Environment Simulation Report

Objective

The purpose of this simulation is to validate the SOCaaS design by showing how logs flow from different sources (endpoints, domain controller, IDS) into the Wazuh SIEM, and how alerts are generated, correlated, and forwarded to SOAR.

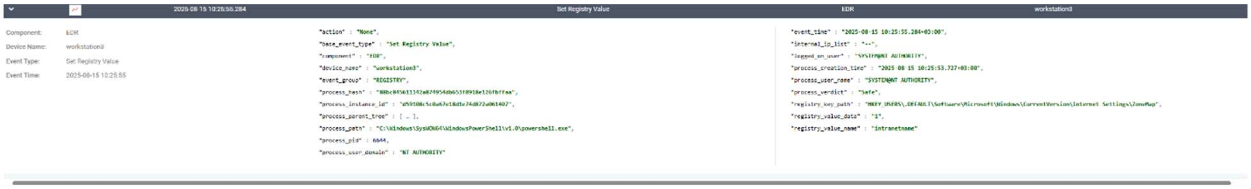
Environment Overview

- Endpoints (5 Windows Workstations): Each workstation is configured with Sysmon, OpenEDR, and the Wazuh Agent. Logs generated by these tools are forwarded to the Wazuh Manager.
- Domain Controller (Windows Server): Collects Windows Security Events, Sysmon telemetry, and OpenEDR logs via the Wazuh Agent.
- Suricata IDS (VPN Sensor): Monitors VPN and LAN traffic on Tailscale. Suricata outputs JSON logs (which are collected by a Wazuh Agent.
- Wazuh Manager (SIEM): Collects logs from all agents, normalizes data, applies detection rules, and raises alerts.
- Shuffle SOAR: Receives alerts from Wazuh via Webhook.

Log Flow

Endpoint Activity

- Sysmon generates detailed process, registry, and network connection events.
- OpenEDR generates malware detections, blocked process execution logs, and prevention alerts. (Figures 1.1,1.2)
- Wazuh Agent forwards logs to the Wazuh Manager.



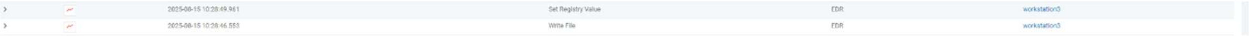
```
2025-08-15 10:25:55.284        Set Registry Value        EDR        workstation3

Component:      EDR
Device Name:    workstation3
Event Type:     Set Registry Value
Event Time:     2025-08-15 10:25:55

"action" : "None",
"base_event_type" : "Set Registry Value",
"component" : "EDR",
"device_name" : "workstation3",
"event_group" : "REGISTRY",
"process_hash" : "88bc845611142a874954db653f8918e126fbffaa",
"process_instance_id" : "d59108c5c0a67e18d1e74d872a061407",
"process_parent_tree" : [ … ],
"process_path" : "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe",
"process_pid" : 6644,
"process_user_domain" : "NT AUTHORITY"

"event_time" : "2025-08-15 10:25:55.284+03:00",
"internal_ip_list" : "--",
"logged_on_user" : "SYSTEM@NT AUTHORITY",
"process_creation_time" : "2025-08-15 10:25:53.727+03:00",
"process_user_name" : "SYSTEM@NT AUTHORITY",
"process_verdict" : "Safe",
"registry_key_path" : "HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap",
"registry_value_data" : "1",
"registry_value_name" : "intranetname"
```

Figure 1.1: OpenEDR Log Details

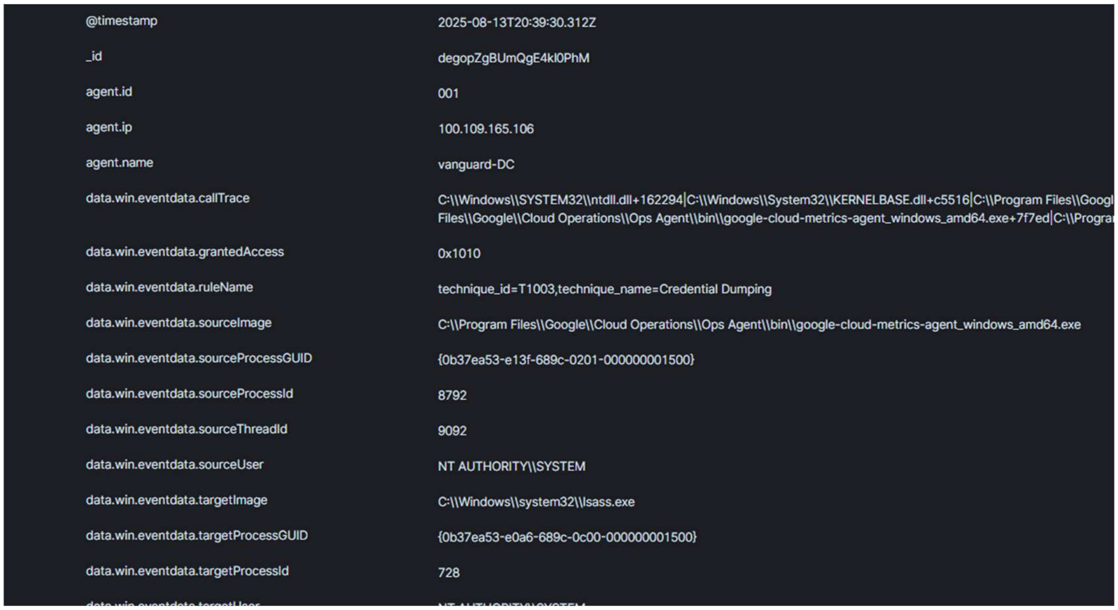


```
>    2025-08-15 10:28:49.961    Set Registry Value    EDR    workstation3
>    2025-08-15 10:28:46.553    Write File            EDR    workstation3
```

Figure 1.2: OpenEDR Logs

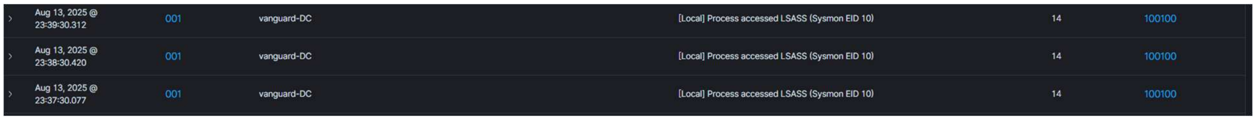
Domain Controller Activity

- Windows Security Events (e.g., logons, account changes, GPO modifications) are captured.
- Sysmon adds process monitoring. (Figures 2.1,2.2)
- Wazuh Agent sends these logs to Wazuh Manager.



```
@timestamp                              2025-08-13T20:39:30.312Z
_id                                     degopZgBUmQgE4kl0PhM
agent.id                                001
agent.ip                                100.109.165.106
agent.name                              vanguard-DC
data.win.eventdata.callTrace            C:\\Windows\\SYSTEM32\\ntdll.dll+162294|C:\\Windows\\System32\\KERNELBASE.dll+c5516|C:\\Program Files\\Googl
                                        Files\\Google\\Cloud Operations\\Ops Agent\\bin\\google-cloud-metrics-agent_windows_amd64.exe+7f7ed|C:\\Progra
data.win.eventdata.grantedAccess        0x1010
data.win.eventdata.ruleName             technique_id=T1003,technique_name=Credential Dumping
data.win.eventdata.sourceImage          C:\\Program Files\\Google\\Cloud Operations\\Ops Agent\\bin\\google-cloud-metrics-agent_windows_amd64.exe
data.win.eventdata.sourceProcessGUID    {0b37ea53-e13f-689c-0201-000000001500}
data.win.eventdata.sourceProcessId      8792
data.win.eventdata.sourceThreadId       9092
data.win.eventdata.sourceUser           NT AUTHORITY\\SYSTEM
data.win.eventdata.targetImage          C:\\Windows\\system32\\lsass.exe
data.win.eventdata.targetProcessGUID    {0b37ea53-e0a6-689c-0c00-000000001500}
data.win.eventdata.targetProcessId      728
data.win.eventdata.targetUser           NT AUTHORITY\\SYSTEM
```

Figure 2.1: Sysmon Log Detail

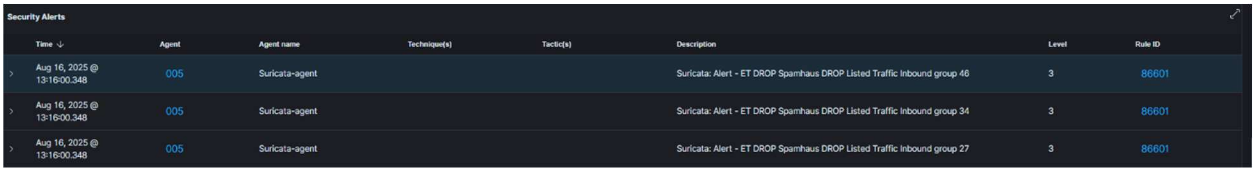


Aug 13, 2025 @ 23:39:30.312	001	vanguard-DC	[Local] Process accessed LSASS (Sysmon EID 10)	14	100100
Aug 13, 2025 @ 23:38:30.420	001	vanguard-DC	[Local] Process accessed LSASS (Sysmon EID 10)	14	100100
Aug 13, 2025 @ 23:37:30.077	001	vanguard-DC	[Local] Process accessed LSASS (Sysmon EID 10)	14	100100

Figure 2.2: Sysmon Logs

Suricata IDS Activity

- Suricata inspects network traffic and generates alerts (Exploit attempts, C2 traffic).
- Wazuh Agent installed on the Suricata VM forwards these JSON logs into Wazuh Manager. (Figure 3)



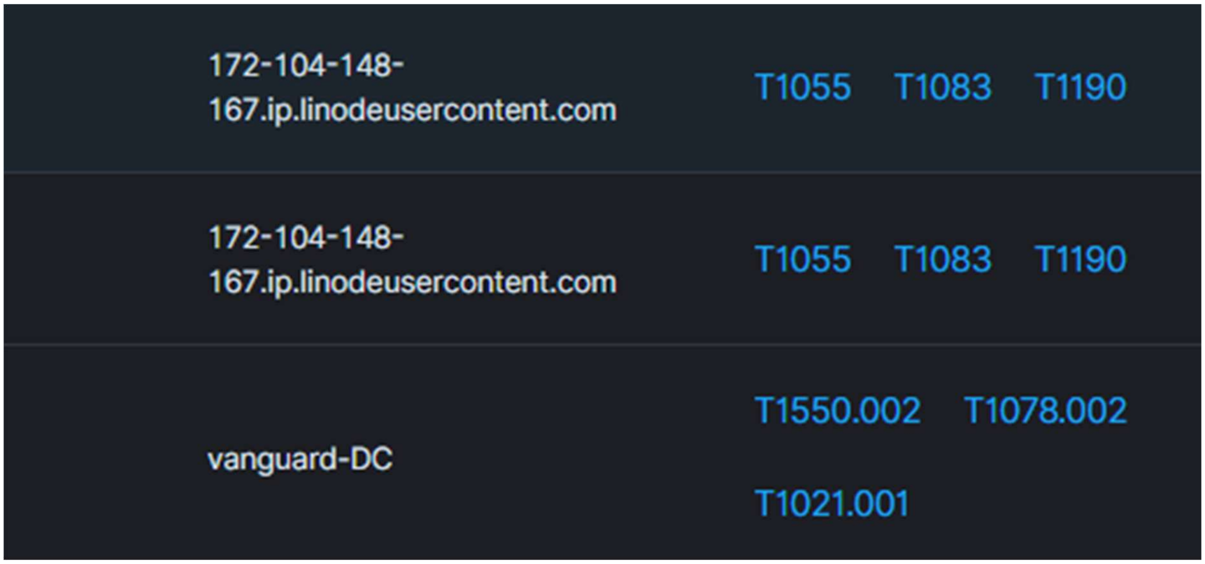
Security Alerts

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 16, 2025 @ 13:16:00.348	005	Suricata-agent			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 46	3	86601
Aug 16, 2025 @ 13:16:00.348	005	Suricata-agent			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 34	3	86601
Aug 16, 2025 @ 13:16:00.348	005	Suricata-agent			Suricata: Alert - ET DROP Spamhaus DROP Listed Traffic Inbound group 27	3	86601

Figure 3: Suricata Alerts

Wazuh Manager Processing

- Aggregates all logs from endpoints, DC, and Suricata.
- Normalizes events, correlates against rules, and maps to MITRE ATT&CK techniques. (Figure 4)
- Generates alerts when detection logic is matched.

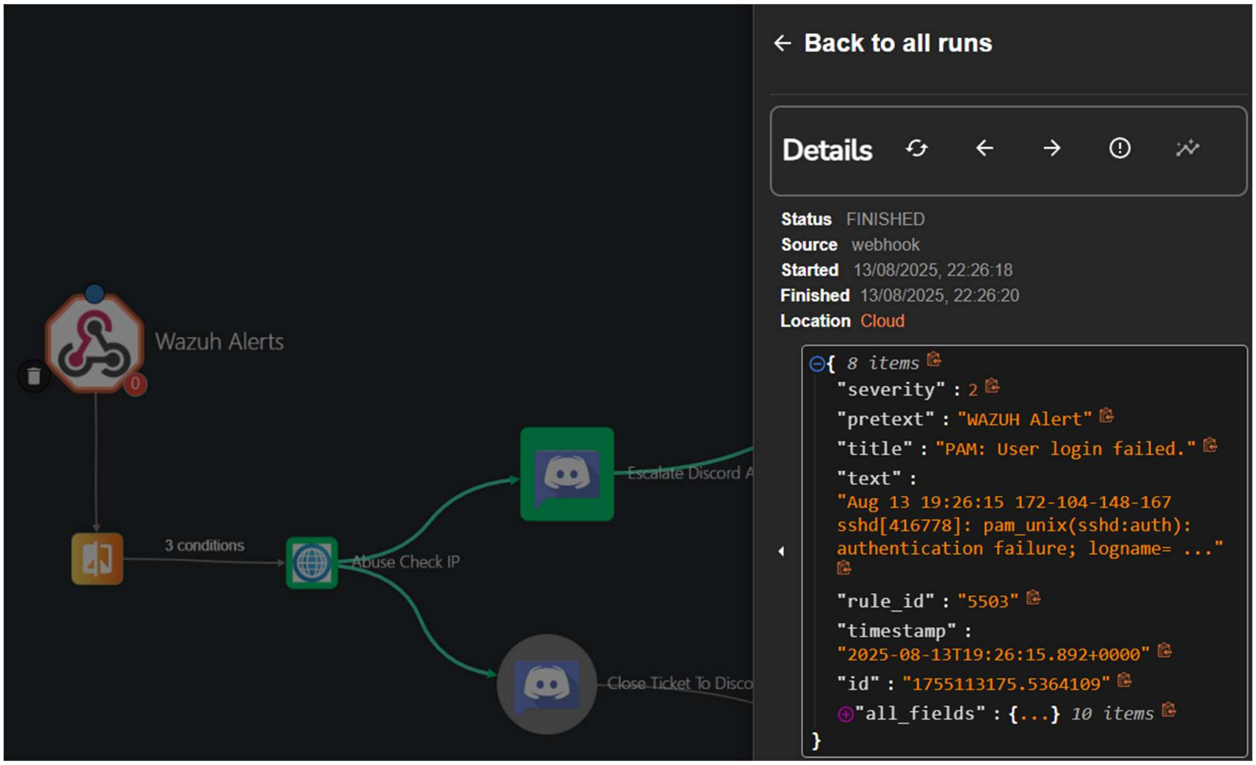


172-104-148-167.ip.linodeusercontent.com	T1055 T1083 T1190
172-104-148-167.ip.linodeusercontent.com	T1055 T1083 T1190
vanguard-DC	T1550.002 T1078.002 T1021.001

Figure 4: MITRE Mapping

SOAR Integration

- Wazuh Manager forwards alerts to Shuffle SOAR using Webhooks. (Figure 5)
- Shuffle triggers playbooks for automated enrichment (VirusTotal, AbuseIPDB) and escalation actions (Discord Notification (Figure 6:)



Status FINISHED
Source webhook
Started 13/08/2025, 22:26:18
Finished 13/08/2025, 22:26:20
Location Cloud

```
{ 8 items
  "severity" : 2
  "pretext" : "WAZUH Alert"
  "title" : "PAM: User login failed."
  "text" :
  "Aug 13 19:26:15 172-104-148-167
  sshd[416778]: pam_unix(sshd:auth):
  authentication failure; logname= ..."
  "rule_id" : "5503"
  "timestamp" :
  "2025-08-13T19:26:15.892+0000"
  "id" : "1755113175.5364109"
  "all_fields" : {...} 10 items
}
```

Figure 5: Wazuh Alert in Shuffle

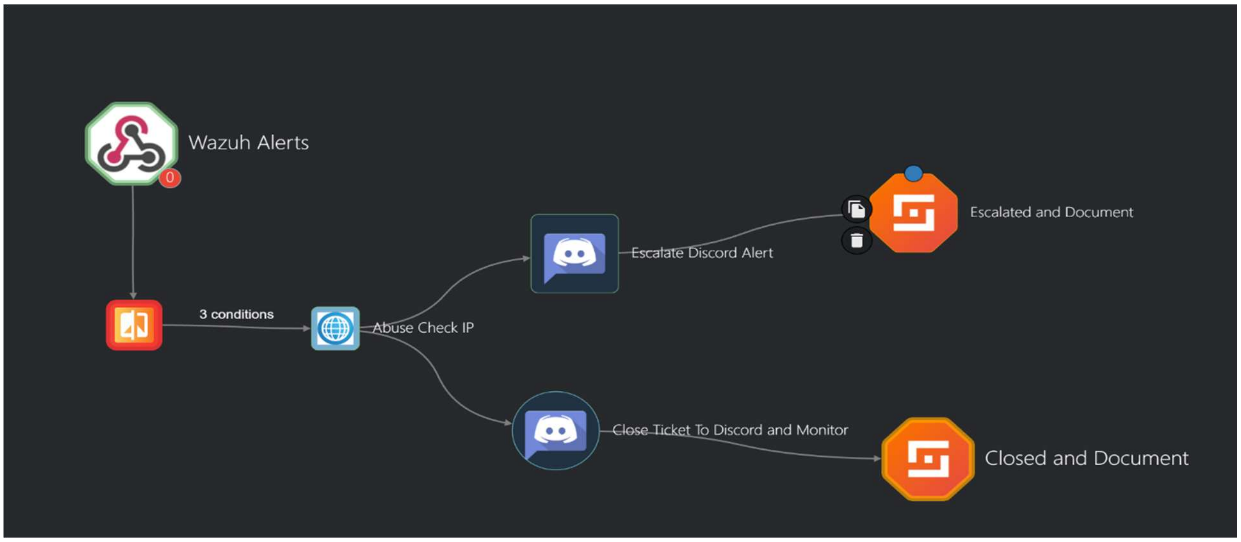
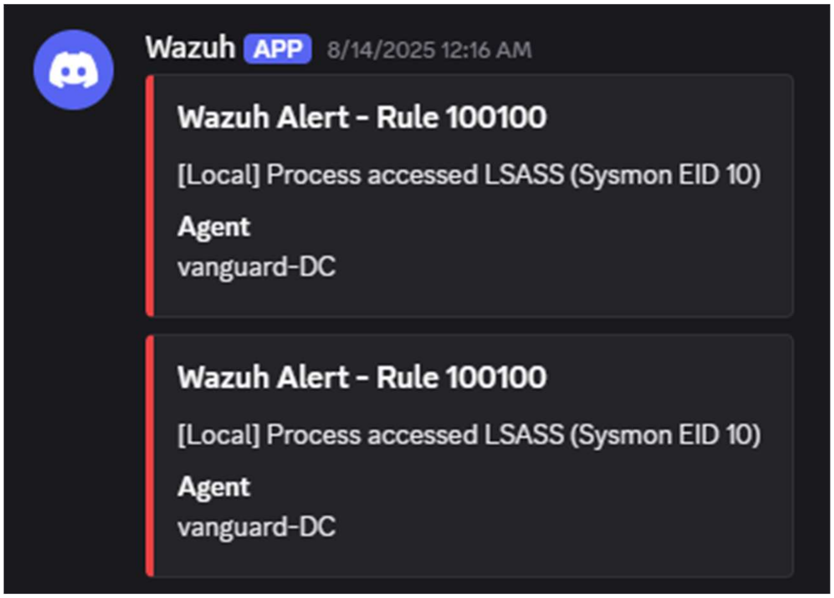


Figure 6: Playbook Example in Shuffle

Note: Since I failed in Shuffle playbook executions, I made wazuh send the notifications to discord based on rule severity. (Figure 7)



Wazuh APP 8/14/2025 12:16 AM

Wazuh Alert - Rule 100100

[Local] Process accessed LSASS (Sysmon EID 10)

Agent
vanguard-DC

Wazuh Alert - Rule 100100

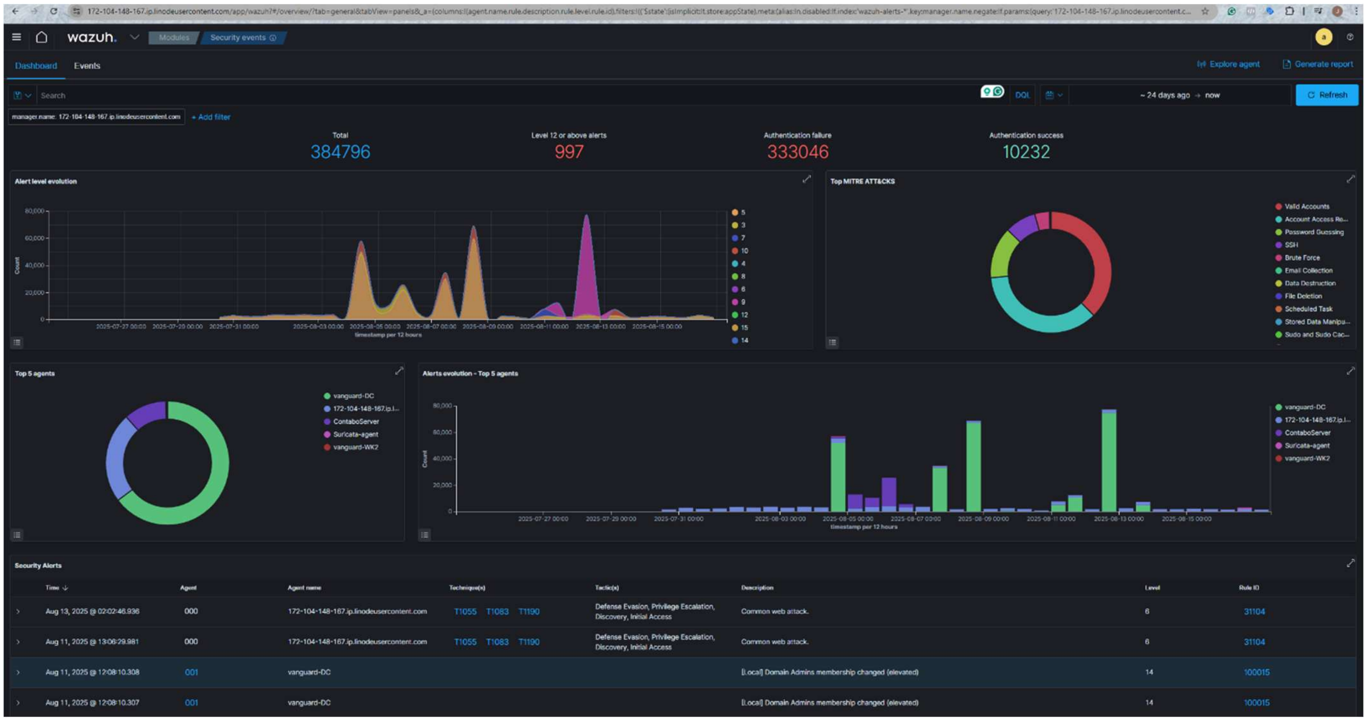
[Local] Process accessed LSASS (Sysmon EID 10)

Agent
vanguard-DC

Figure 7: Discord Alert from Wazuh

Alert Visibility

- Wazuh Dashboard: Provides real-time visibility into alerts, searchable by rule ID, event ID, or agent. (Figure 8)



manager.name: 172-104-148-167.ip.linodeusercontent.com

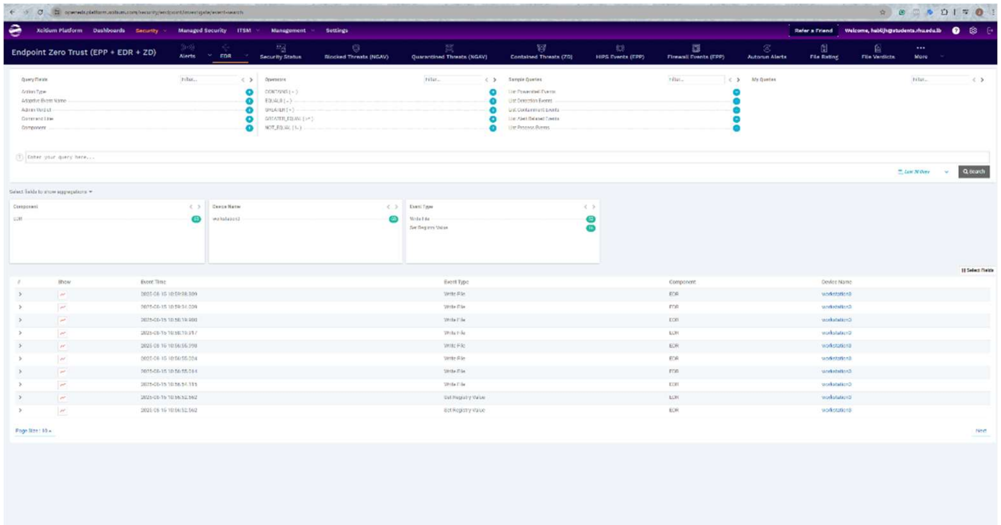
Total	Level 12 or above alerts	Authentication failure	Authentication success
384796	997	333046	10232

Security Alerts

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 13, 2025 @ 02:02:46.936	000	172-104-148-167.ip.linodeusercontent.com	T1055 T1083 T1190	Defense Evasion, Privilege Escalation, Discovery, Initial Access	Common web attack.	6	31104
Aug 11, 2025 @ 13:06:29.981	000	172-104-148-167.ip.linodeusercontent.com	T1055 T1083 T1190	Defense Evasion, Privilege Escalation, Discovery, Initial Access	Common web attack.	6	31104
Aug 11, 2025 @ 12:08:10.308	001	vanguard-DC			[Local] Domain Admins membership changed (elevated)	14	100015
Aug 11, 2025 @ 12:08:10.307	001	vanguard-DC			[Local] Domain Admins membership changed (elevated)	14	100015

Figure 8: Wazuh Dashboard

- OpenEDR Dashboard: Shows malware prevention events, quarantines, and telemetry from endpoints. (Figure 9)



#	Show	Event Time	Event Type	Component	Device Name
>		2025-08-15 10:59:38.309	Write File	EDR	workstation3
>		2025-08-15 10:59:34.009	Write File	EDR	workstation3
>		2025-08-15 10:58:19.900	Write File	EDR	workstation3
>		2025-08-15 10:58:19.917	Write File	EDR	workstation3
>		2025-08-15 10:56:56.398	Write File	EDR	workstation3
>		2025-08-15 10:56:55.004	Write File	EDR	workstation3
>		2025-08-15 10:56:55.014	Write File	EDR	workstation3
>		2025-08-15 10:56:54.115	Write File	EDR	workstation3
>		2025-08-15 10:56:52.562	Set Registry Value	EDR	workstation3
>		2025-08-15 10:56:52.562	Set Registry Value	EDR	workstation3

Figure 9: OpenEDR Dashboard

- Shuffle SOAR: Displays incoming alerts from Wazuh and playbooks (Figure 10)

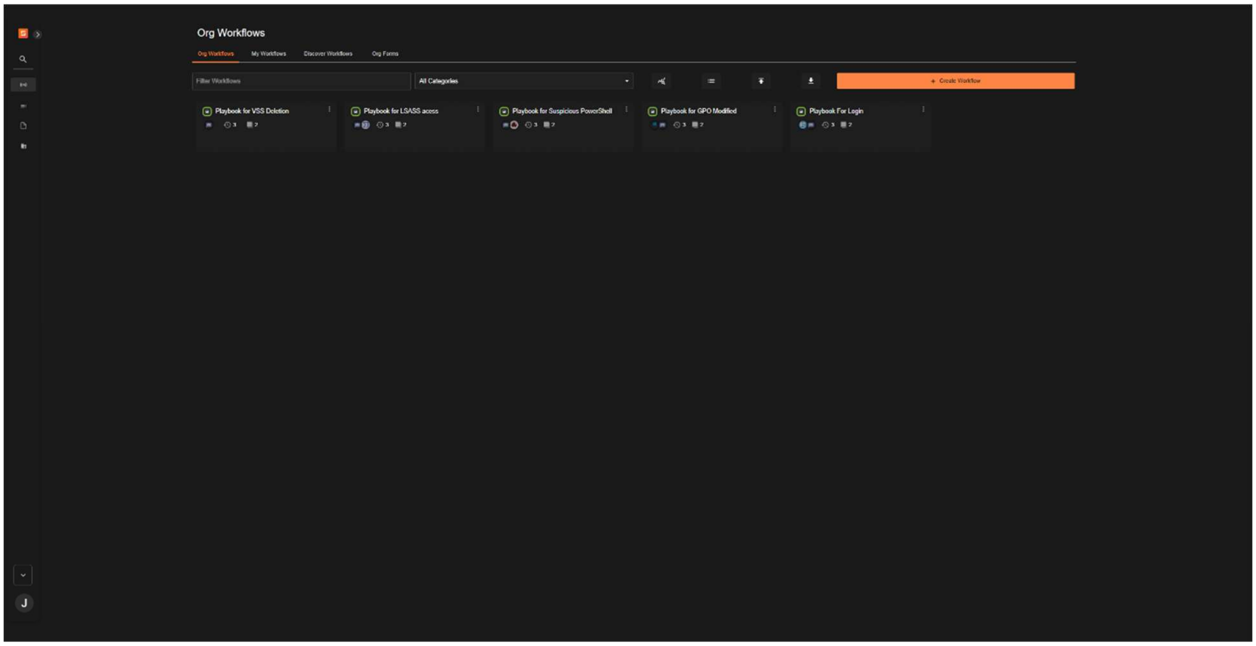


Figure 10: Shuffle Dashboard for Playbooks

Conclusion

This environment simulation demonstrates that logs from endpoints, the domain controller, and IDS flow correctly into Wazuh. Wazuh successfully generates alerts, which are then forwarded to Shuffle SOAR. This validates the SOCaaS design and provides confidence in the monitoring and response capabilities. Unfortunately, Shuffle SOAR playbooks weren't correctly setup to allow automated incident response and execution.