CYBOT™

Automated Investigation & Hunting Platform

Datasheet: Analytics Package

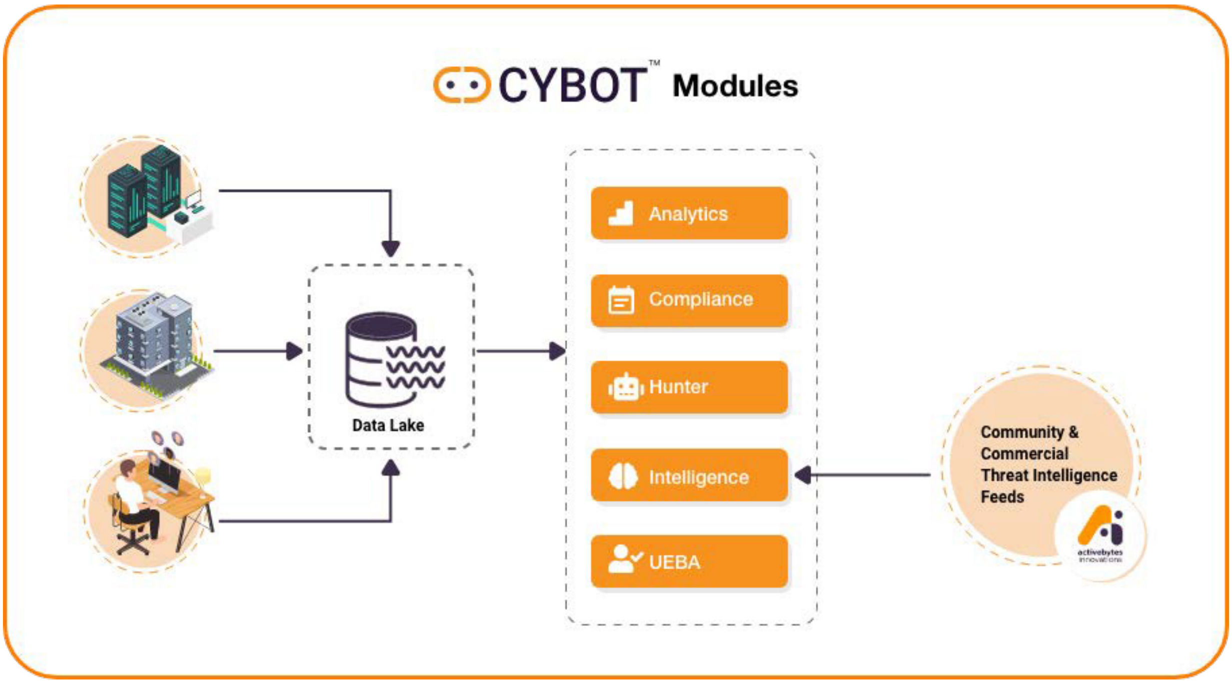
www.active -bytes.com / contact@active-bytes.com

+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 ™

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.

© 2022 - ActiveBytes Innovations, All Rights Reserved

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.

✓ **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**

✓ **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**

© 2022 - ActiveBytes Innovations, All Rights Reserved