REDSEAL

Continuous Threat Exposure Management (CTEM) Powered by RedSeal

Adopt a reliable process for proactively reducing cyber risk

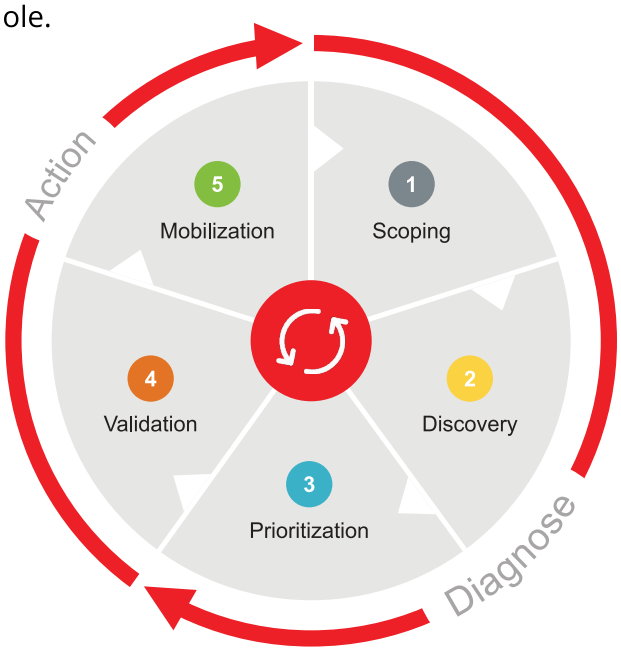
Continuous Threat Exposure Management (CTEM) is a strategic security framework to proactively mitigate cyber risks and strengthen security postures. Originally defined by leading analyst firm Gartner, CTEM helps organizations move away from the reactive, siloed, and sporadic methods of vulnerability management today that fail to keep pace with evolving threats and growing attack surfaces. With CTEM, organizations take a more proactive, holistic, and continuous approach to managing exposures of all types and staying ahead of threats. The outcomes are greater operational efficiency, faster and more reliable remediation, and reduced business risk.

The five steps of CTEM

As outlined by Gartner, the CTEM process consists of five steps: the scoping, discovery, prioritization, and validation of exposures, followed by the mobilization of remediation teams. While CTEM is powered by people and technology, automation is key to success.

Rely on the RedSeal platform to power the CTEM process

A cybersecurity pioneer, RedSeal delivers a powerful platform enabling a proactive, holistic, and continuous approach to network exposure management. With its unique ability to model and analyze the entire connected environment all at once, the RedSeal platform brings unparalleled network insights to every CTEM step that integrate, simplify, and accelerate the process as a whole.



	CTEM required capabilities	How RedSeal does it
1. Scoping (of attack surfaces and business risks)	Identify organizational priorities, understand the systems and assets involved, and determine risk owners and appetites. What is critical to our business operations, and what would happen if it is compromised?	Brings all resources from hybrid IT, OT, and IoT environments into a single, visually organized model—a network digital twin. Helps stakeholders easily map business-critical systems and assets and define scopes in business context.
2. Discovery (of assets and exposures)	For each scope, discover connected assets and assess them for threats, vulnerabilities, and other exposures, both direct and indirect. What do we have to protect? What is exposed and what is not exposed?	Maintains an accurate inventory of assets and continually analyzes them for exposures, including those due to misconfigurations, unmanaged and unknown assets, unintended connections, policy violations, and vulnerabilities.
3. Prioritization (of exposure management work)	Prioritize exposures considering internal, external, business, and technical factors. Go beyond severity and CVSS score to include concepts of visibility, exploitability, business criticality, and potential impact.	Combines prioritization and validation into a single step by automatically validating exposures before prioritizing them. Evaluates all possible access—from north, south, east, and west—across the entire network to assess the viability of exploitation and measure the true impact (blast radius) of each exposure. Considers all possible consequences from direct and indirect (downstream) threats. Calculates risk scores by combining vulnerability and business data with unmatched network context, ensuring exposures with greater business impact take higher priority.
4. Validation (of exposure exploitability and impact)	Prove that the prioritized exposures could actually be exploited and estimate the highest potential impact, considering lateral movement. Filter the priority list based on successful validation.	
5. Mobilization (of teams and processes)	Technical and business stakeholders must collaborate on how to remediate an exposure, whether that means fixing it or accepting the risk. The goal here is to remove friction in the decision making process.	Serves as the single source of truth for teams collaborating on CTEM, delivering detailed exposure evidence with the exact controls and assets involved. Results in more efficient communication, simplified decision making, and faster risk reduction.

Why RedSeal is the single best technology platform to power CTEM

CTEM is designed to break down attack surfaces and remediation work into more manageable pieces. But the fact remains: organizations need a complete and accurate understanding of their entire connected network to be successful with CTEM. This fundamental concept has been at the heart of the RedSeal network exposure management platform from day one. Today, organizations use RedSeal to spot exposures other tools can't see, prioritize risks based on network context other tools can't provide, and be holistic, proactive, and continuous about cybersecurity in a way other tools can't support.

The most comprehensive network view reveals the true risks

RedSeal's ability to uncover and map hybrid infrastructure is unparalleled. Unlike solutions that only evaluate siloed security controls, RedSeal analyzes every aspect of the network: endpoints, assets, infrastructure, security controls, attack surfaces, and all possible connections and access across the network, on premises and in the cloud. Integrating with products from more than 75 vendors, only RedSeal gives you a comprehensive, network-wide view of exposures and reveals the true impact to the business.

100% of RedSeal deployments find previously unknown network assets, subnets, and connections.

The most comprehensive exposure management functionality lowers total cost

There are many point products on the market that support the CTEM process. Only RedSeal delivers powerful exposure management capabilities in a single platform, supporting every step in the CTEM process and eliminating the need for multiple tools and manual integrations. This results in a simplified CTEM tech stack and lower overall costs.

The most accurate and efficient prioritization engine includes validation

RedSeal's proprietary algorithms consider a range of internal, external, business, and technical factors to assess risk and prioritize exposures. This includes security controls, asset criticality, and vulnerability data, as well as the visibility, exploitability, exploitation potential, and potential impact of the exposure. With RedSesal, exposures are automatically validated before they are prioritized, eliminating the time, effort, and expense of manual validation steps.

Start your CTEM journey with RedSeal

CTEM is more than a strategy—it's a shift in how organizations approach cybersecurity, turning overwhelming attack surfaces into manageable priorities and proactively reducing risk. But without full visibility into the entire connected network, even the most robust CTEM program can fall short. That's where RedSeal makes the difference.

For more than 20 years, RedSeal has partnered with federal agencies and F500 companies to strengthen their cybersecurity posture. In a world where every exposure counts, RedSeal ensures you have the insights to stay ahead.

Contact RedSeal to learn more or request a demo today.

RedSeal, a leader in network exposure management, offers proactive insights to close security gaps in hybrid environments. It creates a network digital twin for comprehensive visibility and protection. Trusted by Fortune 1000 companies and U.S. military branches, RedSeal enhances operational efficiency, boosts productivity, and reduces business risk.
www.redseal.net | info@redseal.net | +1 408-641-2200 | 888-845-8169