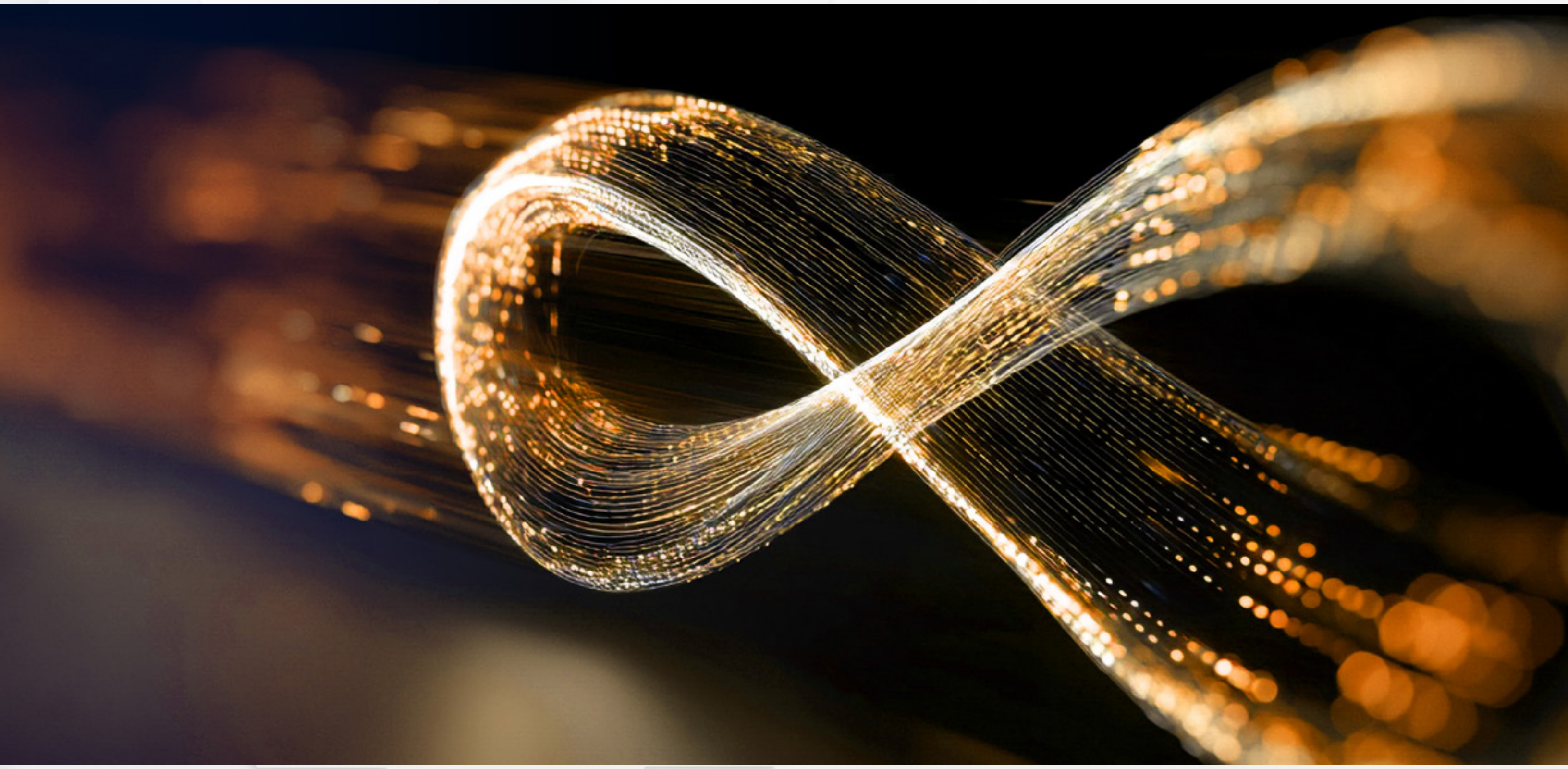
BEST PRACTICES

GUIDE

FOR THREAT EXPOSURE MANAGEMENT



DEEPWATCH™

TABLE OF **CONTENTS**

EXECUTIVE SUMMARY

Continuous Threat Exposure Management (CTEM) is essential for modern enterprise security, enabling organizations to keep pace with evolving adversaries through unified risk visibility and proactive mitigation. Deepwatch operationalizes CTEM best practices to deliver preemptive, proactive AI-driven security within the Deepwatch Guardian MDR Platform™ (Deepwatch MDR).

Introduction: The Imperative for CTEM

- Cyber threats adapt rapidly, exploiting gaps in legacy vulnerability management and incident response solutions.
- The move from periodic scans and static controls to continuous, intelligence-driven threat exposure management is foundational for resilience, compliance, and business continuity.
- Deepwatch CTEM shifts operations from reactive firefighting to preemptive, proactive, risk-driven defense, supporting executive decision-making and operational effectiveness.

Foundations of CTEM Best Practices

1. PRECISE SCOPING

- Map critical assets and regulatory environments (cloud, on-premises, hybrid).
- Assign ownership and align security priorities with business impact.
- Focus on business-critical workloads, compliance obligations, and attack surface expansion.

2. CONTINUOUS DISCOVERY

- Move beyond periodic vulnerability scans; employ real-time asset discovery.
- Use active and passive techniques, cloud posture tools, and external attack surface management.
- Uncover shadow IT, unmanaged endpoints, cloud resources to ensure complete attack surface visibility.

3. CONTEXTUAL PRIORITIZATION

- Model contextual risk using exploitability, business impact, real-world threat intelligence, and asset criticality.
- Prioritize exposures most likely to be targeted, not just those with high CVSS scores.

4. VALIDATION

- Conduct breach simulations, adversary emulation, and red teaming.
- Verify that exposures are truly exploitable and sharpen incident response plans.

5. MOBILIZATION & REMEDIATION

- Automate remediation, integrate with ITSM, security orchestration, and patch management.
- Iterate closing of validated exposures for sustained risk reduction.

CTEM vs. Traditional Vulnerability Management

Legacy approaches suffer from static scans, disconnected risk context, fragmented reporting, and slow remediation.

CTEM enables:

- Persistent visibility into attacker opportunities.
- Real-time prioritization by business and threat context.
- Unified workflows for seamless discovery, validation, and mobilization.

Deepwatch CTEM: Operationalizing CTEM at Scale

- CTEM aggregates telemetry from all tools (SIEM, EDR, CSPM, etc.) into a centralized data mesh.
- This unified view eliminates silos, correlates exposures, and highlights high-impact risks.

Dynamic Risk Metrics & Executive Reporting

- CTEM quantifies organizational risk with dynamic risk scoring, analytics, and board-ready reports.
- Enables security leaders to demonstrate ROI, regulatory compliance, and business alignment.

Agentic AI & Automation

- CTEM automates over 80% of routine risk processing: asset discovery, threat enrichment, reporting, and remediation.
- AI and machine learning provide enriched telemetry, correlation, and anomaly detection.

Proactive Exposure Management

- Continuous posture assessments identify and close gaps before attacks can occur.
- Replaces reactive vulnerability response with upstream risk mitigation and predictive analytics.

Seamless Ecosystem Integration

- CTEM integrates across AWS, Okta, Wiz, Splunk, Microsoft, and more.
- Leverages existing investments and orchestrates automated playbooks across multi-cloud/hybrid estates.

Operational Excellence & Impact: Organizations Running Deepwatch CTEM Experience

- Accelerated time to remediation (TTR) and response (MTTR).
- Unified visibility across fragmented, hybrid environments.
- Scalable, compliance-ready reporting and analytics for executive leadership and board.
- Lower signal fatigue and improved SOC efficiency via context-driven filtering and automation.

The Preemptive/Proactive Paradigm: The Deepwatch Guardian MDR Platform

PREEMPTIVE MDR

- Anticipates, validates, and neutralizes threats before compromise—using adversary simulation, continuous assessment, and dynamic risk scoring.
- “Shift left” mentality for cybersecurity: intervene in early kill chain phases, not just post-breach.

PROACTIVE THREAT SIMULATION & CONTROL VALIDATION

- Runs internal fire drills using adversary emulation to ensure layered defense readiness.
- Validates real-world exploitability of exposures, not just theoretical risk.

EARLY-STAGE ATTACK DISRUPTION

- Integrates proactive threat hunting.

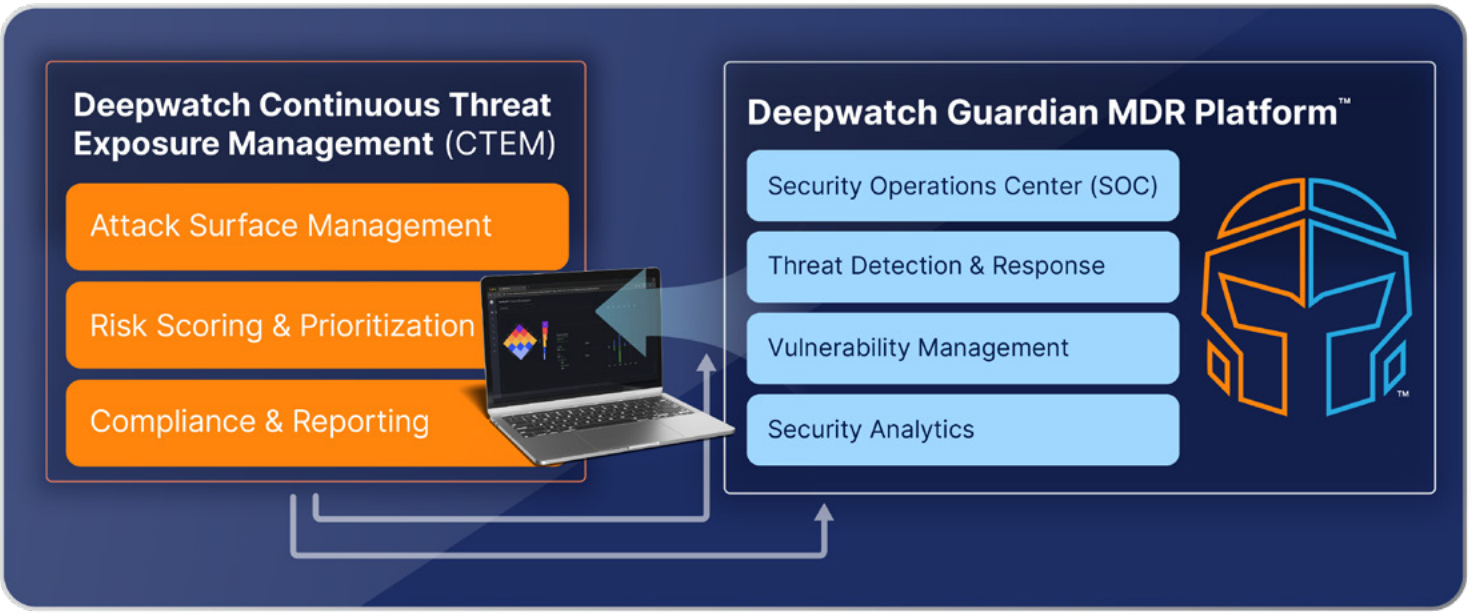
AUTOMATED THREAT CONTAINMENT

- Response playbooks isolate endpoints, block processes, and update firewall configurations before threats escalate.
- Automation ensures speed and repeatability, freeing human analysts for strategic threat investigation.

REAL-WORLD OUTCOMES

- Organizations deploying Deepwatch CTEM report measurable improvement in detection lead times, reduced incident volumes, and optimized security posture.
- CTEM drives regulatory readiness (supporting NIST CSF, ISO 27001, GDPR, HIPAA, etc.), streamlining compliance and reporting cycles.

Two-Way Integration of the Deepwatch Guardian MDR Platform & Deepwatch CTEM


Deepwatch Continuous Threat Exposure Management (CTEM)
Attack Surface Management
Risk Scoring & Prioritization
Compliance & Reporting
Deepwatch Guardian MDR Platform™
Security Operations Center (SOC)
Threat Detection & Response
Vulnerability Management
Security Analytics
™

The Deepwatch Guardian MDR Platform and Deepwatch CTEM work together to provide a holistic cybersecurity solution. Deepwatch CTEM is an add-on that augments the core capabilities of Deepwatch MDR. The two-way integration facilitates a continuous loop of data and action, enhancing threat detection, risk prioritization, and overall security posture.

From CTEM to Deepwatch MDR: CTEM provides risk-centric data and contextual prioritization to MDR. It aggregates and normalizes security signals from various sources, helping MDR to focus on the most critical threats based on business impact, not just technical severity. This information allows the MDR platform to improve its threat detection accuracy and reduce false positives.

From MDR to Deepwatch CTEM: MDR provides real-time threat and incident data back to CTEM. As threats are detected and incidents are responded to, this information is fed into CTEM to continuously update the enterprise risk metrics and risk profiles. This ensures that the risk scores and prioritization remain dynamic and reflective of the current threat landscape, enabling the platform to provide up-to-date insights and recommendations.

Implementation Guidance & Operational Challenges

SUCCESS FACTORS

- Start with asset inventory/data mesh.
- Align exposure priorities with business impact.
- Invest in automation and agentic analytics.

COMMON CHALLENGES

- Tuning sensitivity to minimize false positives in early-stage detection.
- Integrating legacy platforms and orchestrating response across hybrid enterprise environments.
- Managing cultural shift from reactive incident response to proactive, continuous improvement.

BEST-PRACTICES ADOPTION ROADMAP

- **PHASE 1:** Map enterprise attack surface, integrate CTEM with existing Deepwatch MDR workflows.
- **PHASE 2:** Automate asset discovery and contextual risk scoring.
- **PHASE 3:** Deploy breach simulations and safe adversary emulation.
- **PHASE 4:** Roll out responsive playbooks for automated remediation and compliance reporting.

FUTURE TRENDS IN CTEM & PREEMPTIVE SECURITY

- Expanded use of machine learning/AI for anomaly detection, adversary engagement, and adaptive access control.
- Enterprise-wide XDR platforms for unified, contextual threat visibility and risk scoring.
- Advanced deception technologies to catch low-signal threats earlier.

Conclusion

CTEM is redefining enterprise cyber defense. Deepwatch CTEM delivers core best practices—in unified visibility, risk analytics, and adaptive automation—within the Deepwatch Guardian MDR Platform, empowering organizations to achieve true preemptive and proactive protection. By operationalizing CTEM at scale, Deepwatch ensures sustained risk reduction and improved security posture in a complex and rapidly evolving threat landscape.

DEEPWATCH™

Always Watching. Always Protecting.™

Contact Sales at Deepwatch to

Secure your enterprise with Continuous Threat Exposure Management

Deepwatch® is the leader in Precision MDR powered by AI and humans. We amplify human expertise with AI insights to reduce the risks that matter most to your business. Our protection is proactive, preemptive and responsive, tuned to your business, with no black boxes, and watched by experts 24/7/365.

Learn More:

www.deepwatch.com/deepwatch-ctem-continuous-threat-exposure-management

Follow us:

Blog | LinkedIn | Facebook