seemplicity

# Jumpstart Your CTEM Program

The Seemplicity RemOps Platform as the Foundation for CTEM

DATASHEET

As organizations face increasingly complex cybersecurity threats, the need for a continuous and integrated approach to risk management becomes critical. The Gartner Continuous Threat Exposure Management (CTEM) program outlines a strategic framework for ongoing risk assessment and remediation, ensuring robust security posture.

## Key Challenges Addressed by CTEM

### DYNAMIC THREAT LANDSCAPE

Modern cyber threats evolve rapidly, requiring continuous monitoring and adaptation.

### COMPLEX IT ENVIRONMENTS

The proliferation of cloud services, mobile devices, and remote access increases exposure points.

### INEFFECTIVE MANUAL PROCESSES

Periodic and manual security assessments are insufficient for addressing real-time threats.

## CTEM Framework

CTEM is a holistic approach encompassing the entire lifecycle of vulnerability and exposure management. It consists of five essential steps:

DIAGNOSE

**Scope:** Define critical assets and systems based on business importance.

**Discover:** Identify vulnerabilities across the scoped environment.

**Prioritize:** Rank vulnerabilities by risk level to focus remediation efforts.

ACTION

**Validate:** Test the exploitability of vulnerabilities in the organization's context.

**Mobilize:** Coordinate and execute remediation efforts.

## Seemplicity's Remediation Operations (RemOps) Platform

RemOps solutions, like the Seemplicity platform, operationalize the CTEM framework, providing a structured approach to vulnerability remediation. As the leading RemOps solution, the Seemplicity platform streamlines and enhances the process of identifying, prioritizing, and remediating cybersecurity vulnerabilities. It enables organizations to accelerate remediation and improve their overall cybersecurity posture by enabling effective collaboration between security, development and operations teams.

## CTEM Powered by the Seemplicity RemOps Platform

| CTEM STEP | SEEMPLICITY'S REMOPS DELIVERY |
|---|---|
| **STEP ONE** Scoping | Apply context to findings to enable scope-based choices |
| **STEP TWO** Discovery | Collect & consolidate vulnerability and risk findings |
| **STEP THREE** Prioritization | Dynamically prioritize based on severity, scope, fixer, etc. |
| **STEP FOUR** Validation | Utilize validation tool findings and bidirectional integration |
| **STEP FIVE** Mobilization | Automate processes using no-code rules, queues & routing |

## Key Benefits

### COMPREHENSIVE COVERAGE

Integrates various security tools and processes into a cohesive workflow, ensuring all CTEM phases are addressed seamlessly.

### REDUCED MEAN TIME TO REMEDIATE (MTTR)

Workflow automation accelerates the remediation process, shortening response times and reducing the window of exposure.

### OPTIMIZED RESOURCE ALLOCATION

Prioritization ensures that resources focus on the most significant threats, strengthening security posture.

### CONTINUOUS IMPROVEMENT

Ongoing feedback and analytics to regularly identify and address security gaps, enhancing the effectiveness of CTEM strategies.

### ENHANCED COORDINATION

Streamlines collaboration between security, development and operations teams, ensuring efficient and effective vulnerability management.

seemplicity

WANT TO LEARN MORE?

## Check out the full RemOps for CTEM whitepaper.

DOWNLOAD WHITEPAPER