# Attack Path Analysis FAQ

## Quick Reference Guide

Last Revised: May 18, 2023

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Nessus, Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

# Table of Contents

# Attack Path Analysis FAQ

The following are common questions and answers about Attack Path Analysis.

### What data sources does Attack Path Analysis currently support?

Attack Path Analysis currently supports these Tenable products: Tenable Identity Exposure and Tenable Vulnerability Management.

### What attack techniques does Attack Path Analysis currently support?

For the complete list of attack techniques, see Attack Path Analysis Attack Techniques.

### What is an Attack Path?

An attack path defines a source, a target, and one or more attack techniques leading an attack from the source to the target.

### How does Attack Path Analysis calculate attack paths?

Attack Path Analysis receives data and pairs it with advanced graph analytics, MITRE ATT&CK™, and Open Web Application Security Project® (OWASP) to map the possible attack techniques.

### What triggers a specific Attack Path Analysis technique?

See the prerequisite section of each attack technique in Attack Path Analysis Attack Techniques to find the conditions that must exist for an attack query to run.

### What is a finding shown on the Findings page?

A finding is an attack technique that exists in one or more attack paths leading to one or more critical assets.

### How do you measure the severity of a finding?

The calculation includes mathematical algorithms, to assess the following:

- Likelihood: The number of attack paths using the technique associated with the finding.
- Impact: The number of critical assets that the technique allows an adversary to compromise.

- Method: The tactic associated with the technique such as lateral movement, privilege escalation, etc.
- Path: The starting point and ending point of the technique.

### How does Attack Path Analysis determine if the asset is a Computer, Server, Workstation, or Domain Controller?

Attack Path Analysis determines the asset type as follows:

- Computer, Server, or Workstation – By parsing the operating system type and mapping it to the relevant type to determine if the asset is a Workstation, Server, or Computer.
- Domain Controller – By determining the domain controller through User Account Control.
- Other computer assets– By considering Computer as the base type for unknown assets.

### When I delete an asset from Findings > Asset, how long does it take for Attack Path Analysis to remove that asset?

Attack Path Analysis triggers a data processing job every 30 minutes and it takes up to two hours to update the data.

### What are the different asset types inside the Discover Query Builder?

The **Discover** > **Query Builder** includes the following asset types:

| Asset Types | Definition |
|---|---|
| **CriticalAsset** | • An asset with an Asset Criticality Rating (ACR) equal or greater than 7.<br>• Other Tenable-defined static identifiers, such as domain administrators. |
| **PrivilegedUser** | A user account with administrator access on more than 10 devices. |
| **DomainAdmin** | A user account that is part of a group with full control of the domain including domain administrators, enterprise administrators, and administrators. |
| **GlobalAdministrator** | The global administrator is a user account with access to all admin- |

| | |
|---|---|
| | istrative features in Azure Active Directory. |
| **ServiceAccount** | A special type of non-human privileged account that can execute applications and run automated services, virtual machine instances, and other processes. |
| **Executive** | A human associated user account at the top of the organizational hierarchy, based on manager attribute in Windows-based systems. |