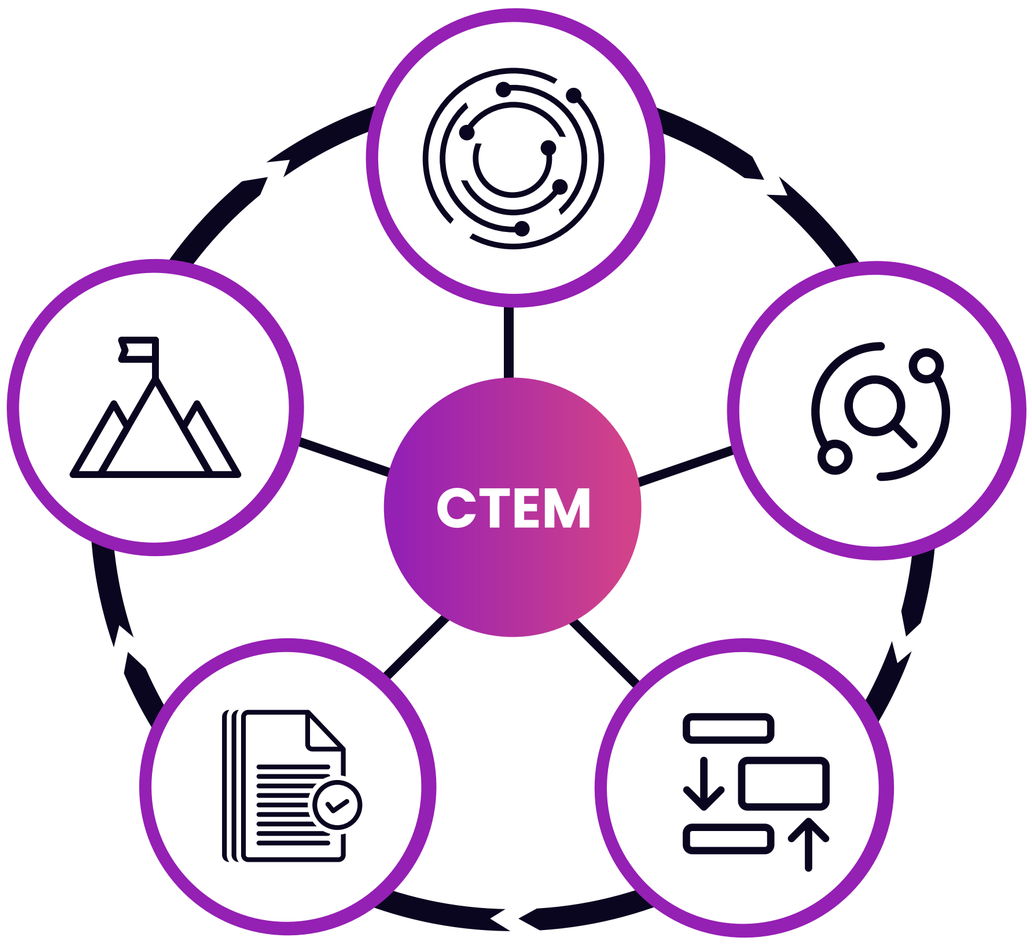
seemplicity

RemOps for Continuous Threat Exposure Management

WHITEPAPER

This paper makes the case for implementing a Continuous Threat Exposure Management (CTEM) program by using a Remediation Operations (RemOps) solution, such as the Seemplicity platform. A RemOps solution is the most effective and comprehensive method for operationalizing a CTEM program to effectively manage cybersecurity risks.

The paper provides a conceptual understanding of CTEM and the integral role of Remediation Operations in delivering a practical foundation for CTEM program implementation. As part of that, the paper discusses the limitations of CTEM-phase-specific products – such as Attack Surface Management (ASM) or Breach and Attack Simulation (BAS) products, and highlights the benefits of an all-encompassing approach such as that provided by a Remediation Operations platform. The whitepaper also showcases the significance of the Seemplicity platform in executing on one of the most challenging CTEM tasks – remediation and why Seemplicity was recognized by Gartner as a Cool Vendor.



Gartner Continuous Threat Exposure Management (CTEM)

Gartner's Continuous Threat Exposure Management (CTEM) is a strategic framework for assessing an organization's security posture and, specifically, identifying and managing vulnerabilities and other security gaps in an organization's digital infrastructure. The "Continuous" in Continuous Threat Exposure Management is an acknowledgement that modern digital technology requires organizations to take a continuous approach to posture assessment and risk remediation. Thus, CTEM values an ongoing, automated approach over the periodic, manual approaches in place in most organizations. CTEM is crucial because it helps organizations adapt to the constantly changing threat landscape by maintaining a continuous understanding of their attack surface and exposure points. This proactive stance enhances an organization's ability to reduce risk, prevent breaches, and respond to threats swiftly and effectively.

CTEM aligns cybersecurity with strategic business objectives by safeguarding critical assets, maintaining customer trust, and complying with regulatory requirements. CTEM also enables businesses to optimize resource allocation, improve response times to risks and threats, and foster a culture of ongoing improvement, which enhances operational efficiency.

The complexity of modern IT environments, with cloud services, mobile devices, and remote access, further underscores the need for an all-encompassing CTEM-like approach.

Seemplicity Take

In cybersecurity, a "continuous" process demands more than basic automation. It requires a structured framework where actions are executed and also monitored, measured, and optimized consistently, leveraging data and clear metrics to ensure progress and efficiency.

From a program management perspective, a continuous workflow is characterized by:

- **A systematic, ongoing process.**
- **Process instrumentation with data collection and retention.**
- **Independent Key Performance Indicators (KPIs) to gauge effectiveness.**
- **Ongoing performance measurement analysis, and reporting.**

CTEM is a Top Technology Trend

CTEM is recognized as one of Gartner's Top Strategic Technology Trends for 2024. It's worth noting that these are the top trends from multiple technology domains, security being just one; signifying just how important CTEM is for businesses, and highlights its growing importance in the technology landscape. Its inclusion in the list urges organizations to adopt proactive security measures that continuously identify, assess, and mitigate risks that impact an organization's security posture. With businesses always adopting and using new technology, and cyber threats becoming more sophisticated, CTEM reflects a necessary industry shift towards ensuring resilience and security in digital environments. CTEM's recognition by Gartner not only emphasizes its critical role in modern cybersecurity strategies but also positions it as a key component of future technological development and organizational preparedness.

The Five-Steps of CTEM

The CTEM framework revolves around a five-step model that forms a comprehensive, ongoing cycle:

STEP ONE
Scope

Scope defines the relevant groups (e.g., departments, technology stacks, applications, data sensitivity levels, etc.), based on business importance, for which the other CTEM steps will be performed.

STEP TWO
Discover

Discover involves identifying all relevant assets - visible and hidden - and the subsequent vulnerabilities within the scoped environment, ensuring no blind spots.

STEP THREE
Prioritize

Prioritize ranks these vulnerabilities based on their risk to the organization, considering factors such as likelihood of being exploited and impact of compromise, ensuring efforts are focused where they are most needed.

STEP FOUR
Validate

Validate tests the real-world applicability of prioritized vulnerabilities, assessing whether they are truly exploitable in the organization's specific context, and whether the current response plan is sufficient in protecting the business.

STEP FIVE
Mobilize

Mobilize refers to the coordinated response to remediate or mitigate the prioritized vulnerabilities, closing the loop on the management cycle and preparing for its next iteration.

The Two Halves of CTEM

CTEM can be divided into two broad halves: **Diagnose** and **Action**.

DIAGNOSE

Encompasses the first three phases—Scope, Discover, and Prioritize—where organizations define what assets are critical, identify vulnerabilities within those assets, and then prioritize those vulnerabilities based on risk.

ACTION

Includes the Validate and Mobilize phases, focusing on confirming the real-world applicability of identified vulnerabilities and then taking the necessary steps to remediate or mitigate them, effectively closing the loop on the CTEM process.

The Role of Automation and Ongoing Improvement in CTEM

Automation and continuous improvement serve as foundational elements to CTEM, significantly enhancing the security framework's ability to adapt to and mitigate evolving threats. Automation not only accelerates the process of detecting, assessing, and remediating vulnerabilities – thereby reducing the response time from identification to resolution – but also serves as a critical augmentation layer that multiplies the effectiveness of security teams. By enabling the management and mitigation of risks at a larger scale, it allows personnel to pivot from manual, repetitive tasks to focus on higher-level, strategic decision-making. Ongoing improvement, anchored in the cycle of feedback and analytics, refines and evolves security strategies in real-time, ensuring that the organization's defenses are always aligned with the latest threats and technological advances. This dynamic interplay between automation and constant improvement fosters a resilient, proactive security posture, ensuring that CTEM not only addresses current security challenges but is also well-prepared to anticipate and neutralize future threats.

CTEM is Holistic, Not Product-Centric

CTEM is a conceptual framework that applies across the entire vulnerability management process; it is not a product category and doesn't identify specific products to be used in the five individual phases, or to achieve CTEM overall. Still, there are many different products that support each CTEM phase. That is probably why some product vendors position themselves as CTEM solutions and often oversimplify the comprehensive nature of CTEM. By focusing on a solution for a specific phase, like discovery or validation, they neglect the full lifecycle that CTEM embodies, including asset prioritization, risk assessment, and remediation. This selective emphasis, while capitalizing on CTEM's growing popularity, presents an incomplete view of what it truly takes to achieve continuous threat exposure management. CTEM requires a more holistic approach, integrating various tools and processes across the entire spectrum of threat management activities.

Limitations of Phase-Specific Solutions

	WHAT IS IT?	WHY IT ISN'T CTEM?
Attack Surface Management	Attack Surface Management (ASM) involves continuously discovering, classifying, prioritizing, and monitoring assets to identify and reduce exposures that could be exploited by attackers. A key ASM product category is External Attack Surface Management (EASM), which focuses specifically on externally facing digital assets visible from the internet. ASM products help organizations understand and minimize potential attack vectors, enhancing overall cybersecurity posture.	ASM products are essential components of a robust CTEM program and fit within CTEM's Scope and Discover phases in that they help discover and classify digital assets. However, they are not sufficient for achieving CTEM. For example, while some ASM solutions boast their ability to perform testing, most organizations need – and already have – multiple domain-specific vulnerability, application security and cloud security scanning solutions in place. A more integrated, comprehensive approach that spans beyond asset discovery to encompass the full spectrum of threat exposure management activities is required for CTEM.
Breach and Attack Simulation	Breach and Attack Simulation (BAS) tools automate simulated cyberattacks against an organization's network to evaluate its defenses. Primary BAS use cases include identifying vulnerabilities, testing security controls' effectiveness, ensuring compliance with security policies, training security teams, and notably, validation. The BAS validation use case directly aligns with the CTEM validation step, offering a proactive assessment of the organization's preparedness against real-world threats. This use case is critical for confirming the efficacy of security measures and ensuring that prioritized vulnerabilities are accurately mitigated, making it a very relevant tool in the CTEM framework.	While BAS solutions are a valuable tool for the CTEM Validation phase, BAS alone is not sufficient to serve as the foundation for a CTEM program. BAS solutions do not address the full spectrum of CTEM activities, such as asset discovery, risk based prioritization, and remediation of identified vulnerabilities. A comprehensive CTEM approach requires integrating various tools and methodologies that cover the entire lifecycle, from identifying and prioritizing threats to remediating them and continuously monitoring for new vulnerabilities. BAS is an essential component within this broader ecosystem but needs to be complemented with other solutions to achieve a holistic CTEM strategy.

Get Started with CTEM using Remediation Operations

Remediation Operations (RemOps) is a structured process of addressing and fixing security vulnerabilities within an organization's IT environment. It encompasses the entire cycle from the identification of vulnerabilities to their resolution, ensuring that discovered security risks are efficiently and effectively mitigated. RemOps aims to streamline the collaboration between security teams and IT operations – one of the areas of greatest friction and inefficiency in vulnerability management and remediation – by leveraging automation to accelerate the remediation process. This approach not only enhances an organization's security posture but also aligns with broader risk management strategies, making it a critical component of modern cybersecurity frameworks.

What is Remediation Operations

THE REMOPS PROCESS INVOLVES SEVEN STEPS:

STEP ONE

Collect

Collect security findings from various sources.

STEP TWO

Consolidate

Consolidate to deduplicate and normalize data.

STEP THREE

Choose

Choose remediation priorities based on risk and remediation owners.

STEP FOUR

Route

Route tasks to the appropriate teams.

STEP FIVE

Receive

Accept responsibility for remediation.

STEP SIX

Remediate

Remediate by fixing the vulnerabilities.

STEP SEVEN

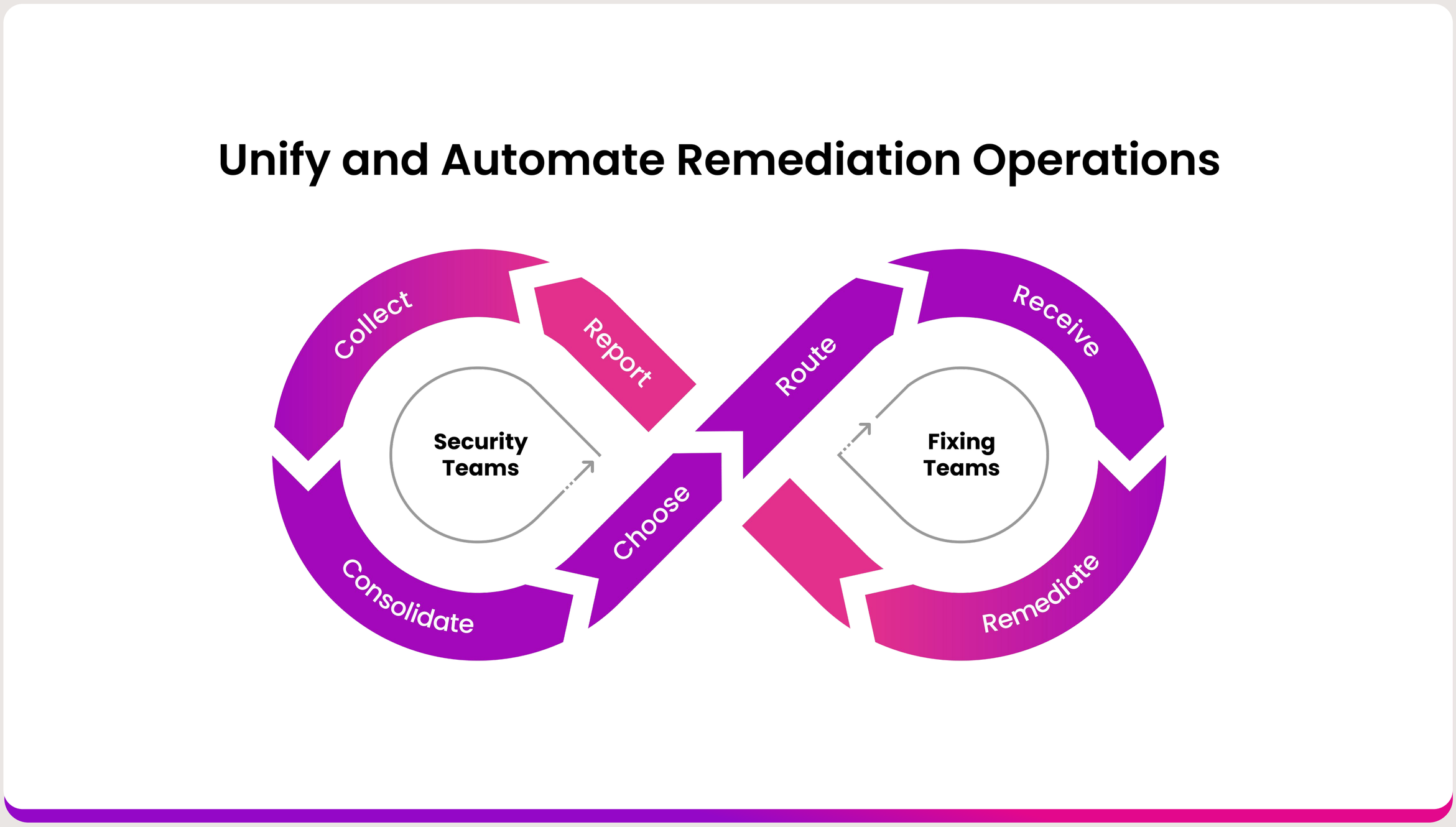
Report

Report on the remediation efforts and outcomes.

The Need for a Holistic Approach to CTEM

Building a CTEM program requires a comprehensive strategy that goes beyond the capabilities of individual, siloed products such as ASM and BAS. True CTEM effectiveness is realized through an integrated approach that encompasses the entire spectrum of risk management—from initial discovery through to final remediation. This necessitates a combination of tools and processes – many of which are already in place – working together to continuously identify, assess, and mitigate vulnerabilities, ensuring a robust and adaptive security posture against the dynamic cyber threat landscape.

But, importantly, making CTEM operational also requires an overarching platform that brings all of the individual tools together in a comprehensive process. Solutions seeking to deliver on the promise of CTEM, therefore, must synthesize the five stages of the CTEM process, from the initial discovery to the final mobilization, to ensure that no aspect of posture assessment and risk management is overlooked. This holistic, platform approach is necessary to effectively manage the sheer volume and sophistication of threats, streamline security operations, reduce the window of exposure, and ensure that the most critical vulnerabilities and security gaps are addressed promptly.

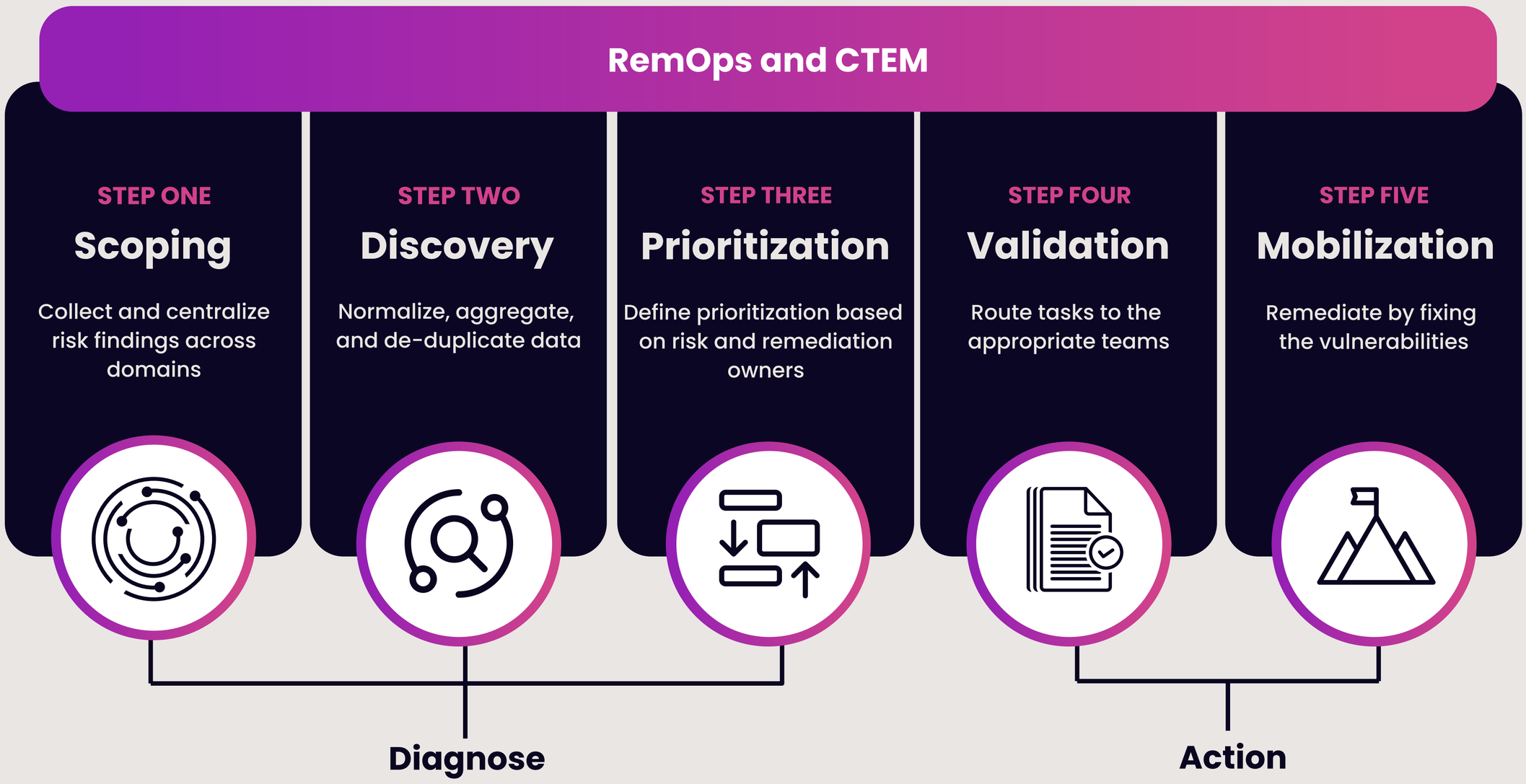


RemOps and CTEM Alignment

RemOps platforms offer a unified solution that aligns with both the Diagnose and Action halves of CTEM, as well as the individual phases. Unlike previously described point solutions that typically address only specific stages of the CTEM lifecycle, a RemOps platform integrates seamlessly across all stages, ensuring a comprehensive and cohesive vulnerability remediation strategy.

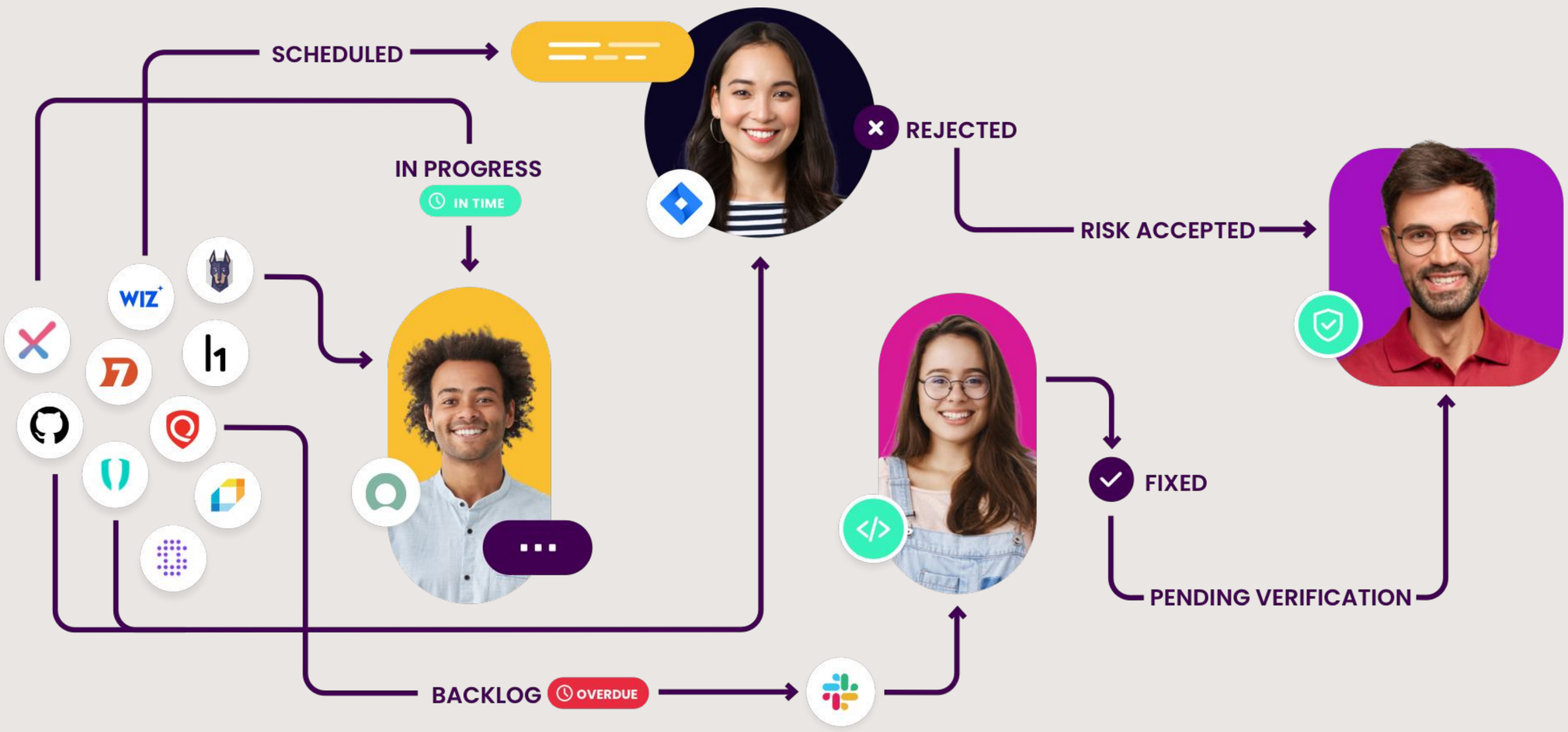
The RemOps-CTEM alignment begins with the **Diagnose** portion of CTEM—Scope, Discover, and Prioritize—which corresponds to the Collect, Consolidate, and Choose steps in RemOps. This phase ensures that vulnerabilities are not just identified and assessed, but also prioritized based on their potential impact on the organization. Transitioning to the **Action** portion of CTEM, the Validate and Mobilize steps are mirrored by the Receive, Route and Remediate steps in RemOps, facilitating the practical application of remediation efforts. Finally, the reporting phase in RemOps complements the entire CTEM cycle by providing feedback for continuous improvement, making it an indispensable tool for learning and refining posture and vulnerability management processes.

Implementing a CTEM program through a RemOps platform offers a practical, efficient, and effective way to manage cybersecurity risks. By leveraging a RemOps platform, organizations can ensure a holistic approach to exposure management, integrating various security tools and processes into a cohesive business process that continuously addresses the entire lifecycle of vulnerability management. This not only streamlines the process of securing an organization's attack surface but also enhances an organization's ability to adapt to and mitigate evolving cyber threats.



Seemplicity is a RemOps Pioneer

Seemplicity introduced the RemOps category in 2023, and continues to innovate and lead the market. The Seemplicity platform streamlines and enhances the process of identifying, prioritizing, and remediating cybersecurity vulnerabilities. The platform enables organizations to accelerate remediation and improve their overall cybersecurity posture by enabling effective collaboration between security, development and operations teams.



Conclusion

As organizations navigate the evolving cybersecurity landscape, the need for comprehensive strategies like CTEM becomes increasingly clear. By establishing a CTEM program, they can enhance their ability to manage and mitigate threats continuously, ensuring a robust defense mechanism that aligns with both current and future security requirements.

Building an effective CTEM program requires the adoption and use of a RemOps solution. Through a detailed exploration of the CTEM framework and the inherent limitations of phase-specific security products, this paper illustrated that a holistic, platform-based approach, exemplified by Seemplicity, is essential for a successful CTEM implementation. Seemplicity's recognition by Gartner as a Cool Vendor underscores the platform's effectiveness in addressing the complex challenges of CTEM, particularly in the critical area of remediation.

Adopting a RemOps platform is not just a step towards building a CTEM program and improving cybersecurity posture; it's a strategic move that prepares organizations for the challenges of tomorrow.