Approach to Continuous Threat Exposure Management (CTEM)

Gartner has adopted a new methodology for ensuring continuous threat expousure is managed. This process adopts several techniques to identify a qualified threat-risk exposure's weakness / vulnerability. Then to quantify the probability of the vulnderability to actually be exploited, and prioritize the prospect of threat exposure against the organizations risk management protective measures to determine resiliency. Lastly, to repeat this in a continuous cycle to ensure the organization's resiliency to exposure is managed within its means and financial tolerances.

Gartner Quote from CTEM Program published July 2022: (ID G00763954)

> **Enterprises fail at reducing their exposure to threats through self-assessmentof risks because of unrealistic, siloed and tool-centric approaches. Security and risk management leaders must initiate and mature a continuous threat exposure management program to stay ahead of threats.**

The RiskOpsAI™ fulfillment of Gartner's emerging CTEM (Continuous Threat Exposure Management) category offers a continuous and predictive AI Native Integrated Risk Modeling & Decisioning Platform® (IRMD®) approach to wholistic threat-risk governance / management. RiskOpsAI™ provides this ability through a series effective AI driven quantitative foresight threat-risk exposure decision-making techniques as aligned with the organization's risk goals and objects driving brand protections.

- Organizations carry significant risk in today's rapidly changing informational and operational technology landscapes, where predicting and minimizing the impact of smaller multiple resiliency risks can indirectly or directly represent a significant material breach.
- The current tactical approach to digital risk management (reactive, siloed, periodic and piecemeal) fails to connect the impact of risk to an organization's business goals and objectives.

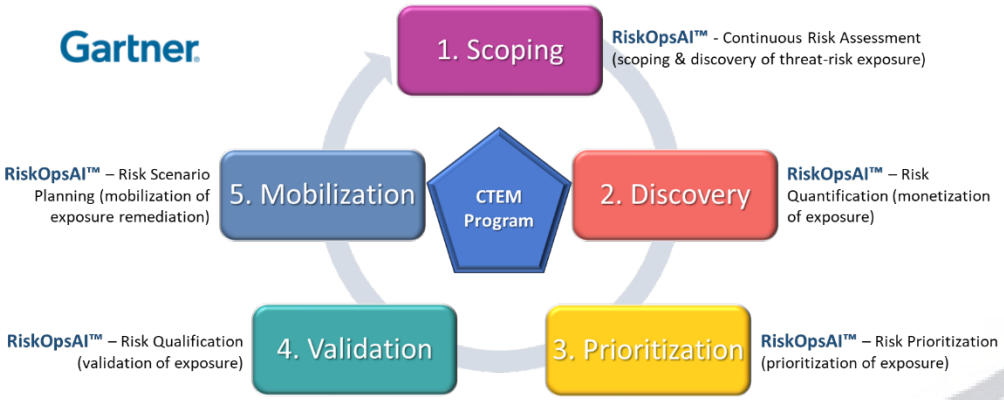
Continuous Threat-Risk Resiliency-Exposure Management™ (CTREM™)

RiskOpsAI's AI Native CTREM™ solution broadens the scope of coverage to include a governance centric approach to traditional IT / Cyber Security with the addition of IOT/OT/IIOT (ICS) driven under the IEC 62443 controls which brings digital business into a common threat-risk exposure management structure.

- ✓ The RiskOpsAI™ CTREM™ platform provides detailed drill down analytics (by threat/risk framework, provider, function, Geo, product or in a hybrid view as needed) where each threat-risk exposure is identified, quantified, prioritized, and reported for informed decision-making.
- ✓ These can then be correlated with actionable remediation or other measures which may be automated with Risk Orchestration Automation Response® (ROAR®).

A Comprehensive View of CTEM within RiskOpsAI™ CTRM™

This illustrates the steps through the CTEM process which is defined to address and ensure the ability to continuously monitor threat exposure. RiskOpsAI™ uses these steps with our CTRM™ models to bring them to life in near-real-time modes.



Step 1: is establishing the process for continuous risk assessments.

Step 2: is designed to ensure threat-risk exposure is monetized using quantification.

Step 3: is the prioritization which is the tricky part if not aligned with a quantification prioritization methodology.

Step 4: is the quantification of exposure to align with a monetized value of probable financial impact to the brand and the resilience to absorb, resist, or contain threat-risks as the occur and not via an anticipated scenario predicted based on historical data.

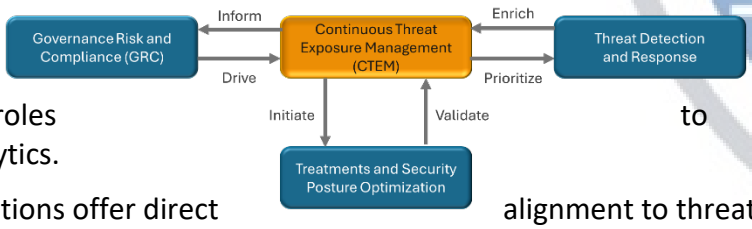
Step 5: is the ability of the organization to swiftly act upon this quantified information to address threat-risk as the velocity in which they evolve and not as they have been.

The true value of an AI Driven qualitative and quantitative approach establishes the ML to learn through the organizations' unique characteristics, what resiliency means to the organization.

AI Native Continuous Threat-Risk Exposure Analytics & Visibilities

RiskOpsAI™ AI Native CTREM™ platform generates dashboards that are highly configurable for multiple use cases and personas. Furthermore, each dashboard is highly customizable for multiple purposes and roles to generate a wide range of Digital Providers analytics.

Continuous Threat-Risk Resilience Exposure Management



Comprehensive and customizable visual illustrations offer direct alignment to threat correlations which quickly identify where threat-risks originate and their impact on business operations. This provides direct correlations to Gartner's Continuous Threat Exposure Management (CTEM) capability extended with ROAR®.

Governing decision, through meaningful / prioritized visualization insights minimize negative events, enables continuous support for resources and support business goals.

About OptimEyes AI® d.b.a. RiskOpsAI™ (Risk Operations Using AI™)

San Diego-based OptimEyes AI® doing business as RiskOpsAI™ known as the Integrated Risk Modeling & Decisioning® Company, is a pioneer of AI-driven, IRMR methodologies. Built by cyber, risk, and compliance veterans, our software-as-a-service (SaaS) platform helps Fortune 2000 organizations discover, measure, prioritize, predict, and optimize cybersecurity, data privacy, and enterprise risks. For more information, contact us at info@optimeyes.ai, and visit https://optimeyes.ai, and follow us on:

**** For a No Obligation Risk Assessment evaluation, please contact: sales@optimeyes.ai***