EPIPHANY SYSTEMS

SNAPSHOT | A Security Leader's Guide

How to Start Risk Hunting with Epiphany

INTRODUCTION

Risk hunting with Epiphany gives you complete visibility of your strategic business risks—not just your technical vulnerabilities. And risk hunting prioritizes your most important risks—so you can focus mitigation more efficiently.

With Epiphany, you're not limited to counting how many vulnerabilities have been patched. And you don't have to simply react to threats. The Epiphany Intelligence Platform is proactive—it goes to work before an attack occurs.

Epiphany hunts down the points in your environment where technical threats meet your business operations. It looks at vulnerabilities in context with the systems that drive your revenue, control your costs, and protect your reputation.

If your security programs are overwhelming you with data, and you're chasing too many false-positive alerts, it's time you started risk hunting instead.

Here's how to start risk hunting with Epiphany.

THE FIVE TACTICAL STEPS OF RISK HUNTING

1 PREPARE | **2 ASSOCIATE** | **3 EXPLORE** | **4 ASK** | **5 HUNT**

There's a logical progression to successful risk hunting, and it starts with good preparation. To accurately align your security posture with your true business risks, you need to evaluate your systems on three levels: business, operating process, and supporting assets.

Business Level

Work with executive leadership to identify business risks at the organizational level:

- What keeps the business running?
- What puts the business at risk?
- Which things are critical? What creates emergencies for IT?
- Which associated metrics are important (e.g., revenue, uptime, data handling, exposure)?

Examples of assets that can be mapped to processes include:

- Configuration management database
- Vulnerability data
- Third-party penetration testing reports
- Threat intelligence feeds
- Network configuration information
- Endpoint protection data
- Vulnerability scan results
- Firewall rules and access control lists
- Routing rules
- Windows AD configuration

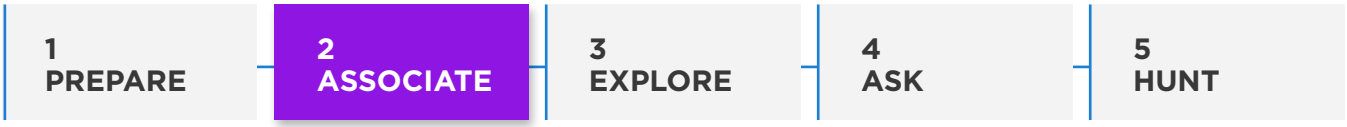
OPERATING PROCESS LEVEL

Map metrics for business impacts to systems, processes, and assets. Each element should be categorized by its importance in driving your business. Elements may include detailed sub-elements, supported by multiple IT systems.

Also map people (system users) to the processes they impact in your organization. For example, responsibility for financial accounting processes would belong to a CFO or a VP of a business unit.

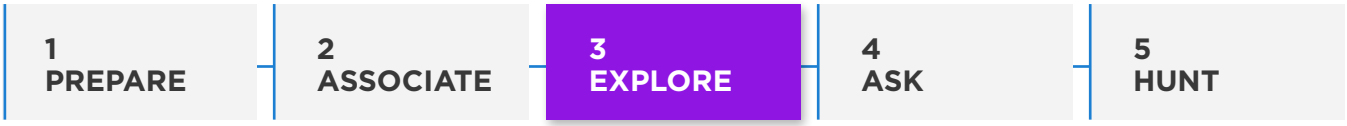
SUPPORTING ASSET LEVEL

Identify both IT and non-IT data sources associated with critical systems, processes, and users. This should connect clean lines between specific assets, processes, and process owners—and show how they map to metrics. (Note: non-IT data is especially helpful in understanding how risks affect people.)



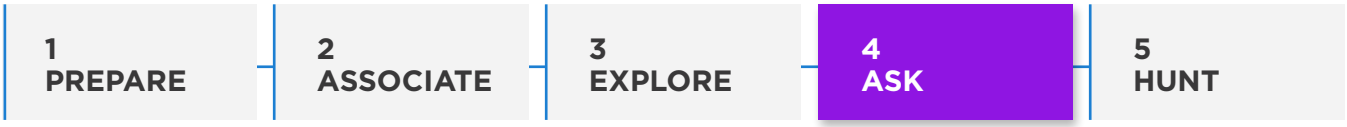
Integrate data sources into the Epiphany Intelligence Platform for aggregation and correlation. Epiphany can scale almost infinitely, integrating new data sources as they become available.)

Use Epiphany to understand associations between assets and business operations. What critical systems, processes, and users does each asset support? If any asset is compromised, what might happen? What critical systems, processes, and users could be at risk?



Use Epiphany to mine and define detailed contextual relationships between business processes and their supporting assets.

Evaluate the resulting data. Is it logical? Are the assets associated correctly? Do the connections between business processes and assets meet or differ from expectations?



Formulate questions for Epiphany to answer, such as: What processes are most essential for my business? How could these processes be attacked and stopped? What assets contain the “keys to the kingdom”? What are all the ways those assets could potentially be compromised? And can impacts be measured with the metrics you identified in Step 1?

By ingesting and processing vast amounts of meaningful data, Epiphany gives you the unique ability to answer broad questions like these. The answers will guide Epiphany in identifying threat actors and the attack surfaces they could exploit. This threat modeling will validate Epiphany’s ability to prioritize critical business processes.

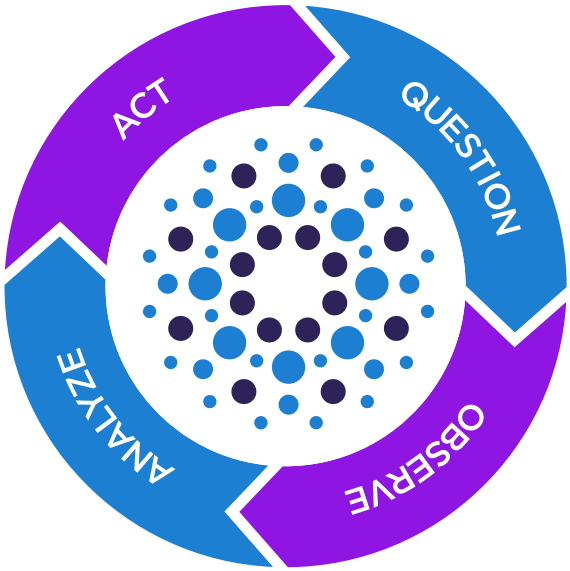
With the threat model defined, you can then ask Epiphany: What would a threat actor do with access? How could an attacker gain domain administrator access, change configuration settings, or access source code? Are the attack paths correctly identified? What is the probability that different types of attacks would succeed? And what would the business impacts actually be?

1 PREPARE	2 ASSOCIATE	3 EXPLORE	4 ASK	5 HUNT

Once you've completed Steps 1–4, you can start actively hunting for risks throughout your environment. Epiphany will align your assets, processes, and technical vulnerabilities with the critical operations and objectives that drive your business. And show you—with visualizations you can share easily with all stakeholders—which risks need the most urgent attention.

Even better, Epiphany will continuously identify and prioritize new or shifting risk conditions as your environment changes. This risk hunting cycle helps ensure that you stay ahead of risks—before they can impact your business.

1. **QUESTION.** Determine potential attack paths into your environment—and targets of opportunity along those paths—with Epiphany's visualization tools.
2. **OBSERVE.** Identify key points of transition where attacks could flow inside your environment, and explore possible outcomes. (Once inside, where could an attacker go, and what business impacts would result?)
3. **ANALYZE.** Prioritize each business risk, and isolate the most effective way to negate each risk at specific points.
4. **ACT.** Execute remediation, including patching, to prevent potential attacks—before they start. Then, as your environment changes with time, repeat the Risk Realization Cycle to identify, prioritize, and mitigate additional risks.



Awareness powers protection.

Contact us today to get started with Epiphany.

Contact Us

ABOUT EPIPHANY SYSTEMS

Epiphany delivers world-class cybersecurity solutions for enterprises in every sector of government and industry, including the Fortune 500. We are dedicated to reducing technical and business risks through innovative technologies, including artificial intelligence and machine learning.

Our mission is to safeguard our clients' data, assets, and operations across the globe. We assess each client's unique needs and challenges to ensure that their risks are visible, managed, and mitigated. If it's connected, it must be protected.