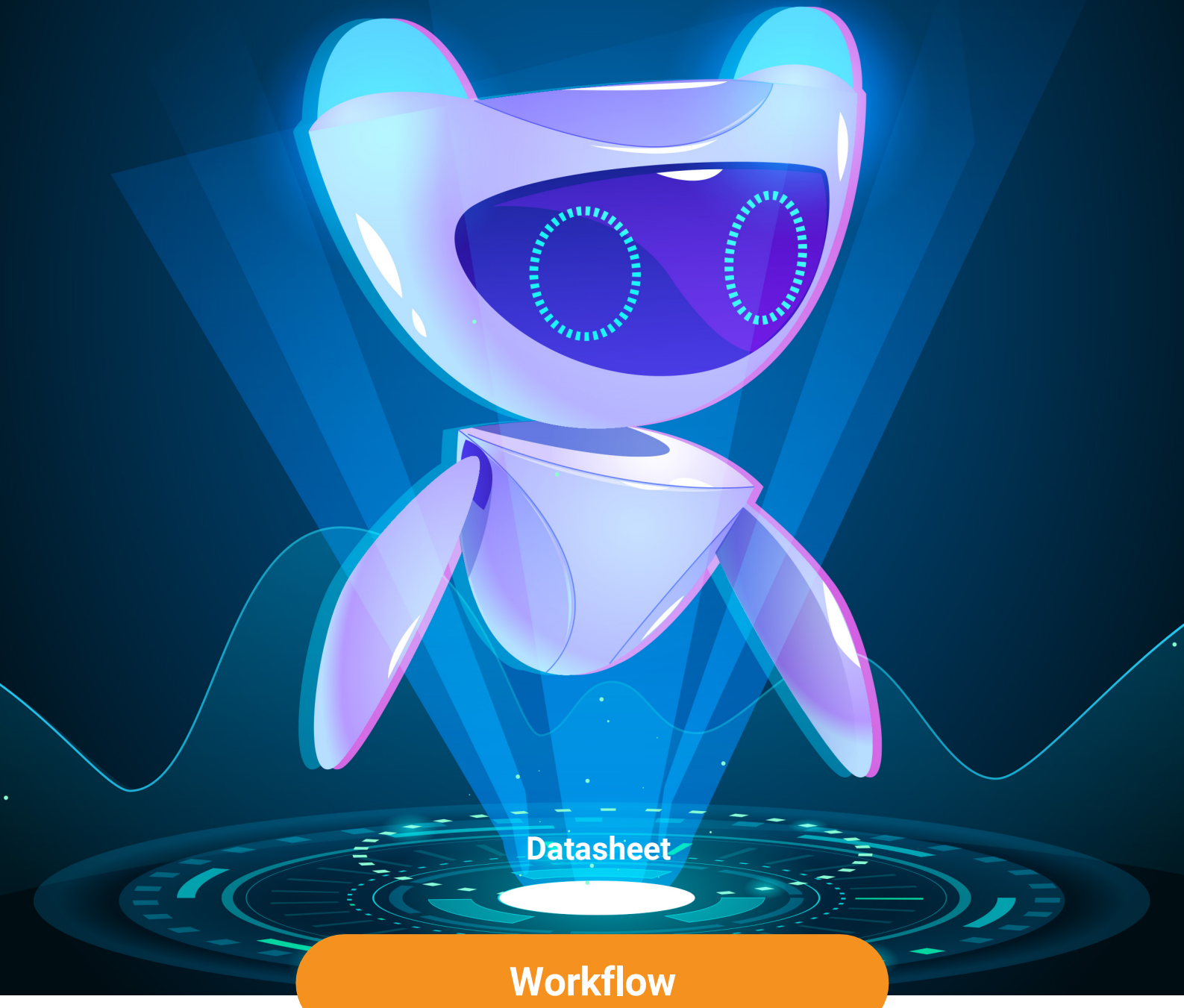
# CYBOT™

Automated Investigation & Hunting Platform



Datasheet

## Workflow

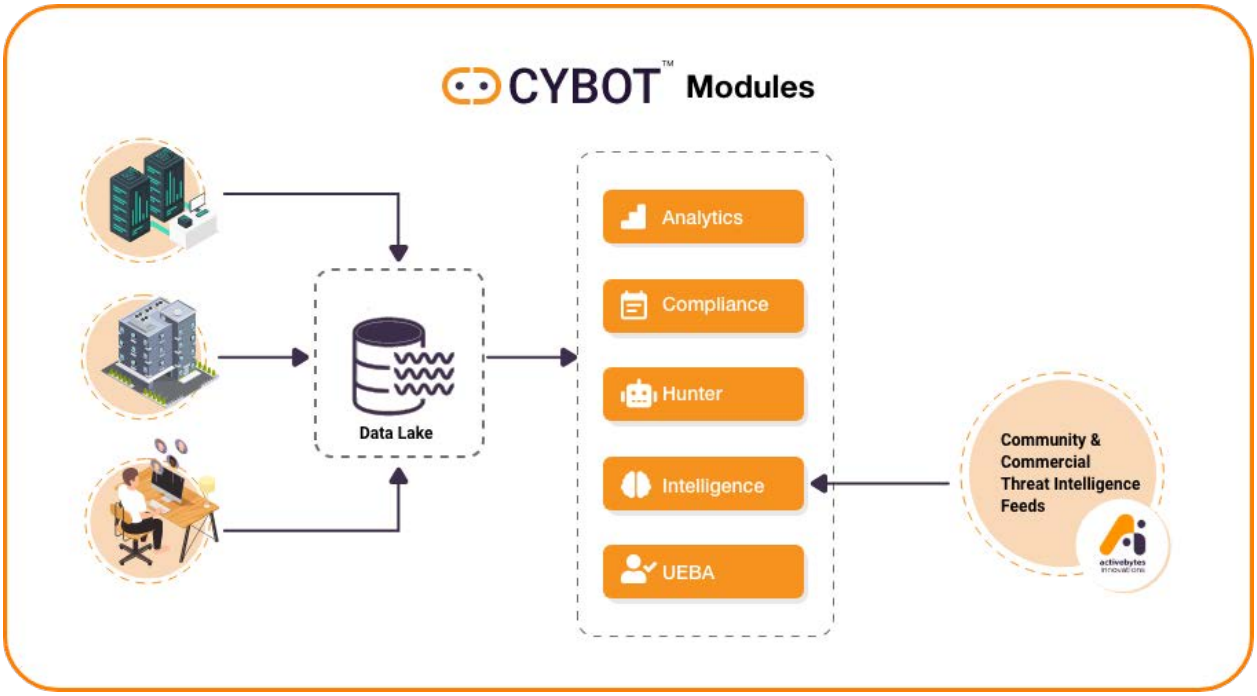
activebytes innovations

www.active-bytes.com

# About 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.

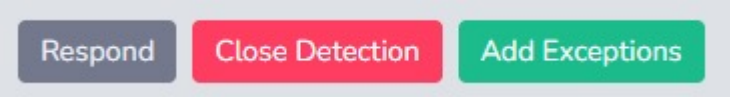



Click here to get an overview of the working of CYBOT™

## CYBOT™ has Unique, Intelligent, Smart Investigation Workflow

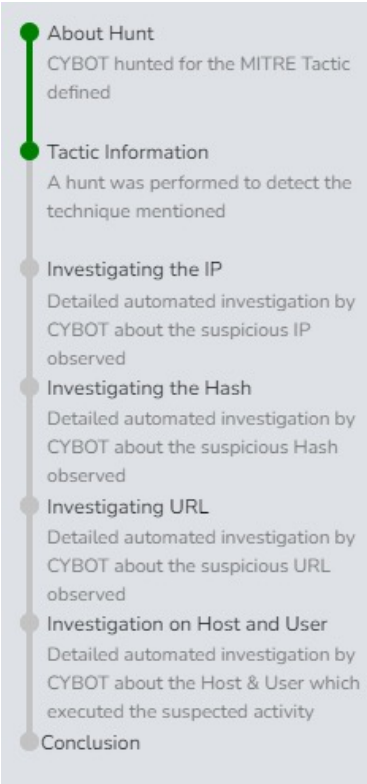
The logs from the enterprise network, endpoints and servers are always a mix of structured and unstruc-tured data. Since it is beyond human capability to handle or analyze huge data, most of the time, a good part of the valuable data goes unattended, and this missing part can be the critical ones. CYBOT™ has built-in intelligent automated workflows that can format and contextualize every data log fed into the CYBOT™ platform and perform an automated investigation on every suspected data. CYBOT™'s automated workflow allows no threats to go undetected, displays every result in technical and non-technical formats, repeated hunts are avoided to save time for analysts, and the speed is accelerated many times than manual effort.

- **CYBOT™ is designed with a unique investigation flow for each type of hunting tactic.**
- **Every suspected IP, Hash, URL, Host and User undergo a drill down the automated investigation, thereby capable to detect even the stealthiest threat in your environment**
- **The automated buttons to Respond in case of threat detection, to close the detection output window of workflow and adding exceptions to avoid a specific IOC investigation, adds to the user-friendliness of the workflows for the analysts.**



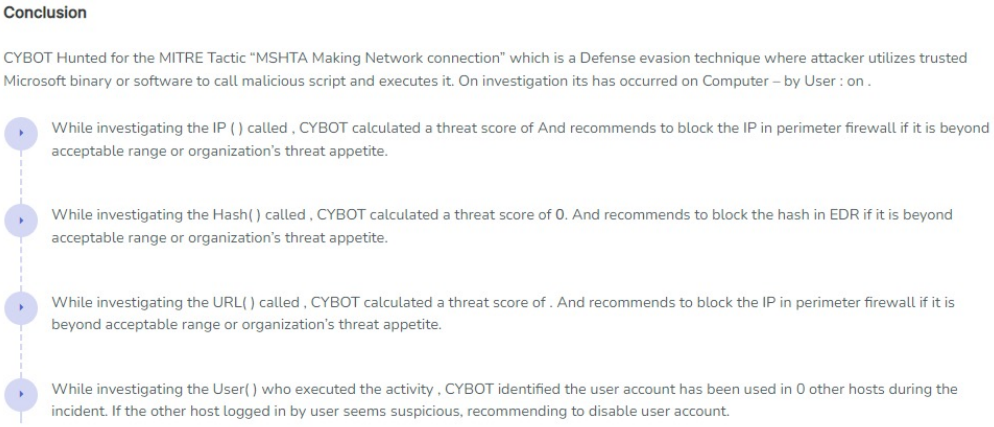

**Playbooks with unique investigation flow**

Each observable from the hunt will have its own investigation flow and is available for analysts.
In the below workflow, a suspicious IP was observed in the logs. The suspicious IP was subjected to detailed investigation first by the workflow. Then the associated hash was investigated. If any URL is associated with observable, then it undergoes drill down investigation. Every host & user associated with these suspected IPs will undergo investigation by the workflow.



## Other features of CYBOT™s Workflow

**Detailed and simplified investigation summary for technical and non-technical teams**

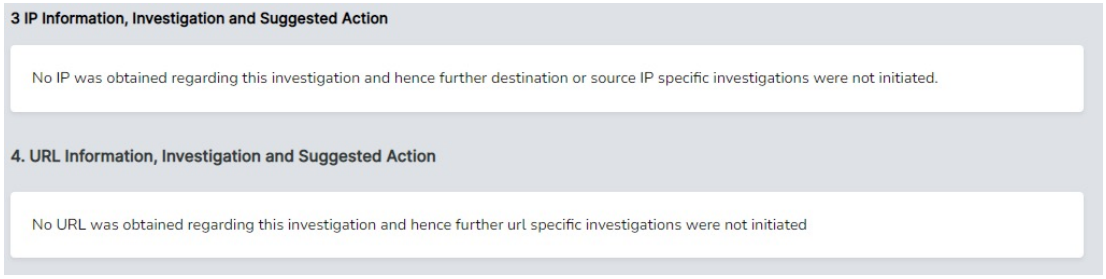


**Conclusion**

CYBOT Hunted for the MITRE Tactic "MSHTA Making Network connection" which is a Defense evasion technique where attacker utilizes trusted Microsoft binary or software to call malicious script and executes it. On investigation its has occurred on Computer – by User : on .

- While investigating the IP ( ) called , CYBOT calculated a threat score of And recommends to block the IP in perimeter firewall if it is beyond acceptable range or organization's threat appetite.
- While investigating the Hash( ) called , CYBOT calculated a threat score of 0. And recommends to block the hash in EDR if it is beyond acceptable range or organization's threat appetite.
- While investigating the URL( ) called , CYBOT calculated a threat score of . And recommends to block the IP in perimeter firewall if it is beyond acceptable range or organization's threat appetite.
- While investigating the User( ) who executed the activity , CYBOT identified the user account has been used in 0 other hosts during the incident. If the other host logged in by user seems suspicious, recommending to disable user account.

**Unwanted observables are avoided and proceeded, thereby saving time, handling remaining valuable data and finishing the hunt at high speed.**



**3 IP Information, Investigation and Suggested Action**

No IP was obtained regarding this investigation and hence further destination or source IP specific investigations were not initiated.

**4. URL Information, Investigation and Suggested Action**

No URL was obtained regarding this investigation and hence further url specific investigations were not initiated

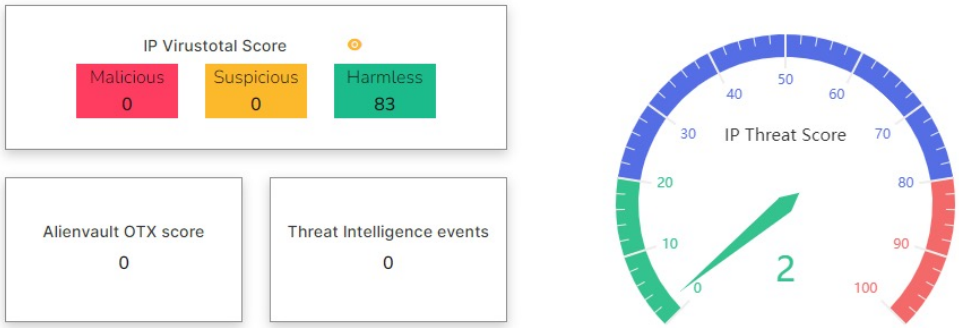
**Workflow can hunt and investigate for malicious IP, hash, domain, user login patterns, unknown processes. etc. that is obtained from threat intelligence and logs.**

**1.3 Detected Observables**

Process Name : netsh.exe
Process Commandline: netsh advfirewall firewall add rule name='My Application' dir=in action=allow program='C:/Users/Administrator/AppData/Local/Temp/asd.exe' enable=yes
Process ID : 4764
Process parent name: cmd.exe
User Name : Administrator
User Domain : WIN-SRH715DO5HR
Host Name : WIN-SRH715DO5HR

Detection Name : Add Programs to firewall exclusions from Temp directory
Last detection : Mar 29, 2021, 5:43:31

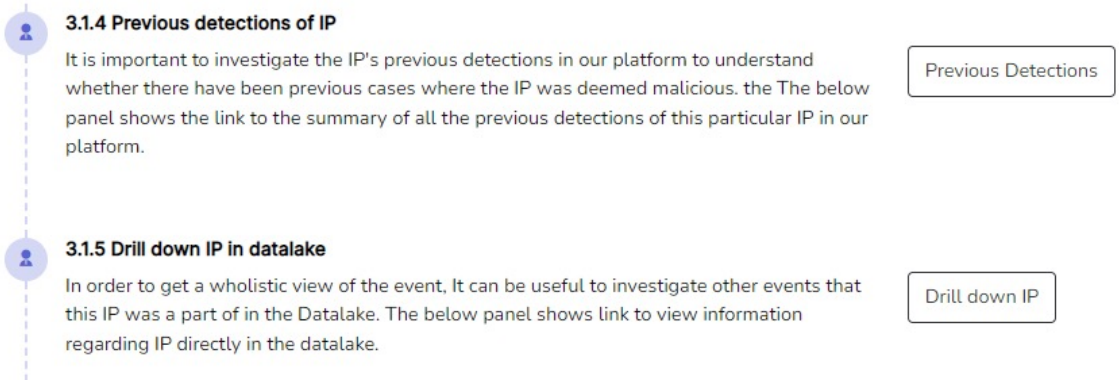
**In each investigation performed, observables are allotted scores based on the information from multiple sources including the security systems in the enterprise, and this contributes to deciding the response action by the analysts.**

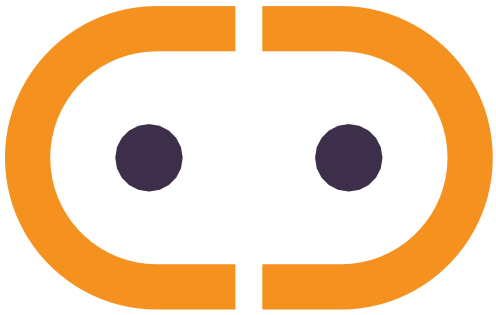






**CYBOT™s automated workflows is scripted to give granular level detail of the observables to the security team, and this gives insight into the weak points in the existing security framework of the enterprise.**





activebytes innovations

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