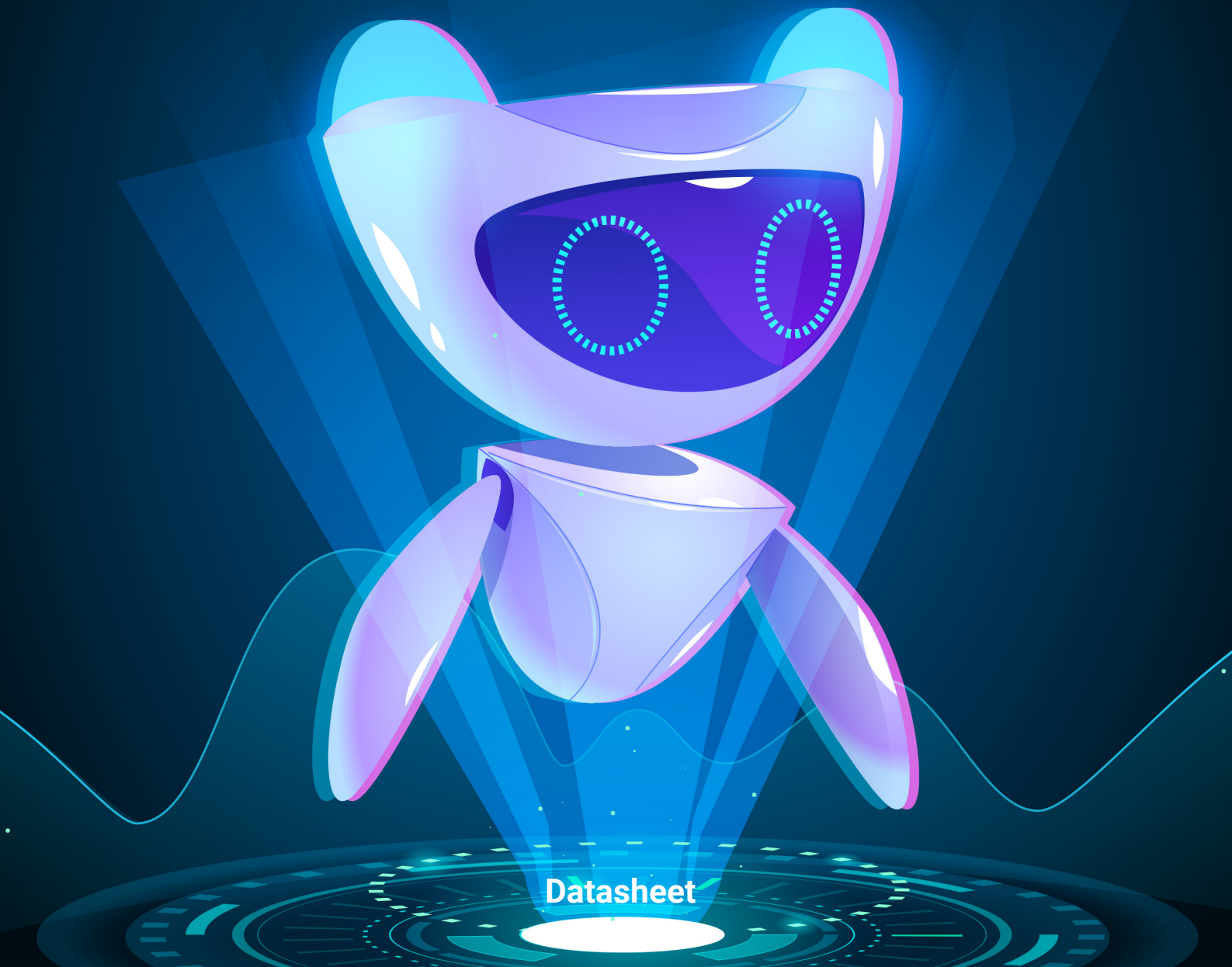
CYBOT™

Automated Investigation & Hunting Platform



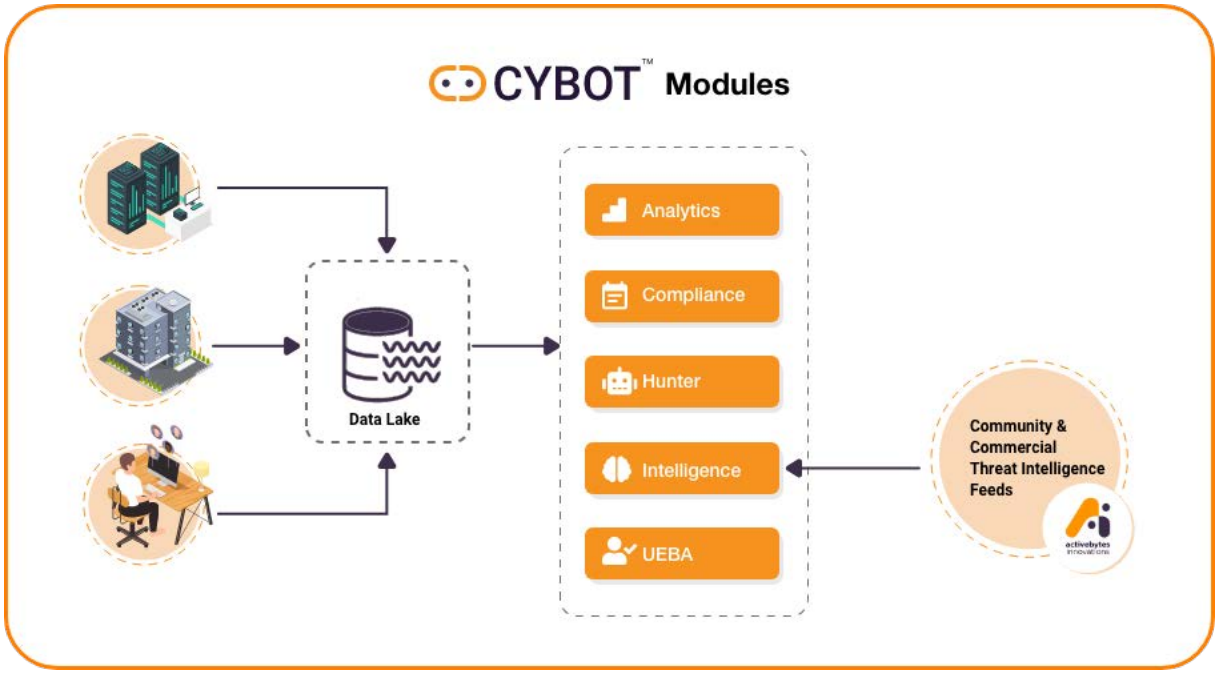
Datasheet

Overview

activebytes innovations

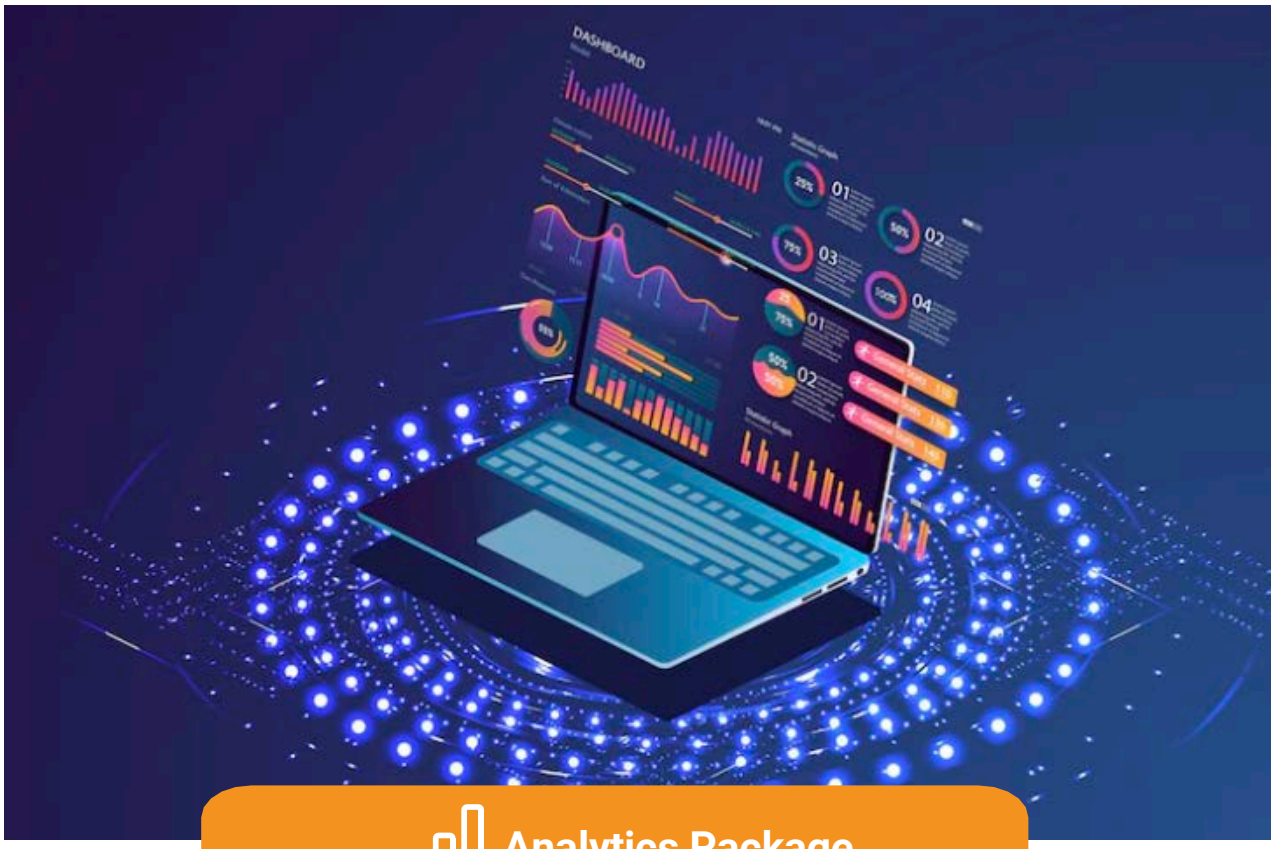
www.active-bytes.com

About the CYBOT™



The working of CYBOT™ is basically divided into five parts:

- First, the Analytics Platform with an analytics engine where the data from network sensors and endpoint sensors get collected. The data from log sources are contextualized, structured and then displayed in user-friendly dashboards for the analysts.
- The second part is the Threat Intelligence Platform, which collects feeds like IOCs and TTPs from community and commercial sources and integrates them with the Threat Hunting Platform. These security intelligence, vulnerability and exploit intelligence feeds add to the adaptive nature of CYBOT™ automated playbooks, thereby making them very effective in hunting and investigation.
- The third part is the Automated Threat Hunting Platform that automatically and intelligently investigates the suspected observables from your enterprise logs in the analytics engine of the analytics platform and correlates them with the known
- The fourth part is the UEBA module, designed to perform behavior analysis of user & hosts with machine learning algorithms. Data from the data lake is fed into the module for prediction of anomalies.
- The fifth part is the Compliance module designed to aid organizations and security teams to meet regulatory standards such as ISO 27001, PCI DSS & NIST through the built-in compliance dashboards and Active monitoring. The data from the data lake, that deviates from the required standard is triggered and displayed in detail. IOCs, patterns and intelligence feeds. After the automated investigation by intelligent playbooks, the result of the hunt is displayed in dashboards at the granular level for the analysts. CYBOT™ is also designed with an option to respond to a threat by clicking a button. This saves time for analysts to perform other critical actions like neutralizing the adversary element that has breached your IT infrastructure security system.



Analytics Package

The CYBOT™ Platform includes a Big Data Analytic Engine, that can store and analyze huge amounts of enterprise raw data which is beyond human capability, with best-in-class analytics and processing capability. The logs collected from the endpoints, servers and network of the enterprise IT infrastructure is contextualized and formatted before performing automated analysis. Then it's displayed as Dashboards at the granular level details for analysts and has information related to file modification, processes, Hash, URL, network traffic, uncommon ports, IP, etc. at the granular level. The data of suspicious nature undergoes further drill down automated investigation and hunting in CYBOT™'s Threat Hunting Platform.

We've made hundreds of Dashboards and Alerts out of the box for both compliance and security analytics use cases. You will have access to our value-added provision of content-library where we update new dashboards and alerts use cases to continuously improve the intelligent automated hunting capability of CYBOT™ and thereby protect your infrastructure from the latest threats.

To view Datasheet of the Analytics Package

CYBOT™ Intelligence

CYBOT™ has a Threat Intelligence Platform which continuously gets updated with knowledge of the latest cyber security attacks, vulnerability and exploit intelligence and their details in the industry worldwide. This makes CYBOT™ adaptive and highly efficient in automated investigation and detection of threats among the huge logs by correlation. The inputted Information from both commercial and community threat intelligence events, news and vulnerabilities is accessible in the CYBOT™ platform to both technical and non-technical teams in the form of user-friendly dashboards, printouts and emails. This provides analysts and incident responders with quality intelligence information, thereby helping them to update their own environment's security framework.

CYBOT™ is designed to avoid repeated investigation on identical observables including IOCs and patterns, thereby reducing false-positives and noise to the analysts. We extend our security specialist's hands for threat intelligence services like domain takedown.

To view Datasheet of CYBOT™s Intelligence

CYBOT™ Hunter

Every data from the enterprise log source cannot be analyzed or subjected to manual threat hunting as it is huge raw data. CYBOT™ is designed to handle any amount of data from every corner of an IT environment, thereby providing a fully efficient automated hunting and investigation platform. The data collected via sensors from the server, network and endpoints of the enterprise environment are fed into the Analytical Engine. The logs are then analyzed in the analytics platform, every suspicious data undergoes automated hunting and end-to-end investigation by built-in intelligent playbooks of CYBOT™. The result from the automated hunts are displayed as dashboards with granular information of the suspected log such as techniques and tactics of the adversary, observables detected, IP information, Hash details, Threat score calculated, URL information, hosts details, process details, etc.

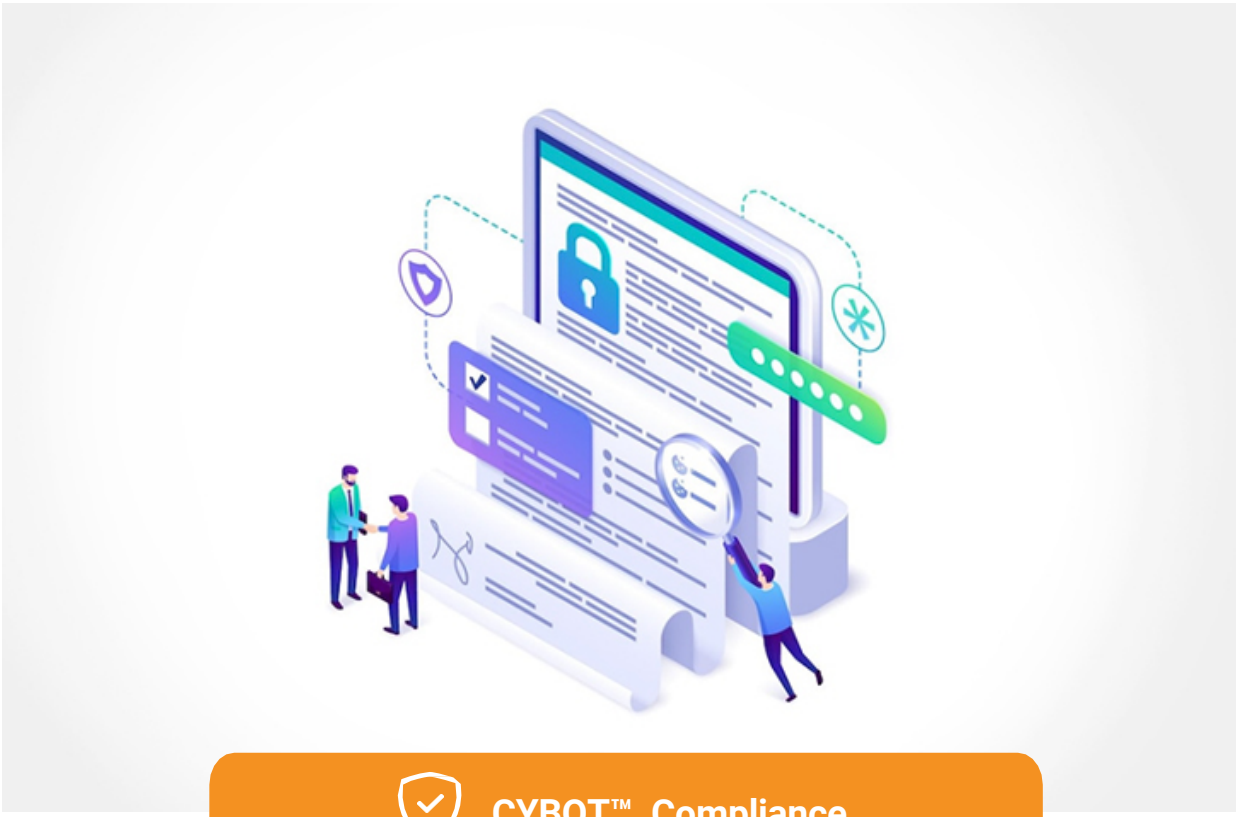
The result summary is also available to be downloaded or taken as printouts. There is automated incident response action in case of an adversary intrusion (analysts can quickly respond via a preconfigured button placed next to the suggestion section in the Dashboard). Hundreds of intelligent playbooks, are available in CYBOT™ and their efficiency and performance are beyond the capability of a human threat hunter

To view Datasheet of CYBOT™ Hunter

CYBOT™ UEBA

UEBA is a type of cyber security solution that discovers threats by finding the deviation in activity from a normal baseline. It can help to discover unusual data access, unusual activity in the IT environment of an organization. The difficult detections like those that don't involve malware, such as credential theft by adversaries by access through network, can be easily detected by UEBA module. The module tracks the normal behavior of a user, host or any entity to build a profile and baseline. Statistical models will then detect the anomalies in the organization environment and alert the relevant security personnel

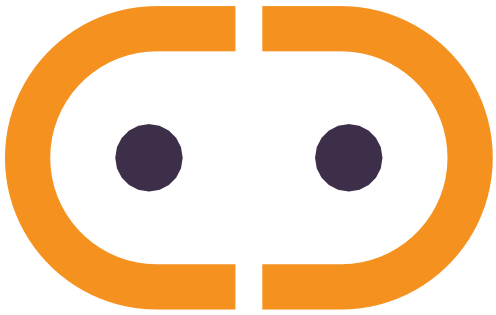
To view Datasheet of CYBOT™ UEBA



CYBOT™ Compliance

We have designed a compliance module in CYBOT solution, with an aim to aid organizations and security teams to meet regulatory standards such as ISO 27001, PCI DSS & NIST. The alerts and dashboards in the module are based on controls requirement. The enterprise data from data lake relevant to compliance controls is visually displayed in an accessible, user-friendly interface that provides actionable insights, and allows administrators to prioritize and respond to the most serious threats first. A compliant company culture establishes an organization's trustworthiness, integrity, and maturity in the industry landscape

To view Datasheet of CYBOT™ Compliance



activebytes
innovations

www.active-bytes.com / contact@active-bytes.com
+971 50 513 3973