CYBOT™

Automated Investigation & Hunting Platform

Datasheet

CYBOT™ Hunter

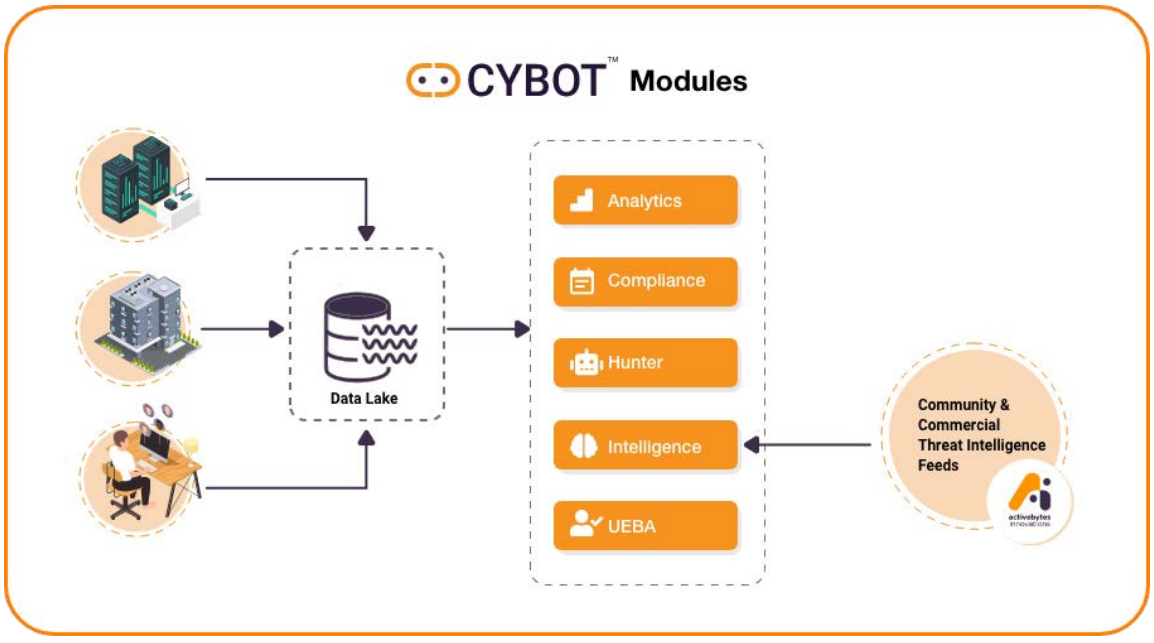
activebytes innovations

www.active-bytes.com

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.

CYBOT™ Threat Hunting

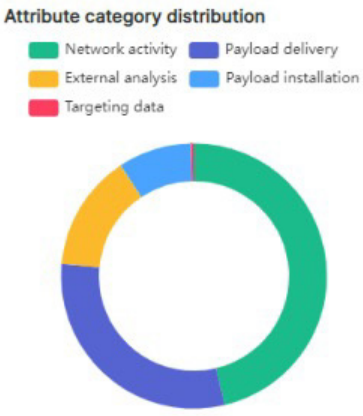
In this era of advanced adversary techniques including non-human cyber attacks, an enterprise needs to point towards a threat hunting solution that is beyond manual capabilities. CYBOT™s intelligent automated playbooks can automatically perform threat hunting and detect the advanced threat that hides in your enterprise environment, thereby helping your enterprise to enhance the IT security infrastructure with high efficiency, without compromising the IT processes. CYBOT™ has a large set of inbuilt automate threat hunting use cases and fast Incident response 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.

CYBOT™ got your IT infrastructure covered

With rich feeds from various IOC sources, host and network sensors, TIP and datalake, makes the automated playbooks work with extra efficiency and speed than a human can perform.

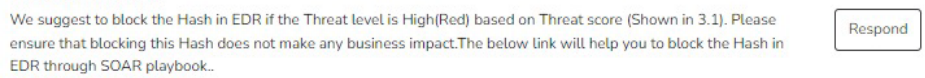
Playbooks in CYBOT™ is scripted based on 3 approaches. CYBOT™ protects your infrastructure with multi-dimensional security.

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

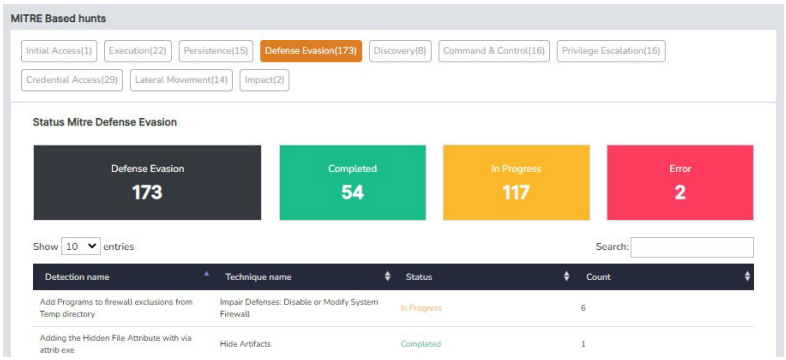


Immediately notifies on adversary through alert & suggestion

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

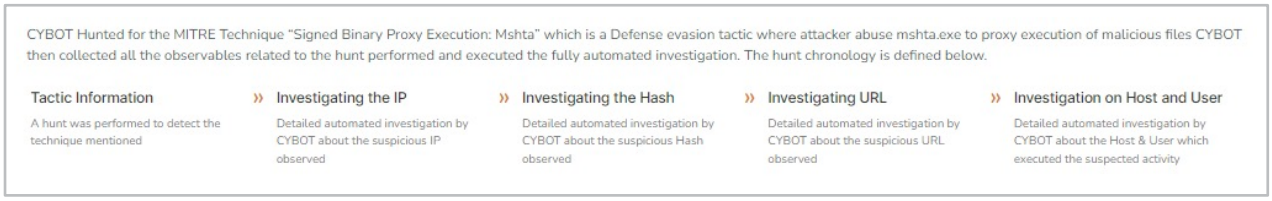


Detailed reports of investigation where a malicious attack technique was detected



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

Every suspicious IOCs, patterns identified from hunts are subjected to analysis in real-time ,thereby saving time for analysts and covering huge data

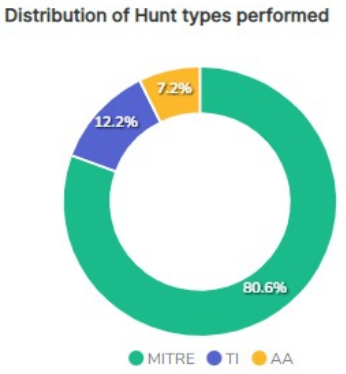


Investigates and suggests to respond via security solutions configured in the enterprise network such as AV, EDR, NDR, Vulnerability scanners, SIEM, etc.

The scores will help analysts in deciding what type of response need 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.

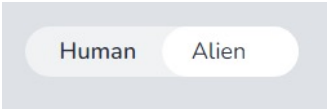
The categorized, detailed results and status of automated investigation benefits the enterprise security team as well as the management in decision making.



Detection name	Execution Status	Count
Malicious Domain Communications	In Progress	7
Malicious Domain Communications	Completed	4
Malicious Hash Communications	In Progress	7

Investigation exception on specific IOCs easily setup, making the hunt flexible to analysts requirement.

Smart and Faster than a Human



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

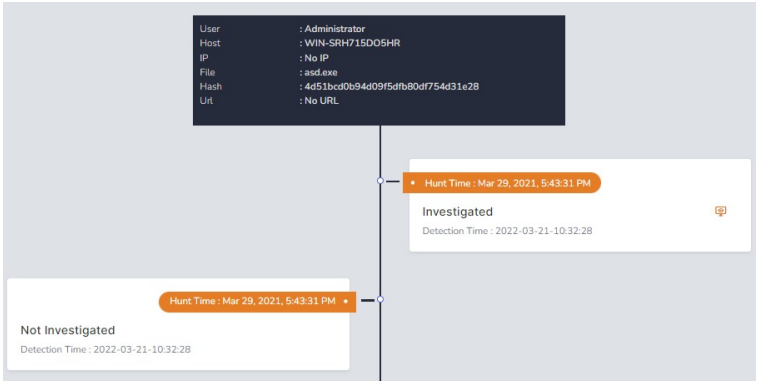
Some features include

- 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.
- Investigate identified observables in internet-based reputations sources.
- Convenient for analysts
  - Score of the hunted threat and the respond button allow the analyst to decide responsive action.
- Clear description of hunting tactic used
  - MITRE
  - IOC Based Hunt
  - Advanced Analytics
- Chained investigation scenarios
- Allow the analyst to automate response actions suggested by the playbooks based on respective observables via a button.
- Has feedback mechanism for easy incident creation on the threat intelligence platform with IOCs of any newly identified threat.

- User-friendly dashboards & respond button, automation exception creation, automation scheduling, user management, backup & restore etc available in the platform, making it flexible according to enterprise environment
- Intelligent & automated threat-hunting framework that effectively protect critical infrastructures against suspicious activity, incidents and vulnerabilities

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.

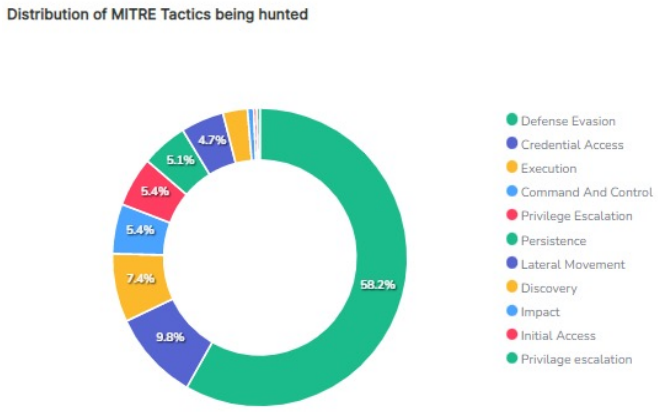


- **Intelligent automation playbooks can hunt and investigate in case any unusual pattern is detected from logs.**
- **The automated workflow of investigation is very fast and hence quick suggestion and response time for analysts.**

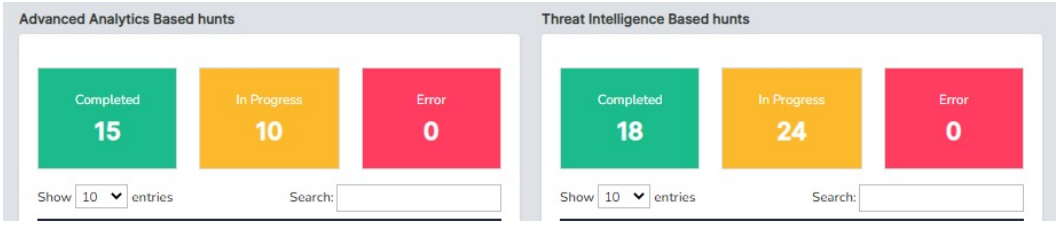
To know details about the Workflow click here

- About Hunt
  CYBOT hunted for the MITRE Tactic defined
- Tactic Information
  A hunt was performed to detect the technique mentioned
- Process Investigation
  Detailed automated investigation by CYBOT about the suspicious Process observed.
- Investigating the IP
  Detailed automated investigation by CYBOT about the suspicious IP 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
- Conclusion

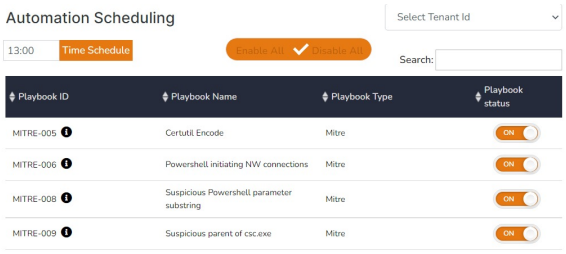
- **In depth automatic hunt with minimum or no manual input, making multiple investigations at a time, which saves analysts' time to stop or neutralize the threat.**



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



- **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.**

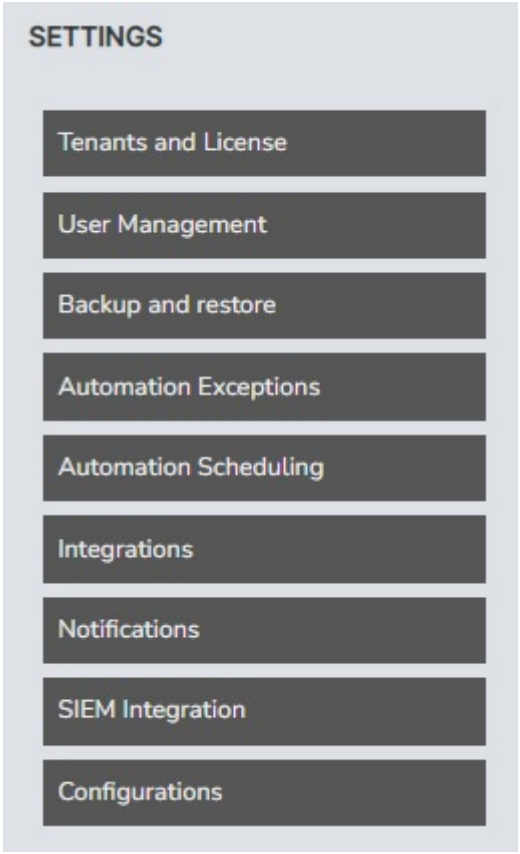


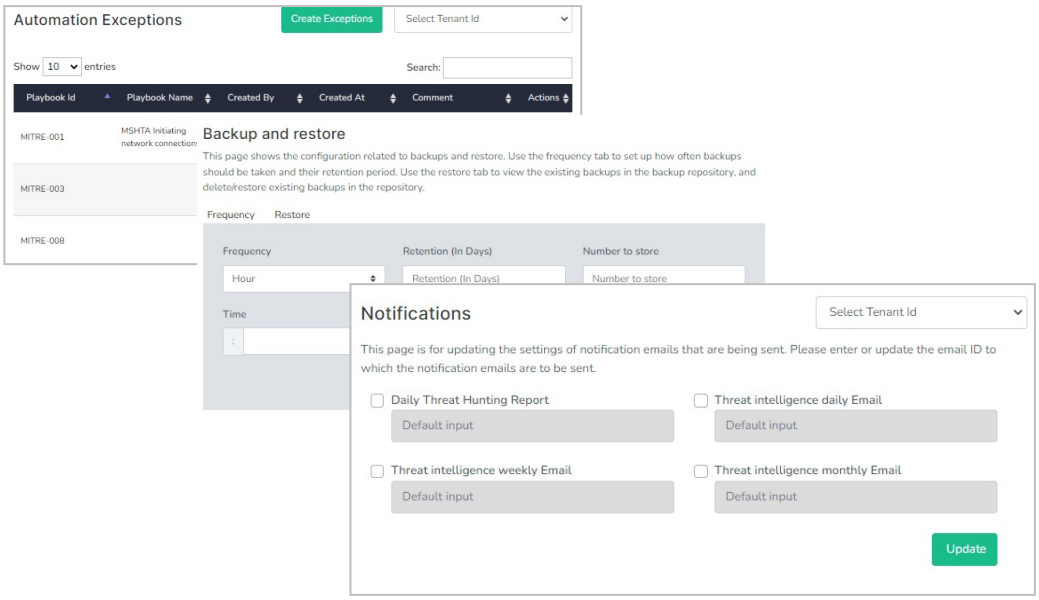
Other Features

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





SAMPLE CYBOT™ INVESTGATION SCENARIO

Platform hunts for an attack tactic, and collect observables if found any occurrences, cross-check the occurrences to recent hunts to reduce noise and false positives, finally present all the detection related information to analysts.

1. Tactic, Hunt Information and Observables

1.1 MITRE Technique Information

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.

Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup. The startup folder path for all users is C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp.

Read More

1.2 Detected Observables

Process Name : explorer.exe
Process Command: No commandline found
Process ID : 792
Process Parent Name : No parent process found
User Name : Alice

User Domain : WIN-SRH715DO5HR
Host Name : WIN-SRH715DO5HR
Process Executable : C:/Windows/explorer.exe
Source IP :
Detection Name : Registry persistence via Shell folders
Last detection : Mar 10, 2021, 10:19:08

Registry Path : HKEY_USERS/S-1-5-21-1176950347-982008390-404917063-1000/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/Shell Folders/AppData
Registry Value : {'strings': ['C://Users//Alice//AppData//Roaming'], 'type': 'REG_SZ'}

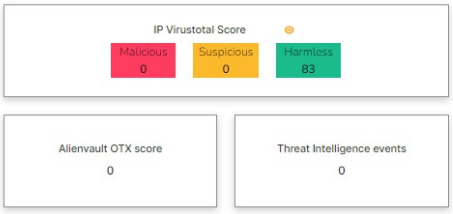
As it is a trusted binary of Microsoft making network traffic, the platform further investigates the reputation of IP, score it. If there are any threat intelligence events, CYBOT™ gives the respective link for seamless access for analysts.

3.1 IP Investigating IP1: 169.254.171.195

3.1.1 IP Threat Score

Information of the observed process was collected from the datalake. The below panel shows the obtained data. This shows useful details like the process hash, commandline, signer etc.

Source IP:
User Name : ASUS
Process Name : WMIC.exe
Detection Name : Detects WMI executing suspicious Commands

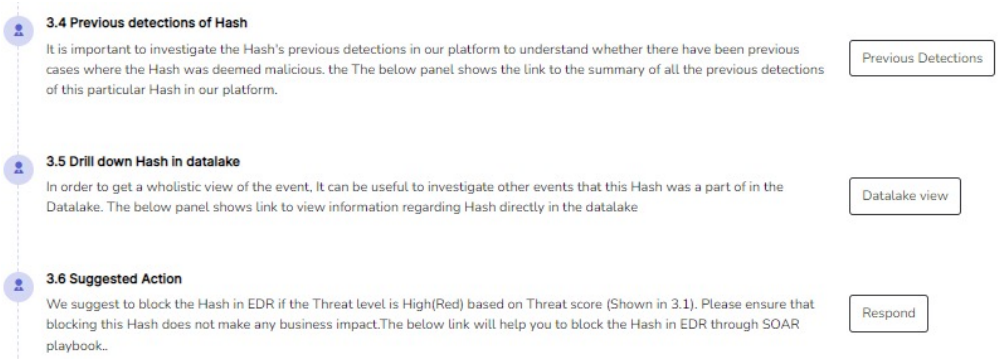


Platform looks for any other servers or user PCs that made traffic to the suspicious IP from entire organization logs.

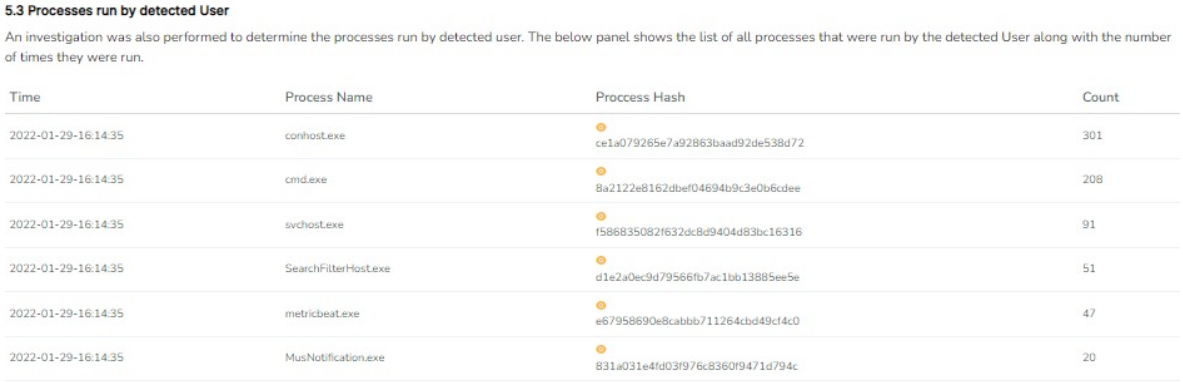
2.3 Traffic from other hosts to detected IP

Further investigation was performed to check if the IP was visited by other hosts in the network. The below panel shows the list of other hosts from which traffic was detected to the observed IP, along with the frequency of the traffic.

Platform then enables users to see previous hunt detections for the same IP as well as investigates further about the traffic to the same IP manually for threat analysts for further insights. Even suggest a response action as well, which calls a playbook of workflow what the organization desires to do in SOAR. Either simply block the IP or drop a mail to the network team for blocking the IP.



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. Processes ran by the same account across the organization. Picking all uncommon process infrastructure wide ran by the user and checking the reputation of all those process hashes



5.6 Uncommon Processes run by detected User

An investigation was also performed to determine the processes run in the detected host. The below panel shows the list of all processes that were run in the detected host around the time of detection along with the number of times they were run.

Time	Process name	Process Reputation (VirusTotal)	Process Hash
2022-02-22-18:16:58	SearchUI.exe	0	67fc4d83f558e0ef85941b00eb01b2f0
2022-02-22-18:16:58	HxTsr.exe	0	f43a716fb10240336c1588482a818a52
2022-02-22-18:16:58	ShellExperienceHost.exe	0	0e60b8fd1d1831e817ac1b5c3bee80d4
2022-02-22-18:16:58	mcupdate.exe	0	abbaf027be8f1ec8efd4119b644cf31d
2022-02-22-18:16:58	whoami.exe	0	2eeeec89e705f73ffbcae014e1828788

Platform then summarizes the investigation out comes for both technical and non-technical resources

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.

LIST OF INTELLIGENT PLAYBOOKS CURRENTLY AVAILABLE IN THE PLATFORM

MITRE Based Hunts			
Sl. No.	Playbook name	Description	MITRE Technique ID
1	Mshta initiating Network Connections	This automation playbook investigates every attempted network connection by MSHTA	T1218.005
2	Unload Sysmon Filter Driver with fltmc.exe	This automation playbook investigates every event where sysmon driver was attempted to be unloaded	T1562.001
3	Suspicious Bitsadmin Job via bitsadmin.exe	This automation playbook investigates every suspicious bitsadmin jobs	T1197
4	Conhost spawned by suspicious parent	This automation playbook investigates conhost spawned by suspicious parent	T1059
5	Office spawning powershell	This automation playbook investigates every time MS office applications spawn powershell	T1137
6	Certutil Encode	This automation playbook investigates every time certutil was used to encode strings or files	T1140
7	Powershell initiating NW connections	This automation playbook investigates every time powershell initiates network connections	T1546.013
8	Install Util execution with suspicious command lines	This automation playbook investigates every time installutil was run with suspicious commandline arguments	T1218.004
9	Suspicious Powershell parameter substring	This automation playbook investigates every time powershell commands where executed with suspicious parameters	T1059.001
10	Suspicious parent of csc.exe	This automation playbook investigates every time csc.exe was called by a suspicious parent process	T1027.004
11	Programs executing from suspicious location	This automation playbook investigates every time programs were executed inside suspicious locations	T1036.005
12	Suspicious Rundll32 Activity	This automation playbook investigates every time rundll32 was executed with suspicious parameters	T1218.001
13	Add Programs to firewall exclusions from Temp directory	This automation playbook investigates every time rundll32 was executed with suspicious parameters	T1204.002
14	Suspicious script executions	This automation playbook investigates every time suspicious scripts where executed	T1059.001
15	Webshell detection with command line keywords	This automation playbook investigates every time webshell scripts were attempted to be executed	T1505.003
16	Rundll initating network connection	This automation playbook investigates every time rundll32 was initiating a network connection	T1218.011
17	Net.exe Execution	This automation playbook investigates every time net.exe was executed	T1569.002
18	Processes created by MMC	This automation playbook investigates every time mmc created a process	T1543
19	Mimikatz detections LSASS Access	This automation playbook investigates every time lsass was accessed using indicators specific to mimikatz	T1003.001
20	Detects WMI executing suspicious Commands	This automation playbook investigates every time wmi was executing suspicious commands	T1047
21	Microsoft binary Github communication	This automation playbook investigates every time github communication was attempted by Microsoft binaries	T1218
22	Microsoft Outlook Spawning Windows Shell	This automation playbook investigates every time outlook was detected to be spawning a windows shell	T1566

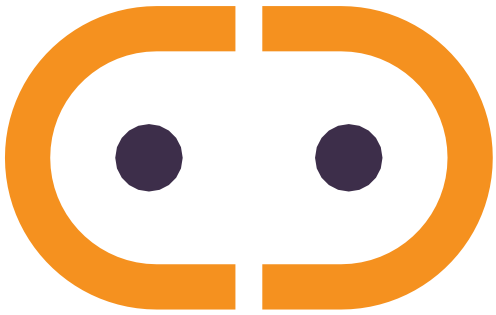
Sl. No.	Playbook name	Description	MITRE Technique ID
23	Suspicious Reconaissance activity	This automation playbook investigates every time suspicious reconnaisance activity was detected	T1018
24	Windows task manager as parent	This automation playbook investigates every time task manager is detected as a parent process for suspicious child processes	T1134.004
25	lsass Access from NON System Account	This automation playbook investigates every time lsass was accessed using non system account	T1003.001
26	RDP or SSH from external IP's	This automation playbook investigates every time ssh was accessed from external network IP addresses	T1219
27	Tor traffic to Internet	This automation playbook investigates every time tor traffic was detected to internet	T1090.002
28	Powershell remote session	This automation playbook investigates every time powershell was detected to be remotely accessed	T1021
29	Adding the Hidden File Attribute with via attrib.exe	This automation playbook investigates every time hidden file attribute was added via attrib.exe	T1564
30	Execution of existing service via cmd	This automation playbook investigates every time services was executed by cmd	T1569.002
31	Volume shadow copy removals	This automation playbook investigates every time volume shadow copy was removed	T1490
32	HH.exe execution	This automation playbook investigates every time hh.exe was executed with suspicious parameters	T1218.001
33	Host artifact deletions	This automation playbook investigates host artifact deletions	T1070
34	Interactive AT jobs	This automation playbook investigates interactive AT jobs creations	T1053.002
35	LSA authentication packages	This automation playbook investigates LSA authentication packages editions in registry	T1003.004
36	LSASS memory dumping	This automation playbook investigates LSASS memory dumping techniques	T1003.001
37	Modification of boot configs	This automation playbook investigates boot configuration editions in registry	T1547.009
38	Modification of logon scripts from registry	This automation playbook investigates logon scripts editions in registry	T1037.001
39	Mounting hidden shares	This automation playbook investigates every time hidden shares were mounted	T1021.002
40	Persistance via Appinit dll	This automation playbook investigates attempted persistence via Appinit.dll	T1546.010
41	Persistance via netsh key	This automation playbook investigates attempted persistence via Netsh key in registry	T1547.009
42	Persistance via screensaver	This automation playbook investigates screensaver persistence via registry	T1546.002
43	Process discovery via builtin tools/windows tools	This automation playbook investigates process discovery using builtin tools	T1057
44	Processes Running with unusual Extensions	This automation playbook investigates process processes running with unusual extensions	T1036.006
45	Registration of winlogon helper dll	This automation playbook investigates winlogon helper dll registration	T1547.004
46	Registry persistence via Shell folders	This automation playbook investigates persistency via shell folders registry entry modification	T1547.001
47	Root Certificate install	This automation playbook investigates root certificate installations	T1553.004

Sl. No.	Playbook name	Description	MITRE Technique ID
48	SAM dumping via reg.exe	This automation playbook investigates SAM dumping via reg. exe	T1003.002
49	Service path modification via sc.exe	This automation playbook investigates SAM dumping via reg. exe	T1543.003
50	Service Stop or disable with sc.exe command	This automation playbook investigates services being stopped or disabled via sc.exe	T1543.003
51	Suspicious script object executions	This automation playbook investigates services being stopped or disabled via sc.exe	T1218.010
52	Possible windows network enumeration	This automation playbook investigates possible windows network enumeration techniques	T1018
53	AD dumping via ntdsutil.exe	This automation playbook investigates possible AD dumping via ntdsutil	T1003.003
54	UAC bypass via eventviewer	This automation playbook investigates possible UAC bypass via eventviewer	T1548.002
55	UAC bypass via sdclt	This automation playbook investigates possible UAC bypass via eventviewer	T1548.002
56	Registry Persistence via Explorer Run key	This automation playbook investigates persistence vua explorer run key modifications in registry	T1547.001
57	Possible No powershell executions	This automation playbook investigates possible no powershell executions	T1546
58	Possible Hooking detections	This automation playbook investigates possible hooking	T1197
59	Renamed Powershell	This automation playbook investigates possible renamed powershell executions	T1059.001
60	Powershell/VBS script downloads from internet	This automation playbook investigates possible script downloads from internet	T1059
61	Possible port Forwarding detected	This automation playbook investigates possible port forwarding	T1572
62	Suspicious use of Public Folder	This automation playbook investigates suspicious usage of public folder	T1036.005
63	Systeminfo executions	This automation playbook investigates systeminfo executions	T1082
64	Suspicious WMIC XSL Script Execution	This automation playbook investigates suspicious wmic xsl script execution	T1220
65	Suspicious control DLL load	This automation playbook investigates suspicious control.exe loading dll	T1218
66	Connection to external Network via Telnet	This automation playbook investigates connection to external network via telnet	T1021
67	Discovery of Remote system's Time	This automation playbook investigates discovery of remote system's time	T1124
68	File And Directory Permissions Modification	This automation playbook investigates file and directory permisions modification	T1222
69	Direct RDP Enabling via psexec	This automation playbook investigates Direct RDP enabling via psexec	T1021.001
70	Detect cmdkey Malicious Activity	This automation playbook investigates malicious cmdkey activity	T1555
71	Potential DNS tunneling via nslookup-TA0011	This automation playbook investigates potential dns tunneling	T1071.004
72	Remote file copy mpcmdrun-T1105	This automation playbook investigates potential file copy via mpcmdrun	T1105

Sl. No.	Playbook name	Description	MITRE Technique ID
73	Remote file copy via Teamviewer-T1105	This automation playbook investigates potential file copy via teamviewer	T1105
74	NTDS or SAM Database File Copied-T1003	This automation playbook investigates potential copy of ntds or sam database file	T1003
75	Execution via Regsvcs/ Regasm-TA002,T1121	This automation playbook investigates potential execution via regsvcs or regasm	T1218.009
76	adfind command activity	This automation playbook investigates potential adfind execution	T1069.002
77	Clearing windows event logs	This automation playbook investigates potential windows event log clearing attempts	T1070.001
78	Windows defender disabled via registry modification	This automation playbook investigates windows defender disabling via registry modifications	T1562

Threat Intelligence Based Hunts		
Sl. No.	Playbook name	Description
1	Malicious IP Communications	This automation playbook investigates malicious IP communications from Threat Intelligence
2	Malicious Domain Communications	This automation playbook investigates malicious domain communications
3	Malicious HASH identification	This automation playbook investigates malicious hashes executions

Advanced Analytics Based Hunts		
Sl. No.	Playbook name	Description
1	User login from unknown location-Bypassing baseline	This automation playbook investigates user logons from unusual locations
2	User login from unusual workstations	This automation playbook investigates user logons from unusual hosts
3	Unknown/New process executions	This automation playbook investigates unusual process executions
4	Unknown/New HTTP POST requests	This automation playbook investigates unusual HTTP post requests
5	Possible C&C beacons	This automation playbook investigates potential C&C beacons
6	Domain Lookup Anomalous increase-DNS	This automation playbook investigates anomalous DNS lookup increase
7	Least common parent child process Combinations	This automation playbook investigates anomalous parent-child process combinations



activebytes innovations

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