentials	Log4j CVE-2021- 44228	Default passwords	Outdated signatures

Fig. 1: Different types of exposures

How Do Exposures Affect Organizations?

Many tools zero-in on individual types of potential exposures, like vulnerabilities, misconfigurations, or identities, and address each element in its own silo.

This perspective is flawed though – it fails to account for the way an attacker sees networks and systems. Attackers don't look at the individual exposure – rather, they leverage the toxic combination of vulnerabilities, misconfigurations, overly permissive identities, and other security gaps to move across systems and reach sensitive assets. This route is called an attack path and this type of lateral movement can go undetected for weeks or months, allowing attackers to cause significant and ongoing damage while hiding inside networks.

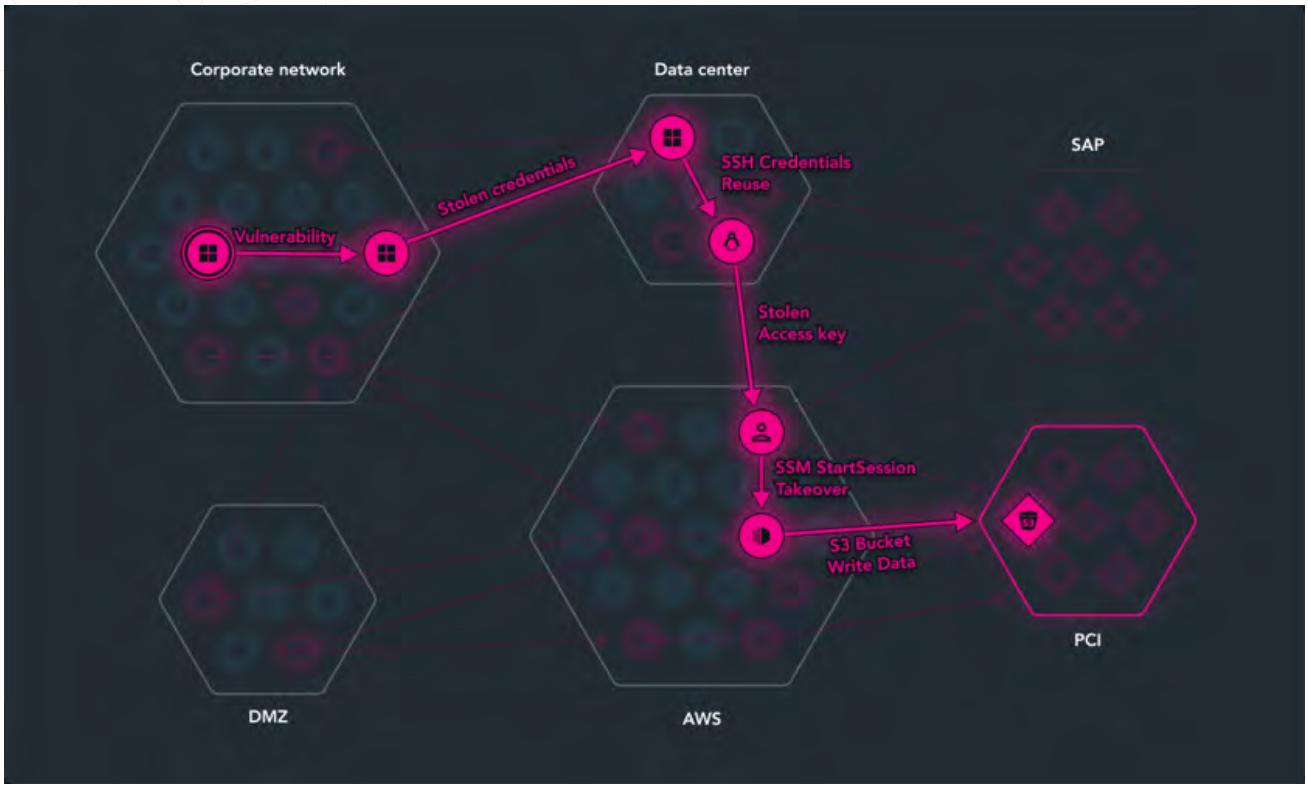

Fig. 2 Example attack path from initial foothold to critical asset, leveraging a variety of exposures

Why Vulnerability Management Programs Need to be Rethought

Organizations regularly make use of vulnerability management tools, trying to address their ever-growing list of exposures. But with thousands of CVEs, many with high severity CVSS scores, fixing all of them is impossible – and so, addressing issues via just CVSS scores is ineffective.

According to Gartner's, "Predicts 2023: Enterprises Must Expand From Threat to Exposure Management"[3] some of the key drivers for exposure management programs are:

1. **The sheer number of security incidents organizations face is already more than their capability to address every last one. Organizations report conflicting priorities resulting from multiple lists for each major threat vector.**
2. **Threats to organizations now more frequently manifest themselves as impacts to brand or availability of critical services. Dependence on third parties that support these business functions requires a broader visibility than the traditional enterprise IT estate.**
3. **Effective communication of the risk to the organization to enable cross-team remediation actions is the main challenge in moving from threat to exposure management.**

To improve on that, Risk-Based Vulnerability Management (RBVM) tools can be used to understand what is actually exploitable in the wild, and to better prioritize issues. These tools prioritize remediation based on the risks they pose to an organization, based on CVE criticality and asset criticality, but also on indicators regarding whether it's used in the wild, if any public exploits exist, AI predictions for public exploits, and so on. It is quite common to see vulnerability management tools today with some RBVM capabilities included.

But this approach too has limitations; it still yields an unmanageable list of issues to be dealt with. Moreover, just because something has been exploited in the wild, it doesn't mean it can be exploited in all environments (i.e. an organization might have that vulnerability but does not have one of the conditions, like network access, for the attacker to exploit it).

Moreover, according to XM Cyber's own in-house research, 80% of exposures don't lead to any critical assets[4] – which means they can be safely deprioritized, which would allow defenders to address the remaining issues that really matter.

What it boils down to is that the current approaches to managing vulnerabilities aren't sustainable and don't address the full scope of issues that put organizations at risk."

> *"Just because something has been exploited in the wild, it doesn't mean it can be exploited in all environments"*

Building a Modern Exposure Management Program

So how do we actually reduce exposures?

At XM Cyber, we believe that only by combining multiple exposures together onto an attack graph that visualizes all possible attack paths, can we understand the relationship and context of risk towards critical assets. And by understanding context, we can accurately prioritize issues to focus on the exposures that need remediating where they converge on choke points. This allows for productive remediation that reduces risk in the most cost-efficient manner.

> *"Only by combining multiple exposures together onto an attack graph that visualizes all possible attack paths, can we understand the relationship and context of risk towards critical assets"*

Modernizing vulnerability management programs involves addressing the challenge of diagnostic fatigue, where organizations are overwhelmed by the sheer volume of information from multiple, trusted, security tools. The traditional approach of simply discovering CVEs in an environment led to security teams being swamped with thousands of issues. The introduction of Risk-Based Vulnerability Management (RBVM) helped to reduce the workload by focusing on exploitable CVEs, but teams were still faced with a large number of problems to manage. With the advent of exposure management, we take a more targeted approach by answering three crucial questions: Are these CVEs exploitable in the current environment? Are they located on an attack path to critical assets? And, most importantly, are they located on a choke point, requiring immediate attention? This approach not only narrows down the focus to the most pressing issues, but also takes into account other exposures such as misconfigurations, credentials, and Active Directory issues, as well as compensating security controls. By clearly communicating the reasoning behind remediation actions in the context of risk reduction, exposure management enables better operational alignment across IT and security teams to be more productive, improve cross-team collaboration, and reduce the constraints of remediation.

"By clearly communicating the reasoning behind remediation actions in the context of risk reduction, exposure management enables better operational alignment across IT and security teams to be more productive, improve cross-team collaboration, and reduce the constraints of remediation"

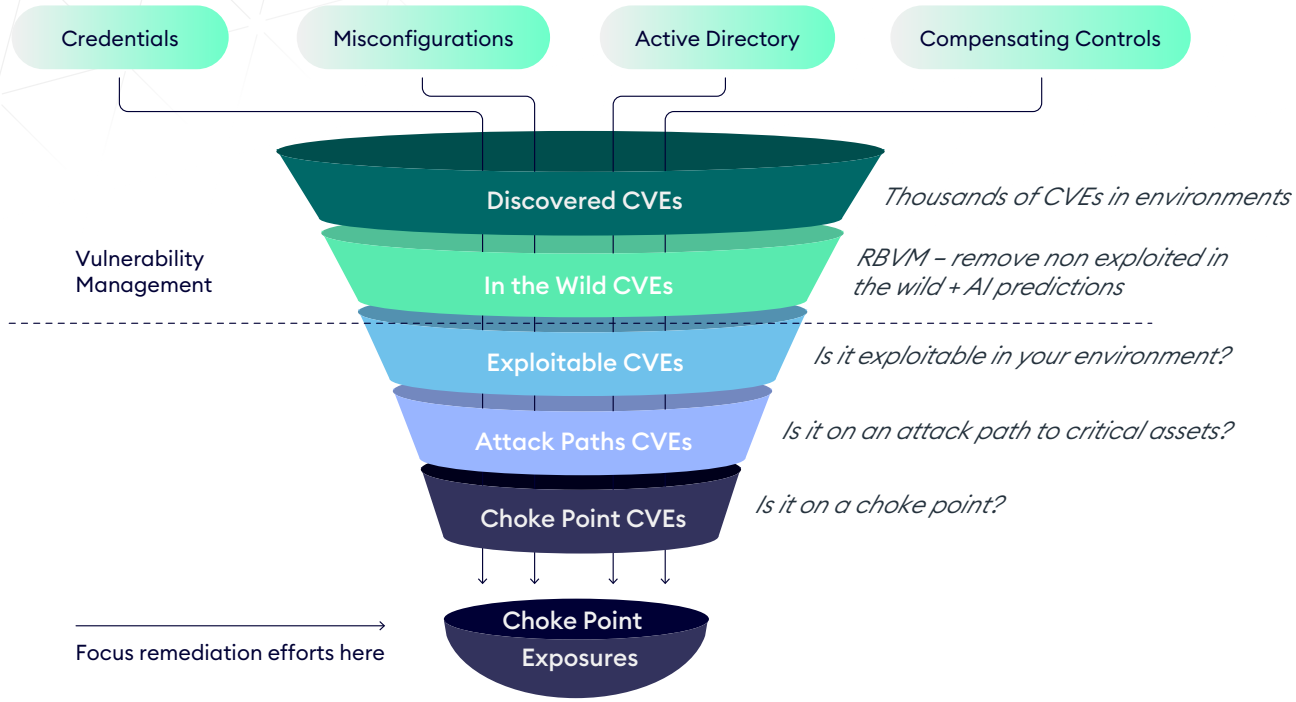

Fig. 3 Prioritization funnel of where to focus remediation efforts

When building a modern exposure management program, it is crucial to recognize the evolution of threat actors and their tactics. They are not limited to exploiting software vulnerabilities, credentials, or social engineering; rather, they orchestrate multiple tools and capabilities to launch attacks. Attackers work in graphs, not lists, meaning that they understand the relationships and dependencies of different exposures to find the most effective attack path. Therefore, building an attack graph in a hybrid way that prioritizes both on-prem and hybrid environments is essential in understanding the context of how an attacker leverages exposures. By doing so, organizations can better prepare and defend against attacks.

Establishing an operational process for ensuring continuous security posture improvement is essential here. According to Gartner, in their report titled Implement a Continuous Threat Exposure Management (CTEM) Program, in order to do this, "Establish regular repeatable cycles as part of your continuous threat exposure management program…thus guaranteeing consistent threat exposure management outcomes."[5]

Overall, it's important for organizations to take steps to protect themselves from exposures, as the consequences can be severe. This may include implementing strong security measures, training employees on security best practices, and regularly monitoring for potential threats.

We recommend a four-part plan to operationalize this approach and put it into practice:

1

Remediation Planning
It all starts with the analysis of risk and building a prioritized remediation plan – a deep analysis to identify risky users, critical assets at risk, and choke points, i.e., junctures where many attack paths converge, and if remediated, can reduce large portions of risk with minimum efforts.

2

Remediation Review
In this step, organizations should review exposures, risks and remediation plans. This crucial step with key stakeholders highlights exposures and best ways to fix them.

3

Risk Mitigation
Here organizations should communicate risks, remediation options and context to relevant teams. By communicating risk, and reviewing with all parties, remediation actions can be easily pushed. This is because there's a major difference between asking IT to fix 10K vulnerabilities versus asking them to fix only 5 exposures which are high risk to the organization.

4

Mitigation Verification
In this last stage, organizations should verify the mitigation is done and the risk has been removed.

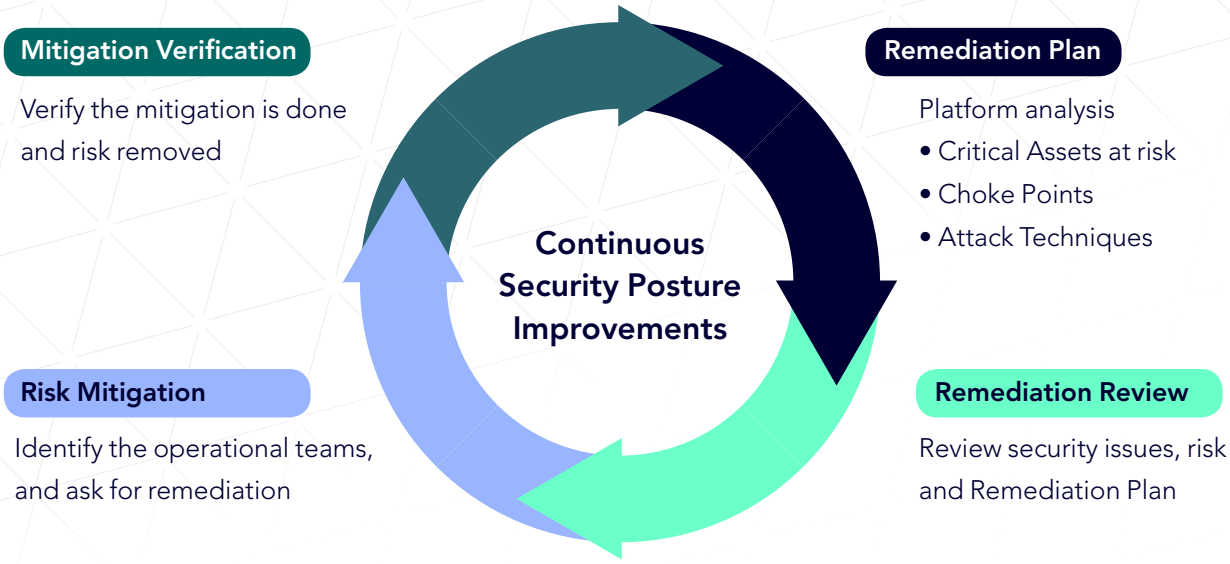

Fig. 5 Operational Process for Continuous Security Posture

When done continually, organizations can create a continuous and holistic process by which exposures are addressed and remediated in a sustainable and scalable way.

The key to building a modern exposure management program is ultimately creating the most efficient process to handle remediations. Now, when looking into all types of exposures, and the risks they pose to organizations, we can map different remediation types to them.

Quick wins
Easy solutions with high ROI

Configuration Auditing
Findings of actual misconfigurations

Long term projects
Fixing things that cause a wide exposure and require a major change, like a network architecture change

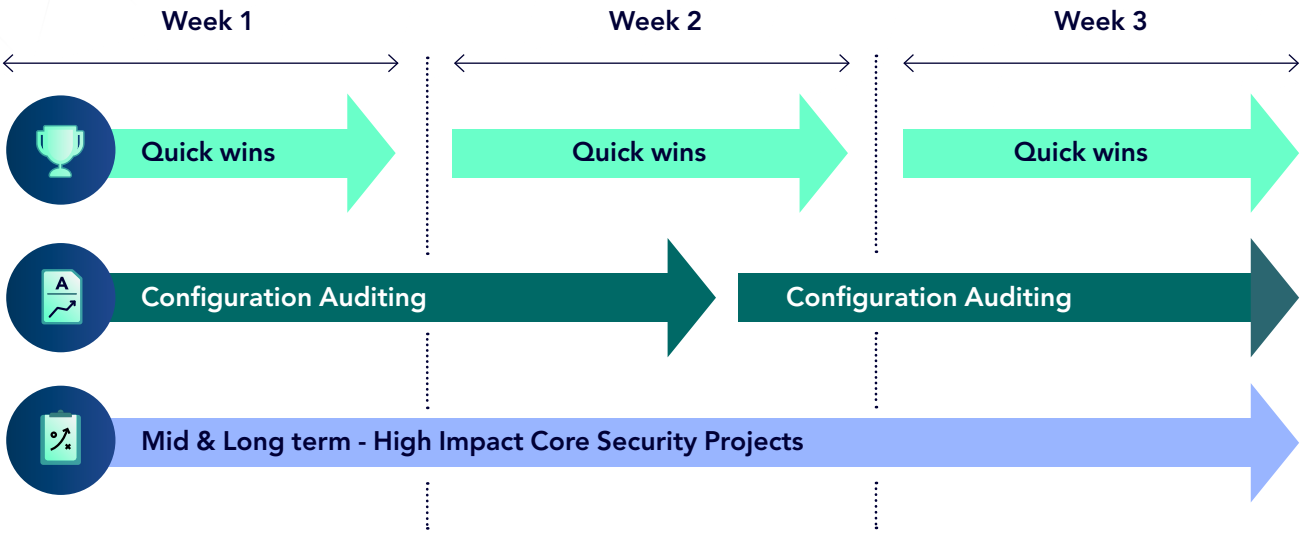

Fig. 6 Example of overall exposure reduction journey

Three Key Pillars to Building Your Exposure Management Program

Understand Exposure Insights

Continuously know what's at risk, see security control gaps and deviation from compliance standards, monitor security score and trends for effective board reporting

Analyze Attack Paths

Gain an attack graph view from any breach point to critical assets with context into what actually puts the business at risk

Prioritize Remediation Efforts

Focus efforts where they are most needed, to reduce overall risk exposure and improve security posture

Conclusion

Preventing exposures from impacting an organization is challenging; but with the right approach, it becomes scalable, no matter how large or complex the network, and sustainable over time, regardless of what types of new exposures emerge.

Using the comprehensive approach to exposure management outlined above enables organizations to essentially see through the eyes of an attacker and vastly reduce their risk.

How can an organization determine if they are correctly adopting a modern exposure management program? Use the table below as a frame of reference to help understand the maturity of your exposure management program.

Old Way of Answering	Question	New Way of Answering
Rely on manual scans and audits, perform periodic pentesting	What does my organization look like from an attacker's perspective?	Real-time visibility into all exposures that can be combined and leveraged by attackers across the hybrid attack surface
Priority based on severity rating, communicate risk to stakeholders based on number of patches applied, % of EDR deployed	How should I prioritize and communicate issues in the context of risk to the business?	Prioritize based on context of what exposures can reach critical business assets, communicate this in the form of a risk score and percentage of critical assets at risk and which attack vectors are exploitable in the organization's own environment
Manually scan to determine if vulnerability exists, we have X number of vulnerable systems	When a new CVE is introduced, how much of a risk is this for us?	Is the CVE exploitable in my environment? Is it on an attack path to critical assets? Understand the percentage or critical assets at risk by the CVE
Limited to no visibility into attack paths and choke points	Which exposures are on attack paths and specifically choke points?	Visibility into attack paths and choke points with prioritized remediation efforts

Old Way of Answering	Question	New Way of Answering
Patch everything, rely on manual processes for remediation, time-consuming	What can we do to mitigate the risk?	Prioritize patching based on systems that introduce most amount of risk to critical assets (choke points)
Direct correlation, struggle to determine impact on cloud environment	What is the blast radius of the vulnerability? (Could this extend to the cloud environment?)	Awareness of how an attacker might operationalize a vulnerability to compromise additional systems, visibility into potential impact on cloud environment, take appropriate steps to mitigate risk
Rely on manual scans and audits, time-consuming, limited visibility	How do changes in my environment affect my security posture?	Real-time visibility into changes in environment, quickly determine impact on security posture
Lack of consistent method for tracking, struggle to see trends	How is my security rating trending over time?	Consistent method for tracking and reporting, see trends and identify areas for improvement

Resources:

1 2022 Data Breach Investigations Report https://www.verizon.com/business/resources/reports/dbir/

2,5 Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, 21 July 2022, Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider

3 Gartner, Predicts 2023: Enterprises Must Expand From Threat to Exposure Management, 1 December 2022, Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, John Watts

4 XM Cyber Exposure Management Impact Report 2022 https://info.xmcyber.com/2022-attack-path-management-impact-report

About XM Cyber

XM Cyber is a leading hybrid cloud security company that's changing the way organizations approach cyber risk. XM Cyber transforms exposure management by demonstrating how attackers leverage and combine misconfigurations, vulnerabilities, identity exposures, and more, across AWS, Azure, GCP and on-prem environments to compromise critical assets. With XM Cyber, you can see all the ways attackers might go, and all the best ways to stop them, pinpointing where to remediate exposures with a fraction of the effort. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, and Israel.

Tel-Aviv: +972-3-978-6668
New-York: +1-866-598-6170
London: +44-203-322-3031
Neckarsulm: +49-7132-30485600
Paris: +33-1-70-61-32-76

xmcyber.com

XM Cyber