MANDIANT
NOW PART OF Google Cloud



# Exposure Management Evaluation Checklist

To effectively mitigate cyber risk, you need a trusted advisor with proven experience in adversary intelligence who can help identify your top threats, exposures and gaps in detection and response coverage. Use the Exposure Management Evaluation Checklist to identify the best vendor to fit your use cases.

## General Vendor Specifications

- The vendor offers strategic services to help establish exposure management strategies
- The vendor has its own incident response division
- The vendor has multiple physical Global Security Operations Centers worldwide providing security services to different organizations
- The vendor offers executive briefings on the latest threat actor activity
- The vendor has an integrated threat intelligence module
- The vendor has a breach and attack simulation capability
- The vendor offers API interoperability for security and management
- The vendor offers role-based access controls for product offerings.

## Scoping Specifications

Can the vendor(s) identify and assess assets relevant to the business and the threats posed to them? The vendor offers a product or framework for external and internal asset discovery.

- The vendor offers a product or framework for external and internal asset discovery.
- The vendor can provide assistance identifying crown jewel, or business critical assets.
- The vendor has a proven strategy for identifying business assets and owners.
- The vendor has a mechanism to identify unknown or unsanctioned assets.
- The vendor supports hybrid, multi-cloud or on-prem environments.
- The vendor can support third-party monitoring use cases, such as M&A, subsidiary monitoring or supply chain monitoring.
- The vendor offers services to help customers define their unique cyber risk thresholds via tabletop exercises.

## Asset and Threat Discovery Specifications

Can the vendor(s) offer continuous monitoring for known and unknown assets and identify adversary targeting and exploitable vulnerabilities? The vendor can perform continuous asset discovery.

- The vendor can identify adversary targeting and behavior.
- The vendor offers an alerting mechanism for threat activity from the deep and dark web.
- The vendor has a mechanism for identifying when assets are vulnerable, misconfigured or exposed.
- The vendor has a native vulnerability intelligence capability.

## Controls Validation Specifications

Can the vendor(s) identify the attack paths from exploitable entry points to test the effectiveness of security controls against targeted attacks?

- The vendor offers products or services to run continuous security control testing programs.
- The vendor can quantify the results from controls testing.
- The vendor offers attack path modeling after identifying a vulnerability.
- The vendor uses real adversary tactics, techniques and procedures (TTPs) to emulate behavior.
- The vendor reports on overall performance and security control-specific performance in alignment to the MITRE ATT&CK Framework.
- The vendor assesses the remediation and response readiness process and determines if they are adequate for the business.

## Prioritization Specifications

Can the vendor(s) enable you to account for asset criticality, adversary activity, exploitation status and control effectiveness when assigning priority to exposures?

- The vendor provides risk or severity ratings on identified security issues.
- The vendor accounts for adversary activity, vulnerability exploitation status and asset exposure when assigning risk or severity ratings.
- The vendor provides context on vulnerabilities including exploitation state and risk rating.
- The vendor offers remediation recommendations for identified security issues.
- The vendor offers a management console to assign and track the progression of security issues.
- The vendor offers vulnerability management or integrates with vulnerability management tools.
- The vendor offers a framework or strategy for prioritization

## Response and Remediation Specifications

Can the vendor(s) support workflow integrations and internal collaboration?

- The vendor integrates with SIEM, SOAR and Ticketing Systems.
- The vendor enables self-service user management.
- The vendor offers managed or a la carte services to help customers at a strategic, tactical and operational level.
- The vendor offers easily shareable reporting on exposure and remediation progress.
- The vendor helps define what is acceptable risk in the context of the customer organization.
- The vendor can support customers experiencing a breach or incident.

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