# Threat Management Platform

## Components: UEBA

# CYBOT UEBA

UEBA (User and Entity Behavior Analytics) detects threats by identifying deviations from normal activity within an organization's IT environment. While leading solutions often limit UEBA capabilities to EDR data, Cybot UEBA sets itself apart by ingesting all rich data. This comprehensive approach enables Cybot UEBA to provide detailed user profiles, offering a holistic view of the entity's activities from inception, surpassing the limitations of traditional UEBA implementations.
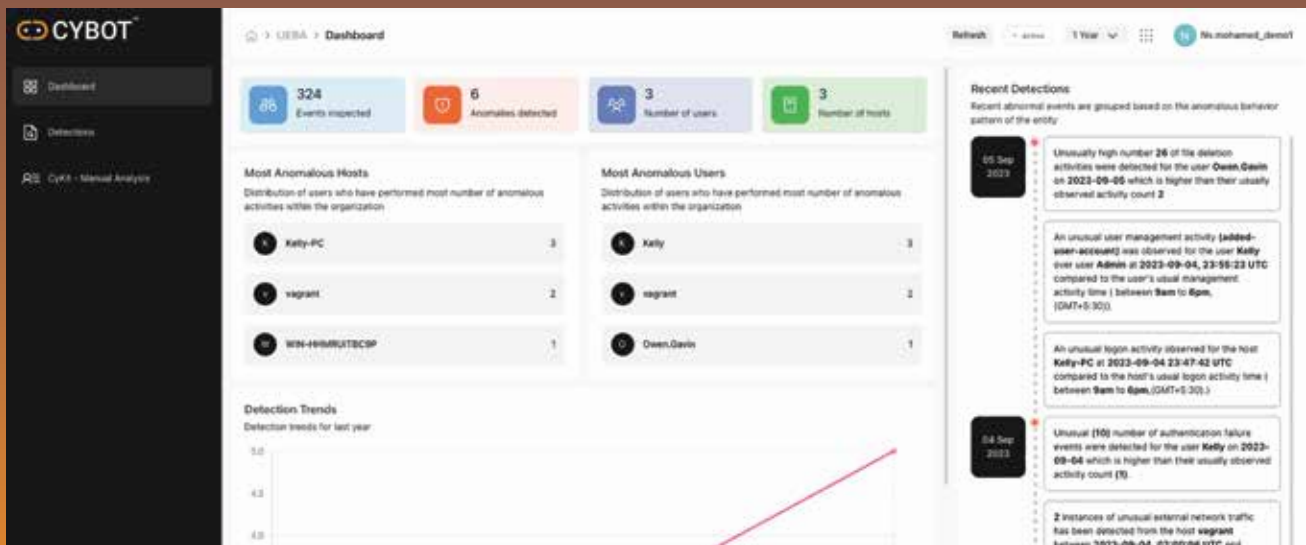


- Real-time display of top anomalous hosts, users, event summaries, and anomalies detected. The dashboard showcases detection trends and recent abnormal events, grouped based on anomalous behavior patterns.

- Explore the Most Anomalous Hosts and Users effortlessly. Select entities directly from the dashboard to instantly view detailed detections, providing a user-friendly feature for swift response to potential threats.

- Instantly view and understand recent abnormal events, grouped by entity behavior patterns for quick threat identification and proactive response.
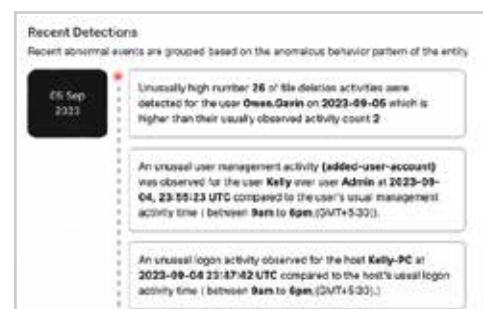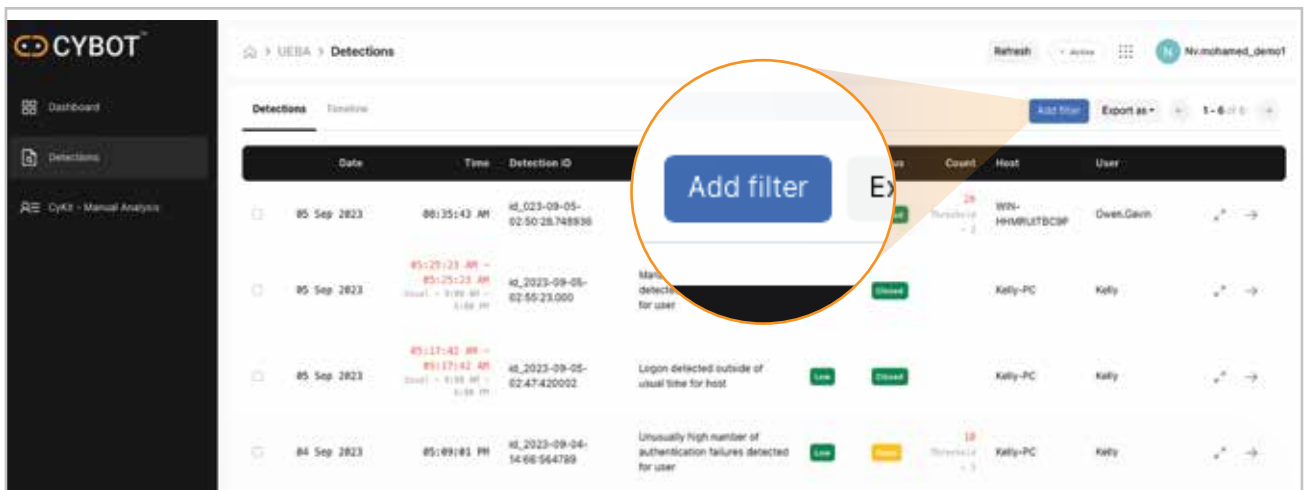
✓ Your go-to destination for comprehensive detection details. Drill down into each event for in-depth investigation, unravel anomalies, and enhance your understanding of potential threats.

✓ Utilize **filters** to view the timeline activity of users or hosts, export results, and drill down for manual analysis. Perform in-depth investigation using the detection summary and anomalies detected.
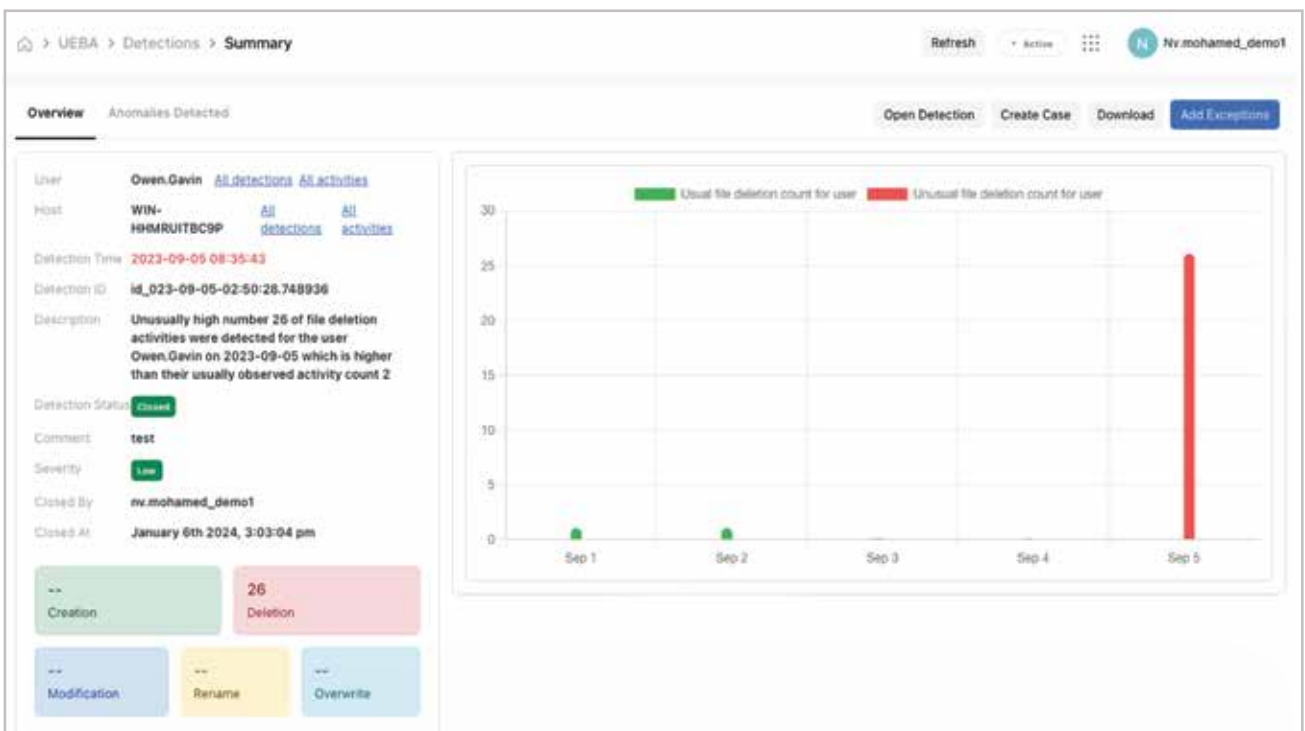


✓ UEBA Detection Summary provides a concise overview of detections, displaying deviations with clarity. Easy-to-understand presentation of events and timelines. Interactive display for seamless navigation to all events associated with the detection, ensuring a user-friendly experience.

Open Detection   Create Case   Download   Add Exceptions
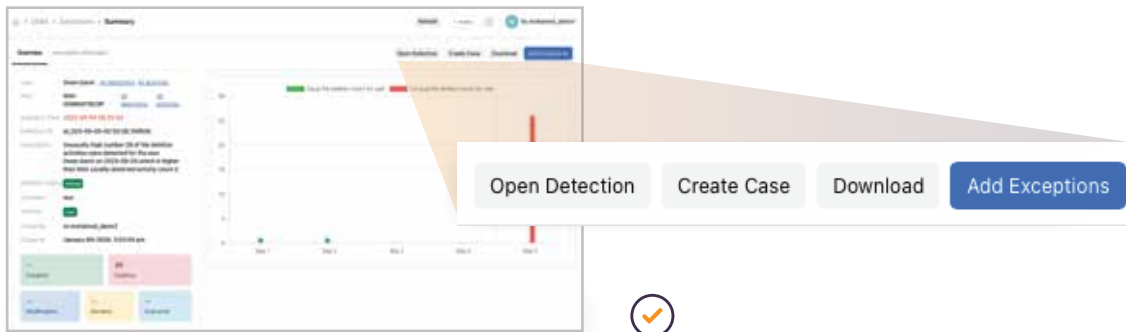
✓ Close the alert for validated activities; submit a ticket swiftly for in-depth investigation, ensuring precise threat detection.

✓ Incorporate exceptions for validated activities to minimize false positives. Ensure precise threat detection and reduce unnecessary alerts.
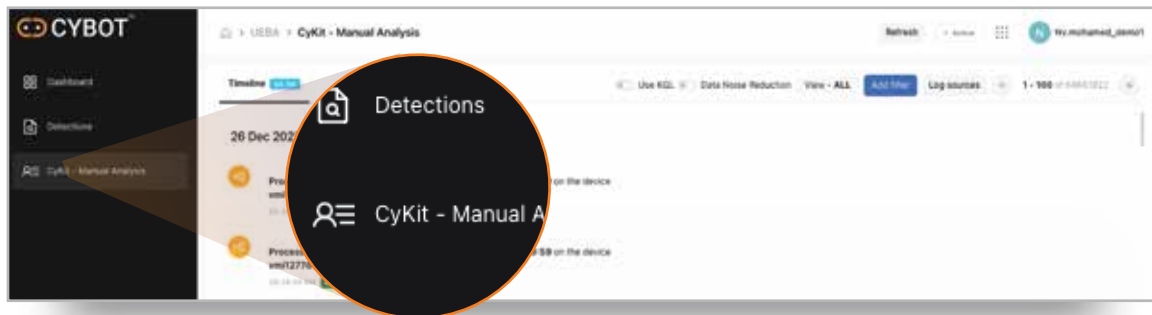


✓ Explore defaulters' timelines with precision by excluding system, user, and computer accounts. Utilize our unique log collection method, capable of filtering the timeline based on diverse log sources from almost every corner of your environment. Enhance analysis and gain insightful, refined data.

## Notice

This document contains information about the proprietary property of ActiveBytes Innovations. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of ActiveBytes Innovations.

Nothing in this document constitutes a guarantee, warranty, or license, express or implied. ActiveBytes Innovations disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to Fitness for a particular purpose; merchantability; not infringement of intellectual property or other rights of any third party or of ActiveBytes Innovations; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technology discussed herein and is advised to seek the advice of competent legal counsel, without obligation of ActiveBytes Innovations.

ActiveBytes Innovations retains the right to make changes to this document at any time, without notice. ActiveBytes Innovations makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein.

## Copyright

## Trademarks

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owner's benefit, without any intent to infringe.

# Contact Us

## ActiveBytes Innovations

Sharjah Media City, Sharjah, UAE, Dubai, UAE +971 505676727
www.active-bytes.com