Operationalized Threat Intelligence

SPONSORED BY

A SANS First Look

Written by **Matt Bromiley** | November 2023

Introduction

The threat landscape is vast and diverse. Adversary campaigns gain new or utilize existing tactics, techniques, and procedures (TTPs), forcing security teams to determine where to focus their resources and defenses. However, trying to keep up with every adversary can be an exercise in futility. Converting threat intelligence and knowledge of adversary TTPs into actionable measures is labor intensive.

Perhaps even more challenging is aligning and analyzing the relationship between cyber threats and defensive measures in place. How can a security team possibly expect to evaluate exposure risk within their security ecosystem in this ever-changing landscape? In this SANS First Look, we learned about Interpres Security ("Interpres"), a platform that turns these challenges around.

As a continuous threat exposure platform, Interpres simplifies the comparison of knowing the *threats that matter* and how an organization's security posture stands up against them. The platform empowers organizations to assess their level of cyber readiness in response to the latest advisories, vulnerabilities, or adversary campaigns. With this knowledge, organizations have the insight to defend against the most relevant cyber threats.

A Look at Interpres Security

We began our look at Interpres with an initial understanding of the problem that the platform is designed to solve. Current methodologies of transforming threat intelligence into actionable security posture assessments are time-intensive and laborious tasks. These processes are predominantly centered on indicators of compromise (IOCs) or restricted to a narrow range of technologies, leading to potential coverage gaps or a false sense of security against threats. Furthermore, organizations often find it difficult to prioritize threats respective to their organizations and subsequently report on their readiness against those threats.

Interpres helps security teams solve these issues, providing real-time situational awareness and assessing threats against in-place security controls. Figure 1 provides an example of Interpres's workflow diagram.

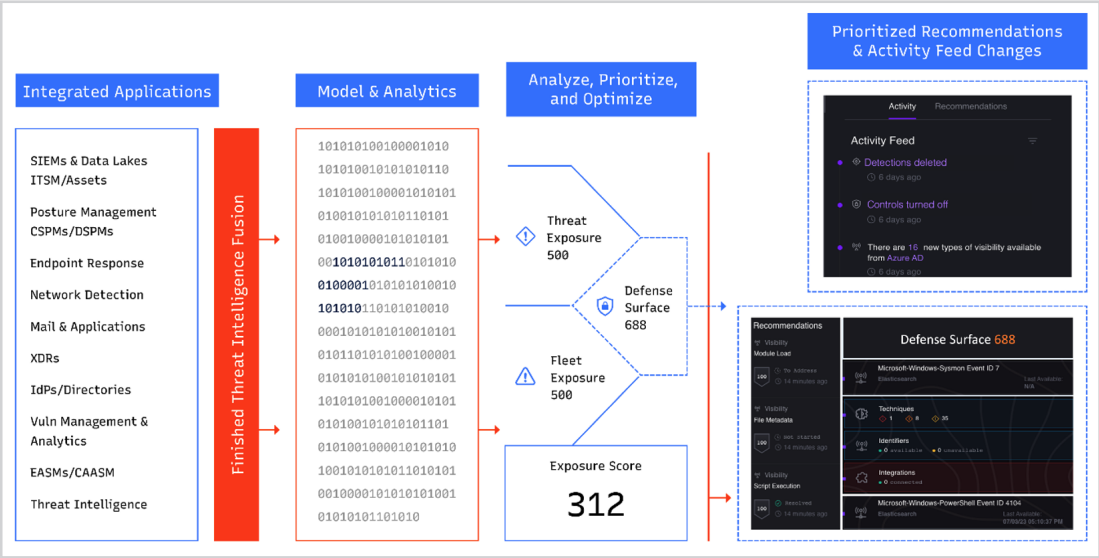

Figure 1. Interpres Workflow Diagram

Interpres looks at an organization's defensive posture and its ability to mitigate, provide visibility into, and detect adversarial activity. This is coupled with raw threat intelligence feeds and its custom models and analytics. The resulting output, the "Interpres Exposure Index," is a simple score that can help organizations determine "just how exposed are we?"

Operationalizing Threat Intelligence

The first hurdle Interpres helps organizations overcome is the operationalizing of threat intelligence. As mentioned earlier, continuously taking threat reports or raw intelligence feeds and rendering them actionable with respect to an organization's custom environment is tedious. For many organizations, this is achieved by converting data into some category of detection and ensuring that they are active across their environment. Interpres observed two gaps in this process:

1. The uphill part of this task.
2. Not all threats matter to all organizations.

The latter is the most critical assessment: Should *every* organization try to defend against every threat? No, of course not. However, how does an organization know where to focus its efforts?

To help answer this, Interpres examines key attributes of various threats, including targets, industries, and TTPs of choice, among many other factors. This granular knowledge of threats and threat actors allows it to offer a voice of confidence that some organizations are more likely targets than others.

There is an essential lesson for security teams here (hence, Interpres's value): Organizations simply *cannot* prioritize defenses against every threat out there. Resources are not unlimited, nor do security analysts have time to keep up with every new threat campaign released. Interpres shoulders this responsibility, allowing organizations to know what attacks they have a higher chance of experiencing. Security teams can focus and prioritize their defense posture accordingly.

It's worth noting that although we call out *the threats that matter*, this does not mean "ignore all other threats." Threat actor TTPs often overlap—tools or techniques in particular—and defense against one often can equal defense against many. Interpres helps organizations focus their resources and capital.

Continuous Assessment and Exposure

In addition to prioritizing the threats that matter, Interpres constantly evaluates an organization's defensive posture against those threats. Adversaries can change daily, and so can an organization's ability to defend against them. Furthermore, security configurations can fall out of sync. A critical log may get disabled or a security tool may be misconfigured. One of the key value points of Interpres's platform is the ability to continuously assess and evaluate changes in the relationship between elements of threat and defensive capability, resulting in dynamic exposure scoring. That gives organizations the ability to continuously evaluate their exposure.

We found this to be one of the biggest advantages to this platform: a constant, up-to-the-minute assessment of your defense posture. Far too often, security teams have a "point-in-time" assessment (consider a penetration test or vulnerability scan). These data points were useful *on the day* the scan or test was conducted. However, such an assessment does not capture changing adversary techniques.

Another valuable takeaway is an assessment of what an organization's security controls can and cannot do—compared to what the security team *thought* they could do. A tough lesson to learn is when a security control "fails," only for an organization to realize that the control could not do what was asked of it. Without proper testing or assessment, how would they ever know?

A quick note: Interpres is not a replacement for red teaming operations or attack surface management. Rather, it focuses on *defensive* capabilities and helps prioritize necessary actions. Again, with operationalized threat intelligence, there's no longer a need for an organization to worry "if" it's protected. Interpres helps it confirm it is.

Closing Thoughts

Aligning an organization's security posture to the threats that matter is often easier said than done. It is manual and tedious to take information from a threat intelligence source and convert it into actionable, realized defenses. So much so that it is rarely implemented correctly to provide feedback to the security team. In this First Look, we examined Interpres Security, a platform that reverses that equation.

With its threat correlation and deep insight, Interpres provides a dynamic understanding of an organization's defense capabilities and alignment to active threats. This helps the security team understand where they have gaps in coverage or detection capabilities and gives the organization an accurate idea of exposure risk.

Finally, this is not a point-in-time assessment. Interpres is continuous, morphing its risk assessment based on active threats and the defensive stack at any time. Security teams are no longer guessing if they are defended. Interpres provides actionable assessment results that help keep the team focused and adversaries at bay.

Sponsor

SANS would like to thank this paper's sponsor: