CYBOT™

www.active-bytes.com

Threat Management Platform

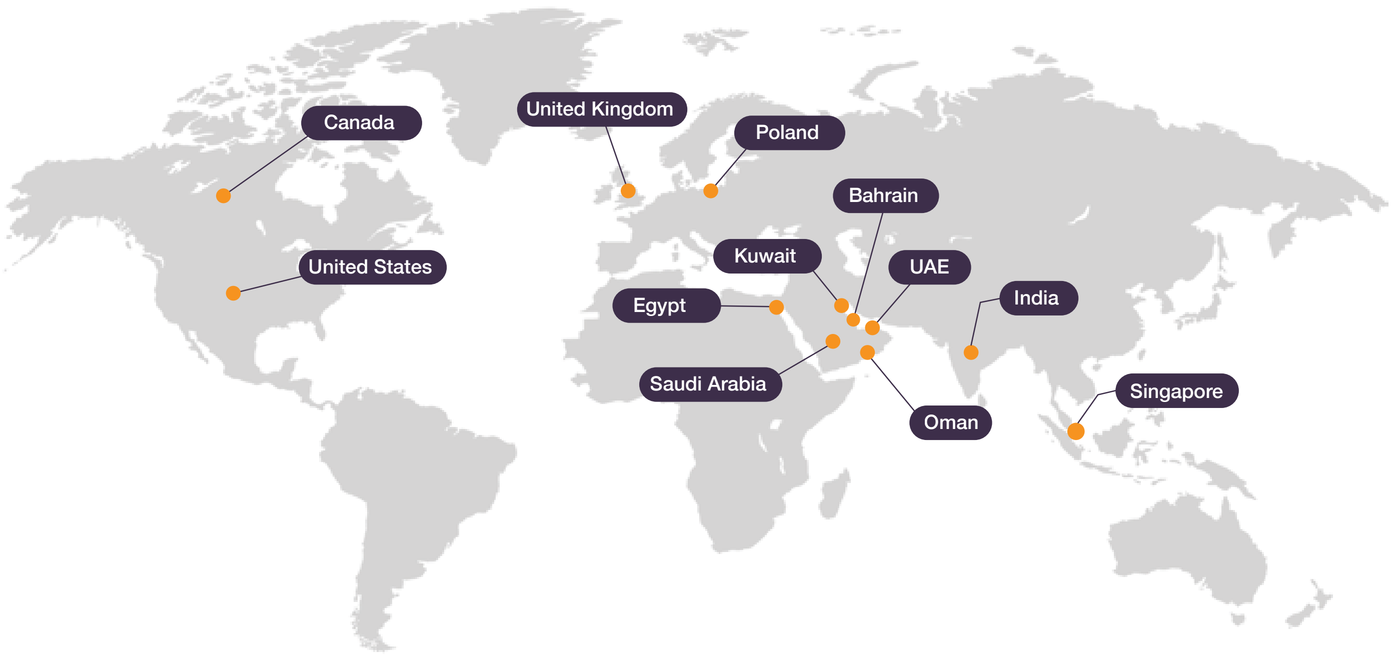
CONTENTS

Who We Are

Building Cyber-resilient Organizations

ActiveBytes Innovations has a proven track record of executing successful Information Security Projects for numerous large enterprises across different locations around the globe.

We proudly serve clients from multiple industry sectors, demonstrating our ability to adapt and provide tailored solutions to diverse business environments. Here are a few notable examples showcasing our expertise across various industries:



Safeguarding Diverse Industry Sectors With State of the Art Managed Security Service

Financial

Banking

Government

Oil & Gas

Real Estate & Hospitality

Logistics & Supply Chain

Healthcare

Aviation

Our Range of Services

IT Security Service:

ActiveBytes Innovations delivers comprehensive IT Security solutions, including risk assessment, threat detection, and incident response, safeguarding clients' digital assets and ensuring business continuity.

Compliance:

ActiveBytes Innovations' Compliance services help clients meet regulatory requirements, manage data protection, privacy, and incident response, ensuring a strong security posture and continuous improvement.

Governance:

ActiveBytes Innovations' Governance services establish effective security management, compliance with regulations, and swift incident response, safeguarding digital assets and ensuring exceptional results

CYBOT - Threat Management Platform

CYBOT, our Threat Management Platform, is an essential cybersecurity service designed to enhance your defense strategies. This user-friendly platform utilizes advanced technology to detect and neutralize threats in real time. Offering simplicity in threat detection and management, it provides actionable insights for swift response.

Risk:

Our Risk services proactively identify and manage security threats through comprehensive risk assessments, threat intelligence, and robust incident response strategies for secure infrastructure and data protection.

Managed Security Services:

Our MSOC is your cybersecurity ally, providing constant threat detection, swift incident response, and cutting-edge CTI. We excel in proactive threat hunting, vigilant security monitoring, robust vulnerability management, and user-friendly endpoint protection. Tailored solutions ensure resilience against evolving threats, fortifying your organization with a personalized touch for proactive cybersecurity.

Active Sense Awareness:

Immerse your team in real-world cybersecurity scenarios with our training platform. Through simulations, exercises, and hands-on training, we elevate your organization's preparedness for cyber threats. Experience the practical side of cybersecurity, ensuring your teams are adept at handling evolving challenges and enhancing their skills to safeguard your organization effectively.

Transforming Cyber Defence with Our Unique Approach

> We lead in cybersecurity with an unmatched approach to security operations, providing comprehensive support beyond periodic reports and alerts. True peace of mind for organizations, knowing their security matters are in capable hands.

ActiveBytes Innovation: Transforming Security Operations

Our unique approach provides comprehensive services, delivering practical insights into incidents and a well-rounded perspective tailored to your organization's needs.

State of the art Technologies for Optimum Security

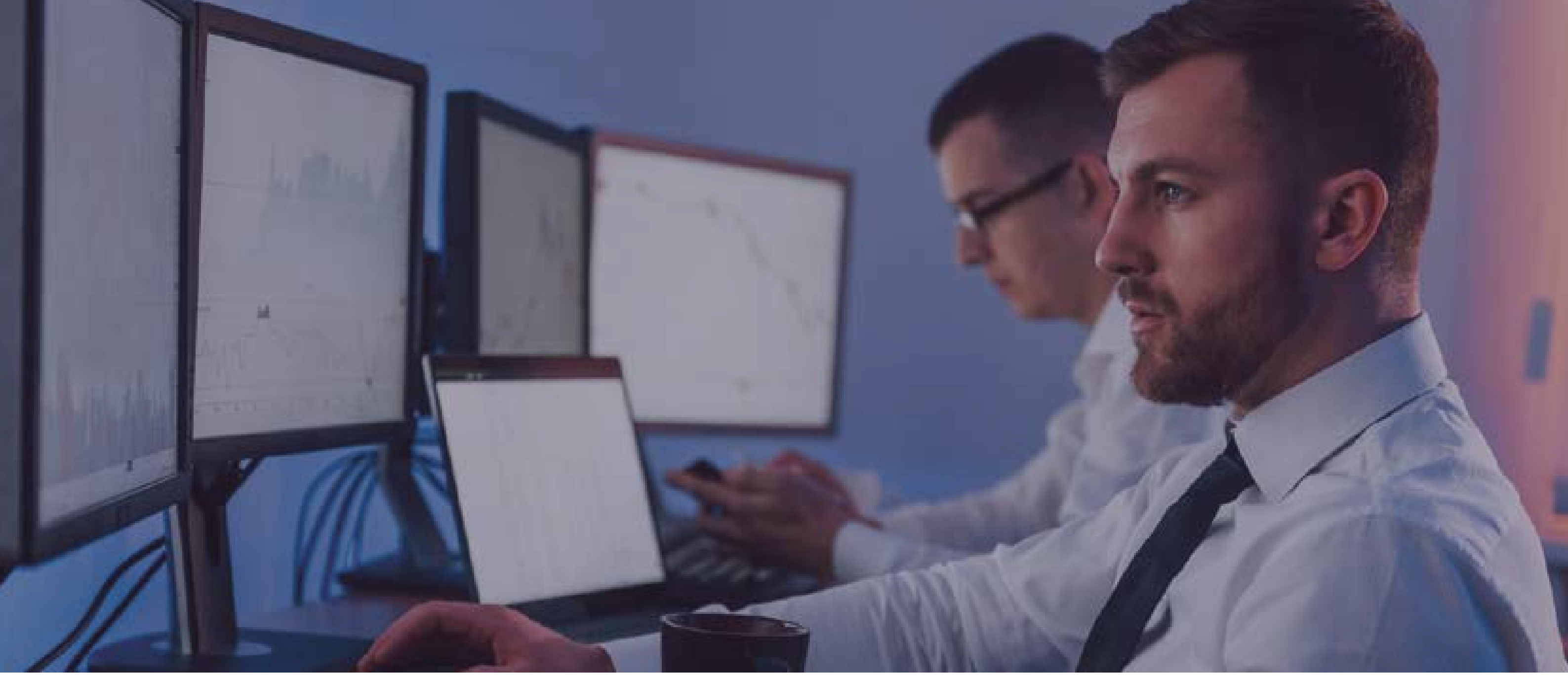
Utilizing state-of-the-art products built upon powerful open-source solutions, our Analytical Engine offers robust reporting, alerting, and log enrichment. Compatibility across log formats and machine learning-powered anomaly detection ensures faster search and response times.

Our Unique Formula: Effective Outcome-Based Approach

Drawing from extensive cybersecurity experience, our formula maximizes automation and accuracy. Focusing on real incidents, we minimize false positives, aligning risk priorities with your organization's goals.

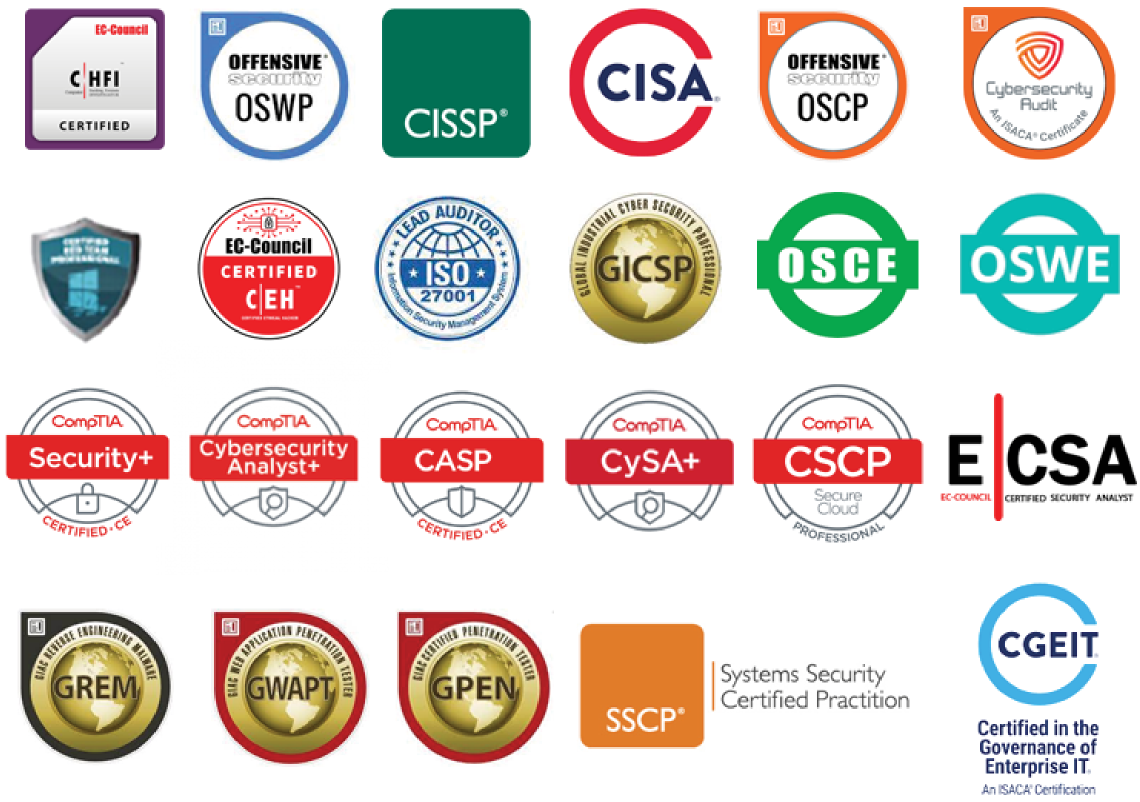
Outstanding support and personalized services

Understanding your unique needs, we offer services like real incident reporting, ongoing security assessments, expert audit assistance, dark web breach monitoring, vendor security verification, and prioritized vulnerability lists.



Our Extraordinary Team of Cybersecurity Experts!

- Cybersecurity experts with deep technical knowledge
- Industry-recognized security-certified team for new confidence and protection


EC-Council C|HFI CERTIFIED
OFFENSIVE security OSWP
CISSP
CISA
OFFENSIVE security OSCP
Cybersecurity Audit An ISACA Certificate
EC-Council CERTIFIED C|EH
LEAD AUDITOR ISO 27001 Information Security Management System
GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL GICSP
OSCE
OSWE
CompTIA Security+ CERTIFIED · CE
CompTIA Cybersecurity Analyst+
CompTIA CASP CERTIFIED · CE
CompTIA CySA+
CompTIA CSCP Secure Cloud PROFESSIONAL
E|CSA EC-COUNCIL CERTIFIED SECURITY ANALYST
GIAC REVERSE ENGINEERING MALWARE GREM
GIAC WEB APPLICATION PENETRATION TESTER GWAPT
GIAC CERTIFIED PENETRATION TESTER GPEN
SSCP Systems Security Certified Practition
CGEIT Certified in the Governance of Enterprise IT An ISACA Certification

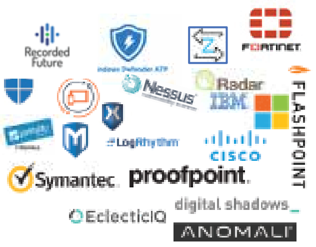
CYBOT™

Threat Management Platform

The CYBOT Difference

We Collect data from Everywhere.

We enable you
Irrespective of the products you have.



We do ingest the data to CYBOT

No Limits of PS Efforts
If the products you have a way to collect data, we collect, process and make use of it in CYBOT

We store the unified data in our Data Repository with no limits.

No Limits

- On Events per second
- On GB Per day
- Cloud or On-prem
- On Retention, You can have a single node with minimal, or a cluster of nodes to have high availability and longer retention

Unified Security Management Platform

In today's enterprise landscape, the volume and complexity of logs generated from network, endpoints, and servers can be overwhelming. Valuable data often goes unattended, leaving critical insights untapped. ActiveBytes Innovations addresses this challenge with CYBOT™, a groundbreaking solution that harnesses the power of intelligent automated workflows.

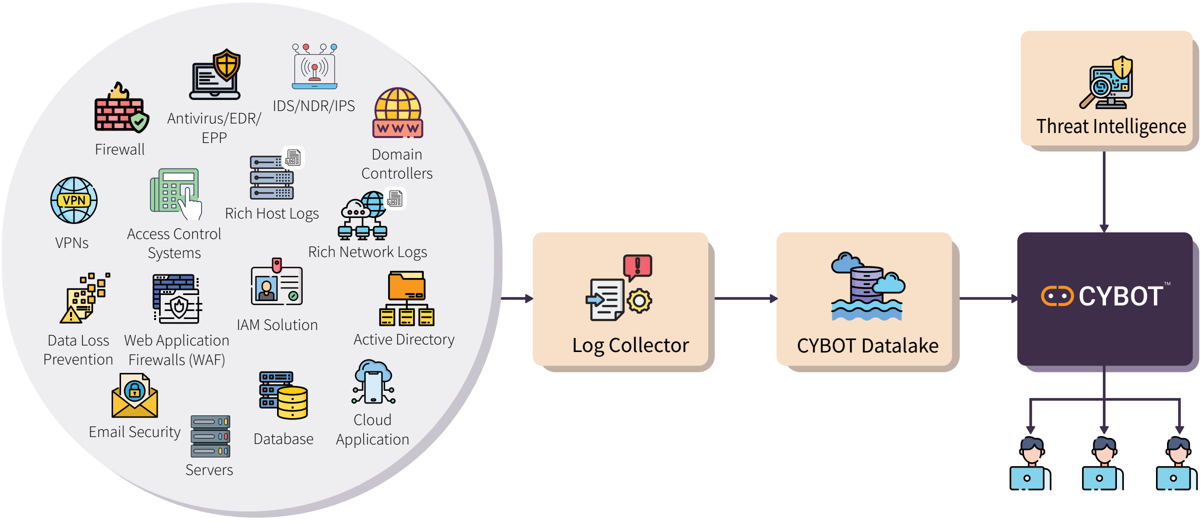
NO EPS

Event Per Second

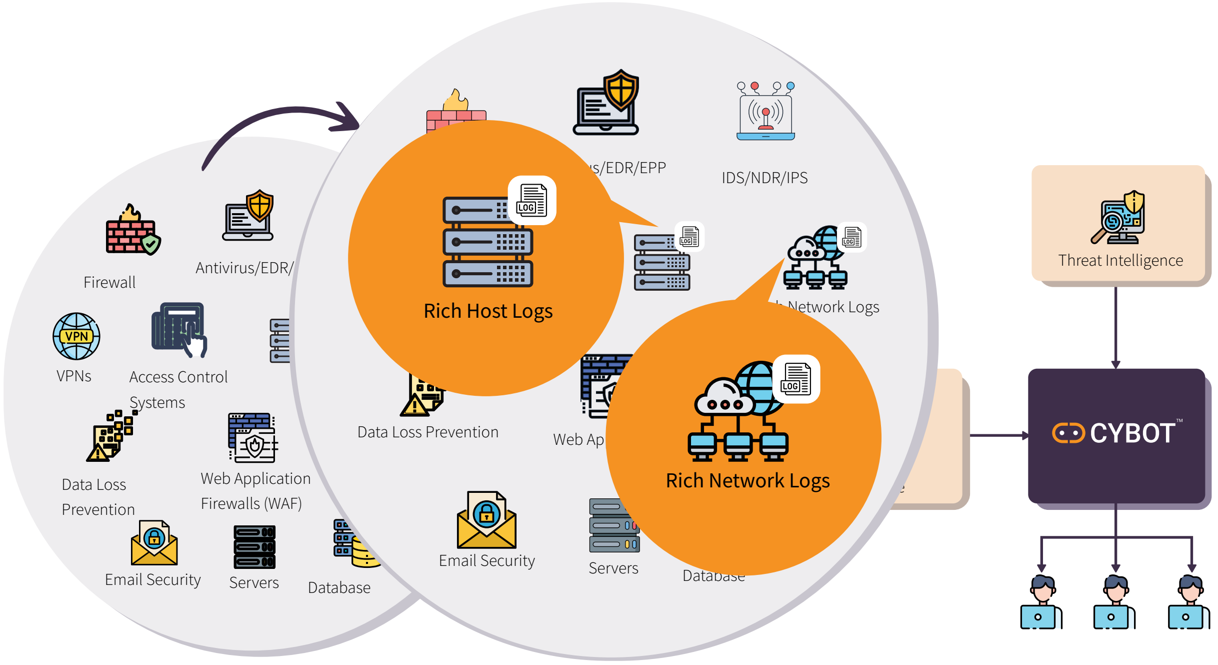
CYBOT™

The CYBOT Concept

The Design and Solution Placement



- ✓ We collected data from the whole IT/OT/IOT Infrastructure
- ✓ We ingest our Threat Intelligence information into the platform
- ✓ Ingested them in a Unified and Normalized format on the CYBOT Data Lake
- ✓ Utilized platform capability to automated SOC investigations and hunting on the unified data.

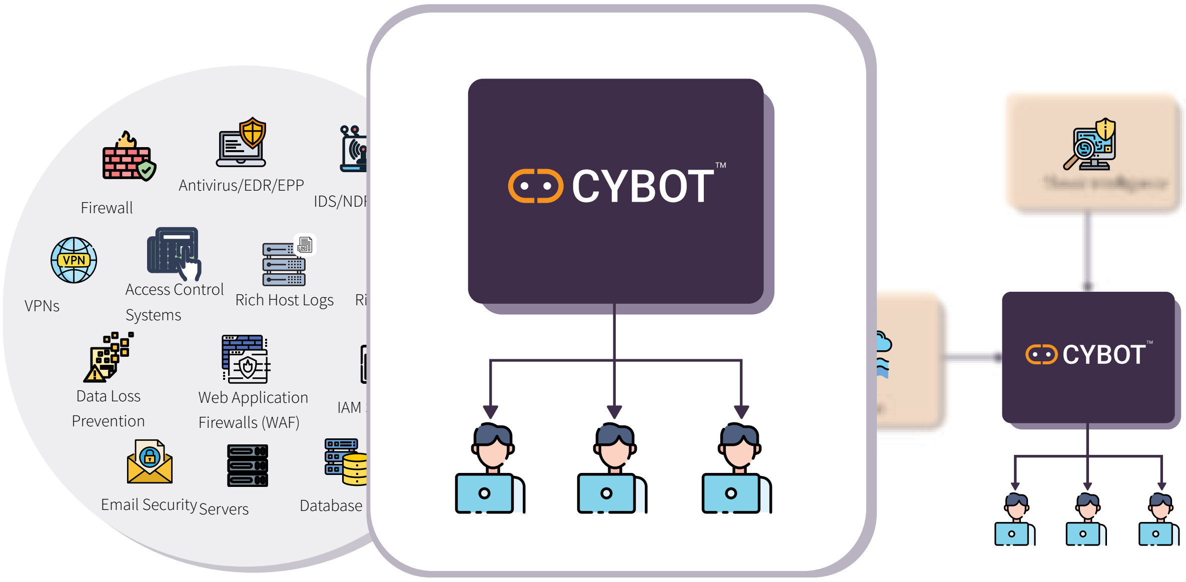


Organization’s IT/OT/IOT infrastructure

✓ **Limitless Log Collection:** CYBOT's log collection has no limitations, ensuring that no critical security event goes unnoticed.

✓ **Direct Integration with EDR:** Seamlessly collect rich host data directly from EDR and NDR solutions, leaving no gaps in our investigation and analysis.

✓ **Comprehensive Coverage:** Our log collection strategy guarantees that no critical events are missed, leaving no security gaps untouched.



Organization's IT/OT/IOT infrastructure

✓ **Beyond traditional solutions:** CYBOT transcends traditional security solutions by conducting automated investigations, and swiftly responding to threats.

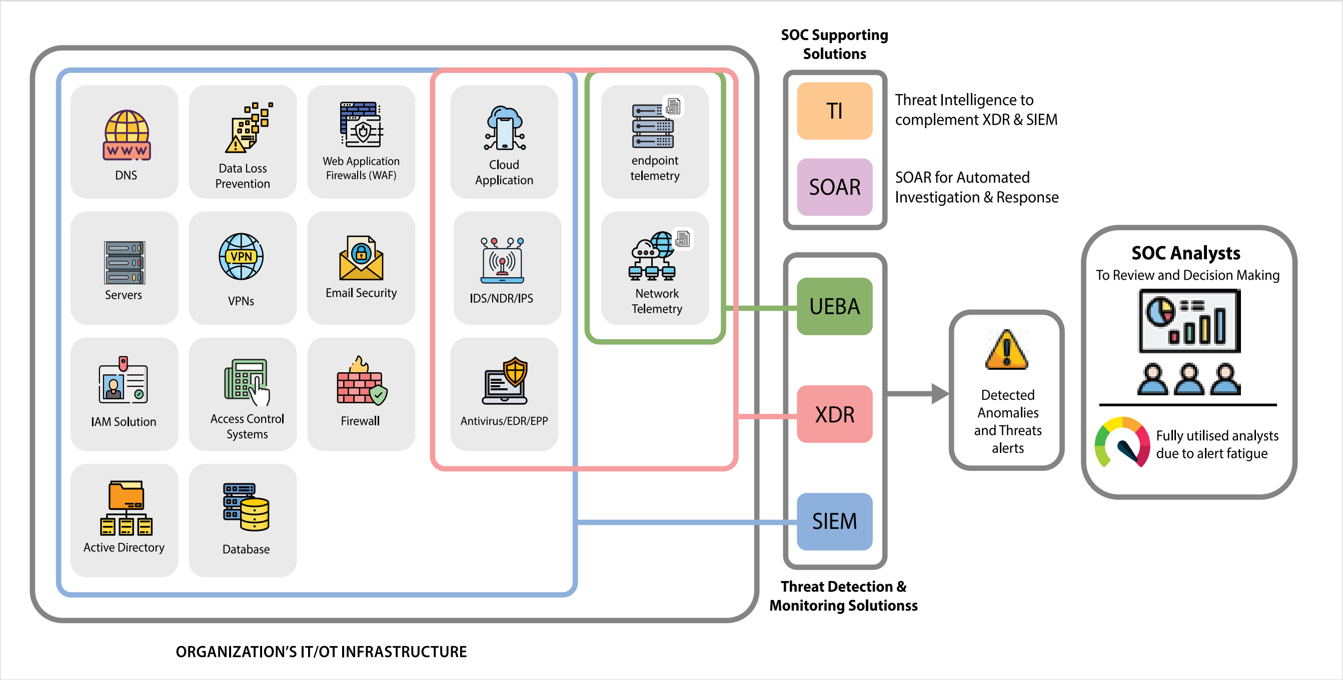
✓ **Visibility:** CYBOT features multiple modules offering deep insight into the organizations threats at every level of their security infrastructure.

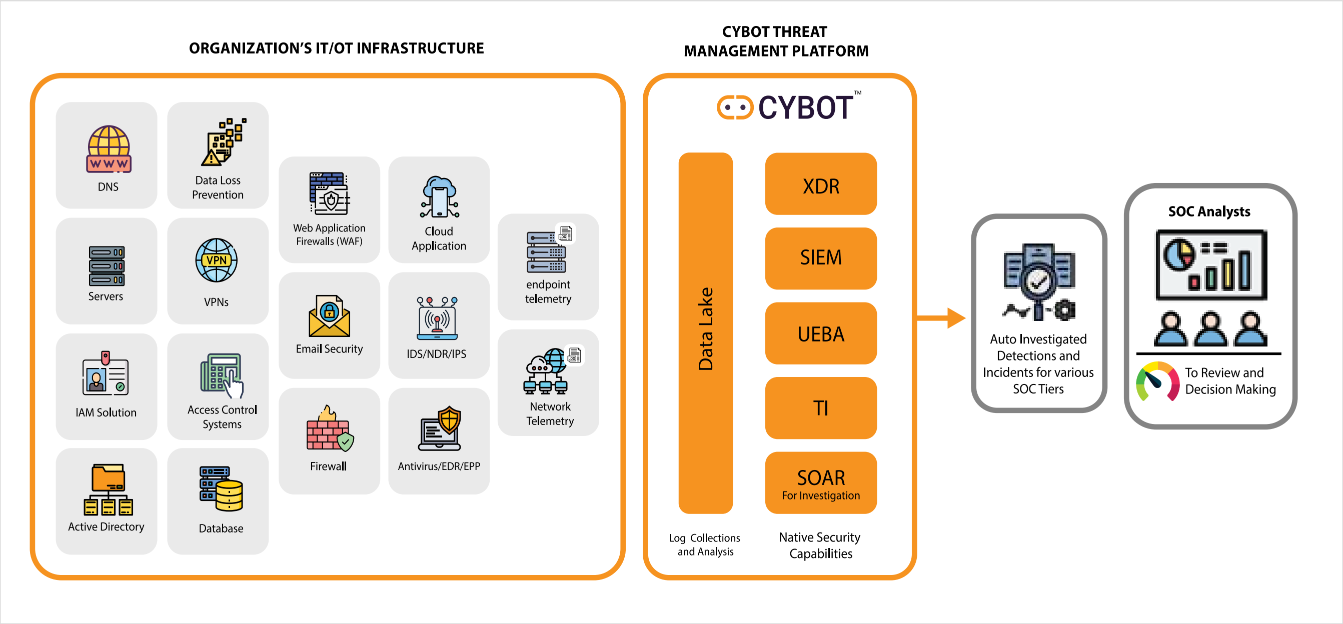
✓ **User Experience:** Designed with users in mind, CYBOT offers a user-friendly experience, providing informative insights to enhance your security operations.

- Customizable
- Wide coverage
- Deep visibility
- Latest threat intelligence
- Automated investigation and hunting
- AI ML powered behavior analytics
- Compliance coverage

Threat Management Portal

Security Solutions and Their Visibility on Threats


SOC Supporting Solutions
TI
Threat Intelligence to complement XDR & SIEM
SOAR
SOAR for Automated Investigation & Response
DNS
Data Loss Prevention
Web Application Firewalls (WAF)
Cloud Application
endpoint telemetry
Servers
VPNs
Email Security
IDS/NDR/IPS
Network Telemetry
IAM Solution
Access Control Systems
Firewall
Antivirus/EDR/EPP
Active Directory
Database
UEBA
XDR
SIEM
Detected Anomalies and Threats alerts
SOC Analysts
To Review and Decision Making
Fully utilised analysts due to alert fatigue
Threat Detection & Monitoring Solutionss
ORGANIZATION'S IT/OT INFRASTRUCTURE



The CYBOT's Role

Cybot is positioned to replace traditional SIEM solutions and standalone XDR platforms by offering a unified and comprehensive approach to threat detection, analysis, and response. It further Compliments the organization with native capability of Behaviour Analytics (UEBA) , Threat Intelligence (TI) , Threat Hunting and Automated Investigation.

© 2023 ActiveBytes®. All Rights Reserved.

CYBOT Components

Partner with us for fully customizable Threat Management Platform that align with your specific requirements.

Core Components

- Investigate
- User Behavior Analysis
- Threat Hunting
- Threat Intelligence
- Compliance

Supporting Components

- Orchestrator
- Case Management
- Mangaement Dashbaord

Core Components

Investigate

CYBOT's core threat detection and response revolve around the Investigate components. 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.

Threat Intelligence

The Threat Intelligence component stays updated with global cybersecurity information, including the latest attacks, vulnerabilities, and exploits. It's further improved by client's commercial TI subscriptions.

UEBA

This components extensively learns the client environment over time, monitoring all entity actions. When it identifies unusual behavior, it alerts your analysts for deeper investigation. What sets it apart from other UEBA solutions is its ability to detect anomalies across all collected logs in the data lake.

Compliance

CYBOT's compliance component offers user-friendly dashboards and actionable insights. It includes compliance dashboards and active monitoring tailored to PCI DSS, NIST, and ISO 27001 standards, helping companies navigate regulatory compliance effectively.

Threat Hunting

The Hunter components comes with with multiple hunt scenarios, designed to uncover hidden threats within your organization. These scenarios continuously scan for patterns and tactics in the digital landscape. When an anomaly is detected, the component promptly alerts your analysts to act.

Supporting Components

Orchestrator

Your dedicated command center for overseeing, fine-tuning, expanding, and customizing security use cases. Centralize playbook management to stay ahead of threats and maintain a streamlined, effective security environment. Experience control, precision, and security convergence with Orchestrator.

Mangaement Dashbaord

The Management Dashboard offers an intuitive, real-time view of your organization's cybersecurity landscape. It provides insights into alerts and threats from each security solution, alongside detailed views of inbound and outbound traffic, including location maps. Additionally, it covers email and file activities, Active Directory events, user and host activities, and more.

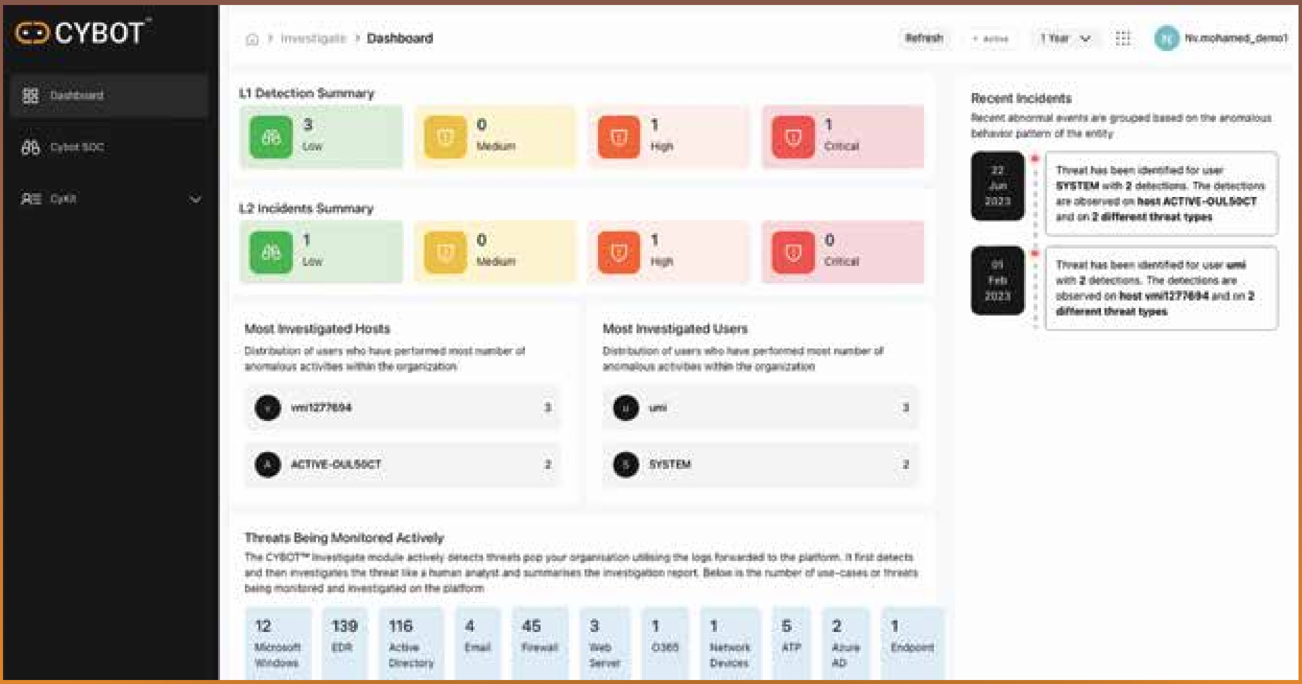
Case Management

CYBOT is now your all-in-one security solution, incorporating a Case Management feature that streamlines our security incident and ticket tracking. No need to seek external Incident and Service Ticket Management (ISTM) solutions or investing in additional tools; CYBOT covers it all.

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.



L1 Detection Summary

3 Low	0 Medium	1 High	1 Critical

L2 Incidents Summary

1 Low	0 Medium	1 High	0 Critical

Most Investigated Hosts

Distribution of users who have performed most number of anomalous activities within the organization

vmi1277694	3
ACTIVE-OUL50CT	2

Most Investigated Users

Distribution of users who have performed most number of anomalous activities within the organization

umi	3
SYSTEM	2

Threats Being Monitored Actively

The CYBOT™ Investigate module actively detects threats pop your organisation utilising the logs forwarded to the platform. It first detects and then investigates the threat like a human analyst and summarises the investigation report. Below is the number of use-cases or threats being monitored and investigated on the platform

12 Microsoft Windows	139 EDR	116 Active Directory	4 Email	45 Firewall	3 Web Server	1 O365	1 Network Devices	5 ATP	2 Azure AD	1 Endpoint

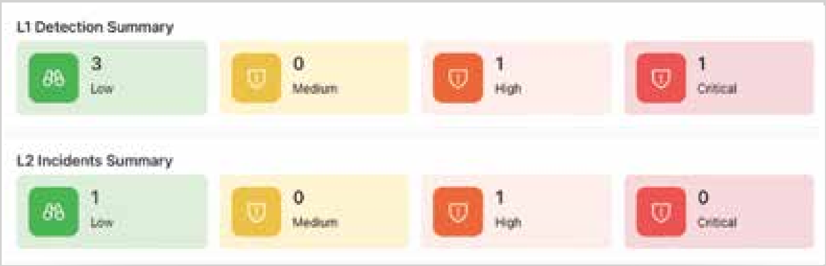
Recent Incidents

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-OUL50CT** and on **2 different threat types**

05 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**

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



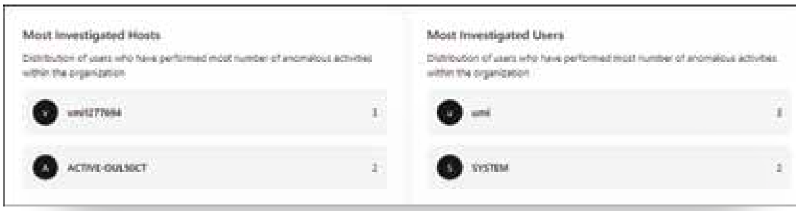
L1 Detection Summary

3 Low	0 Medium	1 High	1 Critical

L2 Incidents Summary

1 Low	0 Medium	1 High	0 Critical

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

Distribution of users who have performed most number of anomalous activities within the organization

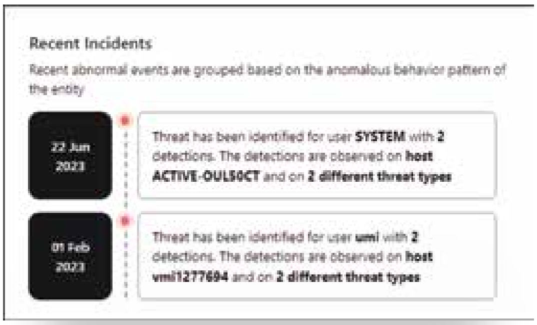
V vmi1277694	1
A ACTIVE-OULSOCT	2

Most Investigated Users

Distribution of users who have performed most number of anomalous activities within the organization

U umi	2
S SYSTEM	2

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



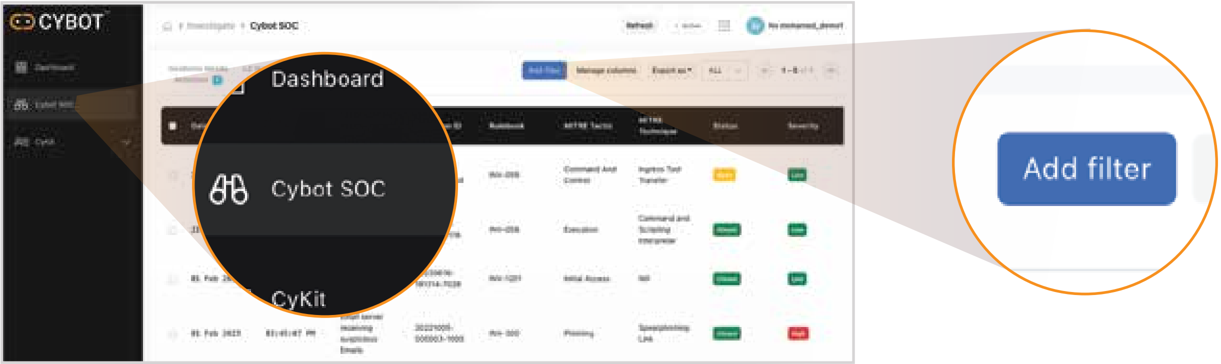
Recent Incidents

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-OULSOCT** 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.

✓

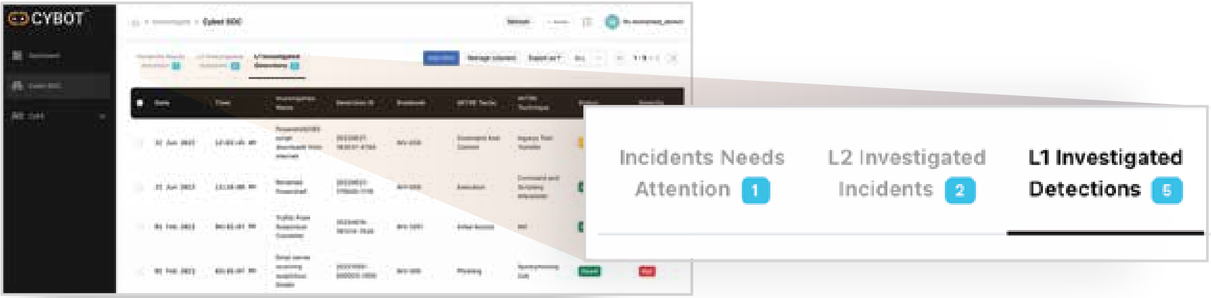
Advanced Filtering:
Utilize advanced filters to precisely refine your data, with the added convenience of saving and loading filters for future use.

✓

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

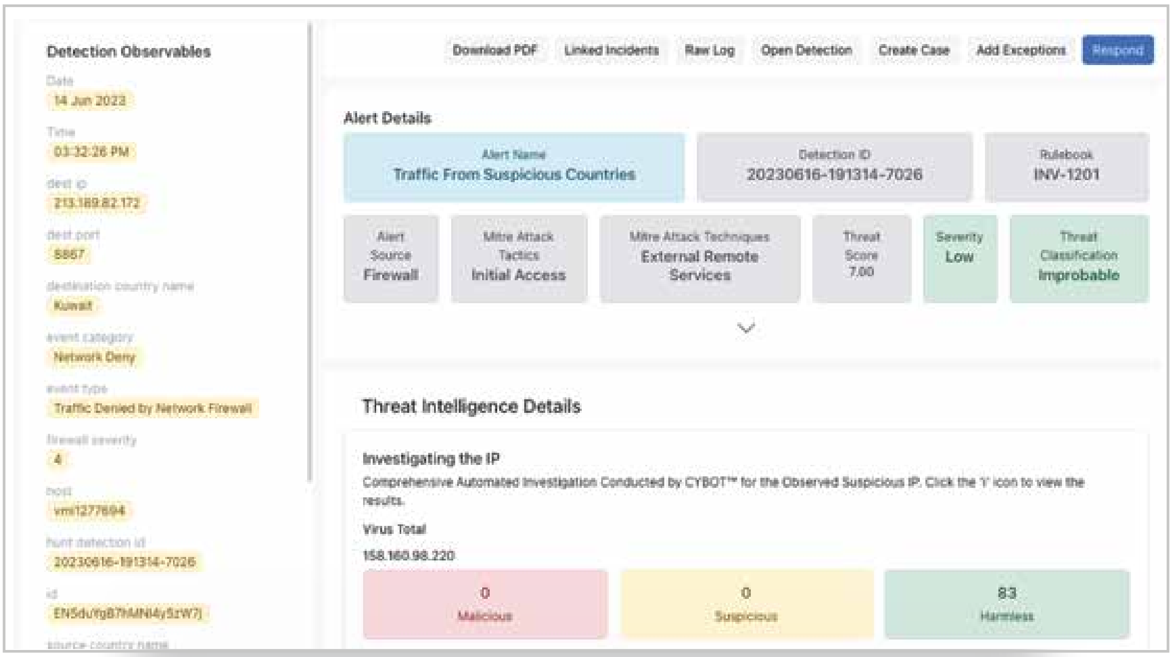
✓

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



CYBOT
Cybot SOC
Incidents Needs Attention 1
L2 Investigated Incidents 2
L1 Investigated Detections 5

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.



Detection Observables

Date	14 Jun 2023
Time	03:32:26 PM
dest ip	213.189.82.172
dest port	8667
destination country name	Kuwait
event category	Network Deny
event type	Traffic Denied by Network Firewall
firewall severity	4
host	vmi1277694
hunt detection id	20230616-191314-7026
id	ENSdu/YgB7hMNl4y5zW7j
source country name	

Alert Details

Alert Name	Traffic From Suspicious Countries
Detection ID	20230616-191314-7026
Rulebook	INV-1201
Alert Source	Firewall
Mitre Attack Tactics	Initial Access
Mitre Attack Techniques	External Remote Services
Threat Score	7.00
Severity	Low
Threat Classification	Improbable

Threat Intelligence Details

Investigating the IP

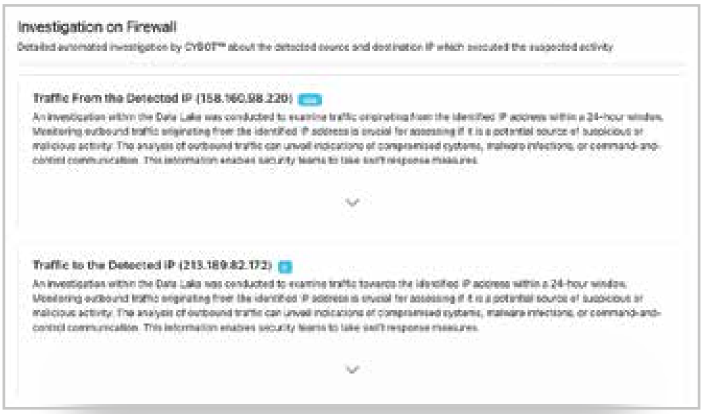
Comprehensive Automated Investigation Conducted by CYBOT™ for the Observed Suspicious IP. Click the 'i' icon to view the results.

Virus Total

158.160.98.220

Malicious	Suspicious	Harmless
0	0	83

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.



Investigation on Firewall

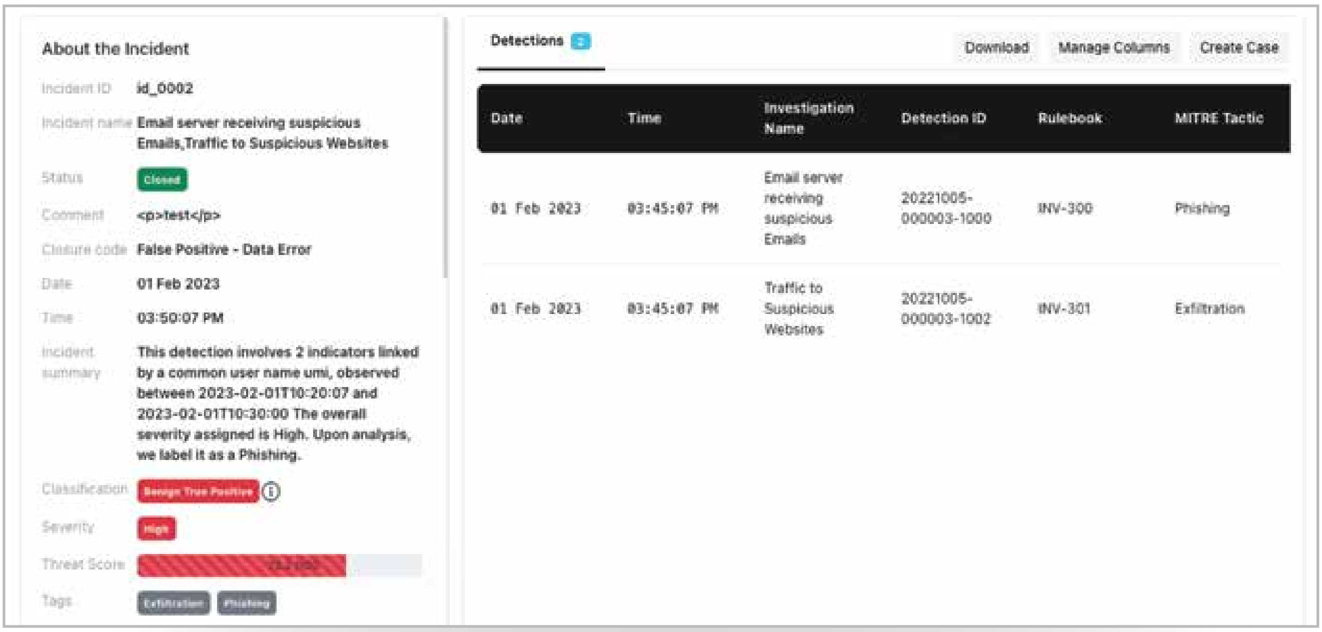
Detailed automated investigation by CYBOT™ about the detected source and destination IP which executed the suspected activity

Traffic From the Detected IP (158.160.98.220)

An investigation within the Data Lake was conducted to examine traffic originating from the identified IP address within a 24-hour window. Monitoring outbound traffic originating from the identified IP address is crucial for assessing if it is a potential source of suspicious or malicious activity. The analysis of outbound traffic can unveil indications of compromised systems, malware infections, or command-and-control communication. This information enables security teams to take swift response measures.

Traffic to the Detected IP (213.189.82.172)

An investigation within the Data Lake was conducted to examine traffic towards the identified IP address within a 24-hour window. Monitoring outbound traffic originating from the identified IP address is crucial for assessing if it is a potential source of suspicious or malicious activity. The analysis of outbound traffic can unveil indications of compromised systems, malware infections, or command-and-control communication. This information enables security teams to take swift response measures.



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: Benign True Positive

Severity: High

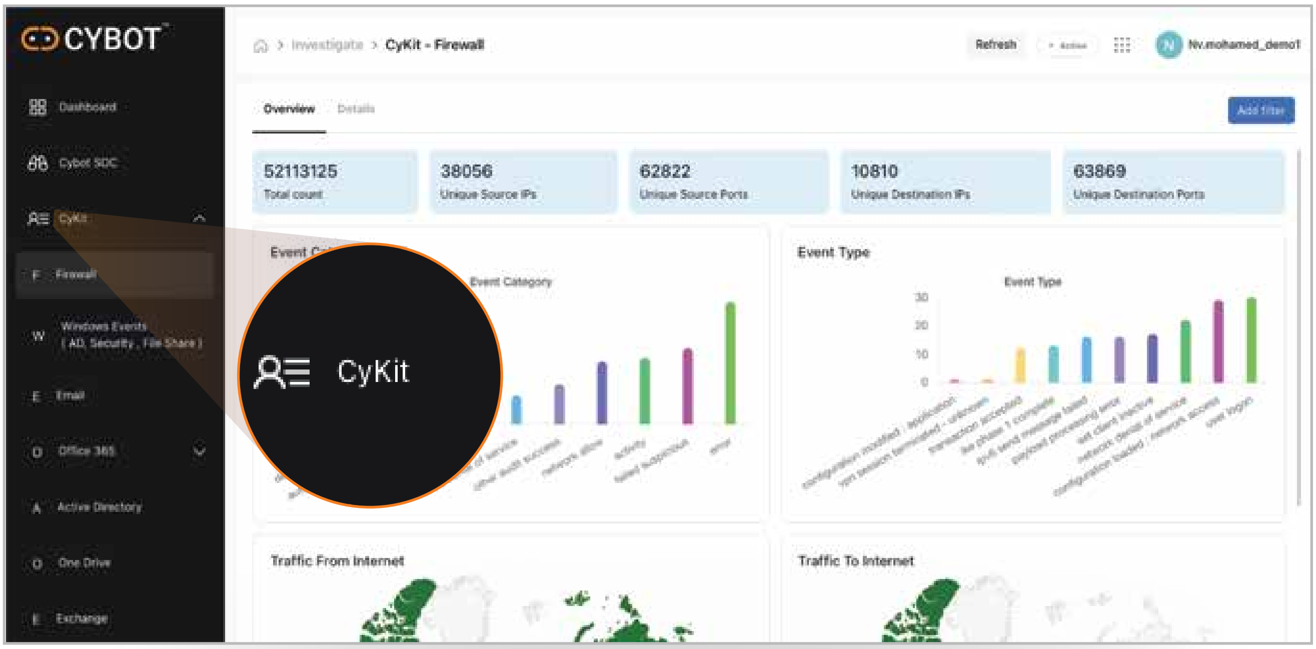
Threat Score:

Tags: Exfiltration Phishing

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.



52113125 Total count

38056 Unique Source IPs

62822 Unique Source Ports

10810 Unique Destination IPs

63869 Unique Destination Ports

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

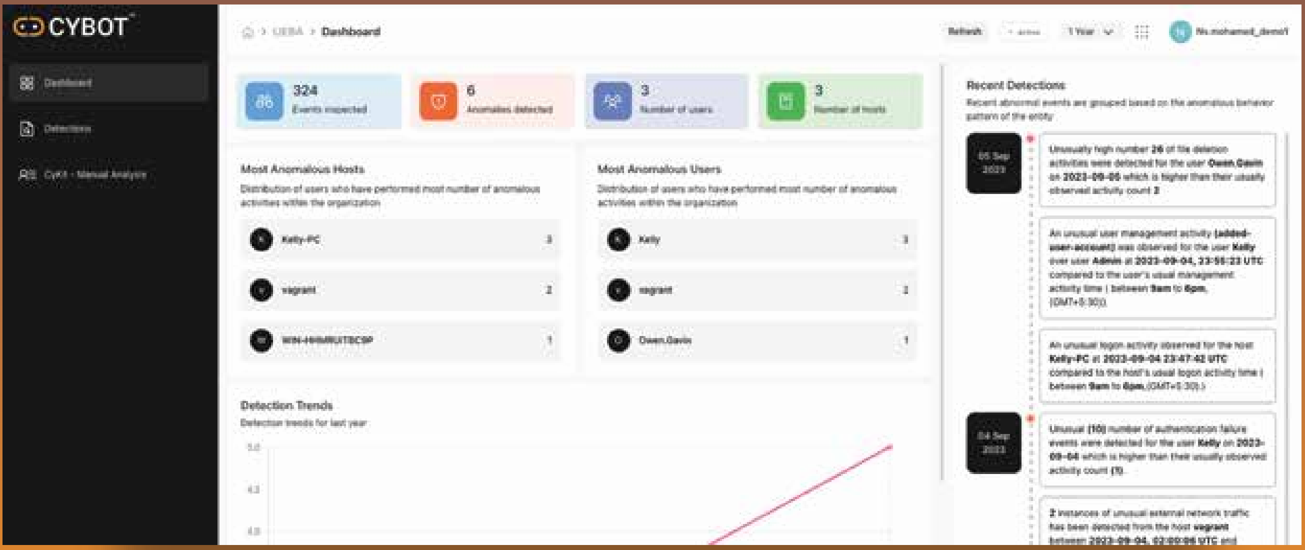
This unique capability provides the internal security team with replicas of essential security solutions including firewalls, ATP, and Office 365.

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.

Component

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.



Most Anomalous Hosts

Distribution of users who have performed most number of anomalous activities within the organization

Kelly-PC	3
vagrant	2
WIN-HH6MRUITBCSP	1

Most Anomalous Users

Distribution of users who have performed most number of anomalous activities within the organization

Kelly	3
vagrant	2
Owen.Davis	1

Recent Detections

Recent abnormal events are grouped based on the anomalous behavior pattern of the entity

05 Sep 2023

Unusually high number **26** of file deletion activities were detected for the user **Owen.Davis** on **2023-09-05** which is higher than their usually observed activity count **2**

An unusual user management activity **(added-user-account)** was observed for the user **Kelly** over user **Admin** at **2023-09-04, 23:55:23 UTC** compared to the user's usual management activity time (between **9am** to **6pm**, (GMT+5:30)).

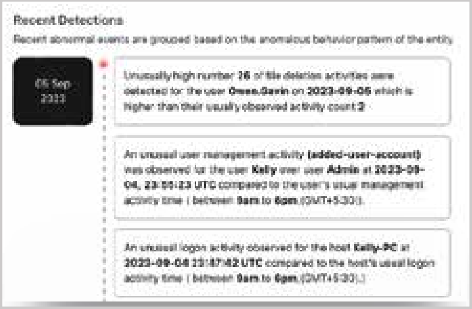
An unusual logon activity observed for the host **Kelly-PC** at **2023-09-04 23:47:42 UTC** compared to the host's usual logon activity time (between **9am** to **6pm**,(GMT+5:30).)

04 Sep 2023

Unusual **(10)** number of authentication failure events were detected for the user **Kelly** on **2023-09-04** which is higher than their usually observed activity count **(1)**.

2 instances of unusual external network traffic has been detected from the host **vagrant** between **2023-09-04, 02:00:06 UTC** and

- ✓ 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.



Recent Detections

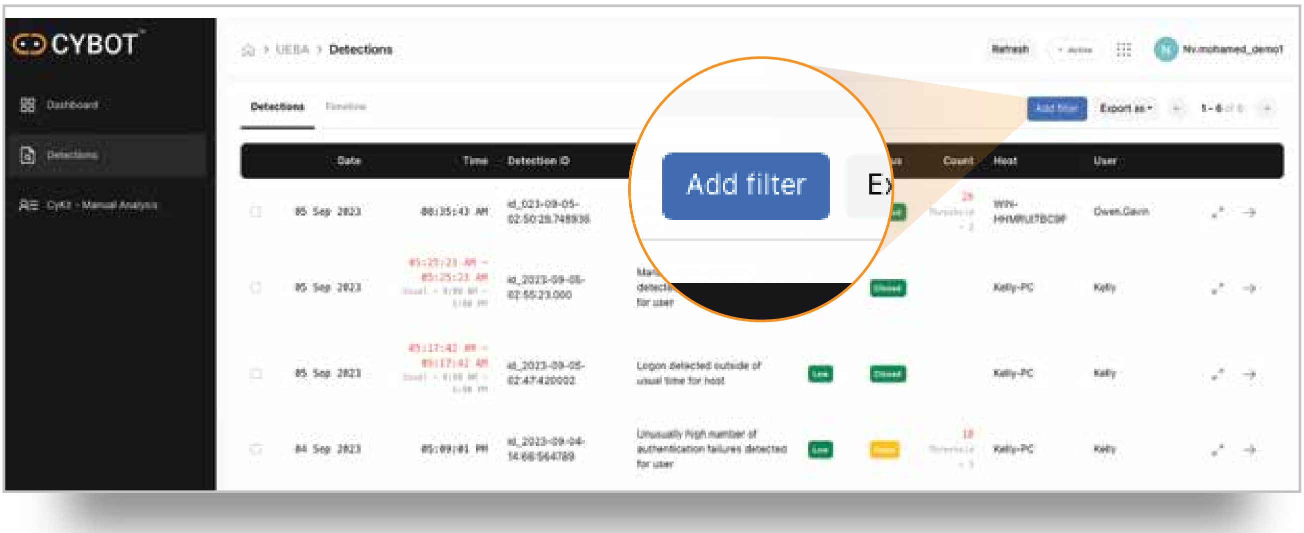
Recent abnormal events are grouped based on the anomalous behavior pattern of the entity

05 Sep 2023

Unusually high number **26** of file deletion activities were detected for the user **Owen.Davis** on **2023-09-05** which is higher than their usually observed activity count **2**

An unusual user management activity **(added-user-account)** was observed for the user **Kelly** over user **Admin** at **2023-09-04, 23:55:23 UTC** compared to the user's usual management activity time (between **9am** to **6pm**,(GMT+5:30)).

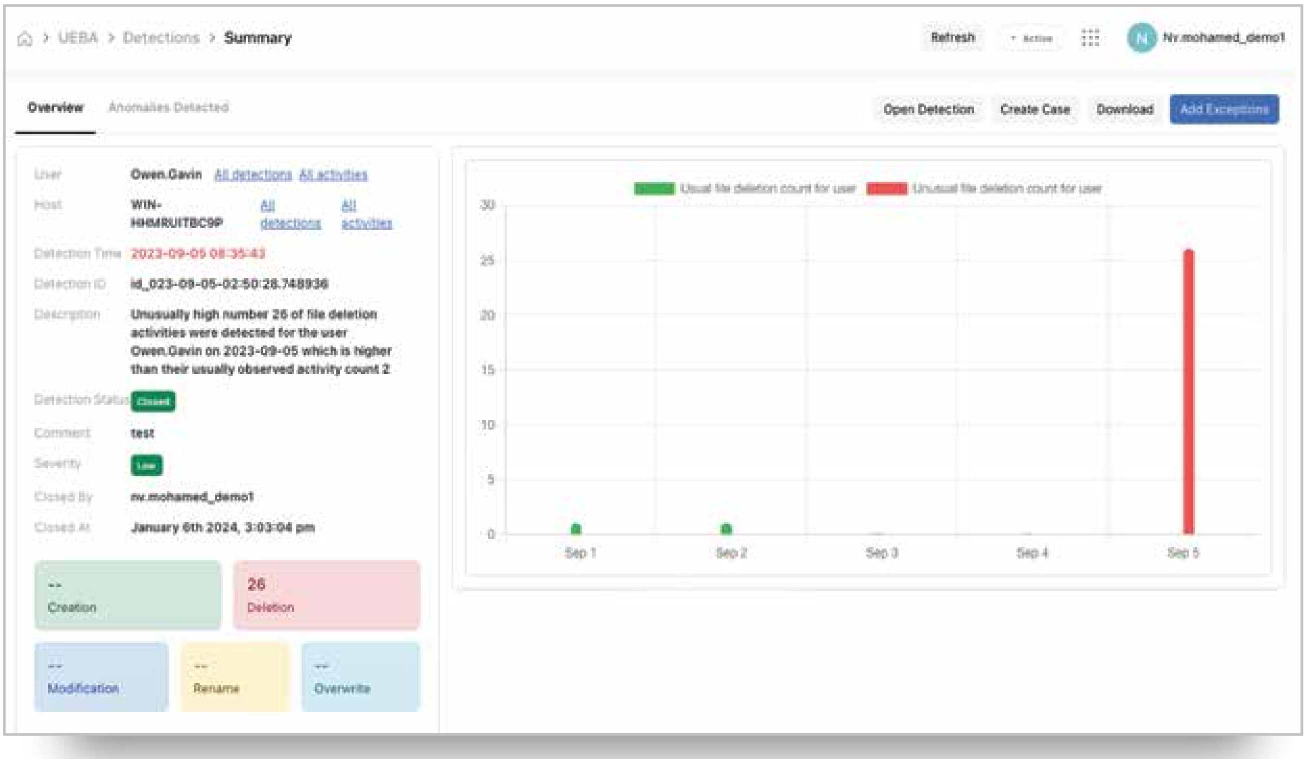
An unusual logon activity observed for the host **Kelly-PC** at **2023-09-04 23:47:42 UTC** compared to the host's usual logon activity time (between **9am** to **6pm**,(GMT+5:30).)



	Date	Time	Detection ID			...us	Count	Host	User
□	05 Sep 2023	08:35:43 AM	id_023-09-05-02:50:28.748936			...ed	26 Threshold - 2	WIN-HHMRUITBC9P	Owen.Gavin
□	05 Sep 2023	05:25:23 AM - 05:25:23 AM Usual - 9:00 AM - 5:00 PM	id_2023-09-05-02:55:23.000	Man... detect... for user		Closed		Kelly-PC	Kelly
□	05 Sep 2023	05:17:42 AM - 05:17:42 AM Usual - 9:00 AM - 5:00 PM	id_2023-09-05-02:47:420002	Logon detected outside of usual time for host	Low	Closed		Kelly-PC	Kelly
□	04 Sep 2023	05:09:01 PM	id_2023-09-04-14:68:564789	Unusually high number of authentication failures detected for user	Low	Open	18 Threshold - 3	Kelly-PC	Kelly

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.

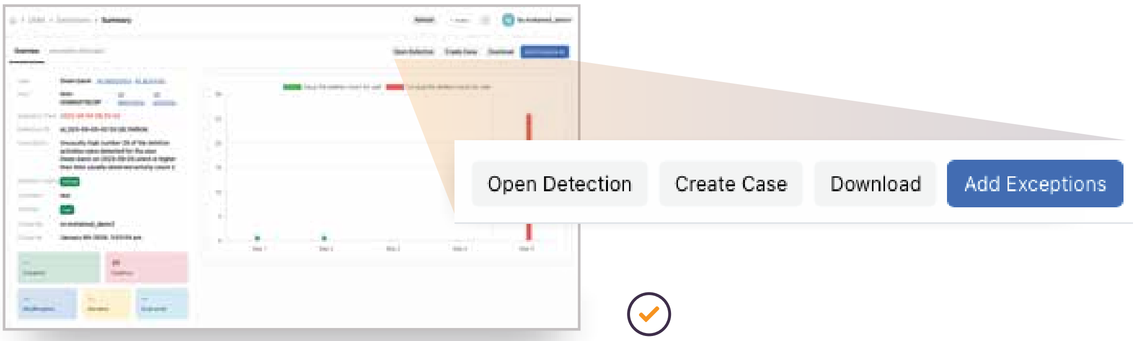
Utilize **filters** to view the timeline activity of users or hosts, export results, and drill down for manual analysis. Perform in-depth investigation using the detection summary and anomalies detected.



User Owen.Gavin All detections All activities
Host: WIN-HHMRUITBC9P All detections All activities
Detection Time: 2023-09-05 08:35:43
Detection ID: id_023-09-05-02:50:28.748936
Description: Unusually high number 26 of file deletion activities were detected for the user Owen.Gavin on 2023-09-05 which is higher than their usually observed activity count 2
Detection Status: Closed
Comment: test
Severity: Low
Closed By: nv.mohamed_demo1
Closed At: January 6th 2024, 3:03:04 pm

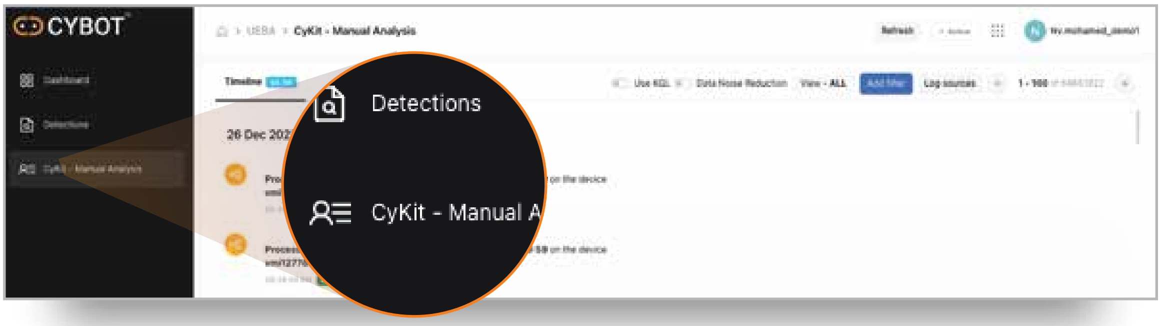
Creation	Deletion	Modification	Rename	Overwrite
--	26	--	--	--

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.



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.

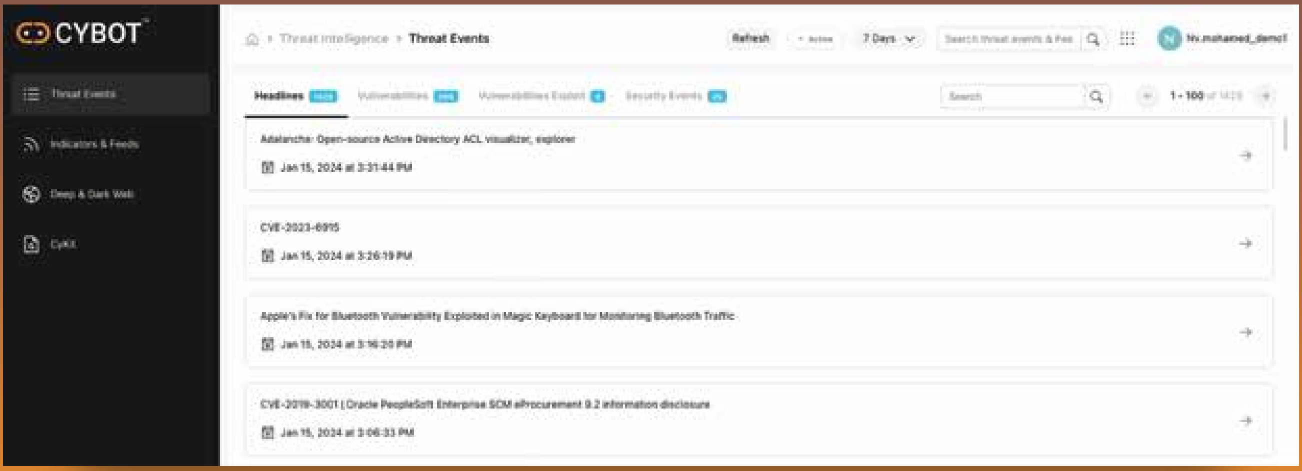


Explore defaulters' timelines with precision by excluding system, user, and computer accounts. Utilize our unique log collection method, capable of filtering the timeline based on diverse log sources from almost every corner of your environment. Enhance analysis and gain insightful, refined data.

Component

CYBOT THREAT INTELLIGENCE

Empower your security with CYBOT™—a pre-loaded CTI component, eliminating the need for costly external subscriptions. Powered by CYKIT, it enables ad-hoc hunting, delivering efficient.



CYBOT™

- Threat Events
- Indicators & Feeds
- Deep & Dark Web
- CyKit

Threat Intelligence > Threat Events

Refresh | + Active | 7 Days | Search threat events & Fee | Nv.mohamed_demo1

Headlines 1431 | Vulnerabilities 596 | Vulnerabilities Exploit 9 | Security Events 25 | Search | 1 - 100 of 1431

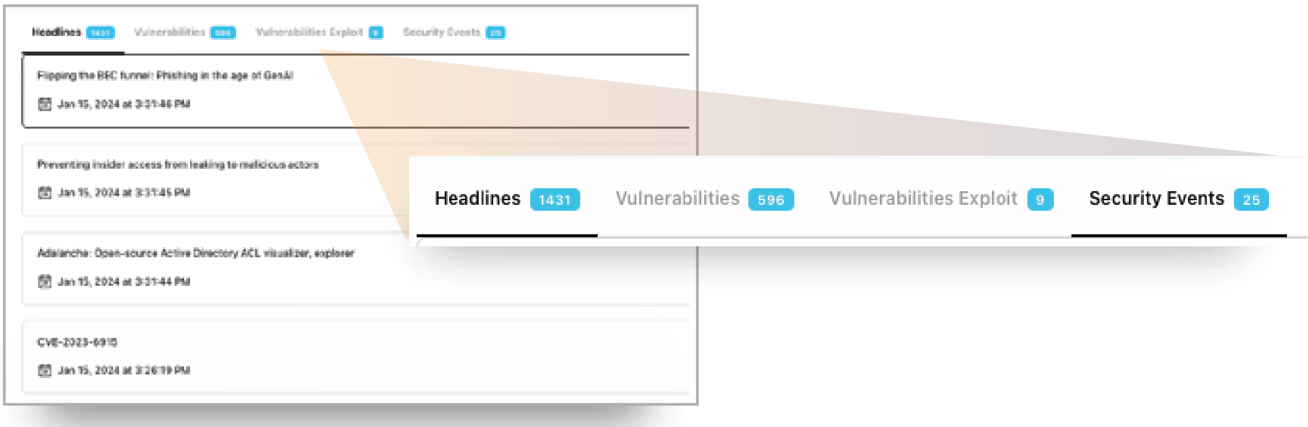
Adalanche: Open-source Active Directory ACL visualizer, explorer
Jan 15, 2024 at 3:31:44 PM

CVE-2023-6915
Jan 15, 2024 at 3:26:19 PM

Apple's Fix for Bluetooth Vulnerability Exploited in Magic Keyboard for Monitoring Bluetooth Traffic
Jan 15, 2024 at 3:16:20 PM

CVE-2019-3001 | Oracle PeopleSoft Enterprise SCM eProcurement 9.2 information disclosure
Jan 15, 2024 at 3:06:33 PM

- ✓ Accessible through user-friendly interfaces, CYBOT™ ensures both technical and non-technical teams have quality insights for a robust security framework. Say goodbye to repeated investigations, reduce false-positives, and upgrade your security with CYBOT™ —advanced, cost-effective, and powerful.



Headlines 1431 | Vulnerabilities 596 | Vulnerabilities Exploit 9 | Security Events 25

Flipping the BEC funnel: Phishing in the age of GenAI
Jan 15, 2024 at 3:31:46 PM

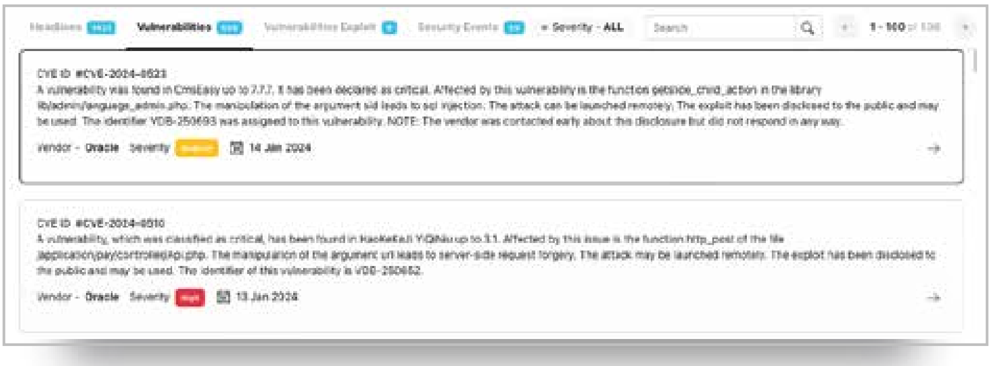
Preventing insider access from leaking to malicious actors
Jan 15, 2024 at 3:31:45 PM

Adalanche: Open-source Active Directory ACL visualizer, explorer
Jan 15, 2024 at 3:31:44 PM

CVE-2023-6915
Jan 15, 2024 at 3:26:19 PM

- ✓ Stay informed with CYBOT™—our free CTI component delivers real-time updates on global cyber threats, vulnerabilities, and exploits. Effortlessly access insightful **headlines** to enhance your organization's security posture. With CYBOT™, receive timely and relevant intelligence without the hefty price tag. Upgrade your threat awareness and response capabilities today.

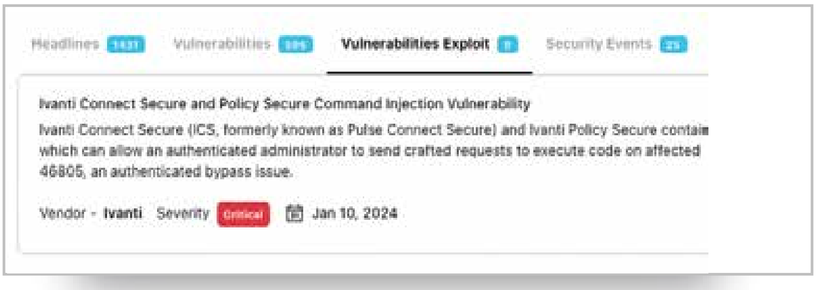
- Enhance your defense strategy with CYBOT™ our free CTI component provides timely **vulnerability** intelligence. Stay ahead of threats by receiving valuable insights into the latest vulnerabilities and exploits. Empower your security team with the knowledge needed to fortify your organization against potential risks. CYBOT™ —your ally in proactive and effective vulnerability management.



CVE ID #CVE-2024-0523
A vulnerability was found in CmsEasy up to 7.7.7. It has been declared as critical. Affected by this vulnerability is the function getslide_child_action in the library lib/admin/language_admin.php. The manipulation of the argument sid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250693 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
Vendor - Oracle Severity Medium 14 Jan 2024

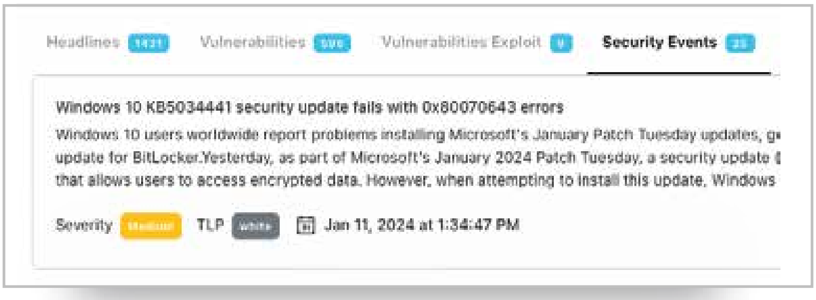
CVE ID #CVE-2024-0510
A vulnerability, which was classified as critical, has been found in HaoKeKeJi YiQiNiu up to 3.1. Affected by this issue is the function http_post of the file application/pay/controller/Api.php. The manipulation of the argument url leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250652.
Vendor - Oracle Severity High 13 Jan 2024

- Elevate your security posture with CYBOT™—our free CTI component delivers real-time insights into **vulnerabilities and associated exploits**. Stay ahead of potential threats by accessing timely information, enabling your organization to proactively address and mitigate risks. CYBOT™ empowers your security team with valuable intelligence, reinforcing your defense against evolving cyber threats.

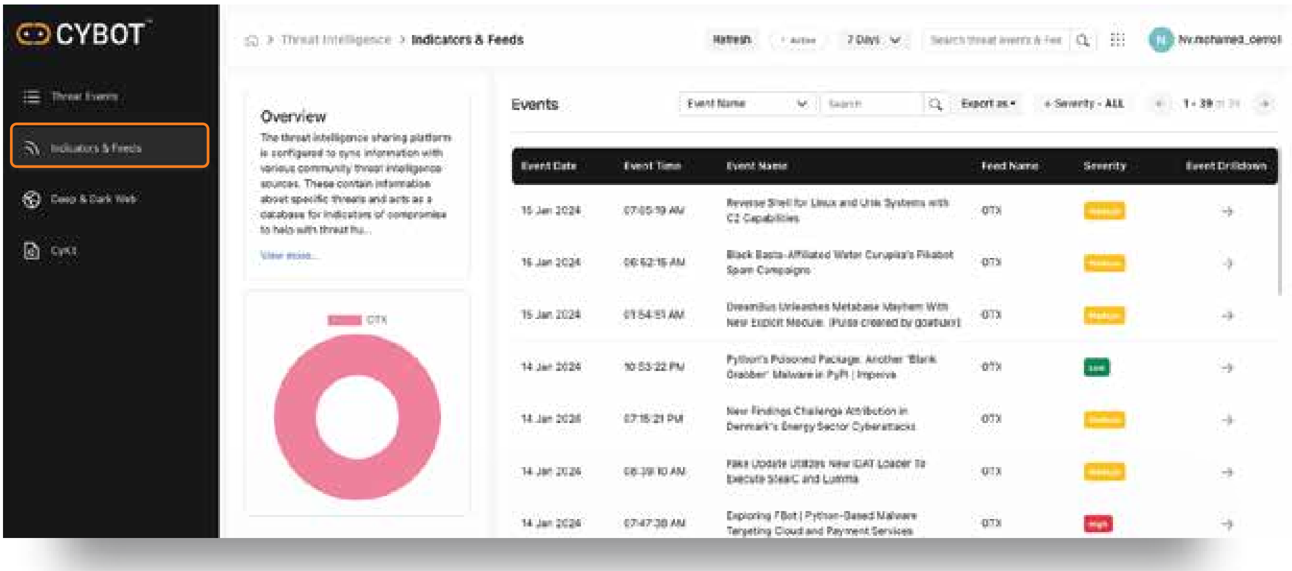


Ivanti Connect Secure and Policy Secure Command Injection Vulnerability
Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure contai
which can allow an authenticated administrator to send crafted requests to execute code on affected
46805, an authenticated bypass issue.
Vendor - Ivanti Severity Critical Jan 10, 2024

- Stay informed about the **latest incidents**, threat actor activities, and emerging trends. Empower your security team with real-time insights, enhancing your organization's ability to detect and respond to security events effectively. CYBOT™—keeping you ahead in the dynamic realm of cybersecurity.



Windows 10 KB5034441 security update fails with 0x80070643 errors
Windows 10 users worldwide report problems installing Microsoft's January Patch Tuesday updates, g
update for BitLocker.Yesterday, as part of Microsoft's January 2024 Patch Tuesday, a security update
that allows users to access encrypted data. However, when attempting to install this update, Windows
Severity Medium TLP White Jan 11, 2024 at 1:34:47 PM

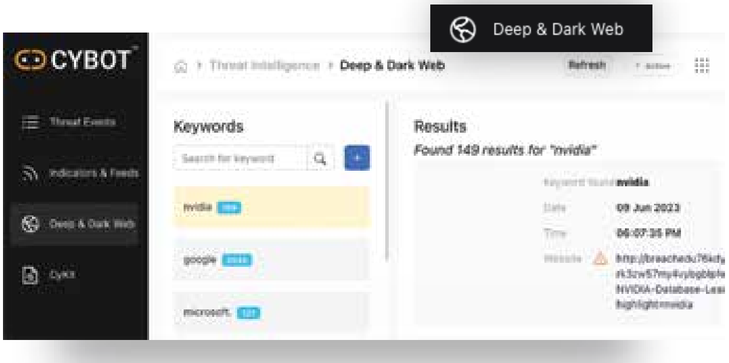


Overview

The threat intelligence sharing platform is configured to sync information with various community threat intelligence sources. These contain information about specific threats and acts as a database for indicators of compromise to help with threat hu...

Event Date	Event Time	Event Name	Feed Name	Severity	Event Drilldown
15 Jan 2024	07:05:19 AM	Reverse Shell for Linux and Unix Systems with C2 Capabilities	OTX	Medium	→
15 Jan 2024	06:52:15 AM	Black Basta-Affiliated Water Curupira's Pikabot Spam Campaigns	OTX	Medium	→
15 Jan 2024	01:54:51 AM	DreamBus Unleashes Metabase Mayhem With New Exploit Module (Pulse created by goatsark)	OTX	Medium	→
14 Jan 2024	10:53:22 PM	Python's Poisoned Package: Another 'Blank Grabber' Malware in PyPI | Imperva	OTX	Low	→
14 Jan 2024	07:15:21 PM	New Findings Challenge Attribution in Denmark's Energy Sector Cyberattacks	OTX	Medium	→
14 Jan 2024	08:39:10 AM	Fake Update Utilizes New IDAT Loader To Execute StealC and Lumma	OTX	Medium	→
14 Jan 2024	07:47:38 AM	Exploring FBot | Python-Based Malware Targeting Cloud and Payment Services	OTX	High	→

Syncs with diverse community threat intelligence sources, acting as a comprehensive database for Indicators of Compromise. Visualizations showcase data summaries, including feed distribution, timeline of arrivals, and types of obtained Indicators/Attributes for efficient threat hunting and intelligence-driven activities.



Results

Found 149 results for "nvidia"

Keyword found nvidia

Date 09 Jun 2023

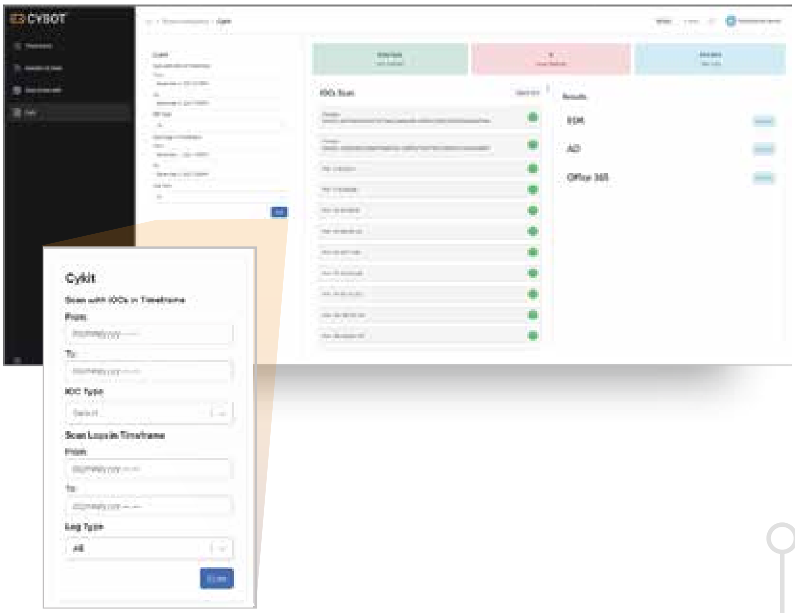
Time 06:07:35 PM

Website http://breachedu76kdy...#k3zw57my4vybgbfe...NVIDIA-Database-Lea...highlight=nvidia

Gain insights into cybercriminal activities, leaked credentials, and emerging risks. Empower your security team to proactively address vulnerabilities and stay one step ahead of evolving threats in the hidden corners of the internet. CYBOT™ —defending your organization in the shadows.

Empower quick ad-hoc hunting with CYKIT™—a powerful tool for swift identification of potential threats. Seamlessly match the latest IOCs against your organization's data, enhancing threat intelligence capabilities for proactive defense.

Stay agile and informed with CYKIT™ —your ally in rapid threat detection.



Cykit

Scan with IOCs in Timeframe

From: dd/mm/yyyy --:--

To: dd/mm/yyyy --:--

IOC Type: Select

Scan Logs in Timeframe

From: dd/mm/yyyy --:--

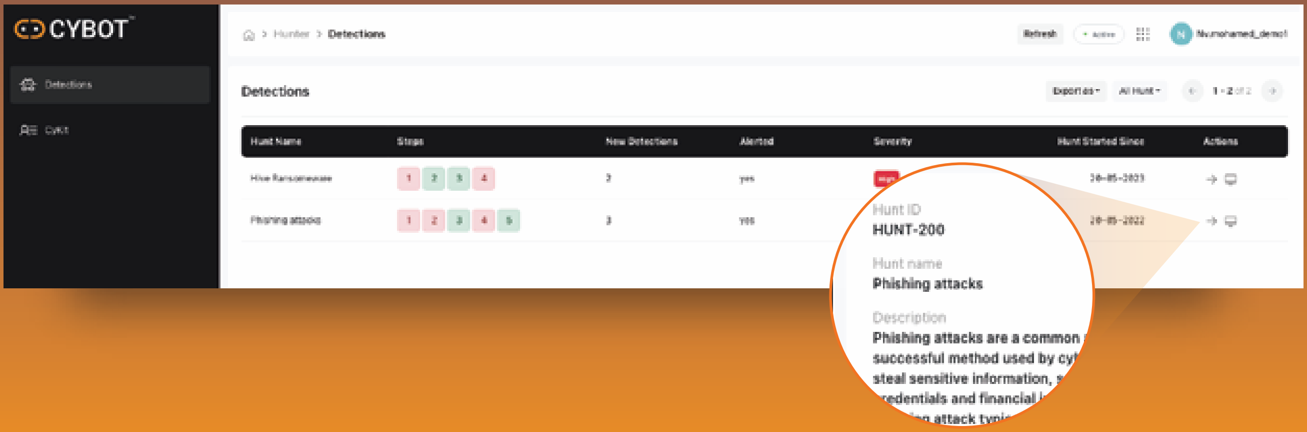
To: dd/mm/yyyy --:--

Log Type: All

Component

CYBOT HUNTER

The Hunter component comes with 25+ default hunt scenarios, designed to uncover hidden threats within your organization. These scenarios continuously scan for patterns and tactics in the digital landscape. When an anomaly is detected, the component promptly alerts your analysts to act.



Detections

Hunt Name	Steps	New Detections	Alerted	Severity	Hunt Started Since	Actions
Hive Ransomeware	1 2 3 4	2	yes	High	20-05-2023	→
Phishing attacks	1 2 3 4 5	3	yes		20-05-2022	→

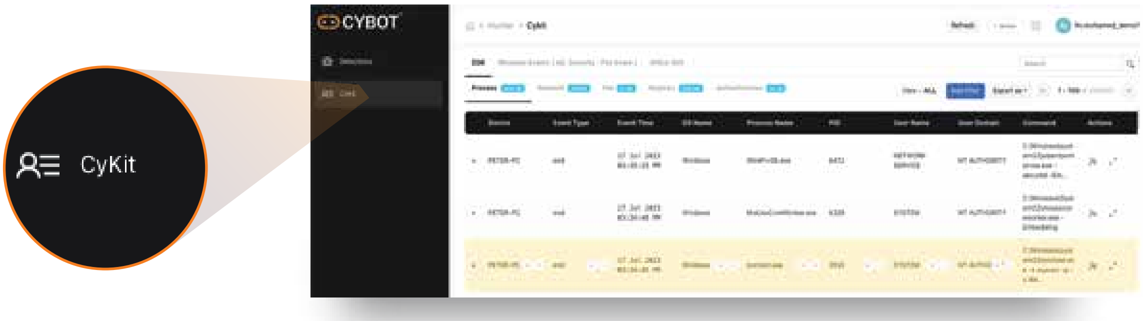
Hunt ID
HUNT-200

Hunt name
Phishing attacks

Description
Phishing attacks are a common
successful method used by cy
steal sensitive information,
redentials and financial
attack typic

Experience proactive threat hunting with CYBOT, conducting thorough investigations across the hosting environment to identify and address existing threats.

Gain a comprehensive view of hunts and their detection statuses. Access detailed investigations, review detection observations, and stay one step ahead of potential threats for an enhanced security posture.



Unlock a concise event overview from diverse organizational solutions. Select EDR, AD, and Office 365 data sources to scrutinize activities.

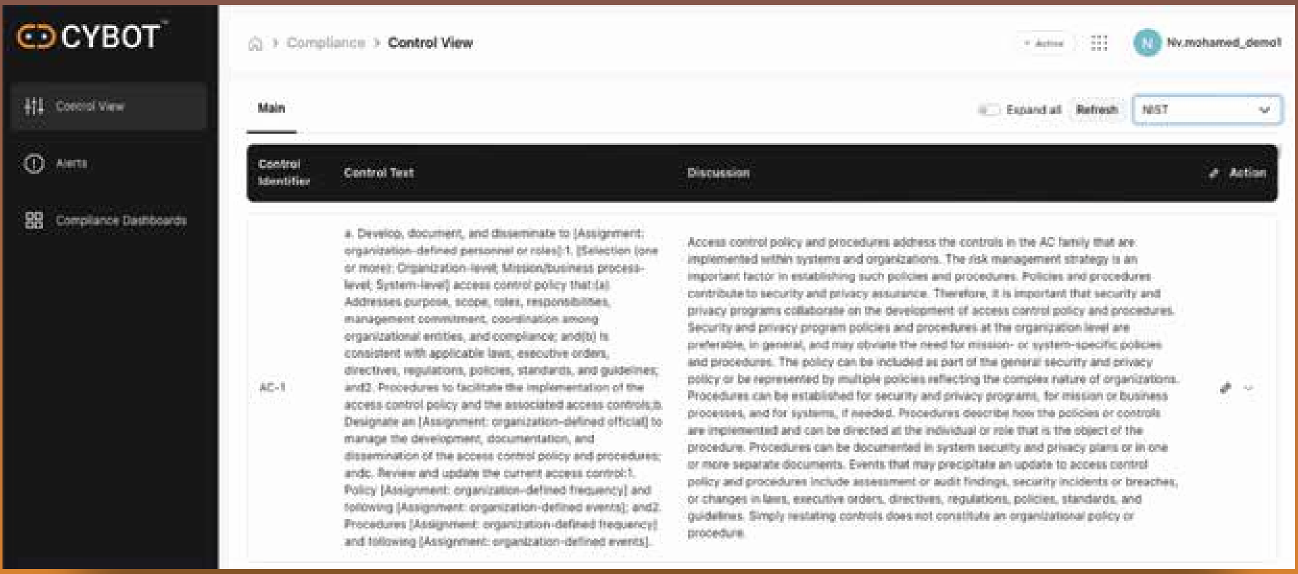
Key features include focused analysis with data source filtering, anomaly identification, filter preservation for future use, and seamless data export for investigation or reporting.

Hunter CyKit enables efficient and comprehensive data analysis.

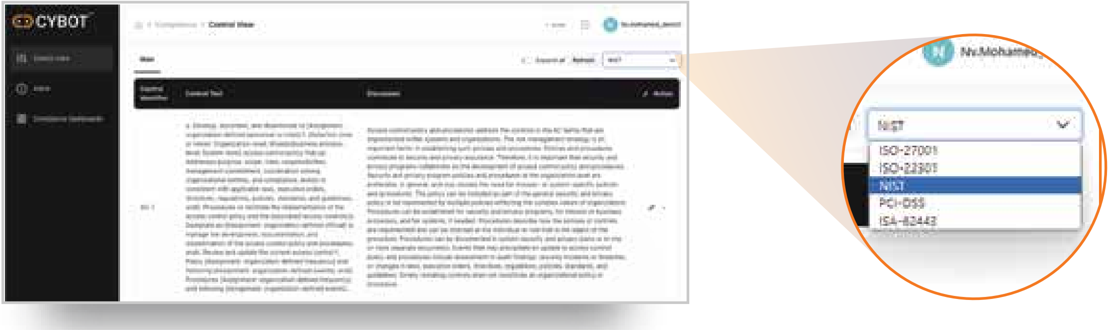
Component

CYBOT COMPLIANCE

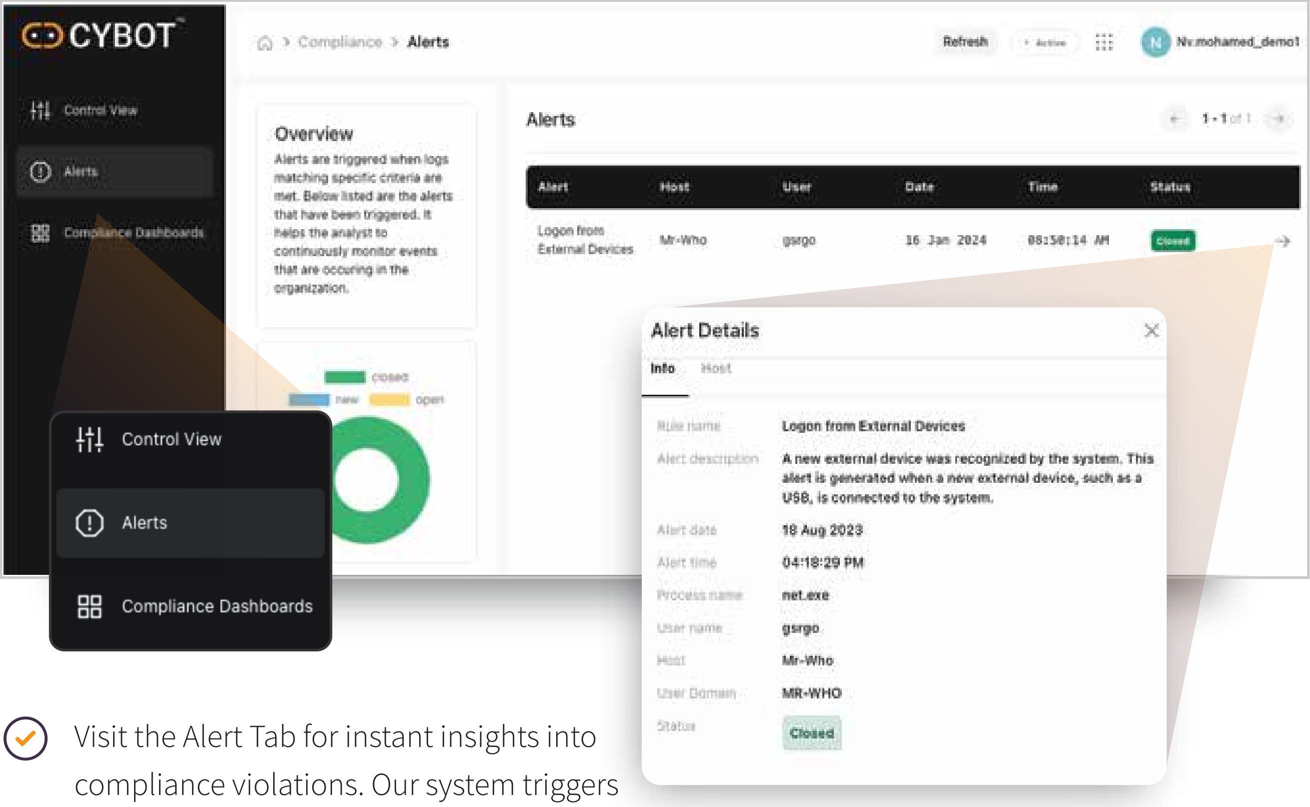
At ActiveBytes Innovations, we recognize the vital importance of compliance with industry regulations such as ISO 27001, PCI DSS, and NIST. To support organizations and security teams in their compliance journey, we've integrated a dedicated compliance module within the Threat Management Platform.



Control Identifier	Control Text	Discussion	Action
AC-1	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that:(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the access control policy and the associated access controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; andc. Review and update the current access control:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.	



Enjoy the flexibility to tailor our services to your organization's specific needs. Whether it's ISO 27001, PCI DSS, NIST, or any other framework, we provide the adaptability to meet your unique requirements.



Overview

Alerts are triggered when logs matching specific criteria are met. Below listed are the alerts that have been triggered. It helps the analyst to continuously monitor events that are occuring in the organization.

Alerts

Alert	Host	User	Date	Time	Status
Logon from External Devices	Mr-Who	gsrgo	16 Jan 2024	08:50:14 AM	Closed

Alert Details

Rule name	Logon from External Devices
Alert description	A new external device was recognized by the system. This alert is generated when a new external device, such as a USB, is connected to the system.
Alert date	18 Aug 2023
Alert time	04:18:29 PM
Process name	net.exe
User name	gsrgo
Host	Mr-Who
User Domain	MR-WHO
Status	Closed

- Visit the Alert Tab for instant insights into compliance violations. Our system triggers alerts when logs match specific criteria, allowing you to proactively monitor and swiftly respond to any breaches.

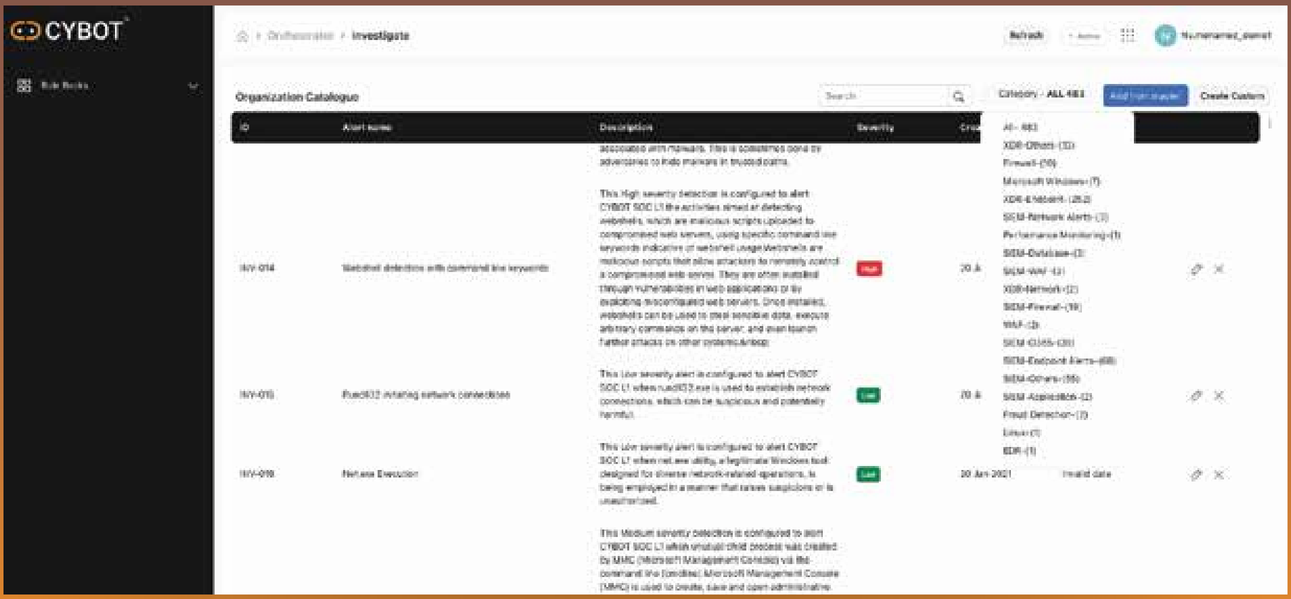
- **Compliance Dashboards** provide an organized view of an organization's compliance status, aligned with standards like PCI DSS, NIST, and ISO 27001.

  These visual representations enable quick identification of gaps and potential risks, facilitating proactive measures.

Component

CYBOT ORCHESTRATOR

Introducing CYBOT Orchestrator, your advanced automation hub for streamlined cybersecurity investigations in the data lake. Seamlessly define, configure, and manage detections across CYBOT components, addressing SOC challenges.



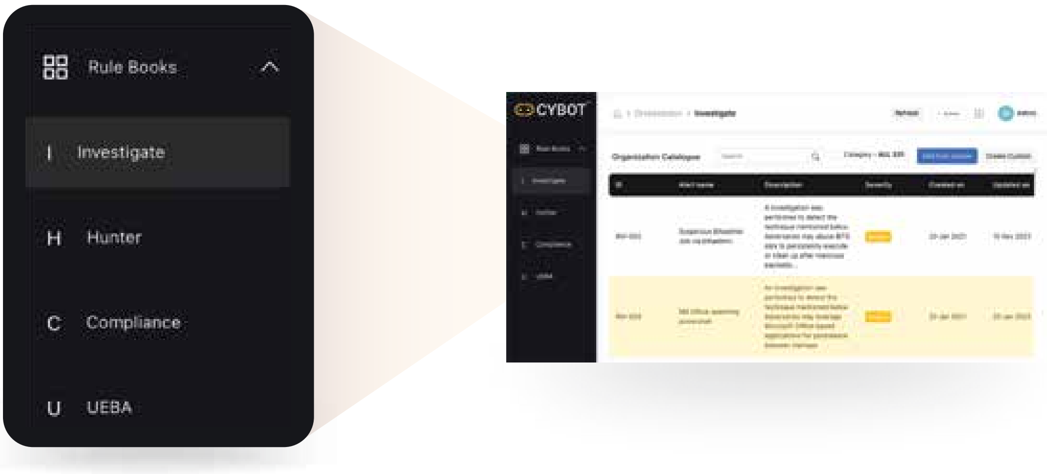
ID	Alert name	Description	Severity	Cre	
		associated with malware. This is sometimes done by adversaries to hide malware in trusted paths.			
INV-014	Webshell detection with command line keywords	This High severity detection is configured to alert CYBOT SOC L1 the activities aimed at detecting webshells, which are malicious scripts uploaded to compromised web servers, using specific command line keywords indicative of webshell usage.Webshells are malicious scripts that allow attackers to remotely control a compromised web server. They are often installed through vulnerabilities in web applications or by exploiting misconfigured web servers. Once installed, webshells can be used to steal sensitive data, execute arbitrary commands on the server, and even launch further attacks on other systems/network.	High	20 A	
INV-015	Rundll32 initiating network connections	This Low severity alert is configured to alert CYBOT SOC L1 when rundll32.exe is used to establish network connections, which can be suspicious and potentially harmful.	Low	20 A	
INV-016	Net.exe Execution	This Low severity alert is configured to alert CYBOT SOC L1 when net.exe utility, a legitimate Windows tool designed for diverse network-related operations, is being employed in a manner that raises suspicions or is unauthorized.	Low	20 Jan 2021	Invalid date
		This Medium severity detection is configured to alert CYBOT SOC L1 when unusual child process was created by MMC (Microsoft Management Console) via the command line (cmdline). Microsoft Management Console (MMC) is used to create, save and open administrative			

All - 483
XDR-Others-(33)
Firewall-(10)
Microsoft Windows-(7)
XDR-Endpoint-(252)
SIEM-Network Alerts-(3)
Performance Monitoring-(1)
SIEM-Database-(3)
SIEM-WAF-(2)
XDR-Network-(2)
SIEM-Firewall-(19)
WAF-(3)
SIEM-O365-(35)
SIEM-Endpoint Alerts-(68)
SIEM-Others-(35)
SIEM-Application-(2)
Fraud Detection-(3)
Linux-(1)
EDR-(1)

With preloaded proprietary use cases and ongoing integration by our Detection team, Orchestrator provides a user-friendly interface for efficient security posture enhancement.

Its automation extends beyond traditional solutions, enabling continuous scanning for potential threats.

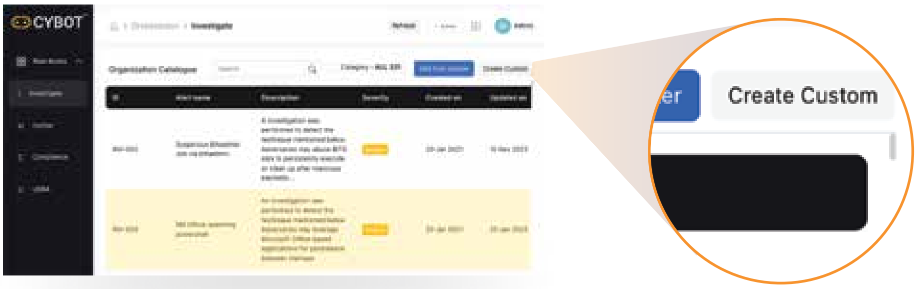
CYBOT Orchestrator: your practical solution for creating, managing, and fortifying defenses against evolving adversary tactics.

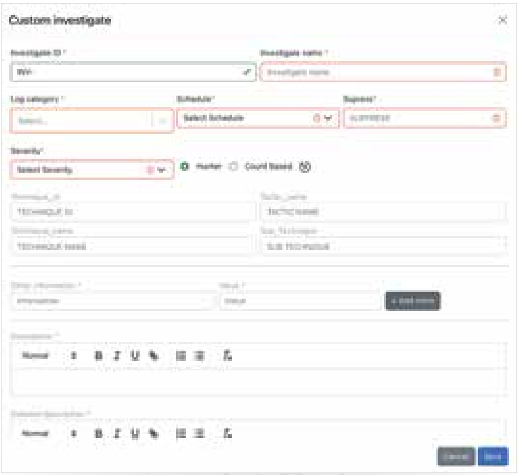


- Unlock precision and control in your cybersecurity strategy with CYBOT Orchestrator's intuitive navigation menu. Choose your rule book components effortlessly and take command of your use cases.

Navigate, create, and manage seamlessly — CYBOT Orchestrator empowers you at every click.

- Explore the **Investigate** components for seamless management of deployed cases, delve into the **Hunter** components for specialized use cases, and ensure **compliance** with ease in the dedicated Compliance components.

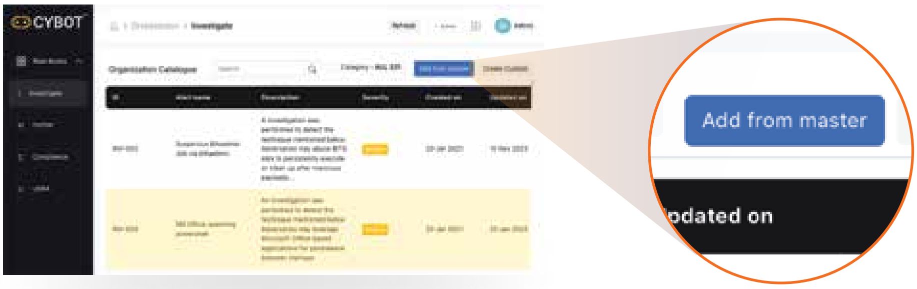




- CYBOT Orchestrator offers a unique **Create Custom** feature, allowing administrators to craft and deploy use cases tailored to organizational requirements.

- Unlike traditional SIEMs, CYBOT goes beyond by enabling the selection of specific automated investigations to run alongside detections.

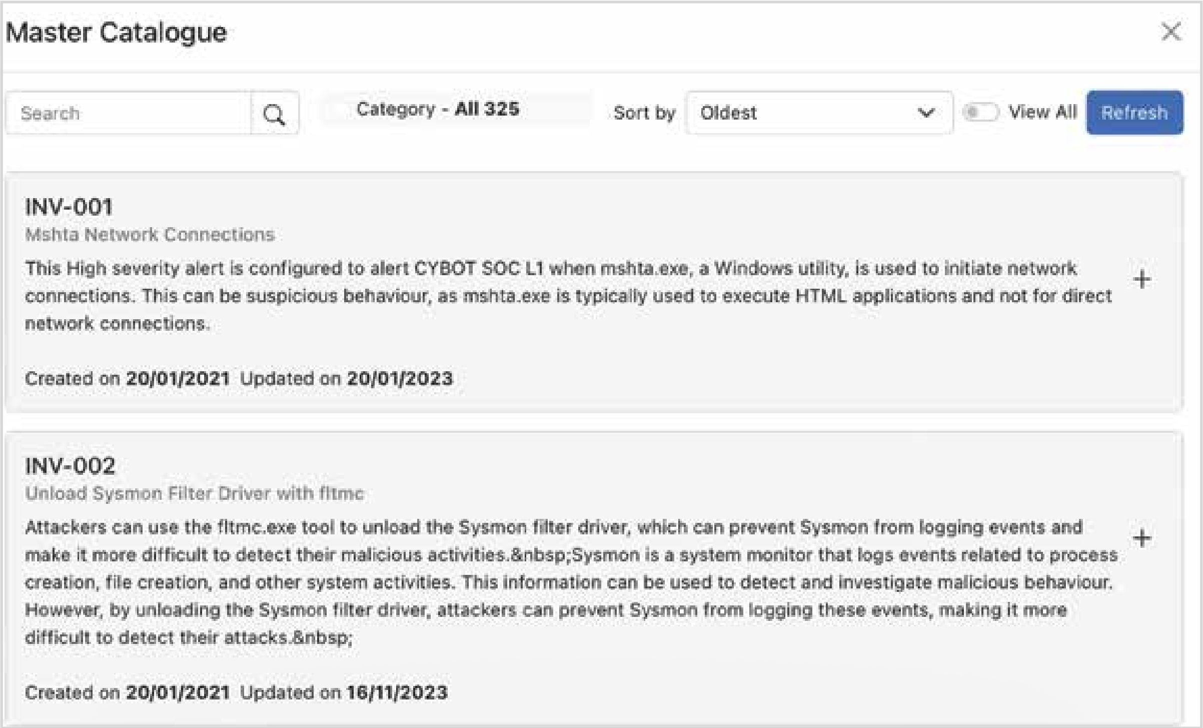
- This technical flexibility ensures a proactive and customized response to emerging threats, enhancing our cybersecurity capabilities beyond conventional solutions.



Simplify your workload with CYBOT Orchestrator – our Detection Engineering team takes charge of new threat identification.

When they pinpoint a new ATP activity or attack vector, a corresponding use case is promptly added to the **master repository**.

Admins can effortlessly access the master library, adding required use cases to their environment without the need for manual creation. It's that straightforward.



Master Catalogue

INV-001

Mshta Network Connections

This High severity alert is configured to alert CYBOT SOC L1 when mshta.exe, a Windows utility, is used to initiate network connections. This can be suspicious behaviour, as mshta.exe is typically used to execute HTML applications and not for direct network connections.

Created on **20/01/2021** Updated on **20/01/2023**

INV-002

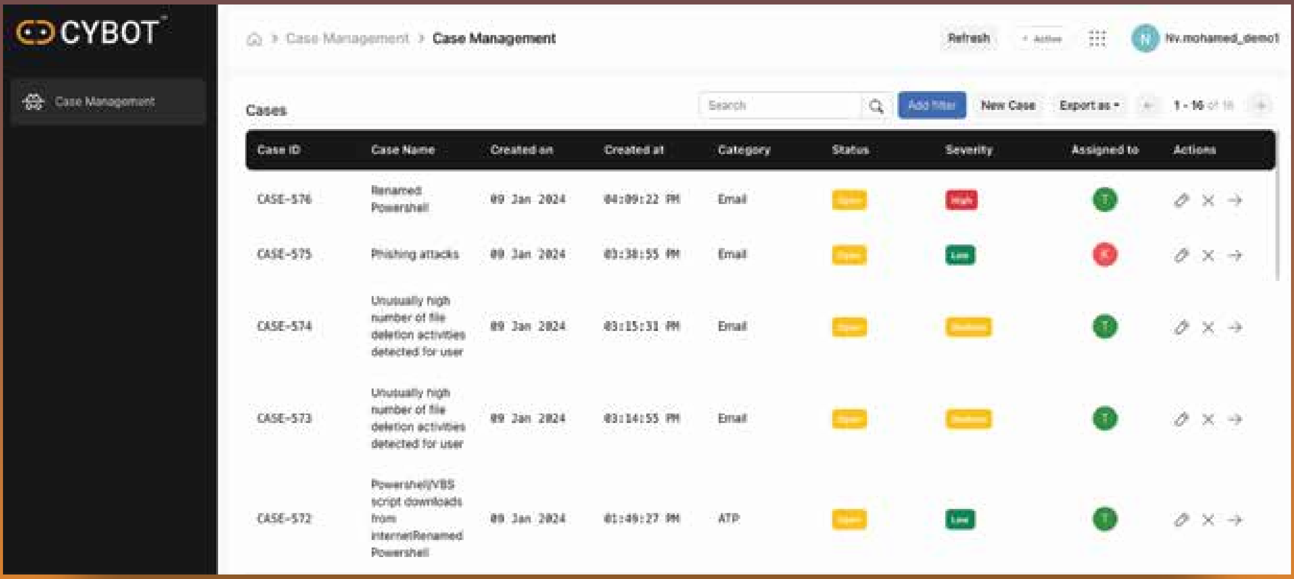
Unload Sysmon Filter Driver with fltmc

Attackers can use the fltmc.exe tool to unload the Sysmon filter driver, which can prevent Sysmon from logging events and make it more difficult to detect their malicious activities. Sysmon is a system monitor that logs events related to process creation, file creation, and other system activities. This information can be used to detect and investigate malicious behaviour. However, by unloading the Sysmon filter driver, attackers can prevent Sysmon from logging these events, making it more difficult to detect their attacks.

Created on **20/01/2021** Updated on **16/11/2023**

Component

CYBOT CASE MANAGEMENT



Cases

Case ID	Case Name	Created on	Created at	Category	Status	Severity	Assigned to	Actions
CASE-576	Renamed Powershell	09 Jan 2024	04:09:22 PM	Email	Open	High	T	✎ ✕ →
CASE-575	Phishing attacks	09 Jan 2024	03:38:55 PM	Email	Open	Low	K	✎ ✕ →
CASE-574	Unusually high number of file deletion activities detected for user	09 Jan 2024	03:15:31 PM	Email	Open	Medium	T	✎ ✕ →
CASE-573	Unusually high number of file deletion activities detected for user	09 Jan 2024	03:14:55 PM	Email	Open	Medium	T	✎ ✕ →
CASE-572	Powershell/VBS script downloads from internetRenamed Powershell	09 Jan 2024	01:49:27 PM	ATP	Open	Low	T	✎ ✕ →

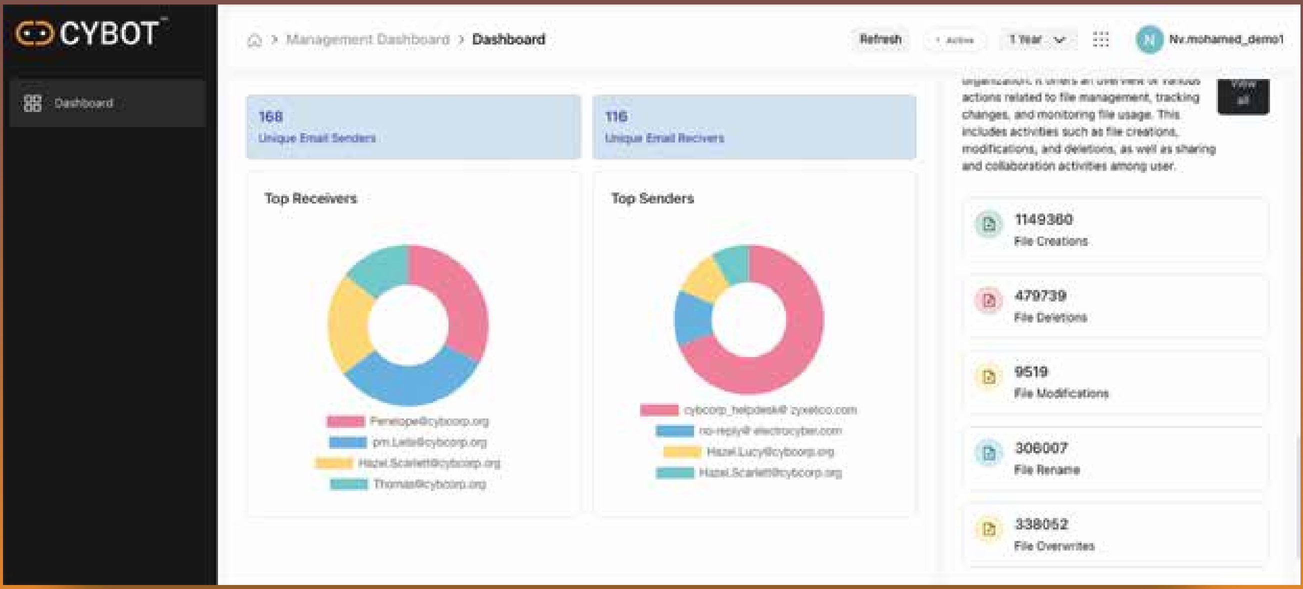
- ✓ CYBOT is now your all-in-one security solution, incorporating a Case Management feature that streamlines our security incident and ticket tracking. No need to seek external Incident and Service Ticket Management (ISTM) solutions or investing in additional tools; CYBOT covers it all.

- ✓ The Case Management component seamlessly tracks security incidents originating from the Investigate and UEBA components. CYBOT's Case Management allows analysts to easily add investigation notes, attach evidence, monitor ticket changes, create new tickets, or link them to existing child tickets, among other functions. It serves as our central hub for efficiently managing security incidents, granting us full control and visibility over the incident handling process.

- ✓ This achievement establishes a comprehensive Threat Management Platform, empowering our organization to proactively detect, respond to, and manage security threats with confidence. CYBOT's Case Management has significantly enhanced your incident response capabilities while simplifying the entire process, reducing the need for external tools and streamlining our security operations.

Component

CYBOT MANAGEMENT DASHBOARD



168
Unique Email Senders

116
Unique Email Recivers

Top Receivers

- Penelope@cybcorp.org
- pm.Laila@cybcorp.org
- Hazel.Scarlett@cybcorp.org
- Thomas@cybcorp.org

Top Senders

- cybcorp_helpdesk@ zyxelco.com
- no-reply@ electrocyber.com
- Hazel.Lucy@cyboorp.org
- Hazel.Scarlett@cybcorp.org

organization. It offers an overview of various actions related to file management, tracking changes, and monitoring file usage. This includes activities such as file creations, modifications, and deletions, as well as sharing and collaboration activities among user.

1149360	File Creations
479739	File Deletions
9519	File Modifications
306007	File Rename
338052	File Overwrites

- Eliminate the tedious process of requesting dashboards and reports from various teams to keep up with your organization's cybersecurity status and to present to senior management. We found the perfect solution in CYBOT's built-in Management Dashboards.

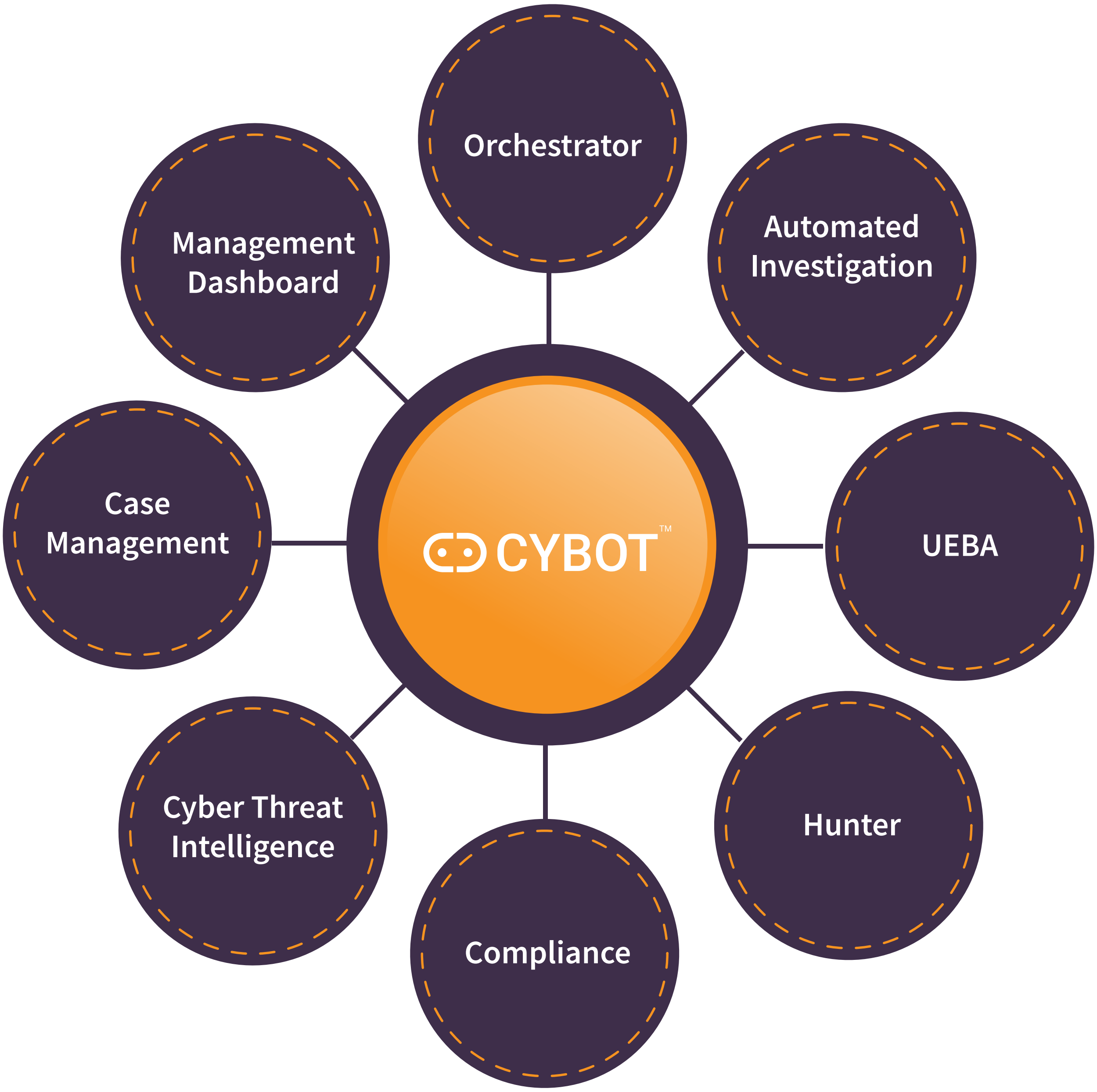
- This component now provides customers with an intuitive, real-time, and comprehensive view of your organization's cybersecurity landscape. The Management Dashboard offers insights into alerts and threats triggered by each security solution, along with detailed views of inbound and outbound traffic, complete with location maps. It also provides overviews of email and file activities, Active Directory events, user and host activities, and much more.

- The capabilities are virtually limitless, and we can tailor the dashboard to meet any specific requirements. With CYBOT's Management Dashboard, you can make swift, well-informed decisions like never before, all while maintaining a high-level perspective of our organization's security posture. This feature has significantly streamlined our cybersecurity monitoring and reporting processes, enabling you to respond proactively and effectively.

With a single, all-encompassing Threat Management Platform, you achieve far more than you ever imagined.

CYBOT will not only transform your approach to cybersecurity but will elevated your capabilities beyond our expectations.

You will stand equipped to face the dynamic and ever-evolving landscape of cyber threats with unwavering confidence, making the safety and security of our organization our top priority.



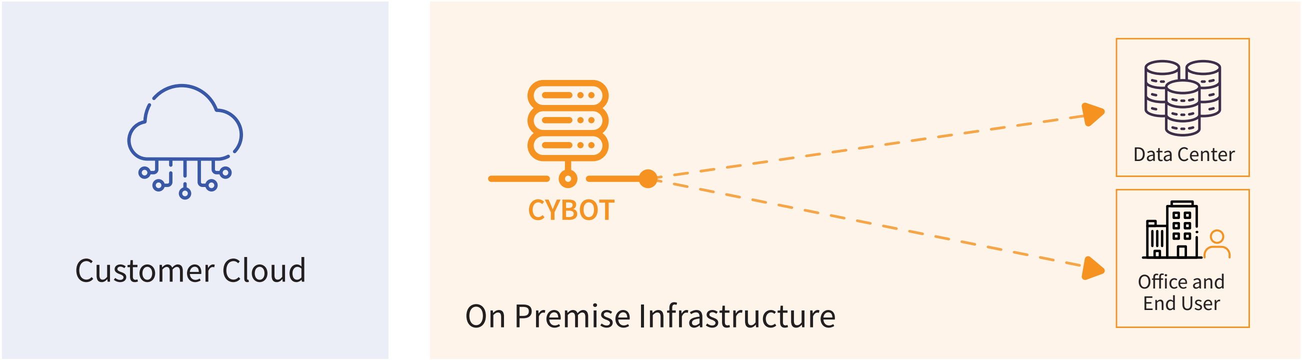
Robust Deployment and Hosting

ActiveBytes Innovations delivers unparalleled security solutions with a robust infrastructure and cutting-edge technology. Our hosting plans, CYBOT threat management platform, and Forti SOAR integration create a secure, reliable, and efficient cybersecurity environment for you.

- ✓ Fully On-Premises Hosting
- ✓ ActiveBytes Managed Cloud Hosting
- ✓ Customer-Owned Cloud Hosting
- ✓ Hosting with Your SIEM

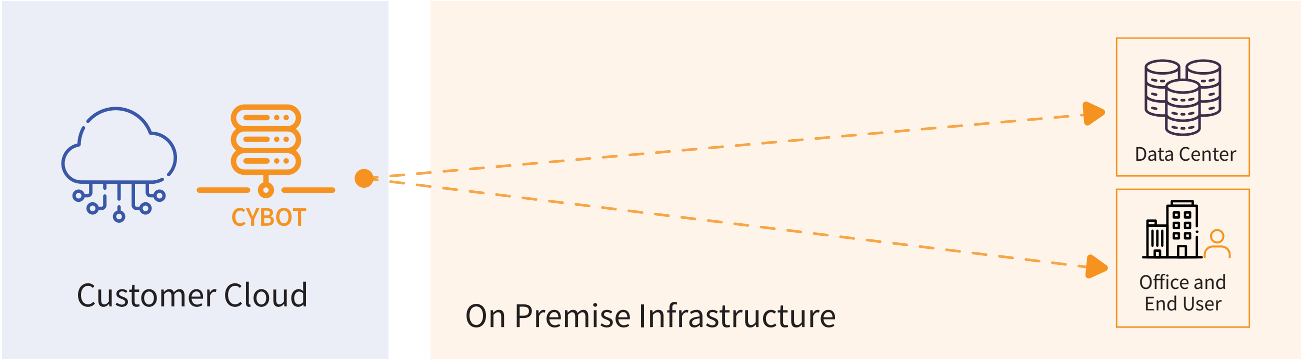
Fully On-Premises Hosting

- CYBOT installed and operated within your organization's infrastructure.
- All hardware, software, and networking managed by your IT team on your premises.
- Provides the highest level of control and data security.
- Ideal for organizations with strict compliance requirements or a preference for complete infrastructure ownership.



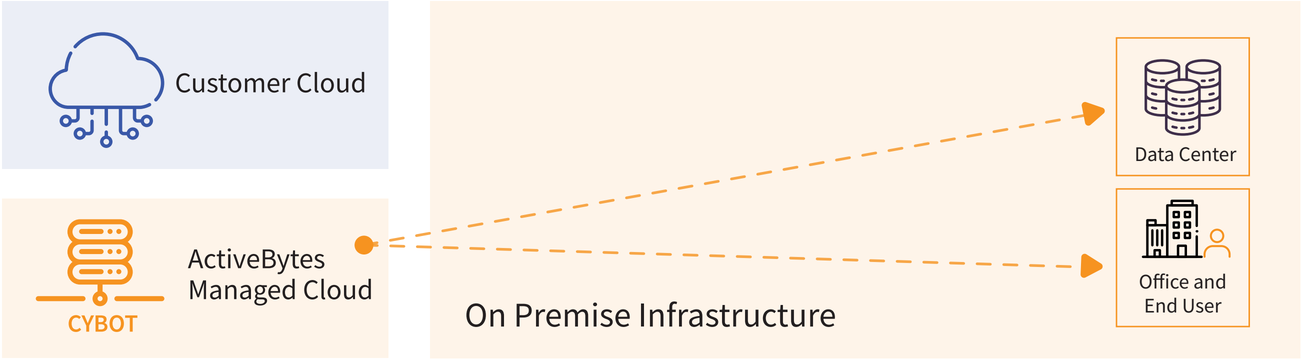
Customer-Owned Cloud Hosting

- CYBOT deployed and operated within your cloud infrastructure.
- Utilizes popular cloud platforms like AWS, Azure, or GCP.
- You take responsibility for provisioning and maintaining cloud resources.
- Leverages cloud scalability, flexibility, and cost-efficiency while retaining control over your cloud environment.



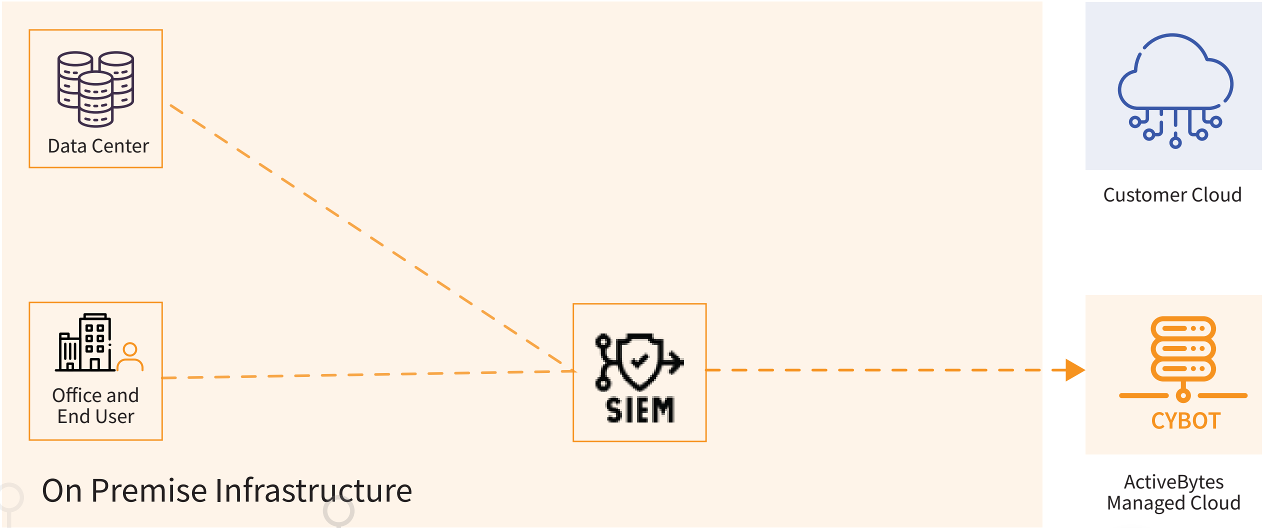
ActiveBytes Managed Cloud Hosting

- ActiveBytes deploys, manages, and maintains CYBOT in a cloud infrastructure.
- Handles infrastructure management tasks, including resource provisioning, monitoring, updates, and issue resolution.
- Offers convenience, scalability, and expert support.
- Allows you to focus on leveraging CYBOT for your business needs without operational burdens.



Hosting with Your SIEM

- Fully customized hosting that automates SIEM alerts to fit your unique requirements, maximizing threat detection and response capabilities.
- The synergy of your SIEM and Cybot's automated investigation empowers you with unbeatable security, ensuring strong protection against evolving threats.
- Maintains scalability and top-notch performance.



Flexible Hosting Options for Enhanced Data Control

Choose the right hosting model for control and data flexibility. On-premises deployment, customer-owned cloud hosting, and fully managed cloud hosting options are available to meet your needs.

Our platform **seamlessly overlays on top of your existing SIEM** infrastructure, augmenting its capabilities without disrupting its operations or requiring any modifications.

With this integrated approach, you can **maximize the value of your SIEM investment** while bolstering your security capabilities with our advanced threat management platform.

Support and Maintenance:

Comprehensive Support & Maintenance:

- No additional professional services charges during initial deployment
- Ongoing assistance and technical support provided by our expert team.
- Prompt resolution of technical issues, updates, and patches.
- Seamless hosting experience without extra costs for support and maintenance.

Hosting Flexibility:

- Range of hosting models available.
- Choose the option that suits your requirements and preferences.
- Empower your organization and achieve cybersecurity goals confidently.

CYBOT Testimonials

Saved from Legal Trouble: Thanks to CYBOT's CyKit and Data Retention

Industry	:	A Middle East-based government establishment
Size	:	5000+ employees.
Location	:	Middle East.

Problem:

Our government client had a challenge with employee attendance verification. An employee claimed regular attendance and an eight-hour workday, but their presence was unconfirmed, even with biometric login data. The Active Directory team needed to verify daily logins, but data from the critical day was unavailable due to a 20-day retention limit.

Solution:

CYBOT, our powerful threat management platform, collected AD logs with a 90-day retention period, following engineers' guidance. The security team used CyKit within the Investigate component to uncover the employee's login patterns. It revealed the user's frequent login and logout behavior without substantive work, aided by CYBOT's device process events and user activity dashboard. This led to a comprehensive activity report.

Legal Resolution:

The employee's lawsuit alleged mistreatment. CYBOT's data and investigations provided key evidence, leading to the lawsuit's dismissal and legal penalties against the employee for false claims. This highlights CYBOT's effectiveness in resolving attendance issues while protecting the organization's reputation in a legal context.

> *"Thanks to CYBOT's evidence, the judge dismissed the employee's lawsuit and imposed legal penalties for false claims."*

This success story highlights CYBOT's role in resolving attendance issues and protecting the organization's reputation in a legal context.

Massive Cost Savings, Thanks to CYBOT's Zero EPS

Industry	:	Oil and Gas
Size	:	10,000+ employees
Specialties	:	Oil, Petroleum, and Refinery

Problem:

The client faced challenges, including manual processes causing inefficiencies and alert fatigue, the absence of a SOAR platform hindering incident response, limitations of the traditional SIEM with data volume and costs, and the need to parse and normalize unstructured data from custom applications.

Solutions Implemented:

- **Assessment:** Evaluated existing infrastructure.
- **Customization:** Tailored CYBOT for unique security needs, including IoT threat detection.
- **Integration:** Seamlessly integrated CYBOT with existing SIEM and solutions.
- **Automation:** Implemented workflows for faster alert handling.
- **Data Lake Expansion:** Increased Data Lake capacity for unlimited logs.
- **Custom Data Parsing:** Optimized log collectors for unstructured data.

Results Achieved:

The implemented solutions have yielded significant results, including streamlined incident response with advanced SOAR capabilities, accelerated alert handling through automation, elimination of EPS limitations for scalable data handling, and efficient normalization of custom app data for unstructured data management.

> *"With CYBOT, we've seen incredible results. Our SOC efficiency has improved, with faster alert investigations and responses. We've also cut costs by eliminating EPS limitations, which saved us from overage charges.*
>
> *CYBOT's powerful capabilities have strengthened our cybersecurity, helping us stay ahead of threats. We're now more confident in our ability to protect our organization's digital assets and future."*

Efficient and Secure Data Storage for a Leading Banking Institution with CYBOT Data Lake

Industry	:	Banking
Size	:	5,000+ employees
Specialties	:	Banking, FinTech, Payment and Card

Problem:

Data Retention Expenses:

The top banking institution faced rigorous compliance requirements, necessitating on-premises data retention with extended periods.
Cloud storage costs were prohibitive, particularly for long-term data retention, straining the budget.

Solution:

- **CYBOT's Data Lake:** To resolve data storage and retention issues, we introduced CYBOT's Data Lake solution.
- **Private Cloud Hosting:** We hosted CYBOT's Data Lake within the client's private cloud environment, ensuring data sovereignty and control.
- **Optimized Architecture:** The Data Lake employed multiple nodes - hot, warm, and cold - for efficient data storage and retrieval.
- **Automated Data Management:** Data was dynamically moved between nodes following retention policies, optimizing storage usage.
- **Cost-Efficiency:** CYBOT's competitive pricing enabled the client to meet compliance requirements within budget constraints.

> *"With this solution, we, as a prominent banking institution, were able to securely store our data in CYBOT's private cloud-based Data Lake. The flexible architecture, featuring hot, warm, and cold nodes, ensured efficient data retention and access, all while keeping our costs manageable and meeting our stringent compliance requirements."*

Enhancing Cybersecurity with On-Premises CYBOT Implementation and Advanced SIEM Capabilities

Industry	:	A GCC based educational institution.
Size	:	10,000+ students.
Location	:	Middle East, with a global presence.

Problem:

SIEM Gap: No SIEM solution.

Data Challenge: No centralized data storage or alerting.

Limited Monitoring: Over-reliance on AV and network teams.

Data Residency Requirement: Must keep data within the country.

Expertise Gap: No in-house SIEM implementation expertise.

Solution:

- **CYBOT Implementation:** Deployed our comprehensive cybersecurity solution.
- **On-Premises Deployment:** Data stays within the organization, aligning with data residency requirements.
- **Onsite Implementation Team:** Smooth deployment without extra cost.
- **Advanced SIEM Capabilities:** Centralized log management, analysis, and real-time alerting.
- **Multi-Layered Security:** Enhanced overall security posture for proactive threat detection.
- **Customization:** Tailored to diverse operational units.
- **Training and Support:** Comprehensive support and training for effective utilization.

> *"Implementing CYBOT on-premises with advanced SIEM capabilities was a game-changer for our organization. It closed our SIEM gap, centralized log management, and enhanced our overall security posture. The on-site deployment team ensured a seamless transition, and the customization options met our specific needs. CYBOT has become an indispensable part of our cybersecurity strategy, delivering outstanding results."*

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