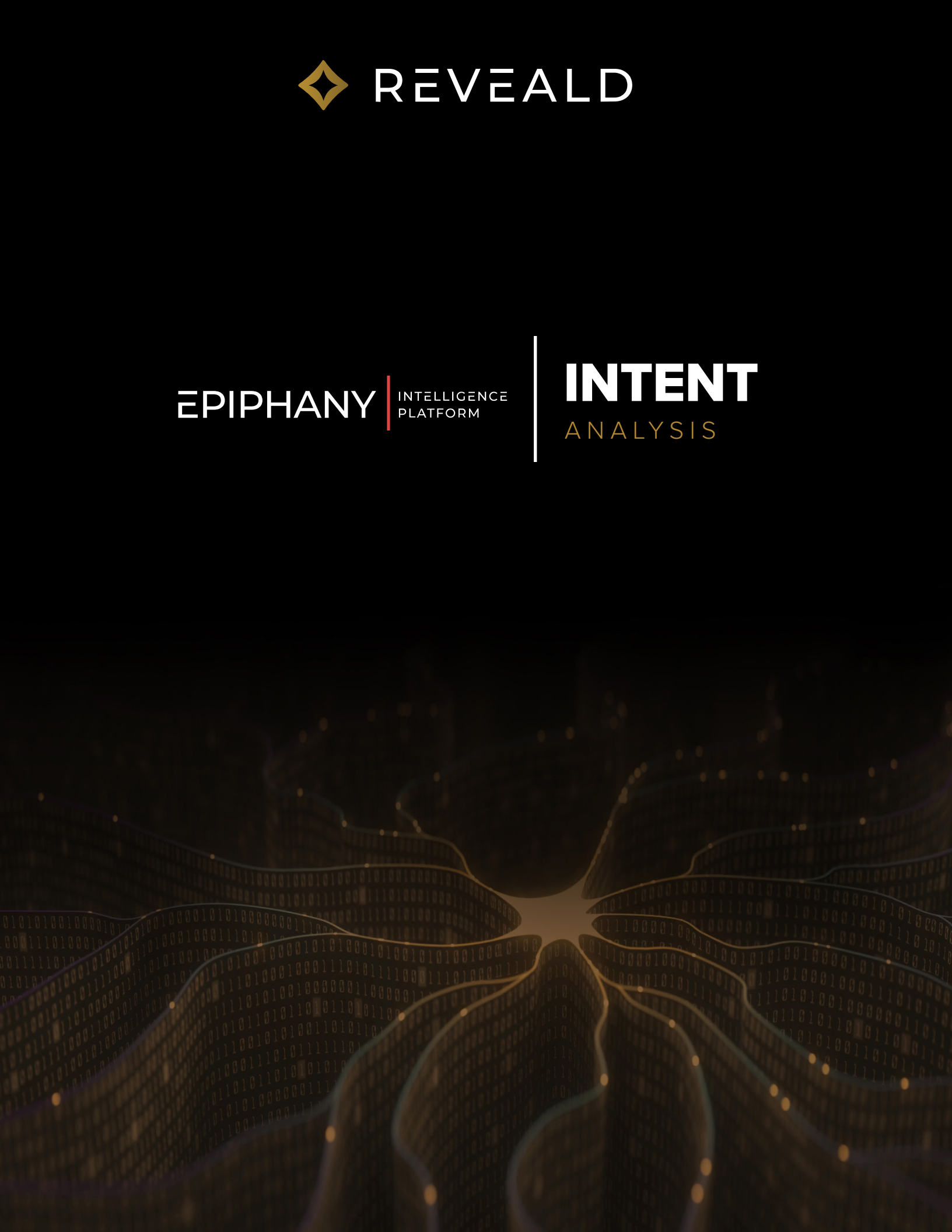
REVEALD

EPIPHANY | INTELLIGENCE PLATFORM

INTENT ANALYSIS



INTRODUCTION

In today's complex threat landscape, organizations face the overwhelming task of monitoring and responding to an increasing number of security events. Security Information and Event Management (SIEM) solutions have become a core tool in this battle, allowing organizations to collect and analyze logs from various sources, but traditional approaches to threat hunting and incident response leave security teams constantly reactiveiii. SIEM rules need to be written, tuned, and maintained to detect specific indicators of compromise (IOC), but the sheer volume of logs and events generated often leads to alert fatigueiii, missed threatsiv, and a collection of helper tools.

The challenge for modern cybersecurity teams is to find a more efficient way to sift through the noise and identify the truly critical threats that can lead to a breach. By focusing on attack paths and known exposures, AI-integrated platforms such as Epiphany narrow the scope of threat hunting to what really matters: the vulnerabilities and weaknesses that adversaries are most likely to exploit, because they facilitate the goals of the adversary – access to data, systems, and control.

In this white paper, we explore how the Reveald Epiphany platform shifts the focus from writing detection engineering rules in SIEMs to a streamlined process of using automated querying for relevant events based on the impact of attack paths as defined by reinforced-learning, pre-trained AI models, allowing organizations to prioritize decisions that protect the environment rather than investigating every potential alert.

THREAT HUNTING TODAY

One useful definition of cybersecurity threat hunting by IBM is[1]:

A proactive approach to identifying previously unknown, or ongoing non-remediated threats, within an organization's network.

To achieve this, current methodologies leverage analysts with significant expertise to sift through mountains of logs and security alerts to uncover threats. Often these analysts are assisted by prioritization algorithms, outlier detection, industry-standard weighting models etc., but the effort is exclusively driven by log data collated from disparate systems. Security teams using traditional SIEMs are responsible for creating detection engineering (DE) rules, which specify what activity should trigger an alert. These rules are typically based on threat intelligence, known attack techniques, or specific signatures of malicious behavior, and are applied to activities that have already happened. Writing detection rules can be complex, many platforms require them to be constructed in standard formats such as YARA or Sigma, coding languages like Python, or database query languages like SQL[2].

While effective to some extent, this method has inherent challenges:

- **VOLUME OF DATA:** SIEMs generate an overwhelming number of alerts, the majority of which may not be relevant or actionable. This often leads to alert fatigue and potential oversight of critical incidents.

[1] *https://www.ibm.com/topics/threat-hunting*

[2] *https://medium.com/@rcxsecurity/detection-engineering-the-soc-writing-a-detection-rule-e24f4d7f69e8*

- **RULE TUNING AND MAINTENANCE:** DE rules require continuous adjustment to stay relevant in an evolving threat landscape. A rule that was effective last week might need to be revised this week, as attackers change their methods.
- **INVESTIGATING FALSE POSITIVES:** Traditional SIEM rules often flag benign activities as malicious, forcing security teams to spend valuable time investigating events that ultimately pose no threat.
- **REACTIVE POSTURE:** Organizations are responding to threats after they've materialized, rather than identifying and addressing exposures that adversaries could leverage in the future.

The result is a reactive, time-consuming process that leaves security teams one step behind attackers.

THREAT HUNTING TOMORROW (WITH EPIPHANY INTENT ANALYSIS)

The Epiphany Intelligence Platform (EIP) transforms threat-hunting processes by shifting the focus from traditional detection rules to identifying, prioritizing, and monitoring the progression of attacks through pre-discovered attack paths and known exposures. This shift not only enhances efficiency but also ensures that organizations focus on protecting critical assets rather than chasing down inconsequential alerts.

With EIP, there is no need for security teams to manually craft and maintain a full comprehensive library of detection rules in their SIEMs. Instead, the platform leverages its deep knowledge of attack paths, which map out the routes adversaries are most likely to take to exploit vulnerabilities in an environment to achieve their goals. By querying SIEM logs for events directly related to these attack paths, Epiphany narrows the scope of investigation to only those activities that could realistically impact the organization.

If a series of preliminary acts of an adversary cannot proceed to achieve an ultimate business impact, even if only the first steps of an attack have been seen, this activity is naturally less critical to address than a sequence which could ultimately create a business risk. The Intent of the adversary's activity can be predicted, and appropriate actions taken.

The shift to intent based prioritization offers several advantages:

- **PRECISION IN THREAT DETECTION:** By focusing only on known exposures and attack paths that result in business risk, Epiphany reduces the noise generated by traditional SIEM alerts and surfaces only the events that truly matter.
- **AUTOMATED QUERYING:** The platform automatically queries logs and correlates relevant events based on attack paths, freeing security teams from the need to manually craft and maintain detection rules.
- **STREAMLINED DECISION-MAKING:** Since Epiphany surfaces only critical alerts, security teams can make informed decisions more quickly, focusing on protecting the environment rather than investigating potential false positives.
- **EFFECTIVE MOBILIZATION:** Epiphany provides full context of each attack path and indicates why it is important for the business to block the attack – requests for changes, patches etc. are qualified in terms of direct business risk.

THE CONTINUOUS AI THREAT HUNTING CYCLE

Epiphany's threat-hunting methodology is powered by an AI-driven engine that continuously analyzes known vulnerabilities, threat intelligence, and real-time events in the context of the organization's attack surface. The platform operates in a continuous loop that ensures no potential threat goes unnoticed, while also reducing the operational burden on security teams.

Here's how the continuous AI threat-hunting cycle works:

- **IDENTIFY ATTACK PATHS:** Epiphany begins by mapping out every potential attack path based on known vulnerabilities and misconfigurations in the environment (retrieved from existing configuration management, security, and assessment tools). These paths represent the routes an attacker could take to compromise critical assets. Paths which result in material risk to the organization are automatically prioritized.
- **QUERY SIEM LOGS:** Rather than relying on predefined rules, Epiphany queries the SIEM for events related to these attack paths. This ensures that only relevant logs and activities are surfaced for review.
- **CORRELATE EVENTS WITH KNOWN EXPOSURES:** The platform automatically correlates events with the organization's known exposures, allowing it to prioritize events that pose an actual risk because they facilitate the progression of attack paths which create material business impact.
- **CONTINUOUS MONITORING:** Epiphany continuously monitors the environment for any changes in attack paths or new events that could impact the organization, ensuring that security teams always have the most up-to-date information.

This continuous AI-driven cycle allows security teams to stay ahead of potential threats without drowning in irrelevant data, because events can be described in terms of the Intent of the attack to gain a position within the environment which is advantageous to the attacker.

Benefits of Moving to **This Methodology**

Adopting Epiphany's approach to threat hunting offers several key benefits for threat hunting teams that enhance an organization's security posture and operational efficiency:

- **REDUCED ALERT FATIGUE:** By filtering out irrelevant alerts and focusing only on events related to attack paths to material risk, Epiphany dramatically reduces the number of alerts security teams need to prioritize for investigation.
- **INCREASED OPERATIONAL EFFICIENCY:** With Epiphany automating the querying process and surfacing only critical alerts, security teams can allocate more time to proactive security measures rather than manual rule-writing and investigation.
- **PROACTIVE RISK MANAGEMENT:** Rather than reacting to events after they happen, Epiphany's approach allows organizations to focus on known exposures and attack paths before they can be exploited, shifting the security posture from reactive to proactive.
- **ACTION DRIVEN:** By providing contextualized alerts that are directly tied to the organization's attack surface, Epiphany enables security teams to make faster, more informed decisions to drive change.

THE CONTINUOUS CYCLE: IDENTIFY RISKS, PRIORITIZE, VALIDATE MONITORING, MONITOR FOR EXPLOITATION

Epiphany's methodology follows a continuous cycle of risk identification, prioritization, validation, and monitoring. This process ensures that organizations can stay ahead of evolving threats while maintaining a clear focus on protecting critical assets.

- **IDENTIFY RISKS:** Epiphany continuously scans the environment for vulnerabilities and misconfigurations that could lead to an exploit.
- **PRIORITIZE FOR REMEDIATION:** Based on the attack paths and the criticality of assets, Epiphany prioritizes vulnerabilities for remediation, ensuring that security teams focus on the most impactful risks.
- **VALIDATE MONITORING AND CONTROLS:** The Epiphany Validation Engine generates test events to confirm that your security controls, such as the EDR, are functioning effectively. By continuously mapping attack paths and identifying those that are actively being exploited, Epiphany can demonstrate that the control can produce the alert necessary for Epiphany to detect a path being exploited.
- **MONITOR FOR EXPLOITATION:** Once controls are in place, Epiphany continues to monitor the environment for signs of exploitation, ensuring that any new threats are quickly identified and addressed.

This cycle not only ensures that known vulnerabilities are addressed but also that any new risks are swiftly identified and prioritized.

CONCLUSION

In the evolving world of cybersecurity, traditional threat-hunting methods are no longer enough to keep up with the pace of modern attackers. Epiphany's innovative Intent-based approach to using attack paths and querying SIEMs for relevant events offers a new way forward. By focusing on known exposures and reducing the need for manual rule-writing, Epiphany allows organizations to move from a reactive to a proactive security posture, enabling faster, more informed decision-making.

The result is a streamlined, efficient threat-hunting process that reduces noise, prioritizes critical risks, and ensures that security teams can focus on what matters most: protecting the environment from real threats. Epiphany's continuous AI-driven methodology ensures that no potential vulnerability goes unnoticed, providing organizations with the tools they need to stay ahead of the threat landscape and secure their critical assets.