



# Attack Path Analysis Generative AI Best Practices Guide

---

Last Revised: May 11, 2026



# Table of Contents

|  |          |
|--|----------|
| <b>Attack Path Analysis: Generative AI</b> ..... | <b>3</b> |
| Attack Path Summarization .....                  | 3        |
| AI Explainability .....                          | 4        |
| Mitigation Guidelines .....                      | 4        |
| <b>Sample Questions</b> .....                    | <b>6</b> |
| <b>Limitations</b> .....                         | <b>6</b> |
| Context .....                                    | 6        |
| Rate Limit .....                                 | 9        |
| Quota .....                                      | 10       |



# Attack Path Analysis: Generative AI

This document emphasizes the different use cases using generative AI in Attack Path Analysis. It highlights some of the limitations and provides tips on how to get the most out of it for your business use.

In Attack Path Analysis, you can find AI-generated content when using the following features:

## Attack Path Summarization

This feature allows users to view executive summary information for a specific attack path generated using the [Attack Path Query Builder](#). By transforming the visual representation of an attack path into a human language summary, Attack Path Analysis provides an option for less technical users to ingest the data in a different way. Additionally, users can easily share this summary with colleagues to easily highlight attack paths that need their attention.

**Public-facing app exploited to access and expose cloud storage** AI

An attacker initially gains access to tenboneresearch.com by exploiting a public-facing web application vulnerability (T1190). Once inside, they leverage the DNS record tenboneresearch.com to route their way to the load balancer my-app-eg1 and target group vulnerable-web-app-target-group. The attacker then accesses the computer instance aws\_instance.i-0bc32964521c8896b and uses the Cloud Instance Metadata API (T1552.005) to obtain the attached role cg-ec2-role-apacs-resource and associated AWS policies cg-ec2-role-policy-apacs-resource. The attacker executes a malicious file (T1204.002) on the compromised computer aws\_instance.i-0bc32964521c8896b to further infiltrate the system. Finally, they use Cloud Storage Object Discovery (T1619) to gain access to sensitive data stored in tenable-attack-path-close-acl-bucket.

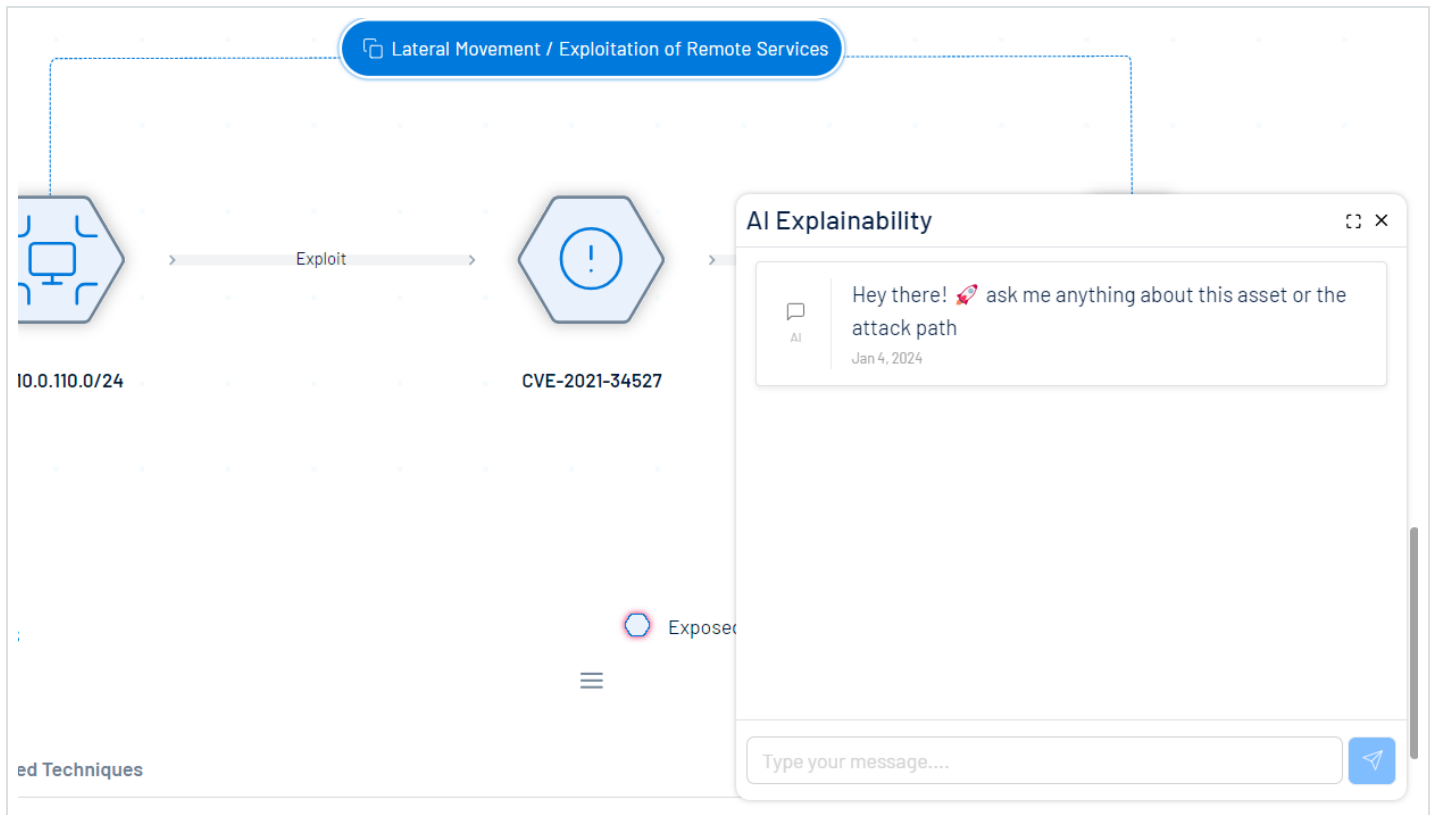
The diagram illustrates an attack path starting from Public Internet, moving through tenboneresearch.com, then to my-app-eg1, vulnerable-web-app-target-group, and finally to aws\_instance.i-0bc32964521c8896b. From there, it branches to cg-ec2-role-apacs-resource and cg-ec2-role-policy-apacs-resource, and finally to tenable-attack-path-close-acl-bucket. Key actions are highlighted in blue boxes: 'Public-facing app exploited', 'Exploited Access / Cloud Instance Metadata API', and 'Discovery / Cloud Storage Object Discovery'.

Tip: Seeing a No insights available message? Click the button to retry.



## AI Explainability

This feature allows users to ask questions about a specific attack path generated using the [Attack Path Query Builder](#) or the [Asset Query Builder](#). Using this search, users can better understand the attack path and its associated risk. Here, you can also gain additional insight into the assets affected by the attack path.



Users can access this chat window by right-clicking a node within the graph view and selecting the Ask AI About This Node menu option.

## Mitigation Guidelines



This feature allows users to obtain practical guidelines for how to mitigate their Attack Path Findings. This feature empowers users to self-service by acting on the recommendations and ultimately eliminating their most critical attack paths.

## Step by Step Mitigation Guide AI ×

Please follow all the below steps to mitigate the risk.

### Step 1: Assess System Requirements

Before implementing Credential Guard, ensure that your hardware and firmware meet the system requirements. Credential Guard requires: - A 64-bit CPU with virtualization extensions (Intel VT-x or AMD-V) - UEFI firmware version 2.3.1 or higher with Secure Boot enabled - TPM 2.0 (optional, but recommended for additional security)

### Step 2: Enable Virtualization in BIOS/UEFI

Ensure that virtualization extensions (Intel VT-x or AMD-V) are enabled in your system's BIOS/UEFI settings.

### Step 3: Enable Secure Boot

Enable Secure Boot in your system's UEFI settings to ensure that only trusted boot components are loaded during the boot process.

### Step 4: Enable Device Guard and Credential Guard

Enable Device Guard and Credential Guard using Group Policy:

1. Open the Group Policy Management Console (GPMC).
2. Navigate to Computer Configuration > Administrative Templates > System > Device Guard.
3. Double-click "Turn on Virtualization Based Security."
4. Select "Enabled."
5. Under "Select Platform Security Level," choose "Secure Boot and DMA Protection."



---

## Sample Questions

---

The following are some sample questions to help you get started with generative AI within Attack Path Analysis. You can ask these questions to any AI-powered search within the Attack Path Analysis interface (for example, AI Explainability.)

**Tip:** You do not need to define the specific asset within your question, because the Attack Path Analysis AI is only connected to the asset node and its related attack path.

- What can you tell me about this asset?
- Does this asset have any exploitable vulnerabilities?
- Is this asset vulnerable to CVE-XXX-XXX? How can I mitigate it?
- How many users have access to it?
- Who are the local administrator users?
- What questions can I ask about this path?
- Can you summarize XXXX (for example, golden ticket, dcsync, lsass memory, etc.) attack?
- Does this device run software with a vulnerability?
- What security controls are installed on this asset?

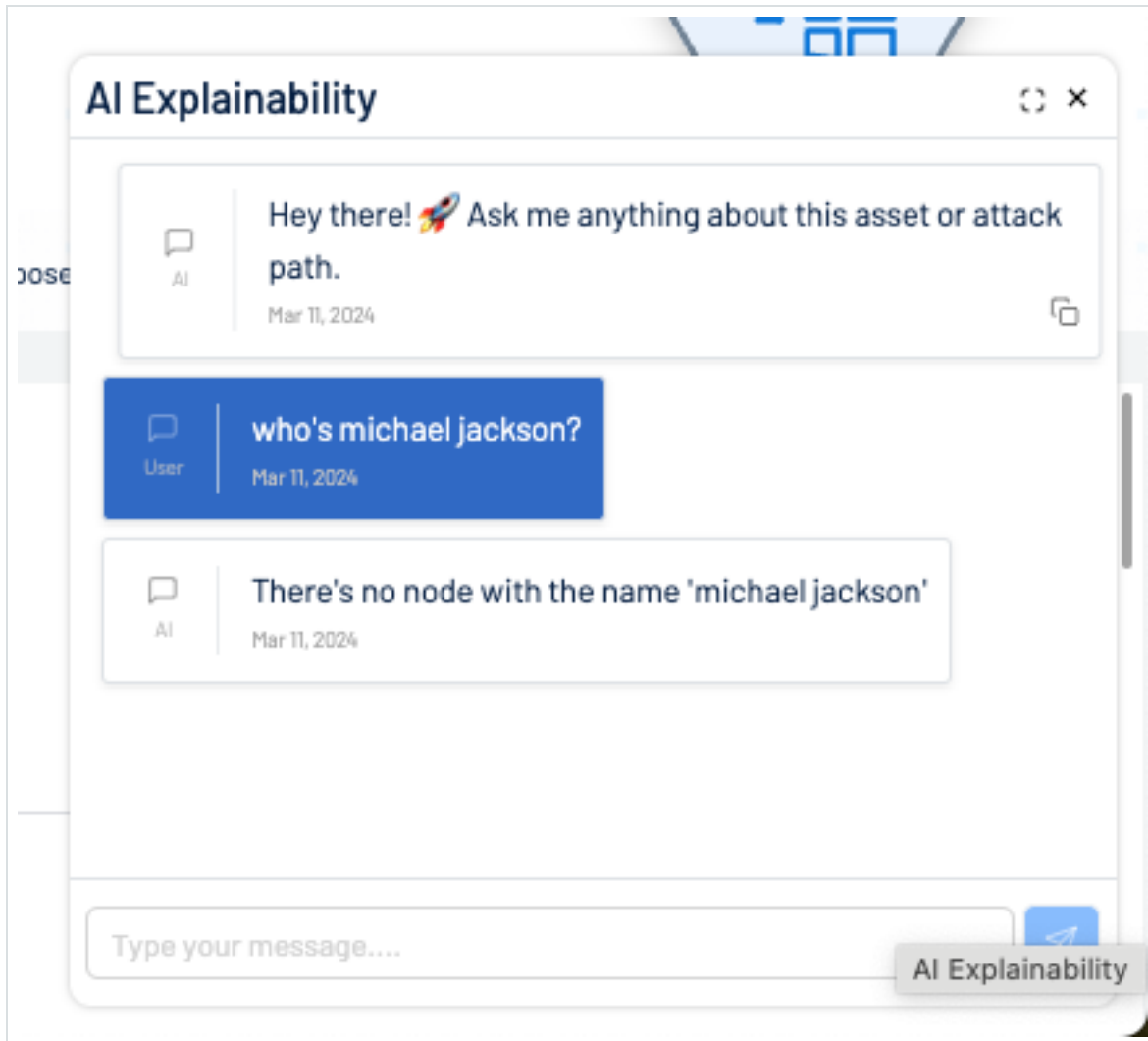
## Limitations

---

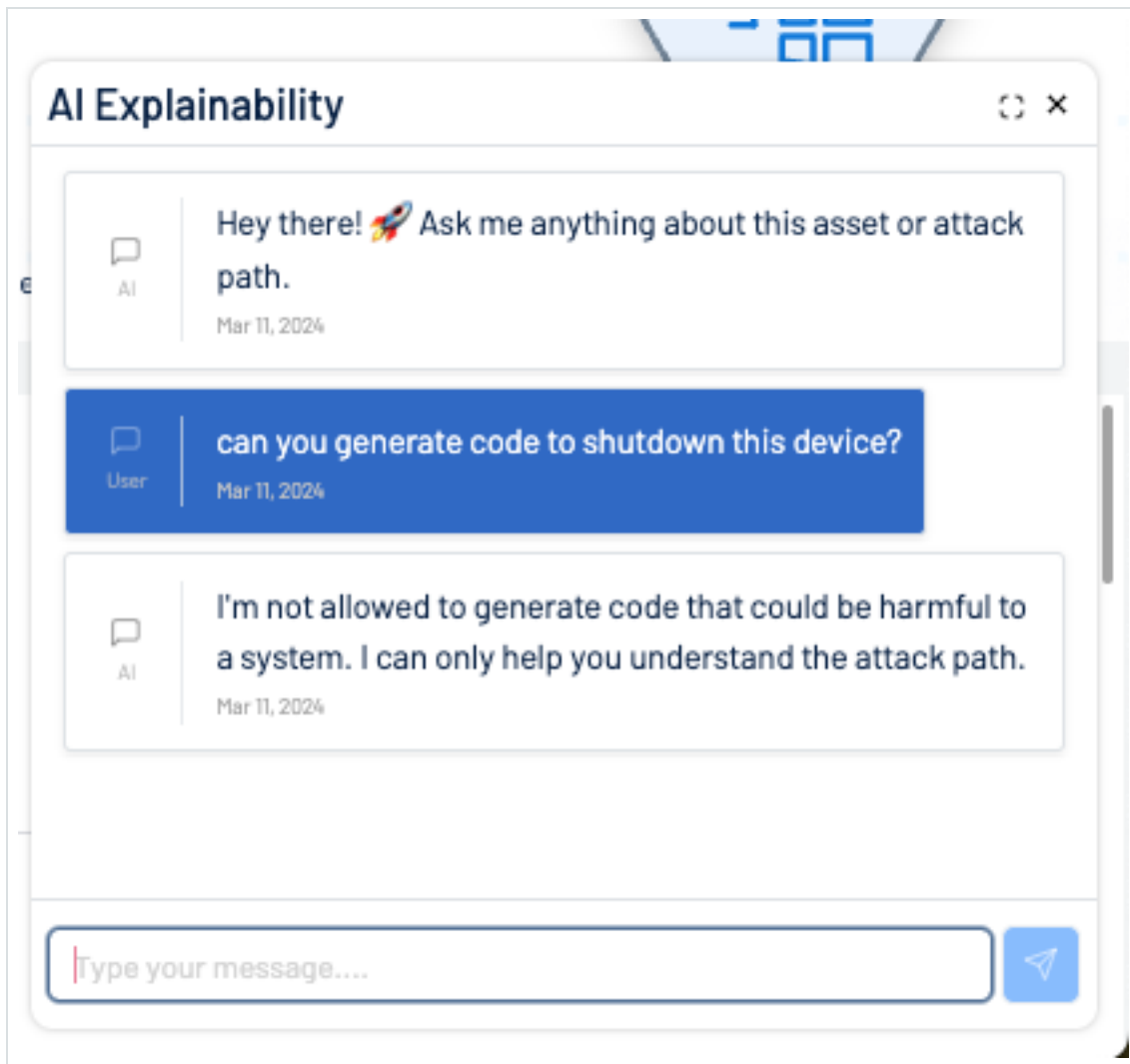
## Context



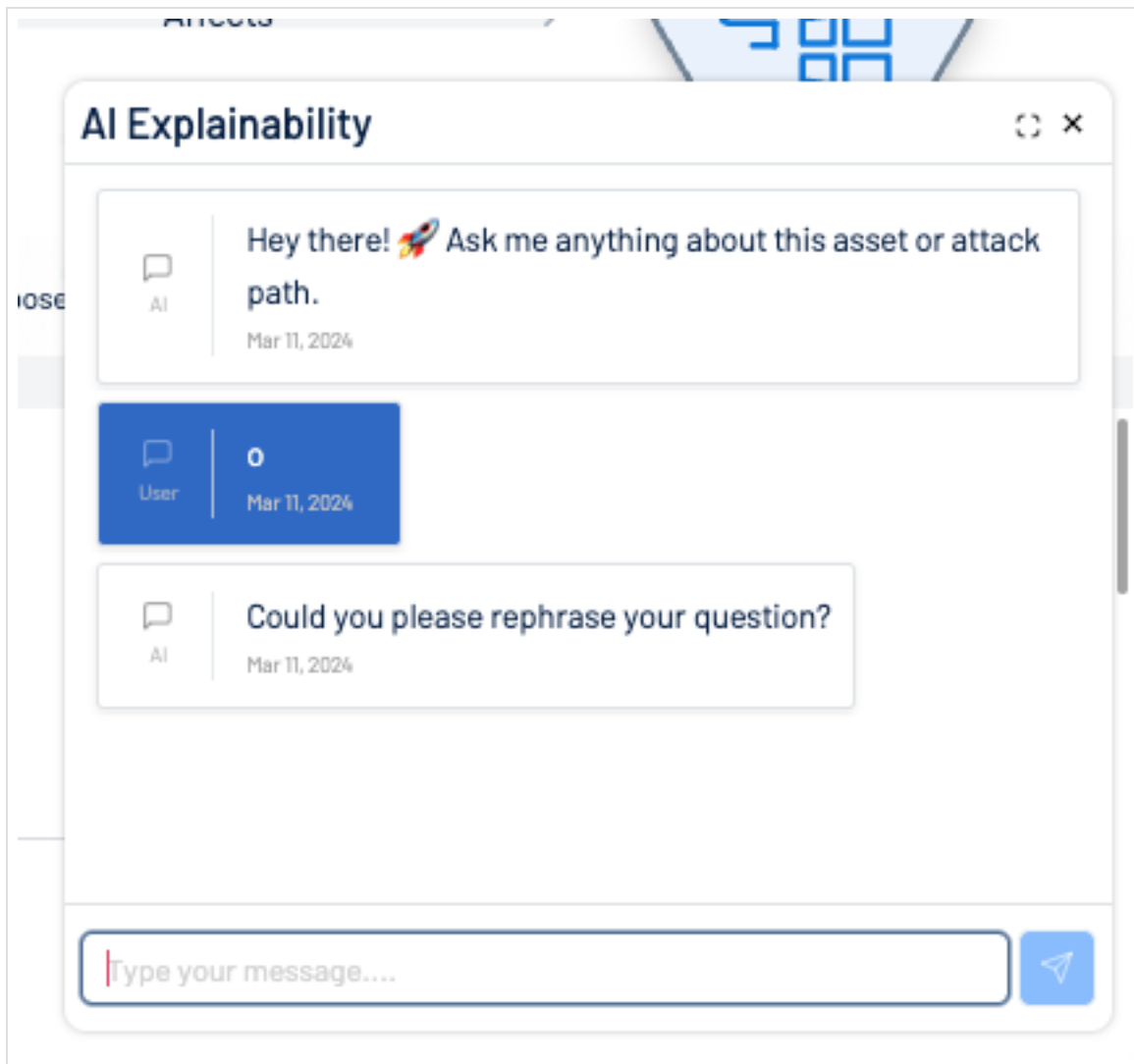
It is important to remember that questions can be asked only in the context of the displayed attack path. Anything not related to the attack path will NOT be answered (for example, who's Michael Jackson?)



This limitation is being done by using prompt engineering to guide the AI engine to rely only on a specific context (in this case, the attack path context). For anything unrelated, the AI is configured not to respond. This helps the AI to avoid the possibility of generating malicious code.



Random text without context might result in random responses or a request to rephrase the question. For example, in the following screenshot, we typed o and pressed "Ask AI." The AI asked us to rephrase the question.



The same question could lead to different answers if asked twice. The context should still be the same, but we shouldn't expect the technology to provide the same response every time. There's a variable in GenAI called temperature which is used to control the diversity or determinism of the AI. High temperatures (closer to 1) provide more creative responses but are less consistent, whereas low temperatures (closer to 0) are more deterministic but less creative. We use a temperature of 0.7, which is considered common in the industry.

## Rate Limit



The AI Assistant can generate up to 50 summaries per minute. If the summaries generated are new (that is, not previously viewed and cached by Attack Path Analysis), you may experience a brief unavailability while the AI generates the content.

## **Quota**

The questions quota for the AI Assistant is set to 100 questions per month. You will not be able to ask more questions once the quota is exceeded. If you need to increase the quota or have any questions about the AI Assistant, contact your CSM.