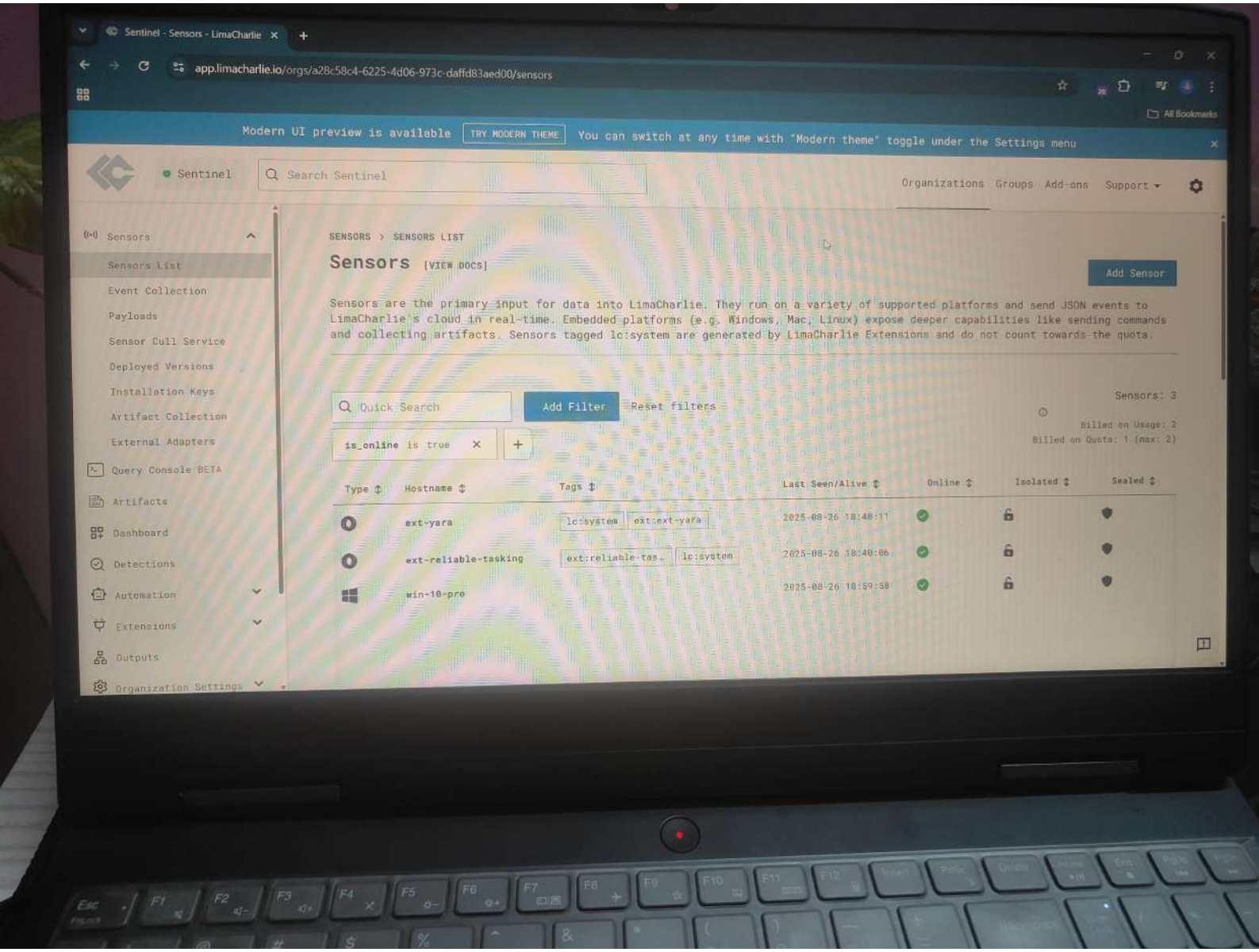
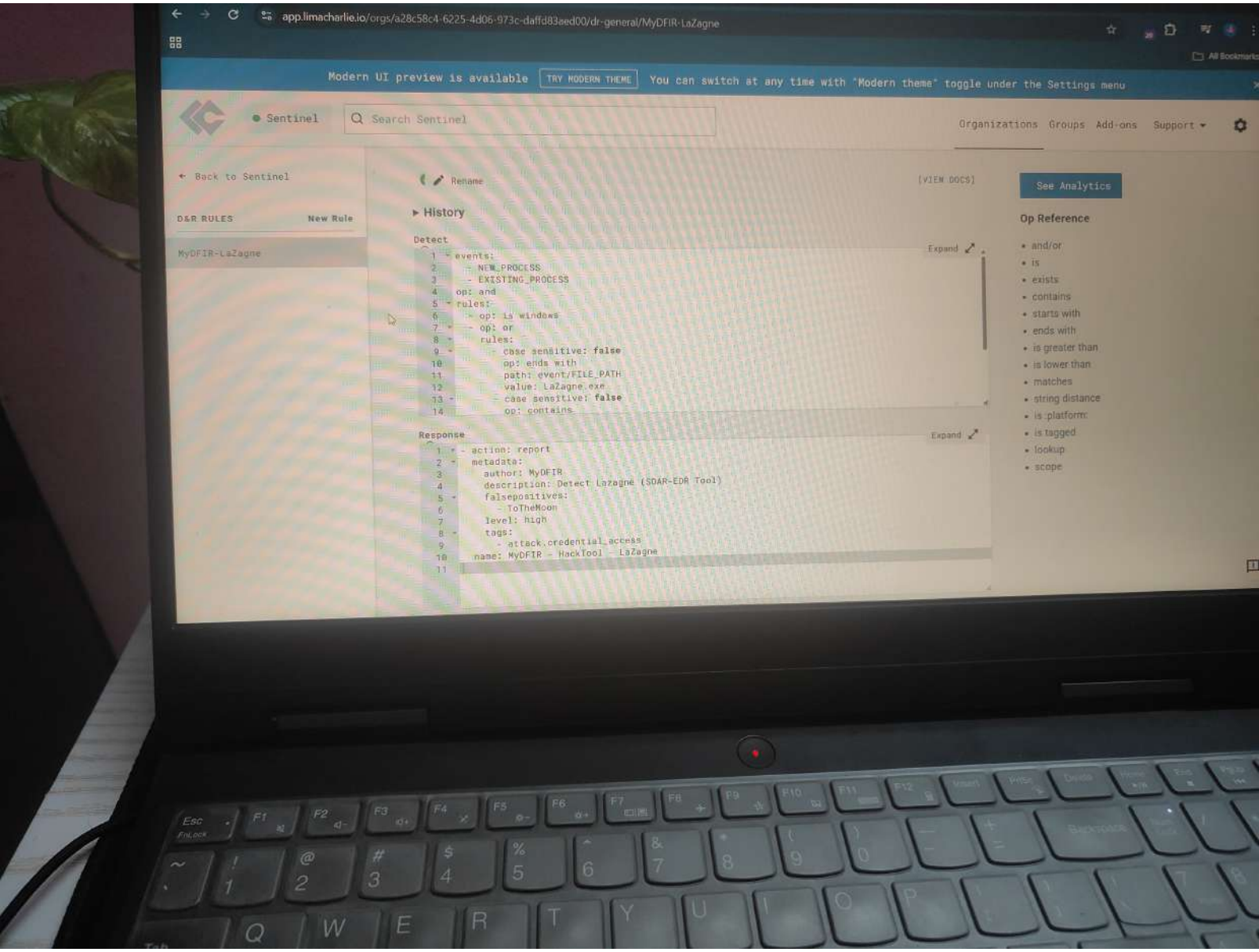
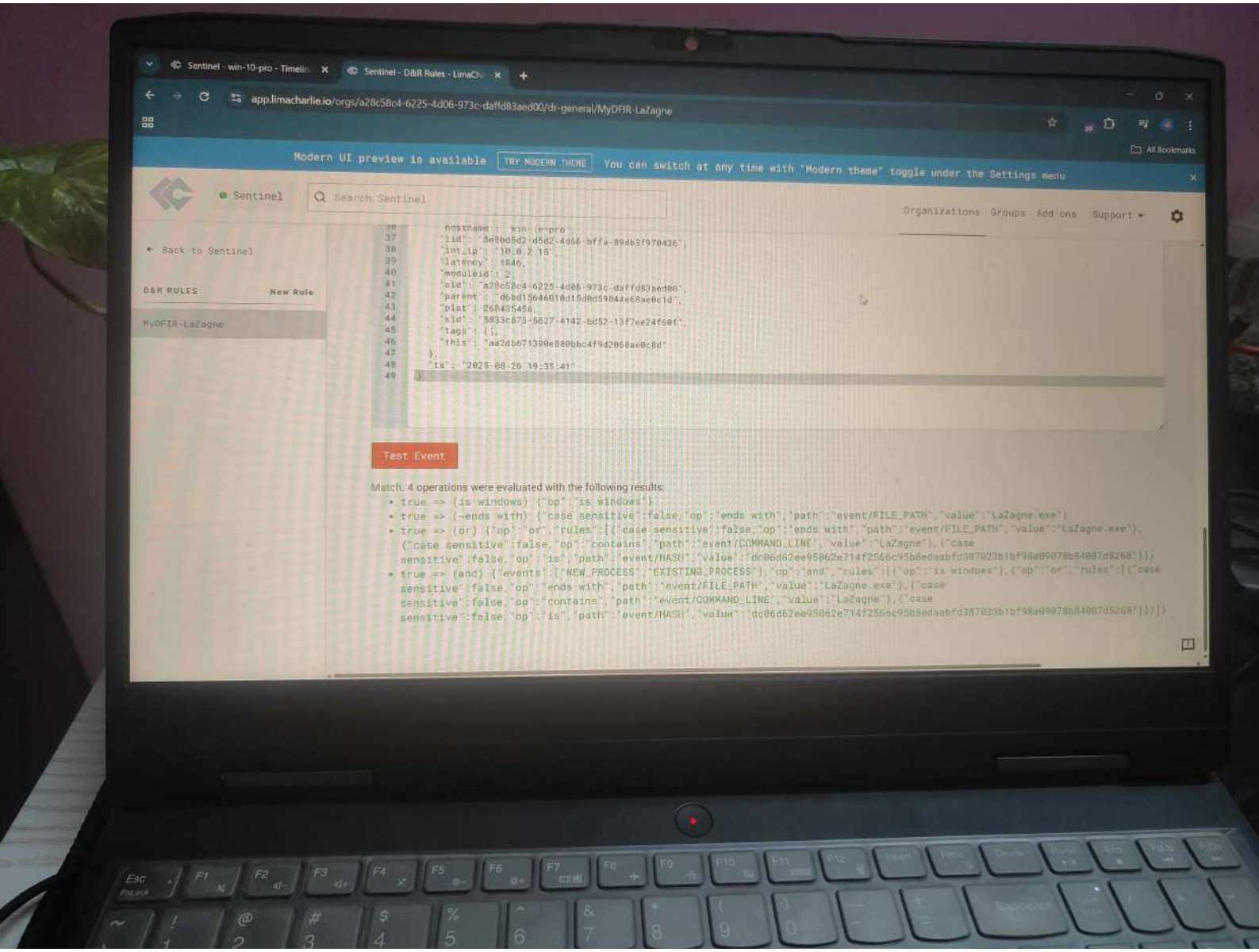
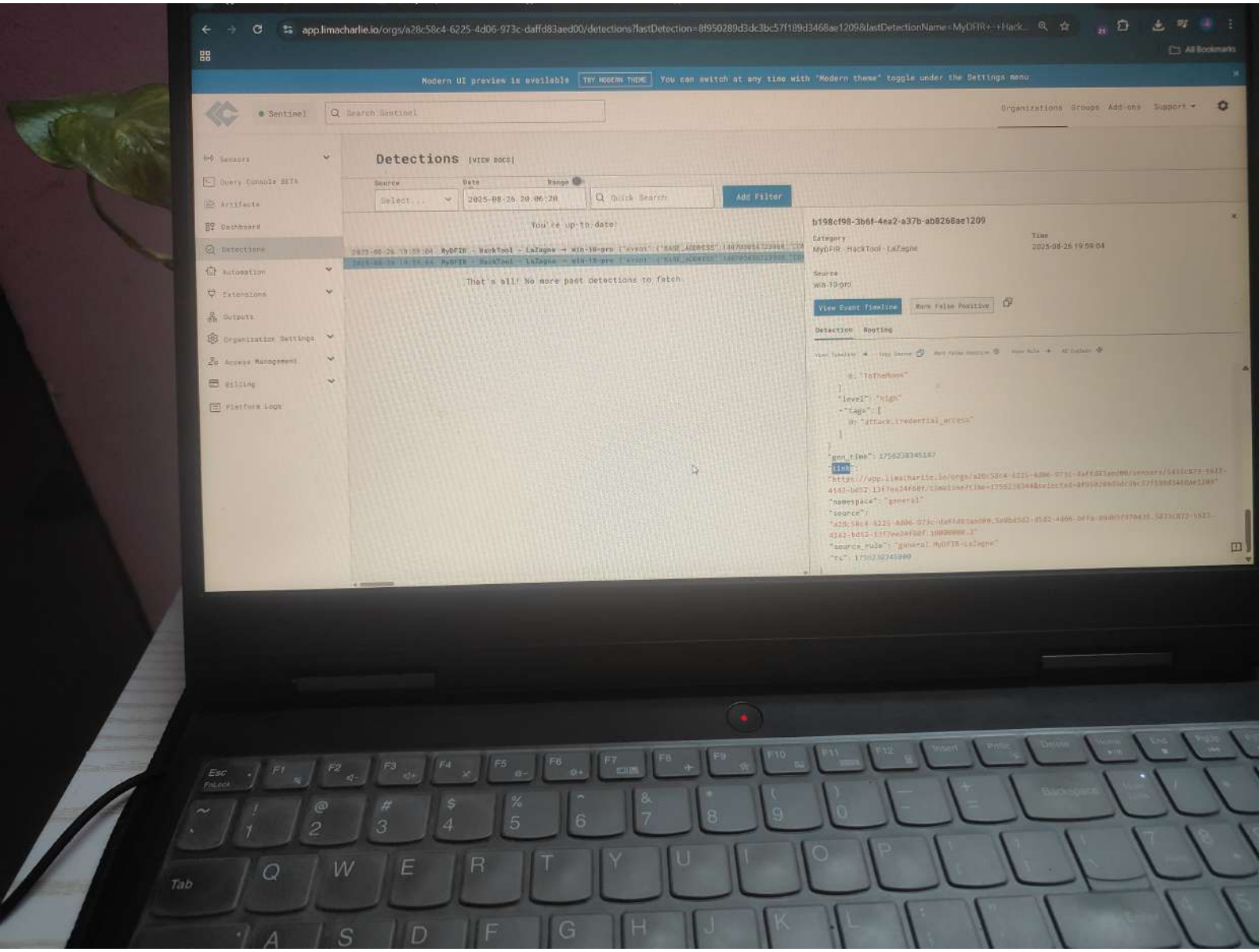
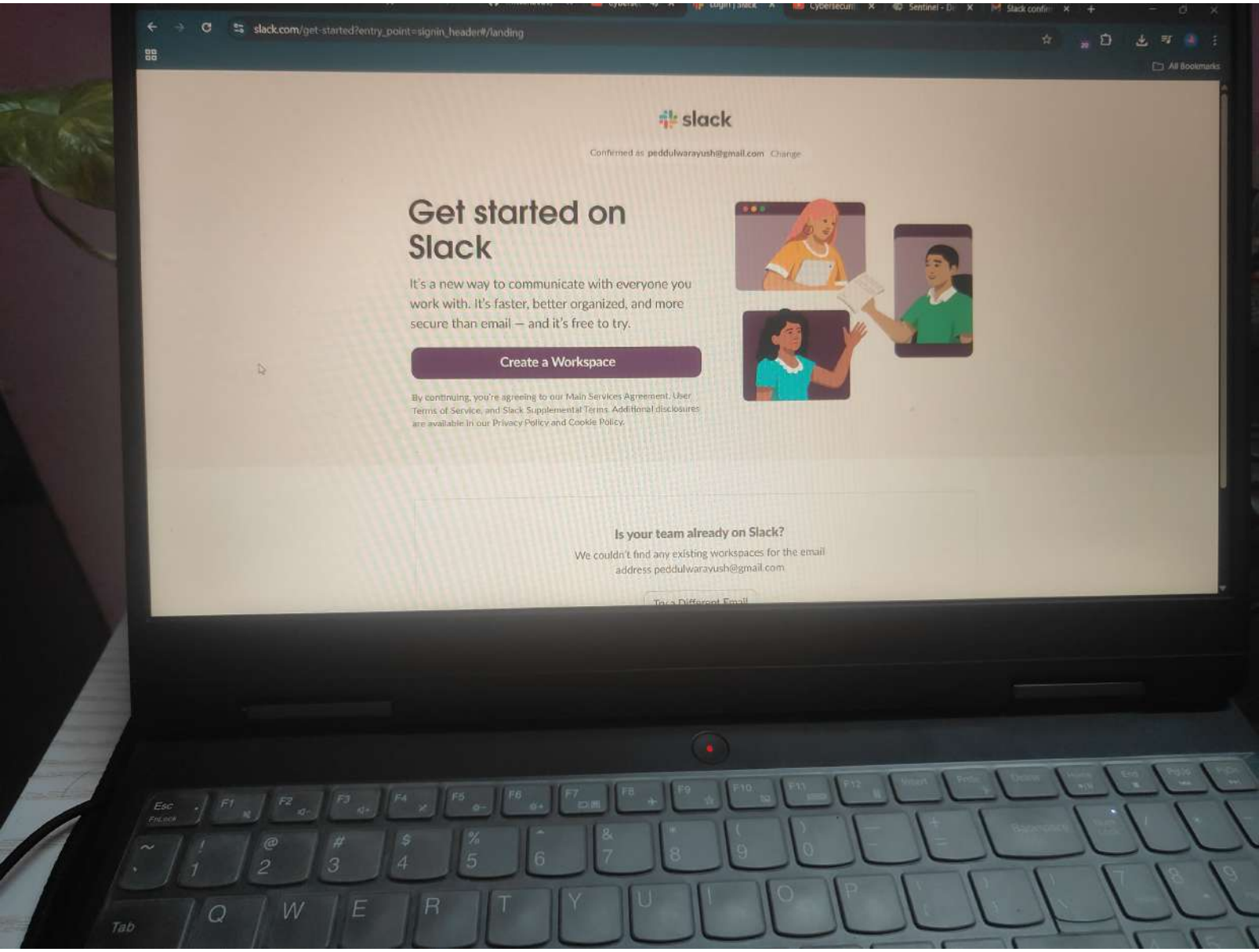
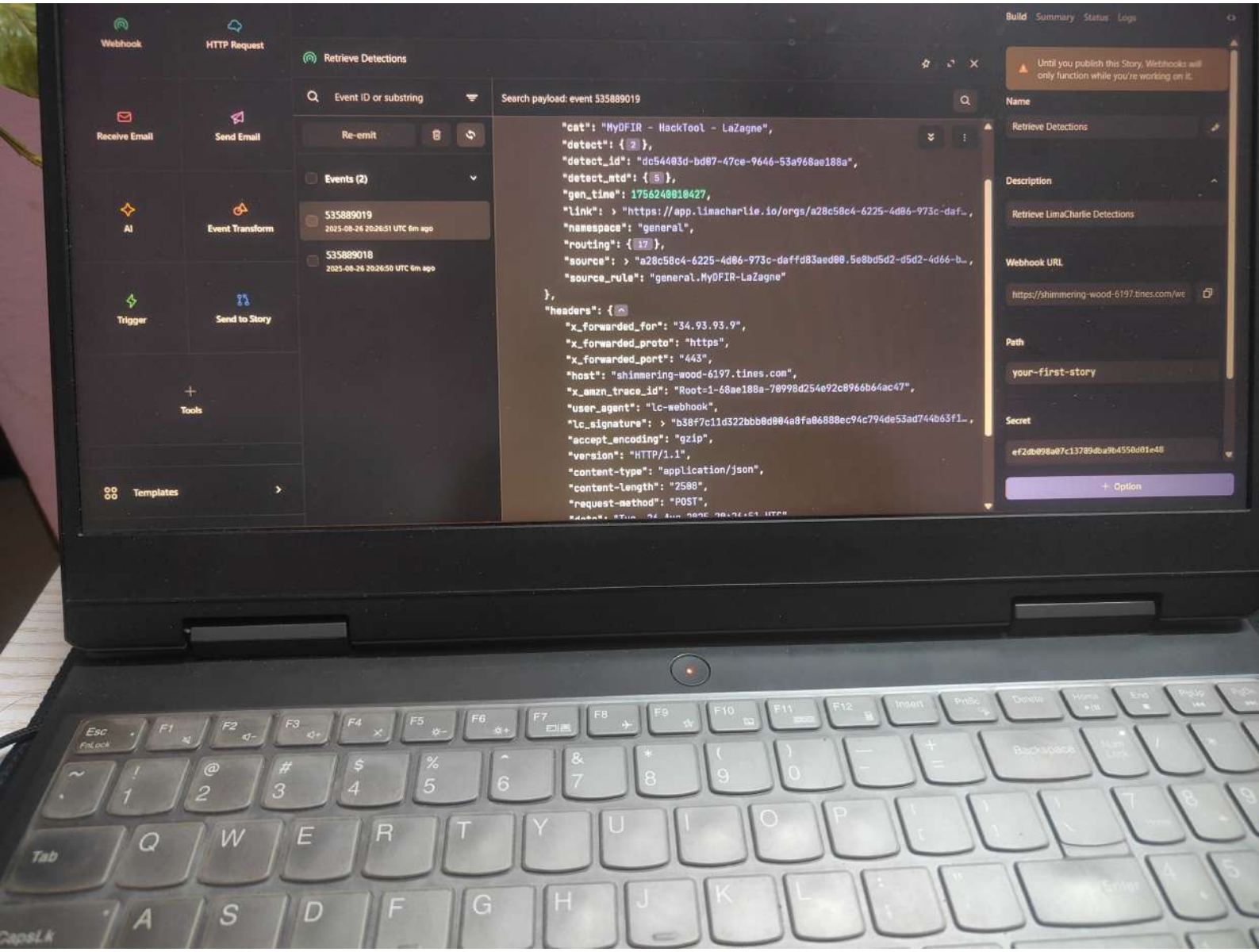

Sentinel - Sensors - LimaCharlie
app.limacharlie.io/orgs/a28c58c4-6225-4d06-973c-daffd83aed00/sensors
Modern UI preview is available
TRY MODERN THEME
You can switch at any time with "Modern theme" toggle under the Settings menu
Sentinel
Search Sentinel
Organizations
Groups
Add-ons
Support
Sensors
Sensors List
Event Collection
Payloads
Sensor Cull Service
Deployed Versions
Installation Keys
Artifact Collection
External Adapters
Query Console BETA
Artifacts
Dashboard
Detections
Automation
Extensions
Outputs
Organization Settings
SENSORS › SENSORS LIST
Sensors
[VIEW DOCS]
Add Sensor
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.
Quick Search
Add Filter
Reset filters
Sensors: 3
Billed on Usage: 2
Billed on Quota: 1 (max: 2)
is_online is true
Type
Hostname
Tags
Last Seen/Alive
Online
Isolated
Sealed
ext-yara
lc:system
ext:ext-yara
2025-08-26 18:48:11
ext-reliable-tasking
ext:reliable-tas.
lc:system
2025-08-26 18:40:06
win-10-pro
2025-08-26 18:59:58

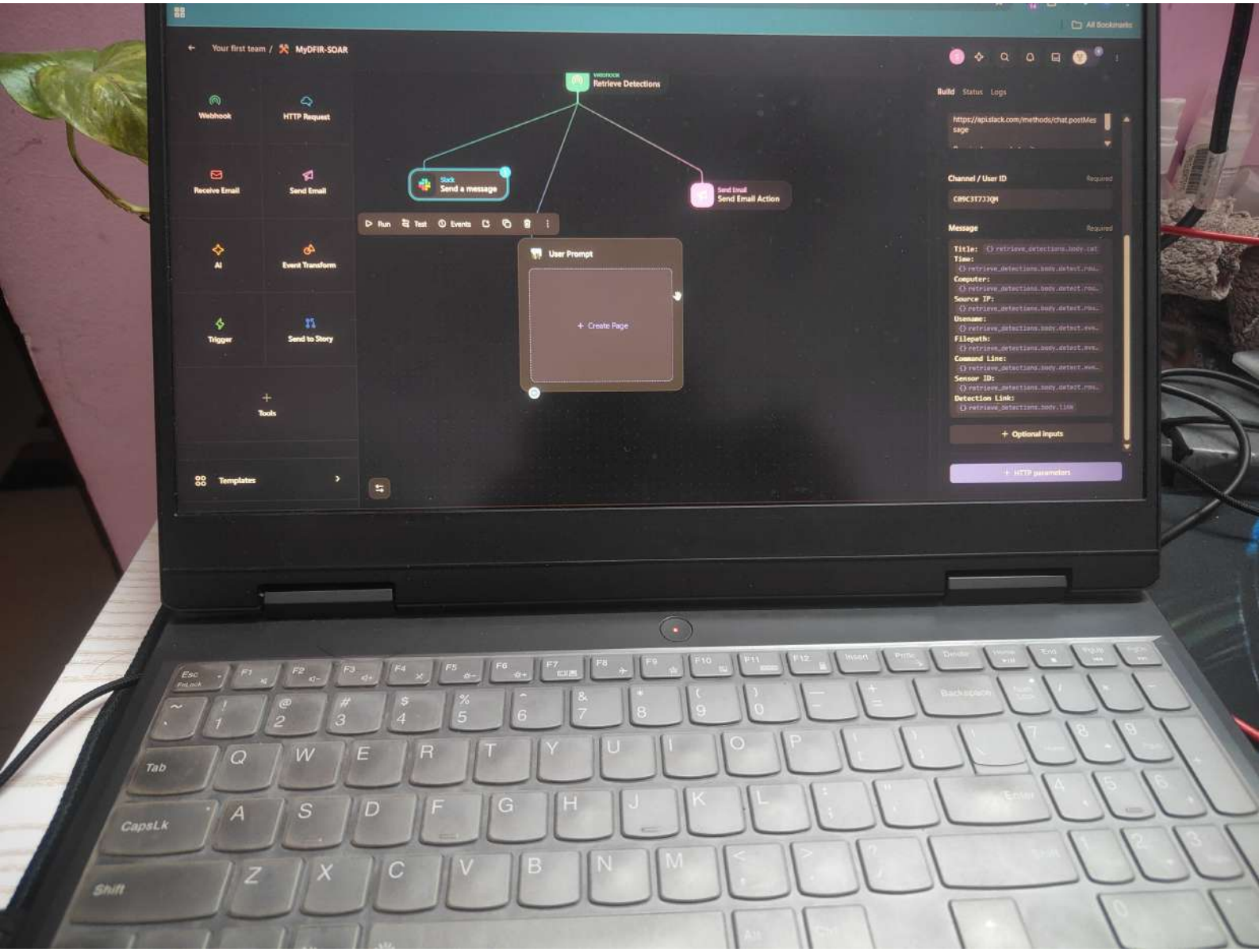

app.limacharlie.io/orgs/a28c58c4-6225-4d06-973c-daffd83aed00/dr-general/MyDFIR-LaZagne
Modern UI preview is available
TRY MODERN THEME
You can switch at any time with "Modern theme" toggle under the Settings menu
Sentinel
Search Sentinel
Organizations
Groups
Add-ons
Support
Back to Sentinel
D&R RULES
New Rule
MyDFIR-LaZagne
Rename
[VIEW DOCS]
See Analytics
History
Detect
Expand
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
Response
Expand
- action: report
metadata:
author: MyDFIR
description: Detect Lazagne (SOAR-EDR Tool)
falsepositives:
- ToTheMoon
level: high
tags:
- attack.credential_access
name: MyDFIR - HackTool - LaZagne
Op Reference
and/or
is
exists
contains
starts with
ends with
is greater than
is lower than
matches
string distance
is platform
is tagged
lookup
scope

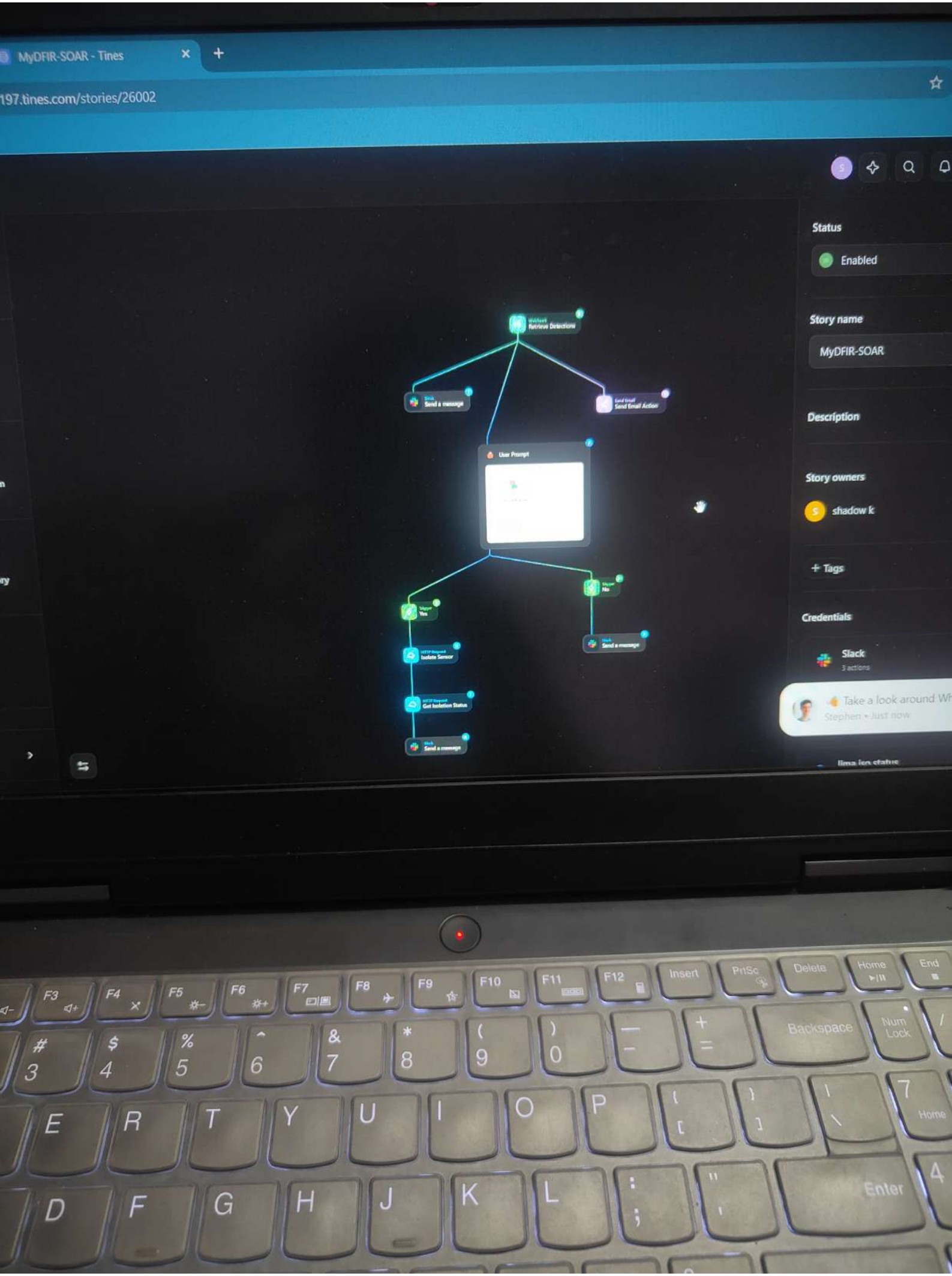

Sentinel - win-10-pro - Timelin
Sentinel - D&R Rules - LimaCh
app.limacharlie.io/orgs/a28c58c4-6225-4d06-973c-daffd83aed00/dr-general/MyDFIR-LaZagne
Modern UI preview is available
TRY MODERN THEME
You can switch at any time with "Modern theme" toggle under the Settings menu
Sentinel
Search Sentinel
Organizations
Groups
Add-ons
Support
Back to Sentinel
D&R RULES
New Rule
MyDFIR-LaZagne
"hostname" : "win-10-pro",
"iid" : "5e8bd5d2-d5d2-4d66-bffa-89db3f970436",
"int_ip" : "10.0.2.15",
"latency" : 1846,
"moduleid" : 2,
"oid" : "a28c58c4-6225-4d06-973c-daffd83aed00",
"parent" : "d6bd15646010d15d0d59844e68ae0c1d",
"plat" : 268435456,
"sid" : "5833c673-5627-4142-bd52-13f7ee24f60f",
"tags" : [],
"this" : "aa2db671390e880bbc4f9d2068ae0c8d"
},
"ts" : "2025-08-26 19:35:41"
}
Test Event
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":"dc06d62ee05062e714f2566c95b8edaabfd387023b1bf98a09078b84007d5268"}]}
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":"dc06d62ee05062e714f2566c95b8edaabfd387023b1bf98a09078b84007d5268"}]}]}


app.limacharlie.io/orgs/a28c58c4-6225-4d06-973c-daffd83aed00/detections?lastDetection=8f950289d3dc3bc57f189d3468ae1209&lastDetectionName=MyDFIR+-+Hack...
Modern UI preview is available
TRY MODERN THEME
You can switch at any time with "Modern theme" toggle under the Settings menu
Sentinel
Search Sentinel
Organizations
Groups
Add-ons
Support
Sensors
Query Console BETA
Artifacts
Dashboard
Detections
Automation
Extensions
Outputs
Organization Settings
Access Management
Billing
Platform Logs
Detections
[VIEW DOCS]
Source
Date
Range
Select...
2025-08-26 20:06:20
Quick Search
Add Filter
You're up-to-date!
That's all! No more past detections to fetch.
b198cf98-3b6f-4ea2-a37b-ab8268ae1209
Category
MyDFIR - HackTool - LaZagne
Time
2025-08-26 19:58:04
Source
win-10-pro
View Event Timeline
Mark False Positive
Detection
Routing


slack.com/get-started?entry_point=signin_header#/landing
slack
Confirmed as peddulwarayush@gmail.com Change
Get started on Slack
It's a new way to communicate with everyone you work with. It's faster, better organized, and more secure than email — and it's free to try.
Create a Workspace
By continuing, you're agreeing to our Main Services Agreement, User Terms of Service, and Slack Supplemental Terms. Additional disclosures are available in our Privacy Policy and Cookie Policy.
Is your team already on Slack?
We couldn't find any existing workspaces for the email address peddulwarayush@gmail.com


Webhook
HTTP Request
Receive Email
Send Email
AI
Event Transform
Trigger
Send to Story
Tools
Templates
Retrieve Detections
Event ID or substring
Re-emit
Events (2)
535889019
2025-08-26 20:26:51 UTC 6m ago
535889018
2025-08-26 20:26:50 UTC 6m ago
Search payload: event 535889019
"cat": "MyDFIR - HackTool - LaZagne",
"detect": { 2 },
"detect_id": "dc54403d-bd07-47ce-9646-53a968ae188a",
"detect_mtd": { 5 },
"gen_time": 1756240010427,
"link": "https://app.limacharlie.io/orgs/a28c58c4-6225-4d06-973c-daf…",
"namespace": "general",
"routing": { 17 },
"source": "a28c58c4-6225-4d06-973c-daffd83aed08.5e8bd5d2-d5d2-4d66-b…",
"source_rule": "general.MyDFIR-LaZagne"
},
"headers": {
"x_forwarded_for": "34.93.93.9",
"x_forwarded_proto": "https",
"x_forwarded_port": "443",
"host": "shimmering-wood-6197.tines.com",
"x_amzn_trace_id": "Root=1-68ae188a-70998d254e92c8966b64ac47",
"user_agent": "lc-webhook",
"lc_signature": "b38f7c11d322bbb0d004a8fa06888ec94c794de53ad744b63f1…",
"accept_encoding": "gzip",
"version": "HTTP/1.1",
"content-type": "application/json",
"content-length": "2588",
"request-method": "POST",
Build
Summary
Status
Logs
Until you publish this Story, Webhooks will only function while you're working on it.
Name
Retrieve Detections
Description
Retrieve LimaCharlie Detections
Webhook URL
https://shimmering-wood-6197.tines.com/we
Path
your-first-story
Secret
ef2db098a07c13789dba9b4550d01e48
+ Option


Your first team / MyDFIR-SOAR
Webhook
HTTP Request
Receive Email
Send Email
AI
Event Transform
Trigger
Send to Story
Tools
Templates
Retrieve Detections
Send a message
Send Email Action
Run
Test
Events
User Prompt
+ Create Page
Build
Status
Logs
https://api.slack.com/methods/chat.postMessage
Channel / User ID
Required
Message
Title:
Time:
Computer:
Source IP:
Username:
Filepath:
Command Line:
Sensor ID:
Detection Link:
+ Optional inputs
+ HTTP parameters


MyDFIR-SOAR - Tines
197.tines.com/stories/26002
Status
Enabled
Story name
MyDFIR-SOAR
Description
Story owners
shadow k
+ Tags
Credentials
Slack
3 actions
Retrieve Detections
Send a message
Send Email Action
User Prompt
Yes
No
Isolate Sensor
Get Isolation Status
Send a message
Send a message
Stephen • Just now