CYBOT™

Automated Investigation & Hunting Platform

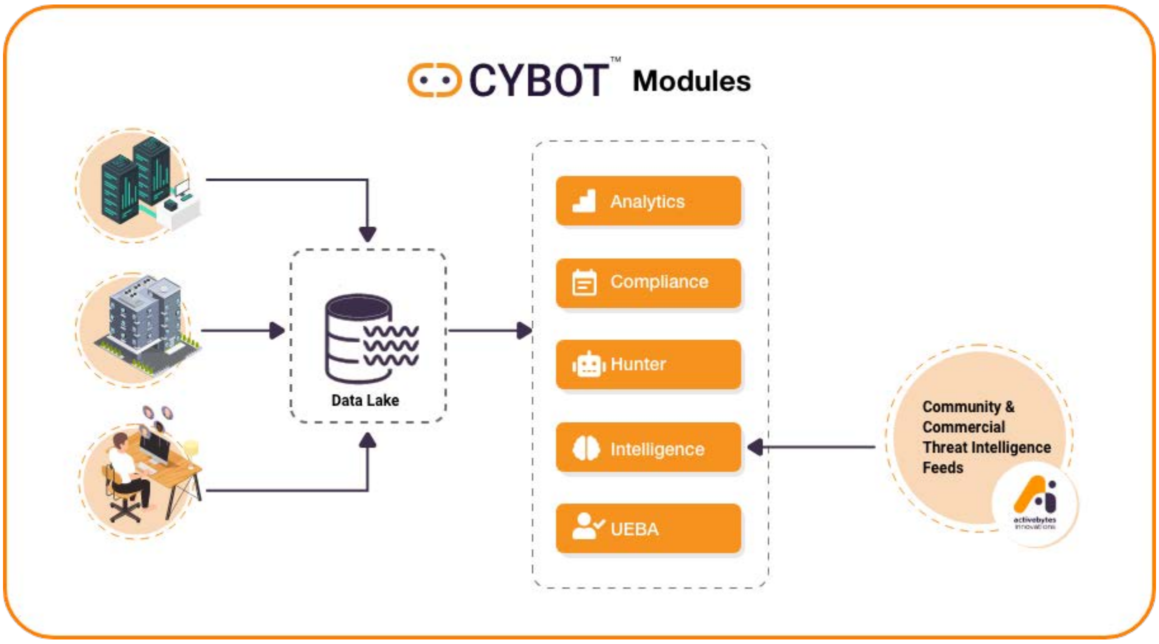
Datasheet: CYBOT™ Intelligence

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 Automated Adaptive Threat Hunting Solution ?

CYBOT™ Threat Intelligence

CYBOT™ has a Threat Intelligence Platform which continuously gets updated with knowledge of the latest cyber security threats in the industry worldwide. 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 effective intelligence. 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 take down.

CYBOT™ -Threat Intelligence

CYBOT™ transforms raw feeds from various commercial and community sources into useful intelligence. The value-added analyzed and contextualized intelligence feeds from Activebytes innovations is also inputted to the platform. This effective intelligence gives and an extra edge to the security team about the latest adversary techniques and tactics, sector targeted, threat landscape, etc. that take place in the world. The huge pool of relevant intelligence feeds helps CYBOT™ in early detection of hidden, unknown, and emerging threats and this helps the analysts to quickly defend and secure their environment.

✓ **CYBOT™ protects your infrastructure from even the darkest corners**

Threat intelligence feeds from various open sources and dark web sources make the CYBOT™ platform adaptive and efficient in detecting threats that escaped your defence system.

✓ **No malicious executions go undetected with TIP**

With intelligence sharing, the latest technique adversary executions are fed to CYBOT™ and hence can perform faster malicious IP detection, Domain, Hash detection, etc.

✓ **User friendly technical and non-technical management summary reports generated with option to download and set notifications**

Some other features include

- Receiving and sharing threat intelligence information in a controlled, contextualized and structured manner benefiting the enterprise.
- Receives the latest emerging threat intelligence information from commercial sources as well.
- CYBOT™ is Pre-configured to receive threat intelligence data from multiple sources and contextualize the data for effective correlation with observables in the enterprise environment.
- Role-based access control and can be managed in the Settings option in the platform.
- Records all types of IOCs including IP, URLs, text, files, hashes, IDS signatures, etc. and hence even manually undetectable threats don't escape the investigation.
- Allows internal team to collaborate and discuss security and vulnerability intelligence events and this benefits the whole team with knowledge of the latest attacks and the ways to defend from the same.

- No restrictions with the number of users and new users can be easily added by the admin.
- API for all major functionality allows seamless integration with other security solutions.
- Automatically co-relates and marks related to previous incidents for effective tracking.
- Commercial threat feeds and services from ActiveBytes Innovations' dedicated threat intelligence team for effective threat information analysis, identification, domain takedown, etc.
- TI Feeds on Malware Information, Threat Intelligence News, Vulnerability and exploits information makes CYBOT™'s resource pool rich with the latest adversary factors.

✓ **Capable to securely gather, share, store and correlate IoCs of targeted attacks, vulnerability information etc. This makes the automated hunt faster and efficient.**

✓ **Detailed information on each intelligence event, thereby providing the analysts and the management an insight on emerging threats. This will also help to decide the changes to be made in your present security defence framework. The print button can be used to get the details printed.**

✓ **Every IOC is listed in indicators table with in-depth information, making the latest events resourceful for analysts**

✓ **The time distribution gives insight into the adversary attacks, vulnerabilities that trend during a particular time in the world, thereby providing an idea for changes required in the defence system**

✓ **The Impact region helps you to understand the threat landscape and the degree of impact, a particular attack has caused.**

✓ **Vulnerabilities and exploits are crucial information to security teams since these need to be given extra focus during patch management**

✓ **Expert analysis and comments on security intelligence and vulnerability intelligence are very important for any security team to update their own IT infrastructure security accordingly.**

✓ **Any vulnerabilities in your environment can lead to a security breach and getting updates about the same for enterprise benefit is an added advantage**