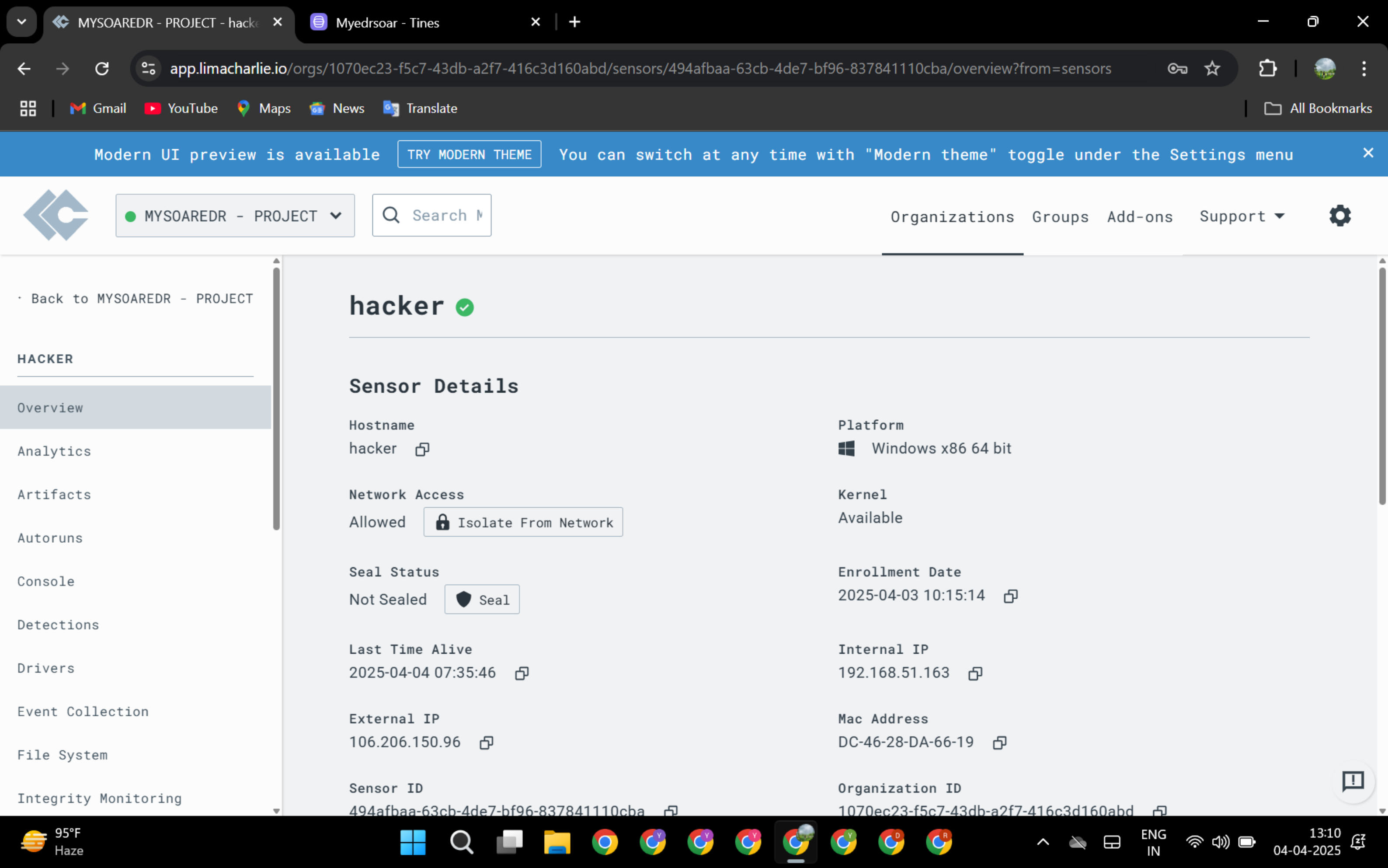

MYSOAREDR - PROJECT - hacke
Myedrsoar - Tines
app.limacharlie.io/orgs/1070ec23-f5c7-43db-a2f7-416c3d160abd/sensors/494afbaa-63cb-4de7-bf96-837841110cba/overview?from=sensors
Gmail
YouTube
Maps
News
Translate
All Bookmarks
Modern UI preview is available
TRY MODERN THEME
You can switch at any time with "Modern theme" toggle under the Settings menu
MYSOAREDR - PROJECT
Search M
Organizations
Groups
Add-ons
Support
· Back to MYSOAREDR - PROJECT
HACKER
Overview
Analytics
Artifacts
Autoruns
Console
Detections
Drivers
Event Collection
File System
Integrity Monitoring
95°F
Haze
ENG
IN
13:10
04-04-2025

hacker

Sensor Details

Hostname
hacker

Platform
Windows x86 64 bit

Network Access
Allowed
Isolate From Network

Kernel
Available

Seal Status
Not Sealed
Seal

Enrollment Date
2025-04-03 10:15:14

Last Time Alive
2025-04-04 07:35:46

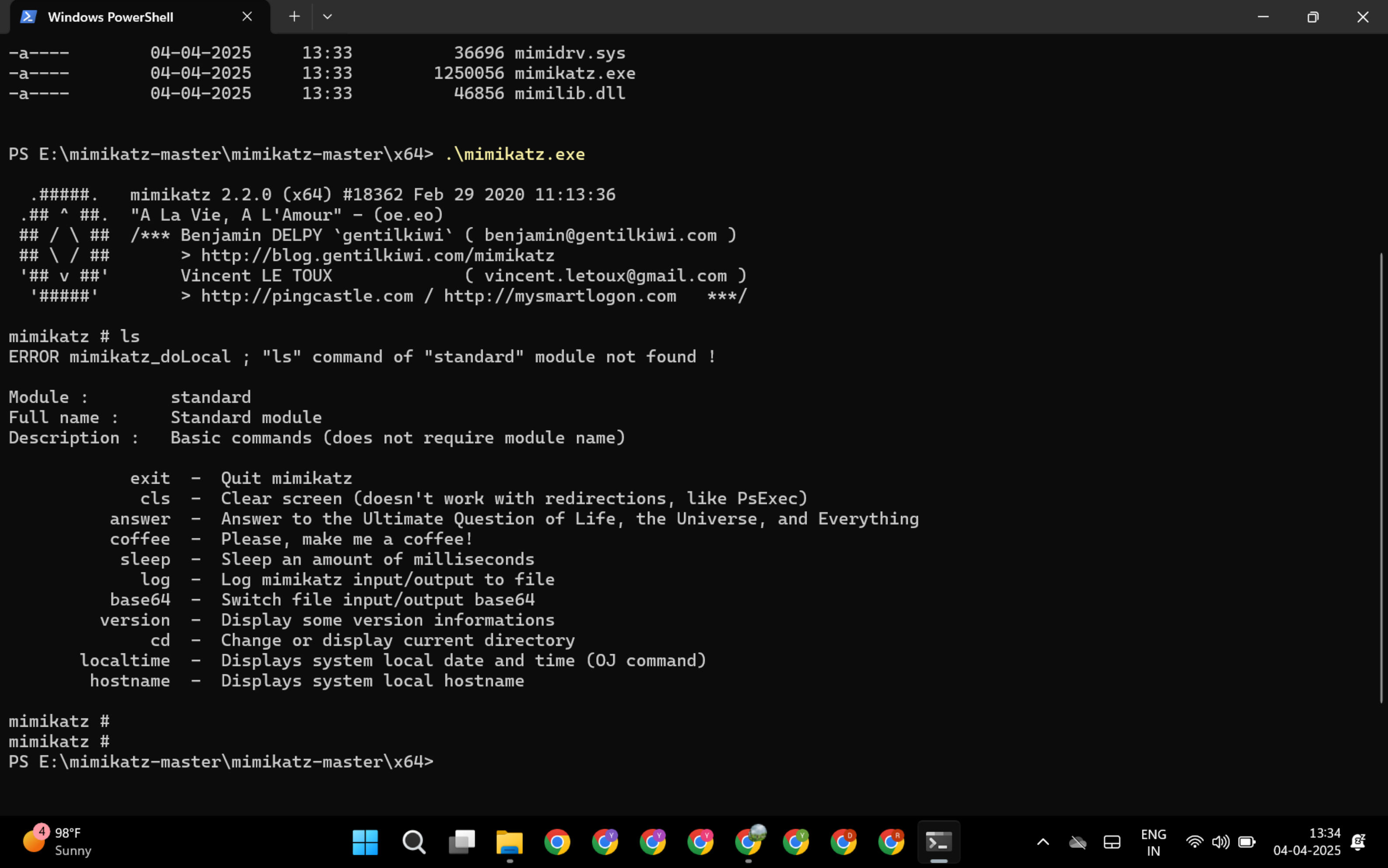
Internal IP
192.168.51.163

External IP
106.206.150.96

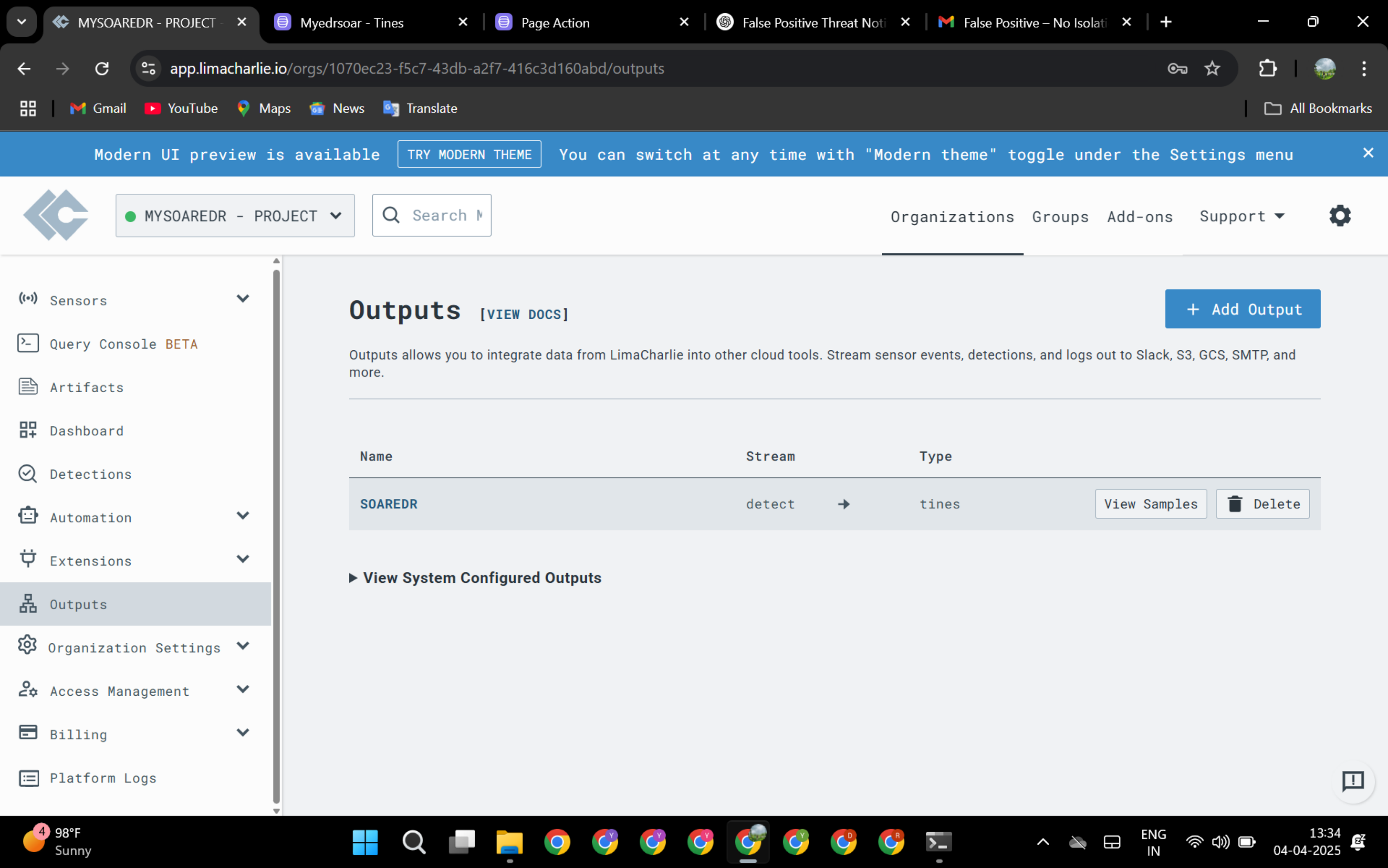
Mac Address
DC-46-28-DA-66-19

Sensor ID
494afbaa-63cb-4de7-bf96-837841110cba

Organization ID
1070ec23-f5c7-43db-a2f7-416c3d160abd



```
-a----        04-04-2025     13:33          36696 mimidrv.sys
-a----        04-04-2025     13:33        1250056 mimikatz.exe
-a----        04-04-2025     13:33          46856 mimilib.dll


PS E:\mimikatz-master\mimikatz-master\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # ls
ERROR mimikatz_doLocal ; "ls" command of "standard" module not found !

Module :        standard
Full name :     Standard module
Description :   Basic commands (does not require module name)

            exit  -  Quit mimikatz
             cls  -  Clear screen (doesn't work with redirections, like PsExec)
          answer  -  Answer to the Ultimate Question of Life, the Universe, and Everything
          coffee  -  Please, make me a coffee!
           sleep  -  Sleep an amount of milliseconds
             log  -  Log mimikatz input/output to file
          base64  -  Switch file input/output base64
         version  -  Display some version informations
              cd  -  Change or display current directory
       localtime  -  Displays system local date and time (OJ command)
        hostname  -  Displays system local hostname

mimikatz #
mimikatz #
PS E:\mimikatz-master\mimikatz-master\x64>
```

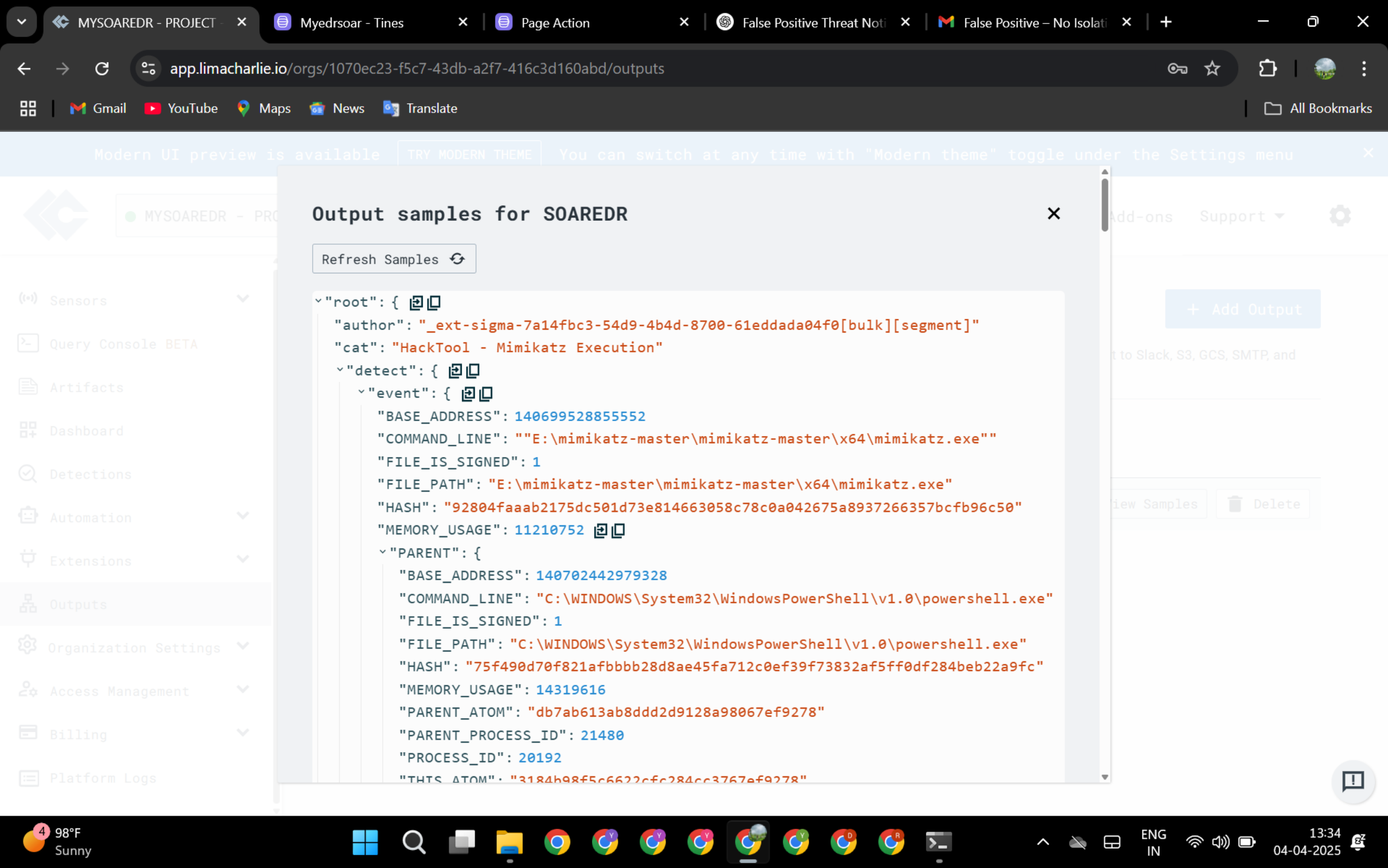


Outputs [VIEW DOCS]

Outputs allows you to integrate data from LimaCharlie into other cloud tools. Stream sensor events, detections, and logs out to Slack, S3, GCS, SMTP, and more.

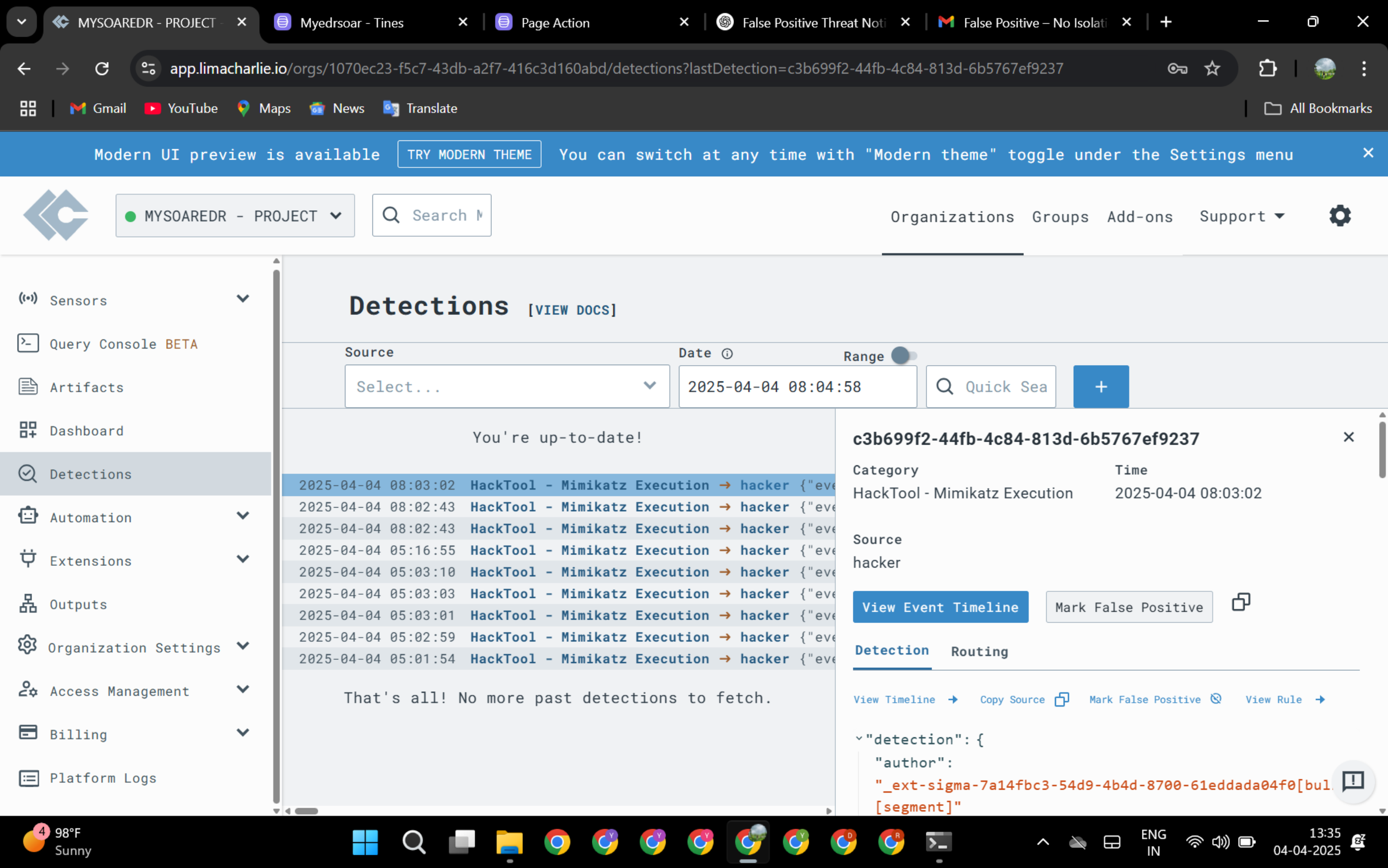
Name	Stream		Type
SOAREDR	detect	→	tines

▶ View System Configured Outputs



Output samples for SOAREDR

```
"root": {
  "author": "_ext-sigma-7a14fbc3-54d9-4b4d-8700-61eddada04f0[bulk][segment]"
  "cat": "HackTool - Mimikatz Execution"
  "detect": {
    "event": {
      "BASE_ADDRESS": 140699528855552
      "COMMAND_LINE": ""E:\mimikatz-master\mimikatz-master\x64\mimikatz.exe""
      "FILE_IS_SIGNED": 1
      "FILE_PATH": "E:\mimikatz-master\mimikatz-master\x64\mimikatz.exe"
      "HASH": "92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50"
      "MEMORY_USAGE": 11210752
      "PARENT": {
        "BASE_ADDRESS": 140702442979328
        "COMMAND_LINE": "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe"
        "FILE_IS_SIGNED": 1
        "FILE_PATH": "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe"
        "HASH": "75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc"
        "MEMORY_USAGE": 14319616
        "PARENT_ATOM": "db7ab613ab8ddd2d9128a98067ef9278"
        "PARENT_PROCESS_ID": 21480
        "PROCESS_ID": 20192
        "THIS_ATOM": "3184b98f5c6622cfc284cc3767ef9278"
```



app.limacharlie.io/orgs/1070ec23-f5c7-43db-a2f7-416c3d160abd/detections?lastDetection=c3b699f2-44fb-4c84-813d-6b5767ef9237

Modern UI preview is available   You can switch at any time with "Modern theme" toggle under the Settings menu

Detections [VIEW DOCS]

Source: Select...   Date: 2025-04-04 08:04:58   Range   Quick Sea

You're up-to-date!

```
2025-04-04 08:03:02  HackTool - Mimikatz Execution → hacker {"eve
2025-04-04 08:02:43  HackTool - Mimikatz Execution → hacker {"eve
2025-04-04 08:02:43  HackTool - Mimikatz Execution → hacker {"eve
2025-04-04 05:16:55  HackTool - Mimikatz Execution → hacker {"eve
2025-04-04 05:03:10  HackTool - Mimikatz Execution → hacker {"eve
2025-04-04 05:03:03  HackTool - Mimikatz Execution → hacker {"eve
2025-04-04 05:03:01  HackTool - Mimikatz Execution → hacker {"eve
2025-04-04 05:02:59  HackTool - Mimikatz Execution → hacker {"eve
2025-04-04 05:01:54  HackTool - Mimikatz Execution → hacker {"eve
```

That's all! No more past detections to fetch.

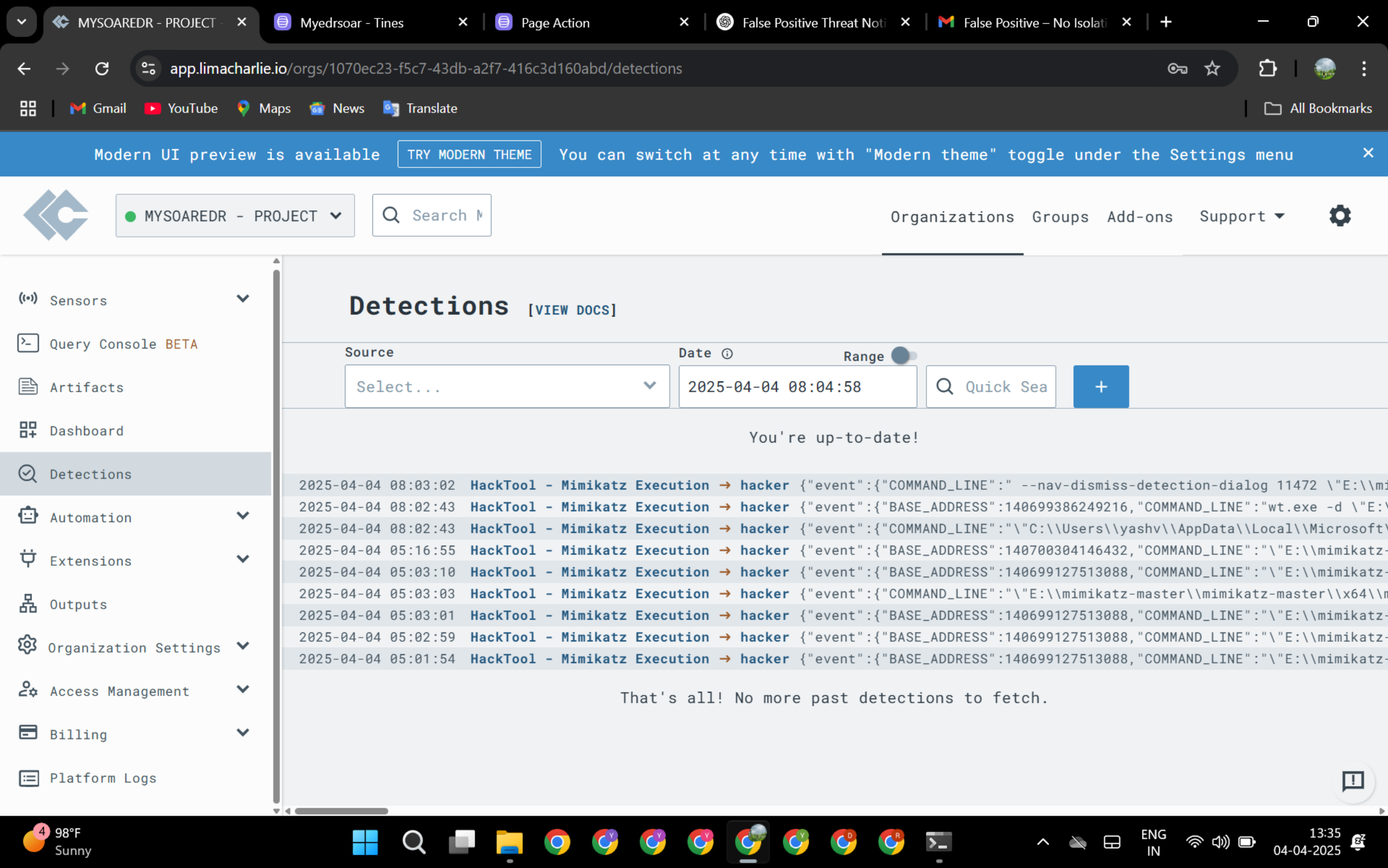
c3b699f2-44fb-4c84-813d-6b5767ef9237

Category: HackTool - Mimikatz Execution

Time: 2025-04-04 08:03:02

Source: hacker

```
"detection": {
  "author":
  "_ext-sigma-7a14fbc3-54d9-4b4d-8700-61eddada04f0[bul
  [segment]"
```



Modern UI preview is available TRY MODERN THEME You can switch at any time with "Modern theme" toggle under the Settings menu

Detections [VIEW DOCS]

Source: Select...

Date: 2025-04-04 08:04:58

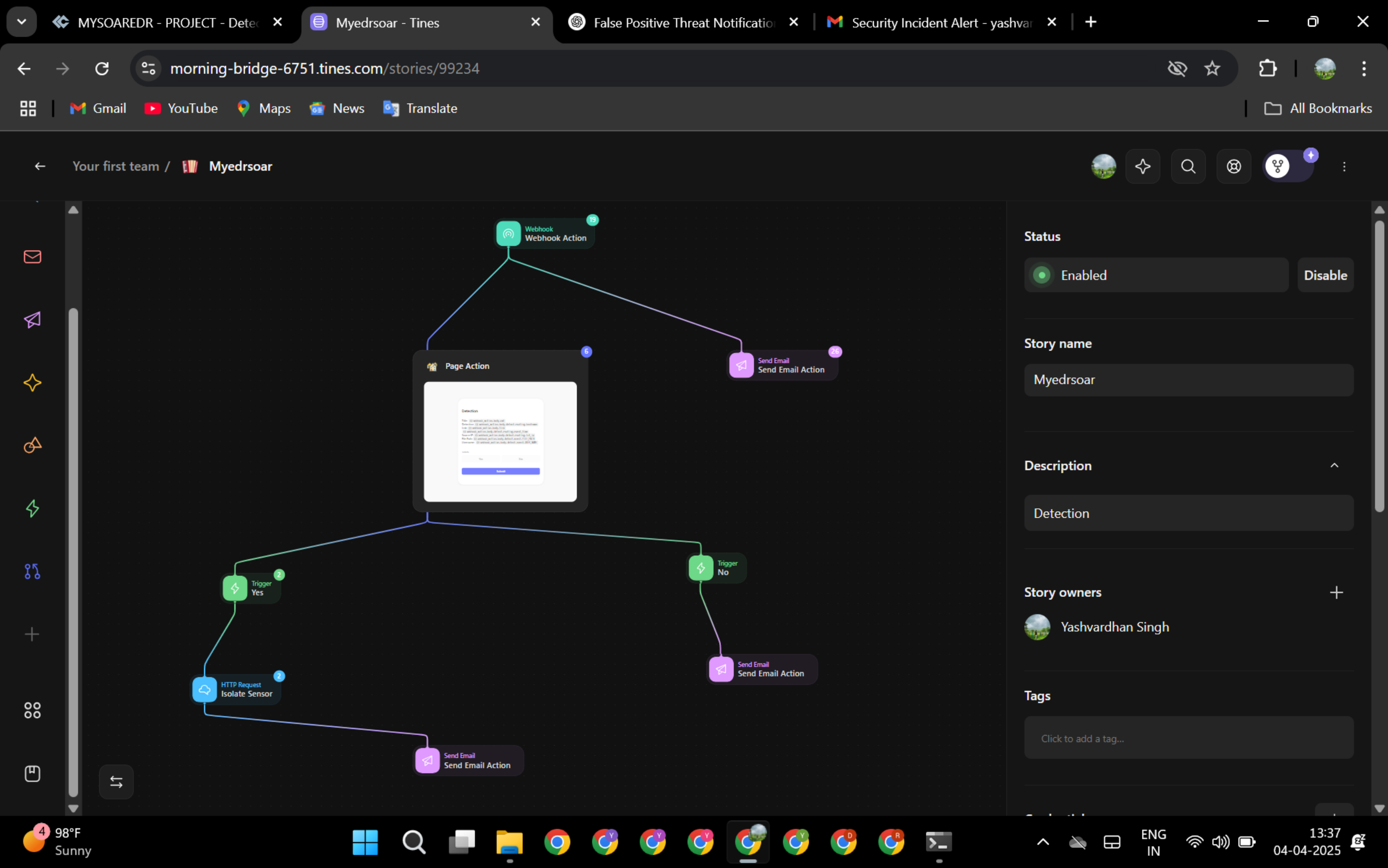
Range

Quick Sea

You're up-to-date!

```
2025-04-04 08:03:02 HackTool - Mimikatz Execution → hacker {"event":{"COMMAND_LINE":" --nav-dismiss-detection-dialog 11472 \"E:\\mi
2025-04-04 08:02:43 HackTool - Mimikatz Execution → hacker {"event":{"BASE_ADDRESS":140699386249216,"COMMAND_LINE":"wt.exe -d \"E:\
2025-04-04 08:02:43 HackTool - Mimikatz Execution → hacker {"event":{"COMMAND_LINE":"\"C:\\Users\\yashv\\AppData\\Local\\Microsoft
2025-04-04 05:16:55 HackTool - Mimikatz Execution → hacker {"event":{"BASE_ADDRESS":140700304146432,"COMMAND_LINE":"\"E:\\mimikatz-
2025-04-04 05:03:10 HackTool - Mimikatz Execution → hacker {"event":{"BASE_ADDRESS":140699127513088,"COMMAND_LINE":"\"E:\\mimikatz-
2025-04-04 05:03:03 HackTool - Mimikatz Execution → hacker {"event":{"COMMAND_LINE":"\"E:\\mimikatz-master\\mimikatz-master\\x64\\m
2025-04-04 05:03:01 HackTool - Mimikatz Execution → hacker {"event":{"BASE_ADDRESS":140699127513088,"COMMAND_LINE":"\"E:\\mimikatz-
2025-04-04 05:02:59 HackTool - Mimikatz Execution → hacker {"event":{"BASE_ADDRESS":140699127513088,"COMMAND_LINE":"\"E:\\mimikatz-
2025-04-04 05:01:54 HackTool - Mimikatz Execution → hacker {"event":{"BASE_ADDRESS":140699127513088,"COMMAND_LINE":"\"E:\\mimikatz-
```

That's all! No more past detections to fetch.



Status

Enabled   Disable

Story name

Myedrsoar

Description

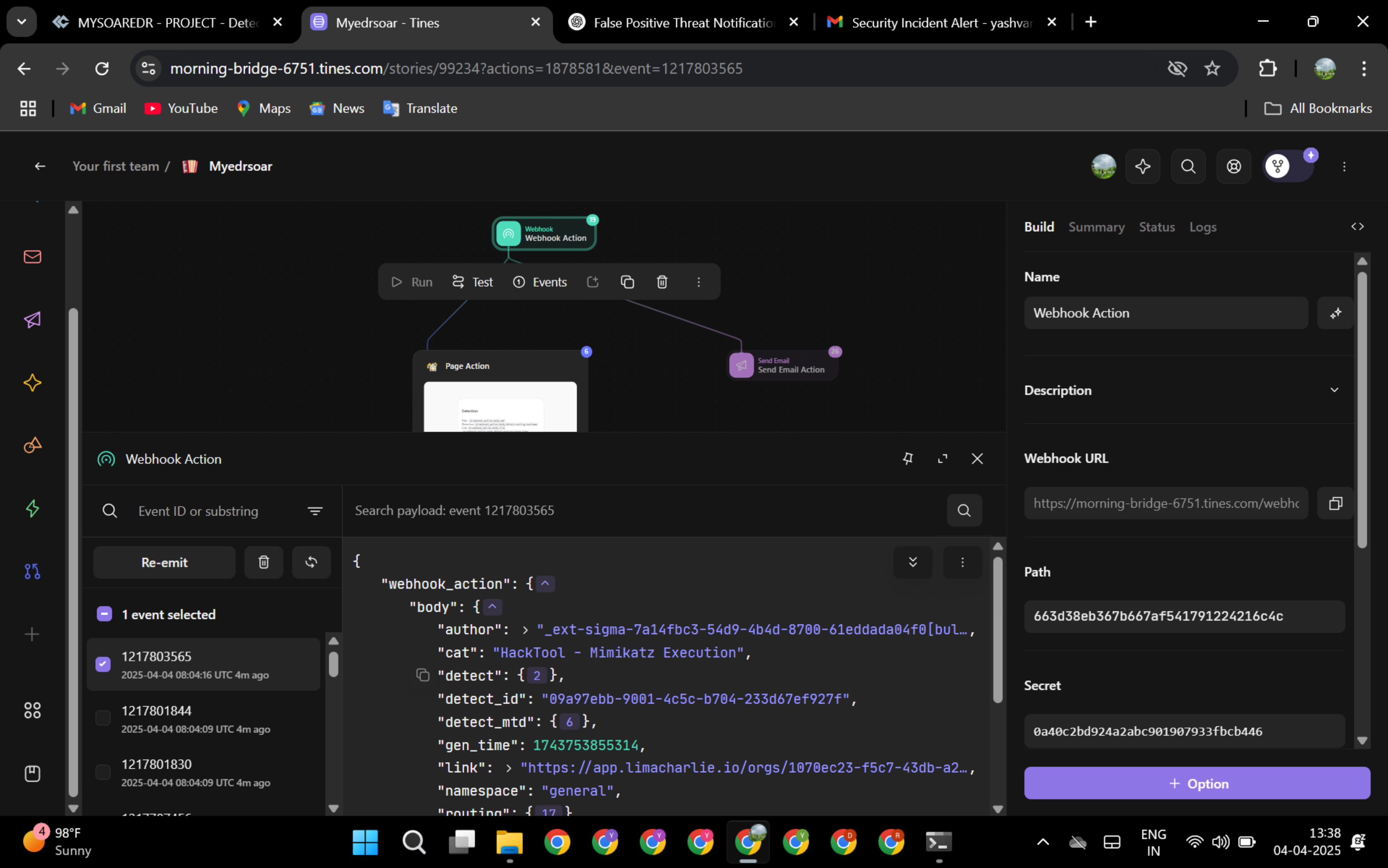
Detection

Story owners

Yashvardhan Singh

Tags

Click to add a tag...



1 event selected

☑ 1217803565
2025-04-04 08:04:16 UTC 4m ago

□ 1217801844
2025-04-04 08:04:09 UTC 4m ago

□ 1217801830
2025-04-04 08:04:09 UTC 4m ago

```
{
    "webhook_action": {
        "body": {
            "author": > "_ext-sigma-7a14fbc3-54d9-4b4d-8700-61eddada04f0[bul…,
            "cat": "HackTool - Mimikatz Execution",
            "detect": { 2 },
            "detect_id": "09a97ebb-9001-4c5c-b704-233d67ef927f",
            "detect_mtd": { 6 },
            "gen_time": 1743753855314,
            "link": > "https://app.limacharlie.io/orgs/1070ec23-f5c7-43db-a2…,
            "namespace": "general",
            "routing": { 17 }
```

Name

Webhook Action

Description

Webhook URL

https://morning-bridge-6751.tines.com/webhc

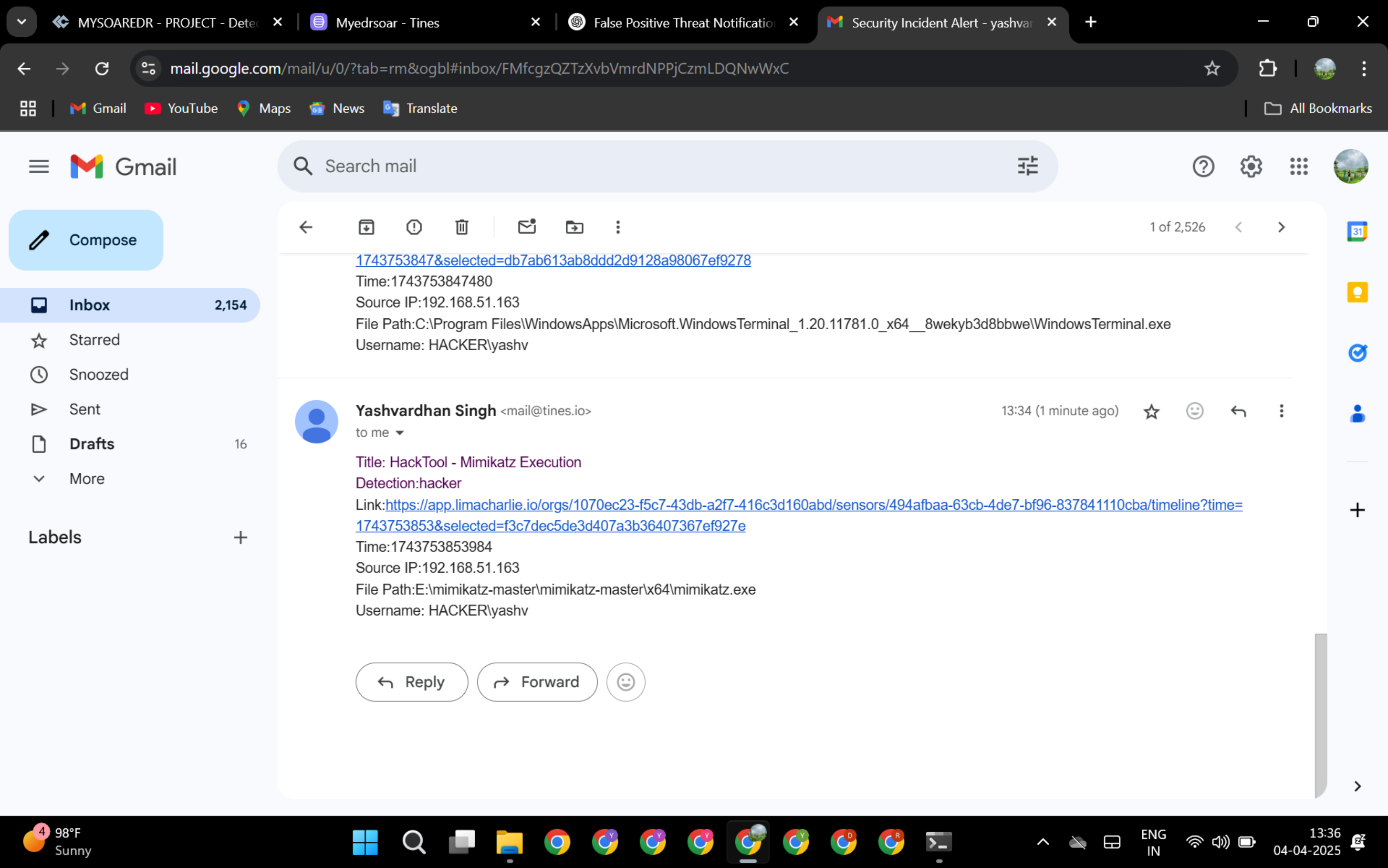
Path

663d38eb367b667af541791224216c4c

Secret

0a40c2bd924a2abc901907933fbcb446

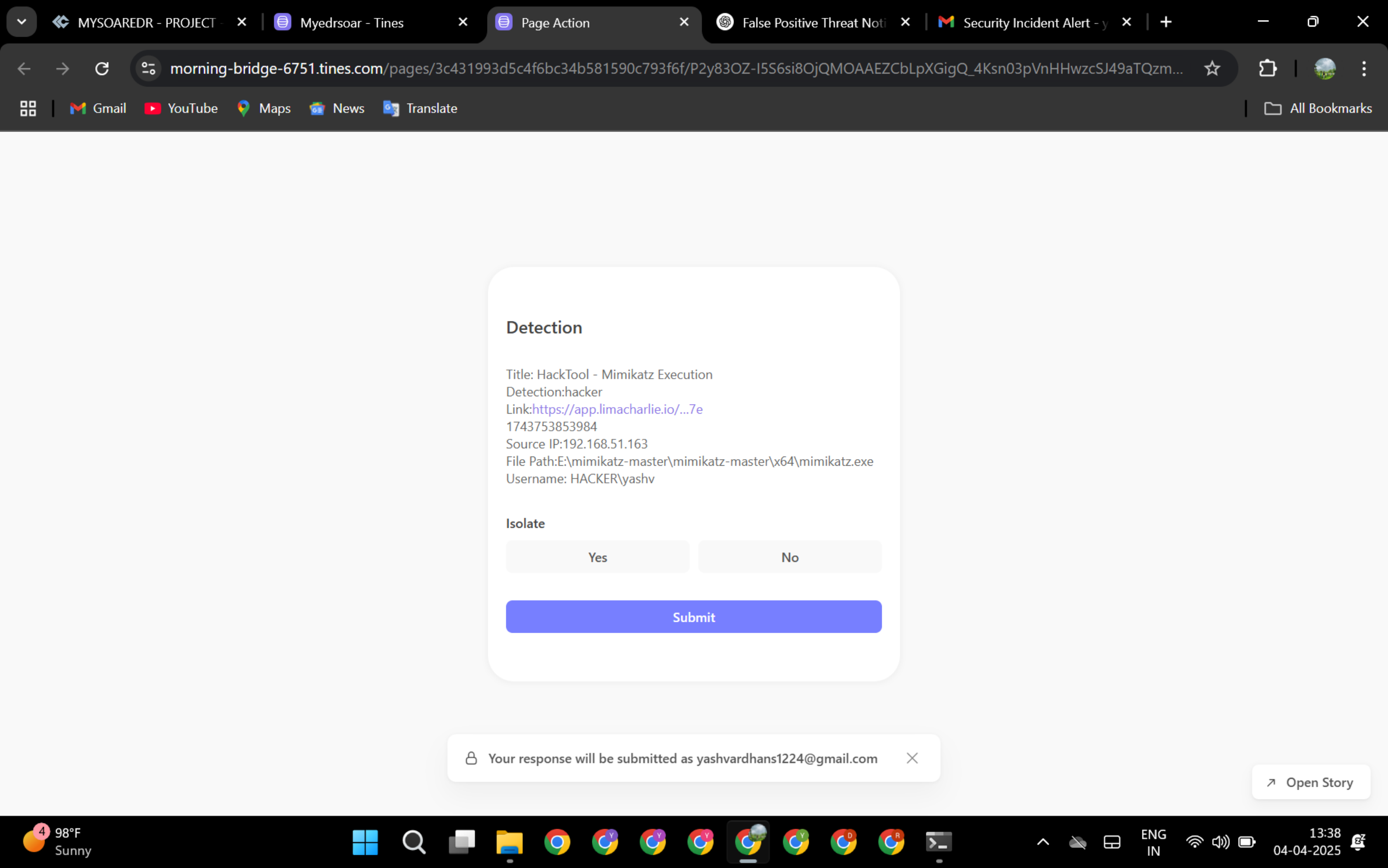
+ Option


MYSOAREDR - PROJECT - Detec
Myedrsoar - Tines
False Positive Threat Notificatio
Security Incident Alert - yashvar
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgzQZTzXvbVmrdNPPjCzmLDQNwWxC
Gmail
YouTube
Maps
News
Translate
All Bookmarks
Gmail
Search mail
Compose
Inbox 2,154
Starred
Snoozed
Sent
Drafts 16
More
Labels
1 of 2,526

1743753847&selected=db7ab613ab8ddd2d9128a98067ef9278
Time:1743753847480
Source IP:192.168.51.163
File Path:C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.20.11781.0_x64__8wekyb3d8bbwe\WindowsTerminal.exe
Username: HACKER\yashv

Yashvardhan Singh <mail@tines.io>
to me
13:34 (1 minute ago)

Title: HackTool - Mimikatz Execution
Detection:hacker
Link:https://app.limacharlie.io/orgs/1070ec23-f5c7-43db-a2f7-416c3d160abd/sensors/494afbaa-63cb-4de7-bf96-837841110cba/timeline?time=1743753853&selected=f3c7dec5de3d407a3b36407367ef927e
Time:1743753853984
Source IP:192.168.51.163
File Path:E:\mimikatz-master\mimikatz-master\x64\mimikatz.exe
Username: HACKER\yashv


MYSOAREDR - PROJECT
Myedrsoar - Tines
Page Action
False Positive Threat Noti
Security Incident Alert - y
morning-bridge-6751.tines.com/pages/3c431993d5c4f6bc34b581590c793f6f/P2y83OZ-I5S6si8OjQMOAAEZCbLpXGigQ_4Ksn03pVnHHwzcSJ49aTQzm...
Gmail
YouTube
Maps
News
Translate
All Bookmarks

Detection

Title: HackTool - Mimikatz Execution
Detection:hacker
Link:https://app.limacharlie.io/...7e
1743753853984
Source IP:192.168.51.163
File Path:E:\mimikatz-master\mimikatz-master\x64\mimikatz.exe
Username: HACKER\yashv

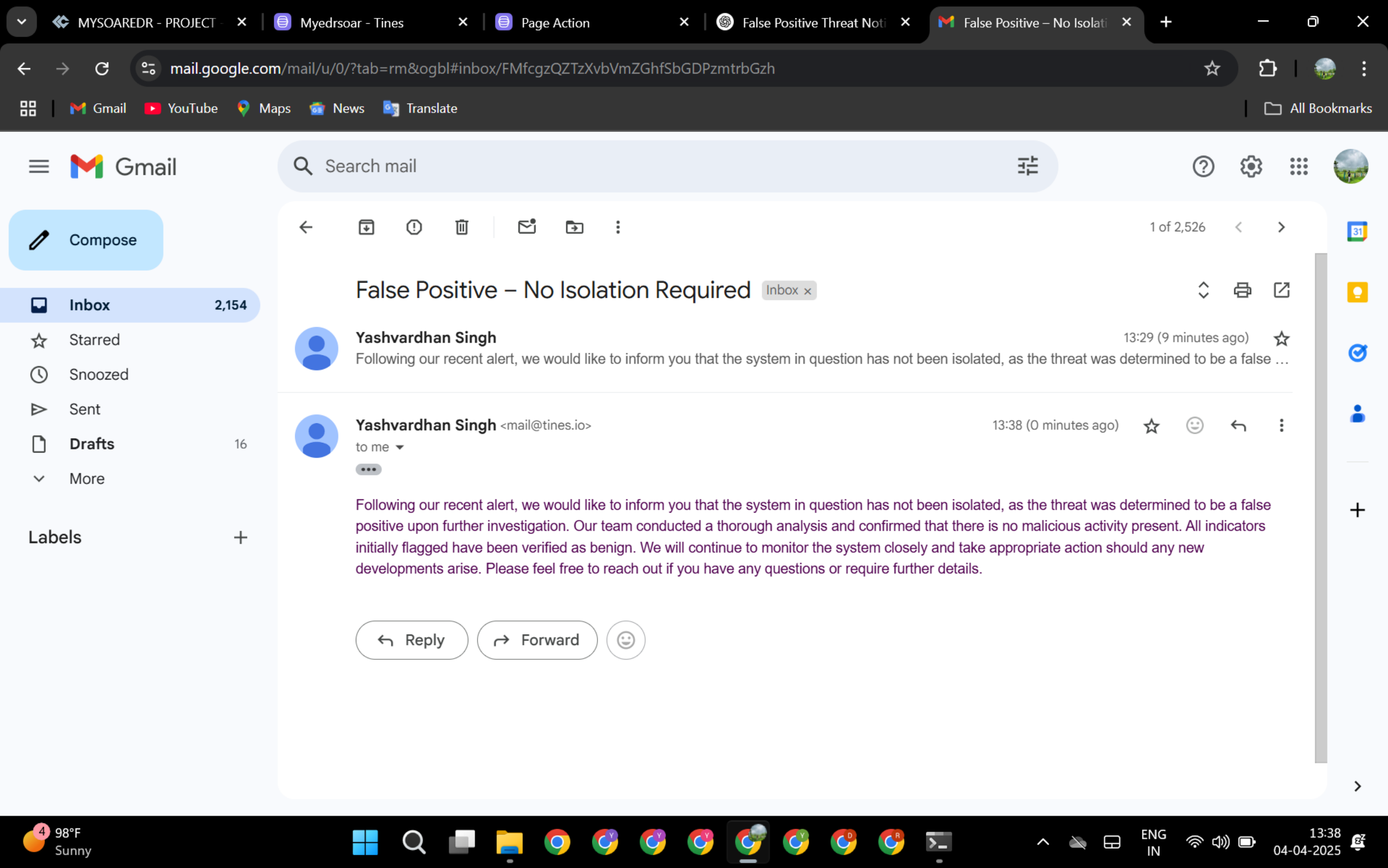
Isolate

Yes | No

Submit

Your response will be submitted as yashvardhans1224@gmail.com

Open Story
98°F
Sunny
ENG
IN
13:38
04-04-2025



False Positive – No Isolation Required Inbox ×

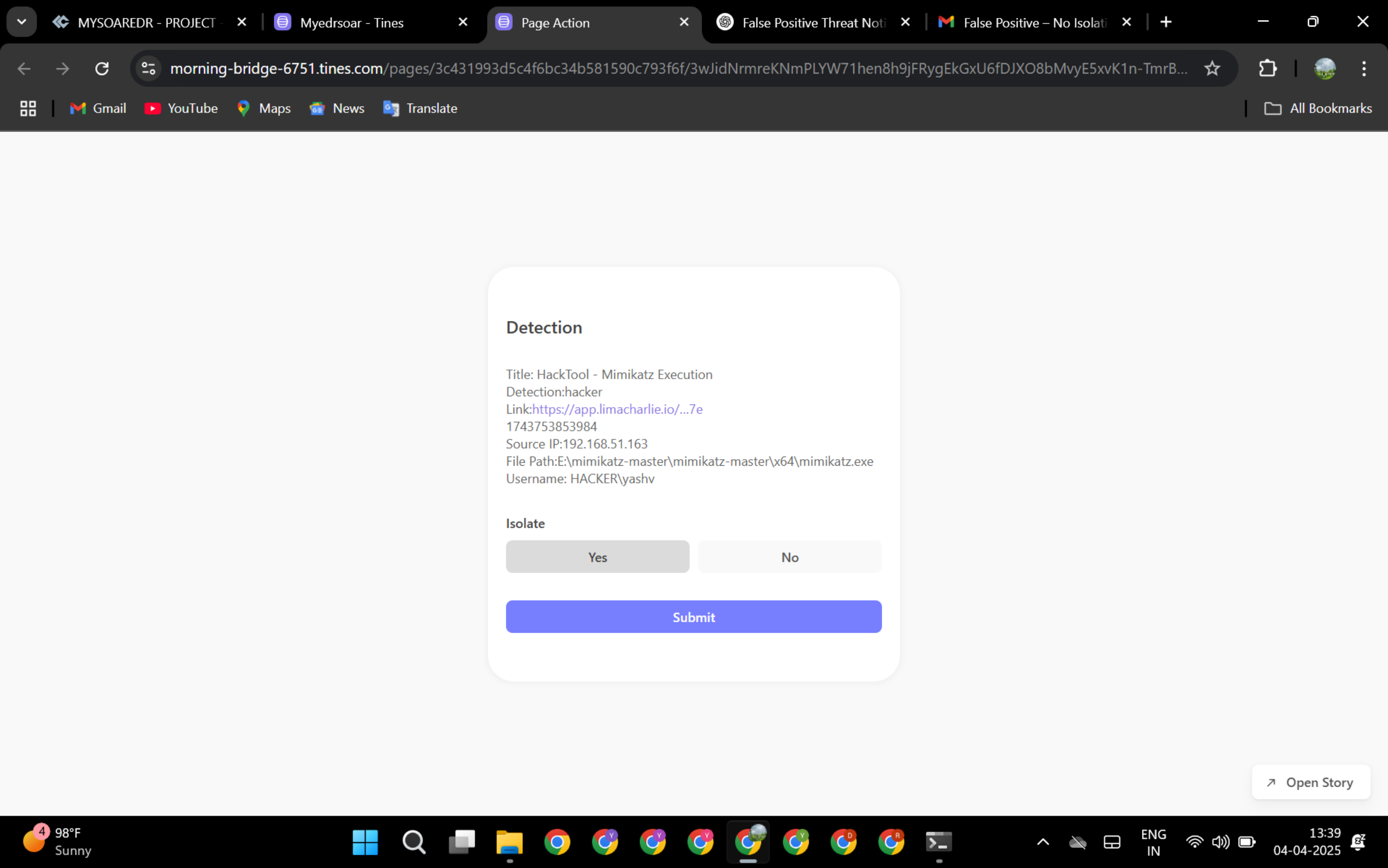
Yashvardhan Singh 13:29 (9 minutes ago)

Following our recent alert, we would like to inform you that the system in question has not been isolated, as the threat was determined to be a false …

Yashvardhan Singh <mail@tines.io> 13:38 (0 minutes ago)

to me

Following our recent alert, we would like to inform you that the system in question has not been isolated, as the threat was determined to be a false positive upon further investigation. Our team conducted a thorough analysis and confirmed that there is no malicious activity present. All indicators initially flagged have been verified as benign. We will continue to monitor the system closely and take appropriate action should any new developments arise. Please feel free to reach out if you have any questions or require further details.


MYSOAREDR - PROJECT
Myedrsoar - Tines
Page Action
False Positive Threat Noti
False Positive – No Isolati
morning-bridge-6751.tines.com/pages/3c431993d5c4f6bc34b581590c793f6f/3wJidNrmreKNmPLYW71hen8h9jFRygEkGxU6fDJXO8bMvyE5xvK1n-TmrB...
Gmail
YouTube
Maps
News
Translate
All Bookmarks
Open Story
98°F
Sunny
ENG
IN
13:39
04-04-2025

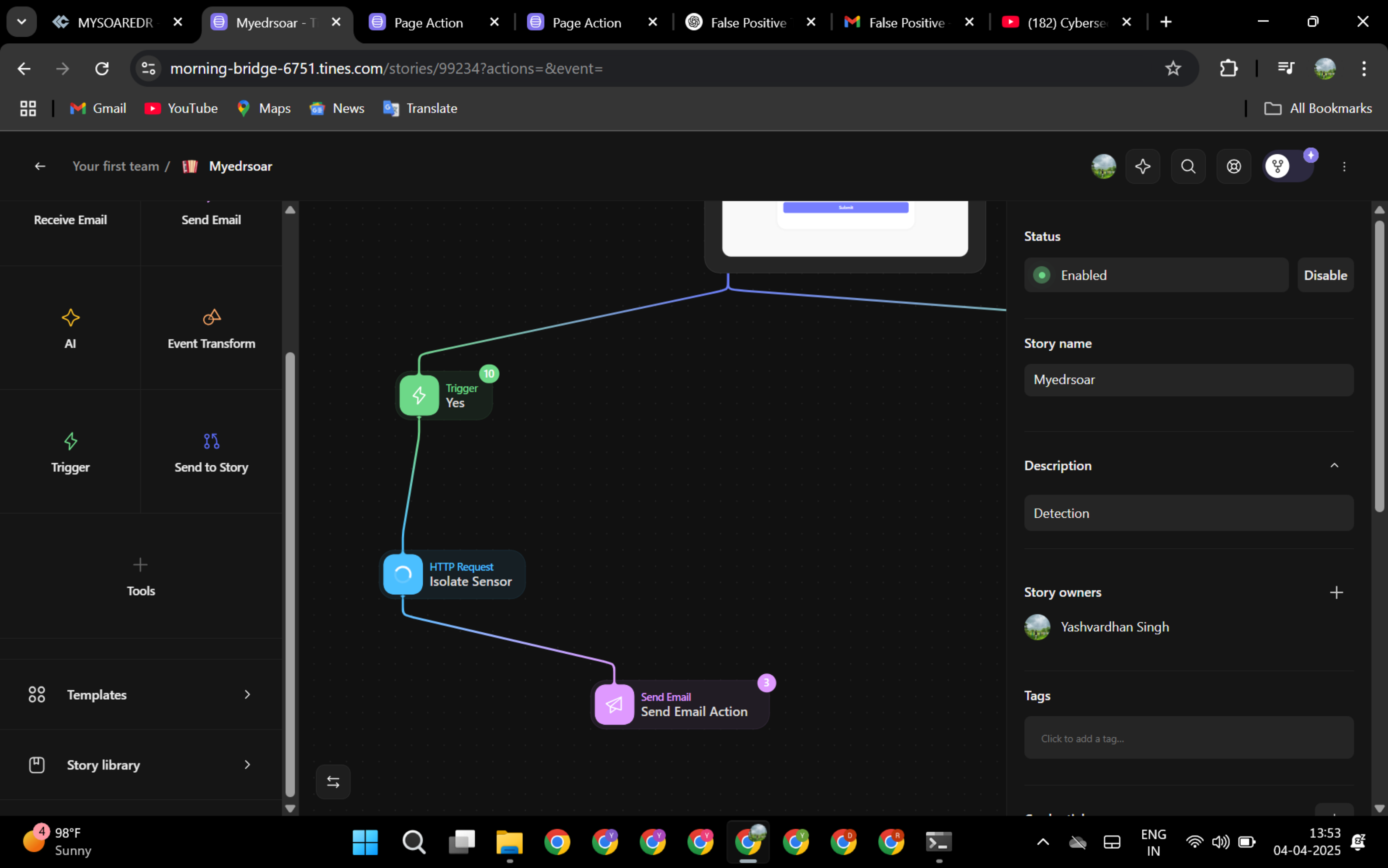
Detection

Title: HackTool - Mimikatz Execution
Detection:hacker
Link:https://app.limacharlie.io/...7e
1743753853984
Source IP:192.168.51.163
File Path:E:\mimikatz-master\mimikatz-master\x64\mimikatz.exe
Username: HACKER\yashv

Isolate

Yes [✓] No

Submit



Status

Enabled

Story name

Myedrsoar

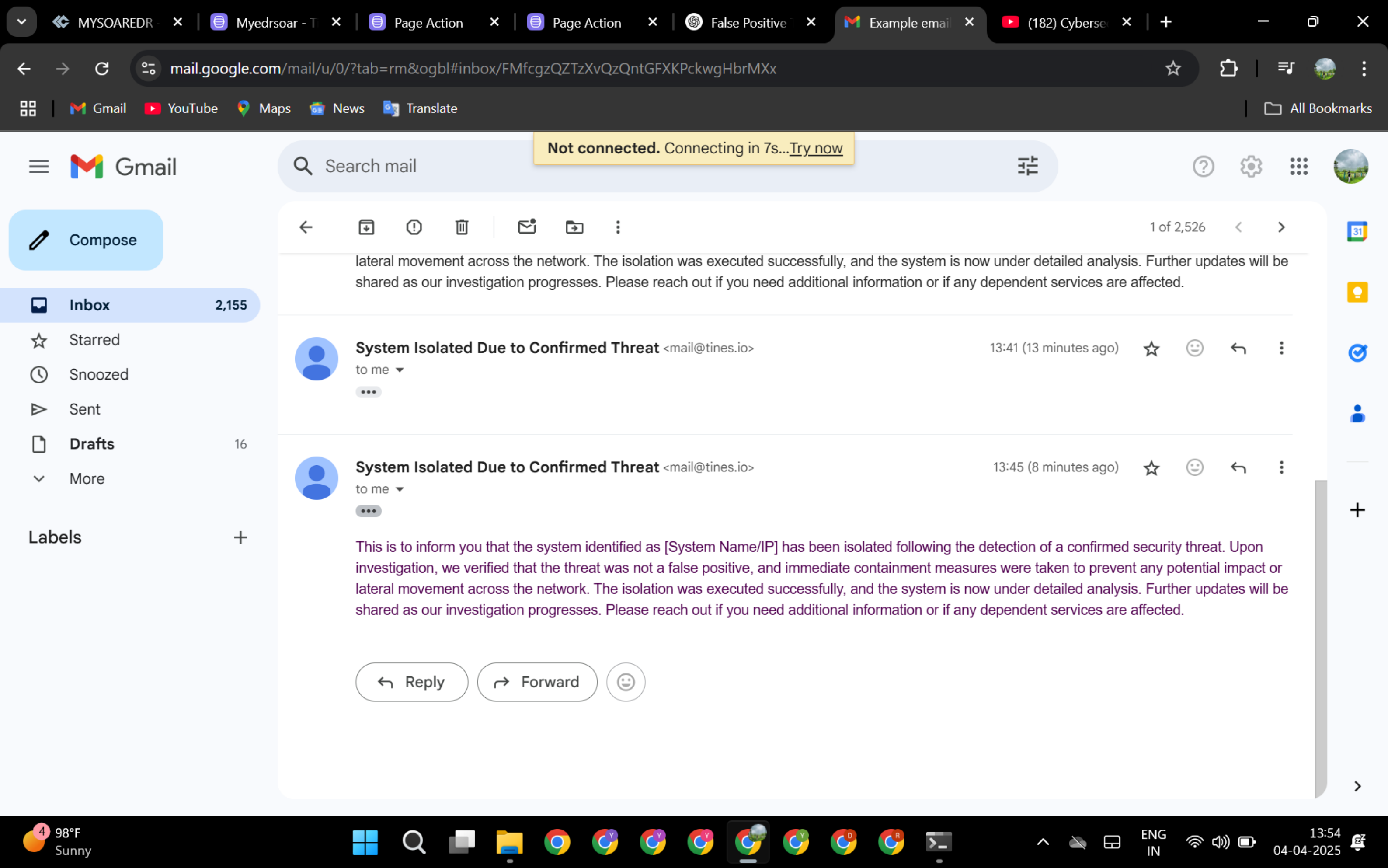
Description

Detection

Story owners

Yashvardhan Singh

Tags



lateral movement across the network. The isolation was executed successfully, and the system is now under detailed analysis. Further updates will be shared as our investigation progresses. Please reach out if you need additional information or if any dependent services are affected.

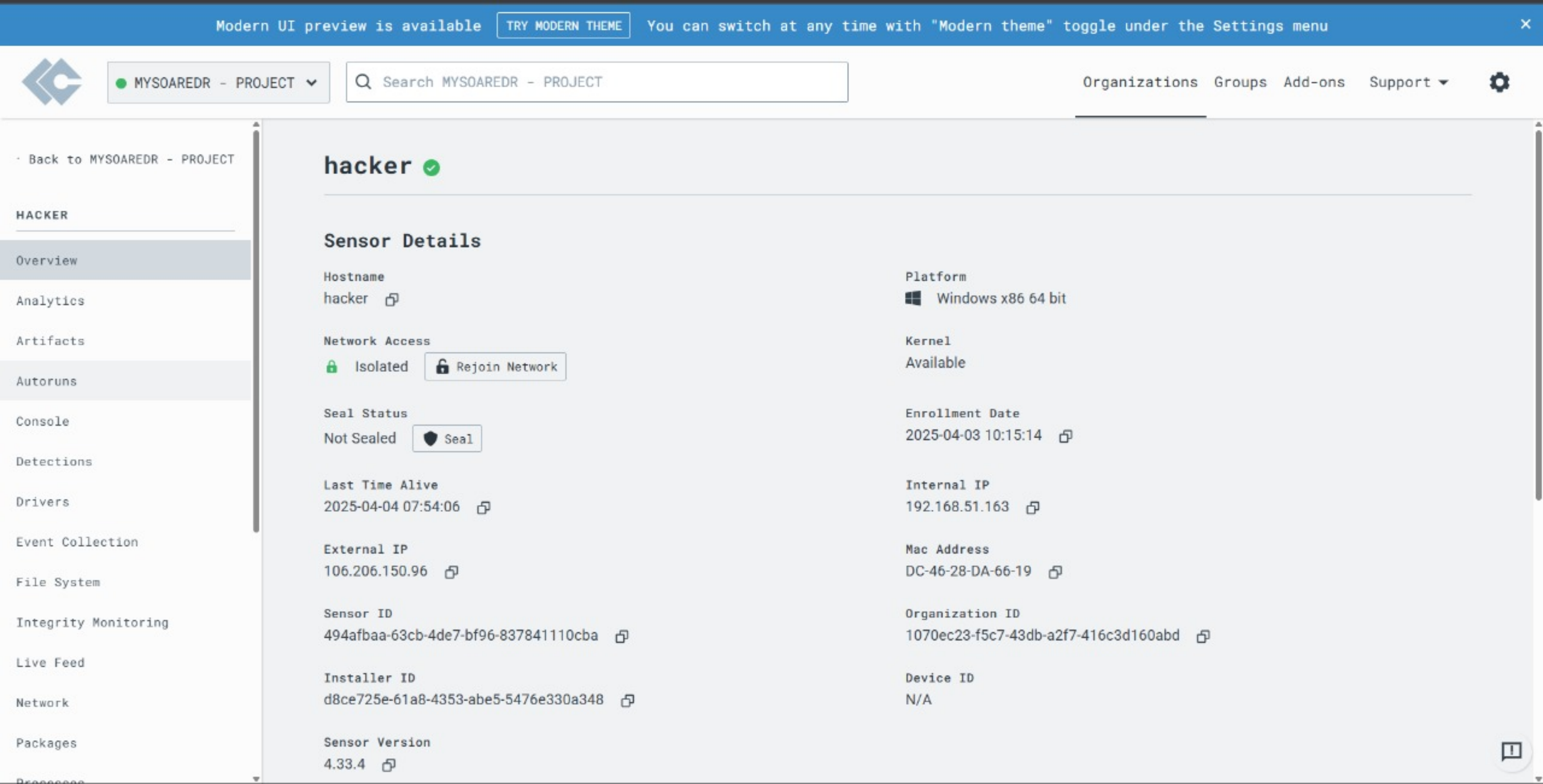
System Isolated Due to Confirmed Threat <mail@tines.io> 13:41 (13 minutes ago)

to me

System Isolated Due to Confirmed Threat <mail@tines.io> 13:45 (8 minutes ago)

to me

This is to inform you that the system identified as [System Name/IP] has been isolated following the detection of a confirmed security threat. Upon investigation, we verified that the threat was not a false positive, and immediate containment measures were taken to prevent any potential impact or lateral movement across the network. The isolation was executed successfully, and the system is now under detailed analysis. Further updates will be shared as our investigation progresses. Please reach out if you need additional information or if any dependent services are affected.



hacker ✓

Sensor Details

Hostname
hacker

Platform
Windows x86 64 bit

Network Access
🔒 Isolated

Kernel
Available

Seal Status
Not Sealed

Enrollment Date
2025-04-03 10:15:14

Last Time Alive
2025-04-04 07:54:06

Internal IP
192.168.51.163

External IP
106.206.150.96

Mac Address
DC-46-28-DA-66-19

Sensor ID
494afbaa-63cb-4de7-bf96-837841110cba

Organization ID
1070ec23-f5c7-43db-a2f7-416c3d160abd

Installer ID
d8ce725e-61a8-4353-abe5-5476e330a348

Device ID
N/A

Sensor Version
4.33.4