TAG

HOW BALBIX LEVERAGES ARTIFICIAL INTELLIGENCE FOR CYBER RISK QUANTIFICATION

DR. EDWARD AMOROSO,
FOUNDER & CEO, TAG
RESEARCH PROFESSOR, NYU

HOW BALBIX LEVERAGES ARTIFICIAL INTELLIGENCE FOR CYBER RISK QUANTIFICATION

DR. EDWARD AMOROSO, CEO, TAG,
RESEARCH PROFESSOR, NYU

This report outlines groundbreaking work at Balbix where artificial intelligence (AI) is enabling cybersecurity teams across all sectors and sizes to obtain accurate, on-demand, aggregated cyber risk quantification (CRQ) of applicable target networks. We provide here a background on CRQ, AI, and the Balbix platform, followed by an examination of how AI-powered CRQ from Balbix can advance security operations toward greater accuracy and coverage.

INTRODUCTION

The complex task of protecting an enterprise from cyber threats is now shifting from art to science, and one of the most promising methods driving this trend is the quantification of cyber risk. By quantification, we mean the measured use of collected telemetry for the purpose of analysis with respect to a well-defined metric. As one would expect, AI technology is well-suited for this task and is, in fact, now the approach we recommend at TAG.

In this report, we focus on how cybersecurity vendor Balbix employs advanced AI-based processing and analysis to create accurate and complete views of cyber risk posture. The platform offers useful qualitative assistance in the form of high-fidelity information and insights, but perhaps the most valuable aspect of the Balbix approach is that aggregate cyber risk can be quantified in a way that allows for precise and predictive analysis.

Our intent here is to not only introduce and provide an overview of the commercial Balbix platform, which we view as a state-of-the-art tool for security protection, but also to offer guidance on the advantages of cyber risk quantification in general. We hope that reader will come away from our report with a renewed sense that cyber defense does not have to rely on intuition and guessing, but rather on data quantification in the context of a good metric.

WHAT IS CYBER RISK QUANTIFICATION?

The compliance community has been a forceful driver of CRQ, demanding (perhaps irrelevant) metrics on patch coverage, responses to phish tests, completion rates of annual training, and numbers of residual accepted risks. For this reason, many observers equate CRQ with risk dashboards that are intended for auditors, managers, and executives. In the work reported here, we take a much broader view–one that is focused more on real-time posture.

Readers should recognize that when we reference real-time posture, another community comes to mind–namely, the attack surface management (ASM) vendors and their massive user base across enterprise, government, and service providers. This is perhaps more closely aligned with our view of CRQ here–but this is also somewhat limiting because it leaves out static compliance posture, which is an important balancing view for risk quantification.

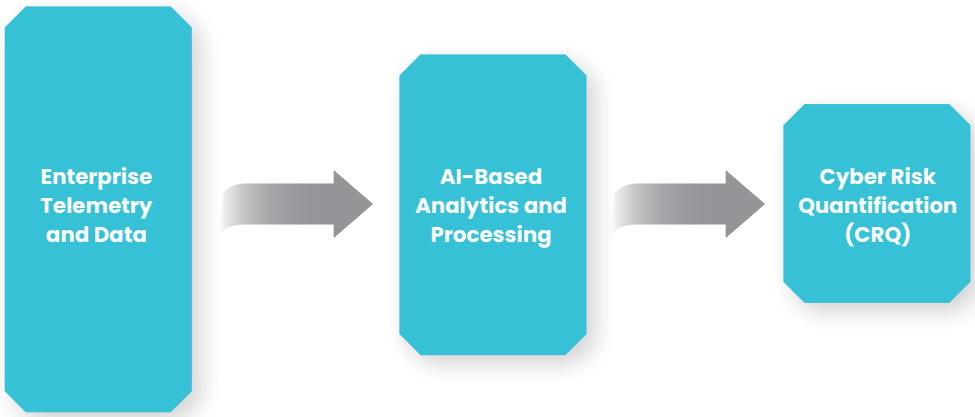

Figure 1. High-Level View of CRQ Pipeline

Thus, we will adopt here a view that CRQ introduces structured, data-driven methods to estimate the financial, operational, and reputational impacts of potential cyber incidents. That is perhaps a mouthful, but as we explain the Balbix approach, hopefully this will become clearer. In short, CRQ should apply to almost any type of inquiry, question, or demand that a security team might have–and AI is well-suited to ensure that the response is proper.

When CRQ is done well, organizations can prioritize their vulnerabilities based on measurable business consequences, rather than simply counting known common vulnerabilities and exposures (CVEs) or issuing severity scores. By tying vulnerabilities, misconfigurations, and exposed assets to actual numeric estimates, security teams can better align remediation efforts with enterprise risk tolerance and strategic objectives.

COMBINING CRQ WITH ASM

When combined with ASM tools, CRQ enables a more dynamic and continuous risk posture. Modern ASM platforms provide near-real-time visibility into internal and external assets that could be targeted by attackers, from cloud workloads and IoT devices to third-party software components. Integrating CRQ methodologies with these discovery and monitoring capabilities allows organizations to maintain an up-to-date, quantified view of their threat exposure.

Perhaps most importantly, CRQ in the context of ASM shifts cybersecurity discussions out of technical silos and into the language of executive leadership and boards. For example, CISOs can present quantifiable risk figures tied to specific elements of the attack surface, such as explaining that "misconfigured cloud storage buckets expose us to a $5M risk scenario," instead of trying to help executives make sense of abstract alerts or vulnerability counts.

It has also been our experience that such financial security posture framing–so long as it is done responsibly–enables better budgeting decisions, supports cyber insurance negotiations, and strengthens the enterprise's overall governance of digital risk. At a time when the attack surface for most organizations continue to expand, CRQ-guided ASM provides a practical, defensible way to prioritize what matters most.

CAN AI IMPROVE CRQ?

Our experience is that AI can significantly improve CRQ within attack surface management (ASM) by making the process faster, more accurate, and more adaptive to changing conditions. This is good news for cybersecurity teams who might be grappling with several pressures at the same time–including the need to address increasingly intelligent and AI-enabled offensive attacks while also dealing with the need to rationalize or even reduce overall costs.

AI models are helpful by automatically correlating vulnerabilities, exposures, and asset data with threat intelligence feeds, incident history, and external risk signals. Instead of relying on manual mapping or static scoring systems, AI can dynamically infer which exposed assets are most likely to be targeted based on attacker behaviors and evolving threat trends, thus providing more precise input for quantification models.

Second, AI can enhance predictive modeling by learning from historical incidents to estimate the likelihood and potential impact of various attack scenarios. For example, by analyzing thousands of previous breaches across industries, machine learning models can help predict the financial impact of a compromised application server versus a misconfigured cloud database, based on context like asset criticality, existing controls, and attacker motivations.

This approach allows enterprises to generate CRQ outputs that are not only based on what is visible in the attack surface today, but also on what could happen tomorrow — essentially creating a forward-looking risk posture. Our experience is that too few security schemes take this issue into account–namely, that most of the problems that must be addressed in the future are only dimly understood today.

Finally, AI can continuously update and recalibrate CRQ outputs as new asset discoveries, configuration changes, or external threat developments occur. Rather than running CRQ as a quarterly or annual exercise, AI-driven systems can provide live risk scores tied to the evolving attack surface, giving CISOs real-time decision support. Over time, reinforcement learning techniques can even fine-tune risk models based on observed incident outcomes.

FIVE SPECIFIC WAYS AI ENHANCES CRQ

For practitioners dealing with enterprise security issues, the question that emerges is how CRQ, enhanced with AI, solves actual problems in their day-to-day work. Our experience suggests that by enabling a more comprehensive means for both CRQ and ASM, CISO-led teams will find real improvements and advantage in the following aspects of their work, at both a management and hands-on level:

1. **Improved Justification for Risk Calculation**–As explained above, the use of AI within Balbix allows for the automated correlation of asset data, vulnerability context, and threat intelligence for risk calculations. Rather than relying on static frameworks or subjective judgment, Balbix's AI models ingest

real-time telemetry and historical incident patterns to produce quantified outputs that can be traced to data-backed justifications. This provides risk managers and CISOs with evidence-based rationales for prioritization, resource allocation, and reporting. It also reduces dependence on manual scoring methods that may not fully capture the attack surface.

2. **Creating Actionable Cyber Risk Recommendations**–Balbix's AI not only quantifies risk but also translates results to remediation actions. For example, the platform can automatically identify high-risk misconfigurations and generate prioritized remediation tasks that reflect their impact on enterprise risk exposure. These recommendations are aligned with business objectives and expressed in financial terms, enabling organizations to make decisions grounded in both technical severity and business consequence. This helps bridge the gap between security teams and business stakeholders, turning telemetry into business-aligned action items.

3. **Enhances Security for Lower Maturity Organizations**–Organizations with lower levels of cybersecurity maturity often struggle with incomplete asset inventories, limited visibility, and unprioritized vulnerabilities. Balbix addresses this with AI to infer missing data, normalize fragmented sources, and build a view of risk without requiring pre-existing infrastructure. This democratizes access to CRQ by making it feasible for mid-sized enterprises and under-resourced security teams to obtain the same quality of insights as more mature teams. As a result, even those early in their security modernization journey can make better risk decisions.

4. **Addresses the Need for Security in Budget**-Constrained Environments–AI-powered CRQ enables smarter security spending by identifying the assets, controls, and exposures that pose the greatest risk. This allows budget-constrained organizations to optimize their resources by focusing investments where they will have the greatest return in terms of risk reduction. Balbix supports this with cost-impact analysis that highlights risk deltas associated with remediation efforts, allowing CISOs to justify expenditures to CFOs and boards in language they understand. In doing so, Balbix helps align security planning with enterprise financial strategy.

5. **Removes Management Doubt Regarding Risk-Related Actions**–Balbix provides a real-time, data-driven foundation for security decision-making that helps eliminate uncertainty by executive management. By presenting quantifications of cyber risk, backed by continuous AI analysis of live telemetry, the platform empowers CISOs to make better recommendations. Executives no longer have to rely on vague assertions about threats or generic severity ratings. Instead, they can see how risk changes over time, which remediation steps are most effective, and where resources should be directed.

HOW DOES BALBIX LEVERAGE AI FOR CRQ?

As we have repeated, Balbix employs an AI-driven approach to CRQ, integrating advanced machine learning techniques to provide an understanding of cyber risk. By analyzing data from cybersecurity and IT tools, as well as external sources, Balbix's ensemble of AI models assists in building a clean asset inventory, identifying vulnerabilities, and evaluating controls. This enables the platform to quantify risk in monetary terms.

The platform's AI capabilities also extend to ASM, where it categorizes assets by type, geolocation, owner, and impact. Balbix's AI models assess risk drivers such as exposure, exploitability, and severity, considering factors like asset configurations, vulnerabilities, adversary behaviors, and the effectiveness of security operations. This allows for a data-driven and actionable risk quantification, enabling organizations to prioritize remediation.

In addition, Balbix's approach facilitates real-time risk assessment and decision-making by continuously updating risk metrics as new data becomes available. The platform's integration with IT and security tools ensures a unified view of assets, exposures, and vulnerabilities, and compliance reporting. By translating technical risks into financial metrics, Balbix empowers leaders to better communicate the ROI of cybersecurity investments.

CYBER RISK QUANTIFICATION MATURITY JOURNEY

One way to view the maturity journey supported by Balbix involves the metaphor of "crawling, walking, running, and then . . . flying." This metaphor for CRQ maturity clearly illustrates the industry progression toward AI-driven, agentic CRQ. This is not proprietary to Balbix, of course, but rather, it provides a universal framework that helps readers evaluate their own maturity.

Ultimately, Cyber Risk Quantification, like many enterprise capabilities, matures through defined phases. The industry is moving from ad hoc, spreadsheet-based approaches ('Crawl') toward automated, AI-driven risk optimization ('Fly'). Balbix's platform aligns with this trajectory, offering tooling that enables organizations to accelerate their progression.

RISK CALCULATION MODEL

In order to understand CRQ, it obviously helps to have a good understanding of cyber risk in general. The textbook view is that risk is drive by the likelihood of an attack, combined with the consequence or impact of that attack. Understanding this equation (usually written as Risk = Probability X Consequence) provides some analytic rigor to the notion of CRQ. This formula is widely accepted and helps ground the AI-based outputs in understandable math.

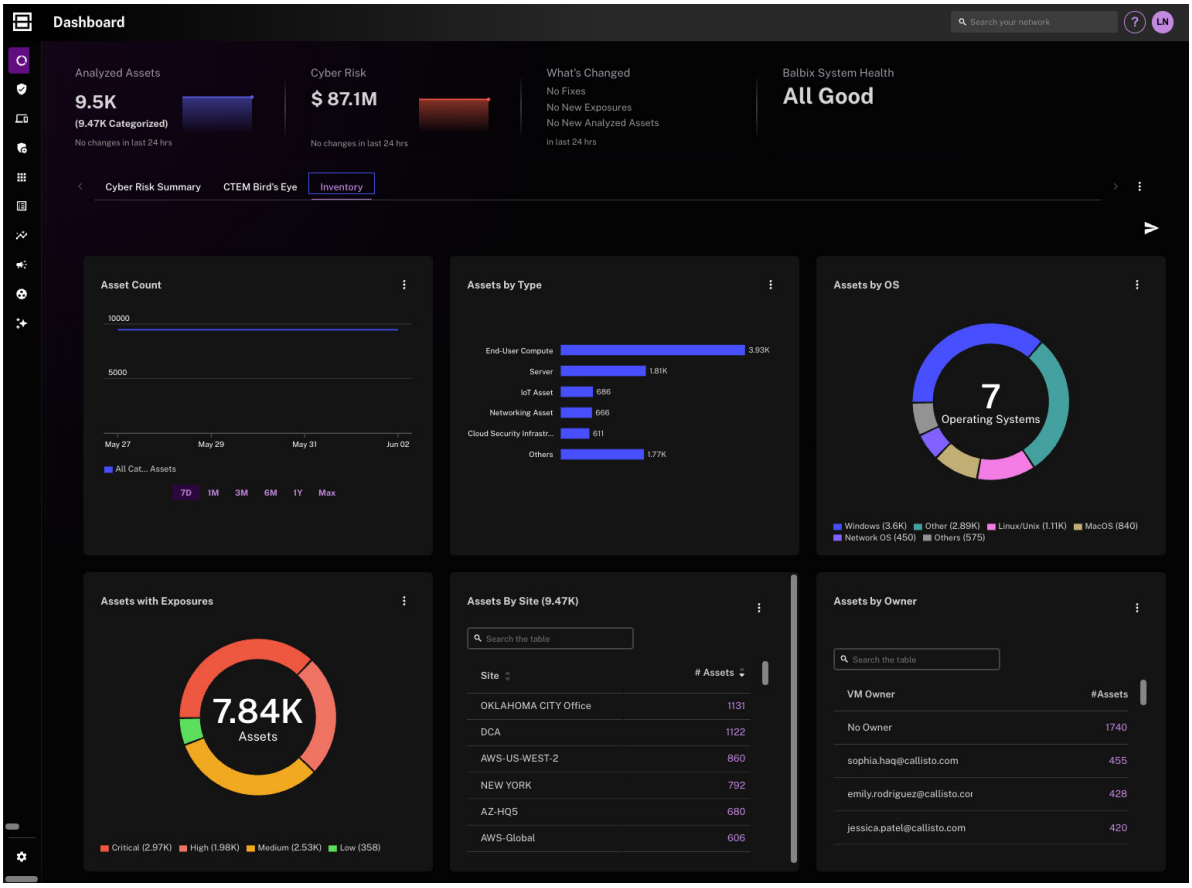

Figure 2. Balbix Dashboard Showing Risk Components

Any CRQ platform, whether AI-enabled or otherwise, must ultimately adhere to a defensible risk model. And as we outline above, the core formula, where risk equals the product of likelihood and consequence, remains foundational. Platforms like Balbix enhance this through dynamic inputs and real-time modeling, but the underlying structure remains constant.

CRQ EXECUTION FLOW

A useful means for understanding CRQ execution flow in practice involves three common stages that enterprise teams will find when they commit to this discipline: The first stage involves visibility, the second stage involves prioritization, and the third stage involves mobilization. We believe that this three-stage process summarizes the operationalization of CRQ in a way that is clear, outcome-driven, and tool-agnostic.

In fact, our view is that successful CRQ adoption depends on more than accurate risk scoring. Enterprises need clear processes to drive decisions. By first gaining visibility, then prioritizing based on risk, and then mobilizing for actual risk reduction captures the practical flow needed to turn CRQ insights into outcomes. Readers are encouraged to instantiate this model to their local context.

BIX CYBER ASSISTANT FOR CRQ

As enterprises move toward continuous risk management, there remains a critical need for intuitive and accessible interfaces that allow technical and non-technical stakeholders to extract value from cybersecurity data. To meet this need, Balbix has developed BIX, an AI-powered assistant designed to serve as the primary conversational interface into the platform's analytics, telemetry, and CRQ insights.

At its core, BIX leverages large language model (LLM) capabilities, tightly integrated with Balbix's underlying AI-driven data fabric. This enables users to pose natural language queries such as "What is the top risk in our cloud environment this week?" or "Which business unit faces the highest potential financial impact from unpatched systems?" The assistant interprets intent and support action from live models, pipelines, and contextual metadata.

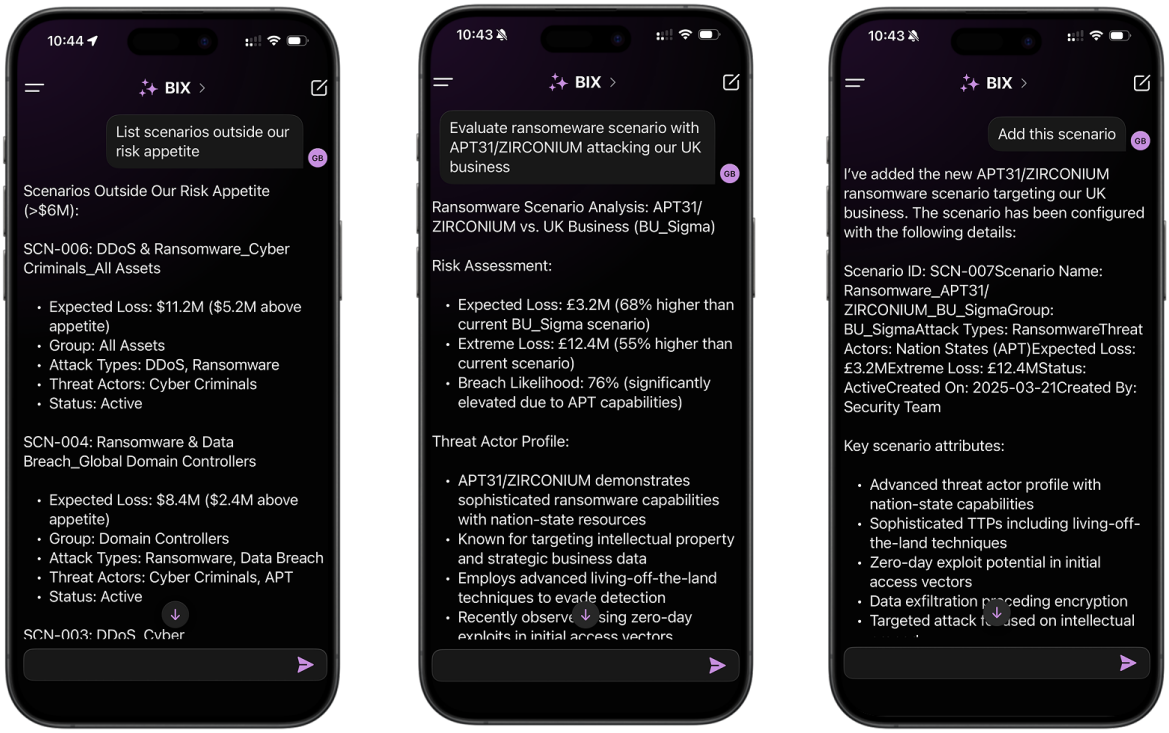

Figure 3. Screen Shots of BIX AI Assistant

BIX is not merely a chatbot or front-end tool. It is context-aware, meaning it understands the risk hierarchies, asset criticality, control effectiveness, and business mappings unique to each enterprise. For example, when asked about risk scenarios related to a specific project or geography, BIX interprets this in light of current threat exposure, historical incident data, and financial risk thresholds. Functionally, BIX supports several key use cases:

- **Live Risk Inquiry:** Users can ask for risk summaries by business unit, asset class, or exposure type, and receive responses enriched with visualizations or drill-down links into the full CRQ model.
- **Remediation Support:** BIX helps identify prioritized actions by surfacing top risk drivers and guiding users to remediation workflows, often integrating with ticketing systems like ServiceNow or Jira.
- **Executive Briefing Preparation:** By compiling risk metrics, historical trends, and supporting rationale, BIX enables faster creation of board-level summaries and presentations, framed in business terms.
- **Training and Onboarding:** New team members can use BIX to quickly understand how risk is structured in the environment and how decisions are made based on quantified data.

We have observed that the BIX design and implementation adhere to strict access controls and enterprise governance rules. It respects role-based access, only disclosing information authorized for a given user. It also supports an audit trail, logging questions and responses to ensure transparency and compliance in regulated environments. This is especially important for any application introduced to highly audited environments.

In our view, BIX represents a real advancement in the usability of CRQ platforms. As AI increasingly mediates the human-machine interface in cybersecurity operations, assistants like BIX will be critical to scaling insights across functional boundaries—reducing dependency on subject-matter bottlenecks and enabling a broader range of stakeholders to engage with and act upon enterprise risk data.

RECOMMENDED ACTION PLAN FOR ENTERPRISE

The following action plan for CISOs should be helpful in their goal to implement Balbix for AI-Driven CRQ and ASM:

Step 1: Define Strategic Objectives and Stakeholder Buy-In
Teams should start by establishing clear goals for the Balbix deployment, including dynamic attack surface visibility, dollar-based risk metrics, optimized prioritization of security efforts, and better board communication. They should then convene executive stakeholders (e.g., CFO, CIO, risk management, internal audit) early to align expectations and emphasize that Balbix will translate technical cyber risk into business terms (e.g., financial exposure).

Step 2: Prepare Data Sources and Enterprise Integrations
Teams should next create an inventory of the systems Balbix needs to ingest from. This can include asset management (e.g., CMDB), vulnerability scanners (e.g., Tenable, Qualys, Rapid7), cloud providers (e.g., AWS, Azure, GCP), identity providers (e.g., Okta, AD), and endpoint tools (e.g., CrowdStrike, Microsoft Defender). It is wise to prioritize clean and reliable feeds, emphasizing that garbage in, garbage out applies heavily to CRQ. Assign a technical team to review and prepare API connections, access rights, and normalization.

Step 3. Deploy Balbix and Tune AI Models
In this step, teams can roll out Balbix initially to a limited but representative environment (e.g., cloud assets plus major data center). They should work with Balbix's implementation team to train the AI ensemble models on local data. This includes the process of customizing risk drivers (e.g., exploitability, exposure, asset criticality) based on enterprise context. The goal here is to validate the automatic asset inventory generation and ensure the Balbix's "single pane of glass" is accurate before expanding.

Step 4. Establish Dynamic Risk Quantification and Reporting
In this step, teams can configure Balbix's risk quantification outputs in financial terms, mapped to business units, projects, and executive reporting structures. They can develop live dashboards showing the organization's quantified risk exposure by category such as external exposure, insider threats, vulnerable systems, etc. The process also benefits if teams implement regular (e.g., weekly) reviews of major risk deltas driven by attack surface changes or new vulnerabilities.

Step 5. Integrate CRQ into Operational Decision-Making
In this step, teams must drive remediation prioritization based not just on CVSS scores, but on financial risk impact as surfaced by Balbix and align vulnerability management SLAs accordingly. They can connect Balbix insights into risk acceptance, cyber insurance strategy, incident response planning, and investment decisions (e.g., why secure Asset X vs. Asset Y based on business risk).

6. Mature Towards Continuous Risk Management
In this final and on-going step, teams can evolve from periodic risk reports to real-time "risk posture management," using Balbix's continuous AI updates. This can include refining AI model tuning over time based on incident outcomes, environmental changes, and emerging threat patterns. In addition, teams can set quarterly improvement targets based on Balbix's risk reduction recommendations and track ROI for security investments.

CLOSING COMMENT

As always, readers are welcome to reach out to the author or the TAG analyst team for assistance in developing plans around CRQ, ASM, or any aspect of the enterprise security equation. Readers who are TAG Research-as-a-Service (RaaS) can initiate discussion through their on-line RaaS portal. And obviously, readers are strongly encouraged to reach out to Balbix for more information and a detailed demonstration and roadmap discussion.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence,.