INTERPRES

Solution Brief: **Public**

Interpres Security: Determining Cyber Defense Readiness

Determining threat exposure and defensive readiness against the latest threats is a daily struggle for the CISO and their teams; it is a manual, spreadsheet exercise, it is time-intensive, and rarely scales to large and complex security environments. Finally, it is static and not actionable.

Whenever a new advisory or threat appears on the horizon, organizations must determine if it applies to them, then they start the cycle of manually assessing their defensive controls in relation to the threat. The readiness assessment process involves comparing threats to controls, detection logic, telemetry, and other data sources, with mapping tracked across multiple spreadsheets.

This process takes anywhere from 4 days to 4-6 weeks and consumes hundreds of labor hours.

The Interpres Threat Exposure Management Platform automates the analysis of adversarial threats to determine readiness within minutes, not days.

Interpres' unique functionality is based on the automated analysis of the relationships between threats, vulnerabilities and defensive controls. Interpres continuously monitors the state of this relationship providing near, real-time situational awareness of your cybersecurity ecosystem.

With Interpres, a Fortune 500 Insurer automated their analysis process and reduced time to readiness from 4-6 weeks to 1 hour.

Interpres
Automated Analysis Process

Interpres starts with understanding key aspects of your organization and unique environment to establish your organization's specific threat profiles.

Interpres baselines your defensive capabilities and identifies systems connected to your network. These measures provide a comprehensive view of your organization's defensive surface.

After understanding your organization's threat profile, Interpres provides insights about your top adversaries.

This is achieved by utilizing finished, national threat intelligence to identify threat actor groups, malware families, and TTPs that are targeted towards organizations with similar threat profiles.

The Interpres process extracts relevant information from an Advisory: TTPs, CVEs, Detection Logic and Log Collection.

Automation and operationalization of this TTP-based threat data across your entire tech ecosystem informs all aspects of the security infrastructure in order to measure cyber readiness against prioritized threats.

A critical element of measuring threat exposure is the ability to analyze the dynamic relationship between adversarial and defensive capabilities.

The Interpres analytics engine holistically ties together all relationships between your defenses, assets, threats, and vulnerabilities. Continuous threat exposure conducted in this manner provides situational awareness to ensure you know exactly how well you are prepared for current and emerging threats. Based on this insight, you're alerted to any shift in your security posture that can allow you to pivot to prioritized threat remediation quickly and proactively before an attack occurs.

For security leaders and their teams, automating the assessment, identification, and management of threat exposure yields quantifiable data on your security posture and the ability to defend against the threats that matter most. Not only do you replace your spreadsheet-driven, manual process, you save time, save resources, and reduce risk exposure faster.

With Interpres

- Gain knowledge of the threats targeting your organization.
- Capture quantifiable data on the readiness of your defensive controls against prioritized threats.
- Leverage one person to do the work of an entire threat intelligence team.
- Understand your threat exposure to proactively fix gaps in your defenses.
- Reduce risk and increase readiness against the threats that matter most.

About Interpres

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, visit **www.InterpresSecurity.com**.

Interpres Security
Published December 2023

Solution Brief: **Public**
SB_CDR_12_2023