CYBOT™

Automated Investigation & Hunting Platform

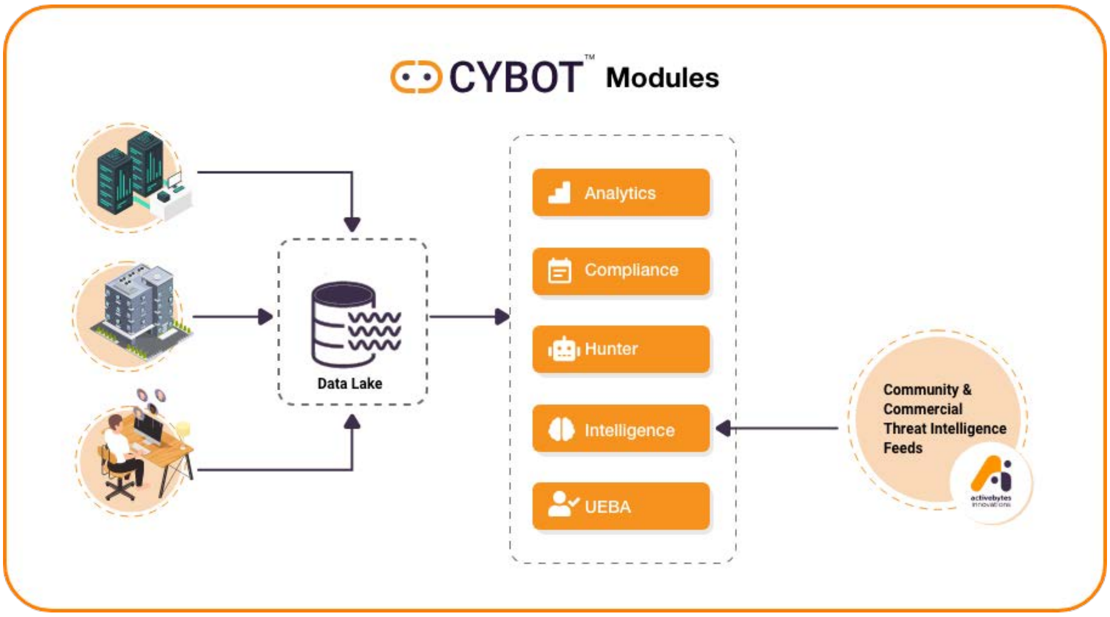
Data sheet: CYBOT™ Hunter

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 Next Gen Threat Hunting Solution?

CYBOT™ - Automated Threat Hunting & Investigation

Raw data collected via sensors from servers, networks and endpoints of the enterprise environment are fed into the Analytical engine and then stored in a unified, contextualized and secured format. CYBOT™ is designed to be intelligent and adaptive. The platform is continuously updated with automated intelligent playbooks. The result from these automated hunts is displayed as dashboards and made available to be downloaded or as prints. The intelligent automation playbooks detect a threat, then execute end-to-end investigation, enrichment, and suggest incident response actions in case of an adversary intrusion. There are hundreds of playbooks, dashboards, and alerts use cases available in CYBOT™ and these use cases are beyond the capability of a human threat hunter.

Pro-Active Automated Hunting & Detection

CYBOT™ Threat Hunting

In this era of advanced adversary techniques including non-human cyber attacks, an enterprise needs to focus on a threat hunting solution that is efficient beyond manual capabilities. CYBOT™s intelligent automated playbooks can automatically perform threat hunting and detect the advanced threats that hides in your enterprise environment, thereby helping your enterprise to enhance the IT security infrastructure with high efficiency, without compromising any IT process. CYBOT™ has a large set of inbuilt automate threat hunting use cases and fast Incident response buttons and alerts in case of suspicious activity detection. Our automation playbooks can quickly hunt and detect the malicious elements that stealthily lurk in your IT environment.

✓ **Every detail of the playbooks hunt status is available to the analysts.**

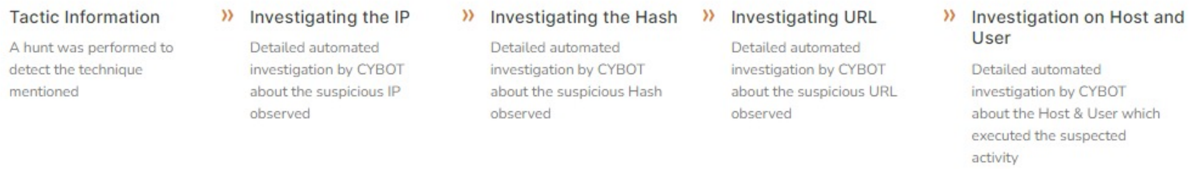
✓ **Immediately notifies on adversary through alert & suggestion**

This critical feature helps the security team in preventing an attack or neutralizing an adversary from further escalation down the kill chain. Clicking the Respond button is always a quick fix.

Playbooks in CYBOT™ is scripted based on 3 approaches. CYBOT™ protects your infrastructure with multi-dimensional security.

- Hypothesis driven investigation
- Investigation based on known Indicators of compromise or Indicators of attack
- Advanced analytics and machine learning investigation

✓ **Playbooks are scripted with rules to do end-to-end investigation, enrichment and incident response in exceptionally faster ways.**



Tactic Information
A hunt was performed to detect the technique mentioned

» Investigating the IP
Detailed automated investigation by CYBOT about the suspicious IP observed

» Investigating the Hash
Detailed automated investigation by CYBOT about the suspicious Hash observed

» Investigating URL
Detailed automated investigation by CYBOT about the suspicious URL observed

» Investigation on Host and User
Detailed automated investigation by CYBOT about the Host & User which executed the suspected activity

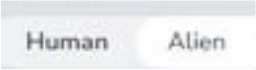
- **Investigates and suggests to respond via security solutions configured in the enterprise network such as AV, EDR, NDR, Vulnerability scanners, SIEM, etc.**
  The threat score will help analysts to decide the type of response to be taken for a particular incident.
- **Reports all the investigation steps like a human analyst does, which is understandable to technical and non-technical security resources.**

  The categorized, detailed results and status of automated investigation benefits the enterprise security team as well as the management in decision making.

✓ **Option to set investigation exception on specific IOCs easily setup, making the hunt flexible to analyst requirement.**

Smart and Faster than a Human

SIMPLIFIED INVESTIGATION VIEW FOR MANAGEMENT RESOURCES AND VERY DETAILED TECHNICAL INFORMATION FOR SECURITY EXPERTS



Some features include

- Automatically and Intelligently hunts for cyber threats inside the organization’s infrastructure, covering huge data from log sources.
- Automatically feed inputs from various sources such as TTP, IoC, TI, OSINT feeds, etc. thereby making it adaptive to the latest adversary elements.
- Chained investigation scenarios
- Has feedback mechanism for easy incident creation on the threat intelligence platform with IOCs of any newly identified threat.

Self avoiding repeated investgation for the same incident

Looks for possible repetition of similar observables and aggregates them to avoid false positives by itself, thereby reducing noise to analysts.

CYBOT™ INVESTGATION SCENARIO

Platform hunts for an attack tactic, and collect observables. If found any history of occurrences, then it cross-check with the recent hunts to reduce noise and false positives, finally present all the detection related information to the analysts. Platform searches the logs for any other servers or user PCs ,that is associated with the suspicious IP/URL/Hash .The platform further investigates the reputation of IP/Hash/URL, and assign a threat score to it. Platform then enables users to see previous hunt detections, suggest response action as well. The platform goes beyond human capabilities by looking into user account activity across the environment, to investigate possibilities of lateral movement in case of a compromise. Details related to the suspicious IP/Hash/URL like all processes & uncommon process executed, command lines run , file activities etc is made available in visualizations. The Platform then summarizes the investigation out comes for both technical and non-technical resources

To know details about the Workflow click here

Other Features

A list of options is available for the security team or administrator which is customizable as per your organization’s requirements.

Some value-added customizable features

- User Management
- Backup & Restore
- Automation Exceptions
- Automation Scheduling
- Integrations
- Notifications
- SIEM Integration
- Configurations
- Tenants & License

- Scheduling of investigation helps analysts to focus on the specific area of security concern and throw visibility on weaknesses and vulnerabilities in existing security systems.

- In depth automatic hunt with minimum or no manual input, making multiple investigations at a time, which saves analysts’ time to stop or neutralize the threat. Also visibility of hunting tactic used, whether MITRE based ,IOC Based Hunt or Advanced Analytics based hunt