



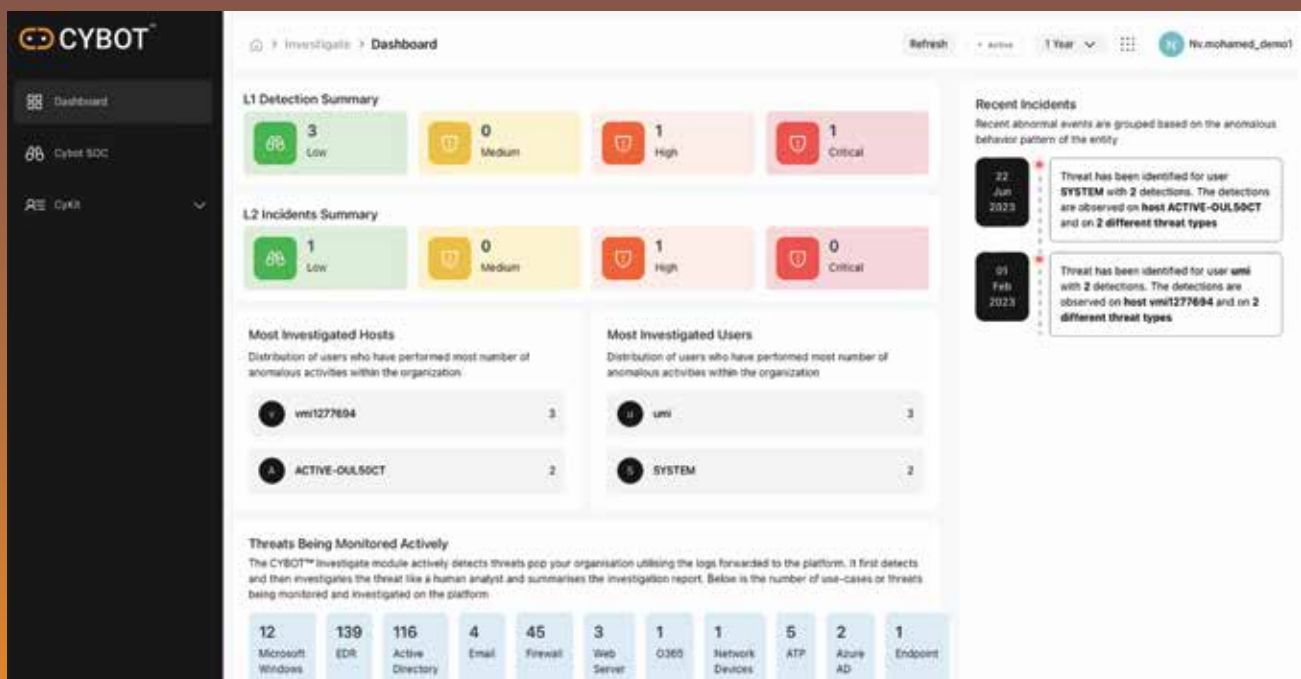
Threat Management Platform

Components: Investigate

Component

CYBOT INVESTIGATE

CYBOT's core threat detection and response revolve around the Investigate component. When a use case triggers, it's instantly available in Investigate. CYBOT automates initial investigations, performing essential checks usually done by analysts. Analysts get a comprehensive report, including a threat score, recommended actions, and an incident response plan.



- ✓ The CYBOT **Investigate Component Dashboard** provides a comprehensive cybersecurity overview of all the detections and incidents in your organization.



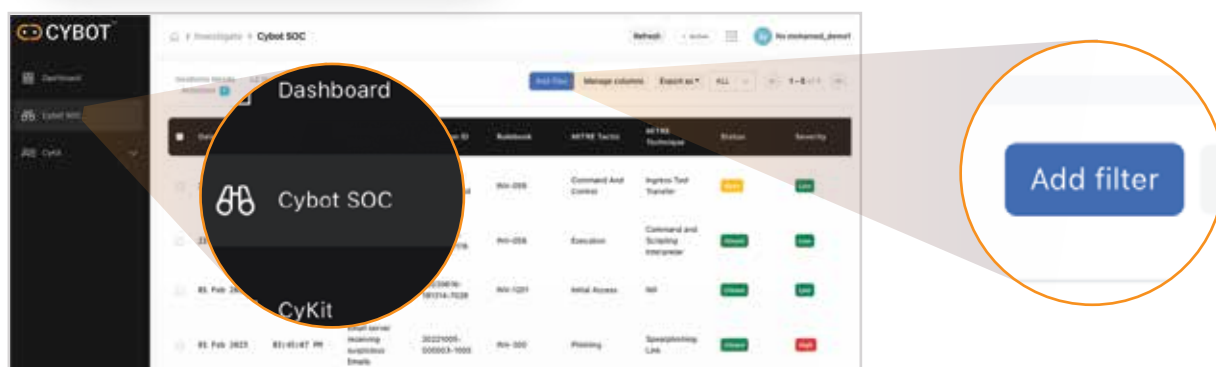
- ✓ The dashboard separates **L1 and L2 detections**, offering high-level info on severity-sorted alerts. Users can quickly spot the top 5 hosts and users linked to detections and incidents.

Most Investigated Hosts		Most Investigated Users	
Distribution of users who have performed most number of anomalous activities within the organization		Distribution of users who have performed most number of anomalous activities within the organization	
vmi1277694	3	umi	3
ACTIVE-OUTS0CT	2	SYSTEM	2

- ✓ Directly select hosts or users for detailed info on detections and incidents, ensuring responsive, accessible design for better understanding across devices.

Recent Incidents	
Recent abnormal events are grouped based on the anomalous behavior pattern of the entity	
22 Jun 2023	Threat has been identified for user SYSTEM with 2 detections. The detections are observed on host ACTIVE-OUTS0CT and on 2 different threat types
01 Feb 2023	Threat has been identified for user umi with 2 detections. The detections are observed on host vmi1277694 and on 2 different threat types

- ✓ Highlights recent detections, displays the total ongoing investigations, and offers a user-friendly interface for easy navigation.

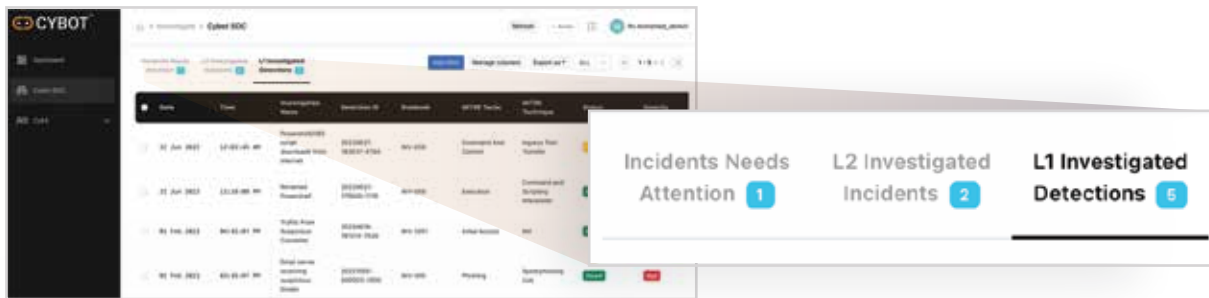


- ✓ Leverage CYBOT's Investigate component, an advanced feature that automatically analyzes triggered alerts, providing comprehensive summaries and recommendations to the security team. This functionality offers a high-level overview of alert types, noisy hosts, and users, reducing alert fatigue, improving investigation quality, and minimizing errors.

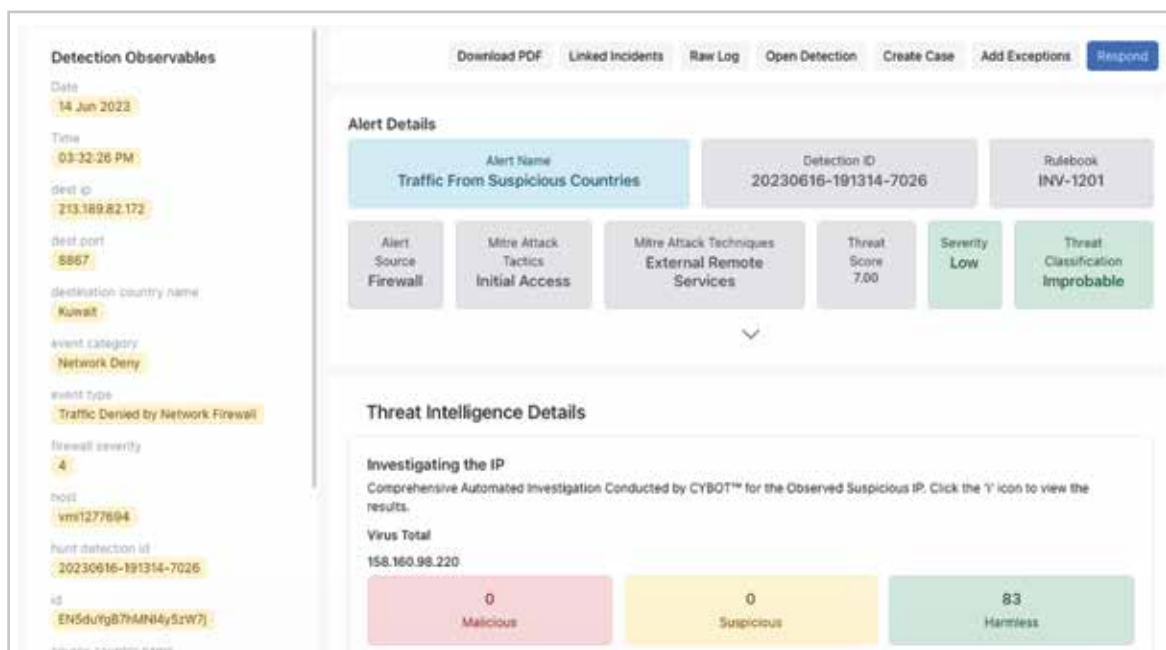
- ✓ **Advanced Filtering:**
Utilize advanced filters to precisely refine your data, with the added convenience of saving and loading filters for future use.

- ✓ **Customizable Display:**
Enhance your viewing experience by tailoring the display to your needs. Choose the relevant columns for a more focused and efficient presentation.

- ✓ **Integrated Reporting:**
Attach and enrich your incident reports effortlessly by exporting results as needed, streamlining the documentation process for comprehensive analysis.



- ✓ The Investigate component automates investigations at both L1 and L2 levels, transforming into a virtual SOC with automated examination, analysis, categorization, and threat scoring. This ensures rapid delivery of detections to the SOC team for prompt responses.



- ✓ Access each detection, view alert artifacts, and benefit from automated investigations. Cybot now handles the SOC analyst's role, swiftly analysing alerts and empowering quick decision-making.



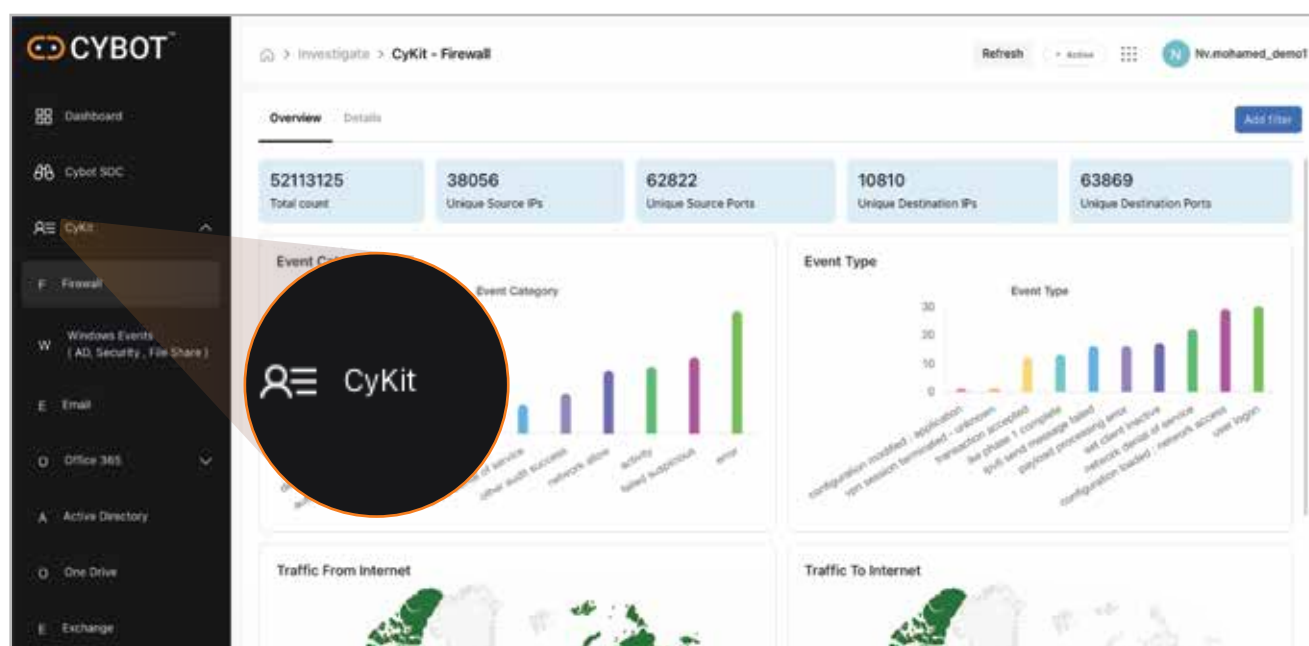
About the Incident Incident ID: id_0002 Incident name: Email server receiving suspicious Emails, Traffic to Suspicious Websites Status: Closed Comment: <p>test</p> Closure code: False Positive - Data Error Date: 01 Feb 2023 Time: 03:50:07 PM Incident summary: This detection involves 2 indicators linked by a common user name umi, observed between 2023-02-01T10:20:07 and 2023-02-01T10:30:00. The overall severity assigned is High. Upon analysis, we label it as a Phishing. Classification: Beneign True Positive Severity: High Threat Score: 75.000 Tags: Exfiltration Phishing		Detections Download Manage Columns Create Case			
Date	Time	Investigation Name	Detection ID	Rulebook	MITRE Tactic
01 Feb 2023	03:45:07 PM	Email server receiving suspicious Emails	20221005-000003-1000	INV-300	Phishing
01 Feb 2023	03:45:07 PM	Traffic to Suspicious Websites	20221005-000003-1002	INV-301	Exfiltration



Incidents are automatically classified, assigned a threat score, and note preparation is fully automated, presenting analysts with incidents requiring minimal investigation.



Automated merging of qualified, multistage detections into incidents streamlines the handover to CYBOT L2 for in-depth investigation.



Distinguishing itself from other solutions, our Investigate component introduces the innovative CyKit feature.



This unique capability provides the internal security team with replicas of essential security solutions including firewalls, ATP, and Office 365.



Analysts are empowered to perform manual analyses using a user-friendly interface that convincingly simulates direct access to these critical security solutions, enhancing the depth and accuracy of investigations.

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

Copyright © ActiveBytes Innovations Information Technology Network LLC


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

A decorative graphic at the bottom of the page consisting of a network of thin grey lines and small circles, resembling a circuit board or data network, extending across the width of the page.