CYBOT™

Automated Investigation & Hunting Platform

Datasheet

Workflow

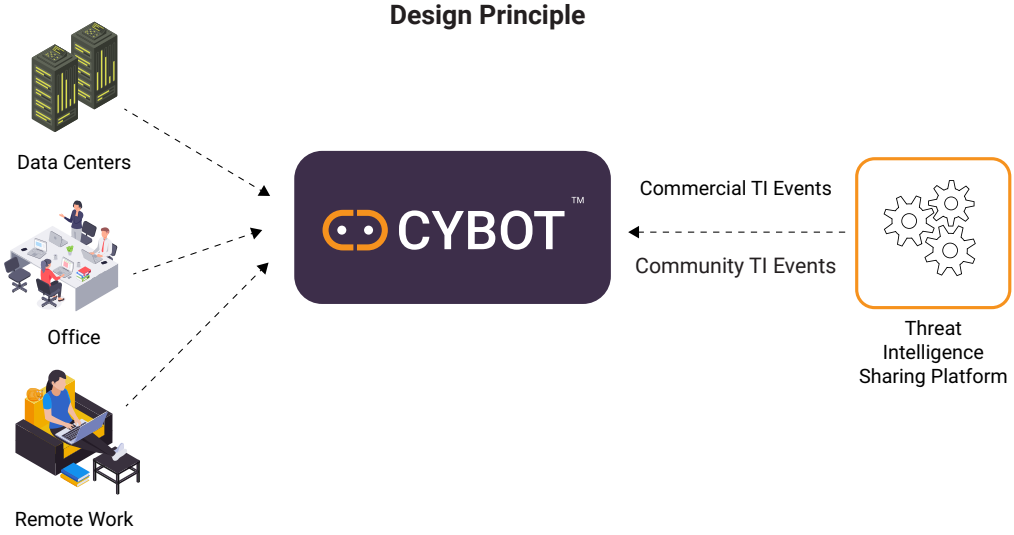
activebytes innovations

www.active-bytes.com

About the CYBOT™

- CYBOT™ collects raw logs from enterprise network, remote users, servers and stores to its analytical engine in a contextualized and secured way. The logs then undergoes intelligent automatic analysis, thereby going the extra mile in threat hunting, which a human cannot do.
- 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 Innovation's 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 and 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 network.

Design Principle

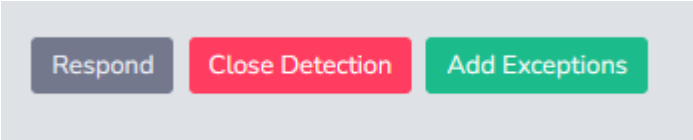


Click here to get an overview of the working of CYBOT™

CYBOT™ has Unique, Intelligent, Smart Investigation Workflow

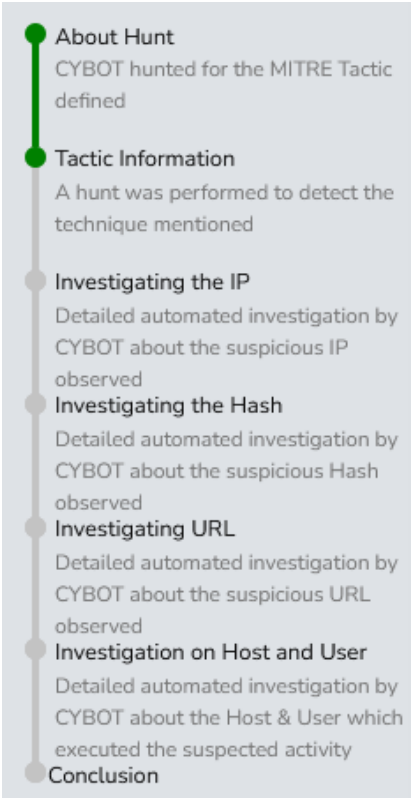
The logs from the enterprise network, endpoints and servers are always a mix of structured and unstructured data. Since it is beyond human capability to handle or analyze huge data, most of the time, a good part of the valuable data goes unattended, and this missing part can be the critical ones. CYBOT™ 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 undergoes a drill down 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.**



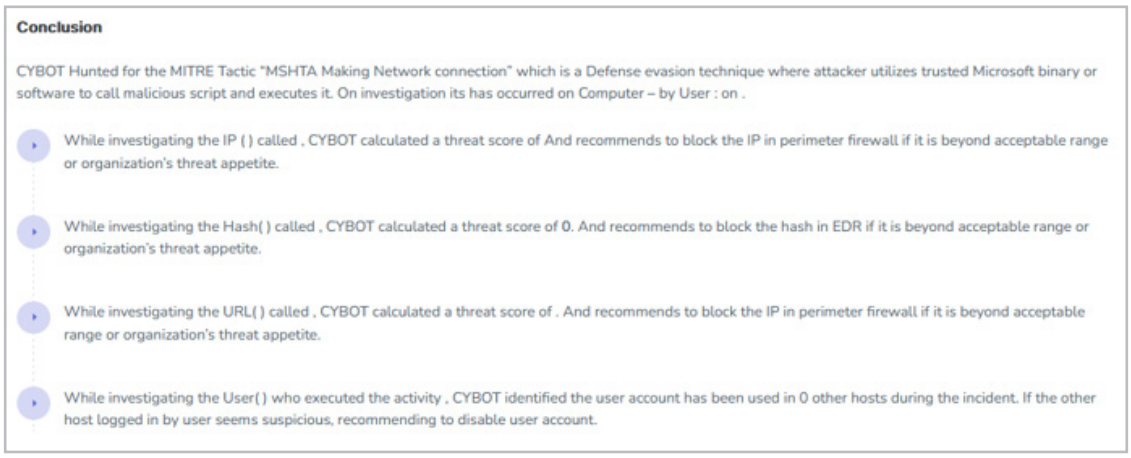
Playbooks With Unique Investigation Flow

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 IP will undergo investigation by the workflow.



Other features of CYBOT™s Workflow

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

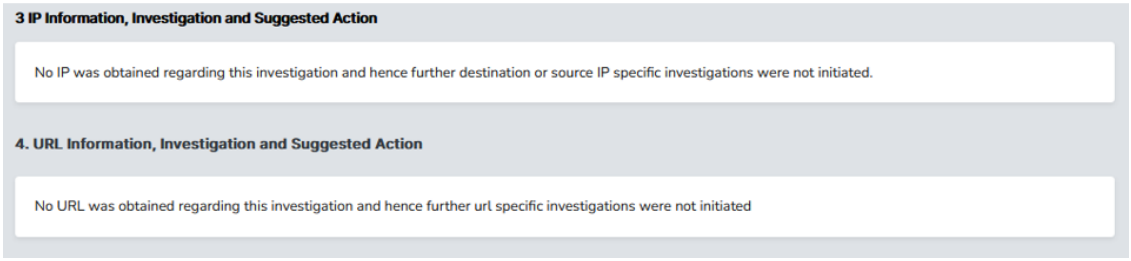


Conclusion

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**



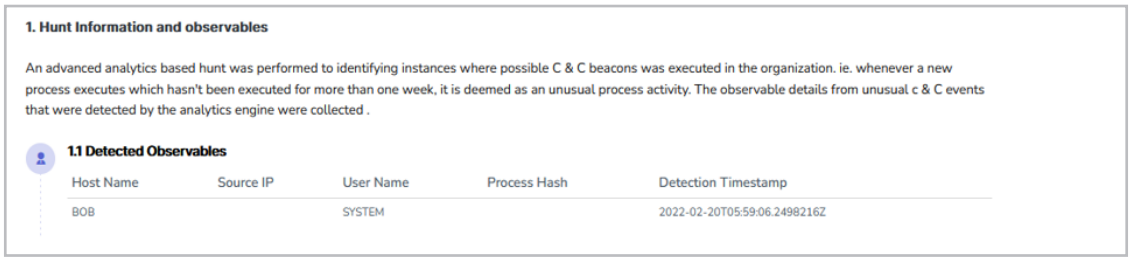
3 IP Information, Investigation and Suggested Action

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.**



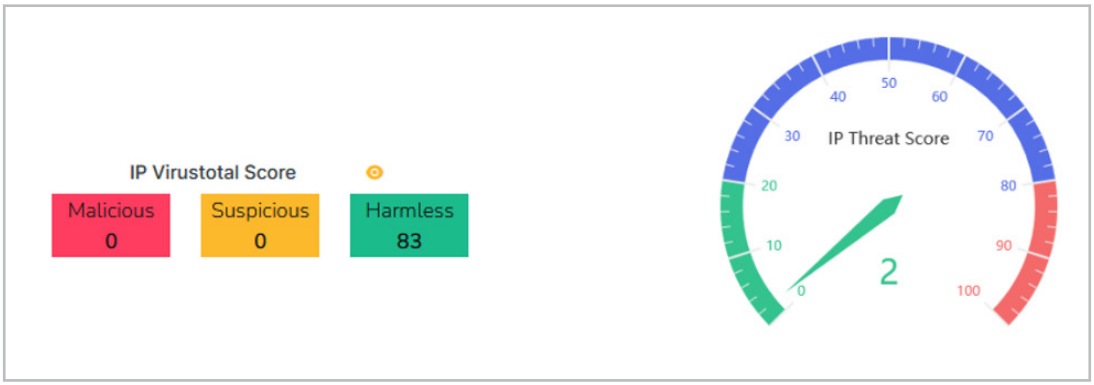
1. Hunt Information and observables

An advanced analytics based hunt was performed to identifying instances where possible C & C beacons was executed in the organization. ie. whenever a new process executes which hasn't been executed for more than one week, it is deemed as an unusual process activity. The observable details from unusual c & C events that were detected by the analytics engine were collected .

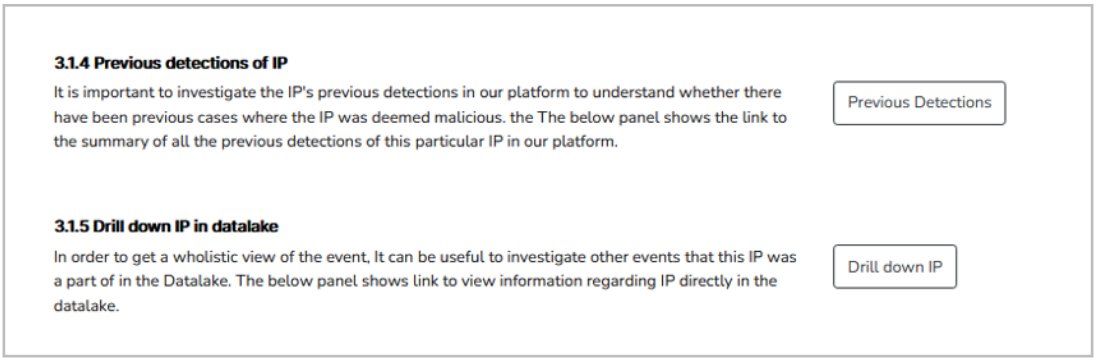
1.1 Detected Observables

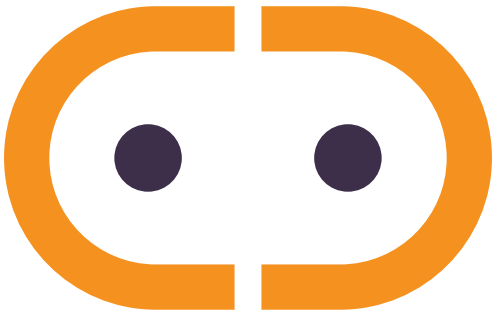
Host Name	Source IP	User Name	Process Hash	Detection Timestamp
BOB		SYSTEM		2022-02-20T05:59:06.2498216Z

- **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