XM Cyber

From Vulnerability Management To Exposure Management

Maturity Model

Introduction - There's A Hole In The Bottom Of The CVE

Vulnerability management has long been a security program cornerstone, with the goal of trying to address vulnerabilities as they are disclosed. Every organization wants to protect its assets from known threats, and to the best of its ability, unknown ones as well. And to do this, they need to employ a process of identifying, classifying, prioritizing, remediating, and mitigating issues as they arise. Getting a handle on vulnerabilities and managing them via the steps listed is presumed to be the optimal way to address issues that arise – how else could an organization be expected to reduce risk, right?

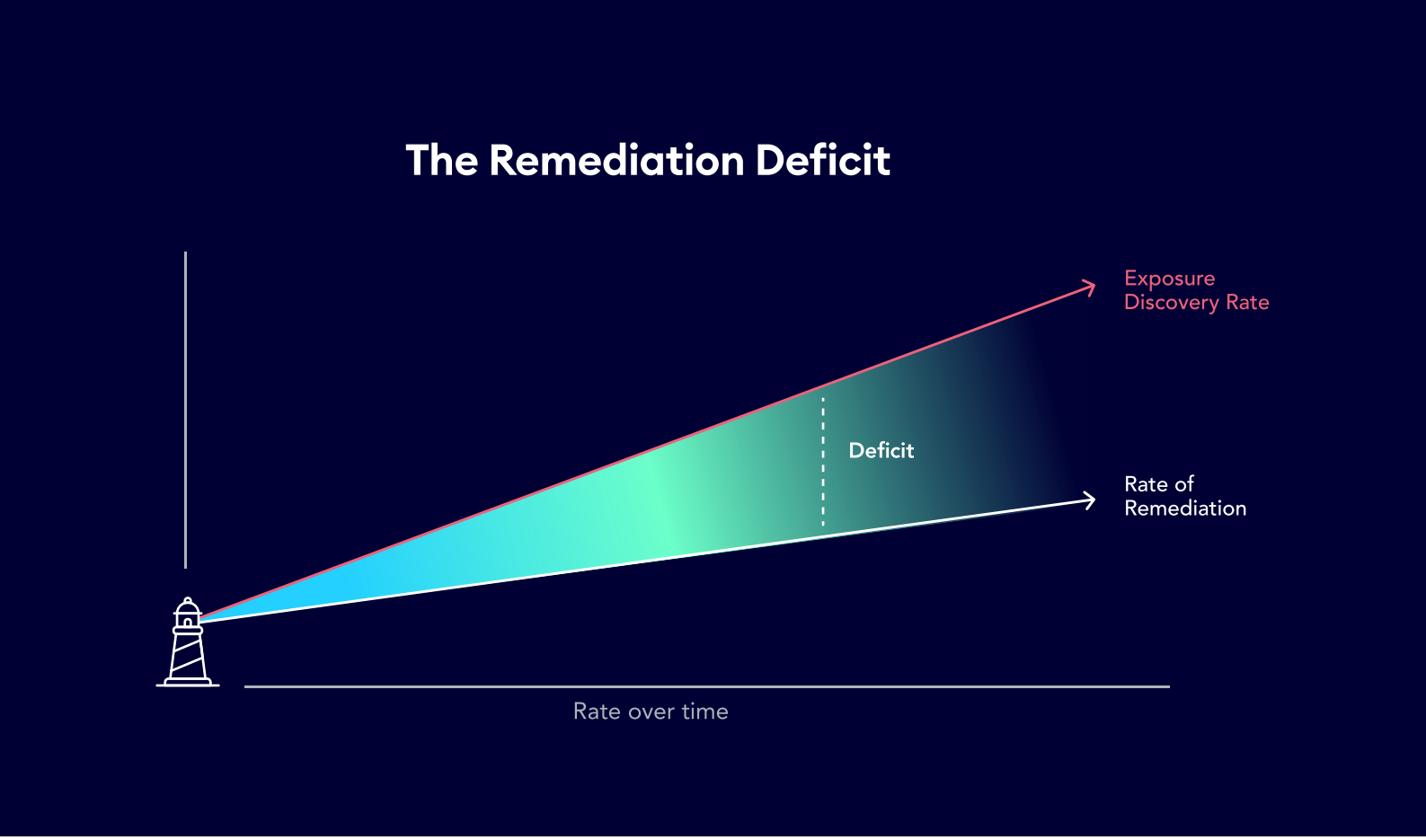
Sure, vulnerability management is an important element in strengthening an organization's security posture. But as organizations grow more complex, managing vulnerabilities using this methodology begins to make less sense.

For starters, most approaches to vulnerability management prioritize based on the Common Vulnerability Scoring System (CVSS). Others add risk-based threat intel, to attempt to answer questions such as: How potentially harmful is the CVE (Common Vulnerabilities and Exposures)? Can this be exploited in the wild? Is there a publicly known exploit in Github/Exploit DB? Does it have an exploit kit?

And in the best case scenario, prioritization tools add asset criticality, i.e., the level of importance of the asset based on issues such as its business purpose and the internet exposure. But in the end, even this process creates an unmanageable list, with no way to determine what matters most.

What's more, just because a CVE doesn't have an exploit today, that doesn't mean that it won't have one next week, which then creates a sudden urgency when indications of exploitations come out. Moreover, not all vulnerabilities are, in actuality, exploitable in real life.

Attempting to manage vulnerabilities this way is like bailing water from a sinking ship with a paper cup; there's too much to take care of and you don't know what to address first. The swirling waters are gathering up way too fast – and you're starting to go under. As Gartner says, "Vulnerability management programs rarely keep up with the aggregate volume of their own organization, leading to quickly expanding attack surfaces." (Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, 21 July 2022) We refer to this phenomenon as the remediation deficit, wherein the emergence of exposures outpaces the ability to remediate them in a timely manner, and thus, staying ahead is virtually impossible.



It's clear that vulnerability management in its current form needs to be rethought and organizations can do better.

But how?

For a start, by establishing scalable methodologies that account for the fact that CVEs and vulnerabilities only tell a portion of the story; they can then leverage the context of these issues within the organization's own environment to understand what issues are the most impactful. Then they can start to see how exposures interact with, and compound, other exposures, to enable them to get the attacker's perspective of the most likely attack paths to critical assets.

This new approach means organizations can move away from siloed, ad-hoc, and reactive Vulnerability Management activities, and instead focus on building sustainable, scalable, and proactive exposure reduction programs.

This Maturity Model is designed to help organizations understand their current posture when it comes to how security exposure risk is addressed and to get the info they need to move up to the next level. When we say "maturity", what we are looking at is how formal and optimized processes are for the approach to reducing cyber exposures. In this case, an Exposure Management Maturity Model is a set of characteristics or indicators that represent the organization's current and future capabilities, and importantly, the pathway to progression via holistic and integrated exposure management efforts and plans.

How To Use This Maturity Model

Step 1:
Evaluate yourself

Assess your current degree of maturity using this interactive quiz.
To do this, go through the three categories – People, Processes, and Technology – and select the option (1-5) that fits your team best.

Note that for the sake of clarity, we have broken this model down into five stages of maturity, with Stage 1 representing a relatively early stage of maturity and progressing onward until Stage 5, which represents an optimal level of maturity. Every organization is unique, and while some elements of the "people, processes, and technology" we include herein may resonate with you and the way you work, others may not. Use the descriptions below as a general indicator to help you gauge your approximate stage of maturity so you can then understand how to "shore up".

The questions have been restated here for clarity. To get your personalized strategy, we recommend taking the interactive quiz linked above first, see your results there and then come back here to get the full strategy.

Step 2:
Decide how far you wish to progress in maturity

This may sound obvious, but once you realize where you are now, you can decide how far you want to go, depending on your budget, resources, and goals. Reaching stage 5, for example, in the people category may sound flashy, but it may not be on your radar as of now – and depending on the circumstances, that may be perfectly fine.

Step 3:
Determine any gaps

Suppose you are at maturity Stage 1 when it comes to the "processes" category but want to advance to Stage 4. There's a significant gap to bridge, so don't expect to jump straight to this advanced goal. Ask yourself, "What do we need to do to progress to Stage 2?" Then establish your goals and make preparations to reach the next stage.

Rinse and repeat as desired.

So now, let's dive right into the Maturity Model Self-Assessment Quiz. Answer the following questions to the best of your ability:

Your People

What does your security team look like and who is responsible for what?

1. **Initial** - Your team, if you have one, is working on establishing the early stages of security posture. Each person wears many hats and has many areas to cover, and there is little productive communication with IT and other non-security teams (DevOps, Infra).
2. **Developing** - You now have or are part of a security team, which may have a decent relationship with IT and other non-security teams. You are all bombarded with issues, but are unsure if the focus is on the right ones.
3. **Defined** - Your team has a working relationship with IT/non-security teams, with regular meetings or information exchanges. The team is starting to think about more than just CVEs, but likely have challenges regarding how to prioritize other security-related issues.
4. **Managed** - Roles and responsibilities for optimization are understood. You have a clear distinction of responsibilities for each system, asset, or application owner within your organization. Your team also understands that reducing risk requires looking at much more than just CVEs.
5. **Continually Optimizing** - You have a dedicated Exposure Management team, who clearly know that reducing risk requires looking at the full scope of exposures (such as misconfigurations, overly permissive IDs and Credential issues) and you work towards optimizing communication around exposure risk with IT.

Your Processes

What are your processes for addressing and remediating exposures?

1. **Initial** - You don't have much in the way of processes – everything is reactive.
2. **Developing** - You try to prioritize where you can but have few defined/documented processes in place.
3. **Defined** - You have processes for automatic patch management, vulnerability scanning, or discovery. You also know that risk reduction isn't just about addressing vulnerabilities, but are still in the mindset of prioritizing based on CVSS score.
4. **Managed** - You have processes for semi-automatic remediation, where you go through manually and then allow the system to deploy patches automatically, and measure risk and business context. You also send remediation requests to ticketing systems.
5. **Continually Optimizing** - You have processes in place to ensure that security doesn't clash with business and instead supports business needs.

Your Technology

What's included in your exposure remediation tech stack?

1. **Initial** - Your remediation efforts are manual and ad-hoc – so you don't have many tools in place at this point.
2. **Developing** - You use patch and asset management systems (like SCCM/Microsoft Endpoint Configuration Manager or BigFix). You also use vulnerability assessment tools.
3. **Defined** - You perform pentesting on an ad-hoc basis or as directed by your compliance requirements.
4. **Managed** - You use vulnerability prioritization technology (VPT), risk-based vulnerability management, and ticketing systems for tracking, managing, and validating the remediation of vulnerabilities. You also have a tool for assessing issues such as misconfigurations, behaviors and credential issues.
5. **Continually Optimizing** - You use some or all of the previously mentioned tools and are continually optimizing to reflect a growing maturity level. For example, you may incorporate support functions such as Attack Surface Management for additional context and insights.

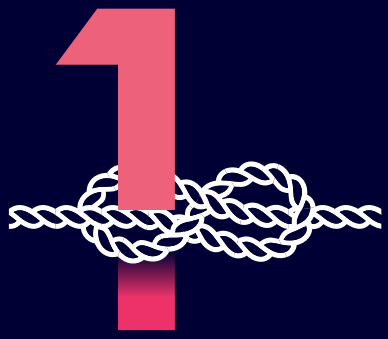
Great going – you now understand where you stand currently in your exposure management maturity.

Now let's address how to move upward in your exposure management maturity, with the goal of building a robust and sustainable program that will proactively reduce risk with less effort and greater efficiency.

Stage One:

Learning The Ropes

This stage is characterized by a lack of organized processes and technologies in place. Vulnerability management processes are (if available at all) reactive, ad-hoc and informal, and are not repeatable, measurable, or scalable.



People

In this first stage, you are using contractors/MSSPs, trying to outsource to get security in place. Here teams/practitioners only consider vulnerabilities, potentially only vulnerabilities that are "high PR" ones, such as Log4j. It's very ad-hoc and reactive, based on external forces or stakeholders, whether it's an audit, or some hype/vulnerability in the news. There's no relationship with IT, and in some cases, IT is security. And no one really has the time or capacity to deal with it.

How To Shore Up

Establish a local security presence with defined stakeholders. Start to work toward building a proactive mindset around vulnerability management. Build relationships with non-security teams.

Processes

In this early stage of maturity, you tend to only take vulnerabilities such as CVEs into account. Remediation is ad-hoc, there's no ticketing, and when it's done, it's done manually. Processes are not documented into Procedures and therefore not being "lived in the organization". You aren't remediating any other (security) issues in their environment, and it's being done sporadically.

How To Shore Up

Document your processes and translate them into Standard Operating Procedures, and adopt a standard around vulnerability management programs like NIST 853. Build processes and leverage best practices, hold workshops with IT to create documented processes, and work with them to understand how to build the optimal workflow.

Technology

At this stage, everything is manual. There are no deployment, patch management (possibly just as a side product), or vulnerability management solutions in place.

How To Shore Up

Research and evaluate patch management and vulnerability management solutions.

Stage Two:

Setting The Course

At this point, a formal program has been initiated to some degree and some processes have been established, defined, and documented, although discipline and "living the process" is lacking.

People

Here you may have a security team, or at least partly, and they may have a decent relationship with IT. But you are bombarded with things and are not focused on the right issues. There is no proper prioritization, or alignment of Business risks.

How To Shore Up

Start to work on creating separate functions; bring someone for compliance, others for cloud security, and others for vulnerability management.

Processes

You might have a manually defined process. This stage often involves some automatic vulnerability management. You may use ticketing and vulnerability assessments to identify and operationalize security issues. You may try to fix everything (top to bottom), pushing tickets to IT manually, might use CVSS for prioritization, and probably don't look at vulnerabilities as anything but CVEs.

How To Shore Up

You may start to see there are too many vulnerabilities and therefore need to prioritize. Create processes for vulnerability analysis and prioritization. Start to measure risk, and ensure you are fully covered on visibility of all assets. Start measuring how long it takes to remediate, try to close gaps.

Technology

You are likely using patch management solutions such as SCCM, BigFix, or similar tools around asset management systems or patch management systems, vulnerability assessment scanning tools, and ticketing systems.

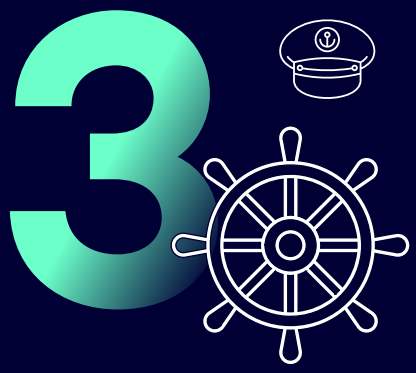
How To Shore Up

Here you should begin implementing components of risk-based vulnerability management (RBVM) tools as well as some type of cybersecurity validation tools, such as pentesting.

Stage Three:

On The Right Track

In this stage, the processes for dealing with CVEs have become formal, standardized, and defined. Better communication is being established and an awareness that vulnerabilities aren't the only issue begins to take root.



People

In this next stage, there is probably a good relationship between non-security teams and Security, with regular meetings or information exchanges. You are starting to think about more than just CVEs, but likely have challenges regarding how to prioritize other security-related issues.

How To Shore Up

Set up vulnerability management steering groups. Collaborate with IT and Business, prioritize issues based on business risks and demands, and explain the risk of each issue to non-security teams, to focus remediation efforts. Now's a good time to start tapping into the attacker's frame of mind and see your environment and exposures the way they do.

Processes

You are likely starting to perform penetration tests every quarter/every six months. And the penetration tests will start highlighting issues that are not just vulnerabilities, such as misconfigurations or overly permissive identities. But these issues are still being addressed and solved via ad-hoc processes, or sometimes not at all. You may also be trying to patch some of those findings that are not just vulnerabilities, yet lack a process.

How To Shore Up

You can finally begin to create and automate your processes. It's time to move from that siloed and limited vulnerability mindset and focus on building out your holistic exposure management program that examines how everything in your environment comes together; the excessive permissions, the misconfigurations, the weak credentials, and so much more – and build plans to continually remediate the ones with the greatest potential business impact. Also, expand your program to cover non-patchable exposures in your SaaS tools and digital supply chain.

Technology

Here you likely employ vulnerability prioritization tools, leverage threat intelligence, and use automated (or manual) penetration testing on a semi-often basis, or as required by compliance regimes.

How To Shore Up

Implement products that cover areas like Cloud Security Posture Management (CSPM) and External Attack Surface Management and tools that cover different areas of exposure and shed light on how to effectively prioritize issues. Consider a platform that shows how exposures come together with other risks like vulnerabilities, misconfigurations, and behaviors to holistically assess what impacts your business most. Work on shrinking the time between scans to get access to continually fresh data, and try to understand how to cover areas of the network that are not covered.

Stage Four:

Navigating The Waters

In this stage, your organization is probably beginning to measure, refine, and adapt exposure management processes to make them more effective and efficient based on the information they receive from their program. Based on these processes, continuous reporting is being given to senior management around security issues and concerns.

People

You know who is patching what and why and when, you understand who the application, asset, or inventory owner is, who deals with SAP, who's dealing with cloud security, etc. You have a clear distinction of responsibilities for each system, asset, or application owner within your organization. In addition, you also understand which business stakeholders are involved in certain processes.

How To Shore Up

You're really on a roll here – just continue to ensure that your team members specialize – i.e., bring in DevSecOps for cloud-related topics, people who specialize in Active Directory, System Hardening, Application Testing, etc.

Processes

You are starting to map between business assets and the right owner to patch that asset. You have a workflow or a ticketing system and there are centralized application owners. You have steering committees that meet every few weeks to discuss hardening and improving on different aspects, like Active Directory security or other initiatives. Moreover you understand that reducing risk requires looking at much more than just CVEs – you look at misconfigurations, weak credentials, excessive permissions, etc.

How To Shore Up

At this point, start to build plans to automate things (where possible), with the goal of addressing vulnerabilities in code and building pipelines to identify, manage, and remediate vulnerabilities before they become an issue.

Technology

You are likely using CMDB, with an integrated ticketing system, and AD security tools, as well as the other tools mentioned previously. Those tools are partly integrated and re-use information through those integrations. Many tasks are somewhat automated.

How To Shore Up

You know about reducing risk in an efficient and scalable way. Now is the time to transform your vulnerability management perspective into a holistic continuous exposure reduction program, with an Exposure Management platform to efficiently address the issues that actually create risk and then cut off attack paths at key junctures.

Stage Five:

Smooth Sailing From Here On

Reaching Stage 5 doesn't mean that your organization's exposure management maturity has peaked. Instead, it means that you are constantly monitoring and evolving your people, processes, and tools to fit a continuous exposure reduction approach. You are not looking into individual problems or security concerns anymore, and instead understand the joint combination of singular security problems. You are leveraging different sources of security issues, coming both from holistic approaches and directly linked inputs.

People

You likely have a dedicated exposure management team. They report findings to IT and IT recognizes the need to address these findings as trust, open lines of communication, and collaboration are strongly ingrained. In addition, non-security teams also report findings on a business level (with business impact) to Senior Management and key stakeholders. Security issues are not seen to be an "IT Problem" but a general concern that needs to be understood across the environment and organization. As a team, you are not looking into individual problems or security concerns anymore and are working towards becoming ever-more efficient where possible.

Processes

Here it's all about shifting left – you may try to push patch management into servers, as well as clients in automatic cycles, alongside other entities within the network. You have automated operationalized processes through integrations, such as automated ticketing, or playbook executions. It's a good bet to assume that you fix before things go to production, since then you won't need to patch them later on. In containers, you try to fix vulnerabilities as part of the release process. You continually try to get the attacker's perspective, putting business and network context into place. You don't look at individual problems or security concerns anymore, and instead understand the joint combination of singular security problems. You are leveraging different sources of security issues, coming both from holistic approaches and directly linked inputs.

Technology

You use some or all of the previously mentioned tools and continually optimize to reflect a growing maturity level. For example, you may incorporate support functions such as Attack Surface Management for additional context and insights. You are also likely running continuous penetration testing holistically, and you probably use business prioritization, as well as automated remediation. You leverage tools that eliminate multiple exposures in one fix and you have context into issues including misconfigurations, vulnerabilities, and risky users and continually understand how they can all be used to compromise critical assets across on-prem, cloud, and SaaS environments. You also put a priority on understanding how you could be attacked, and how much risk exists for critical assets.

The 5 Stages of Exposure Management Maturity

	People	Processes	Technology
Stage 1	One-stop security shop. Vulnerabilities and CVEs are main concerns.	There are no processes, everything is reactive.	Remediation is manual and ad-hoc.
Stage 2	Security team has a decent relationship with non-security teams but isn't focused on the right issues. Lacking proper prioritization of Business risks.	Prioritization is performed but there are no defined/ documented processes in place.	Using patch and asset management systems (like SCCM, BigFix) and vulnerability assessment tools.
Stage 3	Improving relationships with non-security teams. Starting to think about more than just CVEs, but prioritizing is still a problem.	Starting to get on a regular schedule of scanning and patching. Still in the mindset of prioritizing based on CVSS.	Using vulnerability prioritization, threat intelligence, and automated (or manual) pen-testing tools.
Stage 4	Roles and responsibilities are understood. Exposures beyond vulnerabilities/ CVEs are taken into consideration.	Leveraging semi-automatic remediation processes. Measuring risk and business context.	Using RBVM, ticketing for tracking, managing, and validating remediation of vulnerabilities. Also Exposure Management tools to efficiently address issues that actually create risk and cut off attack paths at key junctures.
Stage 5	Security works towards optimizing communication risk with non-security teams. Understand that the combination of individual exposures leads to compromise.	Using automated processes through integrations, such as automated ticketing, or playbook executions.	Tool stack is continually optimized to reflect a growing maturity level and incorporate support functions such as ASM for additional context and insights.

Conclusion: Moving Forward in Exposure Management is a Continual Journey

According to Gartner, "Fixing every known vulnerability has always been operationally infeasible, and odds have worsened as digital transformation has accelerated the expansion of the attack surface." (Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, 21 July 2022). This understanding is propelling the move towards establishing a better model to tackle exposures across organizations today. As you embark on your journey toward adopting a holistic exposure management program, here are the key features and capabilities to look for in a platform:

Enables ultra-efficient remediation

The right tool allows teams to slash multiple exposures in one fix, instead of trying to address issues one by one. This means faster and more accurate remediation by knowing what to fix first to disrupt the most damaging attack paths.

Operationally safe

This has two areas of focus; Firstly, it's important to know how risky the tools are to run in production environments – some tools deploy live exploits! Secondly, make sure to understand how easy the tools are to manage operationally and the level of planning and resource it takes to operate the tool.

Gives full context to all issues

Provides context to misconfigurations, vulnerabilities, and risky users and demonstrates how they can all be leveraged to compromise critical assets across on-prem, cloud, and SaaS environments.

Takes a comprehensive approach

The solution should consider all workstations, entities, virtual machines, containers, user activity, and configurations, etc., as part of attack path analysis to ensure you can see all ways your organization is at risk, to plan prioritized remediation efforts.

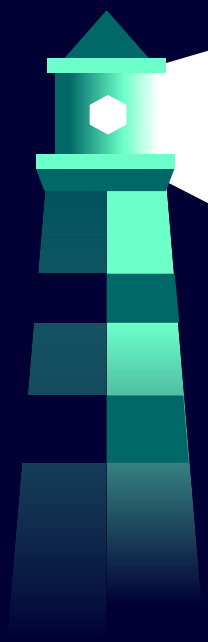
Continually understands the environment

The modern attack surface is dynamic and changes constantly. The right solution will constantly understand attack paths, and inform on how easy they are to update with the latest vulnerabilities and attack techniques, as well as the operational effort required to run continuously.

Provides board-level reporting

Accurately assesses risk and can help support executive and operational reporting processes. The right tool enables boards to quickly grasp how their organization can be attacked, how improvements occur over time because of security investments, changes in processes or implementation of environment hardening, and most importantly, how much risk exists for critical asset.

With these qualifications met, organizations can finally get answers to essential questions such as: "How can I be attacked?", "Which of my critical assets are at risk?", and "How can I mitigate these risks with minimal effort?"



Once you have the right tools, you can build scalable and sustainable exposure management programs, no matter how large or complex your organization and regardless of what types of new exposures emerge.

Authors:
Batya Steinherz - Content Marketing Strategist
Shay Siksik - VP Customer Experience

Contributors:
Menachem Shafran - VP Product & Innovation
Dan Anconina - Chief Information Security Officer
Shira Bendkowski - VP Product
Michael Greenberg - Director of Product Marketing
Tobi Traebing - Technical Director, EMEA

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.