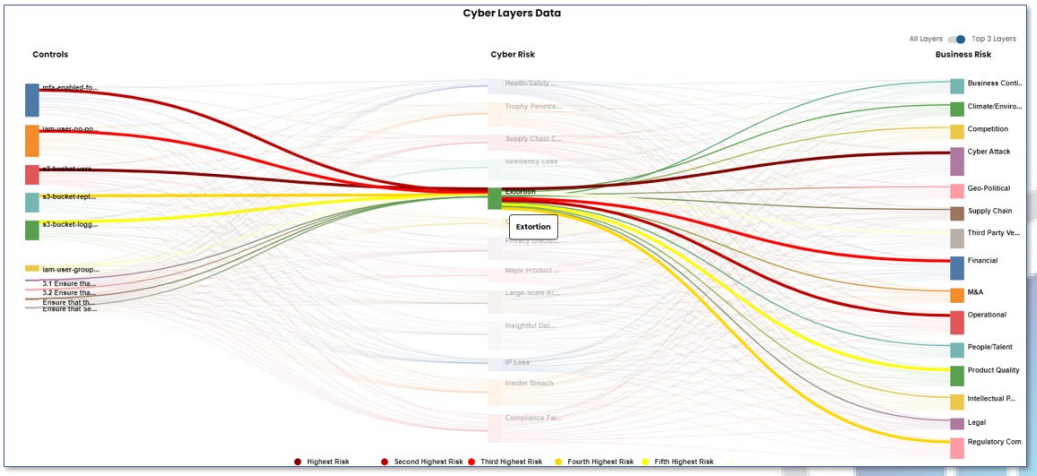
Threat Orchestration Automation Response™ (TOAR®)

Orchestrating Tactical Threat Response against the Strategic Business Risk Layer

Automating the orchestration of intermediation / remediation of threat activities are highly desired features in today's Cyber Security (CS) & Governance Risk Compliance (GRC) landscape. The lack of necessary skills, quality, and availability of these resources drives organizations to incorporate as much intelligent orchestration via automation as possible. This brings the establishment RiskOpsAI's Integrated Risk Modeling & Decisioning Platform® (IRMD®) Threat Orchestration Automation Response™ (TOAR®) to the forefront of requirements for any such platform. To enrich threat driven risk data and then act upon that data using automated common functions, processes, or routine activities which tactically leverage business goals and objective risks as a driving force, is a powerful feature to protect the brand's future.

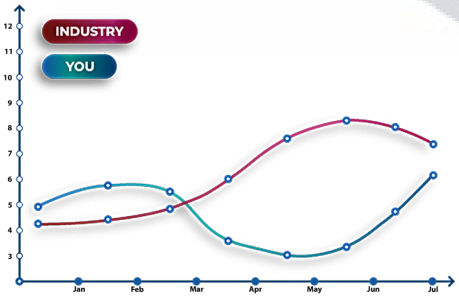


What is TOAR?

TOAR® is the potential to tactically leverage threat landscape information and allow the organization to prevent or lessen brand harm with threat intelligence-based risk data. This shifts the traditional reactionary paradigm with automated intelligent responses to address events at the sheer speed at which organizational threats appear without warning. TOAR® enables swift reaction times to risk(s) exposed within advanced persistent threats (APTs), GenAI driven malware (Ransomware), or other forms of data manipulation, infiltration, loss, or catastrophic material breach. TOAR® is liken to what Gartner's defined SOAR™ (Security Orchestration Automation Response) as having the ability to automate, programmatic or repeatable responses. The difference is TOAR® has a higher degree of threat intelligence behind it where AI/ML is used to enrich the threat data within the context of risk decisioning for which the threats are targeted. The threat causality effect provides the highest degree of risk accuracy and speed of decisioning which is not currently available in traditional ERM/GRC/SOAR programs.

Uniqueness of Brand Threat Protection

The RiskOpsAI™ value is how well we understand threat driven risk affects the levels of business.



Our IRMD® uniqueness is where the act of threats impact to the Business Risk Layer is reduced by establishing orchestrated automation at the appropriate level. This lowers the threat's likelihood while offering visibility, maturity, and agility which provide and protect business operational resiliency.

True value is deploying TOAR® with its integrated ability to facilitate the various business layer objectives and to prioritize them to directly affect Brand threats in the context of a business-driven response.

Cybersecurity Transition to TOAR™

The TOAR® Journey is where RiskOpsAI™ provides a platform from which a cost-effective transition of approximately one FTE for the RiskOpsAI™ TOAR® » translating tactical threats to strategic risk avoidance / mitigation at the various business layers.

Driving risk decisioning based on Brand threat conseqences enhances business resiliency across all operational risk layers. Thus demonstrating the integrated business functionality with Brand awareness.

Threat Decision Orchestration for CXOs

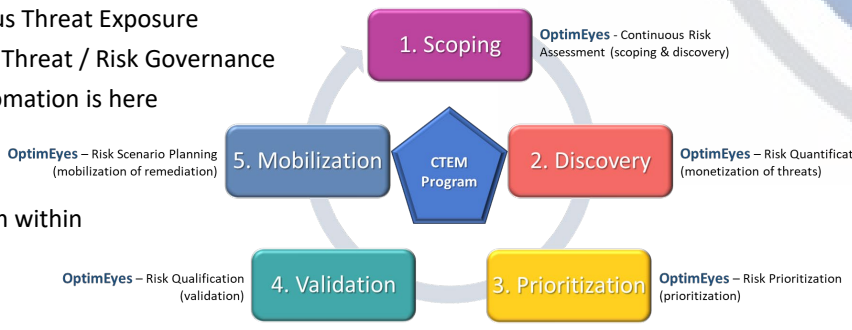
RiskOpsAI™ IRMD® AI/ML driven platform provide a consolidated view of enterprise risk driven by active / prospective threats leveraged within our High Fidelity Single Source of Truth™.

This enables organizations to establish the threat context of many types of risks, in a side-by-side and on-demand reporting context. Threats can impact cybersecurity, data privacy, regulatory compliance, operational effectiveness, supply chain resilience, and more. This tactical threat decisioning is referred to as '**TOAR®' – *Threat Orchestration Automation Response™*** bringing AI/ML capability to life.

This creates a timely and contextualized enterprise-wide view of the organization's unique threat / risk profile. It eliminates informational and operational silos common in enterprise risk management and empowers tactical threat / risk managers, strategic executives, and board members to compare different sources of threat / risk exposure creating clarity of the highest risk-based threats facing the organization.

Need for TOAR®

With industry analysis driving the emergence of Continuous Threat Exposure Management (CTEM' by Gartner) and a holistic Enterprise Threat / Risk Governance model (CSFv2, SEC, DORA, NIS2), the need for tactical automation is here today. The ability to tactically react, response, report and govern the threat / risk landscape to strategic business driven goals and objectives with full visibility from within all layers of business is paramount to every organization.



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 Native, 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***