Exposure Management Evaluation Checklist

To effectively mitigate cyber risk, partner with an 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 help identify the best vendor to fit your use cases.

General Vendor Specifications

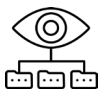
- The vendor can offer strategic services to help establish exposure management strategies
- The vendor can offer incident response services
- The vendor can prove that they have multiple physical Global Security Operations Centers worldwide providing security services to different organizations
- The vendor can offer executive briefings on the latest threat actor activity
- The vendor can offer an integrated threat intelligence module
- The vendor can offer a breach and attack simulation capability
- The vendor can offer API interoperability for security and management
- The vendor can offer 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 can offer a product or framework for external and internal asset discovery
- The vendor can provide assistance identifying crown jewel, or business critical assets
- The vendor can offer a proven strategy for identifying business assets and owners
- The vendor can offer a mechanism to identify unknown or unsanctioned assets
- The vendor can support hybrid, multicloud, 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 can offer 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 continual asset discovery
- The vendor can identify adversary targeting and behavior
- The vendor can offer an alerting mechanism for threat activity from the deep and dark web.
- The vendor can offer a mechanism for identifying when assets are vulnerable, misconfigured or exposed
- The vendor can offer a native vulnerability intelligence capability

Security Controls Validation ☐

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

- The vendor can offer products or services to run continuous security control testing programs
- The vendor can quantify the results from controls testing
- The vendor can offer attack path modeling after identifying a vulnerability
- The vendor can use real adversary tactics, techniques and procedures (TTPs) to emulate behavior
- The vendor can report on overall performance and security control-specific performance in alignment to the MITRE ATT&CK Framework
- The vendor can assess 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 can provide risk or severity ratings on identified security issues
- The vendor can account for adversary activity, vulnerability exploitation status and asset exposure when assigning risk or severity ratings
- The vendor can provide context on vulnerabilities including exploitation state and risk rating
- The vendor can offer remediation recommendations for identified security issues
- The vendor can offer a management console to assign and track the progression of security issues
- The vendor can offer vulnerability management or integrates with vulnerability management tools
- The vendor can offer a framework or strategy for prioritization

Response and Remediation Specifications ☐

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

- The vendor can integrate with SIEM, SOAR and Ticketing Systems
- The vendor can enable self-service user management
- The vendor can offer managed or a la carte services to help customers at a strategic, tactical and operational level
- The vendor can offer easily shareable reporting on exposure and remediation progress
- The vendor can help 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 Google Cloud Security expert.
https://cloud.google.com/security/solutions/proactive-exposure-management?hl=en