Identity Security Insights 23.10

What's New Documentation

Release Date – October 03, 2023

BeyondTrust Identity Security Insights is a powerful solution that helps you protect your organization from identity-driven threats. It leverages machine learning to automatically correlate and contextualize your identity data across on-premises and multicloud environments. This enables you to gain a holistic understanding of your unique identity security posture, and helps you to identify, detect, and respond to threats quickly and effectively.

With Identity Security Insights, your teams have a single source of truth to:

- Identify your greatest identity-driven risks
- Gain proactive recommendations specifically curated for your unique environment
- Detect threats such as lateral movement and privilege escalation

Release Highlights

Identity Security Insights is now integrated with Splunk.

Security Information and Event Management, or SIEM, is a solution that allows organizations to collect and analyze a broad range of log and event data to quickly locate and mitigate potential security threats. Identity Security Insights can help SIEM users to improve detection and incident response with additional identity-driven context and information.

BeyondTrust Identity Security Insights is now integrated with Splunk. When this integration is enabled on your selected Splunk SIEM, BeyondTrust will immediately deliver any new detections and recommendations to your Splunk so your security teams can quickly investigate and act on the findings.

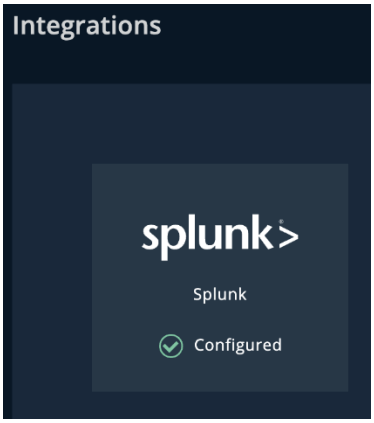

Figure 1 – Splunk connector available to be configured

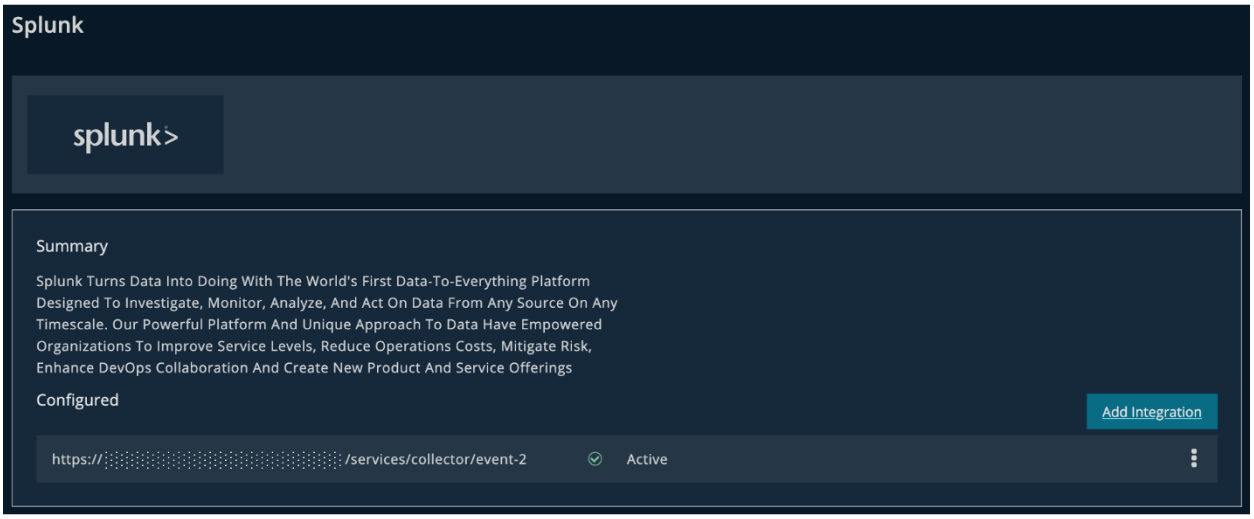

Figure 2 – Integration detail page for Splunk

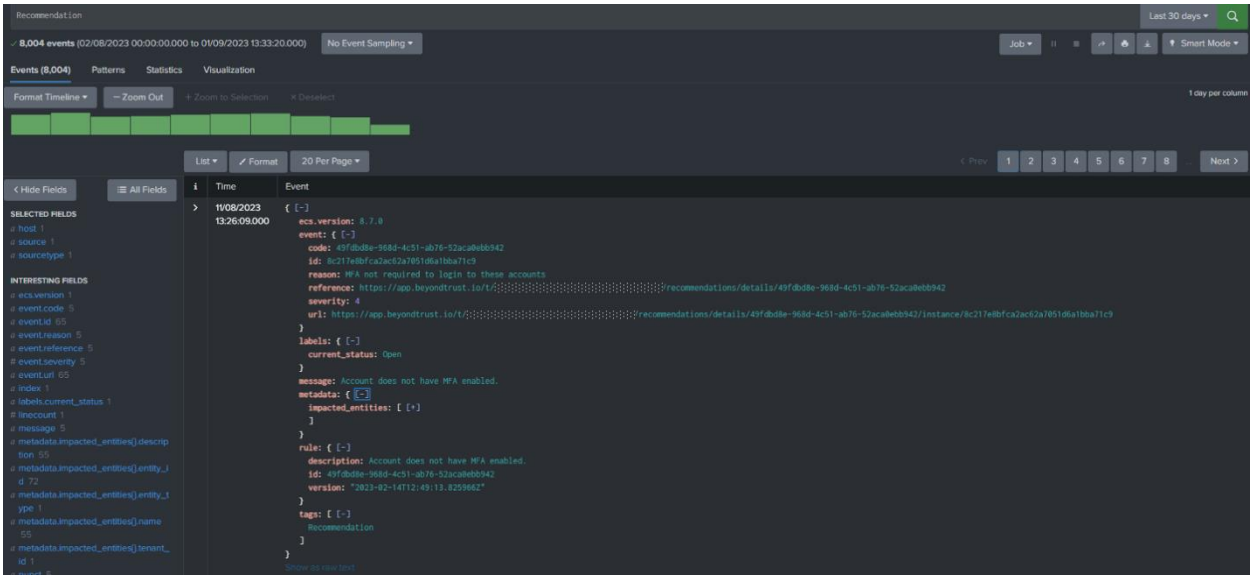

Figure 3 – Example of ECS-formatted Incident forwarded by BeyondTrust Identity Security Insights

New account labels help you filter accounts by key account characteristics.

New account labels help you filter accounts by key characteristics in your reports and dashboards, e.g., is the account dormant? does it have MFA enabled? Is the MFA strong? etc. The new labels are available in all account views. This enhancement can help your teams save time and minimize manual work, increasing productivity and facilitating better security outcomes.

Link available to download on-premises Microsoft Active Directory connector.

The Microsoft Active Directory connector now includes a download link to the installer for the on-premises collector. The download link is available from the connector creation screen as well as the settings section of an already configured connector. Your teams can easily access the link from their workflows for a seamless download, improving the user experience.

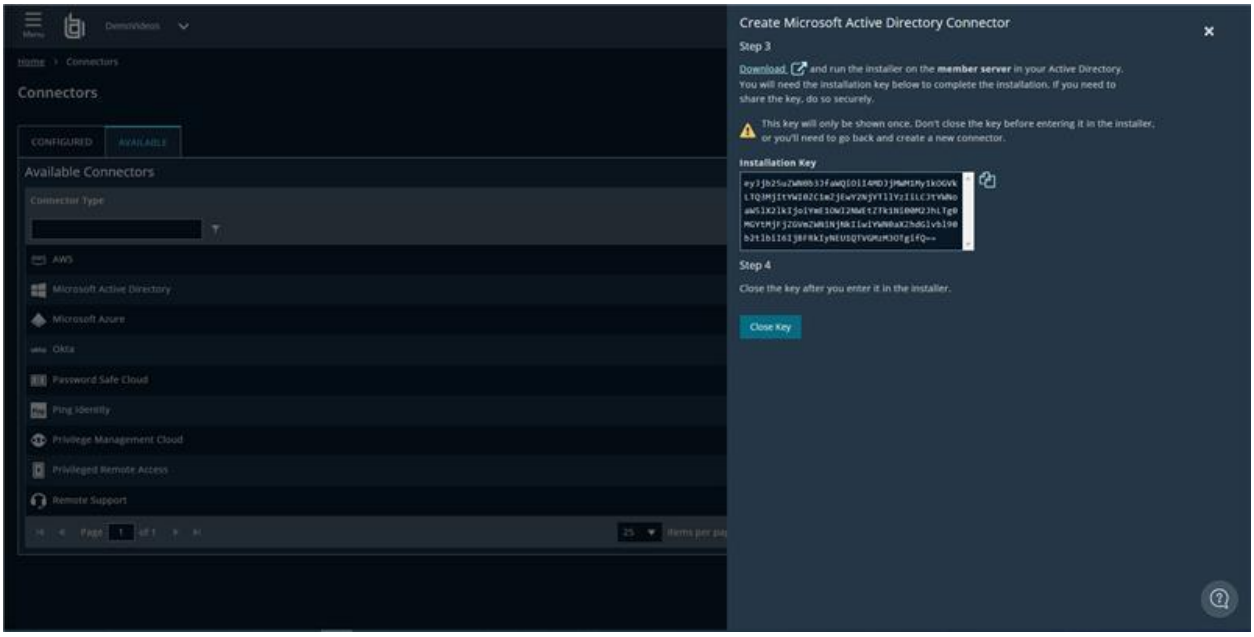

Figure 4 – Example of Active Directory connector download link

Auto-update now enabled for on-premises Active Directory collector.

BeyondTrust is committed to continually making enhancements that improve productivity and ease of use of our products. The on-premises Active Directory collector version 1.5.1 now supports auto-update. This means that the on-premises service will automatically keep itself up to date without the need for user interaction.

New Detections and Recommendations

BeyondTrust consistently introduces new detections and recommendations that empower our customers in countering emerging threats and proactively addressing hygiene concerns. In this latest release cycle, we've rolled out a new set of recommendations focused on preventing privilege escalation attacks. For a complete list of new detection and recommendations in this release, please refer to the release notes.

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.