Mandiant

PROACTIVE EXPOSURE
MANAGEMENT WHITE PAPER

Executive Summary: The Security Leaders' Guide to Exposure Management

The promise and risk of digital expansion

The business world again finds itself in the midst of a digital shift that challenges enterprise risk and security teams. Without a moment to rest on the heels of digital transformation, companies large and small are entering a new era of *digital expansion.* But as organizations extend digital capabilities—building out multicloud strategies and leaning further into SaaS, IaaS, and expanding digital supply chain partnerships with vendors—they also expand their potential for attacks. At the same time, the big business of cybercrime is more sophisticated than ever.

Yet the only thing more dangerous than embracing digital expansion is impeding it.

$10.5 TRILLION

The cost of cybercrime projected to hit by 2025[1]

A new paradigm, a new approach: Cyber resiliency and proactive exposure management

To adapt to this new and accelerating reality of broader attack surfaces and more sophisticated adversaries, enterprise risk and security leaders are increasingly moving toward a new paradigm of cyber defense resiliency. Gartner® first defined this approach as a Continuous Threat Exposure Management (CTEM) program, " 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."[2]

This new approach moves away from traditional SecOps focus on prevention. Instead, it harnesses threat intelligence and effective attack surface mapping to effectively prioritize, prepare for, and respond to exploitable vulnerabilities and threats. The "shift-left", or proactive approach to risk mitigation focuses on exposure and threat identification as a key informant to prevention, detection and response.

Exposures vs. vulnerabilities

Exposures go beyond vulnerabilities to include all potential exploitable entry points that can be used by an adversary to gain initial compromise into an organization or supply chain ecosystem. Exposures include conventional vulnerabilities but also include:

- Server misconfigurations
- Security controls missing detections for specific indicators of compromise (IOCs) or commonly used threat actor tactics, techniques and procedures (TTPs)
- Vulnerable software
- Zero-days
- Stolen credentials
- Unknown assets
- Phishing and vishing
- Missing MFA

1 https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/#:~:text=Cybercrime%20is%20big%20business.,%2410.5%20trillion%20annually%20by%202025

2 Gartner, How to Manage Cybersecurity Threats, Not Episodes. Kasey Panetta. August 2023. 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.

Four capabilities of proactive exposure management

Exposure management is not a tool, technology, or one-time exercise, but rather a continuous *process*. The exposure management process can be more easily understood through four essential capabilities of proactive exposure management:

1. Expanded visibility: Integrating insight across the attack surface

Holistic visibility is the foundation for proactive exposure management. Modern tools must provide broad and reliable visibility across the entire attack surface, especially at the edges of the enterprise ecosystem.

Moreover, attack surface visibility must be centralized and integrated—not siloed in disparate feeds from point solutions—for clear understanding and effective prioritization.

2. Intelligence-led prioritization: Knowing what your attackers know

As threat actors move from spray-and-pray tactics to well-organized, well-funded tactics, their advanced attack patterns often leave a trail. With the right people, processes and technologies, security teams can tap into discussions and planning on the dark web, including threat actors' initial reconnaissance activities targeting an organization's ecosystem. By harnessing real-time threat intelligence, security teams can institute an evaluation filtering process that guides them in intelligence-led prioritization:

79% of security leaders say they make decisions on cyber attacks without insights on who's targeting their organization[3]

3. Validated preparedness: Testing response, not just detection

The cyber resiliency paradigm changes the focus of security validation from, "Do the controls block entry?" to "How will the integrated security stack and security team respond to a given attack path?"

This requires a much more nuanced approach to validation: Beyond testing security controls, validation should quantify the effectiveness of the entire SecOps program in defending against targeted attacks—testing each discrete security team response workflow, with a particular focus on testing communication processes to ensure high-priority exposures are properly escalated through the right channels to drive cross-functional remediation.

This more detailed, nuanced approach to validation, combined with the greatly expanded attack surface, could make validation an impractical burden for many organizations. But the proactive exposure management framework uses intelligence-led prioritization to focus validation where it's most critical:

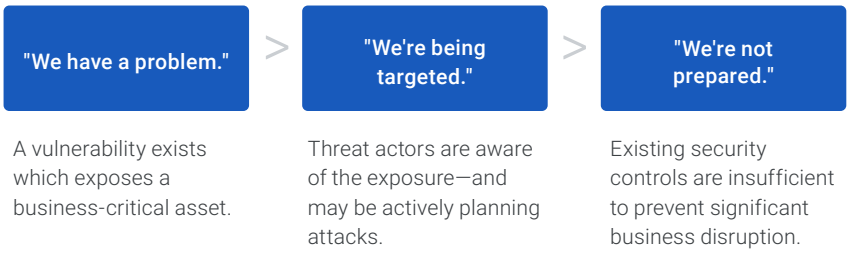
3 Global Perspectives on Threat Intelligence, https://www.mandiant.com/global-perspectives-on-threat-intelligence

4. Optimized remediation: Executing cross-functional response

Modern automated remediation tools are vital for response, but remediating the growing number of critical, non-patchable exposures calls for cross-team collaboration. Security teams must strategize and implement risk reduction tactics such as:

- Integrating threat intelligence into a SIEM or response function
- Communicating with key stakeholders and asset owners
- Reallocating resources to address critical gaps or exposures
- Sharing the current status or posture of the security program and go-forward plan with executives

Shared understanding of cross-functional exposures is key to collective buy-in. The exposure management process serves as a risk filter, enabling security leaders build a business case to address the organization's most business-critical and exploitable exposures:



Building cyber resiliency: Proactively respond to exposures *before your adversaries do*

While the challenges of digital expansion strategies undoubtedly add new pressures for CISOs, this new era also presents an opportunity for the modern CISO to break out of the conventional typecast of "business blocker" and into the role of strategic business *enabler*. Making that shift demands a delicate balance between protecting critical assets and business continuity from increasingly sophisticated attacks—while enabling (not impeding) the speed, agility, collaboration, and innovation of the business.

The emergence of the cyber resilience paradigm is a pragmatic response to this new role of CISO as business enabler. And proactive exposure management provides the framework for making this shift. Leveraging real-time threat intelligence, security teams can triangulate their most attackable, exploitable business-critical assets—and refine that focus through continuous validation to identify where they're prepared, and where they're not. This comprehensive framework arms security leaders with the intelligence to confidently understand, anticipate, and prioritize risk—and effectively focus finite resources where they matter most.

Be proactive, talk to a Google Cloud Security expert.
https://cloud.google.com/security/solutions/proactive-exposure-management