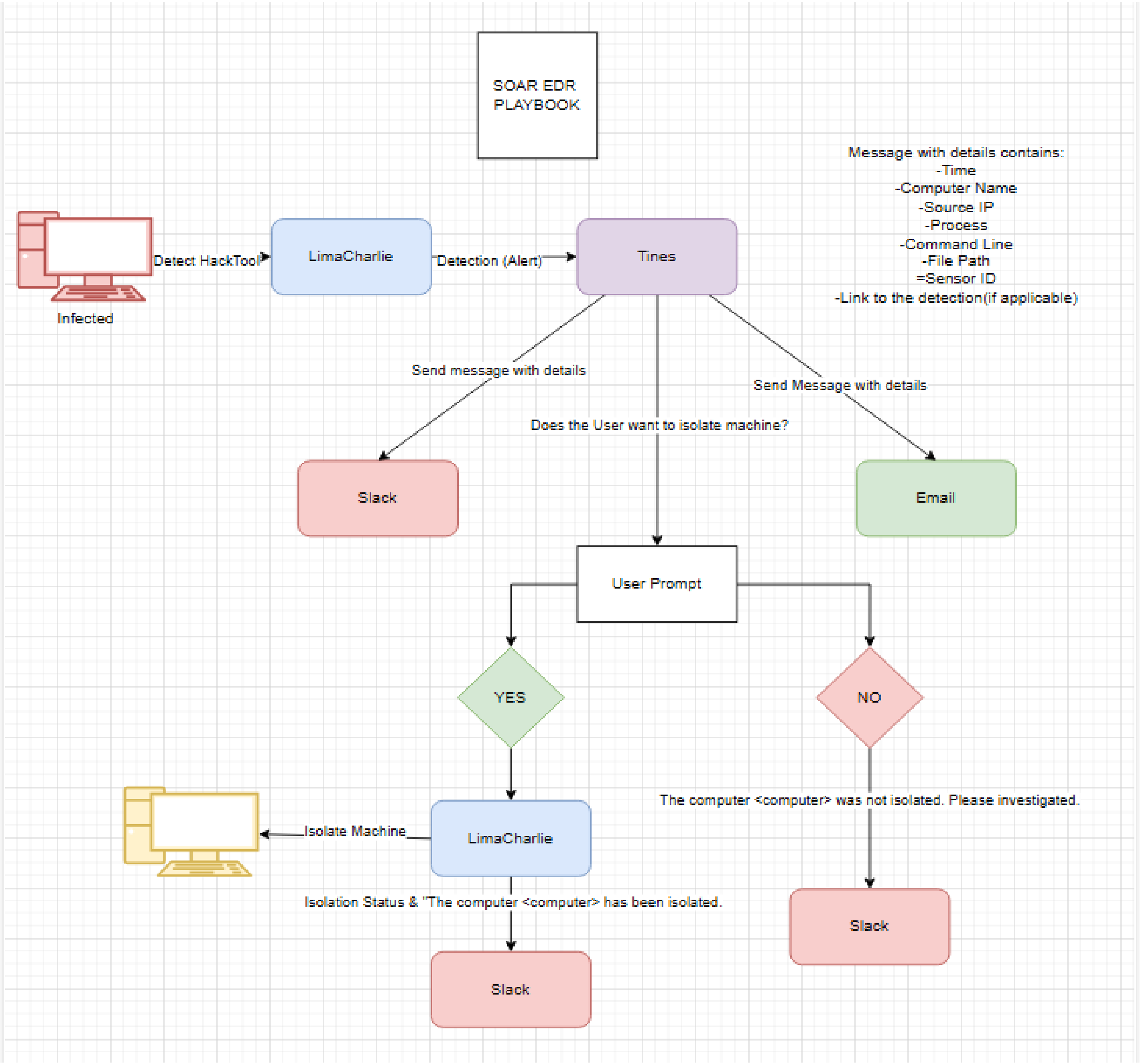
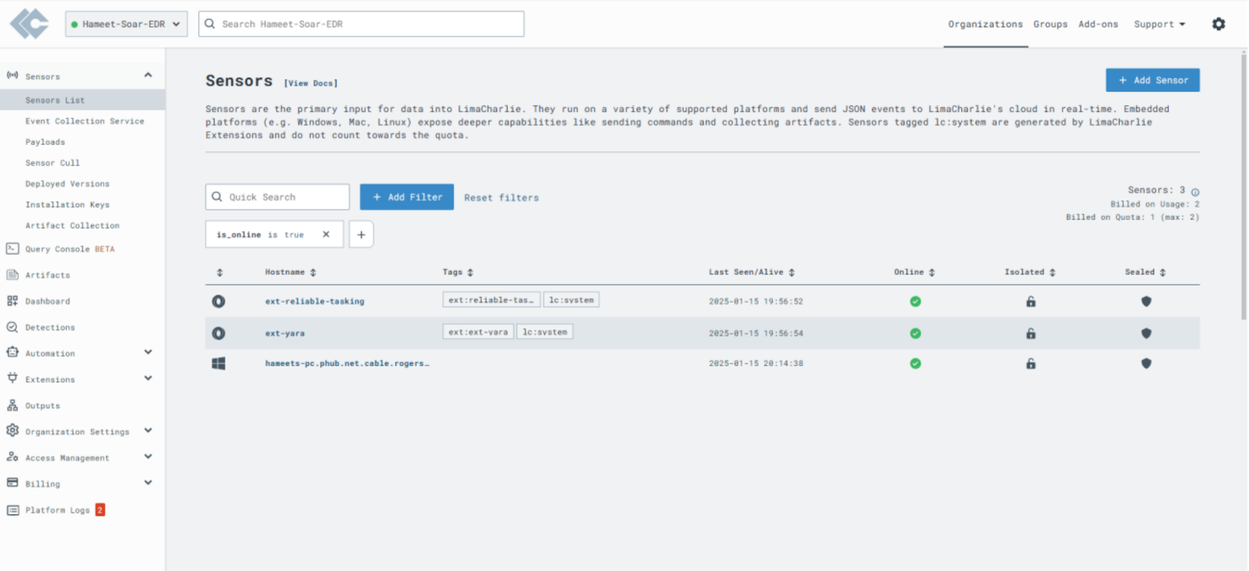
SOAR EDR Project

Hameet Benipal

This project integrates LimaCharlie (EDR) and Tines (SOAR) to automate threat detection and response in a SOC environment. Using LaZagne as a simulated credential-dumping attack, LimaCharlie detects the threat via D&R rules and triggers an automated response in Tines. The SOC analyst receives an alert via email/Slack with an option to isolate the compromised endpoint—if confirmed, LimaCharlie automatically quarantines the affected system from the network. This project showcases EDR-SOAR integration, automated incident response, and real-world SOC workflows.


SOAR EDR PLAYBOOK
Infected
Detect HackTool
LimaCharlie
Detection (Alert)
Tines
Message with details contains:
-Time
-Computer Name
-Source IP
-Process
-Command Line
-File Path
=Sensor ID
-Link to the detection(if applicable)
Send message with details
Send Message with details
Does the User want to isolate machine?
Slack
Email
User Prompt
YES
NO
The computer <computer> was not isolated. Please investigated.
Isolate Machine
LimaCharlie
Isolation Status & "The computer <computer> has been isolated.
Slack
Slack

Ref 1: Playbook and diagram of lab.



Sensors [View Docs]

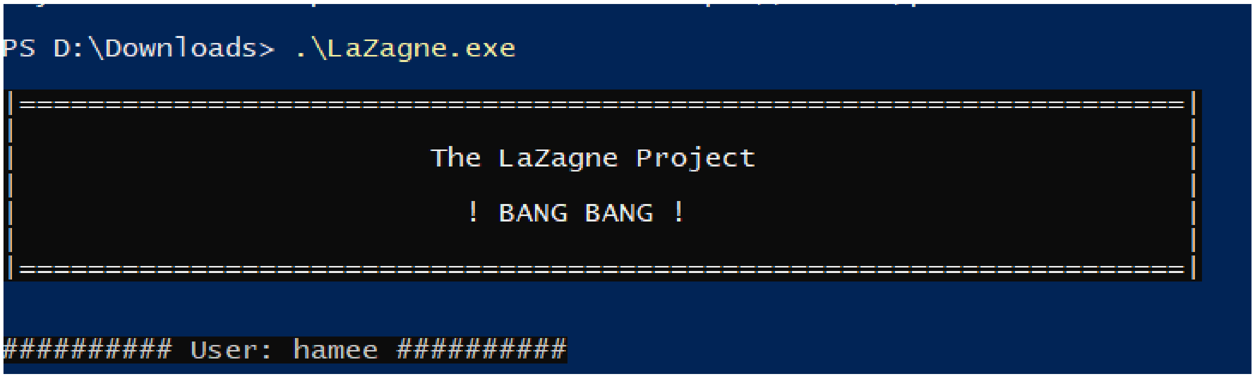
Sensors are the primary input for data into LimaCharlie. They run on a variety of supported platforms and send JSON events to LimaCharlie's cloud in real-time. Embedded platforms (e.g. Windows, Mac, Linux) expose deeper capabilities like sending commands and collecting artifacts. Sensors tagged lc:system are generated by LimaCharlie Extensions and do not count towards the quota.

is_online is true

Sensors: 3
Billed on Usage: 2
Billed on Quota: 1 (max: 2)

	Hostname	Tags	Last Seen/Alive	Online	Isolated	Sealed
	ext-reliable-tasking	ext:reliable-tas… lc:system	2025-01-15 19:56:52	✓		
	ext-yara	ext:ext-yara lc:system	2025-01-15 19:56:54	✓		
	hameets-pc.phub.net.cable.rogers…		2025-01-15 20:14:38	✓		

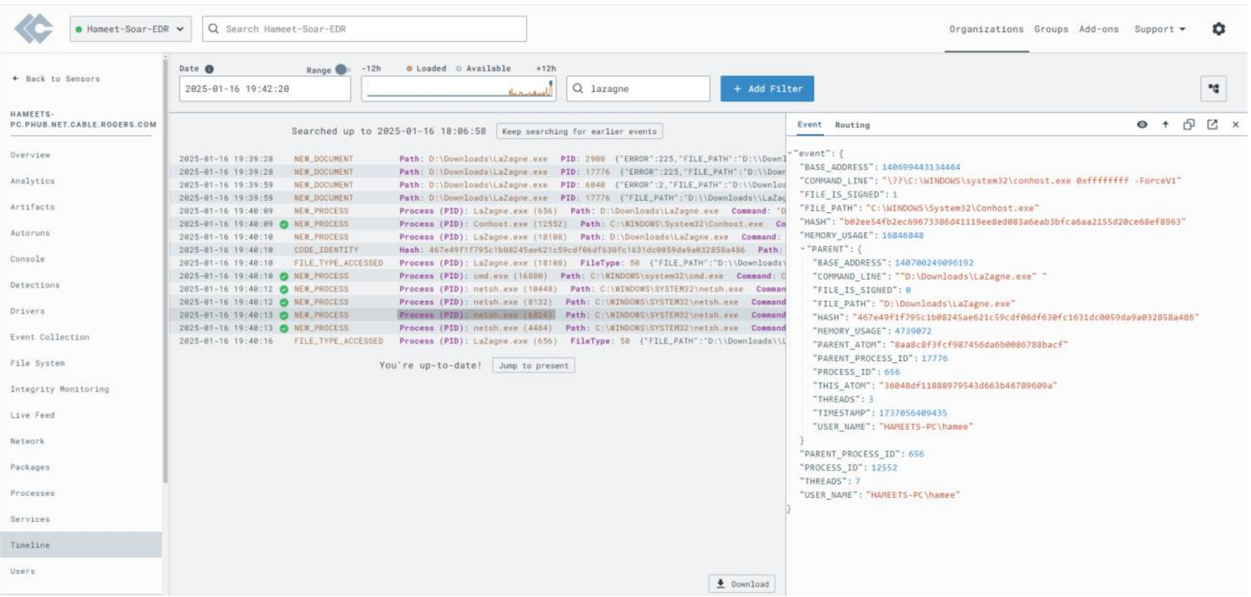
Ref 2: Configure LimaCharlie and add the PC that we are doing this lab on as a sensor.



```
PS D:\Downloads> .\LaZagne.exe

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

########## User: hamee ##########
```



Date 2025-01-16 19:42:20

lazagne

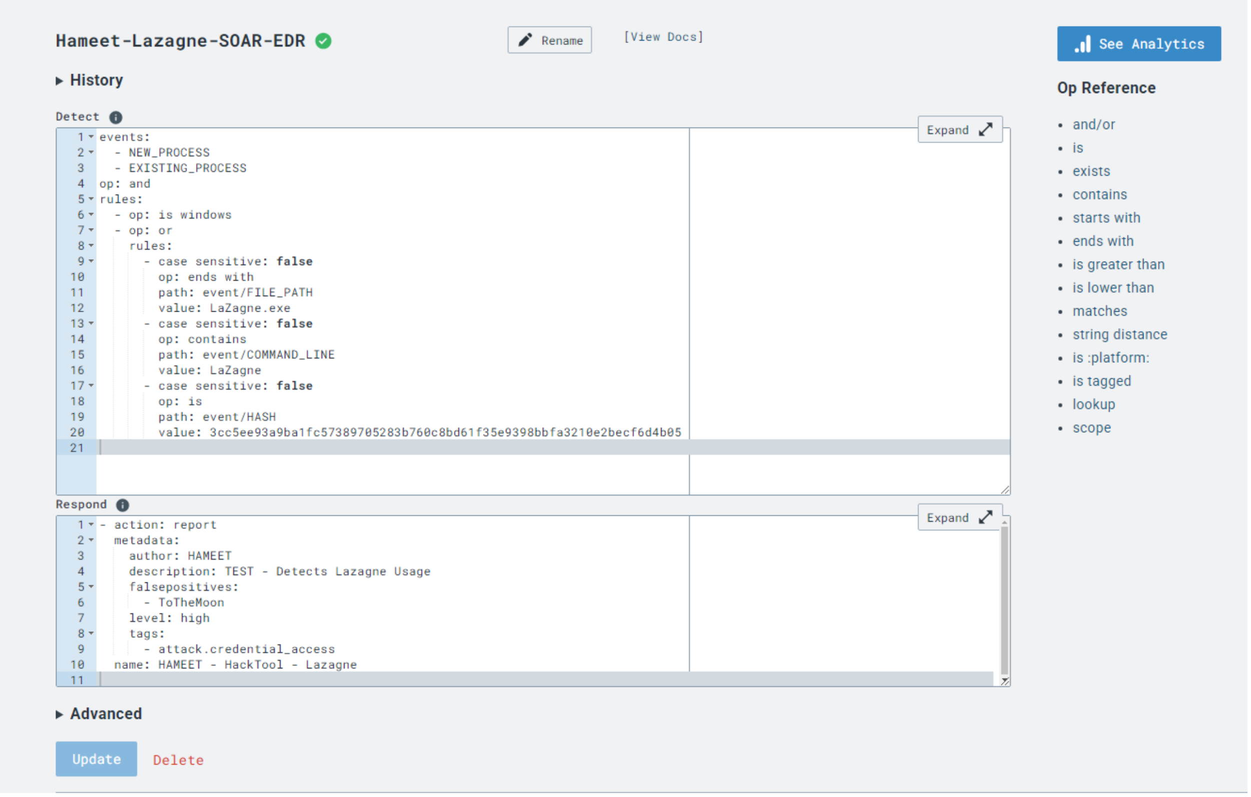
Searched up to 2025-01-16 18:06:58

```
2025-01-16 19:39:28    NEW_DOCUMENT         Path: D:\Downloads\LaZagne.exe  PID: 2900  {"ERROR":225,"FILE_PATH":"D:\\Downl
2025-01-16 19:39:28    NEW_DOCUMENT         Path: D:\Downloads\LaZagne.exe  PID: 17776  {"ERROR":225,"FILE_PATH":"D:\\Dowr
2025-01-16 19:39:59    NEW_DOCUMENT         Path: D:\Downloads\LaZagne.exe  PID: 6040  {"ERROR":2,"FILE_PATH":"D:\\Downlo
2025-01-16 19:39:59    NEW_DOCUMENT         Path: D:\Downloads\LaZagne.exe  PID: 17776  {"FILE_PATH":"D:\\Downloads\\LaZag
2025-01-16 19:40:09    NEW_PROCESS          Process (PID): LaZagne.exe (656)  Path: D:\Downloads\LaZagne.exe  Command: "D
2025-01-16 19:40:09  ✓ NEW_PROCESS          Process (PID): Conhost.exe (12552)  Path: C:\WINDOWS\System32\Conhost.exe  Co
2025-01-16 19:40:10    NEW_PROCESS          Process (PID): LaZagne.exe (18108)  Path: D:\Downloads\LaZagne.exe  Command:
2025-01-16 19:40:10    CODE_IDENTITY        Hash: 467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486  Path:
2025-01-16 19:40:10    FILE_TYPE_ACCESSED   Process (PID): LaZagne.exe (18108)  FileType: 50  {"FILE_PATH":"D:\\Downloads\
2025-01-16 19:40:10  ✓ NEW_PROCESS          Process (PID): cmd.exe (16880)  Path: C:\WINDOWS\system32\cmd.exe  Command: C
2025-01-16 19:40:12  ✓ NEW_PROCESS          Process (PID): netsh.exe (10448)  Path: C:\WINDOWS\SYSTEM32\netsh.exe  Comman
2025-01-16 19:40:12  ✓ NEW_PROCESS          Process (PID): netsh.exe (8132)  Path: C:\WINDOWS\SYSTEM32\netsh.exe  Command
2025-01-16 19:40:13  ✓ NEW_PROCESS          Process (PID): netsh.exe (6824)  Path: C:\WINDOWS\SYSTEM32\netsh.exe  Command
2025-01-16 19:40:13  ✓ NEW_PROCESS          Process (PID): netsh.exe (4484)  Path: C:\WINDOWS\SYSTEM32\netsh.exe  Command
2025-01-16 19:40:16    FILE_TYPE_ACCESSED   Process (PID): LaZagne.exe (656)  FileType: 50  {"FILE_PATH":"D:\\Downloads\\L
```

You're up-to-date!

```
"event": {
  "BASE_ADDRESS": 140699443134464
  "COMMAND_LINE": "\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1"
  "FILE_IS_SIGNED": 1
  "FILE_PATH": "C:\WINDOWS\System32\Conhost.exe"
  "HASH": "b02ee54fb2ec69673386d41119ee8ed083a6eab3bfca6aa2155d20ce68ef8963"
  "MEMORY_USAGE": 16846848
  "PARENT": {
    "BASE_ADDRESS": 140700249096192
    "COMMAND_LINE": ""D:\Downloads\LaZagne.exe" "
    "FILE_IS_SIGNED": 0
    "FILE_PATH": "D:\Downloads\LaZagne.exe"
    "HASH": "467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486"
    "MEMORY_USAGE": 4739072
    "PARENT_ATOM": "8aa8c8f3fcf987456da6b0086788bacf"
    "PARENT_PROCESS_ID": 17776
    "PROCESS_ID": 656
    "THIS_ATOM": "36048df11888979543d663b46789609a"
    "THREADS": 3
    "TIMESTAMP": 1737056409435
    "USER_NAME": "HAMEETS-PC\hamee"
  }
  "PARENT_PROCESS_ID": 656
  "PROCESS_ID": 12552
  "THREADS": 7
  "USER_NAME": "HAMEETS-PC\hamee"
}
```

Ref 3: Download and install LaZagne as the program that will complete the attack. This will *generate telemetry. Then we check the timeline tab on LimaCharlie for events and open the information regarding the new process event including LaZagne.*



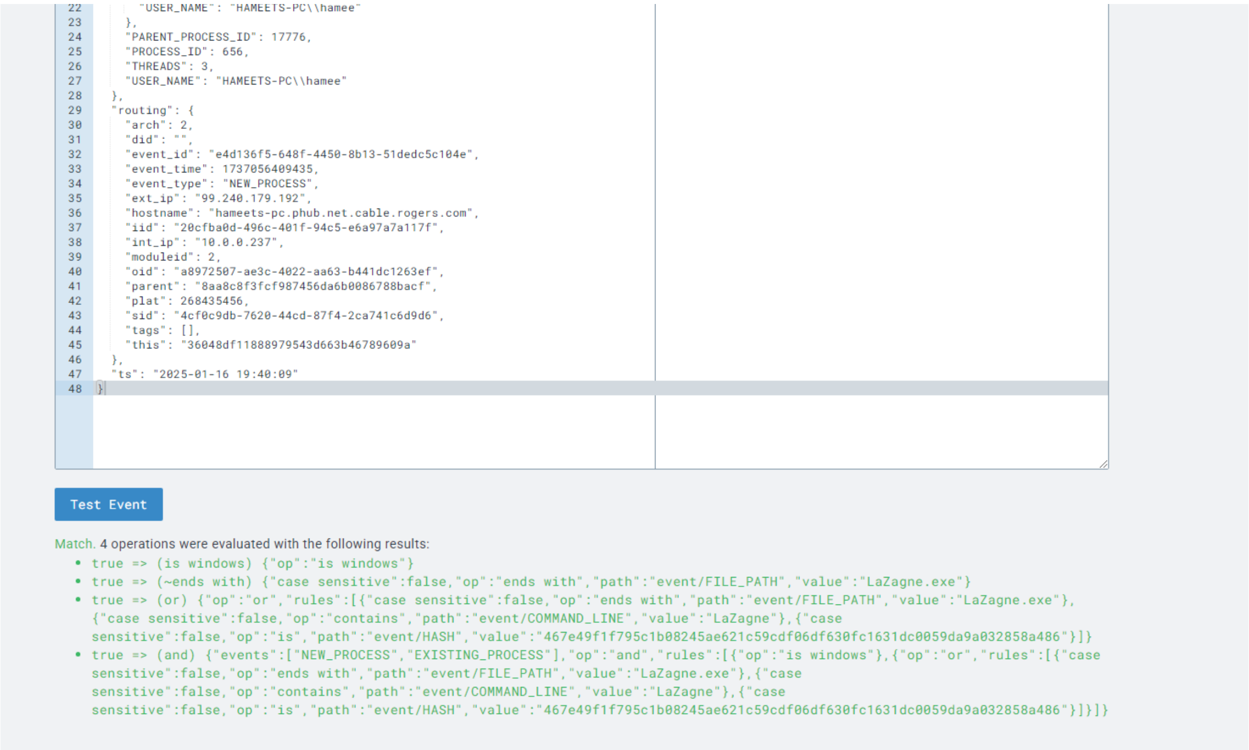
Detect

```yaml
events:
  - NEW_PROCESS
  - EXISTING_PROCESS
op: and
rules:
  - op: is windows
  - op: or
    rules:
      - case sensitive: false
        op: ends with
        path: event/FILE_PATH
        value: LaZagne.exe
      - case sensitive: false
        op: contains
        path: event/COMMAND_LINE
        value: LaZagne
      - case sensitive: false
        op: is
        path: event/HASH
        value: 3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05
```

Respond

```yaml
- action: report
  metadata:
    author: HAMEET
    description: TEST - Detects Lazagne Usage
    falsepositives:
      - ToTheMoon
    level: high
    tags:
      - attack.credential_access
  name: HAMEET - HackTool - Lazagne
```

Ref 4: Create a D&R automation rule under LimaCharlie to detect for file paths, command lines, or hashes that match with LaZagne. This will generate a report if such is detected.

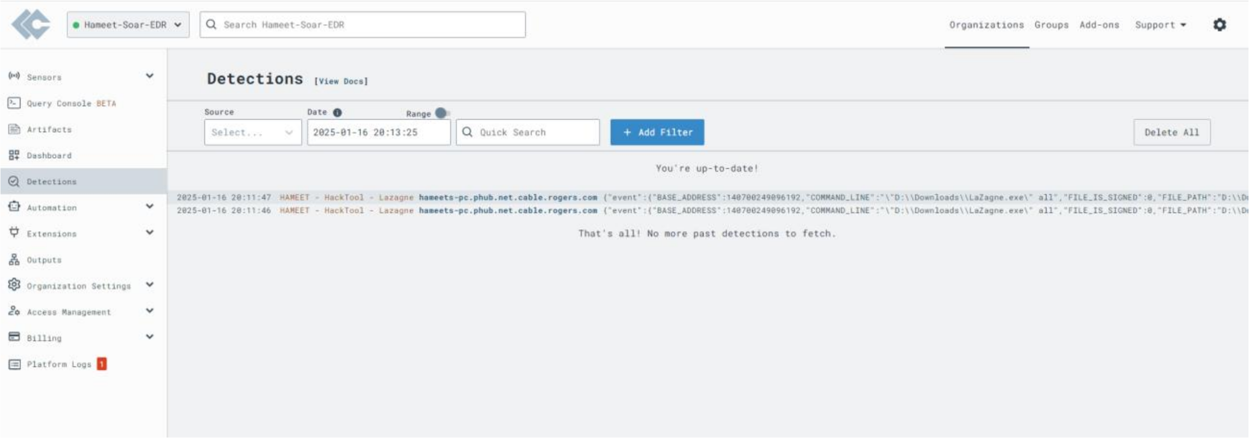


```
      "USER_NAME": "HAMEETS-PC\\hamee"
    },
    "PARENT_PROCESS_ID": 17776,
    "PROCESS_ID": 656,
    "THREADS": 3,
    "USER_NAME": "HAMEETS-PC\\hamee"
  },
  "routing": {
    "arch": 2,
    "did": "",
    "event_id": "e4d136f5-648f-4450-8b13-51dedc5c104e",
    "event_time": 1737056409435,
    "event_type": "NEW_PROCESS",
    "ext_ip": "99.240.179.192",
    "hostname": "hameets-pc.phub.net.cable.rogers.com",
    "iid": "20cfba0d-496c-401f-94c5-e6a97a7a117f",
    "int_ip": "10.0.0.237",
    "moduleid": 2,
    "oid": "a8972507-ae3c-4022-aa63-b441dc1263ef",
    "parent": "8aa8c8f3fcf987456da6b0086788bacf",
    "plat": 268435456,
    "sid": "4cf0c9db-7620-44cd-87f4-2ca741c6d9d6",
    "tags": [],
    "this": "36048df11888979543d663b46789609a"
  },
  "ts": "2025-01-16 19:40:09"
}
```

Match. 4 operations were evaluated with the following results:

```
• true => (is windows) {"op":"is windows"}
• true => (~ends with) {"case sensitive":false,"op":"ends with","path":"event/FILE_PATH","value":"LaZagne.exe"}
• true => (or) {"op":"or","rules":[{"case sensitive":false,"op":"ends with","path":"event/FILE_PATH","value":"LaZagne.exe"},
  {"case sensitive":false,"op":"contains","path":"event/COMMAND_LINE","value":"LaZagne"},{"case
  sensitive":false,"op":"is","path":"event/HASH","value":"467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486"}]}
• true => (and) {"events":["NEW_PROCESS","EXISTING_PROCESS"],"op":"and","rules":[{"op":"is windows"},{"op":"or","rules":[{"case
  sensitive":false,"op":"ends with","path":"event/FILE_PATH","value":"LaZagne.exe"},{"case
  sensitive":false,"op":"contains","path":"event/COMMAND_LINE","value":"LaZagne"},{"case
  sensitive":false,"op":"is","path":"event/HASH","value":"467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486"}]}]}
```

Ref 5: Copy event code from LimaCharlie timeline from when it was first ran (in Ref 3) and paste into the rule testing section. It was run and was successful for 4 matches as shown in screenshot indicating the rule is working as intended.



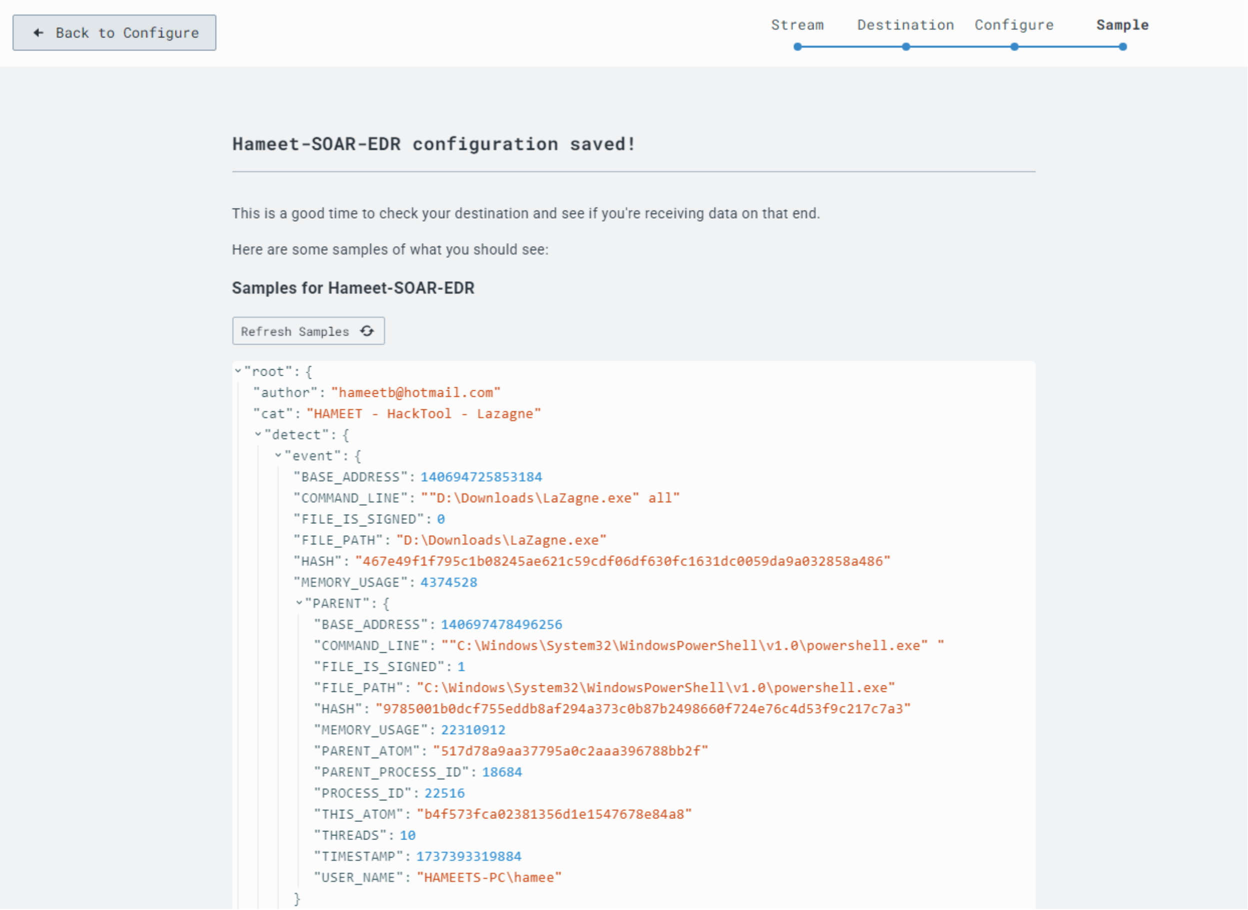
Date: 2025-01-16 20:13:25

You're up-to-date!

```
2025-01-16 20:11:47  HAMEET - HackTool - Lazagne hameets-pc.phub.net.cable.rogers.com {"event":{"BASE_ADDRESS":140700249096192,"COMMAND_LINE":"\"D:\\Downloads\\LaZagne.exe\" all","FILE_IS_SIGNED":0,"FILE_PATH":"D:\\Do
2025-01-16 20:11:46  HAMEET - HackTool - Lazagne hameets-pc.phub.net.cable.rogers.com {"event":{"BASE_ADDRESS":140700249096192,"COMMAND_LINE":"\"D:\\Downloads\\LaZagne.exe\" all","FILE_IS_SIGNED":0,"FILE_PATH":"D:\\Do
```

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

Ref 6: LaZagne was executed one more time and a detection alert was reported on the LimaCharlie dashboard indicating the D&R rule is in effect and working as intended.



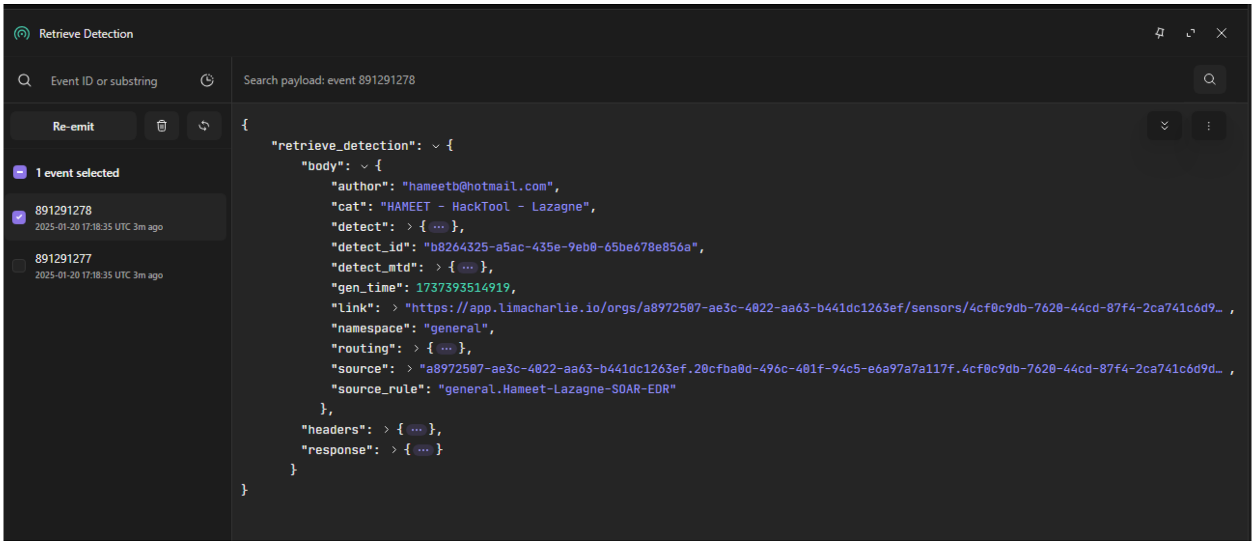
Hameet-SOAR-EDR configuration saved!

This is a good time to check your destination and see if you're receiving data on that end.

Here are some samples of what you should see:

Samples for Hameet-SOAR-EDR

```
˅"root": {
  "author": "hameetb@hotmail.com"
  "cat": "HAMEET - HackTool - Lazagne"
 ˅"detect": {
   ˅"event": {
      "BASE_ADDRESS": 140694725853184
      "COMMAND_LINE": ""D:\Downloads\LaZagne.exe" all"
      "FILE_IS_SIGNED": 0
      "FILE_PATH": "D:\Downloads\LaZagne.exe"
      "HASH": "467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486"
      "MEMORY_USAGE": 4374528
     ˅"PARENT": {
        "BASE_ADDRESS": 140697478496256
        "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": "9785001b0dcf755eddb8af294a373c0b87b2498660f724e76c4d53f9c217c7a3"
        "MEMORY_USAGE": 22310912
        "PARENT_ATOM": "517d78a9aa37795a0c2aaa396788bb2f"
        "PARENT_PROCESS_ID": 18684
        "PROCESS_ID": 22516
        "THIS_ATOM": "b4f573fca02381356d1e1547678e84a8"
        "THREADS": 10
        "TIMESTAMP": 1737393319884
        "USER_NAME": "HAMEETS-PC\hamee"
      }
```

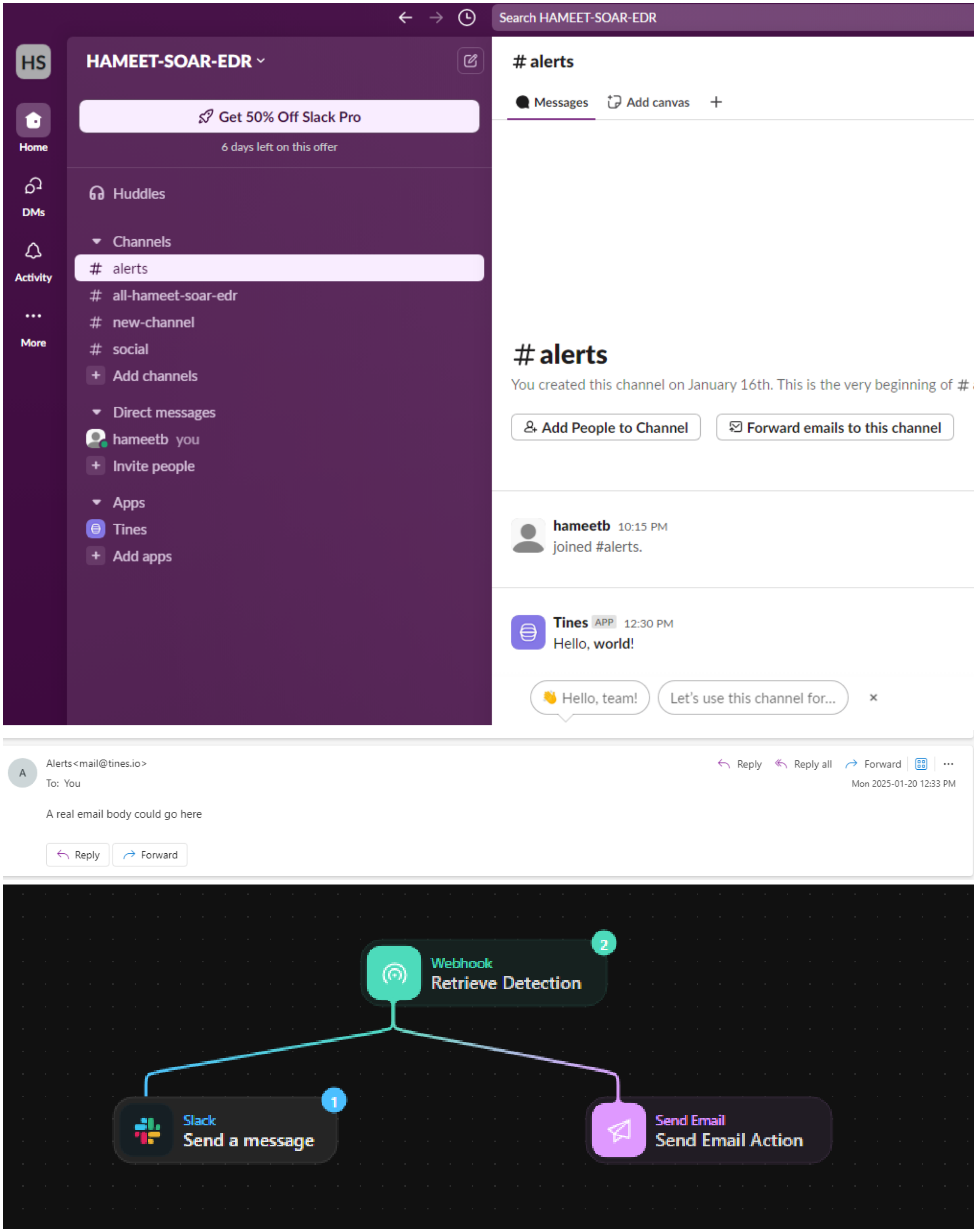


☑ 891291278
2025-01-20 17:18:35 UTC 3m ago

□ 891291277
2025-01-20 17:18:35 UTC 3m ago

```
{
    "retrieve_detection": ˅ {
        "body": ˅ {
            "author": "hameetb@hotmail.com",
            "cat": "HAMEET - HackTool - Lazagne",
            "detect": › { ··· },
            "detect_id": "b8264325-a5ac-435e-9eb0-65be678e856a",
            "detect_mtd": › { ··· },
            "gen_time": 1737393514919,
            "link": › "https://app.limacharlie.io/orgs/a8972507-ae3c-4022-aa63-b441dc1263ef/sensors/4cf0c9db-7620-44cd-87f4-2ca741c6d9… ,
            "namespace": "general",
            "routing": › { ··· },
            "source": › "a8972507-ae3c-4022-aa63-b441dc1263ef.20cfba0d-496c-401f-94c5-e6a97a7a117f.4cf0c9db-7620-44cd-87f4-2ca741c6d9d… ,
            "source_rule": "general.Hameet-Lazagne-SOAR-EDR"
        },
        "headers": › { ··· },
        "response": › { ··· }
    }
}
```

Ref 7: Now it is time to implement the automation portion of this lab on Tines. The LimaCharlie webhook was configured in Tines to detect events and once LaZagne was executed again, events were detected in both LimaCharlie and Tines. The top screenshot is from LimaCharlie, and the bottom is from Tines.



alerts

You created this channel on January 16th. This is the very beginning of #

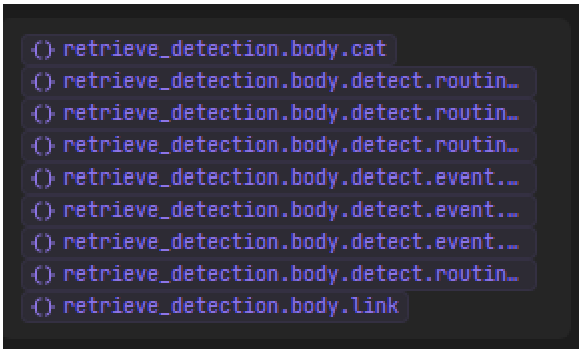
hameetb 10:15 PM
joined #alerts.

Tines APP 12:30 PM
Hello, world!

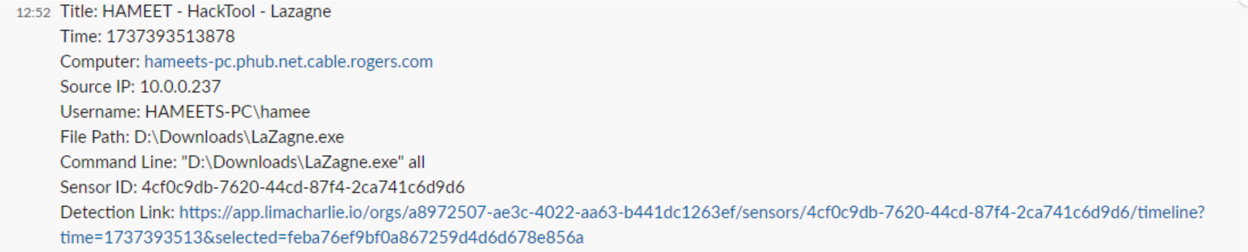
Alerts<mail@tines.io>
To: You
Mon 2025-01-20 12:33 PM

A real email body could go here

Ref 8: Next, the link was established between Tines and Slack and a test message was sent in the Alerts channel to confirm it is functioning correctly. The same was done for a test email.

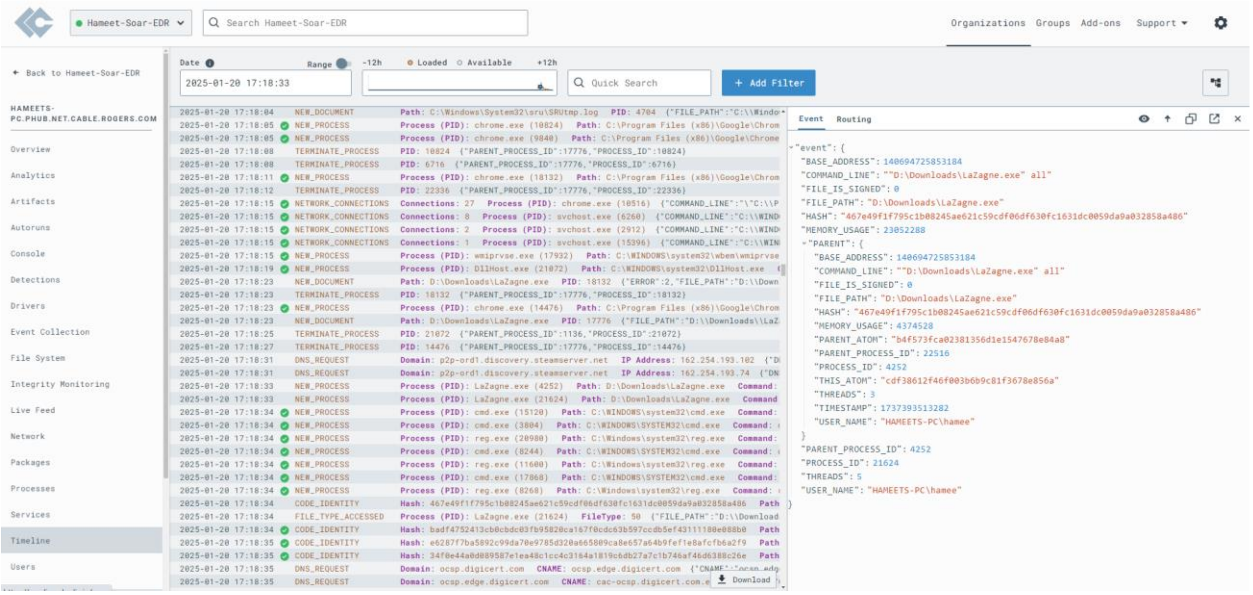


```
{} retrieve_detection.body.cat
{} retrieve_detection.body.detect.routin…
{} retrieve_detection.body.detect.routin…
{} retrieve_detection.body.detect.routin…
{} retrieve_detection.body.detect.event.…
{} retrieve_detection.body.detect.event.…
{} retrieve_detection.body.detect.event.…
{} retrieve_detection.body.detect.routin…
{} retrieve_detection.body.link
```



12:52 Title: HAMEET - HackTool - Lazagne
Time: 1737393513878
Computer: hameets-pc.phub.net.cable.rogers.com
Source IP: 10.0.0.237
Username: HAMEETS-PC\hamee
File Path: D:\Downloads\LaZagne.exe
Command Line: "D:\Downloads\LaZagne.exe" all
Sensor ID: 4cf0c9db-7620-44cd-87f4-2ca741c6d9d6
Detection Link: https://app.limacharlie.io/orgs/a8972507-ae3c-4022-aa63-b441dc1263ef/sensors/4cf0c9db-7620-44cd-87f4-2ca741c6d9d6/timeline?time=1737393513&selected=feba76ef9bf0a867259d4d6d678e856a

Ref 9: Now we change the content of the slack message and email to provide useful information about the detection and not just a sample message.

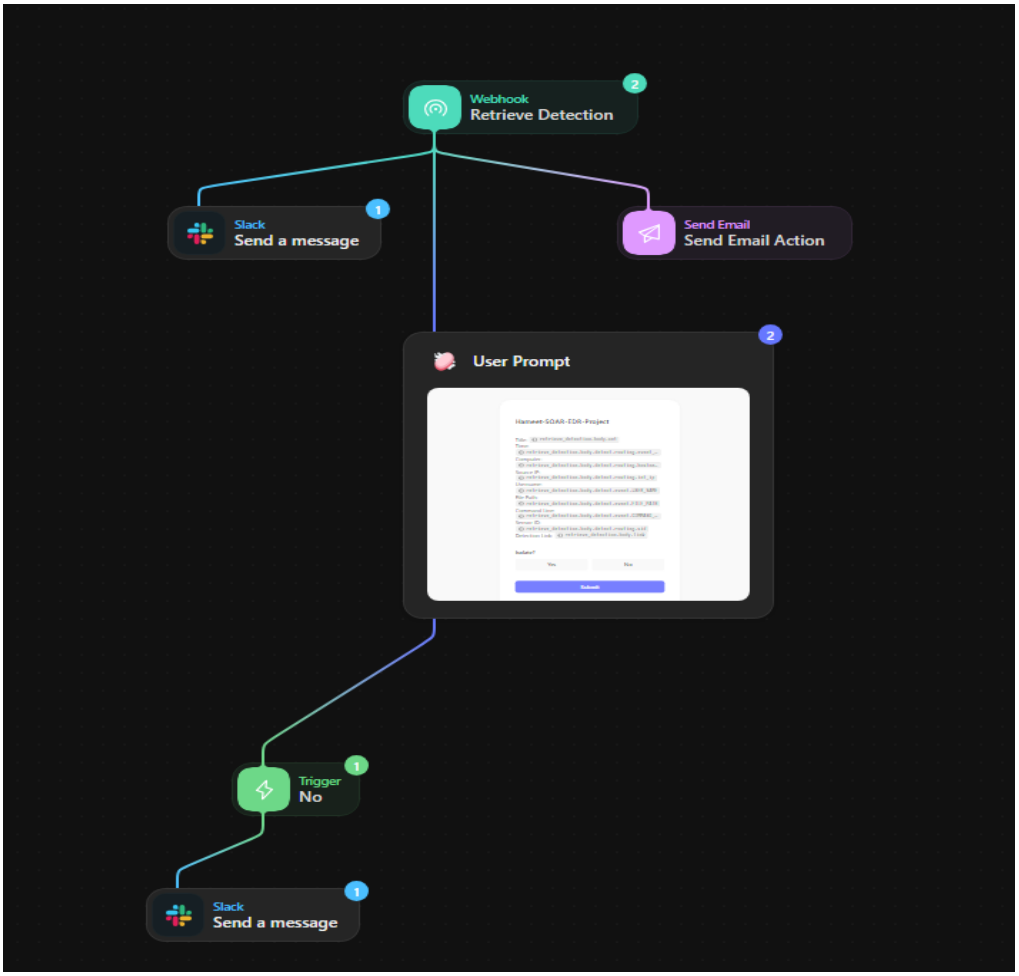


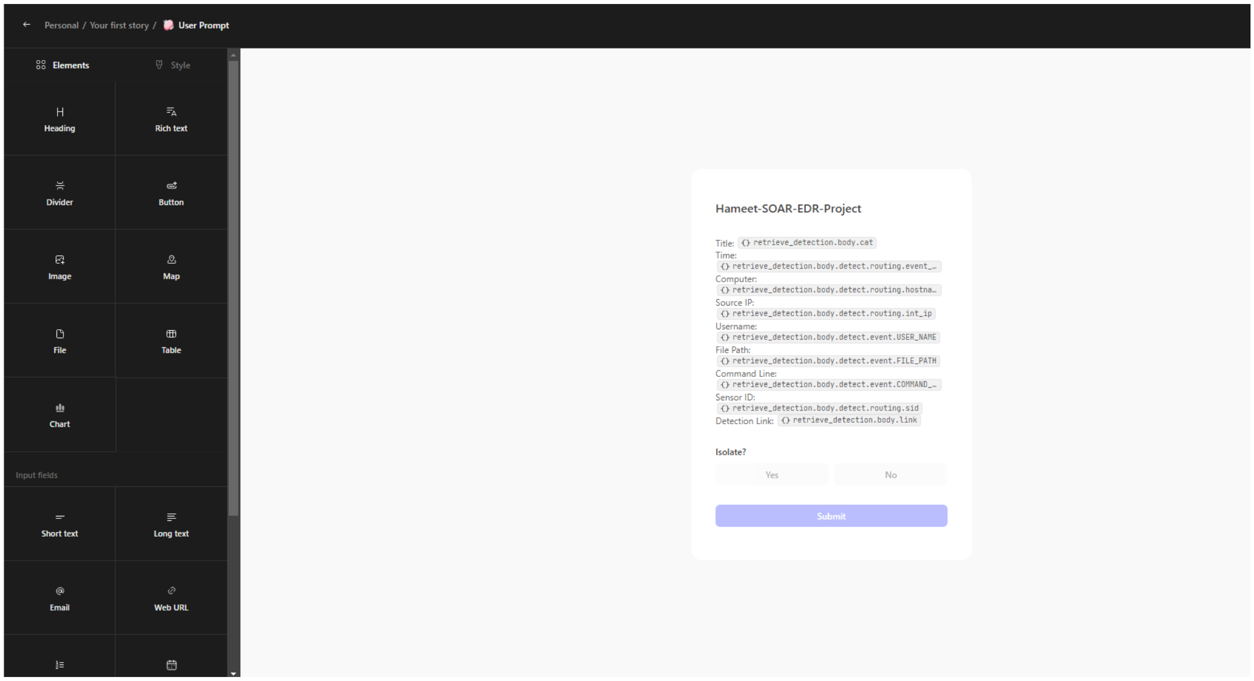
Date: 2025-01-20 17:18:33

```
2025-01-20 17:18:04   NEW_DOCUMENT          Path: C:\Windows\System32\sru\SRUtmp.log   PID: 4704  {"FILE_PATH":"C:\\Windo
2025-01-20 17:18:05 ✓ NEW_PROCESS           Process (PID): chrome.exe (10824)   Path: C:\Program Files (x86)\Google\Chrom
2025-01-20 17:18:05 ✓ NEW_PROCESS           Process (PID): chrome.exe (9840)   Path: C:\Program Files (x86)\Google\Chrome
2025-01-20 17:18:08   TERMINATE_PROCESS     PID: 10824  {"PARENT_PROCESS_ID":17776,"PROCESS_ID":10824}
2025-01-20 17:18:08   TERMINATE_PROCESS     PID: 6716  {"PARENT_PROCESS_ID":17776,"PROCESS_ID":6716}
2025-01-20 17:18:11 ✓ NEW_PROCESS           Process (PID): chrome.exe (18132)   Path: C:\Program Files (x86)\Google\Chrom
2025-01-20 17:18:12   TERMINATE_PROCESS     PID: 22336  {"PARENT_PROCESS_ID":17776,"PROCESS_ID":22336}
2025-01-20 17:18:15 ✓ NETWORK_CONNECTIONS   Connections: 27   Process (PID): chrome.exe (10516)  {"COMMAND_LINE":"\"C:\\P
2025-01-20 17:18:15 ✓ NETWORK_CONNECTIONS   Connections: 8   Process (PID): svchost.exe (6260)  {"COMMAND_LINE":"C:\\WIND
2025-01-20 17:18:15 ✓ NETWORK_CONNECTIONS   Connections: 2   Process (PID): svchost.exe (2912)  {"COMMAND_LINE":"C:\\WIND
2025-01-20 17:18:15 ✓ NETWORK_CONNECTIONS   Connections: 1   Process (PID): svchost.exe (15396)  {"COMMAND_LINE":"C:\\WIN
2025-01-20 17:18:15 ✓ NEW_PROCESS           Process (PID): wmiprvse.exe (17932)   Path: C:\WINDOWS\system32\wbem\wmiprvse
2025-01-20 17:18:19 ✓ NEW_PROCESS           Process (PID): DllHost.exe (21072)   Path: C:\WINDOWS\system32\DllHost.exe   (
2025-01-20 17:18:23   NEW_DOCUMENT          Path: D:\Downloads\LaZagne.exe   PID: 18132  {"ERROR":2,"FILE_PATH":"D:\\Down
2025-01-20 17:18:23   TERMINATE_PROCESS     PID: 18132  {"PARENT_PROCESS_ID":17776,"PROCESS_ID":18132}
2025-01-20 17:18:23 ✓ NEW_PROCESS           Process (PID): chrome.exe (14476)   Path: C:\Program Files (x86)\Google\Chrom
2025-01-20 17:18:23   NEW_DOCUMENT          Path: D:\Downloads\LaZagne.exe   PID: 17776  {"FILE_PATH":"D:\\Downloads\\LaZ
2025-01-20 17:18:25   TERMINATE_PROCESS     PID: 21072  {"PARENT_PROCESS_ID":1136,"PROCESS_ID":21072}
2025-01-20 17:18:27   TERMINATE_PROCESS     PID: 14476  {"PARENT_PROCESS_ID":17776,"PROCESS_ID":14476}
2025-01-20 17:18:31   DNS_REQUEST           Domain: p2p-ord1.discovery.steamserver.net   IP Address: 162.254.193.102  {"D
2025-01-20 17:18:31   DNS_REQUEST           Domain: p2p-ord1.discovery.steamserver.net   IP Address: 162.254.193.74  {"DN
2025-01-20 17:18:33   NEW_PROCESS           Process (PID): LaZagne.exe (4252)   Path: D:\Downloads\LaZagne.exe   Command:
2025-01-20 17:18:33   NEW_PROCESS           Process (PID): LaZagne.exe (21624)   Path: D:\Downloads\LaZagne.exe   Command
2025-01-20 17:18:34 ✓ NEW_PROCESS           Process (PID): cmd.exe (15120)   Path: C:\WINDOWS\system32\cmd.exe   Command:
2025-01-20 17:18:34 ✓ NEW_PROCESS           Process (PID): cmd.exe (3804)   Path: C:\WINDOWS\SYSTEM32\cmd.exe   Command:
2025-01-20 17:18:34 ✓ NEW_PROCESS           Process (PID): reg.exe (20980)   Path: C:\Windows\system32\reg.exe   Command:
2025-01-20 17:18:34 ✓ NEW_PROCESS           Process (PID): cmd.exe (8244)   Path: C:\WINDOWS\SYSTEM32\cmd.exe   Command:
2025-01-20 17:18:34 ✓ NEW_PROCESS           Process (PID): reg.exe (11600)   Path: C:\Windows\system32\reg.exe   Command:
2025-01-20 17:18:34 ✓ NEW_PROCESS           Process (PID): cmd.exe (17868)   Path: C:\WINDOWS\SYSTEM32\cmd.exe   Command:
2025-01-20 17:18:34 ✓ NEW_PROCESS           Process (PID): reg.exe (8268)   Path: C:\Windows\system32\reg.exe   Command:
2025-01-20 17:18:34   CODE_IDENTITY         Hash: 467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486   Path
2025-01-20 17:18:34   FILE_TYPE_ACCESSED    Process (PID): LaZagne.exe (21624)   FileType: 50  {"FILE_PATH":"D:\\Download
2025-01-20 17:18:34 ✓ CODE_IDENTITY         Hash: badf4752413cb0cbdc03fb95820ca167f0cdc63b597ccdb5ef43111100e088b0   Path
2025-01-20 17:18:35 ✓ CODE_IDENTITY         Hash: e6287f7ba5892c99da70e9785d320a665809ca8e657a64b9fef1e8afcfb6a2f9   Path
2025-01-20 17:18:35 ✓ CODE_IDENTITY         Hash: 34f0e44a0d089587e1ea48c1cc4c3164a1819c6db27a7c1b746af46d6388c26e   Path
2025-01-20 17:18:35   DNS_REQUEST           Domain: ocsp.digicert.com   CNAME: ocsp.edge.digicert.com  {"CNAME":"ocsp.edg
2025-01-20 17:18:35   DNS_REQUEST           Domain: ocsp.edge.digicert.com   CNAME: cac-ocsp.digicert.com.e
```

```
"event": {
  "BASE_ADDRESS": 140694725853184
  "COMMAND_LINE": ""D:\Downloads\LaZagne.exe" all"
  "FILE_IS_SIGNED": 0
  "FILE_PATH": "D:\Downloads\LaZagne.exe"
  "HASH": "467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486"
  "MEMORY_USAGE": 23052288
  "PARENT": {
    "BASE_ADDRESS": 140694725853184
    "COMMAND_LINE": ""D:\Downloads\LaZagne.exe" all"
    "FILE_IS_SIGNED": 0
    "FILE_PATH": "D:\Downloads\LaZagne.exe"
    "HASH": "467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486"
    "MEMORY_USAGE": 4374528
    "PARENT_ATOM": "b4f573fca02381356d1e1547678e84a8"
    "PARENT_PROCESS_ID": 22516
    "PROCESS_ID": 4252
    "THIS_ATOM": "cdf38612f46f003b6b9c81f3678e856a"
    "THREADS": 3
    "TIMESTAMP": 1737393513282
    "USER_NAME": "HAMEETS-PC\hamee"
  }
  "PARENT_PROCESS_ID": 4252
  "PROCESS_ID": 21624
  "THREADS": 5
  "USER_NAME": "HAMEETS-PC\hamee"
}
```

Ref 10: Clicking the link in the slack/email will take you to the timeline screen in LimaCharlie where you can see the timeline of events around the detection for further examination and action.





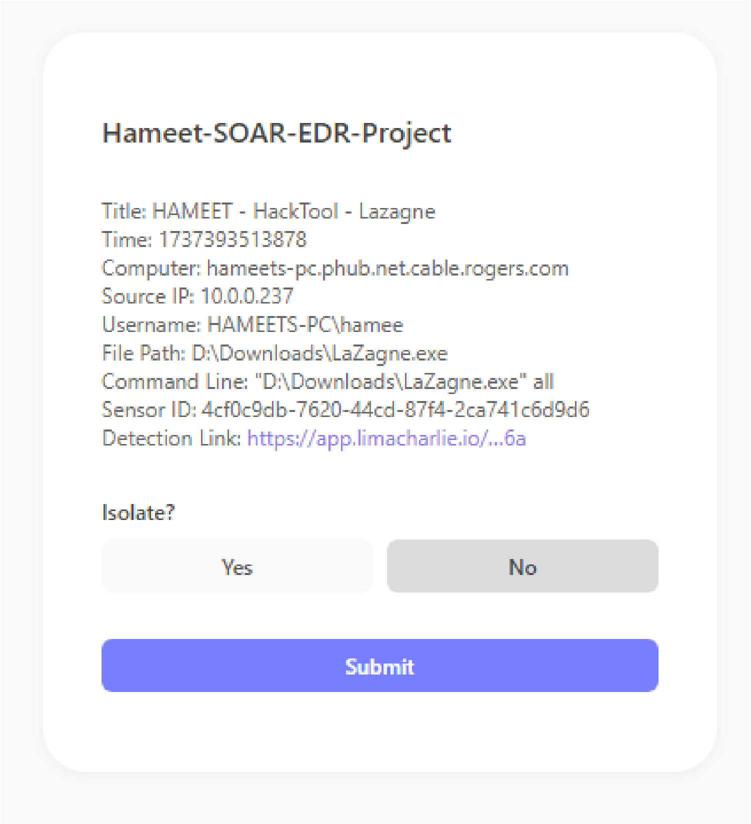
Hameet-SOAR-EDR-Project

Title: {} retrieve_detection.body.cat
Time:
{} retrieve_detection.body.detect.routing.event_…
Computer:
{} retrieve_detection.body.detect.routing.hostna…
Source IP:
{} retrieve_detection.body.detect.routing.int_ip
Username:
{} retrieve_detection.body.detect.event.USER_NAME
File Path:
{} retrieve_detection.body.detect.event.FILE_PATH
Command Line:
{} retrieve_detection.body.detect.event.COMMAND_…
Sensor ID:
{} retrieve_detection.body.detect.routing.sid
Detection Link: {} retrieve_detection.body.link

Isolate?

Yes No

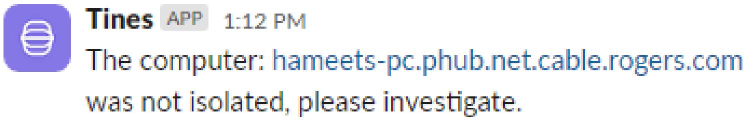
Submit



Hameet-SOAR-EDR-Project

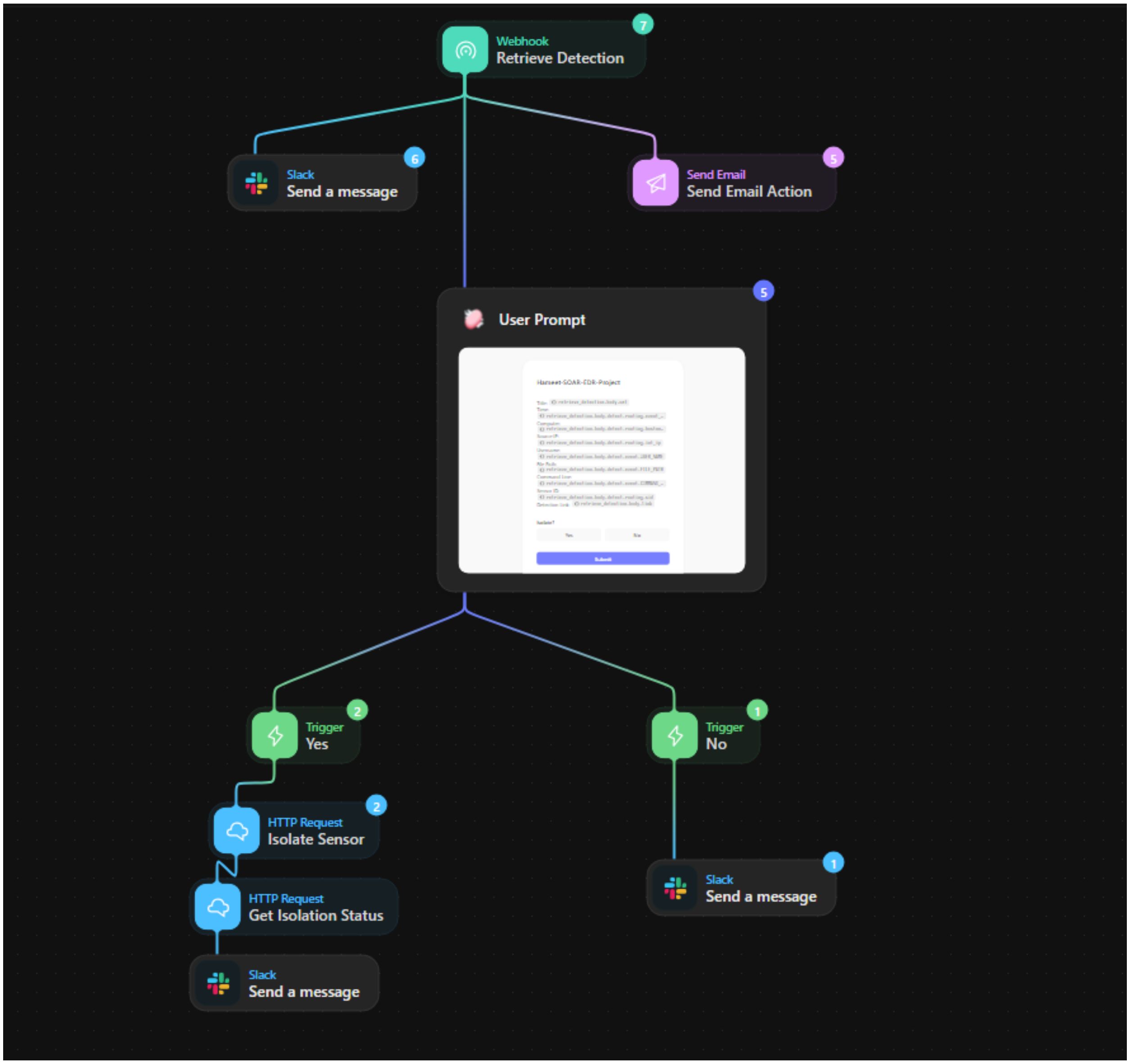
Title: HAMEET - HackTool - Lazagne
Time: 1737393513878
Computer: hameets-pc.phub.net.cable.rogers.com
Source IP: 10.0.0.237
Username: HAMEETS-PC\hamee
File Path: D:\Downloads\LaZagne.exe
Command Line: "D:\Downloads\LaZagne.exe" all
Sensor ID: 4cf0c9db-7620-44cd-87f4-2ca741c6d9d6
Detection Link: https://app.limacharlie.io/...6a

Isolate?

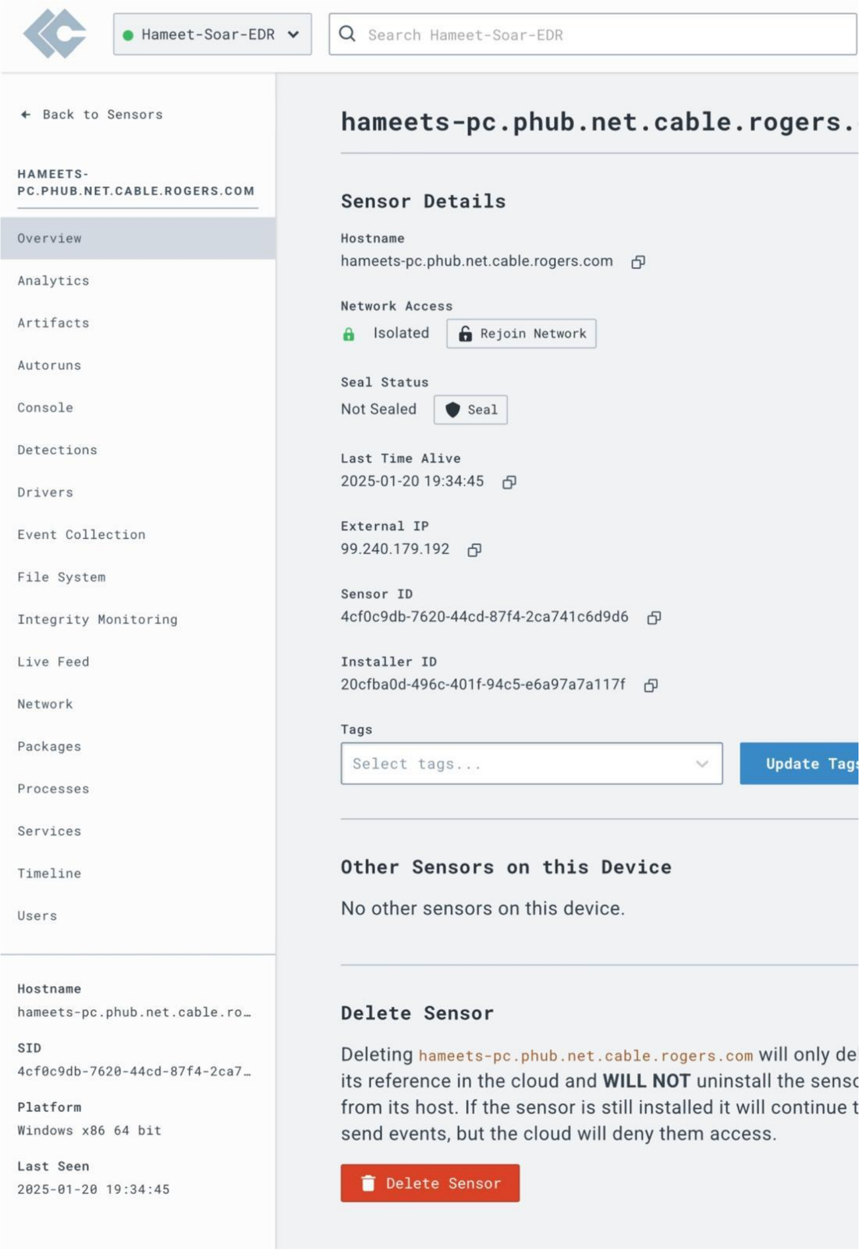


Tines APP 1:12 PM
The computer: hameets-pc.phub.net.cable.rogers.com was not isolated, please investigate.

Ref 11: The user prompt of the workflow was then implemented by adding a page in the Tines story. It was configured to display information about the attack and then prompt the user to either isolate the PC or not. First the “no” option was configured which simply sent a slack message indicating the user chose to not isolate the PC.



Ref 12: The next step was to configure the machine isolation if the user prompt was selected as yes. This is done by using the sensor ID on LimaCharlie and isolating the machine using that as the identifier. Tines has an Isolate Sensor template for LimaCharlie and this was used to trigger the isolation. After that, the Isolation Status is acquired and a message is sent out to the corresponding Slack user.



hameets-pc.phub.net.cable.rogers.

Sensor Details

Hostname
hameets-pc.phub.net.cable.rogers.com

Network Access
Isolated

Seal Status
Not Sealed

Last Time Alive
2025-01-20 19:34:45

External IP
99.240.179.192

Sensor ID
4cf0c9db-7620-44cd-87f4-2ca741c6d9d6

Installer ID
20cfba0d-496c-401f-94c5-e6a97a7a117f

Tags

Other Sensors on this Device

No other sensors on this device.

Delete Sensor

Deleting hameets-pc.phub.net.cable.rogers.com will only de its reference in the cloud and **WILL NOT** uninstall the senso from its host. If the sensor is still installed it will continue t send events, but the cloud will deny them access.

Hostname
hameets-pc.phub.net.cable.ro…

SID
4cf0c9db-7620-44cd-87f4-2ca7…

Platform
Windows x86 64 bit

Last Seen
2025-01-20 19:34:45

Ref 13: Once the user is prompted for a decision to isolate the machine or not, if yes is selected then the machine instantly gets isolated as indicated above. All network connectivity is disabled and the machine is isolated. Additionally, a message indicated the isolation status is sent to Slack.

CONCLUSION

This lab provided hands-on experience in EDR-SOAR integration, automated threat detection, and incident response workflows. By configuring LimaCharlie to detect credential-dumping attacks and automating remediation through Tines, I gained valuable insights into real-world SOC operations, security automation, and threat containment strategies. This project reinforced my skills in incident detection, alerting, and endpoint isolation, demonstrating the power of automation in modern cybersecurity defense.