ISACA Accra Chapter

LANCASTER KUMASI CITY HOTEL, KUMASI

Improving Your Cybersecurity Posture with a Continuous Threat Exposure Management (CTEM) Program

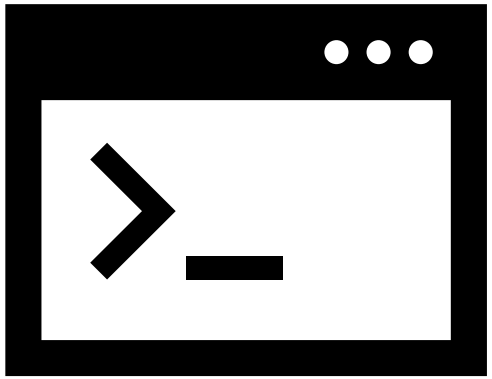
Presentation By: Desmond Israel Esq. CISSP, CIPM, CCT, CC

PROFILE

- **Partner** (Cyberlaw and Technology Practice), AGNOS Legal Company
- **Lecturer**, GIMPA Law School
- **Lead Consultant**, Information Security Architects Ltd
- **Training Consultant**, National Banking College
- **Non-Executive Director**, Zerone Analytiqs (Canada)
- **Member**, EC-Council BETA Testing Committee (United States of America)
- **Volunteer**, ISC2 Exam Development
- **Research Lead**, XRSI Guardian Safety Framework (California)
- **Former Research Fellow**, Center for AI and Digital Policy (Washington DC)
- **Alumni LLM'23**, The George Washington Law School (Washington DC)

AGENDA

- Executive Briefing For CIOs & CISOs
- What Is CTEM?
- Where RDVM Falls Short
- IAM As A CTEM Pillar
- The Five Stages of CTEM
- CISOs – Why Should You Care?
- What Tools Are Best Fit For CTEM
- Key Benefits For The Enterprise
- Implementation Best Practice
- Where To From Here?
- Strategic Call To Action



EXECUTIVE BRIEFING FOR CIOS & CISOS

Reactive cybersecurity practices have become obsolete.

The **attack surface has grown exponentially**—driven by cloud adoption, IoT proliferation, hybrid work models, and third-party integrations.

Continuous Threat Exposure Management (CTEM) emerges as a transformative approach, enabling continuous, **automated**, and **proactive threat mitigation** that aligns with dynamic business and risk landscapes.

WHAT IS CTEM?

According to **Gartner,** CTEM is "a set of integrated and iterative processes that enable organizations to continuously and consistently evaluate the accessibility, exposure, and exploitability of digital and physical assets."

It shifts the focus from **managing vulnerabilities in isolation** to **managing exposure holistically** across five interconnected dimensions:

Asset visibility	Threat likelihood	Exploitability	Business impact
Remediation readiness			

WHERE RBVM FALLS SHORT

Risk-Based Vulnerability Management (RBVM) has long been a cornerstone of enterprise security, but it is no longer sufficient on its own. RBVM tools are primarily focused on known vulnerabilities (CVEs), often neglecting broader elements of exposure such as:

- Misconfigurations and policy gaps
- Unaccounted digital assets (e.g., cloud workloads, containers, IoT)
- Human error and behavioural risk
- Obsolete technologies with unsupported patches

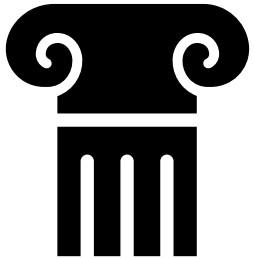
CTEM addresses these blind spots by incorporating the attacker's perspective—prioritizing exposures based on how accessible and exploitable they are in real-world attack scenarios.

This shift from vulnerability-centric to exposure-centric risk management is critical in today's fragmented security environments.

IAM AS A CTEM PILLAR

Identity and Access Management (IAM) is critical in CTEM.

IAM governs **who and what can access enterprise resources**, enforcing **least-privilege access** and **monitoring** for anomalous behaviour.



When integrated with CTEM:

It validates access pathways during breach simulation.

It limits attacker lateral movement during exploit emulation.

THE FIVE STAGES OF CTEM

CTEM is **not a one-off implementation** but a **continuous lifecycle** comprising five iterative stages:

Scoping	Discovery	Prioritization	Validation	Mobilization
Define the attack surface across cloud, endpoint, network, and code repositories. Establish clear KPIs and align with business-critical systems.	Enumerate all known and unknown assets. Identify misconfigurations, weak controls, and exposed APIs or credentials	Move beyond CVSS scores: weigh exposure against exploitability, business impact, and existing compensating controls. Use threat intelligence feeds to contextualize risks.	Simulate adversarial behaviours using Breach & Attack Simulation (BAS) tools. Conduct continuous testing to validate if remediation strategies are working.	Translate findings into actionable tasks for ITOps and DevSecOps. Maintain a feedback loop to refine scoping and prioritization.

CISOS – WHY SHOULD YOU CARE?

CTEM empowers CISOs to tackle five strategic imperatives:

Build a Security Strategy and Defensible Architecture

Align security priorities with business outcomes
Gain a complete view of internal and external attack surfaces
Integrate security controls across tools and teams

Manage Cyber Risks Proactively

Shift from lagging indicators to real-time risk visibility
Pre-empt exploitation by identifying high-risk exposures early
Enable continuous monitoring across threat surfaces

Ensure Governance and Security Compliance

Simplify compliance with structured exposure and risk tracking
Meet regulatory expectations (e.g., NIST CSF, ISO 27001, GDPR) with continuous audit readiness

Collaborate Cross-Functionally with Executives

Communicate exposure trends clearly to the board and non-technical stakeholders
Build consensus around remediation priorities that support operational continuity

Demonstrate ROI on Security Investments

Justify budgets with exposure reduction metrics
Correlate threat simulations with business-critical asset protection

WHAT TOOLS ARE BEST FIT FOR CTEM

To build a successful CTEM framework, organizations should integrate a suite of specialized tools:

EASM (External Attack Surface Management) – Identifies internet-exposed assets and weaknesses

VPT (Vulnerability Prioritization Technology) – Ranks vulnerabilities by business and threat context

PTaaS (Penetration Testing as a Service) – Provides scalable security testing

CAASM (Cyber Asset Attack Surface Management) – Offers internal asset visibility, including shadow IT

VA (Vulnerability Assessment) – Scans for known system vulnerabilities

Patch Management – Automates update workflows for secure software environments

CNAPP (Cloud-Native Application Protection Platform) – Monitors cloud posture and workload protection

BAS (Breach & Attack Simulation) – Emulates attacker behaviour to test resilience

ITSM/Ticketing Tools – Streamlines remediation task tracking and collaboration

It must be interoperable, automated, and provide auditable results to ensure that CTEM becomes a continuous, efficient function—not just an ad hoc initiative.

KEY BENEFITS FOR THE ENTERPRISE

Enhanced Security Posture

- Shift from reactive to anticipatory security.
- Align security controls with attacker behaviour and business priorities.

Cost Reduction

- Prevent high-cost breaches and regulatory fines.
- Automate workflows to reduce labor costs in detection and triage.

Visibility & Risk Clarity

- Eliminate blind spots across the full digital and physical environment.
- Deliver risk dashboards to the board with context and confidence.

Unified Governance

- Align cybersecurity with broader GRC initiatives.
- Break down tool and team silos for collaborative risk management.

IMPLEMENTATION BEST PRACTICE

Start with External Threat Management (EASM)

Identify public-facing exposures like cloud leaks, vulnerable domains, and expired certificates.

Combine with Cyber Asset Attack Surface Management (CAASM) for internal visibility.

Communicate and Align on CTEM Objectives Early

Develop shared language and metrics between security, IT, and business teams.

Create a CTEM charter and review exposure trends during executive reporting.

Integrate IAM, DRP, and NAC Tools

Use IAM for identity validation across attack paths.

Apply Digital Risk Protection (DRP) to monitor brand and asset exposure in deep/dark web.

Network Access Control (NAC) ensures secure access enforcement for endpoints.

Consolidate Tools Where Possible

Avoid tool sprawl by choosing vendors that offer integrated CTEM capabilities (e.g., asset discovery + patch management + threat intelligence).

WHERE TO FROM HERE?

CTEM is not a plug-and-play solution—it's a strategic transformation. Here's a pragmatic roadmap to begin your journey:

Step 1: Educate

Familiarize leadership and security stakeholders with CTEM principles. Explore Gartner and industry whitepapers to build a foundational understanding.

Step 2: Assess Current State

Conduct a gap analysis on existing vulnerability management programs. Identify tool inefficiencies and assess process maturity.

Step 3: Inventory & Baseline

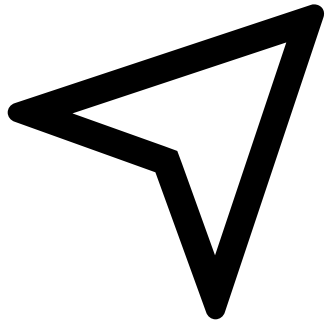
Map out asset inventories, stakeholders, threat intelligence feeds, and current security validation methods. Document weaknesses and silos.

Step 4: Align with ITOps

Engage IT and business units to calibrate priorities and reduce operational friction. Explore vendor options to consolidate tooling.

Step 5: Launch CTEM Pilot

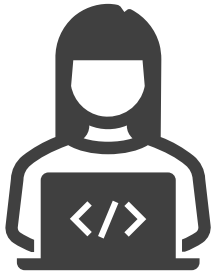
Begin implementation in a high-risk area. Define KPIs, measure effectiveness, and scale based on outcomes.



STRATEGIC CALL TO ACTION

CIOs and CISOs must embed CTEM into their security fabric—transitioning from passive defense to exposure-aware, real-time cybersecurity operations. CTEM creates a living, breathing view of enterprise risk—empowering leaders to respond to threats before they materialize into incidents.

INTERACTIONS



Need a CTEM integration Proof-on-Concept? Let's talk

THANK YOU

www.desmondisrael.legal