NetSPI™

Kickstart Your Continuous Threat Exposure Management (CTEM) Program

Ready to make a move toward a CTEM strategy?
Use these questions to assess your team's current ability to proactively address business-critical exposures.

PHASE 1: SCOPING

1. Do we have a complete catalog of all digital and physical assets, including internal, cloud, and external-facing systems?

2. Who are the key stakeholders in our organization responsible for cybersecurity?

3. Have we defined the cybersecurity objectives that are meaningful to each stakeholder?

4. How would our approach to CTEM work with our existing security frameworks?

PHASE 2: DISCOVERY

1. Are our external attack surfaces clearly identified?

(e.g., websites, applications, third-party integrations)

2. How are we currently identifying vulnerabilities and threats?

(e.g., penetration testing, automated tools)

3. How do we identify changes in our environment and assess their significance to determine if further testing is necessary?

4. What is the cadence and comprehensiveness of our current testing methods?

5. Are our current tools fully optimized and scalable for a CTEM program?

(e.g. Penetration Testing as a Service (PTaaS), External Attack Surface Management (EASM), Cyber Asset Attack Surface Management (CAASM), Breach and Attack Simulation (BAS) as a Service)

6. Are our vendor solutions well-integrated, or do we need unified systems to avoid operational silos?

PHASE 3: PRIORITIZATION

1. Do we know the sensitive assets and data we need to secure most urgently?

2. Do we have a process for triaging and prioritizing vulnerabilities based on technical severity and business impact?

3. Do we have always-on monitoring tools to provide real-time visibility of vulnerabilities and risks?

PHASE 4: VALIDATION

1. How frequently are we testing, retesting, and validating our defenses against newly emerging threats?

2. How often do those tests surface the same vulnerabilities, and are those vulnerabilities business-critical?

3. How do we prioritize addressing gaps in our security controls and validating the remediation?

PHASE 5: MOBILIZATION

1. Are there enough resources and tools to support effective remediation efforts?

2. What is the churn rate of my security team? Is it because of job-specific deliverables/overwhelm or something else unrelated to the security process?

3. How capable is our team at responding to, validating, and mitigating threats in live scenarios?

4. Are we equipped to analyze findings from simulations and adapt our playbooks based on lessons learned?

5. Do we have an up-to-date Incident Response Plan (IRP)?

6. Have we enabled cross-departmental collaboration, including IT, legal, compliance, and operations teams?

7. Does our organization have a clear plan to evolve and future-proof our cybersecurity strategies?

Take Action to Implement a Continuous Threat Exposure Management (CTEM) Strategy Today

Use this worksheet as a launchpad to strengthen your position for CTEM readiness.

Taking steps toward implementing a CTEM program can be challenging, but you don't have to do it alone. At NetSPI, our 350+ in-house security experts are here to guide you every step of the way. With a personalized consultation, we'll help you evaluate your current cybersecurity landscape, identify critical gaps, and create a CTEM strategy tailored to your organization's unique needs.

Reach out today and kickstart your proactive security journey.

ABOUT NETSPI

NetSPI is the proactive security solution used to discover, prioritize, and remediate security vulnerabilities of the highest importance. NetSPI helps its customers protect what matters most by leveraging dedicated security experts and advanced technology, including Penetration Testing as a Service (PTaaS), External Attack Surface Management (EASM), Cyber Asset Attack Surface Management (CAASM), and Breach and Attack Simulation (BAS) as a Service.

Leveraging a unique combination of advanced technology, intelligent process, and dedicated security experts, NetSPI brings a proactive approach to cybersecurity with more clarity, speed, and scale than ever before. In other words, we go beyond for our customers so they can go beyond for theirs.