

MANAGED SECURITY OPERATION CENTER



**PROACTIVE DEFENCE
TO ACCELERATE COMPETENCE**



CONTENTS

03 Who We Are

05 About ActivesBytes Managed SOC Team

06 Managed Security Operations Portfolio

07 Managed SOC Services

21 Introducing Service Credits

24 Service Deployment

28 SOC Service Level Agreement (SLA)

30 Testimonials

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

ABOUT ACTIVESBYTES MANAGED SOC TEAM

Globally dispersed Managed SOC Team

ActiveBytes Managed SOC team is a global force, strategically dispersed across multiple locations to ensure a robust and comprehensive security posture. With well-equipped offices boasting the latest facilities, our team has a strong presence in India, specifically in Trivandrum and Bangalore, and in Kuwait.

Strength and Governance Model of MSOC Team

In catering to each client's unique needs, our Managed SOC operates on a shared service model.

Dedicated L1 analysts, L2, and L3 for every client in each shift, ensuring a personalized and robust approach to security operations.

This setup guarantees not only expertise but also scalability and efficiency, aligning with individual client requirements.

ActiveBytes Managed SOC team provide 24/7 managed security services, ensuring uninterrupted coverage for our clients

In case of any disruption, our robust business continuity plan seamlessly transitions operations to alternative locations.

Our commitment to global connectivity and business continuity sets us apart, guaranteeing the reliability of our managed security services.



MANAGED SECURITY OPERATIONS PORTFOLIO

Active Bytes takes pride in offering a comprehensive suite of bundled Managed Security Services, designed to fortify your organization's cybersecurity posture. Our integrated approach ensures proactive threat management and continuous monitoring, allowing you to stay ahead of evolving security challenges. Here's an overview of our bundled services:



MANAGED SECURITY SERVICES

Threat Detection and Response Service

Swift identification and neutralization of potential threats through real-time monitoring for rapid incident response and asset protection.



Investigate

Investigation lies at the core of our Threat Management Platform, fueling our SOC team's continuous vigilance. With cutting-edge analytics, over 500 preloaded use cases, and automated investigation for both SIEM and XDR alerts, we stay ahead of potential security threats, ensuring rapid and effective responses.

User Behavior Monitoring

Vigilant monitoring of user and host behaviors for anomaly detection, emphasizing early identification of security risks, particularly insider threats and unusual user activities.



UEBA

Our UEBA component is a key part of our Threat Management Platform, analyzing user and host behavior over time and alerting our SOC team to any deviations. Equipped with dashboards, manual investigation options, and more, this module provides comprehensive monitoring and response capabilities.

Threat Intelligence Service

Our in-house solution provides the latest threat information, supports use case creation, and facilitates CTI sharing. Regular updates keep the organization informed and proactive in response to evolving cyber threats.



Threat Intelligence

The Threat Intelligence component acts as a comprehensive repository, gathering the latest intelligence feeds from diverse channels. Alongside incorporating IOC feeds, it conducts thorough dark web monitoring customized to your organization's vulnerabilities and threats. This results in a remarkable 95% reduction in IOC hunting efforts.

Compliance Reporting Service

Adherence to industry regulations and standards with an inbuilt compliance component for active monitoring and addressing violations.



Compliance

Choose your preferred Compliance framework and ensure your organization is audit-ready. Gain access to control views tailored to your chosen security frameworks. The compliance component is designed to alert the SOC team of any violations within your organization.

Threat Hunting Service

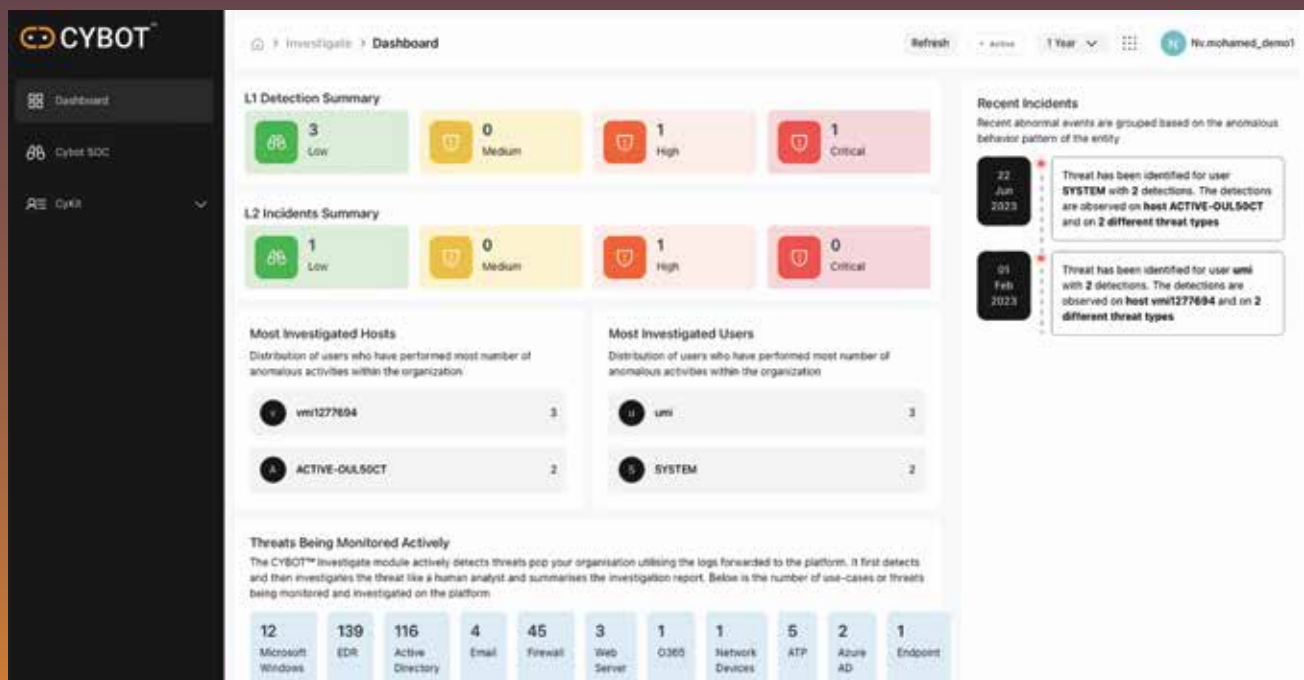
Proactive search for hidden threats using automated hunts and advanced algorithms, ensuring identification and neutralization at various stages.



Hunter

The Hunter component operates 24/7, conducting proactive Threat Hunting with efficiency. Leveraging advanced algorithms and machine learning, our portal swiftly identifies patterns and indicators of compromise, significantly enhancing the effectiveness and resource efficiency of threat hunting.

THREAT DETECTION AND RESPONSE SERVICE



24/7 Availability:

Dedicated managed threat detection and response team is available round the clock, leveraging the Threat Management Platform for comprehensive monitoring.

Rich Repository of Use Cases:

Benefit from a pre-loaded repository of 500+ proprietary use cases within our Threat Management Platform, enhancing the accuracy and efficiency of threat detection.

Automated Alert Investigations:

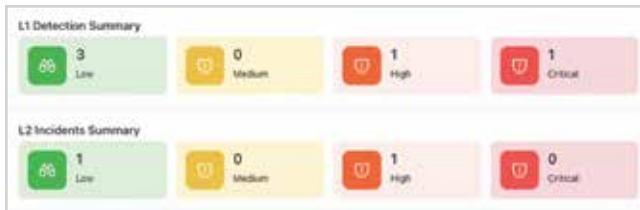
CYBOT automates the investigation of all alerts, a pioneering feature that significantly reduces response time by providing analysts with quick, informed reports for efficient decision-making.

Automated SIEM Alert Investigation

For existing SIEM solution in place, we can seamlessly ingest and investigate alerts using our Threat Management Platform for automated investigation.

Advanced Threat Mitigation

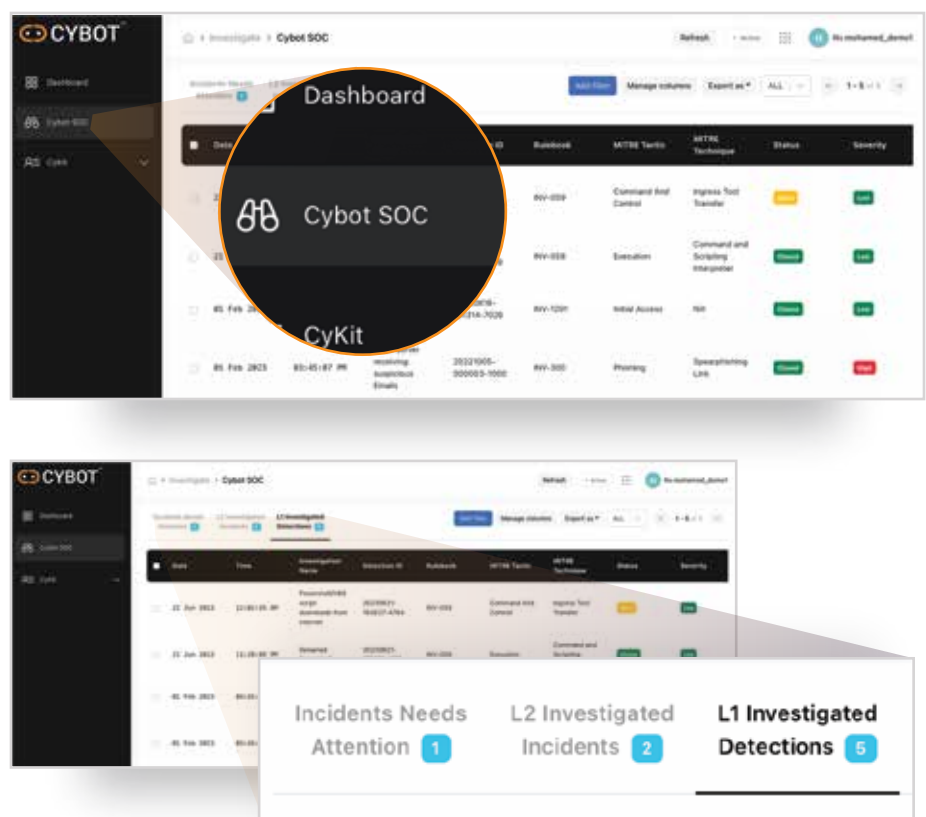
Our service goes beyond detection and response, incorporating advanced threat mitigation functionalities. This proactive approach ensures real-time responses to potential threats, adding an extra layer of defense to neutralize and minimize their impact on your systems and network.



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

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:

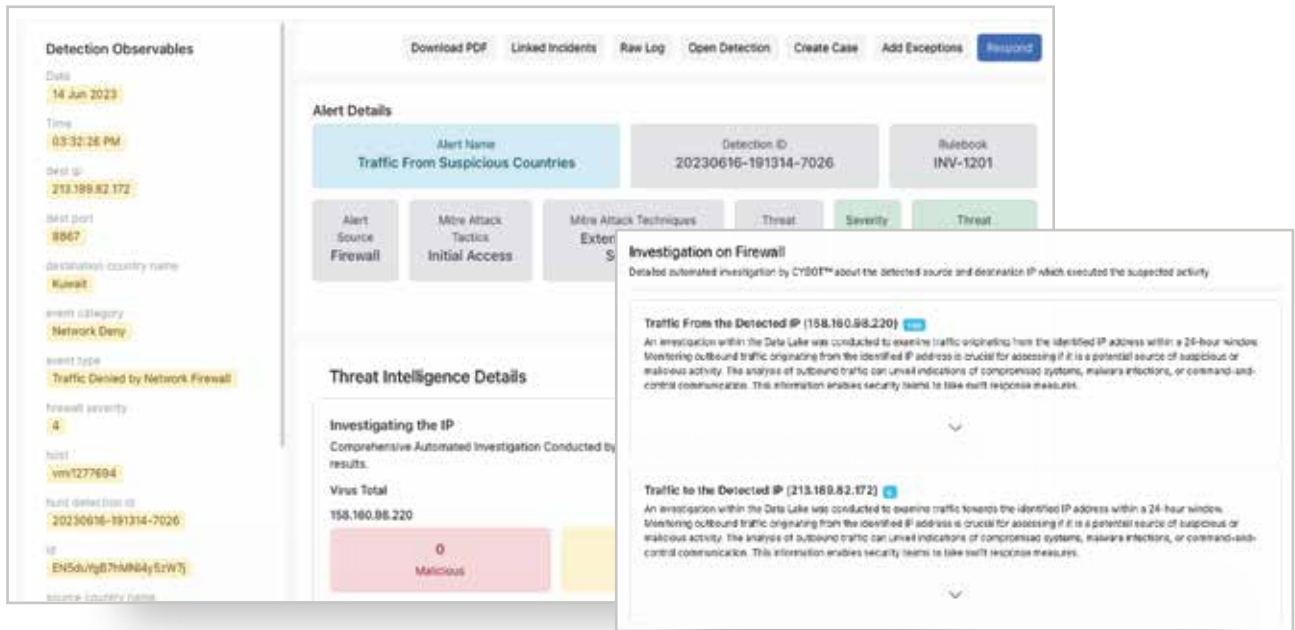
Utilize advanced filters to precisely refine your data, with the added convenience of saving and loading filters for future use.

Customizable Display:

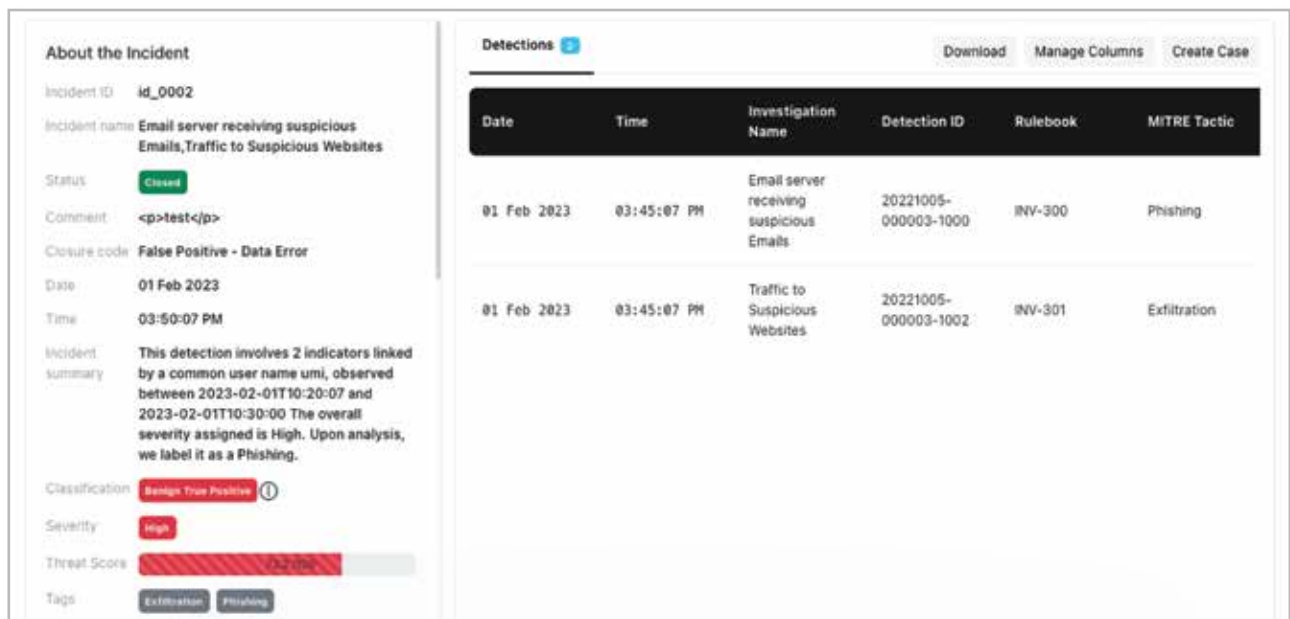
Enhance your viewing experience by tailoring the display to your needs. Choose the relevant columns for a more focused and efficient presentation.

Integrated Reporting:

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



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.

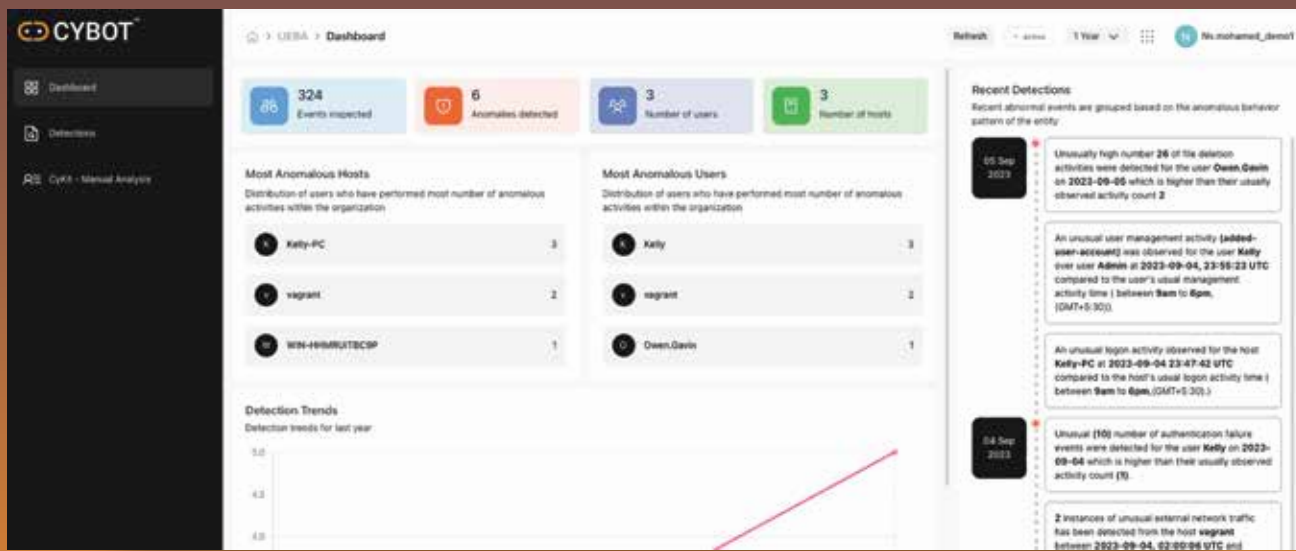


Incidents are automatically classified, assigned a threat score, and note preparation is fully automated, presenting analysts with incidents requiring minimal investigation.

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

UEBA MONITORING SERVICE

Our Managed SOC team is equipped with advanced User and Entity Behavior Analytics (UEBA) capabilities, allowing us to monitor and analyse user and host behavior for any anomalies. Detections triggered by the UEBA component within the Threat Management Platform undergo thorough investigation by our skilled analysts.



Detection and Analysis:

- The UEBA component within our Threat Management Platform is adept at identifying unusual patterns and behaviours associated with user and host activities.
- Our analysts meticulously analyse UEBA alerts to differentiate between normal and potentially malicious activities.

Dedication to Resolution:

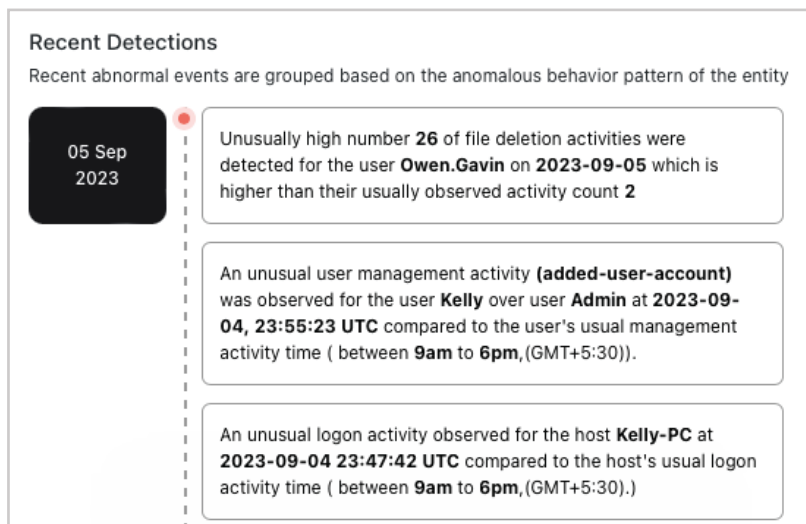
- Our dedicated team ensures that no alert is left unattended. Every detected anomaly undergoes a thorough investigation to maintain the integrity of our monitoring services.
- We are committed to continuous improvement, refining our processes and responses based on evolving threat landscapes and client feedback.

Client Notification and Follow-Up:

- Upon the detection of anomalies that require attention, our SOC team adheres to defined Service Level Agreements (SLAs) to promptly notify the respective clients.
- Our commitment doesn't end with notification. We follow up on each case with the client until resolution is achieved, ensuring transparency and client satisfaction.

Integrity and Continuous Improvement:

- Our focus extends beyond detection to resolution, aiming to maintain the integrity of our monitoring services and deliver comprehensive security solutions.
- We are continuously evolving, incorporating feedback and staying abreast of industry best practices to enhance our UEBA monitoring capabilities.



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.

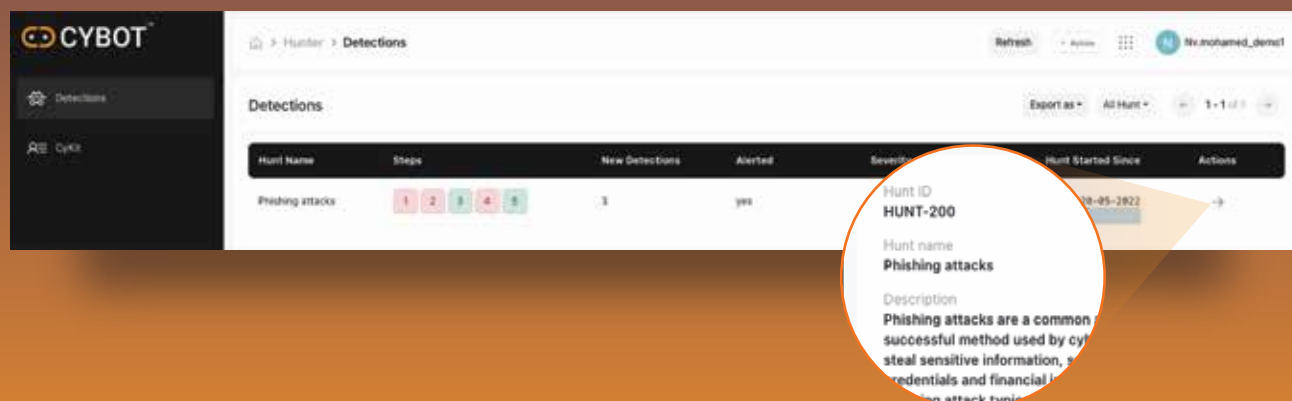
Explore the Most Anomalous Hosts and Users effortlessly. Select entities directly from the dashboard to instantly view detailed detections, providing a user-friendly feature for swift response to potential threats.

Instantly view and understand recent abnormal events, grouped by entity behavior patterns for quick threat identification and proactive response.



THREAT HUNTING SERVICE

Our Threat Hunting Service offers a comprehensive defense strategy without the need for additional spending on external threat hunters. With over 25 automated hunting scenarios utilizing advanced correlation logs, algorithms and machine learning, our Managed SOC team ensures swift identification and proactive mitigation of potential threats at any early stages. This cost-effective solution enhances security, eliminating the necessity for external resources while maintaining a high level of threat detection and response.



Swift Incident Response

- Our Managed SOC team monitors these automated hunts diligently.
- Any initial attempts by attackers are swiftly identified and halted, preventing further damage.

25 Automated Hunt Scenario

- Over 25 hunting scenarios are loaded into our Threat Management Platform, ensuring continuous vigilance.
- Advanced algorithms and machine learning enable automated threat detection, optimizing our response capabilities.

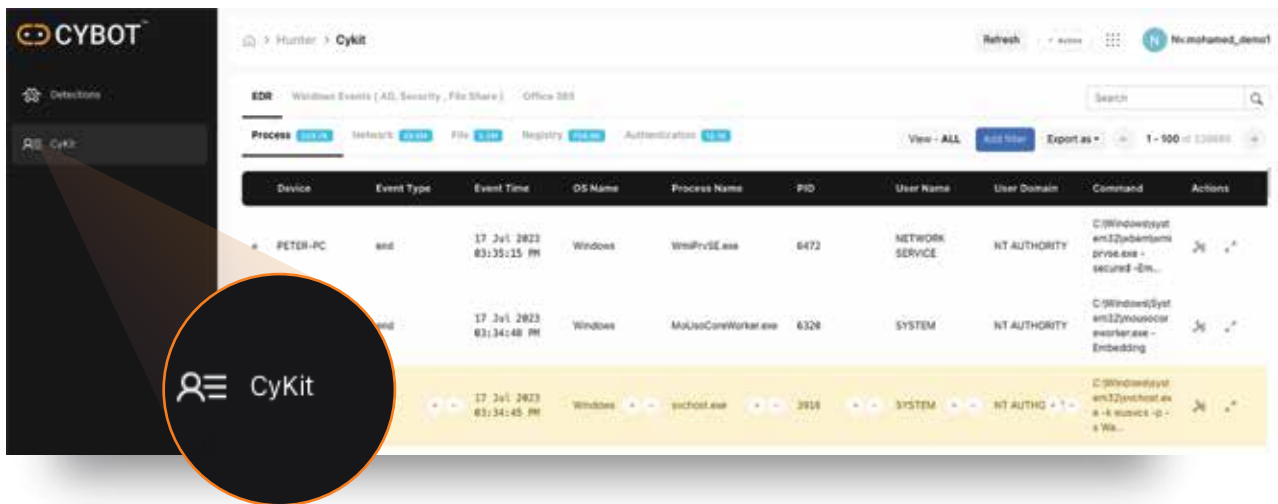
Proactive Mitigation

- This proactive approach ensures rapid incident response and mitigation.
- By stopping potential threats at the early stages, we enhance overall security and minimize the impact on your organization.

Our Threat Hunting Service combines automation with human expertise, providing a robust defense against evolving threats and ensuring the integrity of your security infrastructure.

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.

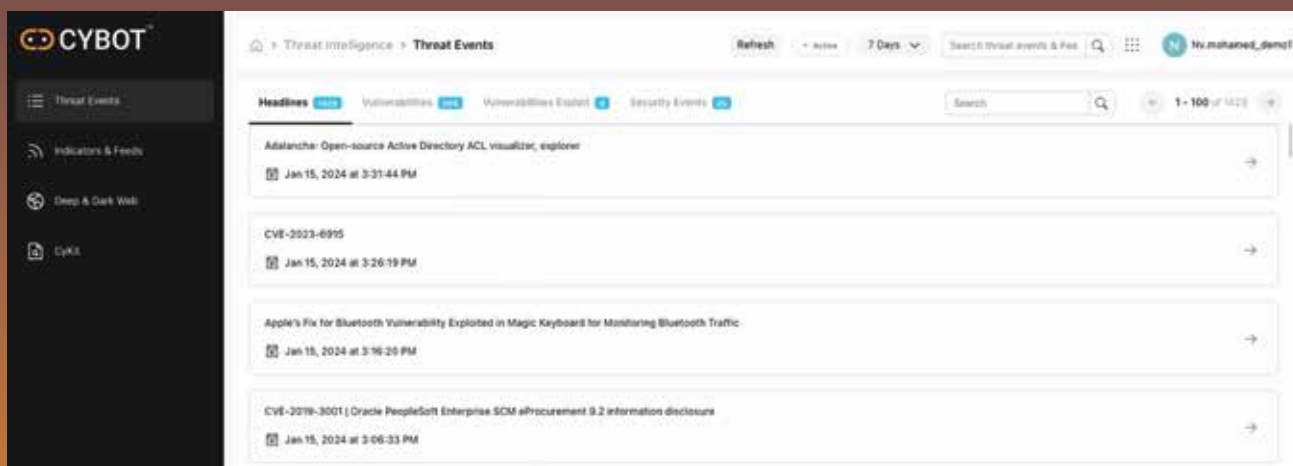
Key features include focused analysis with data source filtering, anomaly identification, filter preservation for future use, and seamless data export for investigation or reporting.

Hunter CyKit enables efficient and comprehensive data analysis.



THREAT INTELLIGENCE SERVICE

No need to rely on external OSINT CTI subscriptions – our Managed SOC team is equipped with a robust Threat Intelligence (TI) component within the Threat Management Platform. This internal component enhances the SOC team's capabilities, providing comprehensive CTI support for all their needs.



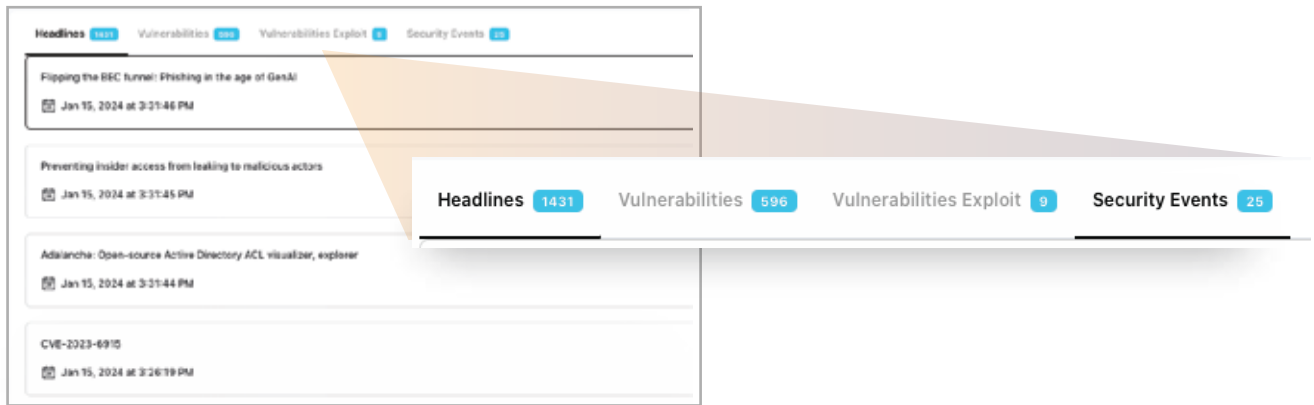
WEEKLY CTI NEWSLETTER

WEEKLY AUTOMATED IOC HUNTS

DEEP AND DARK WEB MONITORING

- Ensure the platform stays up-to-date with the latest threat information.
- Ensure the team operates seamlessly, leveraging the integrated TI component.
- Equip the SOC team with the intelligence necessary to proactively address emerging threats.
- Enable the SOC team to make swift and informed decisions based on real-time threat intelligence.
- Provide actionable insights derived from threat intelligence to keep the organization informed.
- Foster a culture of transparency and collaboration in addressing security concerns.
- Regularly share CTI information with the organization to enhance overall awareness.
- Perform ad-hoc IOC hunts to identify any unknown threats.

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.

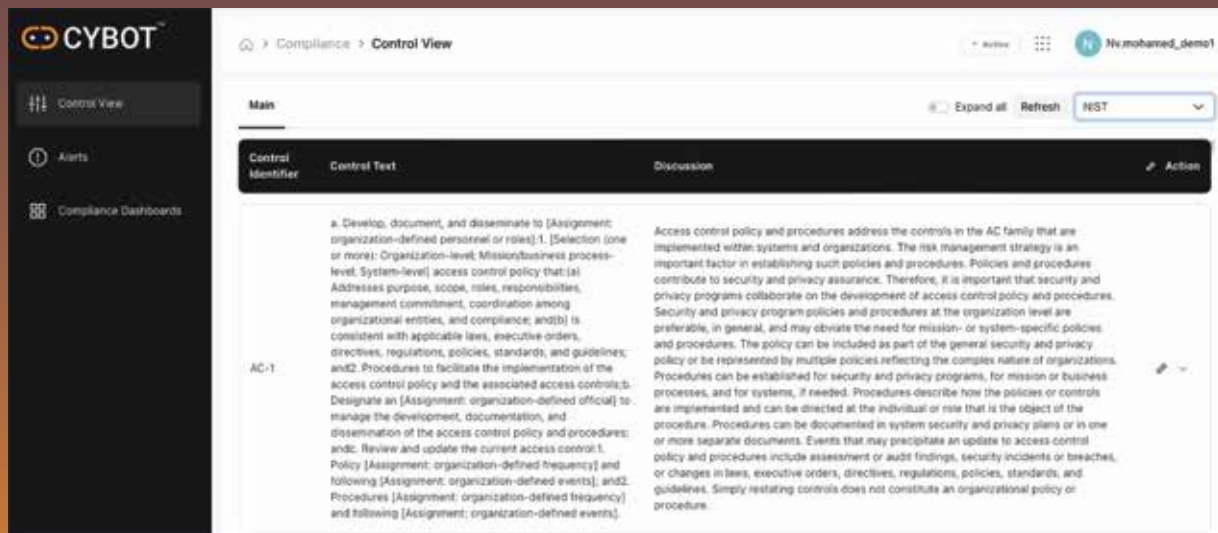


Stay informed with CYBOT™—our free CTI component delivers real-time updates on global cyber threats, vulnerabilities, and exploits. Effortlessly access insightful headlines to enhance your organization's security posture. With CYBOT™, receive timely and relevant intelligence without the hefty price tag.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



COMPLIANCE REPORTING SERVICE

Our Managed SOC team goes beyond threat detection to actively monitor and address compliance violations. The Compliance component, integrated into our Threat Management Platform, is seamlessly managed by both our team and your organization.



Compliance Control View

- Our compliance module offers a streamlined approach to managing regulatory requirement
- Users can access a centralized Compliance Control View, providing a consolidated display of relevant controls.
- Tailor your compliance efforts by choosing the required framework, ensuring a customized and effective approach.

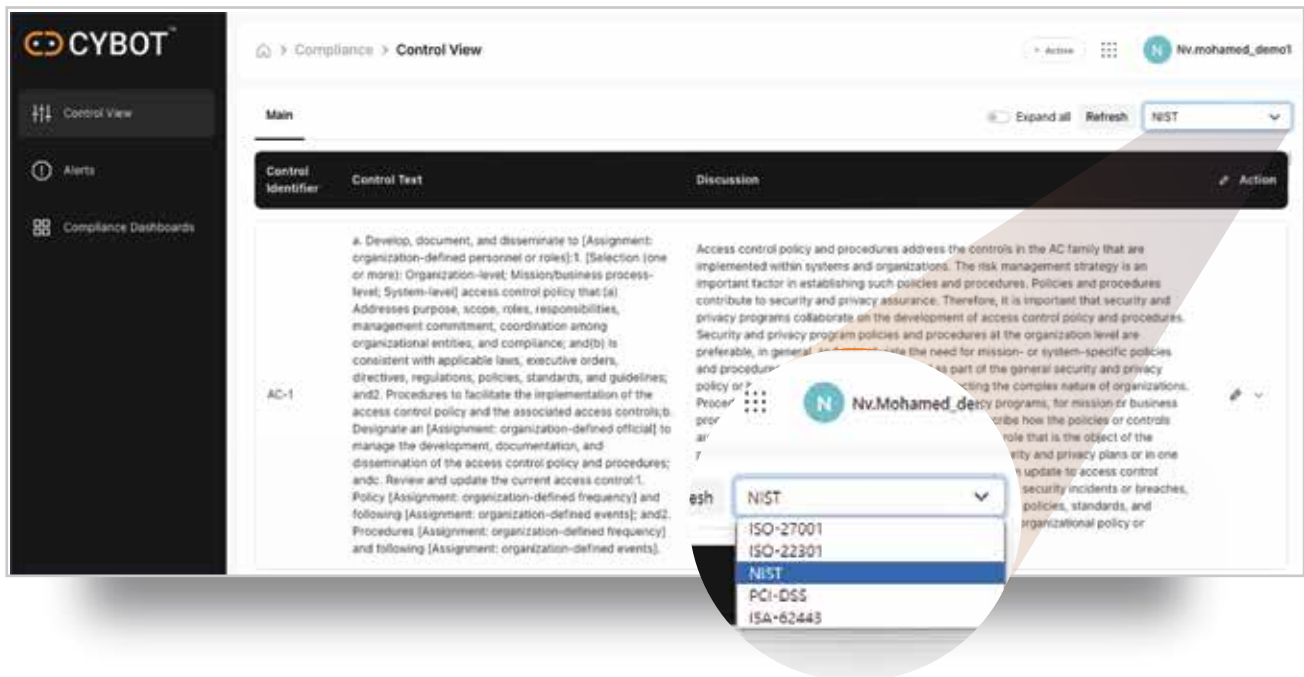
Compliance Alerts

- Instant alert activation when logs fulfill predetermined criteria, ensuring continuous vigilance in standards adherence.
- Swift detection and resolution of compliance concerns, aiding risk management efforts.
- On-demand creation of tailored compliance alerts, accommodating unique organizational needs and regulatory nuances

Compliance Dashboards

- Gain real-time insights into compliance status through intuitive dashboards.
- Monitor key compliance metrics and track progress towards objectives.
- Leverage customizable reports for comprehensive analysis and audit readiness.

By actively managing compliance components within our Threat Management Platform, we provide a collaborative and proactive solution, preparing your organization for audits and ensuring that compliance violations are promptly addressed.



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.

✓ Prepare for Audits

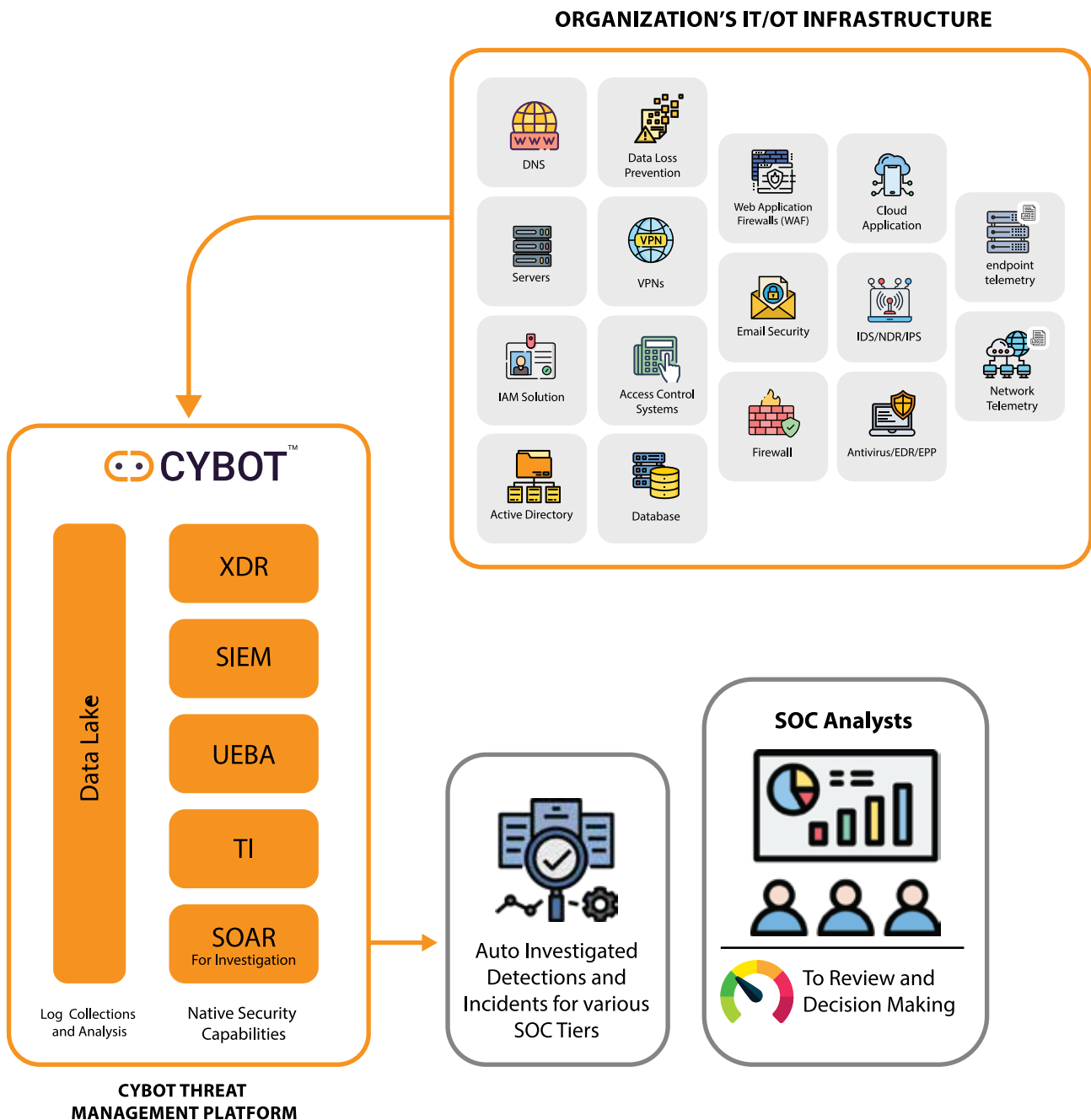
✓ Inbuilt Compliance Components

✓ Proactive Compliance Reporting



MANAGED SOC TECHNOLOGY, DESIGN AND PLACEMENT

At ActiveBytes MSOC, we're transforming security operations through our innovative approach. Our integrated technology seamlessly combines native SIEM and XDR capabilities into a unified platform called CYBOT, revolutionizing the landscape of security solutions.



A background image showing a pair of hands holding three glowing gold stars against a dark blue background with bokeh light effects and falling star particles.

INTRODUCING SERVICE CREDITS

Our Service Credits is a game-changing innovation offering **free service credit points with each Managed SOC subscription, redeemable for tailored supplementary services** to enhance your cybersecurity defenses and meet specific organizational needs.

Flexibility

Service Credits offers additional services for specific security challenges and advanced capabilities beyond the standard offering.

Customization

Tailor your cybersecurity roadmap with specialized services using the Service Credits to match unique requirements and industry needs

Added Value

Maximize ROI in Managed SOC service, unlocking expertise's full potential with the tangible value provided by the Service Credits

✓ 365 Days validity

✓ Redeemable

✓ Optimal Solution

Service Credits

Experience the power of our 24/7 Managed Security Operations Center (MSOC) monitoring and a range of supplementary cybersecurity services. Safeguard your valuable assets and mitigate risks with our holistic approach. Avail add-on services using service credits or opt for direct availing if you don't have credits.

Add-On Service	Description of Service	Scale	Credit
Penetration Testing - Blackbox	Assess the security of applications through Blackbox testing methods.	per asset/URL/IP	30
Penetration Testing - Grey box	Conduct comprehensive assessments of applications with limited knowledge.	per asset/URL/IP	50
Penetration Testing - Infrastructure	Evaluate the security of your infrastructure through targeted testing.	per asset/URL/IP	1.5
Internal Vulnerability Assessment (VA)	Identify vulnerabilities within your internal network and systems.	per asset/URL/IP	0.2
External Vulnerability Assessment (VA)	Detect vulnerabilities from an external perspective to safeguard against external threats.	per asset/URL/IP	0.2
Red Teaming Activity	Simulate real-world attacks to evaluate the effectiveness of your security controls.	per activity	200
Purple Teaming Activity	Foster collaboration between the red and blue teams to improve overall security effectiveness.	per activity	200
OSINT Threat Exposure Assessment	Evaluate your organization's exposure to threats based on Open-Source Intelligence (OSINT).	per activity	100
Threat Modelling	Identify potential threats and vulnerabilities to your systems and applications.	per activity	100
Threat Hunting Service	Proactively search for and identify potential threats within your environment.	per activity	500

Add-On Service	Description of Service	Scale	Credit
Wireless Penetration Testing	Assess the security of your wireless networks and devices.	per asset/URL/IP	50
Security Configuration Assessment	Evaluate the configuration settings of your systems for security weaknesses.	per asset	4
Compliance Audits	Conduct audits to assess compliance with standards such as ISO, NIST, PCIDSS, BCMS.	per activity	300
Automated Investigation	Perform automated investigation for each incident or alert.	Per Automated investigation	30
Custom Hunt Scenario	Create and execute custom threat hunting scenarios for targeted investigations.	Per Custom Hunt scenario	30
User/Host Addition to UEBA List	Add each user or host to the User and Entity Behavior Analytics (UEBA) list for monitoring.	Per user/Host added to UEBA watch-list	1
Custom Dashboard (Investigate or Compliance)	Create each custom dashboard in the Investigate or Compliance module.	Per custom dashboard in investigate or compliance	10
Incident Response	Receive incident response services for each incident requiring assistance.	Per Incident	200
Onboarding and Monitoring	Onboard and monitor each server, application, or device for security management.	Per device/server/application	100
Professional Services (PS)	Avail professional services for specific security needs and consultation.	Per day	40



SERVICE DEPLOYMENT

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

✓ Customer-Owned
Cloud Hosting

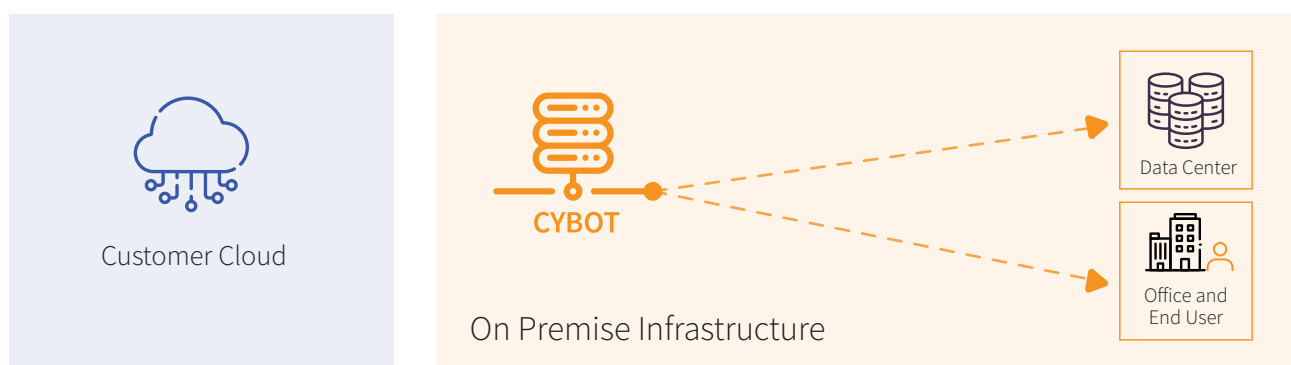
✓ ActiveBytes Managed
Cloud Hosting

✓ Hosting with
Your SIEM



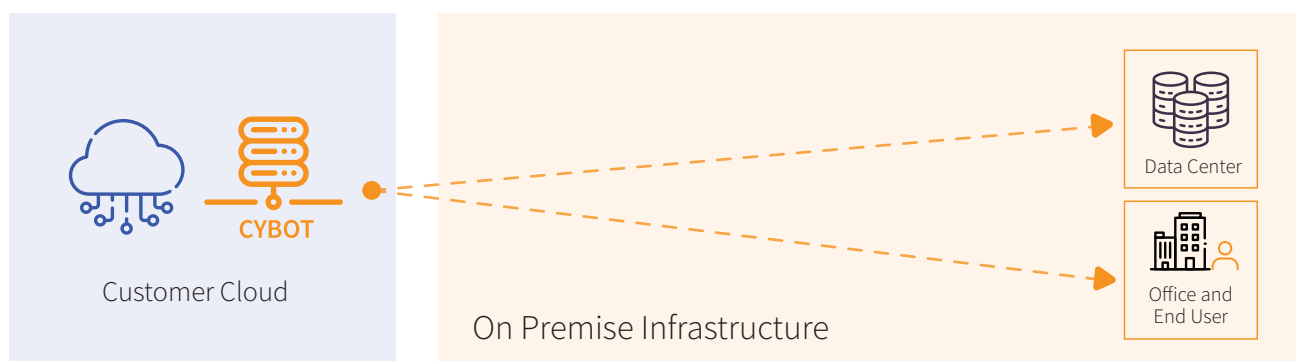
Fully On-Premises Hosting

- 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.



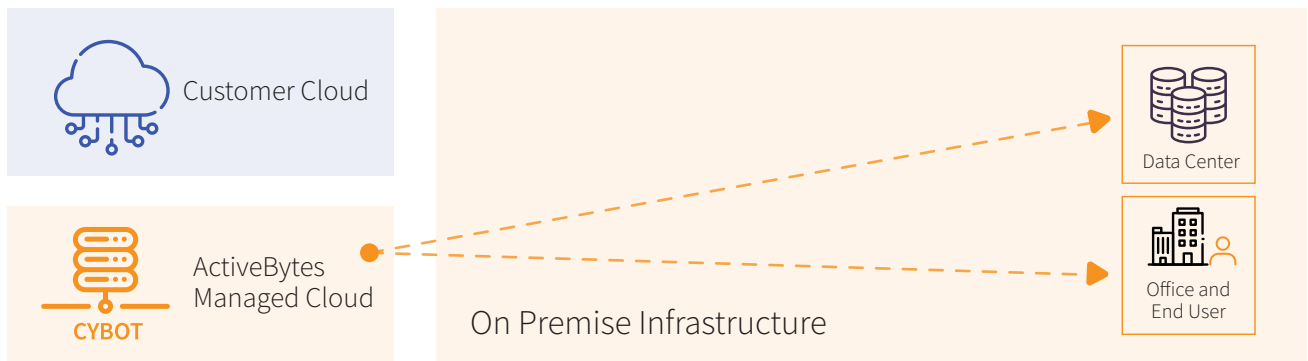
Customer-Owned Cloud Hosting

- 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.



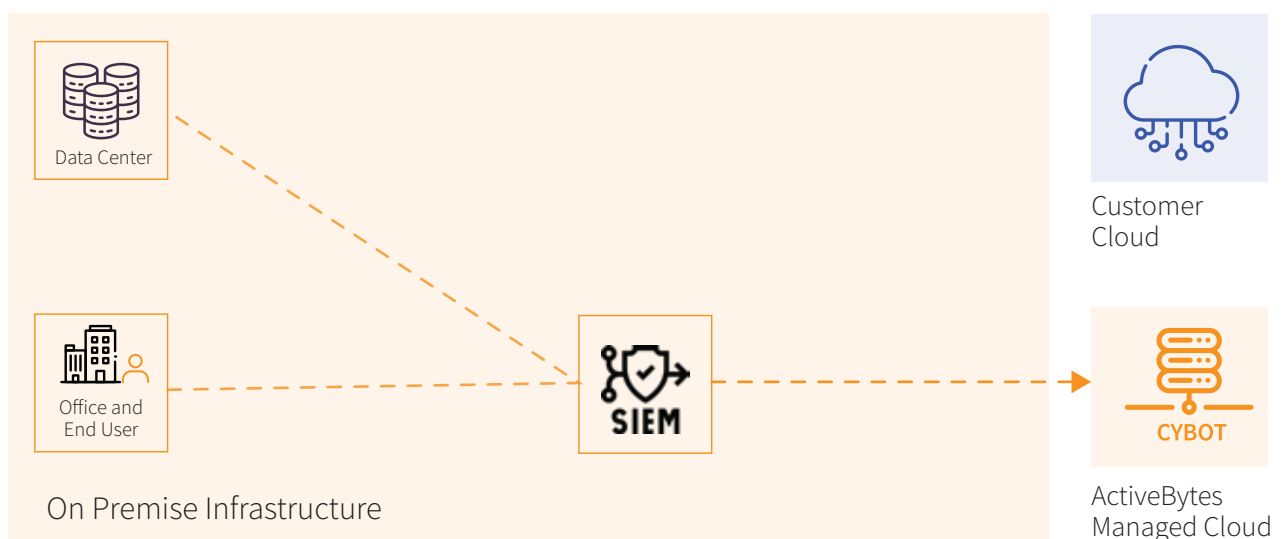
ActiveBytes Managed Cloud Hosting

- 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.





SOC SERVICE LEVEL AGREEMENT (SLA)

Our Managed SOC teams adhere to a stringent Service Level Agreement (SLA) designed to provide our clients with the utmost assurance in thwarting cyber threats. The SLA matrix, tailored to each client's specific needs, outlines our commitment to timely response, mitigation, and resolution. With this proactive approach, we ensure that potential attacks are swiftly identified and effectively neutralized, guaranteeing a robust defense mechanism for our clients. Our focus on SLA compliance underscores our dedication to preventing and mitigating security incidents, offering a high level of confidence in the effectiveness of our managed security services.

TTA**"Time to Acknowledge"**

Enhancing incident response capabilities by measuring the team's quick responsiveness in recognizing and acting on detected or reported threats.

TTE**"Time to Escalate"**

Efficiently measuring how long it takes for a threat or incident to be escalated to higher-level authorities or experts, ensuring effective handling through timely involvement of necessary resources.

TTN**"Time to Notify"**


Timely duration for the SOC team to notify relevant stakeholders once a security incident is confirmed, facilitating prompt response, collaboration, and informed decision-making.

Severity	Description	TTA	TTE	TTN
Critical P1	Alerts triggered from HVA assets or Users	15 minutes	30 minutes	30 minutes
High P2	Potential threats not mitigated	15 minutes	45 minutes	60 minutes
Medium P3	Possible threats mitigated; root cause analysis required	30 minutes	90 minutes	120 minutes
Low P4	Low impact activities requiring validation	60 minutes	120 minutes	240 minutes
Information	Alerts during stabilization phase	N/A	N/A	N/A

*SLA matrix will be finalised as per client requirement



TESTIMONIALS



Active Bytes MSOC: Safeguarding with Expertise, Your Trusted Holiday Cybersecurity Guardians.

Industry : Oil and Gas
Size : 5000+ Employees
Location : Middle East with Presence in Europe

Incident Overview

During the Christmas vacation, a period known for increased cyber threats, Active Bytes MSOC demonstrated proactive cybersecurity measures. Despite heightened risks, our team vigilantly monitored clients. Unfortunately, a user fell victim to a deceptive Christmas coupon phishing email, unknowingly triggering the delivery of a ransomware variant. The malicious software quickly infiltrated the system, initiating execution and file decryption.

Challenges Faced

Confronted with a multi-stage attack, our MSOC team promptly assessed the incidents in CYBOT, confirming the severity of the threat. A delayed response from the client's IT department escalated the urgency of the situation.

Our Response

Without waiting for further assistance, our SOC team initiated Incident Response (IR). Utilizing Cybot's Investigate module, specifically the 'respond' feature, the team isolated the compromised machine, preventing the malware's spread. Additionally, CYBOT was employed to efficiently block remote URLs associated with the attack.

”

What the Client Says

We extend our gratitude to Active Bytes MSOC for their swift and decisive actions. Despite a delayed response from our IT team during the holidays, the MSOC professionals used Cybot's 'respond' feature to isolate the infected machine, preventing further spread. Their quick thinking, including blocking remote URLs, mitigated the risk. Thanks to their expertise, what could have been disastrous was contained, and multiple machines were spared from infection. The MSOC team's dedication and expertise truly made them our holiday cybersecurity heroes. We are grateful for their outstanding service!



MSOC's Swift Response Strengthens Our Cyber Defenses in Manufacturing

Industry : Manufacturing
Size : 2000 + Employees
Location : Egypt

Incident Overview

Despite a robust security system, a manufacturing company encountered an issue when an unauthorized person disabled protection on an unattended test computer. This action went unnoticed by the client's EDR solution due to the disabling, hindering the creation of a multistage incident. Fortunately, the MSOC team detected the anomaly on an unrecognized system and initiated an incident report. They continued monitoring the activities on the compromised computer and discovered the attacker's attempt to establish persistence through scheduled tasks and lateral movement. The SOC team, recognizing the breach, promptly launched an investigation to uncover the attacker's intent.

Challenges Faced

The disabling of the antivirus (AV) solution posed a significant challenge, limiting incident creation and visibility. The compromised system was left vulnerable to potential threats.

Our Response

Upon identifying the incident in CYBOT, our SOC team promptly initiated an IR report. The IT admin was informed of the attack, revealing their lack of awareness. The affected machine, connected to the main network, was swiftly isolated, and the MSOC team took immediate action by removing malware, re-enabling the EDR solution, and enhancing security measures. They introduced new use cases to detect and prevent similar attempts, expanded their monitoring scope, and updated the asset list for comprehensive protection.

”

What the Client Says

We extend our gratitude to the MSOC team for their proactive identification and neutralization of the attack. Their ability to generate a comprehensive incident report was invaluable, providing crucial insights that were shared with our management team. This incident served as a valuable lesson, and the MSOC team's assistance was instrumental. They not only helped us navigate the incident efficiently but also proactively deployed multiple use cases based on this experience. Their commitment to our cybersecurity is commendable.

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.

ActiveBytes Innovations

Sharjah Media City, Sharjah, UAE, Dubai, UAE +971 505676727

www.active-bytes.com