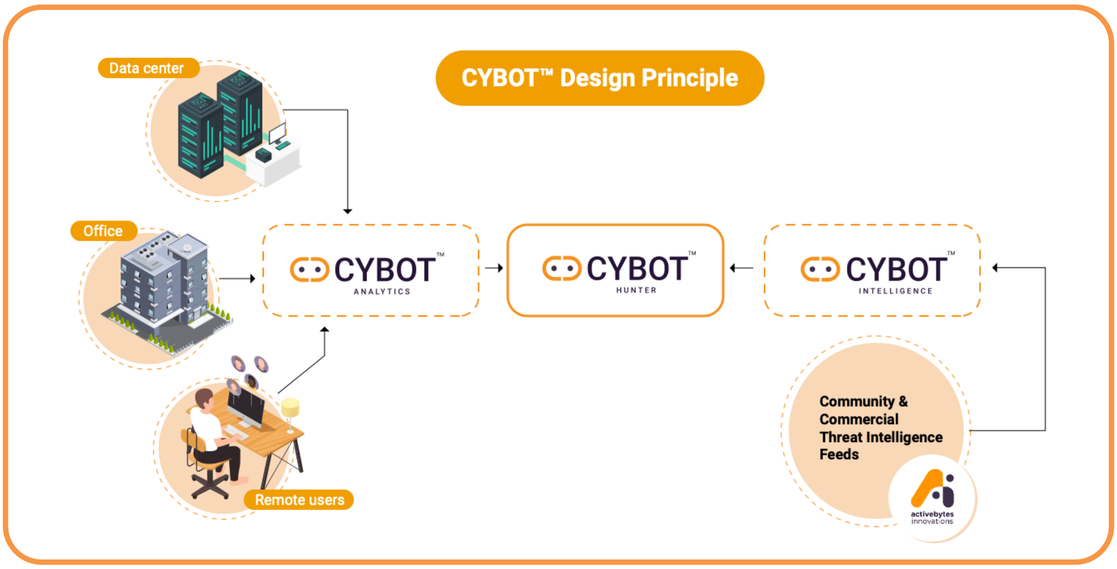
CYBOT™

Automated Investigation & Hunting Platform

Datasheet: CYBOT™ Hunter

About the CYBOT™

- CYBOT™ collects raw logs from the enterprise network, remote users, servers and stores them to its Analytical engine in a contextualized and secured way. The logs then undergo intelligent automatic analysis, thereby going the extra mile in threat hunting which, a human cannot.
- 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 on the network.



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

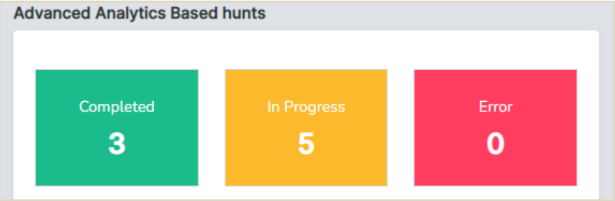
Raw data collected via sensors from servers, networks and endpoints of the enterprise environment are fed into the Analytical engine and then stored in a unified, contextualized and secured format. CYBOT™ is designed to be intelligent and adaptive. The platform is continuously updated with automated 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

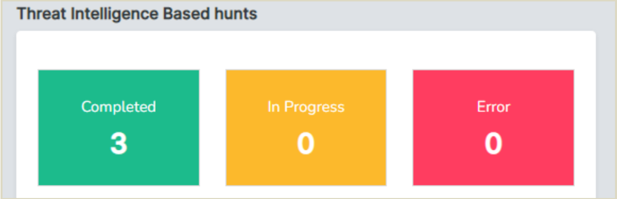
In this era of advanced adversary techniques including non-human cyber attacks, an enterprise needs to focus on a threat hunting solution that is efficient beyond manual capabilities. CYBOT™s intelligent automated playbooks can automatically perform threat hunting and detect the advanced threats that 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.**



Advanced Analytics Based hunts

Completed	In Progress	Error
3	5	0



Threat Intelligence Based hunts

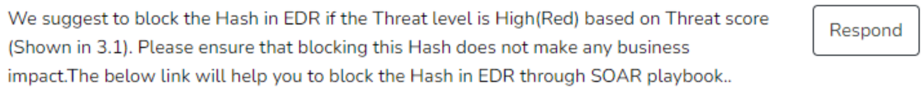
Completed	In Progress	Error
3	0	0

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

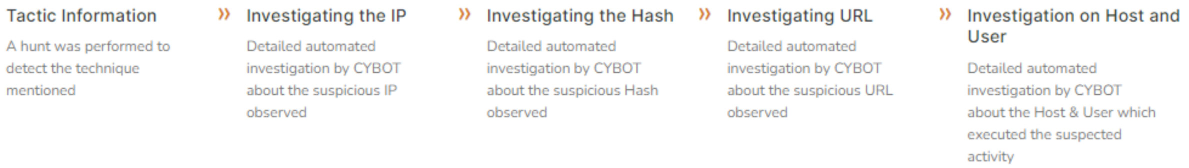
✓ **Immediately notifies on adversary through alert & suggestion**

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



We suggest to block the Hash in EDR if the Threat level is High(Red) based on Threat score (Shown in 3.1). Please ensure that blocking this Hash does not make any business impact.The below link will help you to block the Hash in EDR through SOAR playbook..

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



Tactic Information » Investigating the IP » Investigating the Hash » Investigating URL » Investigation on Host and User

Tactic Information: A hunt was performed to detect the technique mentioned

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

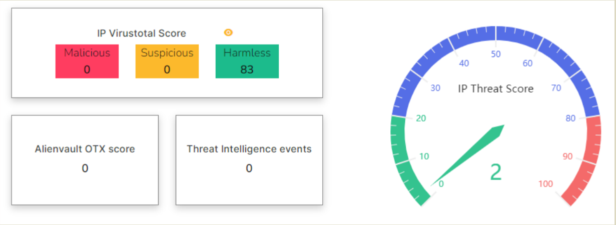
Investigating the Hash: Detailed automated investigation by CYBOT about the suspicious Hash observed

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.

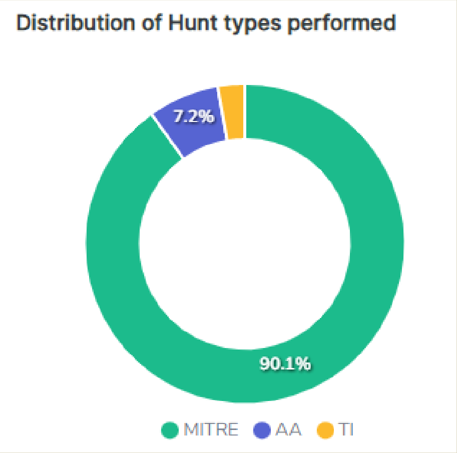


IP Virustotal Score

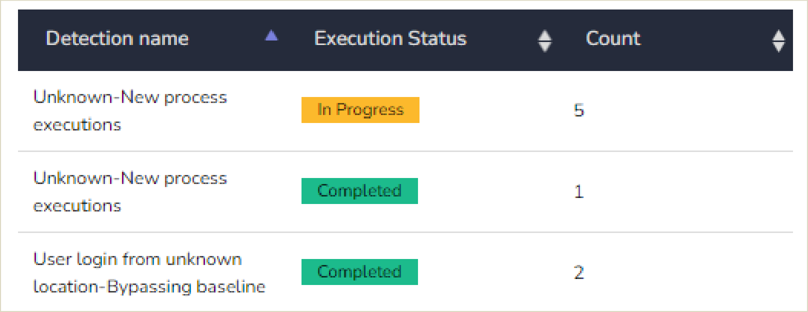
Malicious	Suspicious	Harmless
0	0	83

Alienvault OTX score: 0

Threat Intelligence events: 0

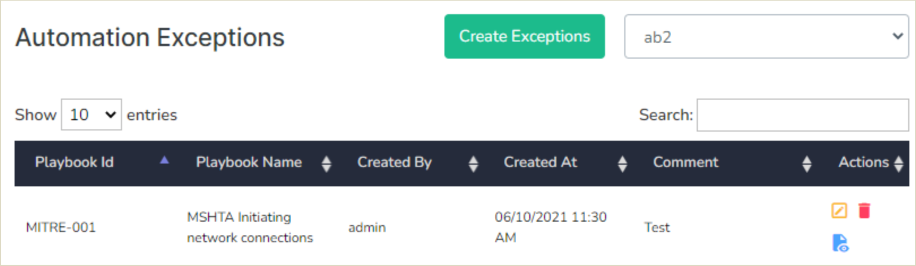


Distribution of Hunt types performed



Detection name	Execution Status	Count
Unknown-New process executions	In Progress	5
Unknown-New process executions	Completed	1
User login from unknown location-Bypassing baseline	Completed	2

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

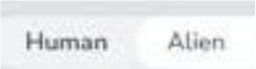


Automation Exceptions

Playbook Id	Playbook Name	Created By	Created At	Comment	Actions
MITRE-001	MSHTA Initiating network connections	admin	06/10/2021 11:30 AM	Test	

Smart and Faster than a Human

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

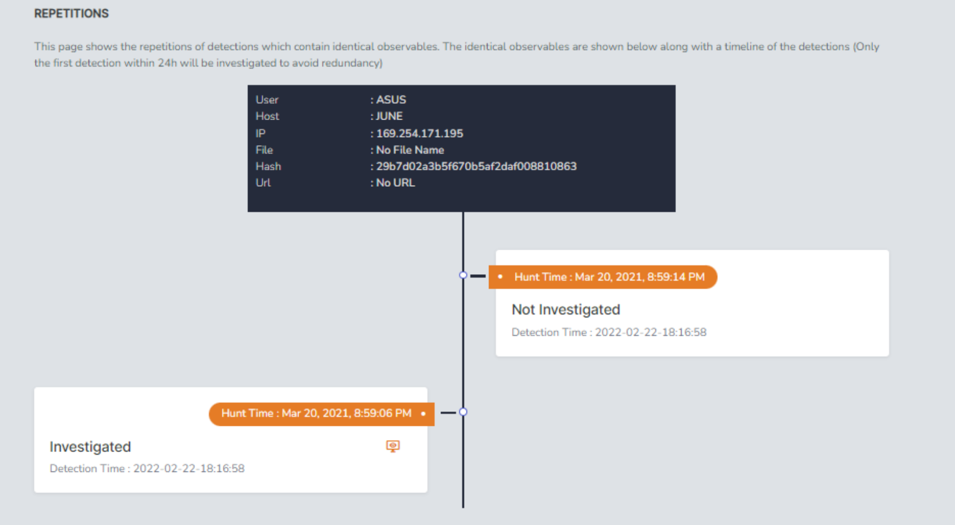


Some features include

- 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.



REPETITIONS

This page shows the repetitions of detections which contain identical observables. The identical observables are shown below along with a timeline of the detections (Only the first detection within 24h will be investigated to avoid redundancy)

```
User      : ASUS
Host      : JUNE
IP        : 169.254.171.195
File      : No File Name
Hash      : 29b7d02a3b5f670b5af2daf008810863
Url       : No URL
```

Hunt Time : Mar 20, 2021, 8:59:14 PM

Not Investigated

Detection Time : 2022-02-22-18:16:58

Hunt Time : Mar 20, 2021, 8:59:06 PM

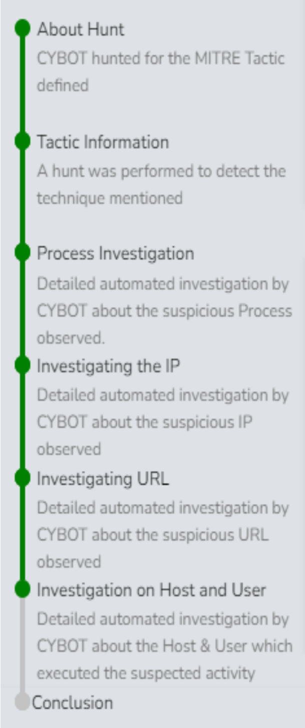
Investigated

Detection Time : 2022-02-22-18:16:58

To know details about the Workflow click here

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



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

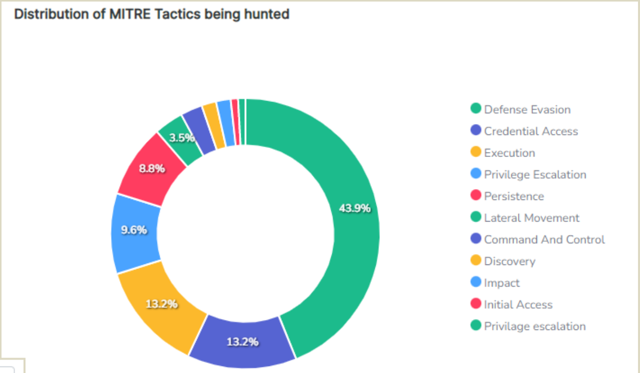
Other Features

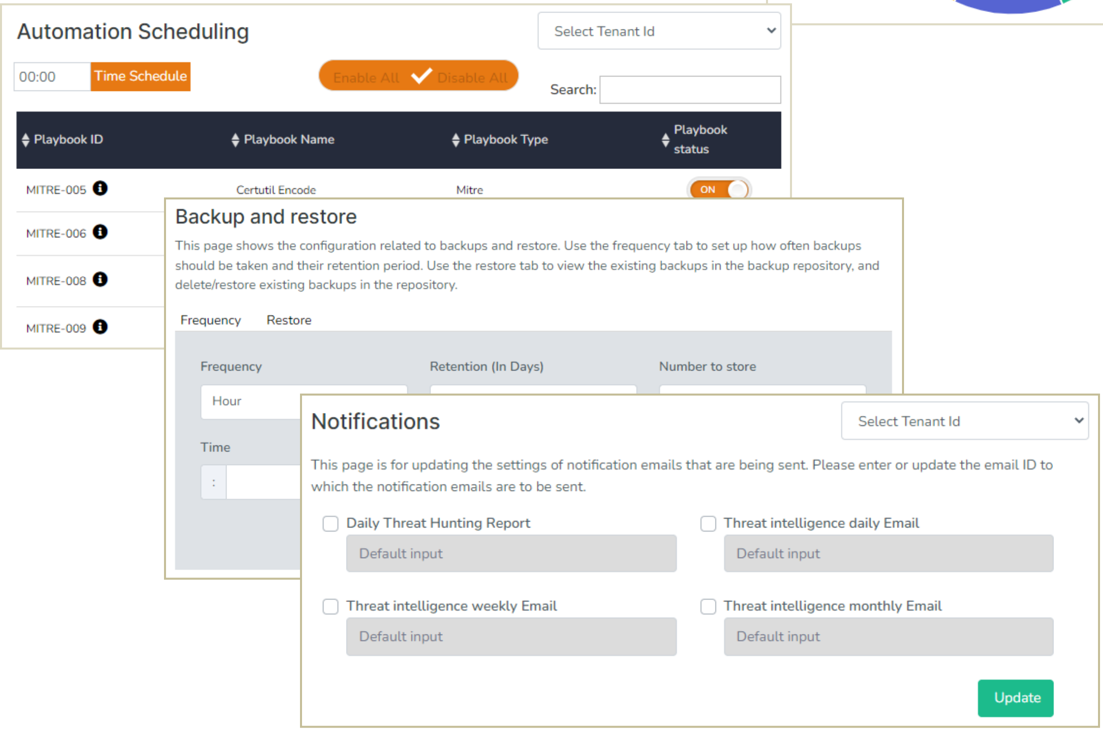
A list of options is available for the security team or administrator which is customizable as per your organization's requirements.

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





Playbook ID	Playbook Name	Playbook Type	Playbook status
MITRE-005	Certutil Encode	Mitre	ON
MITRE-006			
MITRE-008			
MITRE-009			

Backup and restore

This page shows the configuration related to backups and restore. Use the frequency tab to set up how often backups should be taken and their retention period. Use the restore tab to view the existing backups in the backup repository, and delete/restore existing backups in the repository.

Frequency: Hour

Retention (In Days)

Number to store

Time

Notifications

This page is for updating the settings of notification emails that are being sent. Please enter or update the email ID to which the notification emails are to be sent.

- □ Daily Threat Hunting Report: Default input
- □ Threat intelligence daily Email: Default input
- □ Threat intelligence weekly Email: Default input
- □ Threat intelligence monthly Email: Default input

activebytes innovations

www.active-bytes.com / contact@active-bytes.com

+971 50 513 3973

CYBOT™

activebytes innovations