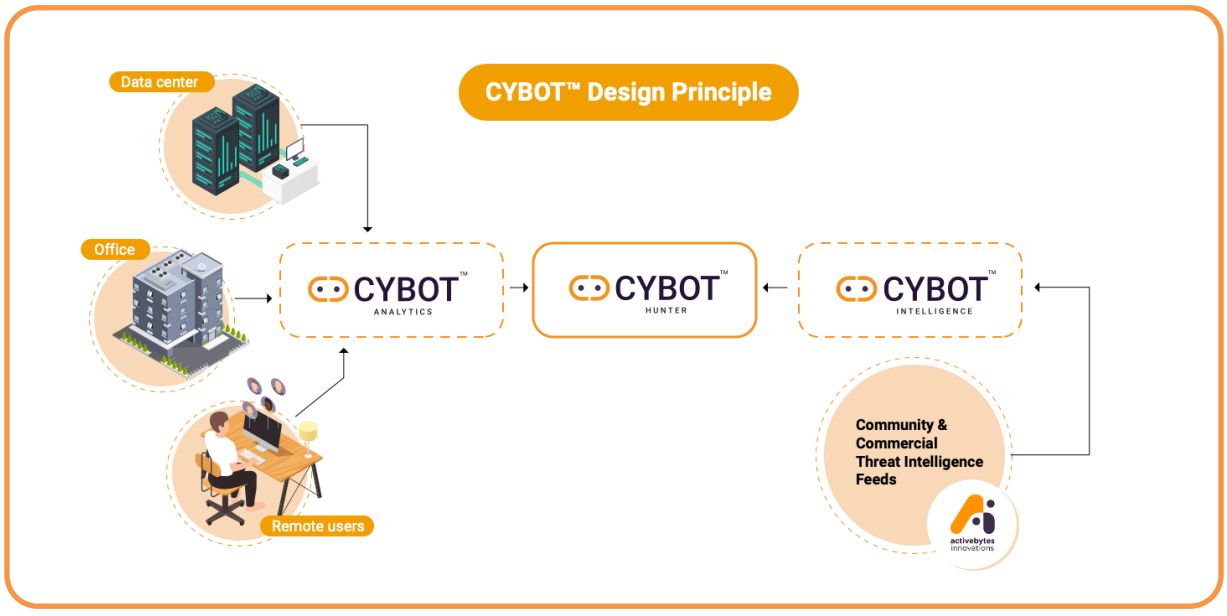
CYBOT™

Automated Investigation & Hunting Platform

Datasheet: Analytics Package

About the CYBOT™

- CYBOT™ collects raw logs from the enterprise's network, remote users, servers and stores to its Analytical engine in a contextualized and secured way. The logs then undergo intelligent automatic analysis, thereby going the extra mile in threat hunting which a human cannot.
- CYBOT™ is designed to be adaptive to the latest adversary techniques and tactics by keeping in track with the threat intelligence events that it is programmed to receive from our trusted community sources and Activebytes dedicated threat intelligence team.
- CYBOT™ intelligently and automatically hunts and investigates the threat leveraging Realtime Logs by performing correlation with TI IOCs received from even the dark sources, thereby detecting adversary attack patterns that a human can never pickup.
- Around the clock monitoring of logs and every unusual, suspected event is subjected to drill down the level of investigation. CYBOT™ is designed to provide automated options to respond along with suggestions and alerts to the security team. This will help analysts to deal with the adversaries that already intruded on the network.



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

Why CYBOT™ is Your Intelligent Analytical Threat Hunting Solution?

CYBOT™ Platform includes a Big Data Analytic Engine that handles huge data which is beyond human ability, with best-in-class analytics and processing capability. We've made hundreds of dashboards and alerts out of the box for both compliance and security analytics purposes. You will have additional access to our ActiveBytes content library is updated with new dashboards and alerts to continuously improve the hunting capability of the platform.

CYBOT™ protects your assets

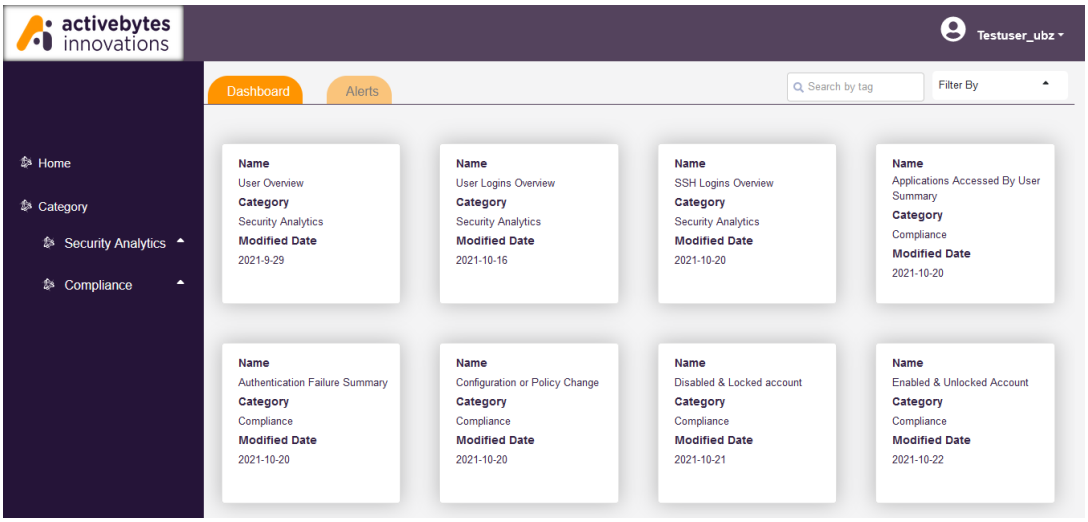
Analytics

CYBOT™, with its advanced analytics design, performs quick profiling of raw data into useful information, analysis of this along with events patterns in the enterprise environment and helps in proactive handling of IOCs, thereby saving the enterprise IT infrastructure from a security breach. CYBOT™ is capable of early detection of even the new generation-based attack attempts with its huge pool of IOCs and pattern recognition capability. The observations that are available as dashboards and the panels with data at granular level allow analysts to quickly neutralize the threat element that breached their defence systems.

Some other features include

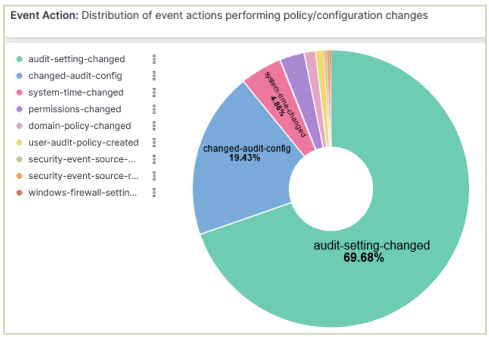
- Huge Data extraction from OS, system behaviour, common user behavior etc
- Analysis of logs of OS binaries execution and registry changes
- Extraction of data related to file creation, deletion and modification activities, other system/ application logs
- Collects, analyze, and generate alerts on every quality IOCs, including Malicious files, URLs, Domains, IPs, Filenames/hashes, Malware families.

- **Analyze ,not only the known IOCs but also patterns from events. Thereby detects adversary acts like a user id or password abuse by correlating the user's typical behavioral pattern with the newly detected pattern.**
- **Faster reports (technical & non technical) and Dashboard generation for historical & real-time data**
- **Capable of extracting domain lookups, communication logs irrespective of TCP/IP Protocols**
- **100+ Pre-built dashboards to review logs against compliance standards such as ISO27K, PCI-DSS, NIST**
- **Easy understanding of user & group management activities and enumerations on every data related to it**



- **Hundreds of Dashboards and Alerts for both compliance and security analytics. Hence covering a wide range of use cases with huge data, in a user-friendly manner.**

- **Major functions supported by APIs and integrates with the company's baseline without affecting the network or IT architecture**

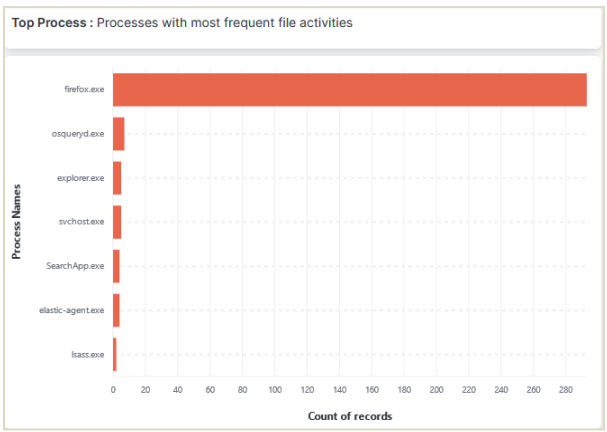


- **Major functions supported by APIs and integrates with the company's baseline without affecting the network or IT architecture**

Recent Traffic to Internet : Details of recently performed internet activities

184898 documents

Time	user.name	host.hostname	process.name	process.pid	destination.ip	destination.port	host.ip	source.ip
Apr 9, 2022 @ 17:14:20.142	root	ip-172-31-15-47	fleet-server	32277	3.140.55.130	9202	127.0.0.1, ::1, 172.31.15.47, fe80::8a:cff:fe30:7636	172.31.15.47
Apr 9, 2022 @ 17:14:14.799	lenovo	DESKTOP-OCNLIIE	Skype.exe	11068	20.185.212.106	443	169.254.169.165, fe80::5d2	192.168.43.118



activebytes innovations

www.active-bytes.com / contact@active-bytes.com

+971 50 513 3973