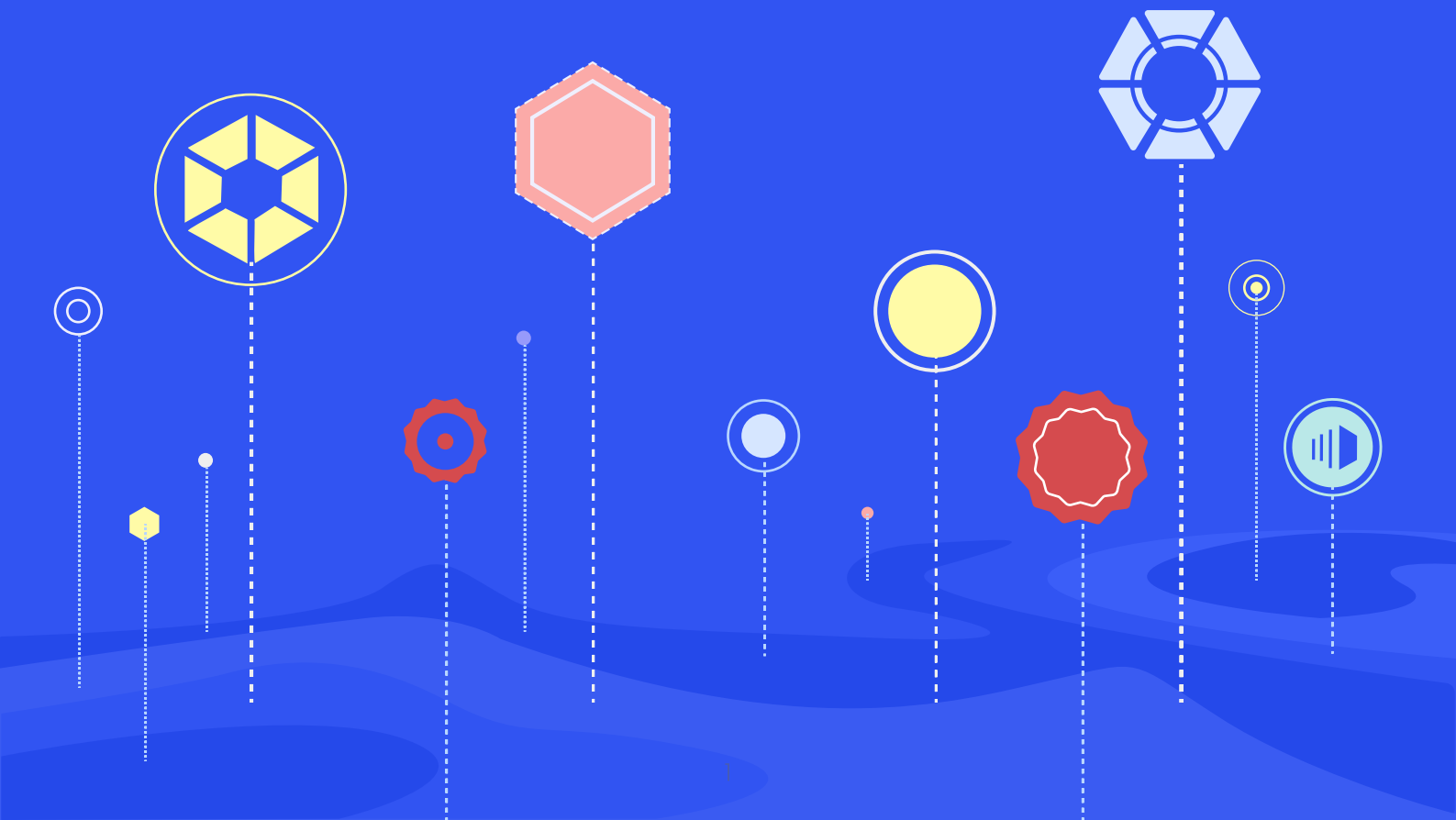
XM Cyber

The Mobilization Trap: Why Remediation Stalls and How to Fix It

An XM Cyber E-Book · June 2026



Contents

The Mobilization Trap 3

Why Automation Alone Won't Fix It 4

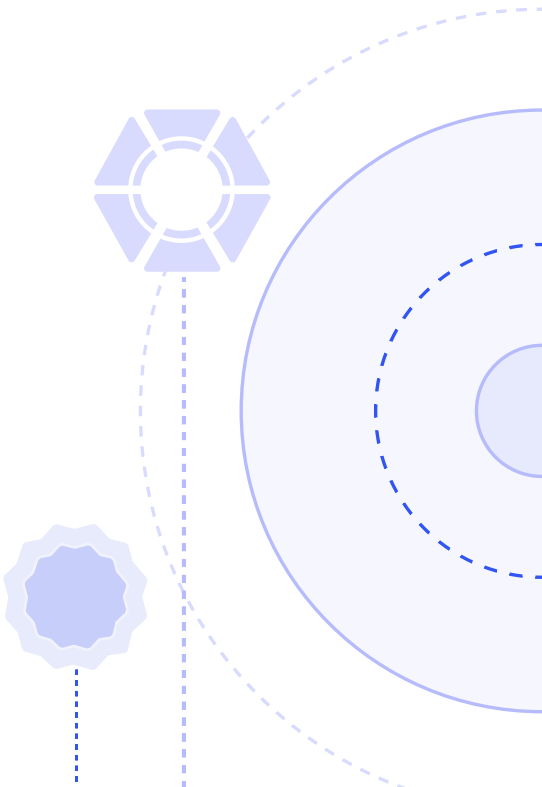
What Effective Mobilization Looks Like 5

The Collaboration Layer 6

Are You Leveraging the Defender's Advantage? 7

The Bottom Line 8

About XM Cyber 9



The Mobilization Trap

Most exposure management programs have no problem discovering and prioritizing findings. Where they consistently break down is at the mobilization stage - getting validated findings to the right teams, through the right tools, and confirming the fix.

It's a common pattern. A security team validates an exposure and routes it to the team responsible for the fix. But that team has its own priorities, its own change windows, and its own definition of 'urgency'. The finding has been technically assigned, but practically? It's unowned. No single process or role bridges the handoff between teams, so findings stall in ticket queues, fixes go unconfirmed, and the exposure stays open.

This failure of coordination shows up in the data:

EXPONENTIAL CVE VOLUMES

Frontier models and Adversarial AI create pervasive challenges of growing CVE backlogs.

49K+

New CVEs expected in 2026
Source: FIRST

LATERAL MOVEMENT HAPPENS FAST

AI-powered attackers are leveraging machine speed more than ever, with time to exploit now measured in hours, not weeks.

29 min

eCrime breakout time in 2025
Source: Crowdstrike 2026

REMEDIATION REMAINS A BLOCKER

Remediation workflows are often hobbled due to enterprise complexity, a stack of tools and non-exploitable systems.

43 days

Median time to remediate KEVs
Source: Verizon DBIR 2026

DIVERSE INITIAL ACCESS VECTORS

While CVEs were the most common initial access vectors, phishing scams or identity exploitation via social profiling remain prevalent.

31%

Breaches where CVE was initial access
Source: Verizon DBIR 2026

EXPLOITS FASTER THAN DISCLOSURE

Attackers increasingly weaponize vulnerabilities before they're even discovered, rendering patch cycles, models obsolete.

42%

YoY rise in CVEs exploited pre-disclosure
Source: Crowdstrike 2026

ATTACKS USING TRUSTED PATHWAYS

The vast majority of breached orgs use compromised valid credentials and trusted access points rather than classic malware.

82%

Malware-free threat detections
Source: Crowdstrike 2026

- The 2026 Verizon DBIR found that remediation timelines grew to 43 days while exploitation timelines compressed to near zero. That's not discovery time or analysis time - it's handoff time. Exploitation moves at machine speed. Mobilization moves at organizational speed.
- The problem gets worse when patching isn't the fix. The CrowdStrike 2026 Global Threat Report found that 82% of attacks used valid credentials rather than malware. That means that adversaries are not even relying on exploits. And remediation for identity and access is often more complex, spanning multiple teams, tools, and approval chains.

This is the mobilization trap: the organization knows what's exposed but can't move fast enough to close it.

Why Automation Alone Won't Fix It

When mobilization is sluggish, the natural response is to automate remediation. And automation (AI-powered or legacy) can indeed close some exposures faster than manual processes – patching known CVEs, rotating credentials, disabling unused accounts.

Yet coordinating that work across teams, tools, and hyper-complex IT environments and approval chains is still where programs stall - and no automation layer solves that. This is because *mobilization is an organizational discipline, not a technology layer.*

Even well-coordinated programs hit the same organizational wall. A finding lands in a remediation queue, and the team responsible for the fix won't act on it because they can't verify it's exploitable. "Show me the proof" is a common response to unvalidated findings. That's because without proof of exploitability, the security team has no way to drive urgency – no proof it's exploitable, no context for what it reaches, no evidence it will ever happen.

And it gets worse. Most remediation teams aren't even at the table. A recent Gartner report found that only 36% of infrastructure and operations teams are actively engaged in vulnerability remediation decisions. That means the remaining 64% aren't part of the process at all – they receive action items without context, ownership, or a clear path to resolution.

> No amount of automation can replace a process that moves validated exposures effectively from the teams that discover them to the teams that fix them.

What Effective Mobilization Looks Like

Mobilization breaks at specific, predictable points. Findings aren't validated, so the handoff stalls. Someone creates a ticket for a workload that can't be patched, and the ticket gets rejected. A fix goes in, no one retests, and the exposure stays open behind a closed ticket. What does it take to fix this? Not new tools – just a set of mobilization best practices that any organization can adopt today.

Scope your program and update the key KPIs used to judge efficacy from CVE volumes and patching % toward the number of exposed critical assets, exposure window, and mean time to eliminate valid attack paths.	**Align on Scope and KPIs**
Continuously validate exposure findings, confirming reachability and exploitability before creating tickets or sending to remediation teams to take action on.	**Validate Findings Before Asking for Action**
Many exposures can't be patched for one reason or another. Wherever possible teams should consider and share alternative mitigation strategies - such as implementing downstream security controls or configuration changes - that eliminate risk in other ways.	**If You Can't Remediate, Mitigate**
By seamlessly integrating exposure management tooling with existing ITSM or case management solutions teams can eliminate friction related to context gathering and information requests.	**Integration Eliminates Friction**
Teams should look to implement AI and automation into their workflows where possible and risk of breaking changes is low.	**Automate Where Possible and Risk is Low**
Continuous testing validates not just that exposures are truly exploitable, but that fixes worked as intended and risk isn't re-introduced into the environment down the line.	**Continuous Testing to Validate Fixes Work**

1. **Focus on choke points, not exposure volume**

   One fix at a convergence point can collapse dozens of attack paths. This was a key reason that XM Cyber won SC Awards Europe 2026 Best Vulnerability Management Solution – our focus on choke points.

2. **Prove exploitability before asking anyone to act**

   Pre-validated findings change the conversation. A remediation team that receives proof of exploitability treats the ticket differently than one that receives a severity score.

3. **Name the alternative when patching isn't an option**

   Compensating controls and workarounds need to be identified before the ticket is created, not after it's rejected.

4. **Route validated findings through existing tools**

   Jira, ServiceNow, whatever's in the stack. The handoff has to meet teams where they already work.

5. **Automate where the risk of the fix is low**

   Credential rotation, disabling unused accounts, and similar changes with easy rollbacks can run without human approval. For higher-risk changes, use automation to stage the workflow and keep a human in the loop for the final decision.

6. **Confirm fixes through continuous retesting**

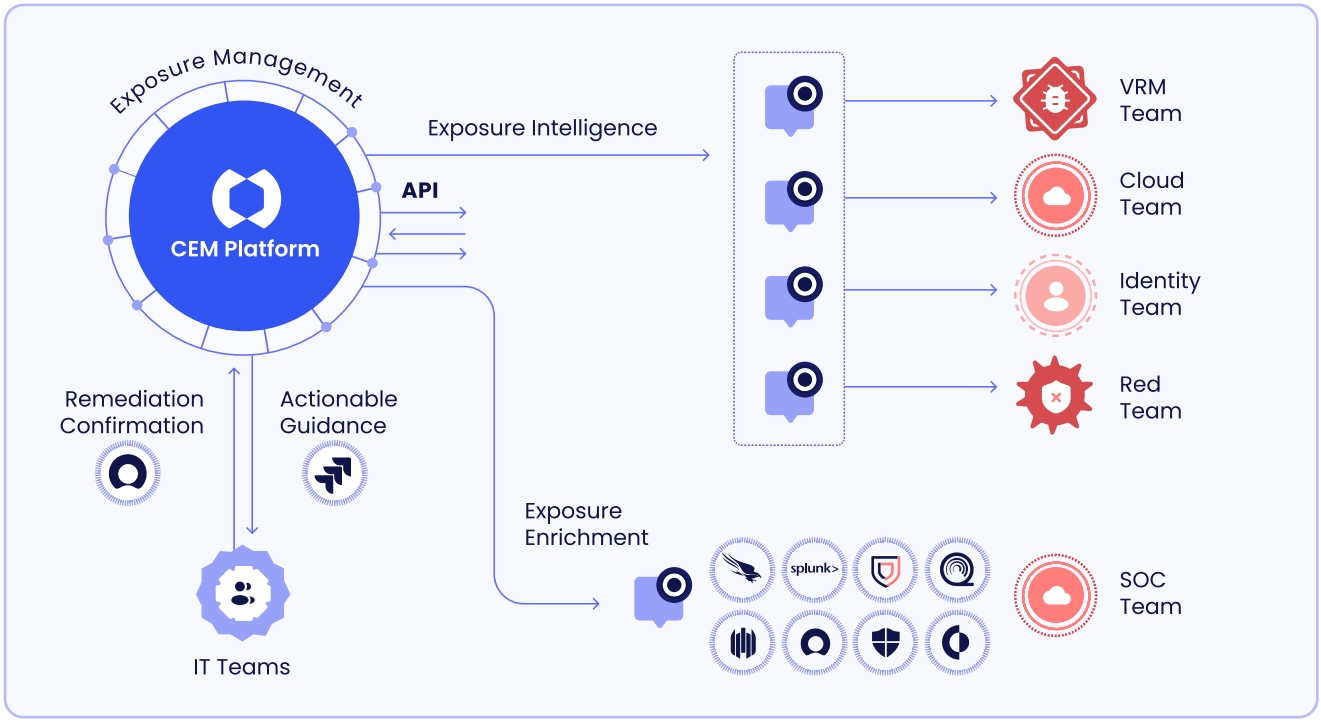
   A closed ticket is not a closed exposure. Assumed closure isn't closure.

Effective mobilization isn't about fixing more – it's about proving what matters, routing it to the right team, and confirming it's closed.

The Collaboration Layer

Security speaks in terms of exposures and attack paths, IT in change windows and uptime, DevOps in deployment cycles, and leadership in risk and revenue. Most organizations are modern Towers of Babel - every team building toward the same goal, none of them speaking the same language. Each team does its job well, yet none share a common frame of reference for what's exploitable, what it could reach, and how urgent remediation is.

Exposure management can serve as that frame - a shared, continuous view that every team reasons from. And this shared view is just the foundation. Someone also has to own the process of keeping teams aligned. Gartner goes so far as to recommend a dedicated Mobilization Coordinator - a program manager who coordinates remediation across teams, functions, and tools.



AI agents can extend that coordination further. They can learn an organization's specific approval chains, change windows, and workflow stages. Then they can build remediation plans tailored to how each organization actually operates - as long as they have a single source of truth for attack surface and exposure context to reason from. The exposure management platform provides that truth. Without it, agents can't reason across disparate data models.

Give every team and every agent the same view of what's exploitable, what it reaches, and what to fix first.

Are You Leveraging the Defender's Advantage?

Defenders operate inside the environment they're protecting. They can see the full topology, identity relationships, compensating controls, and critical assets. Attackers have to discover all of that from the outside. That's a structural advantage no amount of adversarial AI eliminates.

Most exposure management programs don't fully leverage it. Do yours? Try asking these five questions:

1. How many critical corporate assets have a validated attack path from an internet-facing entry point?
2. How has that number changed quarter-over-quarter?
3. What percentage of our remediation effort closed an actual path versus a theoretical finding?
4. Do we know the ways an attacker could create an attack path to our critical assets?
5. Are we continuously assessing all of the possible attack paths to our critical assets?
6. Does our SOC use what we know about our attack surface and exposures to guide detection and response?

If the answers aren't there, the problem isn't discovery or prioritization - it's the process that moves findings from validated risk to confirmed fix.

Track outcomes, not activity. The number of tickets closed means nothing if the paths to your critical assets are still open.

The Bottom Line

The security industry has spent years optimizing the parts of exposure management that technology can solve - discovery, prioritization, validation. Mobilization is the part technology can't solve on its own, and it's where programs often stall.

Defenders see the full environment. Attackers have to guess. That asymmetry can be powerful - yet it erodes when findings die in the space between the team that identified them and the team that owns the fix.

> Mobilization is an organizational discipline. It determines whether everything upstream of it – every scan, every assessment, every validated finding – actually results in reduced risk. The organizations that figure this out will close the paths that matter, confirm they're closed, and prove it in terms everyone understands.

About XM Cyber

XM Cyber is a pioneer in exposure management, transforming how organizations approach cyber risk by continuously validating their hybrid attack surface against real-world threats. By modeling how attackers combine misconfigurations, vulnerabilities, identity exposures, AI exposures, and more across cloud and on-prem environments, XM Cyber shows enterprises all the paths attackers might take, and the most effective ways to block them. This enables leaders to communicate risk effectively and prove security ROI with confident, data-driven reporting.

Acquired by the Schwarz Group in 2021, XM Cyber operates globally with offices in North America, Europe, Asia Pacific, and Israel. For more information, visit www.xmcyber.com.

XM Cyber