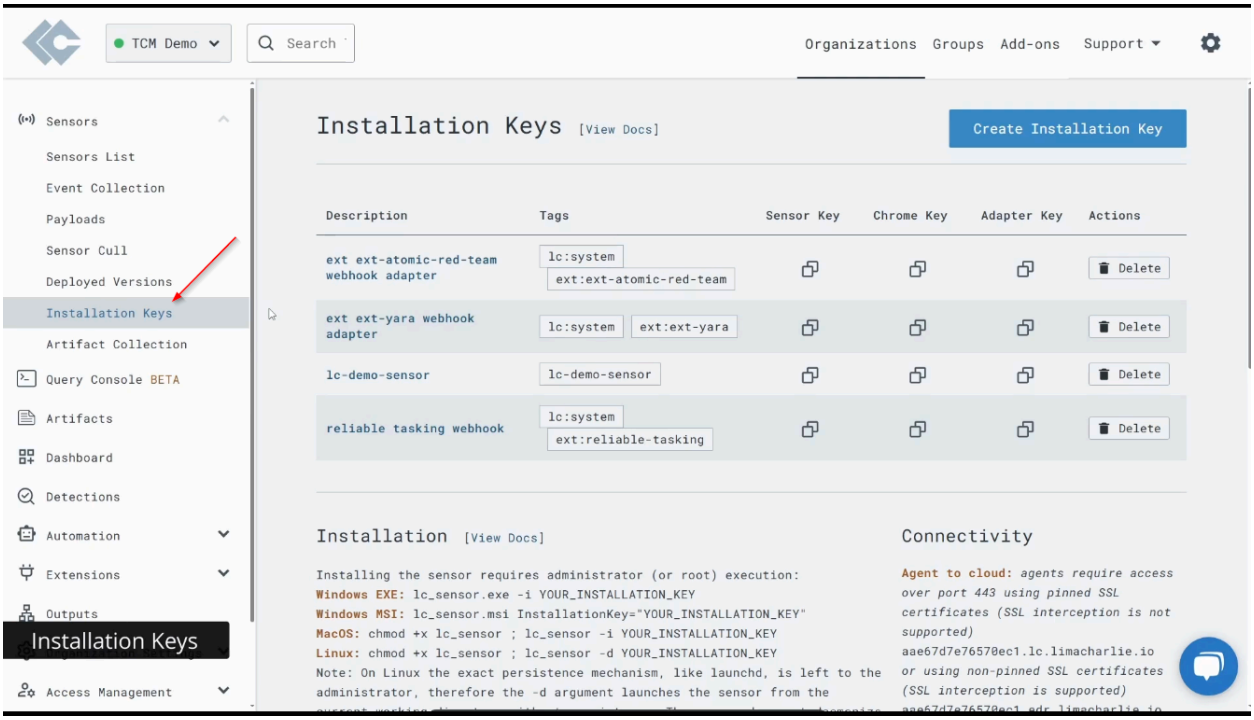
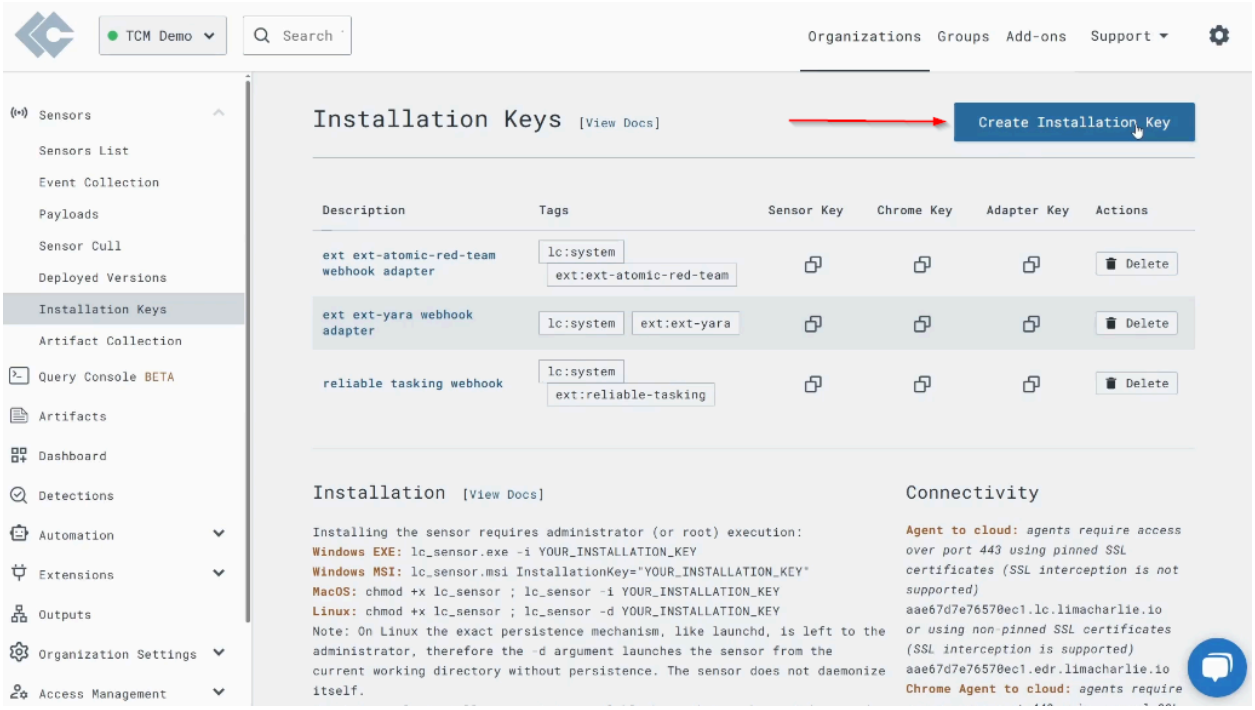
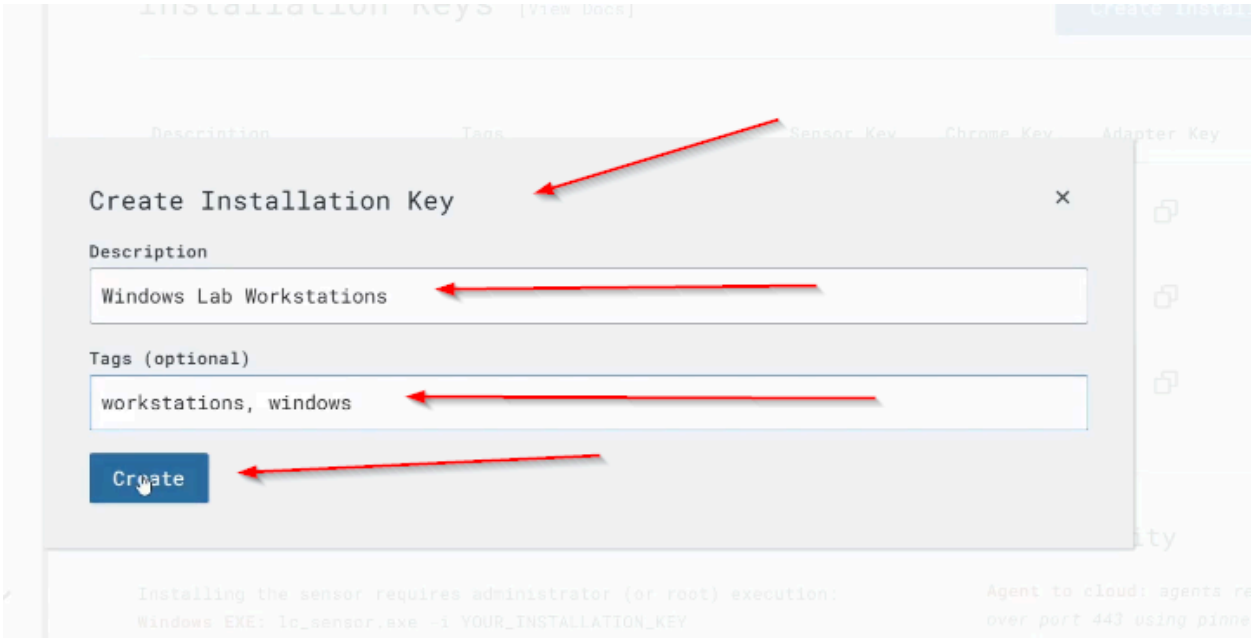
25. Lima Charlie - Deploying Endpoint Agents

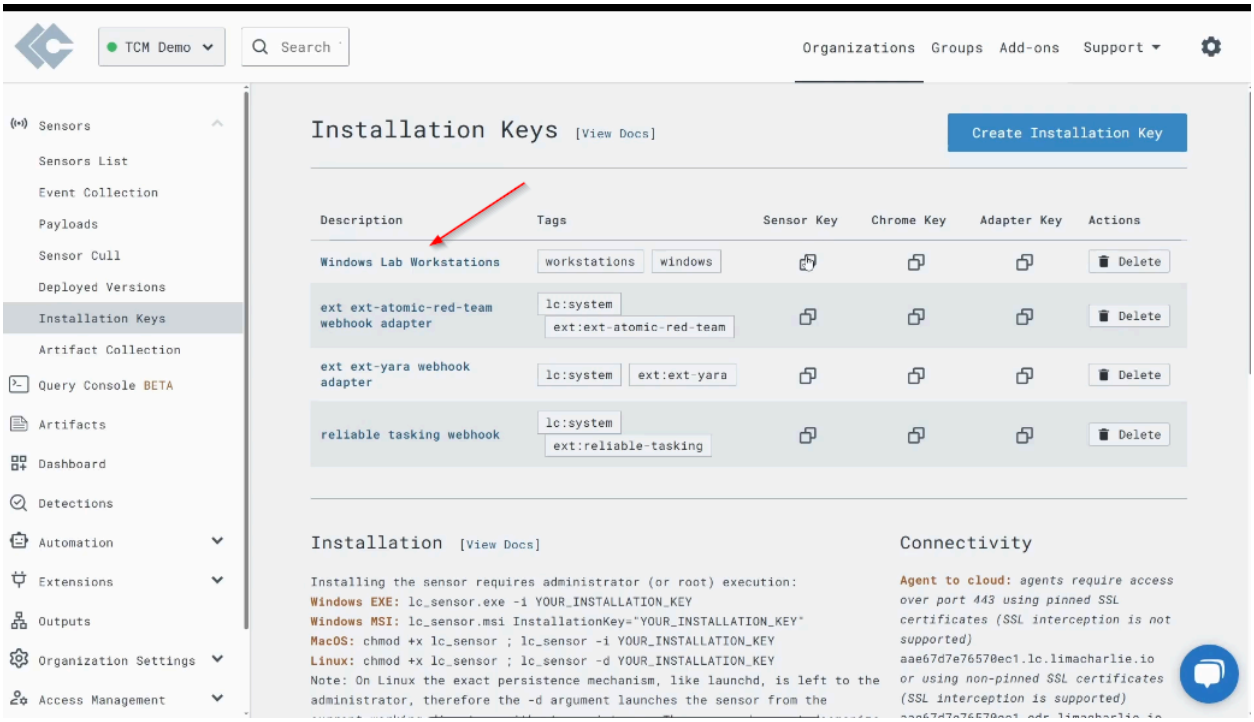
Lima Charlie Install producer:

1.) Installation Keys

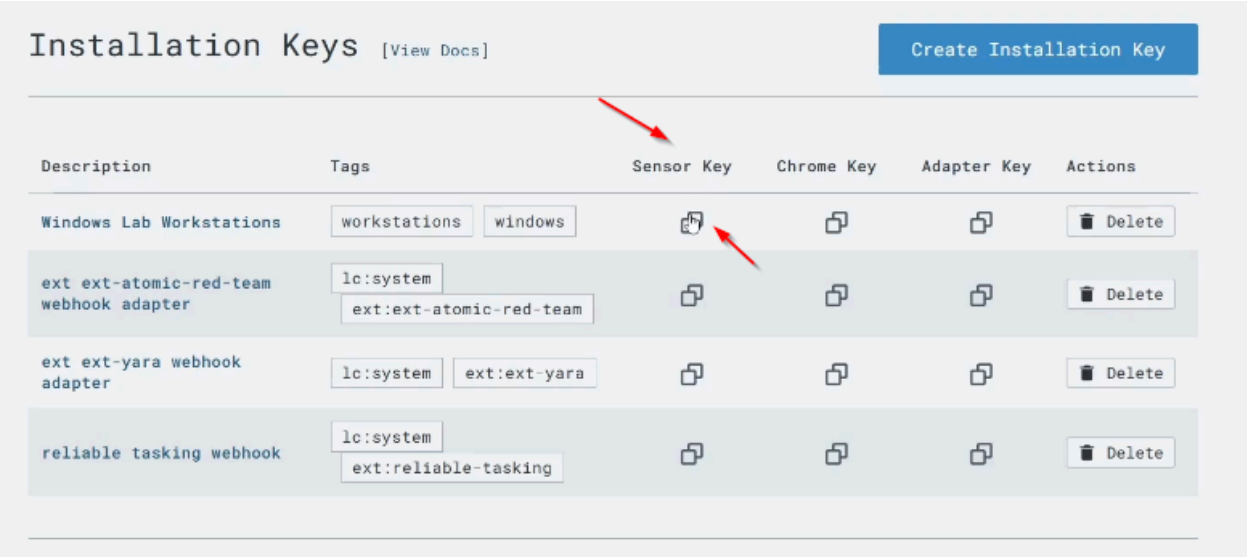



TCM Demo
Search
Organizations
Groups
Add-ons
Support
Sensors
Sensors List
Event Collection
Payloads
Sensor Cull
Deployed Versions
Installation Keys
Artifact Collection
Query Console BETA
Artifacts
Dashboard
Detections
Automation
Extensions
Outputs
Organization Settings
Access Management
Installation Keys [View Docs]
Create Installation Key
Description
Tags
Sensor Key
Chrome Key
Adapter Key
Actions
ext ext-atomic-red-team webhook adapter
lc:system
ext:ext-atomic-red-team
Delete
ext ext-yara webhook adapter
lc:system
ext:ext-yara
Delete
reliable tasking webhook
lc:system
ext:reliable-tasking
Delete
Installation [View Docs]
Installing the sensor requires administrator (or root) execution:
Windows EXE: lc_sensor.exe -i YOUR_INSTALLATION_KEY
Windows MSI: lc_sensor.msi InstallationKey="YOUR_INSTALLATION_KEY"
MacOS: chmod +x lc_sensor ; lc_sensor -i YOUR_INSTALLATION_KEY
Linux: chmod +x lc_sensor ; lc_sensor -d YOUR_INSTALLATION_KEY
Note: On Linux the exact persistence mechanism, like launchd, is left to the administrator, therefore the -d argument launches the sensor from the current working directory without persistence. The sensor does not daemonize itself.
Connectivity
Agent to cloud: agents require access over port 443 using pinned SSL certificates (SSL interception is not supported)
aae67d7e76570ec1.lc.limacharlie.io
or using non-pinned SSL certificates (SSL interception is supported)
aae67d7e76570ec1.edr.limacharlie.io
Chrome Agent to cloud: agents require


Create Installation Key
Description
Windows Lab Workstations
Tags (optional)
workstations, windows
Create

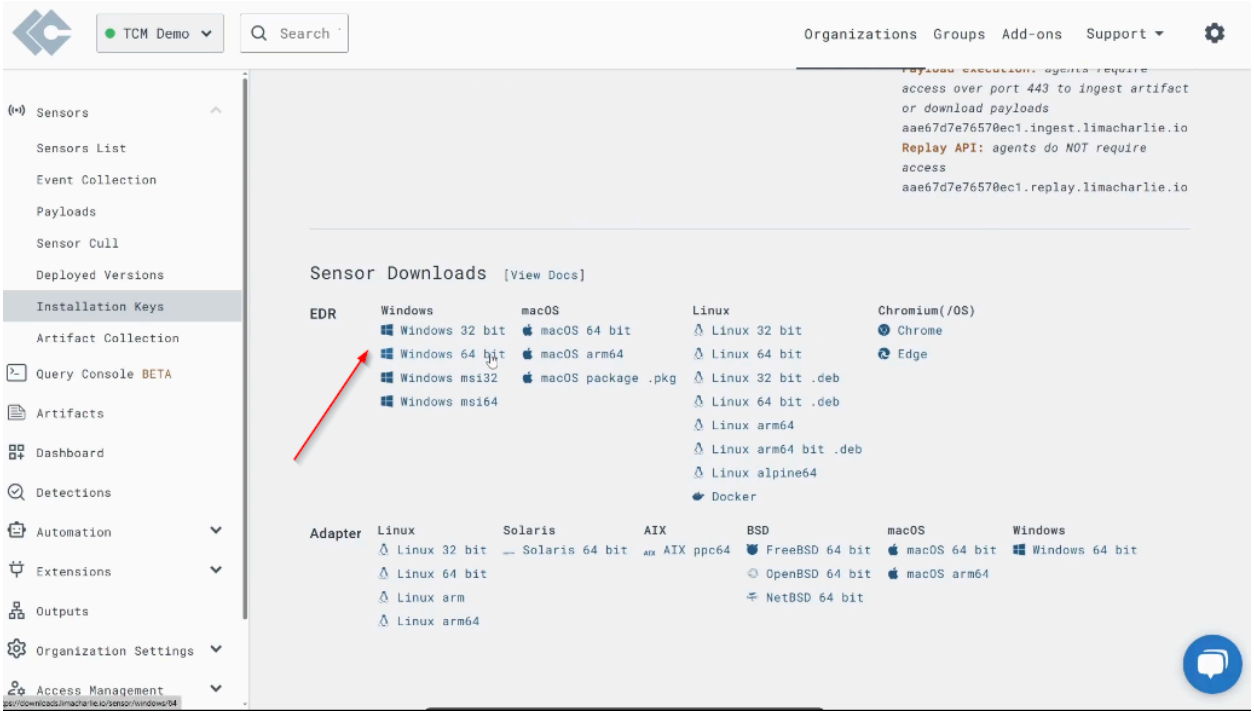


This Sensor key very important so copy

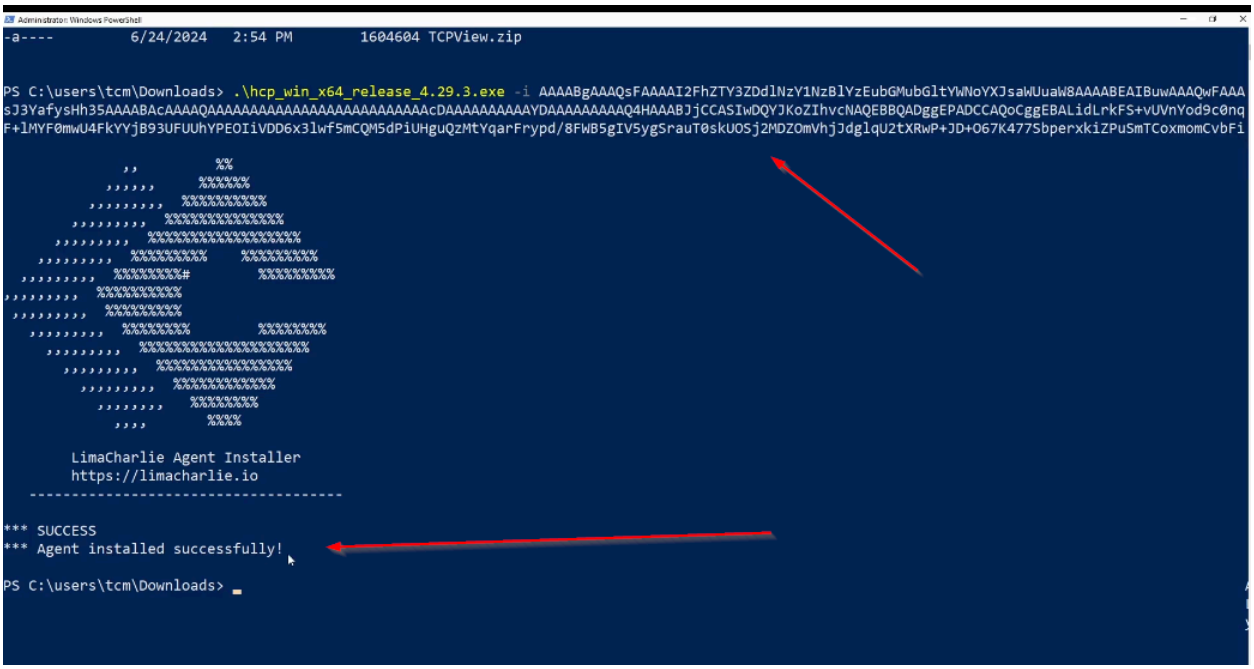


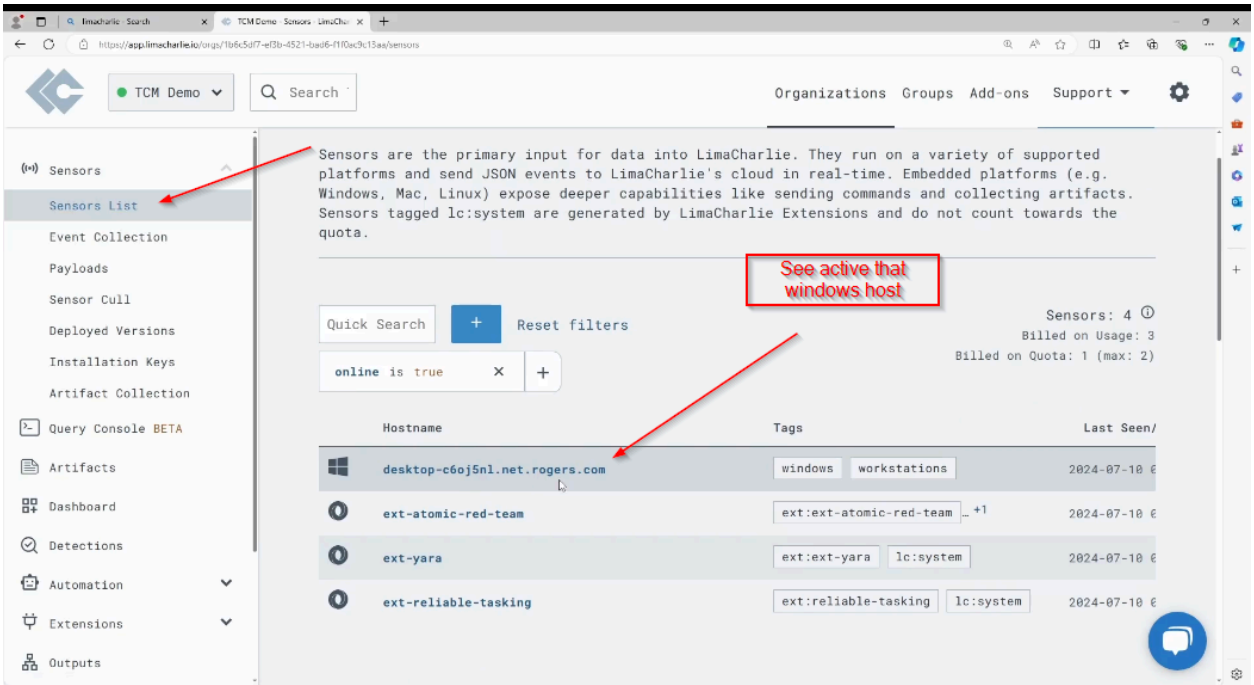
Download agent support OS case

But real case 10000 case endpoint there company so thus use ansible



Install agent in machine:

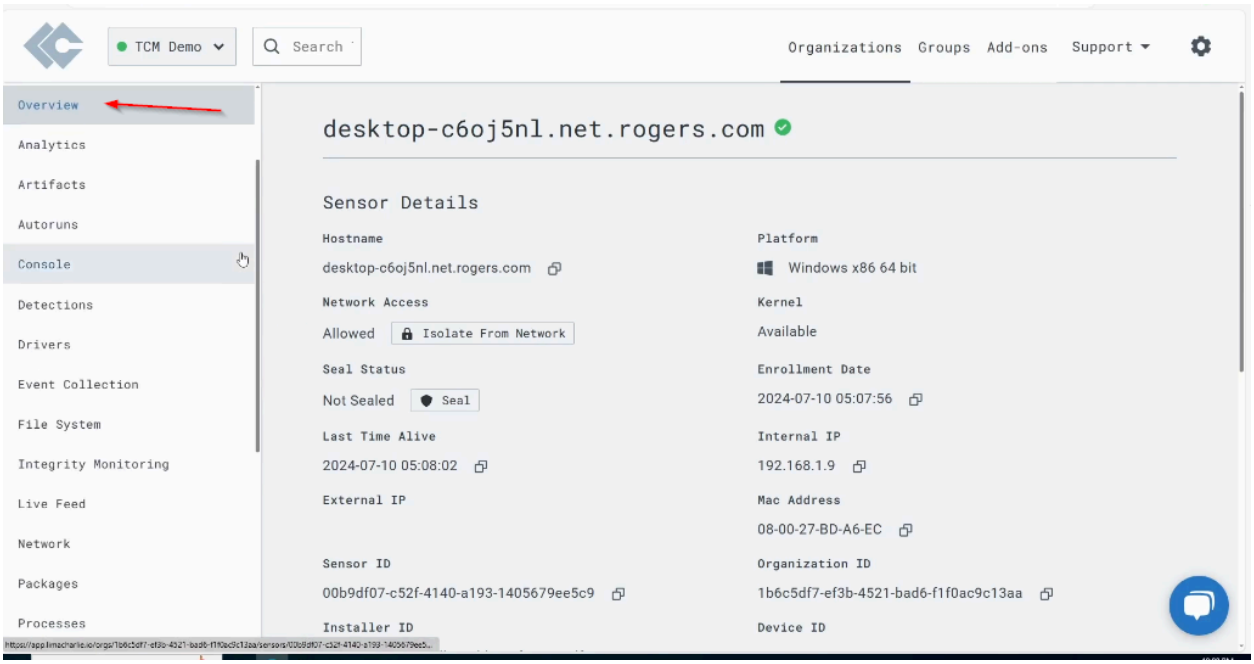

Administrator: Windows PowerShell
-a---- 6/24/2024 2:54 PM 1604604 TCPView.zip
PS C:\users\tcm\Downloads> .\hcp_win_x64_release_4.29.3.exe -i AAAABgAAAQsFAAAAI2FhZTY3ZDdlNzY1NzBlYzEubGMubGltYWNoYXJsaWUuaW8AAAABEAIBuwAAAQwFAAA
sJ3YafysHh35AAAABAcAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAcDAAAAAAAAAAAYDAAAAAAAAAQ4HAAABJjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALidLrkFS+vUVnYod9c0nq
F+lMYF0mwU4FkYYjB93UFUUhYPEOIiVDD6x3lwf5mCQM5dPiUHguQzMtYqarFrypd/8FWB5gIV5ygSrauT0skUOSj2MDZOmVhjJdglqU2tXRwP+JD+O67K477SbperxkiZPuSmTCoxmomCvbFi
LimaCharlie Agent Installer
https://limacharlie.io
*** SUCCESS
*** Agent installed successfully!
PS C:\users\tcm\Downloads>


TCM Demo
Search
Organizations
Groups
Add-ons
Support
Sensors
Sensors List
Event Collection
Payloads
Sensor Cull
Deployed Versions
Installation Keys
Artifact Collection
Query Console BETA
Artifacts
Dashboard
Detections
Automation
Extensions
Outputs
Sensors are the primary input for data into LimaCharlie. They run on a variety of supported platforms and send JSON events to LimaCharlie's cloud in real-time. Embedded platforms (e.g. Windows, Mac, Linux) expose deeper capabilities like sending commands and collecting artifacts. Sensors tagged lc:system are generated by LimaCharlie Extensions and do not count towards the quota.
See active that windows host
Quick Search
Reset filters
online is true
Sensors: 4
Billed on Usage: 3
Billed on Quota: 1 (max: 2)
Hostname
Tags
Last Seen
desktop-c6oj5nl.net.rogers.com
windows
workstations
2024-07-10
ext-atomic-red-team
ext:ext-atomic-red-team
2024-07-10
ext-yara
ext:ext-yara
lc:system
2024-07-10
ext-reliable-tasking
ext:reliable-tasking
lc:system
2024-07-10

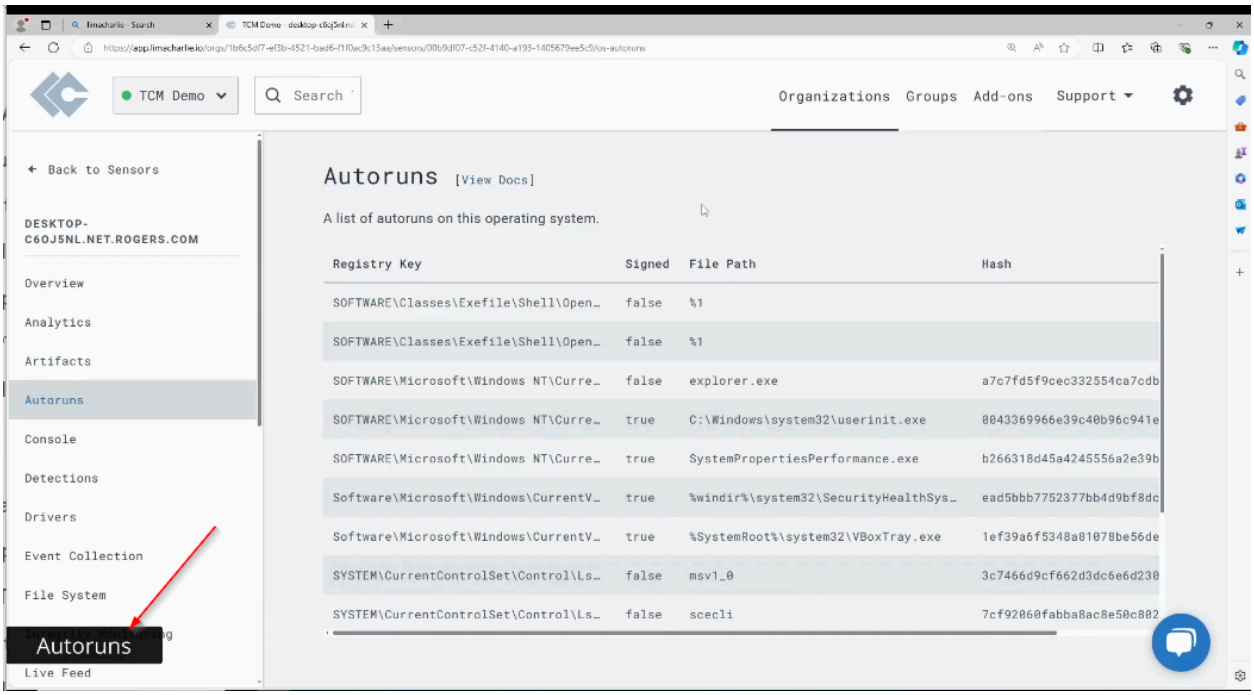
Let analysis Features:

⇒ Note: EDR is solution but false positive always come so use manual skill analysis and always follow manual procedures

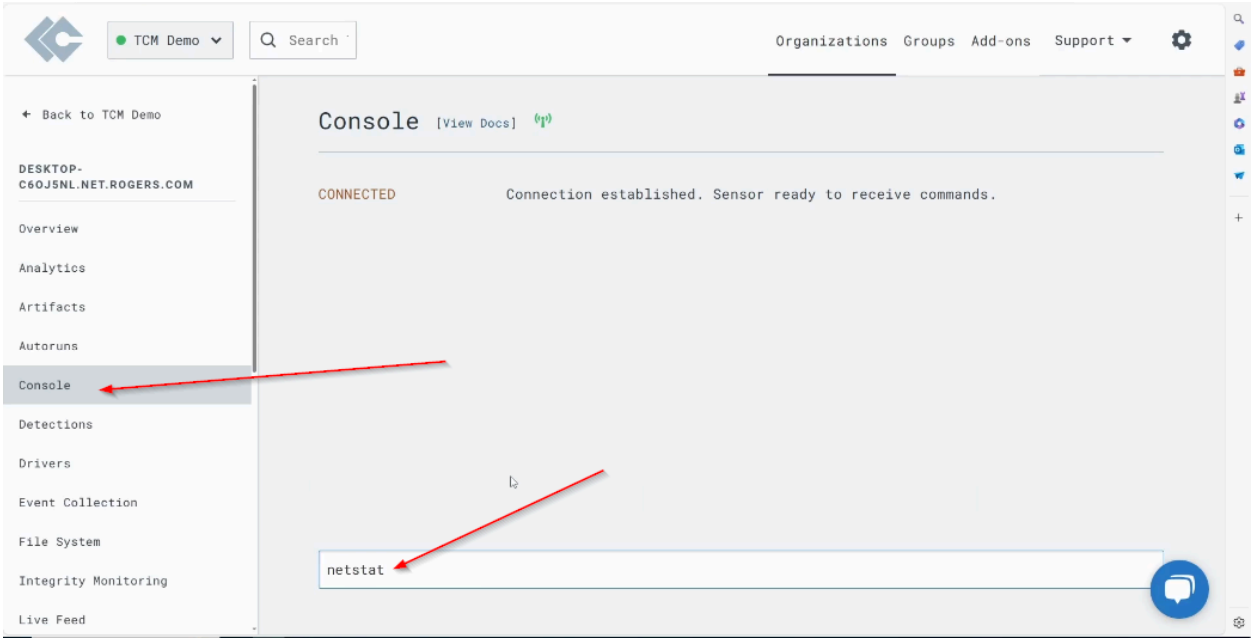
1.) Overview



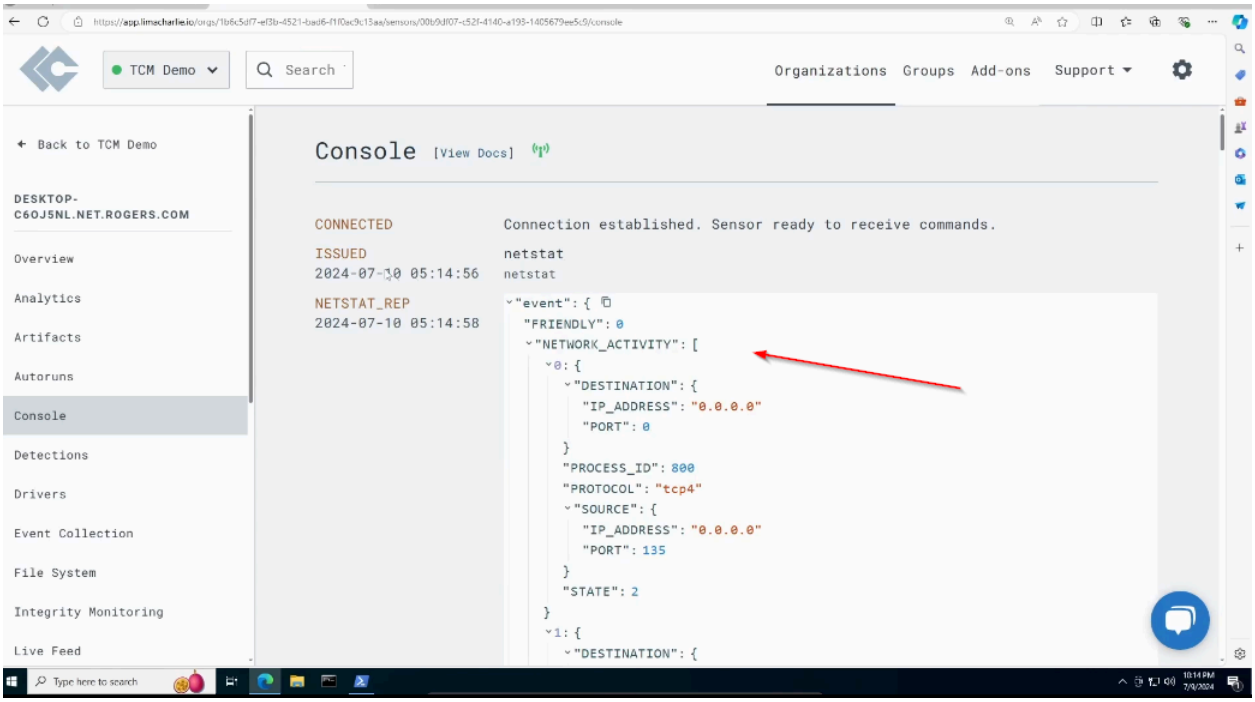
2.) Autoruns


TCM Demo
Search
Organizations
Groups
Add-ons
Support
Back to Sensors
DESKTOP-C6OJ5NL.NET.ROGERS.COM
Overview
Analytics
Artifacts
Autoruns
Console
Detections
Drivers
Event Collection
File System
Live Feed
Autoruns
Autoruns [View Docs]
A list of autoruns on this operating system.
Registry Key
Signed
File Path
Hash
SOFTWARE\Classes\Exefile\Shell\Open…
false
%1
SOFTWARE\Classes\Exefile\Shell\Open…
false
%1
SOFTWARE\Microsoft\Windows NT\Curre…
false
explorer.exe
a7c7fd5f9cec332554ca7cdb
SOFTWARE\Microsoft\Windows NT\Curre…
true
C:\Windows\system32\userinit.exe
0043369966e39c40b96c941e
SOFTWARE\Microsoft\Windows NT\Curre…
true
SystemPropertiesPerformance.exe
b266318d45a4245556a2e39b
Software\Microsoft\Windows\CurrentV…
true
%windir%\system32\SecurityHealthSys…
ead5bbb7752377bb4d9bf8dc
Software\Microsoft\Windows\CurrentV…
true
%SystemRoot%\system32\VBoxTray.exe
1ef39a6f5348a81078be56de
SYSTEM\CurrentControlSet\Control\Ls…
false
msv1_0
3c7466d9cf662d3dc6e6d230
SYSTEM\CurrentControlSet\Control\Ls…
false
scecli
7cf92060fabba8ac8e50c882

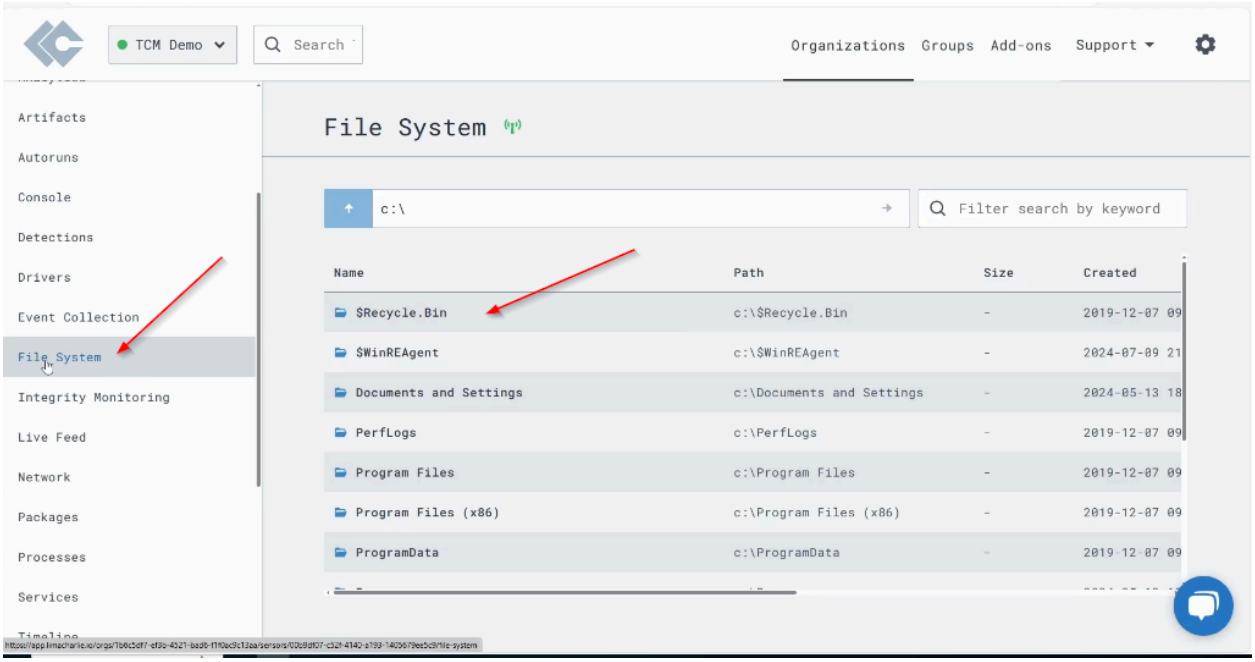
3.) Console


TCM Demo
Search
Organizations
Groups
Add-ons
Support
Back to TCM Demo
DESKTOP-C6OJ5NL.NET.ROGERS.COM
Overview
Analytics
Artifacts
Autoruns
Console
Detections
Drivers
Event Collection
File System
Integrity Monitoring
Live Feed
Console [View Docs]
CONNECTED
Connection established. Sensor ready to receive commands.
netstat

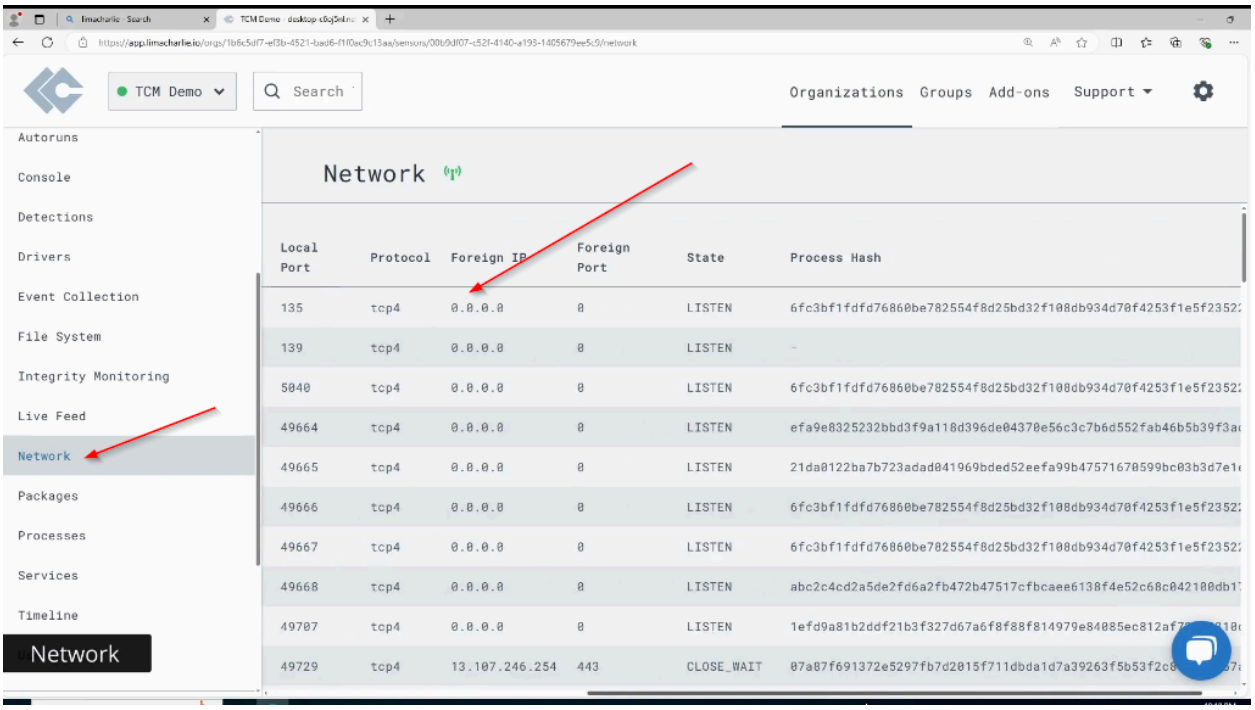
Mini C2



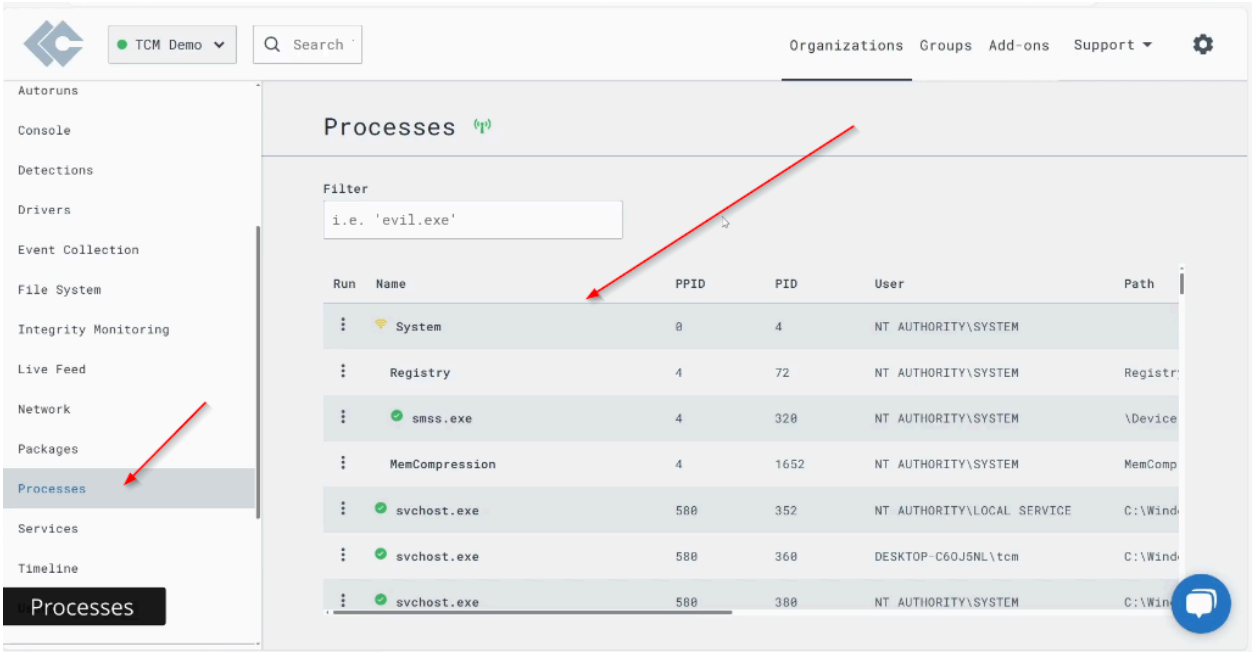
4.) File System:


TCM Demo
Search
Organizations
Groups
Add-ons
Support
Artifacts
Autoruns
Console
Detections
Drivers
Event Collection
File System
Integrity Monitoring
Live Feed
Network
Packages
Processes
Services
File System
c:\
Filter search by keyword
Name
Path
Size
Created
$Recycle.Bin
c:\$Recycle.Bin
2019-12-07 09
$WinREAgent
c:\$WinREAgent
2024-07-09 21
Documents and Settings
c:\Documents and Settings
2024-05-13 18
PerfLogs
c:\PerfLogs
2019-12-07 09
Program Files
c:\Program Files
2019-12-07 09
Program Files (x86)
c:\Program Files (x86)
2019-12-07 09
ProgramData
c:\ProgramData
2019-12-07 09

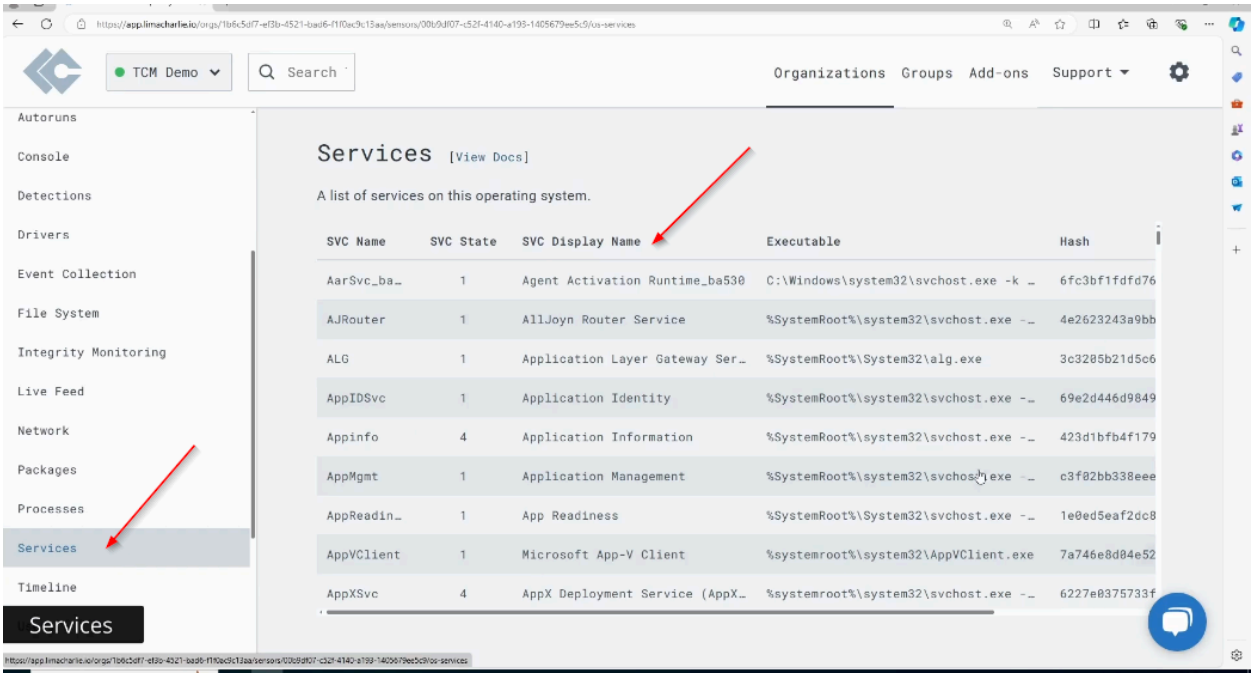
5.) Network

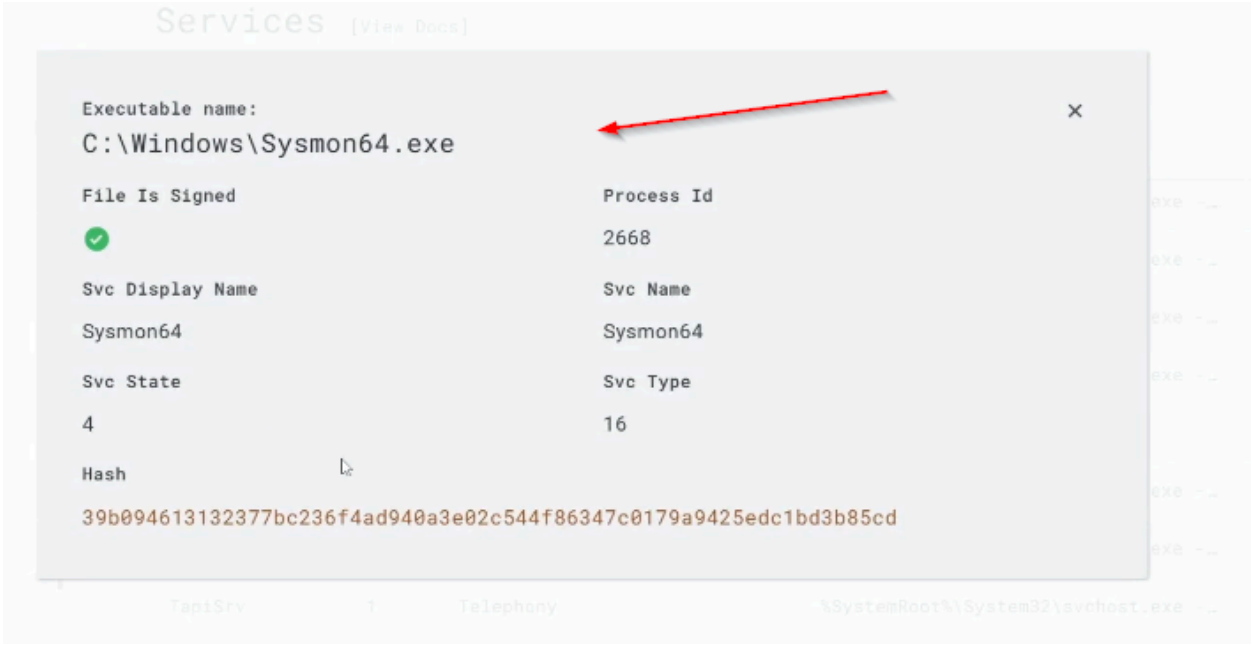

TCM Demo
Search
Organizations
Groups
Add-ons
Support
Autoruns
Console
Detections
Drivers
Event Collection
File System
Integrity Monitoring
Live Feed
Network
Packages
Processes
Services
Timeline
Network
Network
Local Port
Protocol
Foreign IP
Foreign Port
State
Process Hash
135
tcp4
0.0.0.0
0
LISTEN
6fc3bf1fdfd76860be782554f8d25bd32f108db934d70f4253f1e5f2352
139
tcp4
0.0.0.0
0
LISTEN
5040
tcp4
0.0.0.0
0
LISTEN
6fc3bf1fdfd76860be782554f8d25bd32f108db934d70f4253f1e5f2352
49664
tcp4
0.0.0.0
0
LISTEN
efa9e8325232bbd3f9a118d396de04370e56c3c7b6d552fab46b5b39f3a
49665
tcp4
0.0.0.0
0
LISTEN
21da0122ba7b723adad041969bded52eefa99b47571670599bc03b3d7e1
49666
tcp4
0.0.0.0
0
LISTEN
6fc3bf1fdfd76860be782554f8d25bd32f108db934d70f4253f1e5f2352
49667
tcp4
0.0.0.0
0
LISTEN
6fc3bf1fdfd76860be782554f8d25bd32f108db934d70f4253f1e5f2352
49668
tcp4
0.0.0.0
0
LISTEN
abc2c4cd2a5de2fd6a2fb472b47517cfbcaee6138f4e52c68c042100db1
49707
tcp4
0.0.0.0
0
LISTEN
1efd9a81b2ddf21b3f327d67a6f8f88f814979e84085ec812af
49729
tcp4
13.107.246.254
443
CLOSE_WAIT
07a87f691372e5297fb7d2015f711dbda1d7a39263f5b53f2c8

6.) Process



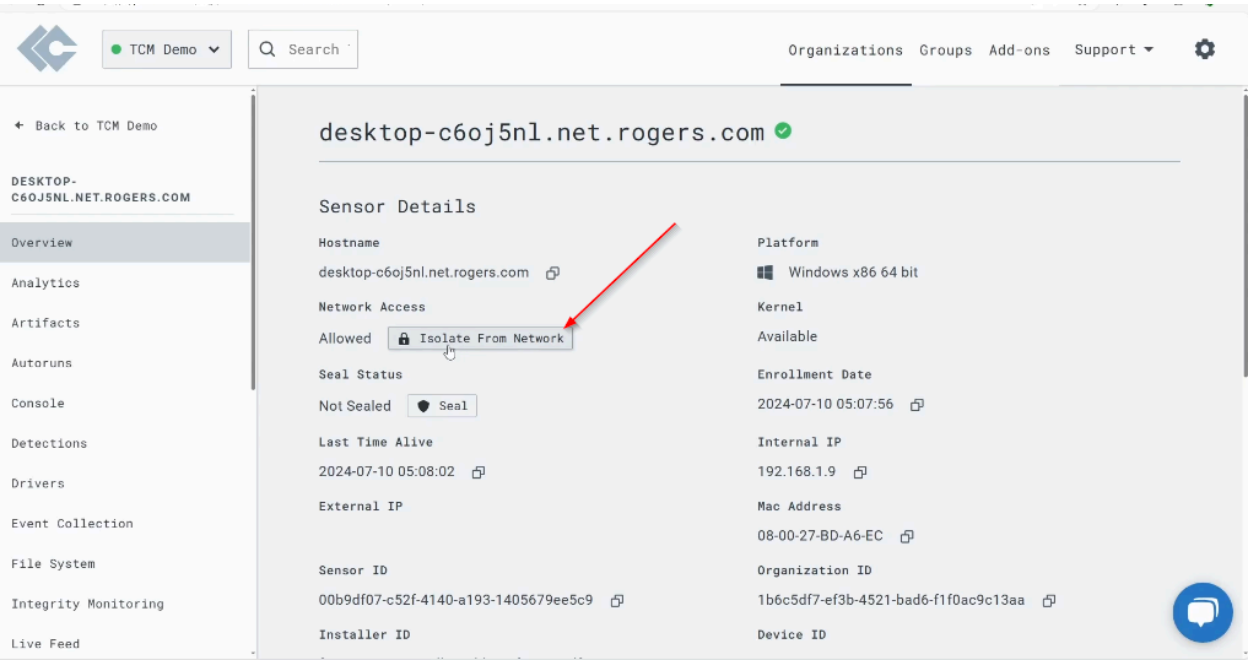
7.) Services



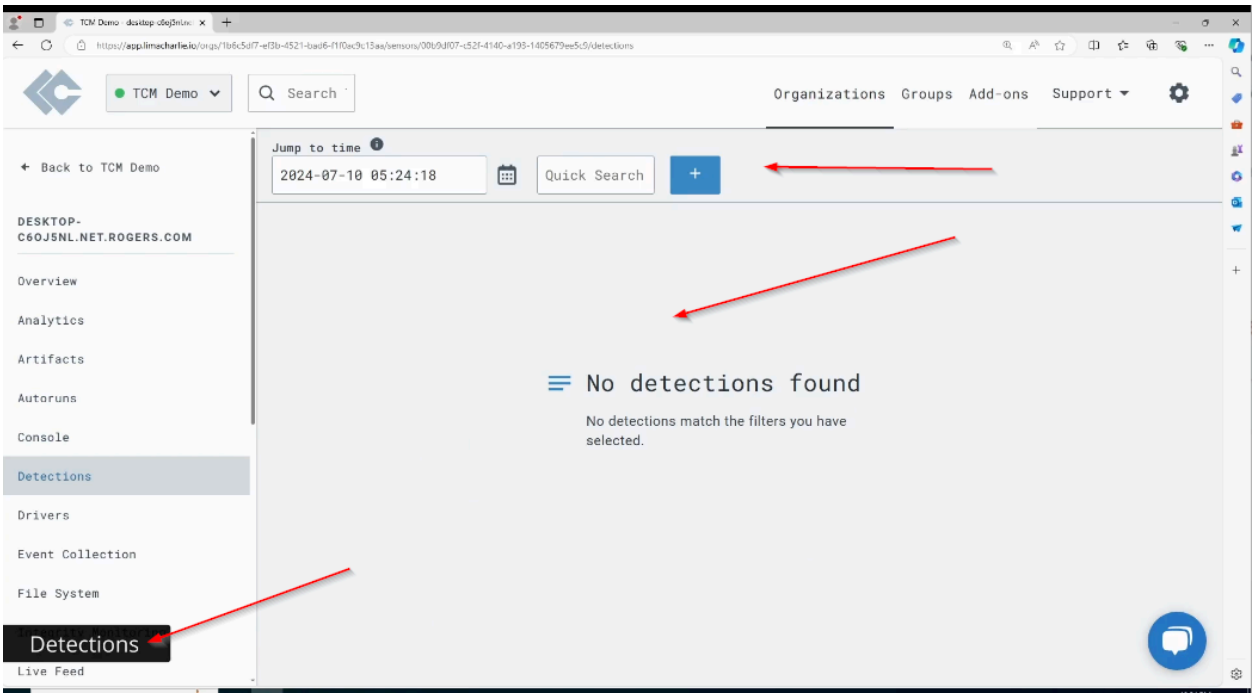


8.) Network Isolation

Network Isolation process



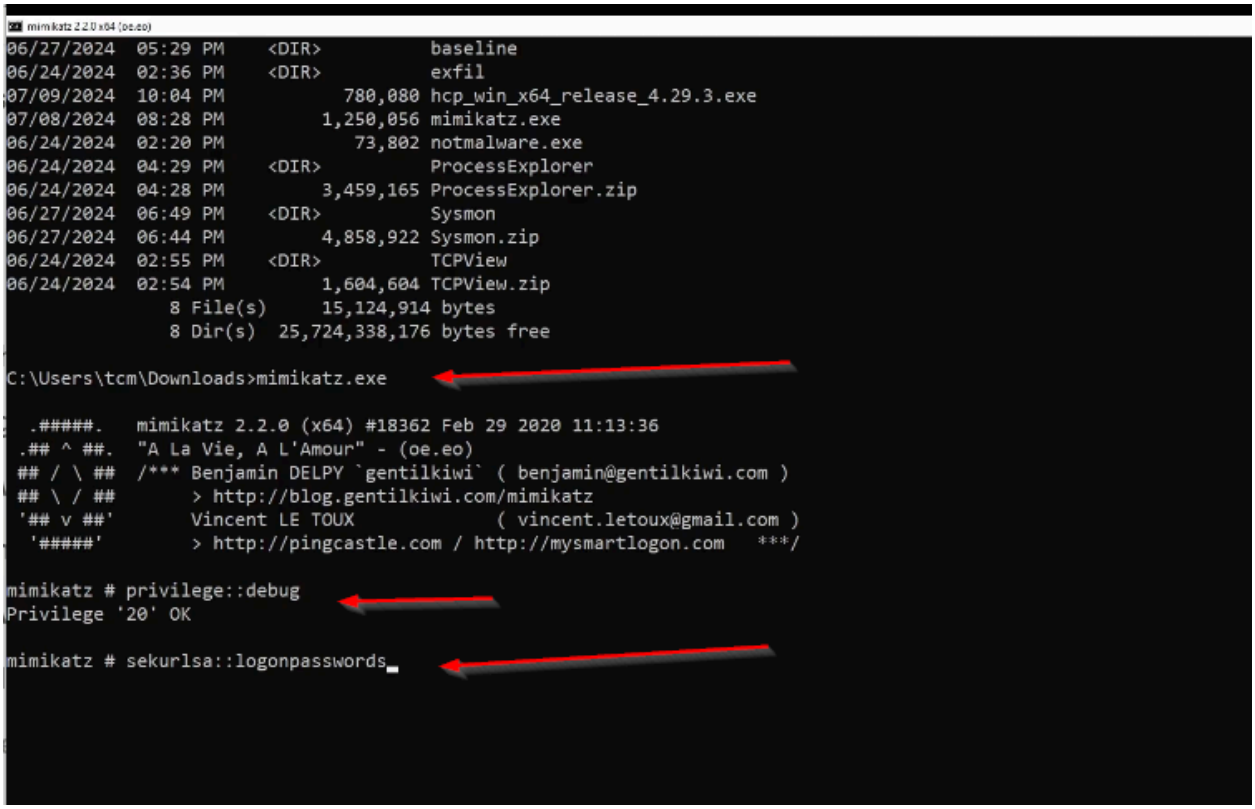
9.) Detections



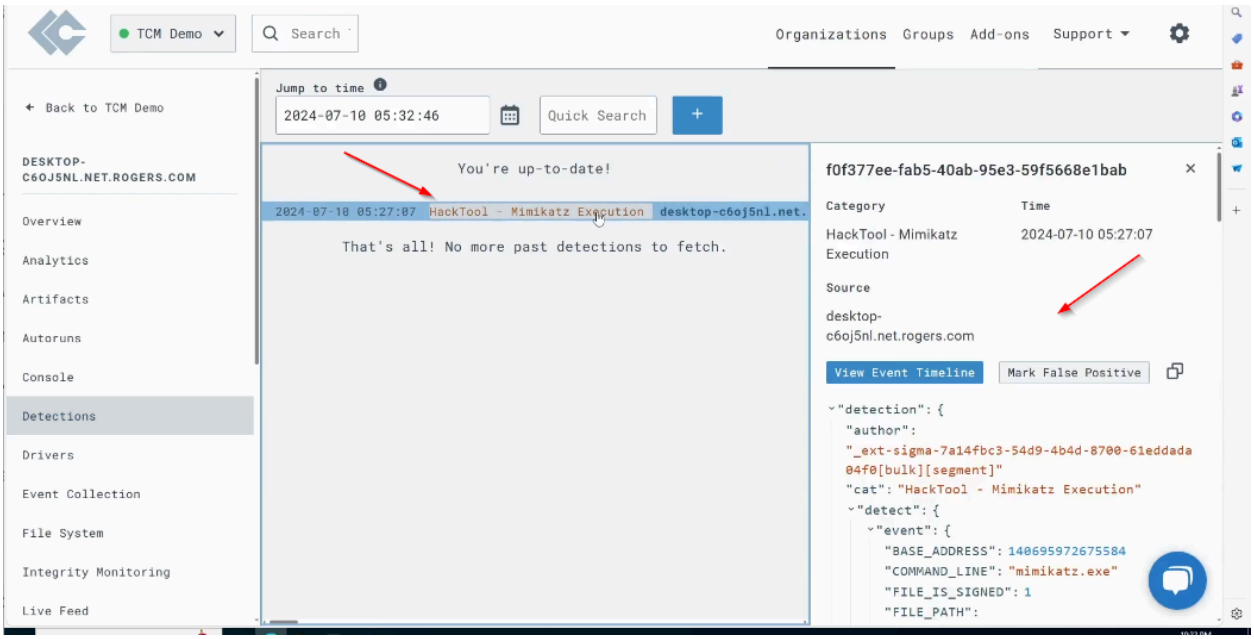
Now Execute real malware (mimikatz tool) via use Lima charlie EDR:

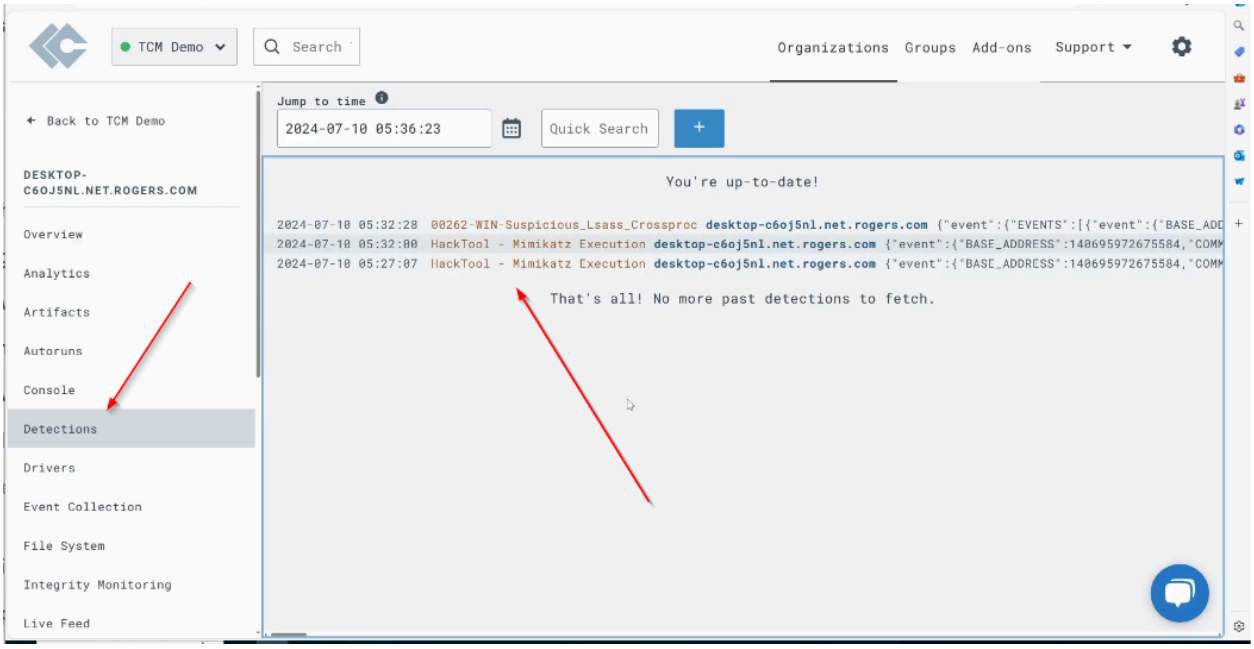
⇒ Good EDR detection mimikatz tool execution

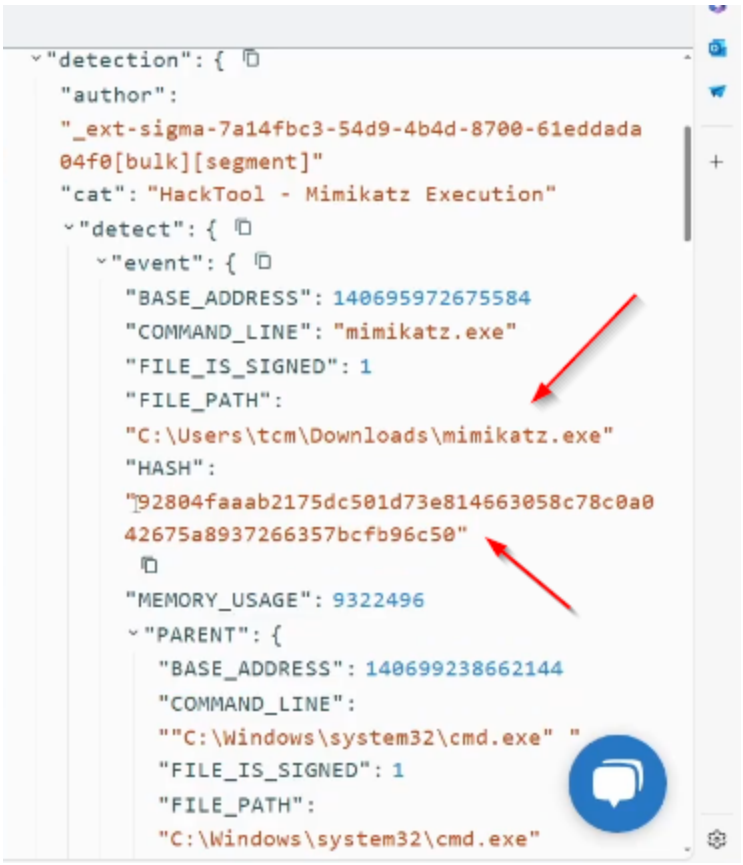
1.) First execute mimikatz

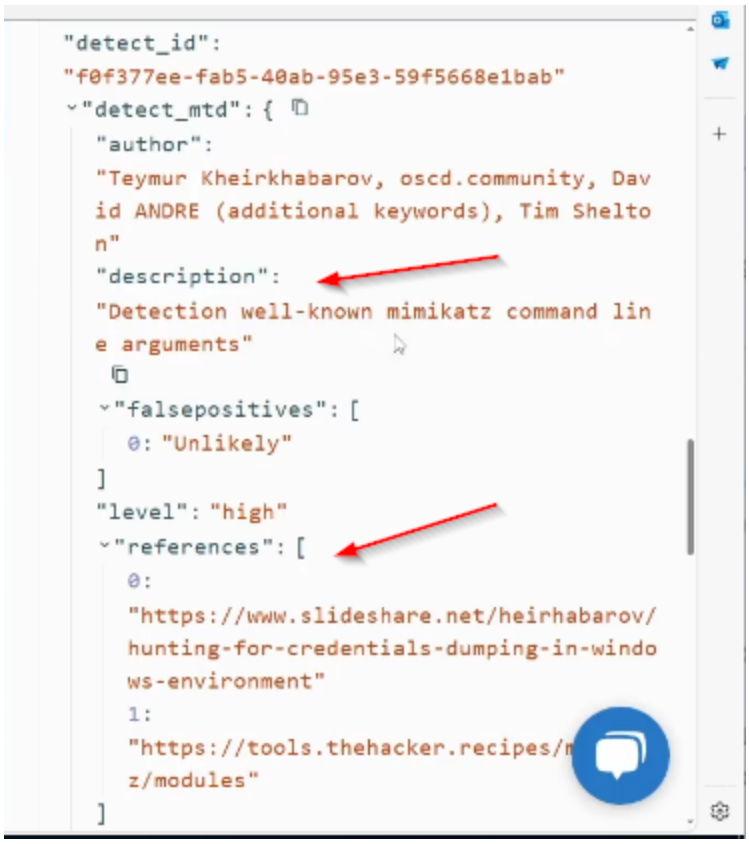


2.) See EDR detect malicious program

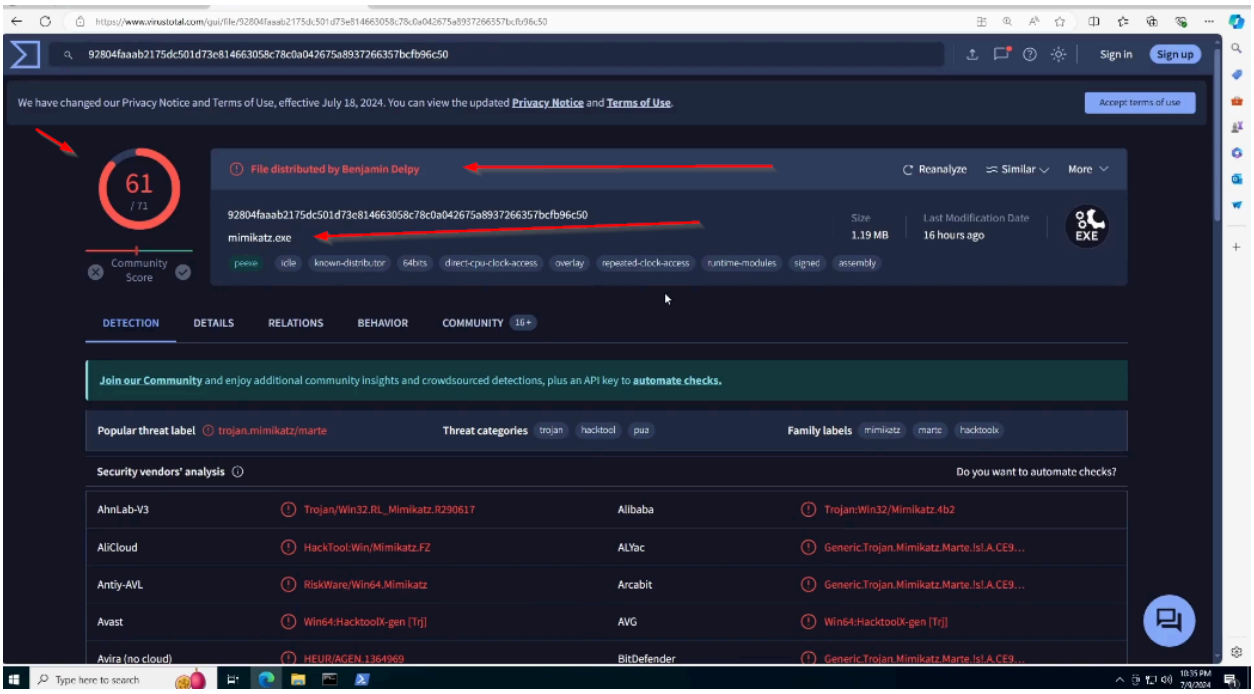

TCM Demo
Search
Organizations
Groups
Add-ons
Support
Back to TCM Demo
Jump to time
2024-07-10 05:32:46
Quick Search
DESKTOP-C6OJ5NL.NET.ROGERS.COM
Overview
Analytics
Artifacts
Autoruns
Console
Detections
Drivers
Event Collection
File System
Integrity Monitoring
Live Feed
You're up-to-date!
2024-07-10 05:27:07 HackTool - Mimikatz Execution desktop-c6oj5nl.net.
That's all! No more past detections to fetch.
f0f377ee-fab5-40ab-95e3-59f5668e1bab
Category
HackTool - Mimikatz Execution
Time
2024-07-10 05:27:07
Source
desktop-c6oj5nl.net.rogers.com
View Event Timeline
Mark False Positive
"detection": {
"author": "_ext-sigma-7a14fbc3-54d9-4b4d-8700-61eddada04f0[bulk][segment]"
"cat": "HackTool - Mimikatz Execution"
"detect": {
"event": {
"BASE_ADDRESS": 140695972675584
"COMMAND_LINE": "mimikatz.exe"
"FILE_IS_SIGNED": 1
"FILE_PATH":


TCM Demo
Search
Organizations
Groups
Add-ons
Support
Back to TCM Demo
Jump to time
2024-07-10 05:36:23
Quick Search
DESKTOP-C6OJ5NL.NET.ROGERS.COM
Overview
Analytics
Artifacts
Autoruns
Console
Detections
Drivers
Event Collection
File System
Integrity Monitoring
Live Feed
You're up-to-date!
2024-07-10 05:32:28 00262-WIN-Suspicious_Lsass_Crossproc desktop-c6oj5nl.net.rogers.com {"event":{"EVENTS":[{"event":{"BASE_ADD
2024-07-10 05:32:00 HackTool - Mimikatz Execution desktop-c6oj5nl.net.rogers.com {"event":{"BASE_ADDRESS":140695972675584,"COMM
2024-07-10 05:27:07 HackTool - Mimikatz Execution desktop-c6oj5nl.net.rogers.com {"event":{"BASE_ADDRESS":140695972675584,"COMM
That's all! No more past detections to fetch.


"detection": {
"author":
"_ext-sigma-7a14fbc3-54d9-4b4d-8700-61eddada
04f0[bulk][segment]"
"cat": "HackTool - Mimikatz Execution"
"detect": {
"event": {
"BASE_ADDRESS": 140695972675584
"COMMAND_LINE": "mimikatz.exe"
"FILE_IS_SIGNED": 1
"FILE_PATH":
"C:\Users\tcm\Downloads\mimikatz.exe"
"HASH":
"92804faaab2175dc501d73e814663058c78c0a0
42675a8937266357bcfb96c50"
"MEMORY_USAGE": 9322496
"PARENT": {
"BASE_ADDRESS": 140699238662144
"COMMAND_LINE":
""C:\Windows\system32\cmd.exe" "
"FILE_IS_SIGNED": 1
"FILE_PATH":
"C:\Windows\system32\cmd.exe"



4.) Then found malicious file check reputation to virustotal



4.) Process analysis