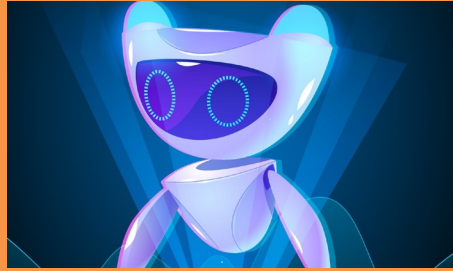
CYBOT™

Automated Investigation & Hunting Platform

Datasheet: UEBA

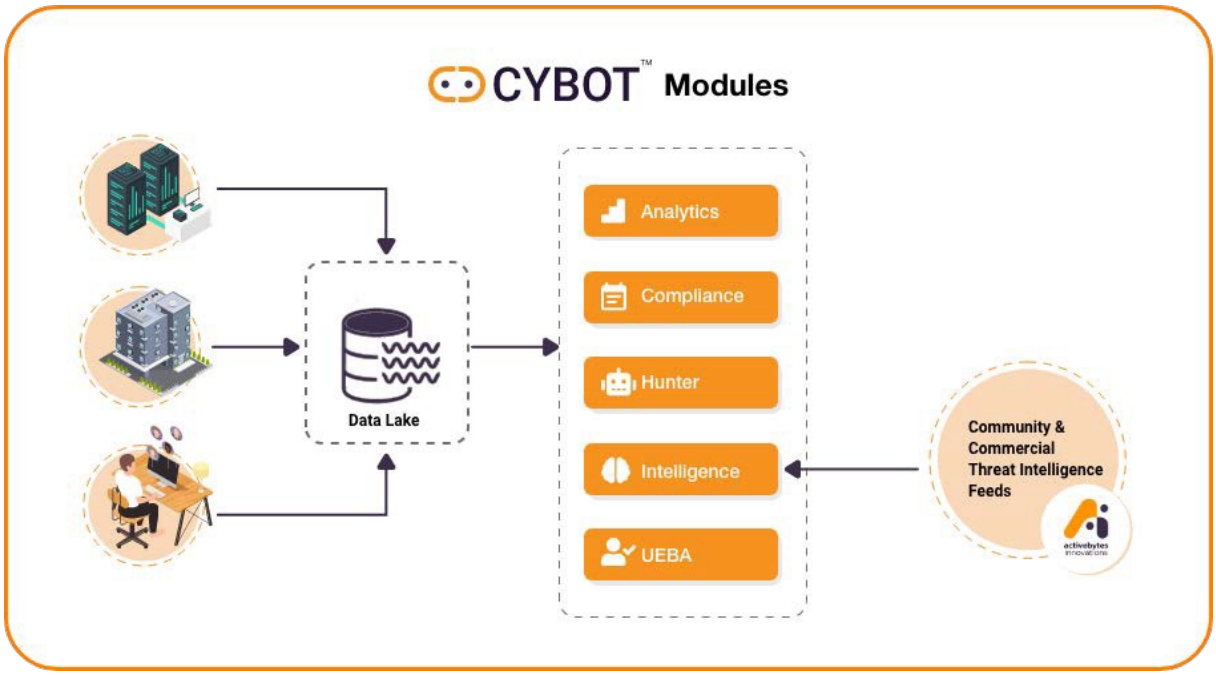


www.active-bytes.com / contact@active-bytes.com
+971 50 513 3973

About the CYBOT™

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

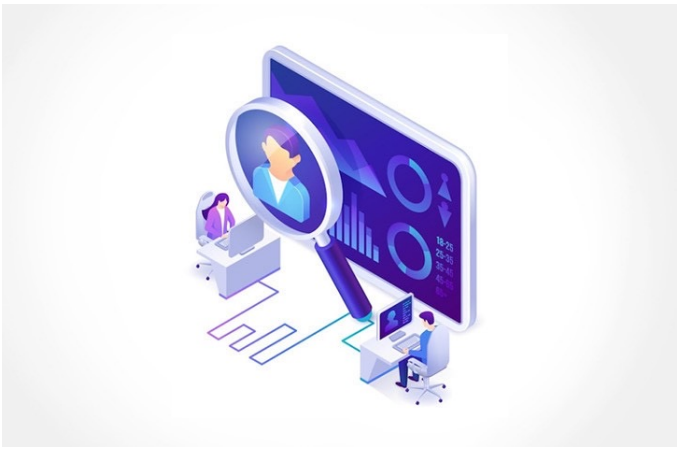
- First, the Analytics Platform with an analytics engine where the data from network sensors and endpoint sensors get collected. The data from log sources are contextualized, structured and then displayed in user-friendly dashboards for the analysts.
- The second part is the Threat Intelligence Platform, 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.



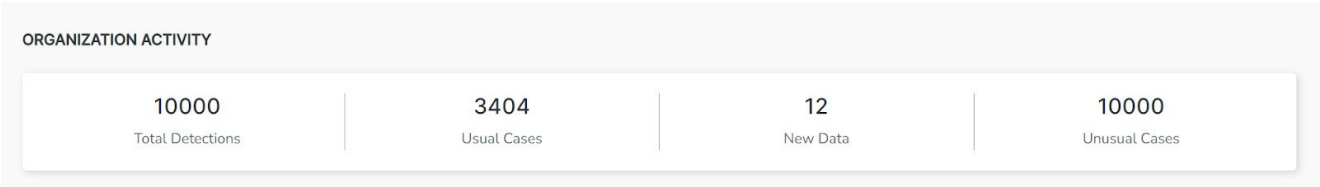
Click here to get an overview of the working of CYBOT ™

UEBA

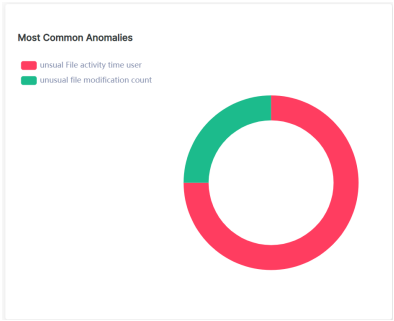
UEBA is a type of cyber security solution that discovers threats by finding the deviation in activity from a normal baseline. It can help to discover unusual data access, unusual activity in the IT environment of an organization. The difficult detections like those that don't involve malware, such as 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



CYBOT has built-in UEBA to perform behavior analysis of user & hosts with machine learning algorithm

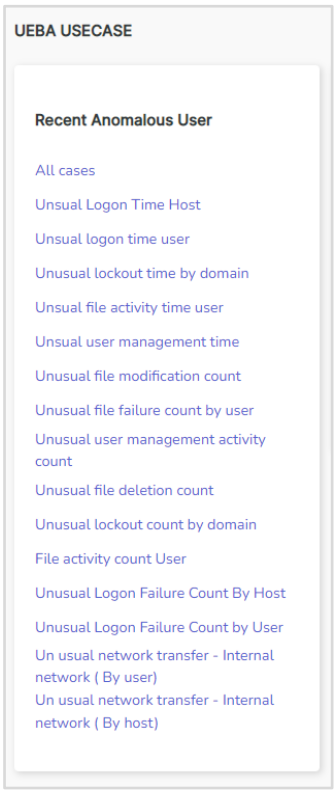


Minimal effort from analysts with its unsupervised algorithm



Some other features of UEBA:

- ✓ UEBA Engine shows usual patterns of a user, in terms of usual host logged in, the usual process executed etc.
- ✓ No license limits on the number of users, servers, the volume of data, bandwidth utilized etc.
- ✓ Built-in dashboards for all use-cases
- ✓ Every anomaly-related detail available
- ✓ Self-learning threat detection which continuously evolves
- ✓ Can capture data from various sources as required by the security team based on their priority in threat modelling
- ✓ Data from UEBA is presented in the form of tables, pie charts, graphs, counts etc.



Organization activity

- ✓ Displays analytics of organization's holistic view on usual patterns, behaviors etc.
- ✓ Easy discrimination of usual processes from unusual process

- ✓ Table representation of process-related data saves time for the security team. Any unusual host or the user performing the process can be easily identified

Most commonly run process-summary

Show 10 entries Search:

User name	Host name	Hunt detection ID	Process name	Detection Time
GOVIND	HP	20220716-486821-1234	TiWorker.exe	Jul 9, 2022, 3:38:26 AM
JUNE	DELL	20220717-486821-1234	TiWorker.exe	Jul 9, 2022, 3:38:26 AM
Kavya-Sathyan	BARCA-GIRL	20220717-486851-1234	TiWorker.exe	Jul 10, 2022, 3:38:26 AM
Kavya-Sathyan	BARCA-GIRL	20220417-486851-1234	wuauclt.exe	Jul 8, 2022, 3:38:26 AM
Kavya-Sathyan	BARCA-GIRL	20220417-486851-1234	LogonUI.exe	Jul 6, 2022, 3:38:26 AM
Kavya-Sathyan	BARCA-GIRL	20220517-486851-1234	TiWorker.exe	Jul 6, 2022, 2:38:26 AM
Kavya-Sathyan	BARCA-GIRL	20220517-486851-1334	WMIC.exe	Jul 7, 2022, 2:38:26 AM
kevin	HP	20220717-486851-1234	TiWorker.exe	Jul 8, 2022, 3:38:26 AM
kevin	HP	20220717-486851-1234	TiWorker.exe	Jul 8, 2022, 3:38:26 AM
kevin	HP	20220417-486851-1234	wuauclt.exe	Jul 8, 2022, 3:38:26 AM

Showing 1 to 10 of 10 entries Previous 1 Next

User Activity

- ✓ Unauthorized access even if it's a single event is detected and displayed
- ✓ Privilege abuse or escalation is quickly detected and notified to relevant people

- ✓ including Insiders in threat profile and hence insider threat identification is not a challenge anymore

- ✓ Anomalies in file modification can be used to identify unusual file activities

Recent File Deletions in Host

file Name	User Name	Host Name	Time	File Path
HxCommAlwaysOnLog.etl	kev	DESKTOP-L5A1LT5	Jun 8, 2021, 2:29:33 PM	C:\Users\kev\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\HxCommAlwaysOnLog.etl
HxCommAlwaysOnLog.etl	kev	DESKTOP-L5A1LT5	Jun 8, 2021, 2:29:33 PM	C:\Users\kev\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\HxCommAlwaysOnLog.etl

Processes Run by User

Process Name	Process Hash	Count	Current Time
mshta.exe	523579d1c1664a5db4d4f9c743ef2c0f	20	2022-06-22-11:51:25
			2022-06-22-11:51:25
mshta.exe	523579d1c1664a5db4d4f9c743ef2c0f	20	2022-06-22-11:51:25
			2022-06-22-11:51:25

Processes Run by Host

Process Name	Process Hash	Count	Current Time
mshta.exe	g7fg2f730j89394h7498	5	2022-06-22-11:51:25
mshta.exe	g7fg2f730j89394h7498	5	2022-06-22-11:51:25

Host activity

- ✓ Automatically detect a wide range of cyberattacks including, insider threats, compromised accounts, brute-force attacks, the creation of new users, and data breaches