Attack Path Analysis vs. Tenable.ad

Quick Reference Guide

Last Revised: November 09, 2022

Table of Contents

Welcome

This document provides a high-level overview of the main differences between the Attack Path modules in Attack Path Analysis and Tenable.ad.

For more information, see:

- *Attack Path Analysis User Guide*
- *Tenable.ad User Guide*

Overview

Tenable One has two products — Attack Path Analysis and Tenable.ad — that have a product page called **Attack Path**. Both products have similar search functionalities, where you can visualize an attack path by providing a start point and an end point (asset).

This document describes some of the main use cases and differences between the **Attack Path** modules of each product so that you can maximize your experience within the platform.

Differences Between Attack Path Analysis and Tenable.ad

Attack Path Analysis and Tenable.ad overlap mainly on the Active Directory attack techniques. The **Attack Path** modules for Attack Path Analysis and Tenable.ad were designed to achieve different objectives.

Attack Path Analysis highlights exploitable and realistic attack paths, which an attacker would likely choose, whereas Tenable.ad enables thorough exploration and visualization of the underlying security relationships of Active Directory. Therefore, Attack Path Analysis is based on the MITRE ATT&CK™ framework and supports attack techniques across the endpoint, network, and cloud, whereas Tenable.ad focuses on Active Directory security.

When to Use Attack Path Analysis and Tenable.ad

Attack Path Analysis was developed from the attacker point of view and it best suits cybersecurity practitioners such as blue and red teams. For Tenable One users, you can use Attack Path Analysis when you want to search for all probable attack paths within the entire security stack across the Cyber Kill Chain.

Although most Tenable.ad Indicators of Exposure (IoEs) are included in the MITRE ATT&CK™ Framework and also supported in Attack Path Analysis, IT administrators and Active Directory Security Engineers should use Tenable.ad for full context and visibility to the bits and bytes of Active Directory.

Inconsistencies in Attack Path Results

There may be inconsistencies when comparing the **Attack Path** results in Attack Path Analysis and Tenable.ad with the same source and target inputs. Mainly, attack paths in Tenable.ad that do not show up in Attack Path Analysis. The following are some of the probable causes for such behavior:

- **Lack of MITRE ATT&CK™ coverage** – Tenable.ad might support attack primitives, security relationships, or configurations that are not covered in MITRE ATT&CK™ Framework and as a result Tenable.ad results do not match with the attack path results in Attack Path Analysis.
- **Lack of Attack Path Analysis coverage** – Attack Path Analysis parsing capabilities may not be on par with Tenable.ad in some cases. Tenable is aware of the lack of support in several scenarios of special Access Control Entry (ACE) or Access Control List (ACLs) and group policy object (GPO) settings where there may be false positive or false negative.
- **Attack Path is not exploitable** – Attack Path Analysis only shows attack paths that are "believed" to be feasible to exploit. Some security relationships that create a vulnerability in Tenable.ad may not be considered exploitable in Attack Path Analysis. Such scenarios include vulnerabilities that can be mitigated by other controls such as network segmentation or endpoint hardening. It is important to note that such behavior is intended and therefore it is a feature and not a bug.
- **Unsynced data** – Unsynced data can cause inconsistencies between the products. Tenable.ad has its own data collection service and is considered to be real-time. However, Attack Path Analysis relies on a data lake and receives data from various Tenable products. A delay to sync the data between Tenable.ad and Attack Path Analysis is expected.