

WHITEPAPER

Foundations for Continuous Threat Exposure Management

Implementing a Threat-Informed
Defense Strategy



Contents

Background	3
Continuous Threat Exposure Management (CTEM)	4
Traps of Implementing a CTEM Program	5
Threat Informed Defense	8
Difficulties of Operationalizing a Threat Informed Defense Strategy	9
Enter Interpres	10
How Interpres Works	10
Analyze	12
Know Yourself: Your Organization's Threat Profile	12
Know the Enemy: Finished Cyber Threat Intelligence	13
Prioritize	14
Adversarial TTPs, Malware Families, Threat Groups, and Vulnerabilities	14
Mitigative Actions	14
Optimize	16
Defense Surface to Defend Against Prioritized Threats	16
Interpres Core Use Cases	18
Defense Readiness	18
Defense Surface Optimization	18
Prioritized Vulnerability Intelligence	19
Security Stack Consolidation/Rationalization	19
Summary: Defense Surface Management is the Foundation	20
About Interpres Security	23

Background

In 2015, the CIO of the Department of Defense (DoD), the Director of the National Security Agency's (NSA) Information Assurance Directorate, and the Director of the Defense Information Systems (DISA) agency posed a simple question, "Are we managing the constantly changing relationship between threat and defensive controls to continuously drive down risk?" That simple question started a program that would drive investments, system security engineering and architectural development across the DoD and the Federal Government. At the same time, the MITRE Corporation began working on its influential ATT&CK® framework, which revolutionized the way we think about cyber threats. Fast forward to 2023, the MITRE ATT&CK® framework has become the de-facto framework which serves as the foundational component of a threat informed defense strategy.

In today's ever-changing cyber threat landscape, organizations face a constant barrage of attacks and vulnerabilities. To combat these threats, many organizations are turning to Continuous Threat Exposure Management (CTEM) and Threat Informed Defense (TID) as two complementary approaches to improve their cybersecurity posture. However, implementing CTEM and TID can be a complex and challenging task, requiring significant resources and expertise.

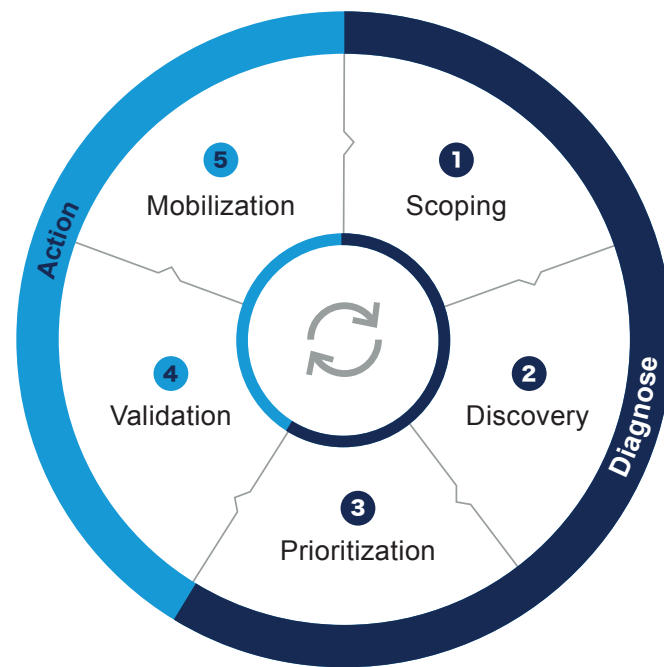
This white paper aims to explore the challenges and benefits of combining CTEM and TID, and how Interpres overcomes these challenges to enhance overall security posture and reduce cyber threat exposure through automation and optimization.

Continuous Threat Exposure Management (CTEM)

Continuous Threat Exposure Management (CTEM) is a program designed to reduce risk by scoping their attack surface, discovering their assets, prioritizing the most likely threats, validating that a vulnerability is exploitable, and the mitigation is sufficient, and finally, mobilization – ensuring that the organization is positioned to act on the remediation.

Continuous Exposure Management Process Stages

Source: Gartner. 763954_C



By 2026, Gartner indicates enterprise organizations that implement a continuous threat exposure management program will be three times less likely to experience a cyberattack.

Source: Gartner:
Implement a Continuous Threat Exposure Management (CTEM) Program, (July 2022). ID: G00763954




Traps of Implementing a CTEM Program

The benefits of implementing a CTEM program are immensely valuable, but successful implementation is not easily achieved. This is due to a variety of factors, including:


Technical Implementation:

-  **Complexity of Technologies:** Managing and integrating a plethora of security tools and technologies can be complex and demanding.
-  **Interoperability:** Ensuring different security tools, platforms, and data sources are compatible and can be integrated effectively.
-  **Data Overload:** Handling and analyzing massive amounts of data generated from continuous monitoring can be overwhelming and resource-intensive.
-  **Skill Shortage:** Lack of skilled cybersecurity professionals who can design, implement, and manage a CTEM program effectively.

Strategic Hurdles:

-  **Prioritization:** Determining which vulnerabilities and threats to prioritize when resources are finite, and threats are manifold.
-  **Aligning Business and Security Goals:** Ensuring that the CTEM program supports and aligns with the overall business goals and strategy.
-  **Scaling Challenges:** Adapting the CTEM program to suit the growing or evolving structure and scope of the organization.

Analytical Issues:

-  **Continuous Improvement:** Ensuring that the CTEM program adapts and improves in response to evolving threats and organizational changes.

Gartner observes that security teams often **fail** at reducing **threat exposure** through self-risk assessments because of an absence a threat-informed strategy and **unrealistic**, stove-piped and tool-centric approaches.

Source: Gartner:
Implement a Continuous Threat Exposure Management (CTEM) Program, (July 2022). ID: G00763954

These tools present a **vast and valuable** repository of information.

However, when used in isolation, their information may lack crucial context pertaining to the business, potential threats, defensive capabilities, and cross-team dynamics required to analyze the organization holistically. Thus, what is needed is an Intelligence Layer that comprehensively contextualizes the information and provides a nuanced bespoke understanding of the environment.

Interpres provides CTEM with the intelligence layer that unifies these required tools into a holistic and orchestrated solution. Interpres fills the technical implementation, strategic, and analytical gaps for successful CTEM implementation.

Threat Informed Defense

A TID strategy is a proactive approach to cybersecurity that emphasizes the importance of understanding the nature and motives of cyber threats to effectively defend against them. This strategy involves collecting and analyzing data about the threat landscape, identifying the most likely and dangerous threats, and then using that information to inform and guide the selection and implementation of security controls and detection engineering.

Rather than simply applying a generic set of security controls to their systems, organizations that use a TID strategy can focus their attention on the specific threats that pose the greatest risk to their systems and data.

Another benefit of a TID strategy is that it can help organizations to stay ahead of the evolving threat landscape. By constantly monitoring and analyzing the threat landscape, organizations can identify new and emerging threats and take steps to mitigate them before they become major security incidents. This helps organizations to become proactive in their security efforts, rather than reactive to threats after they have already impacted the organization.

One of the key benefits of a **TID strategy** is that it **enables** organizations to **prioritize** their security efforts and resources based on the most **critical** and **relevant threats**.

Difficulties of Operationalizing a Threat Informed Defense Strategy

It requires a significant investment in resources, including personnel, tools, and technology, to collect, analyze, and act on threat intelligence information.

This can be challenging for organizations with limited budgets or limited expertise in the field of cybersecurity.

Effective threat intelligence analysis requires a high degree of expertise and technical skill.

It can be difficult for organizations to find and retain skilled cyber security professionals with the necessary knowledge and experience to carry out this work.

The rapidly evolving threat landscape can make it difficult for organizations to keep pace with the latest threats and stay ahead of evolving attack methods.

This requires organizations to continuously monitor and analyze the threat landscape and adjust their TID strategy as needed, which can be a time-consuming and resource-intensive process.

Integrating threat intelligence into an organization's overall security posture can also be challenging.

It requires close collaboration and coordination between various teams and departments within the organization such as the security operations center, the incident response team, and the threat intelligence team, among others.

Due to these challenges, **automation** is the only way to effectively implement a TID strategy as it is impossible for security teams to keep up with the constantly changing relationship between threat and defense.

Enter Interpres

Interpres automates the laborious and time-consuming process of operationalizing threat-informed defense while combining and contextualizing information sourced from Continuous Threat Exposure Management (CTEM) tooling, defensive capabilities, and threat data to function as an intelligence layer that empowers organizations to continuously scrutinize the dynamic interplay between threats and defenses. This comprehensive analysis enables organizations to prioritize and optimize their defenses, thereby reducing threat exposure in a manner that is both efficient and effective.

How Interpres Works

It is widely accepted that Sun Tzu is a master of warfare, and in today's world, information technology infrastructure plays an essential role in the battlefield. Therefore, it is logical to apply Sun Tzu's wisdom to the modern digital landscape in which modern warfare is conducted.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle."

– Sun Tzu, *The Art of War*








Analyze

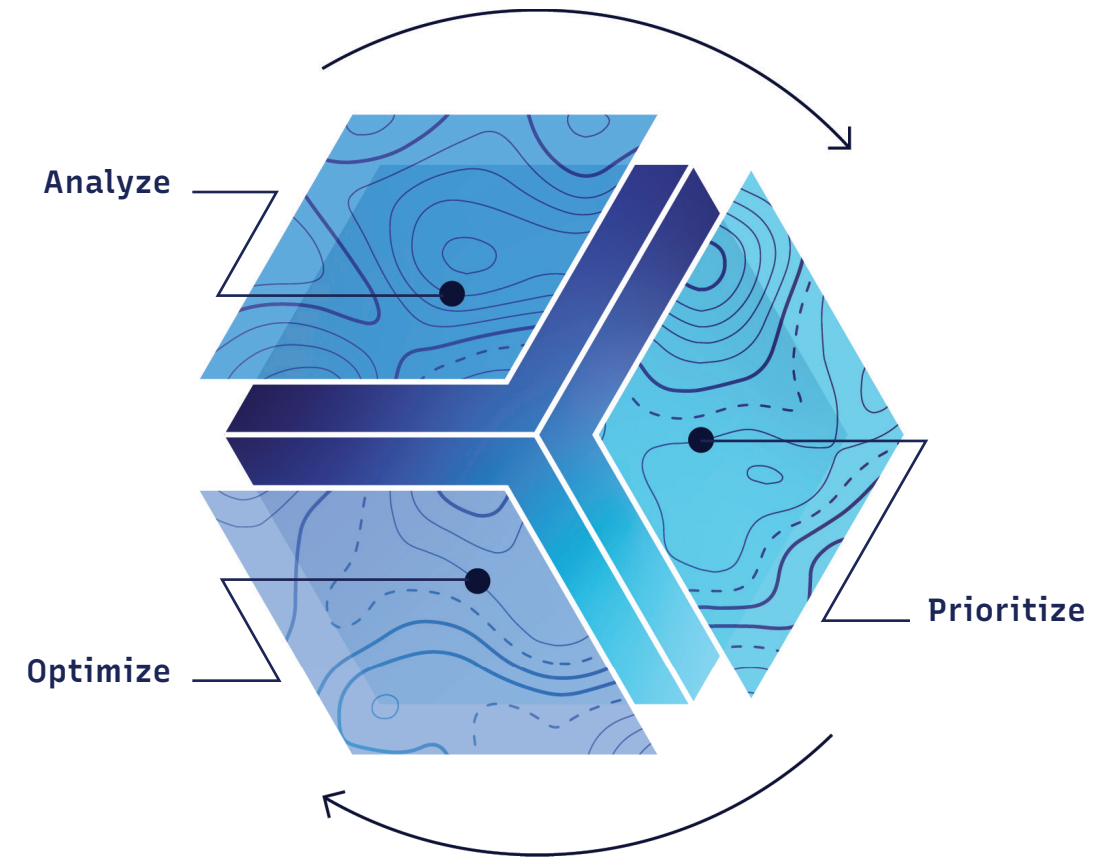
Know Yourself: Your Organization's Threat Profile

The initial step in enabling an effective CTEM capability is to Know Yourself. This means understanding key aspects of your organization to establish your organization's specific threat profile.

Once Interpres establishes a threat profile for your organization, it baselines defensive capabilities and identifies systems connected to your network which is a crucial initial step in positioning your organization's defensive posture. These measures provide a comprehensive view of your organization's defense readiness, including its strengths and weaknesses, and enable you to take proactive measures to strengthen areas of concern.

Some aspects that define a threat profile include:

-  Geolocations of operation
-  Company size
-  Industry Vertical
-  Types of data your organization protects internally or on behalf of customers
-  Platforms and technologies featured within your logical perimeter
-  Defensive tooling and controls mapped to MITRE ATT&CK®
-  Assets that are connected to the network and associated vulnerabilities



Know the Enemy: Finished Cyber Threat Intelligence

After comprehending your organization's threat profile, Interpres provides insights about your top adversaries. Finished cyber threat intelligence is a final product of threat intelligence that furnishes detailed information about cyber breaches and attributes the adversarial tactics, techniques, and procedures (TTPs) to cyber threat actor groups.

Throughout the years, the cyber defense industry has amassed a wealth of TTPs that have been made widely available by organizations such as the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), MITRE's Center for Threat-Informed Defense, and various open-source repositories. Interpres consumes finished cyber threat intelligence to perform analysis on the dynamic relationships between threat vectors and defensive capabilities.

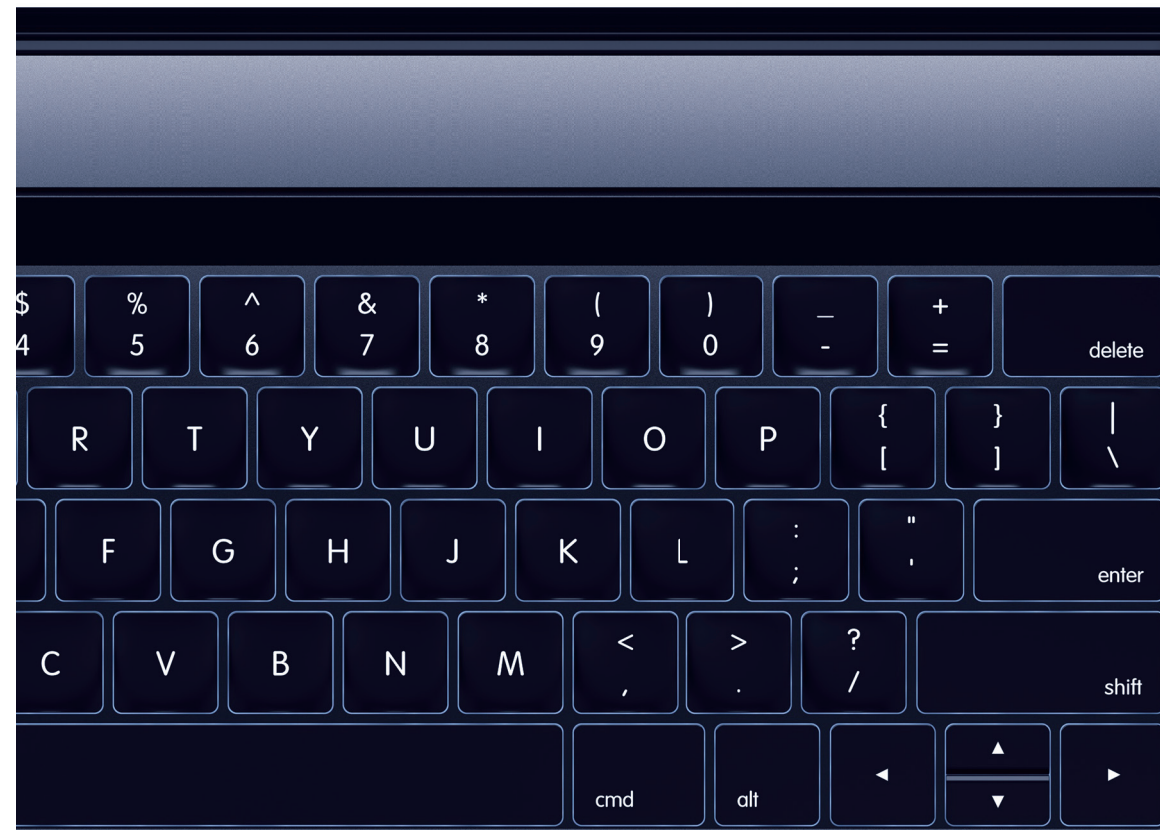
Prioritize

Adversarial TTPs, Malware Families, Threat Groups, and Vulnerabilities

Interpres prioritizes the adversarial Tactics, Techniques, and Procedures (TTPs) that are most likely to be encountered. This can be achieved by utilizing finished threat intelligence to comprehend the threat actor groups, malware families, and TTPs that are targeted towards organizations with similar threat profiles. Interpres also prioritizes vulnerabilities by exploitability and association with the identified threat profile.

Mitigative Actions

Interpres continuously performs automated analysis of your organization's readiness to defend itself against prioritized threat vectors. As the threat and defensive landscape changes, Interpres continuously provides recommended actions to implement that are most impactful with regards to reducing your organization's threat exposure.



Optimize

Defense Surface to Defend Against Prioritized Threats

In the past, cyber defense has typically followed a generalized, one-size-fits-all approach that has frequently resulted in failure. To achieve success, it is critical to customize defenses to combat prioritized threats. With your organization's threat profile identified, Interpres prioritizes threats through its threat modeling engine to align your defense surface technologies to combat the most significant threats. Interpres streamlines the analysis of defense surface tooling, enabling organizations to comprehensively evaluate their capabilities and optimize security posture in the areas of threat mitigation, visibility, and detection.



Mitigation

The preferred approach to threat defense is the complete mitigation of the threat. In this regard, Interpres assesses the extent to which security controls and sensor configurations are optimally enabled to prevent the execution of prioritized threat vectors. For identified areas of concern, Interpres prioritizes vulnerabilities to patch, security controls to enable, and security tool configurations to update that will mitigate threat vector execution.



Visibility

Effective threat detection requires proper visibility of threat activity. If a threat cannot be mitigated, it is imperative to understand the telemetry collection capabilities of the defense surface tools. Interpres leverages multiple perspectives to analyze telemetry collection, identifying gaps in visibility and recommending configuration changes to enhance the visibility of prioritized threats.

Organizations are often inclined to log all available data due to a limited understanding of the precise value of the various telemetry being collected, as well as the optimal manner in which the data should be utilized for both initial detection of adversarial activity and subsequent retrospective investigation of the scope and impact of a security breach. Interpres is designed to effectively identify and measure the most appropriate telemetry required for the detection of adversarial activity and for secondary triage, while also optimizing the most suitable and efficient storage options. This enables organizations to maximize the value of their telemetry while minimizing their data storage costs.



Detection Content

After establishing proper visibility, Interpres assesses whether the applied detection logic is suitable for alerting on adversarial activity discovered within the collected telemetry. Once detection gaps are identified, Interpres recommends detection logic to implement resulting in optimized detection coverage. Recommended detection logic can be injected into various defense surface tooling solutions.

Enterprise security products can analyze and generate alerts on a massive scale, a remarkable feat, however, the detection logic underpinning these products is developed with the broadest possible application in mind to ensure its efficacy across diverse environments. As a result, defenders are often inundated with false positives, leading to an unmanageable signal-to-noise ratio due to detections that are not custom tailored to threat most relevant to your organization. Additionally, the detection logic employed is not optimized to address the specific nuances of a given organization's security environment and industry, leaving gaps in detection coverage. Interpres maps relationships between adversarial TTPs and telemetry enabling your organization to create and inject detection logic suited to your specific threat profile that fill prioritized gaps in coverage.

Interpres Core Use Cases



Defense Readiness

As new threat advisories are released, Interpres automates analysis of adversarial campaigns. Interpres extracts the relevant information (TTPs, CVEs, Detection Logic, Log Collection) from the advisory and allows you to instantly under defensive readiness against the specified threats.



Defense Surface Optimization

Once Interpres baselines your organization's readiness against prioritized adversarial techniques, malware families, vulnerabilities, and threat groups, Interpres provides recommended actions to bolster defenses against the threats that matter most.



Prioritized Vulnerability Intelligence

Interpres connects to all the vulnerability scanning technologies featured within the defended environment and provides a threat centric prioritization which informed which vulnerabilities to patch first.



Continuous Threat Exposure Trending

Measure and maintain situational awareness by continuously monitoring the relationships between threats, vulnerabilities, defensive controls that include visibility, detections, and configurations.

Summary: Defense Surface Management is the Foundation

In conclusion, Continuous Threat Exposure Management (CTEM) and Threat Informed Defense (TID) are two powerful approaches that can help organizations strengthen their cybersecurity posture and reduce exposure of cyber threats. Implementing these approaches, however, can be challenging and require significant resources and expertise.

The Interpres platform automates and optimizes the implementation of CTEM and TID strategies, allowing organizations to efficiently enhance their security posture while minimizing the burden on their security team. Interpres provides a holistic capability that operationalizes TID & CTEM strategies across the entire organization, by combining disparate controls and products into a unified defensive surface that combats threats and minimizes risk in an automated feedback loop for Threat Fusion teams to proactively remediate and harden systems before an incident occurs.

By combining these approaches with Interpres, organizations can **reduce** their cyber threat exposure and **protect** their critical assets against the ever-evolving threat landscape in a **continuous** and **automated** fashion.

About Interpres Security

Interpres Security brings context to measuring security performance with a comprehensive new perspective to managing threat exposure. In today's rapidly changing threat environment, CISO's and security teams need a data-driven and threat-informed approach to measure defensive readiness that is rapid, scalable, and automated replacing lengthy and manual processes. We capture quantifiable data to understand what current controls can detect and defend against, identify gaps, deficiencies, and misconfigurations to optimize the security stack and maximize investments.

Interpres focuses on the dynamic relationship between the defense surface, adversarial TTPs and exploitable vulnerabilities that are likely to be used to attack an organization. Using continuous situational awareness, organizations know exactly how well they are prepared for existing and breaking events, with prioritized and recommended actions to mitigate gaps and optimize defensive coverage.

Interpres Security is backed by a top cybersecurity specialist investor, Ten Eleven Ventures.

To learn more, reach out to your account executive and visit www.InterpresSecurity.com.

Headquarters
Interpres Security

Published April 2024

WTP-A001

© 2024 Interpres Security and/or its affiliates. All rights reserved.

Interpres and the Interpres logo are trademarks or registered trademarks of Interpres and/or its affiliates in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Interpres and any other company.

Cyber**Proof**[®]
A UST Company



INTERPRES