REVEALD

EPIPHANY | INTELLIGENCE PLATFORM

LEVERAGING A.I.

FOR ATTACK PATH PRIORITIZATION

Leveraging A.I. in Epiphany:

Enhancing Threat Detection and Prioritization

INTRODUCTION

In today's rapidly evolving threat landscape, organizations face the challenge of managing an overwhelming number of vulnerabilities, attack paths, and potential risks across their digital assets. As traditional methods of risk management struggle to keep up with the dynamic nature of cyber threats, Epiphany offers an innovative AI-driven approach to effectively classify, prioritize, and address security concerns. This white paper provides insight into how Epiphany utilizes Artificial Intelligence (AI) to transform how organizations identify, assess, and respond to vulnerabilities, making it easier for our partners to understand the value AI brings to the table.

Epiphany's AI capabilities can be categorized into three primary areas:

1. CLASSIFICATION MODELS FOR VULNERABILITY RECLASSIFICATION AND RESCORING

2. REINFORCEMENT MACHINE LEARNING FOR PATH SCORING AND PRIORITIZATION

3.IDENTIFICATION OF HIGH-EXPOSURE OR HIGH-IMPACT ASSETS, IDENTITIES, AND APPLICATIONS

1. AI-POWERED CLASSIFICATION MODELS FOR VULNERABILITY RECLASSIFICATION AND RESCORING

UNDERSTANDING THE CHALLENGE

Vulnerability management tools often produce an overwhelming amount of data, categorizing vulnerabilities into broad, sometimes irrelevant groups, which leads to misclassification, inadequate prioritization, and resource misallocation. This results in critical threats being overlooked or lower-priority vulnerabilities consuming excessive time and attention.

HOW EPIPHANY'S AI ADDRESSES THE ISSUE

Epiphany employs sophisticated classification models to reclassify vulnerabilities into precise, actionable categories such as Local Privilege Escalation (LPE), Remote Code Execution (RCE), and Social Engineering (SE). This AI-driven reclassification process not only helps in accurately identifying the nature of each vulnerability but also ensures that the risk posed by these vulnerabilities is contextually scored according to your organization's unique environment and the attacker's opportunities to leverage them.

KEY BENEFITS

- **GRANULAR RECLASSIFICATION:** Epiphany's AI engine examines each vulnerability, moving beyond generic industry labels to provide an accurate assessment based on real-world exploitation patterns.
- **CONTEXTUAL RISK SCORING:** By considering factors such as asset criticality, potential impact, and exploitability, Epiphany's AI delivers a risk score that reflects the true threat level of a vulnerability in your organization.
- **ENHANCED EFFICIENCY:** Security teams are empowered to focus on vulnerabilities that pose the most significant threat, optimizing resource allocation and reducing remediation timelines.

Example in Practice:

Rather than treating every vulnerability in a critical system as equally dangerous, Epiphany's AI may reclassify an SE vulnerability as a top priority based on its potential to gain access and compromise sensitive data on a system due to a user being present on that system, ensuring your team addresses the most impactful risks first.

2. REINFORCEMENT MACHINE LEARNING FOR PATH SCORING AND PRIORITIZATION

UNDERSTANDING THE CHALLENGE

Organizations often struggle to understand how individual vulnerabilities combine to form complex attack paths, which attackers can exploit to compromise critical assets. Without a clear understanding of these attack paths, organizations may end up addressing isolated vulnerabilities without mitigating the most significant threats.

HOW EPIPHANY'S AI ADDRESSES THE ISSUE

Epiphany utilizes a reinforcement machine learning model to analyze, score, and prioritize entire attack paths, considering the sequence of vulnerabilities, potential attack vectors, defensive control resistance, and the ease of exploitation. By continuously learning from new threat intelligence, user feedback, and observed attack patterns, this AI-driven model

adapts to evolving threats, providing an up-to-date understanding of the most critical attack paths.

KEY BENEFITS

- **COMPREHENSIVE PATH ANALYSIS:** Unlike traditional vulnerability management or attack surface management solutions that assess threats in isolation, Epiphany enumerates all potential paths and allows the AI to evaluate all the attack paths, allowing organizations to see the bigger picture of how threats could unfold. Paths which do not result in a material risk can be deprioritized to reduce noise.
- **DYNAMIC PRIORITIZATION:** As the threat landscape changes, Epiphany's reinforcement learning model updates path scores, ensuring that security teams always have a prioritized list of attack paths to address.
- **EFFECTIVE RESOURCE ALLOCATION:** By focusing on the most valuable paths attackers would exploit, organizations can allocate resources efficiently, addressing high-risk areas before they can be compromised.

Example in Practice:

If an attacker could potentially gain access by exploiting a network-based application, escalate privileges, and then move laterally to a critical database server with a harvested identity, Epiphany's AI would identify this complete attack path, prioritize it based on risk, and recommend mitigation actions at each step to prevent a successful breach. Epiphany's AI is always looking for the paths that have the highest value to the attacker: **lowest risk, highest value, shortest distance.**

3. AI-DRIVEN IDENTIFICATION OF HIGH-EXPOSURE AND HIGH-IMPACT ASSETS, IDENTITIES, AND APPLICATIONS

UNDERSTANDING THE CHALLENGE

Not all assets, identities, or applications within an organization are equally valuable or vulnerable. However, pinpointing which ones present the highest exposure or potential impact based on dynamic and evolving factors can be challenging without advanced analytics.

HOW EPIPHANY'S AI ADDRESSES THE ISSUE

Epiphany's AI models continuously analyze your environment, identifying assets, identities, and applications that exhibit high exposure or high impact characteristics. These models consider various factors, such as access levels, connectivity, and external threat intelligence, to recognize elements that could become high-value targets for attackers.

KEY BENEFITS

- **PROACTIVE IDENTIFICATION:** Epiphany's AI proactively identifies assets, identities, and applications that are at increased risk, even if they haven't been directly compromised, allowing organizations to take preventative actions.
- **CONTEXTUAL AWARENESS:** The system understands the relationships between assets and how they contribute to the overall security posture, enabling more informed decision-making.
- **REDUCED ATTACK SURFACE:** By identifying and protecting high-exposure elements, organizations can significantly reduce their attack surface, making it more challenging for threat actors to exploit vulnerabilities.

Example in Practice:

If an administrative identity is connected to multiple high-value assets with weak or outdated controls, Epiphany's AI will flag this identity as high-risk, allowing the organization to implement **stronger safeguards** before an attacker can take advantage.

4. THE CONTINUOUS AI THREAT HUNTING CYCLE

Epiphany's AI doesn't just stop at classification, path prioritization, or high-exposure identification. It continuously learns and adapts as new threat intelligence is integrated, keeping your organization ahead of emerging risks. This ensures that the platform remains effective in identifying new attack paths, emerging vulnerabilities, and high-impact assets in real-time.

BENEFITS OF USING EPIPHANY'S AI-DRIVEN APPROACH

- **PRECISION AND ACCURACY:** Epiphany's AI ensures that vulnerabilities and attack paths are accurately classified, prioritized, and addressed, reducing false positives and wasted effort.
- **ADAPTABILITY:** As threats evolve, so does Epiphany. Its AI models continuously learn, ensuring that your organization's defenses remain aligned with the latest threat landscape.
- **SCALABLE SOLUTION:** Epiphany's AI-driven approach scales with your organization, allowing even the most complex environments to benefit from advanced threat detection and prioritization.
- **REDUCED WORKLOAD:** By focusing only on critical vulnerabilities and high-risk attack paths, your security team can spend more time on strategic initiatives and less time investigating false alarms.

CONCLUSION

Incorporating AI into vulnerability management and threat hunting is no longer a luxury—it's a necessity. Epiphany's AI-driven approach offers unparalleled insights, precision, and efficiency in managing and mitigating threats, ensuring your organization remain