Identity Security Insights 24.06

What's New Documentation

Release Date – June 04, 2024

BeyondTrust Identity Security Insights safeguards your identity fabric with continuous visibility and sophisticated analysis across all environments. By leveraging both classic and AI/ML techniques, it automatically correlates and contextualizes identity data across on-premises, cloud platforms, SaaS applications, and IdPs. This unified approach allows you to proactively identify and eliminate "true" privileges and paths to privileges before they are compromised, using deep context and integrated workflows and PAM controls.

Release Highlights

Prioritizing threats within Identity Security Insights just got easier with built-in filters.

We know that creating your own filters in complex datasets can be time-consuming. That's why we have introduced built-in filters curated by our security experts.

These out-of-the-box filters are available across all views such as identities, accounts, detections, and recommendations to help you identify your greatest risks, without needing to deep dive into datasets and attributes. Simply choose a filter built on a pre-defined criteria to quickly pinpoint what needs your attention most. For example, instantly identify accounts with paths to privileges that attackers could exploit or see all high-privilege accounts under brute force attack and dormant and not managed by Password Safe.

While you can still manually create advanced filters to meet your specific needs, these built-in filters enable you to uncover critical threats quickly, regardless of your expertise in creating filters, for a more proactive approach.

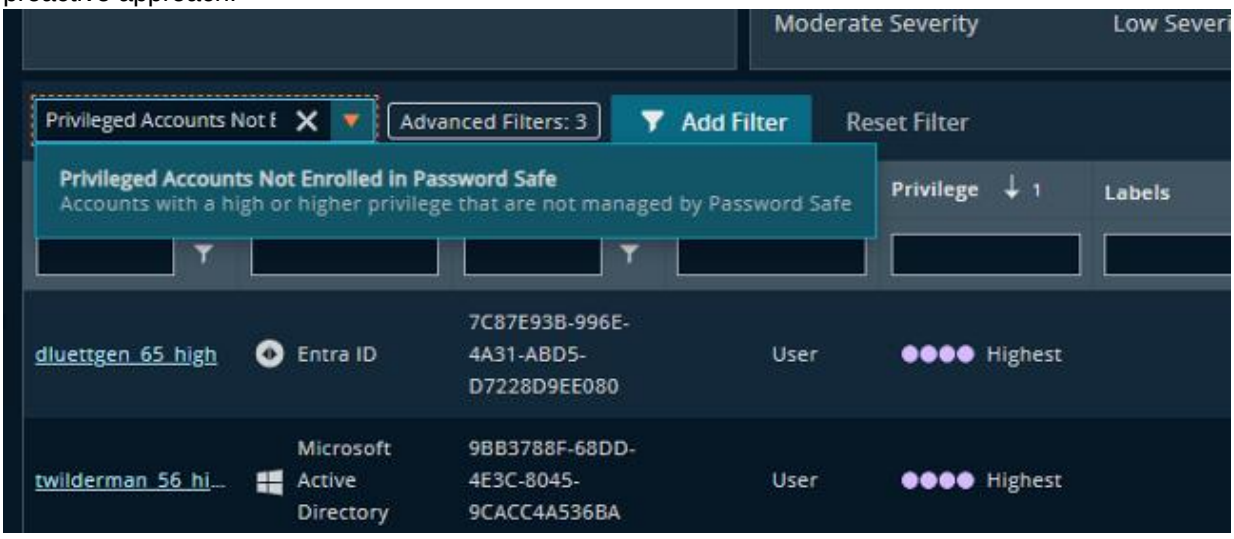

Figure 2 – Built-in filters

New detections, recommendations, and visibility into your Active Directory environment.

Identity Security Insights now uncovers potential misconfigurations in your Certificate Templates and Certificate Authority certificates. These misconfigurations could be exploited by attackers using techniques like ESC1 and ESC4 to escalate privileges and gain unauthorized access to your environment.

Active Directory Certificate Services (ADCS), Microsoft's PKI infrastructure, plays a crucial role in issuing and managing certificates used in secure communication and authentication protocols. Misconfigurations in ADCS can be abused by attackers to escalate privileges within the Active Directory domain, potentially obtaining roles like Domain Administrator and authenticating as a privileged user to compromise your entire interconnected IT environment.

By proactively identifying and addressing ADCS misconfigurations, you can strengthen your certificate management and ensure the integrity of your Active Directory environment.

About BeyondTrust

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

BeyondTrust protects all privileged identities, access, and endpoints across your IT environment from security threats, while creating a superior user experience and operational efficiencies. With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 75 of the Fortune 100, and a global partner network. Learn more at www.beyondtrust.com.