MANDIANT
NOW PART OF Google Cloud

PROACTIVE EXPOSURE MANAGEMENT
WHITE PAPER

# Executive Summary: Building Cyber Resiliency

## Digital expansion overwhelms traditional security paradigm

As organizations move from digital transformation to the new phase of digital expansion, the rapidly expanding attack surface—and sophisticated attacks targeting this complexity—increasingly overwhelms the traditional reactive paradigm of threat detection and response (TDR).

CISOs face an inflection point: They must move from reactive to proactive strategies—getting ahead of their adversaries to drive cyber resiliency. But no security team has limitless resources, nor can security patch every vulnerability on their own. The challenge isn't just gaining visibility—it's effectively prioritizing and mobilizing action.

**69%** of security teams admit feeling overwhelmed[1]

**84%** of security leaders worry they're missing threats and incidents because of alert and vulnerability fatigue[2]

## A framework for proactive exposure management

With these challenges growing daily, forward-thinking security leaders and industry analysts are coalescing around a new framework for proactively prioritized exposure management. Gartner® first named this framework Continuous Threat Exposure Management, or CTEM, defined as "a set of processes and capabilities that allow enterprises to continually and consistently evaluate the accessibility, exposure and exploitability of an enterprise's digital and physical assets."[3] This proactive approach combines a broader, continuous look at the expanding attack surface with a process for prioritizing remediation based on both the potential business impact and the feasibility of a security incident.

## The missing element: Knowing what your adversaries know

Knowing what your adversaries know is an essential factor in assessing attack likelihood or feasibility. This threat intelligence proves even more critical in the face of increasingly sophisticated attacks. Yet today's more sophisticated, patiently planned attack patterns hold a silver lining: attack patterns leave a trail of reconnaissance activity.

A new generation of tools and technologies allows security teams to monitor and track these initial reconnaissance activities on the dark web. This threat intelligence provides evidence-based answers to essential questions for interrupting the attack lifecycle:

- Who's targeting you right now?
- Which vulnerabilities are they targeting?
- What is the current state of planning?
- What do they want?

**79%** of security leaders say they make decisions on cyber attacks without insights on who's targeting their organization[4]

1 Mandiant Global Perspectives on Threat Intelligence. February 2023.
2 Ibid.
3 Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, July 2022. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
4 Mandiant Global Perspectives on Threat Intelligence. February 2023.

## Threat intelligence catalyzes proactive exposure management

Applying real-time threat intelligence catalyzes proactive exposure management. Threat intel brings an essential adversary perspective to the calculus of effective threat prioritization. We believe this perspective transforms the five steps of Gartner's CTEM framework (scoping, discovery, prioritization, validation, and mobilization) into a continuous, four-part process:

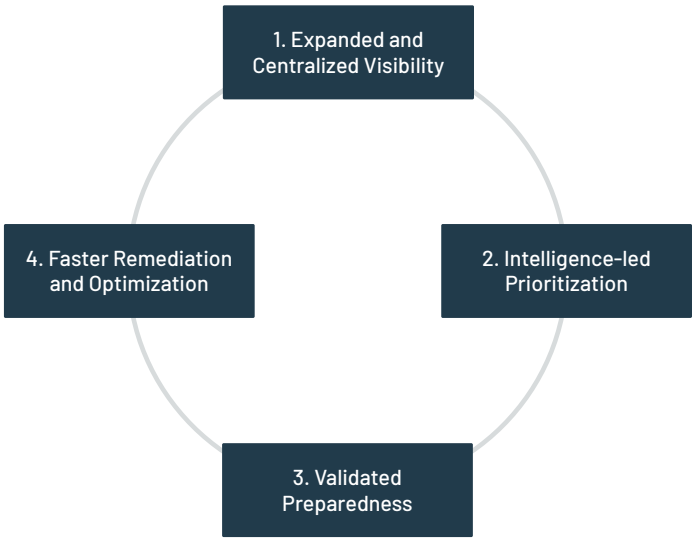



**FIGURE 1.** The continuous process of assessing enterprise assets, digital risks and security posture to continuously evaluate the prioritization and risk mitigation strategy.

### Expanded and centralized visibility

Effectively leveraging new technologies including external attack surface management (EASM), network scanning, and digital risk protection services (DRPS) can help security teams create a more comprehensive map of their organization's full attack surface. But security teams need to think beyond the traditional attack lifecycle in order to identify the creative entry points leveraged by today's cyber attackers. Continuous frontline threat intelligence helps security teams uncover the full breadth of their attack surface and identify specific nodes in that ecosystem that need to be included in the scope of the proactive exposure management program.

### Intelligence-led prioritization

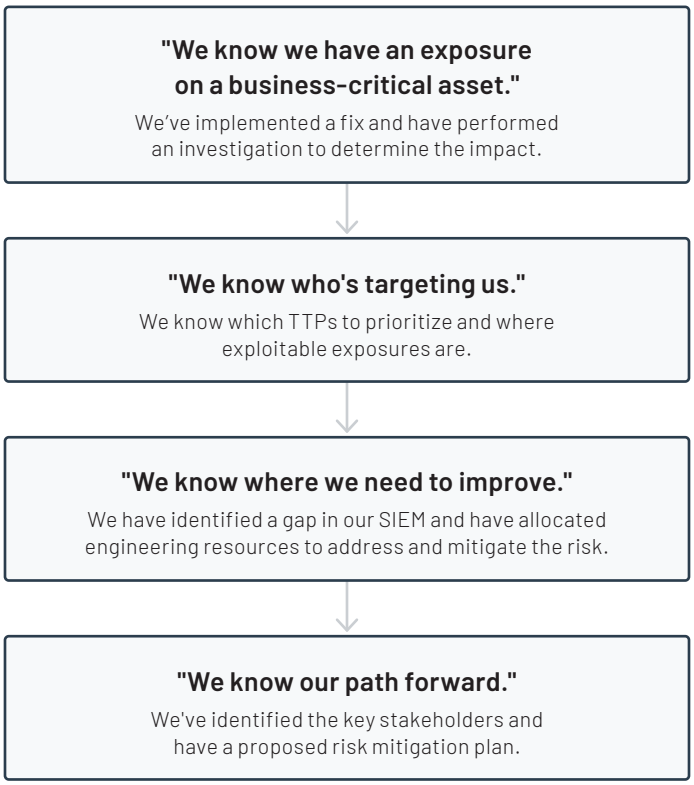
To prioritize effectively, security teams must develop a risk-based approach that considers the likelihood and potential impact of different types of attacks. Proactive exposure management provides a systematic framework for assessing and prioritizing risks so that teams objectively assess the attackability or likelihood of exploitation for a given business-critical exposure. This ensures that the overall calculation and prioritization of risk is focused on those exposures that are most critical to the business and attractive to adversaries.

### Validated preparedness

The exposure management framework brings the same evidence-based prioritization to control validation, targeting critical vulnerabilities and likely attack paths. Using threat intelligence, security teams can think like adversaries and identify exploitable entry points. Security teams can then test the effectiveness of security controls, complementing automated validation tools with more manual approaches like controlled, adversary emulations through penetration testing and red teaming.

### Faster remediation and optimization

The full strength of evidence-based prioritization developed and honed through the first three steps enables security leaders to allocate resources effectively to the most pressing remediation priorities. As non-patchable exposures become more prevalent, this framework empowers security leaders to present a compelling business case to key stakeholders.



## Proactive exposure management: Protecting and enabling the business

With nearly every organization leveraging digital expansion to drive core business operations and create competitive differentiation, CISOs, and security leaders today face a dual mandate: Business protection and business enablement. This layered reality means security leaders must pick their battles. And when they do act, they need to avoid impeding the productivity and collaboration of users or slowing the speed and agility of the business.

Proactive exposure management gives security leaders a framework for walking the line between business protection and business enablement. Critically, frontline threat intelligence powers an even more proactive approach—prioritizing based on attack likelihood and using initial recon to interrupt the attack lifecycle, while hardening infrastructure where it matters most and improving overall cyber resiliency.

Finally, and perhaps most importantly, the evidence-based, threat intel-led approach changes security conversations with other key stakeholders across the business. Instead of talking in terms of theoretical risk, security can motivate stakeholders to take action against very specific, known threats. Armed with an evidence-based business case for focused, strategic action, CISOs can effectively mobilize the cross-functional, collaborative remediation required to resolve the most challenging security gaps—without unduly disrupting the business.

## Prioritize the risks that actually impact your business

As a leader in cyber defense and a trusted advisor to high-assurance organizations building and maturing their cyber security programs, Mandiant provides a comprehensive and purpose-built solution to address the modern enterprise security challenge: Mandiant Proactive Exposure Management helps enterprises reliably and continuously reduce the most critical and attackable exposures—before adversaries act on them.

Be proactive, talk to a Mandiant expert.
https://www.mandiant.com/solutions/proactive-exposure-management

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud