IT INFRASTRUCTURE SECURITY ORCHESTRATION

Guide : Prof. Vishal Badgujar

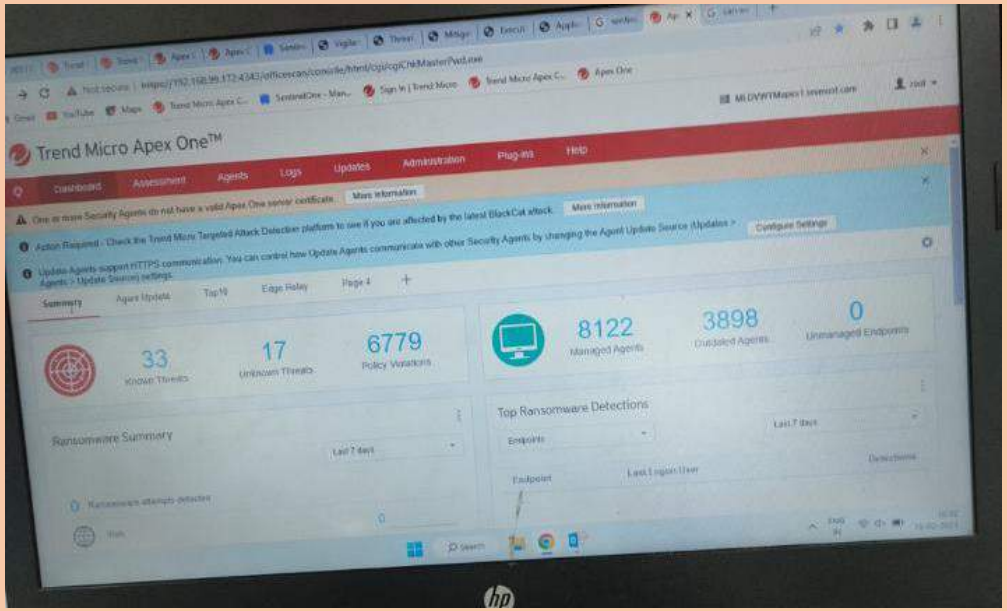
Name : Ankit Makwana

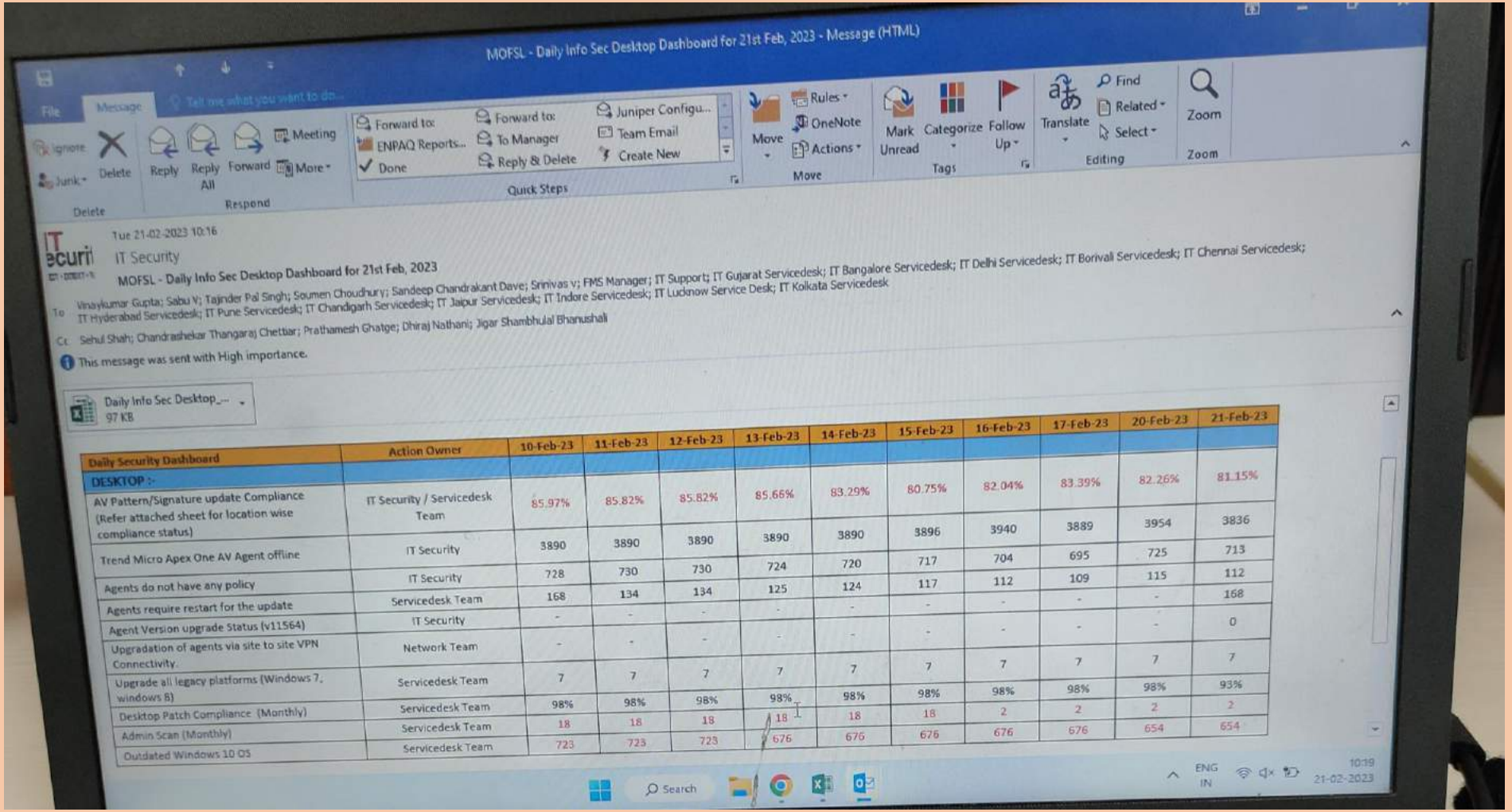
Roll No : 03

Branch : MSc Cyber Security

Monitoring in Trend Micro Apex One

- Trend Micro apex one is used for end point detections and monitor them and accordingly a report is generated on regular basis.





MOFSL - Daily Info Sec Desktop Dashboard for 21st Feb, 2023 - Message (HTML)

File | Message | Tell me what you want to do...

Ignore | Junk | Delete | Reply | Reply All | Forward | Meeting | More | Delete | Respond

Forward to: ENPAQ Reports... | Forward to: To Manager | Reply & Delete | Juniper Configu... | Team Email | Create New | Done | Quick Steps

Move | Rules | OneNote | Actions | Move

Mark Unread | Categorize | Follow Up | Tags

Translate | Find | Related | Select | Editing

Zoom | Zoom

Tue 21-02-2023 10:16

IT Security

MOFSL - Daily Info Sec Desktop Dashboard for 21st Feb, 2023

To: Vinaykumar Gupta; Sabu V; Tajinder Pal Singh; Soumen Choudhury; Sandeep Chandrakant Dave; Srinivas v; FMS Manager; IT Support; IT Gujarat Servicedesk; IT Bangalore Servicedesk; IT Delhi Servicedesk; IT Borivali Servicedesk; IT Chennai Servicedesk; IT Hyderabad Servicedesk; IT Pune Servicedesk; IT Chandigarh Servicedesk; IT Jaipur Servicedesk; IT Indore Servicedesk; IT Lucknow Service Desk; IT Kolkata Servicedesk

Cc: Sehul Shah; Chandrashekar Thangaraj Chettiar; Prathamesh Ghatge; Dhiraj Nathani; Jigar Shambhulal Bhanushali

This message was sent with High importance.

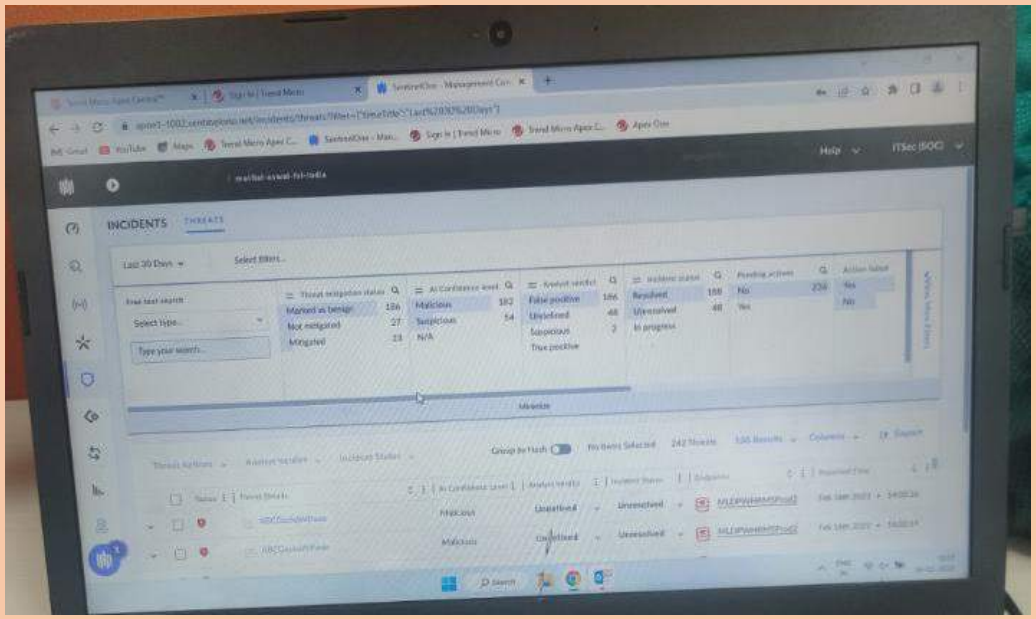
Daily Info Sec Desktop_... 97 KB

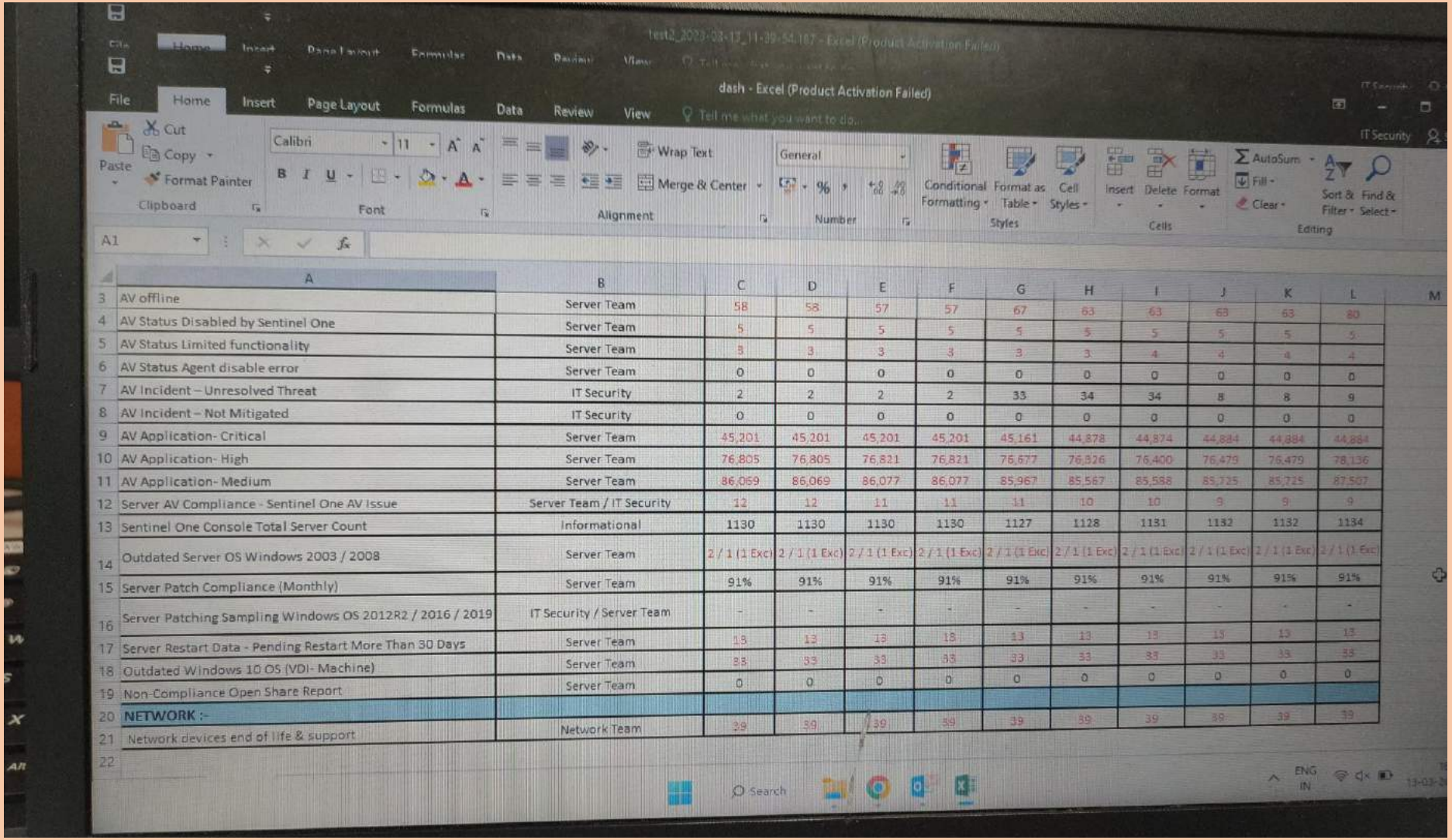
Daily Security Dashboard	Action Owner	10-Feb-23	11-Feb-23	12-Feb-23	13-Feb-23	14-Feb-23	15-Feb-23	16-Feb-23	17-Feb-23	20-Feb-23	21-Feb-23
DESKTOP :-											
AV Pattern/Signature update Compliance (Refer attached sheet for location wise compliance status)	IT Security / Servicedesk Team	85.97%	85.82%	85.82%	85.66%	83.29%	80.75%	82.04%	83.39%	82.26%	81.15%
Trend Micro Apex One AV Agent offline	IT Security	3890	3890	3890	3890	3890	3896	3940	3889	3954	3836
Agents do not have any policy	IT Security	728	730	730	724	720	717	704	695	725	713
Agents require restart for the update	Servicedesk Team	168	134	134	125	124	117	112	109	115	112
Agent Version upgrade Status (v11564)	IT Security	-	-	-	-	-	-	-	-	-	168
Upgradation of agents via site to site VPN Connectivity.	Network Team	-	-	-	-	-	-	-	-	-	0
Upgrade all legacy platforms (Windows 7, windows 8)	Servicedesk Team	7	7	7	7	7	7	7	7	7	7
Desktop Patch Compliance (Monthly)	Servicedesk Team	98%	98%	98%	98%	98%	98%	98%	98%	98%	93%
Admin Scan (Monthly)	Servicedesk Team	18	18	18	18	18	18	2	2	2	2
Outdated Windows 10 OS	Servicedesk Team	723	723	723	676	676	676	676	676	654	654

Search | ENG IN | 10:19 21-02-2023

Monitoring in Sentinel One

- Sentinel One is used for Servers and monitor them and accordingly a report is generated on regular basis.



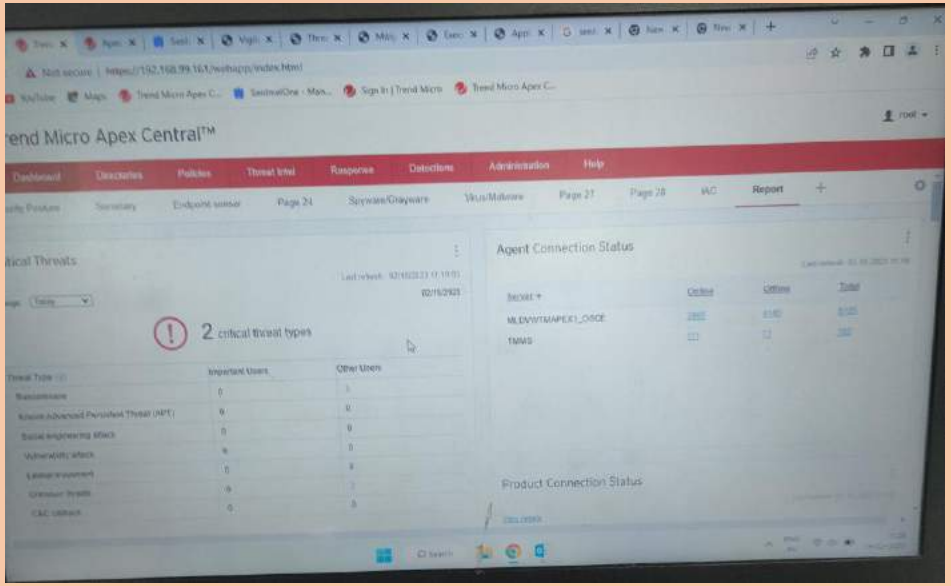


dash - Excel (Product Activation Failed)

	A	B	C	D	E	F	G	H	I	J	K	L
3	AV offline	Server Team	58	58	57	57	67	63	63	63	63	80
4	AV Status Disabled by Sentinel One	Server Team	5	5	5	5	5	5	5	5	5	5
5	AV Status Limited functionality	Server Team	3	3	3	3	3	3	4	4	4	4
6	AV Status Agent disable error	Server Team	0	0	0	0	0	0	0	0	0	0
7	AV Incident – Unresolved Threat	IT Security	2	2	2	2	33	34	34	8	8	9
8	AV Incident – Not Mitigated	IT Security	0	0	0	0	0	0	0	0	0	0
9	AV Application- Critical	Server Team	45,201	45,201	45,201	45,201	45,161	44,878	44,874	44,884	44,884	44,884
10	AV Application- High	Server Team	76,805	76,805	76,821	76,821	76,677	76,826	76,400	76,479	76,479	78,136
11	AV Application- Medium	Server Team	86,069	86,069	86,077	86,077	85,967	85,567	85,588	85,725	85,725	87,507
12	Server AV Compliance - Sentinel One AV Issue	Server Team / IT Security	12	12	11	11	11	10	10	9	9	9
13	Sentinel One Console Total Server Count	Informational	1130	1130	1130	1130	1127	1128	1131	1132	1132	1134
14	Outdated Server OS Windows 2003 / 2008	Server Team	2 / 1 (1 Exc)	2 / 1 (1 Exc)	2 / 1 (1 Exc)	2 / 1 (1 Exc)	2 / 1 (1 Exc)	2 / 1 (1 Exc)	2 / 1 (1 Exc)	2 / 1 (1 Exc)	2 / 1 (1 Exc)	2 / 1 (1 Exc)
15	Server Patch Compliance (Monthly)	Server Team	91%	91%	91%	91%	91%	91%	91%	91%	91%	91%
16	Server Patching Sampling Windows OS 2012R2 / 2016 / 2019	IT Security / Server Team	-	-	-	-	-	-	-	-	-	-
17	Server Restart Data - Pending Restart More Than 30 Days	Server Team	13	13	13	13	13	13	13	13	13	13
18	Outdated Windows 10 OS (VDI- Machine)	Server Team	33	33	33	33	33	33	33	33	33	33
19	Non-Compliance Open Share Report	Server Team	0	0	0	0	0	0	0	0	0	0
20	**NETWORK :-**											
21	Network devices end of life & support	Network Team	39	39	39	39	39	39	39	39	39	39
22												

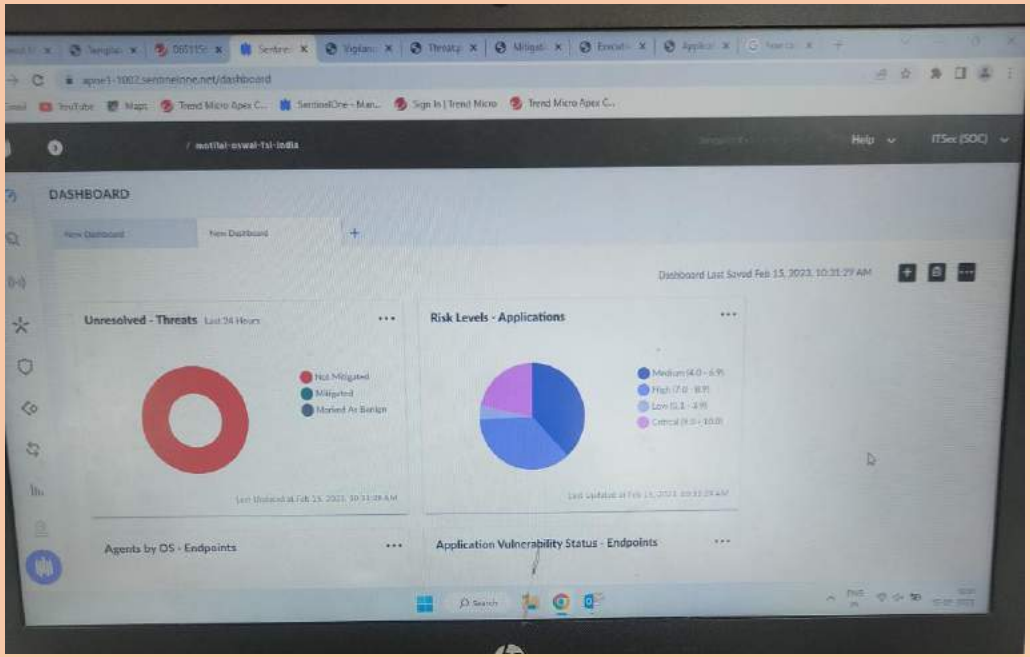
Dashboard In Trend Micro

- In this I have created a customise Dashboard in Trend Micro Apex Central.



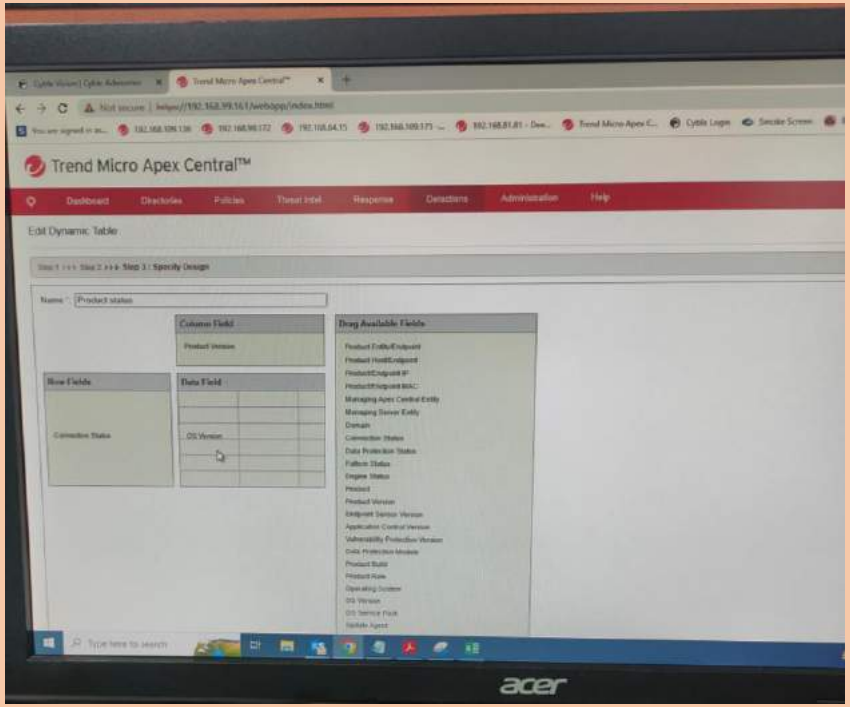
Dashboard In Sentinel One

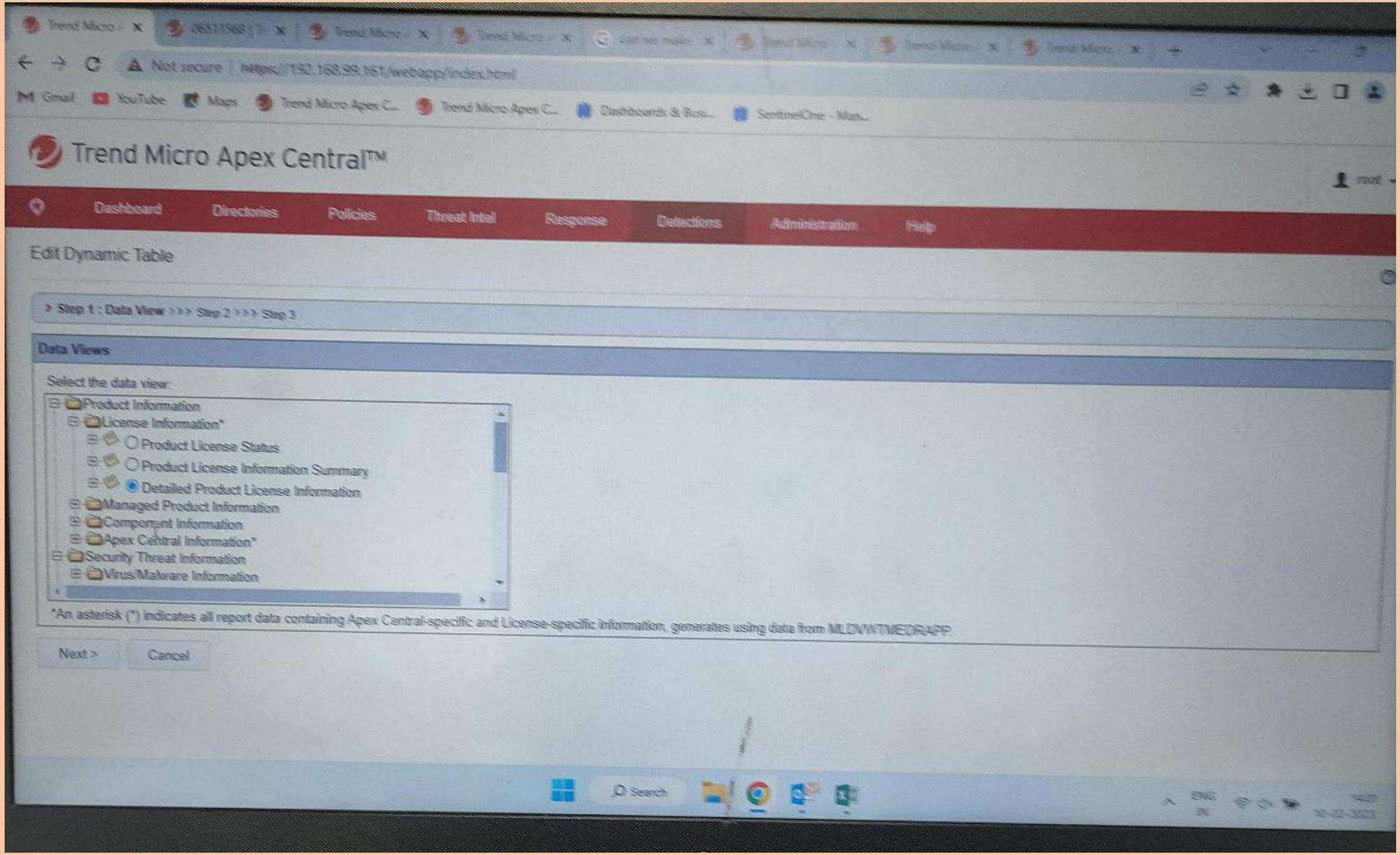
- In this I have created a customise Dashboard in Sentinel One.

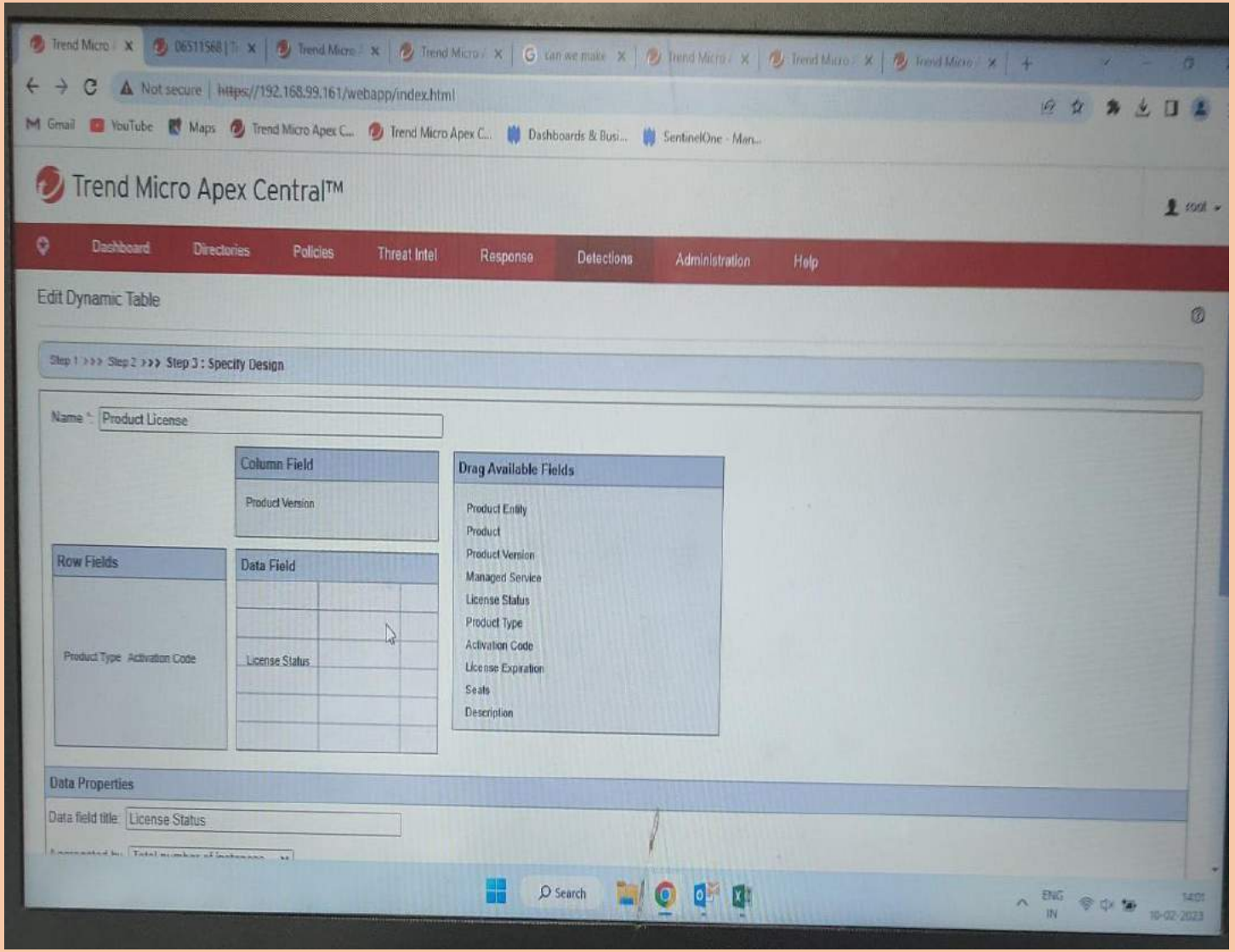


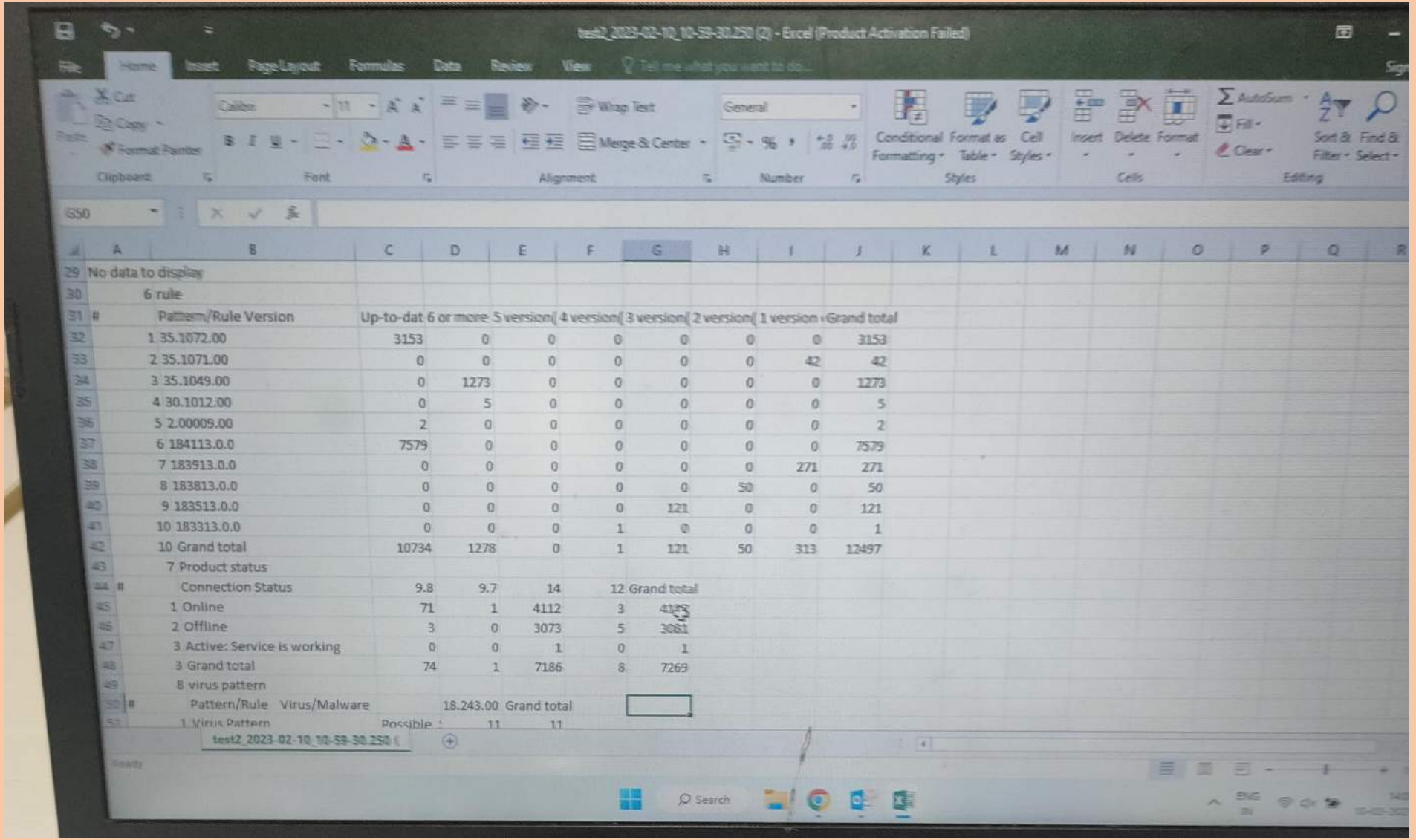
Creating a customise Template in Trend Micro

- In this i have created a customsie template which display data such as Agent online, Agent Offline, Agent Requires updates etc.



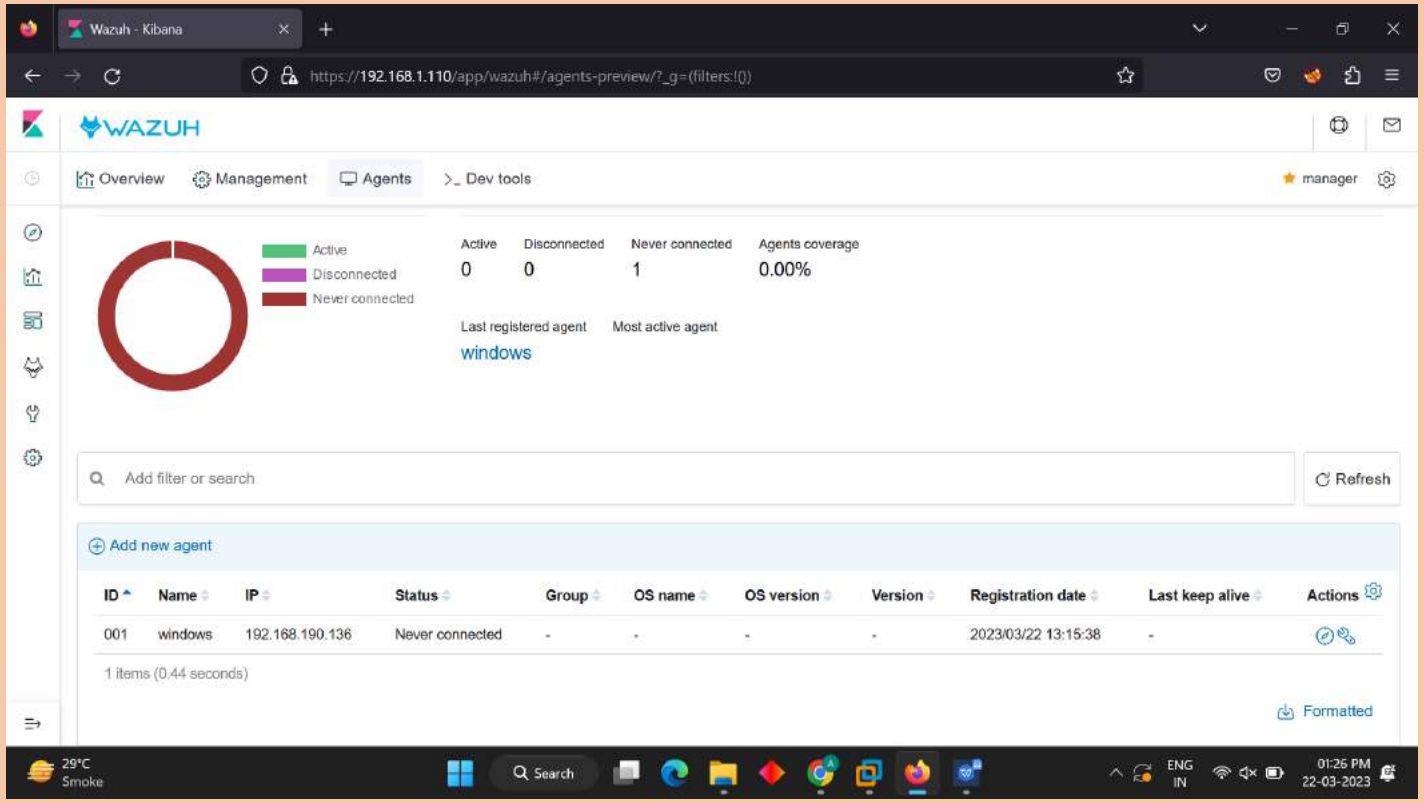

Not secure
Trend Micro Apex Central™
Dashboard
Directories
Policies
Threat Intel
Response
Detections
Administration
Help
Edit Dynamic Table
Step 1 : Data View
Step 2
Step 3
Data Views
Select the data view:
Product Information
License Information*
Product License Status
Product License Information Summary
Detailed Product License Information
Managed Product Information
Component Information
Apex Central Information*
Security Threat Information
Virus/Malware Information
*An asterisk (*) indicates all report data containing Apex Central-specific and License-specific information, generates using data from MLDVWTMEDRAPP
Next >
Cancel

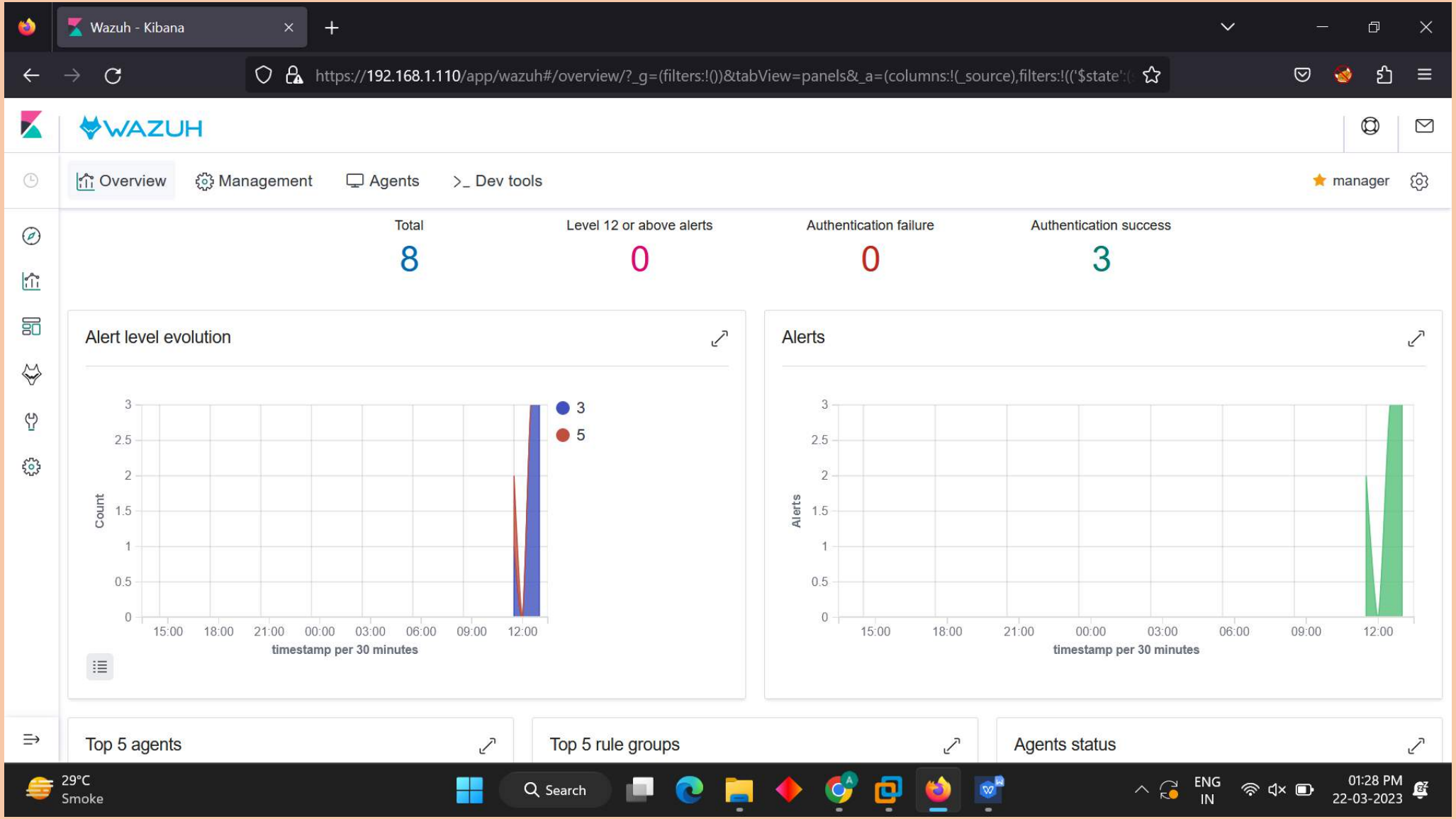

Not secure https://192.168.99.161/webapp/index.html
Trend Micro Apex Central™
Dashboard
Directories
Policies
Threat Intel
Response
Detections
Administration
Help
Edit Dynamic Table
Step 1 >>> Step 2 >>> Step 3 : Specify Design
Name *: Product License
Column Field
Product Version
Drag Available Fields
Product Entity
Product
Product Version
Managed Service
License Status
Product Type
Activation Code
License Expiration
Seats
Description
Row Fields
Product Type Activation Code
Data Field
License Status
Data Properties
Data field title: License Status
Search

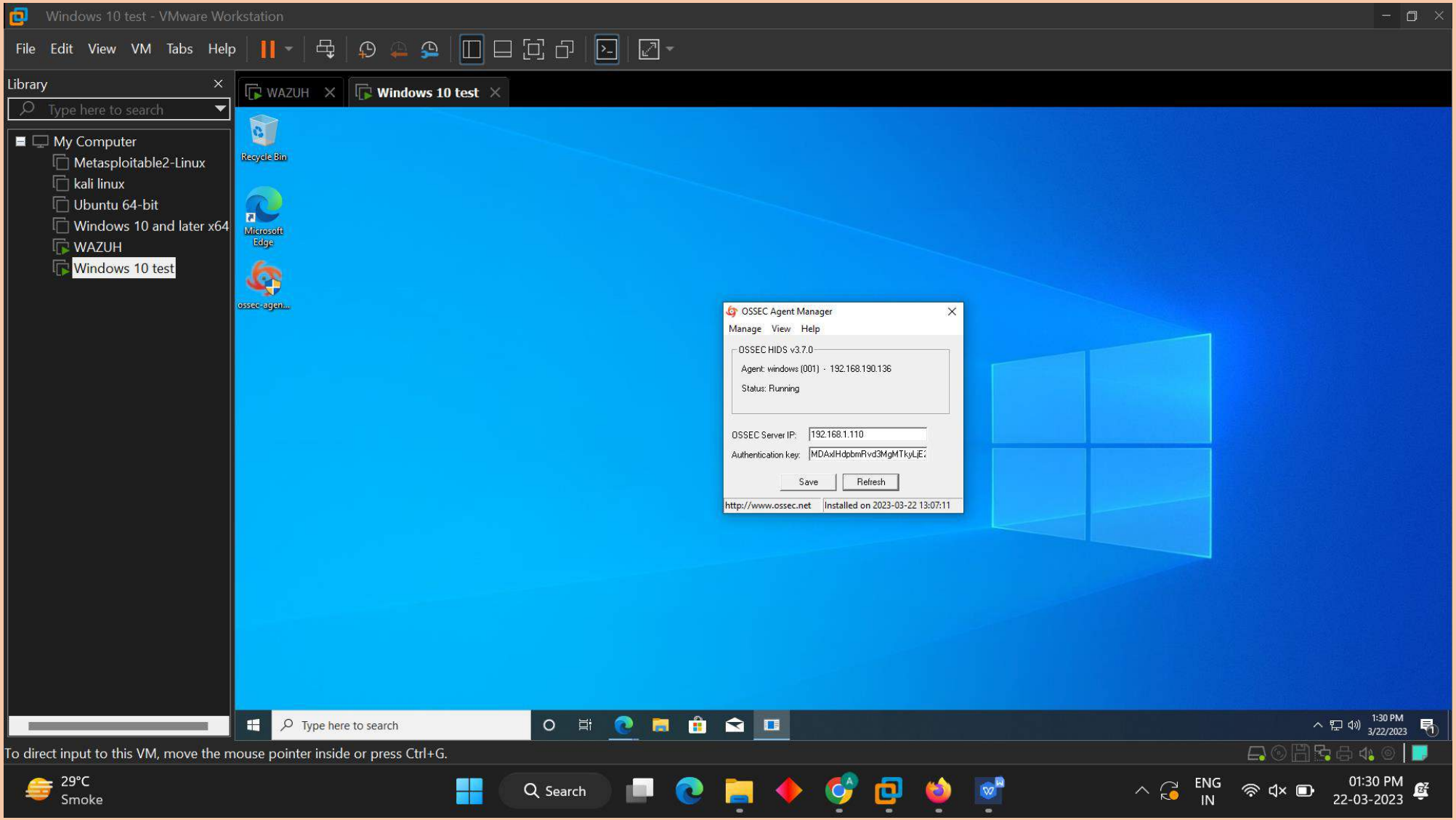

No data to display
6 rule
Pattern/Rule Version Up-to-dat 6 or more 5 version(4 version(3 version(2 version(1 version Grand total
1 35.1072.00 3153 0 0 0 0 0 0 3153
2 35.1071.00 0 0 0 0 0 0 42 42
3 35.1049.00 0 1273 0 0 0 0 0 1273
4 30.1012.00 0 5 0 0 0 0 0 5
5 2.00009.00 2 0 0 0 0 0 0 2
6 184113.0.0 7579 0 0 0 0 0 0 7579
7 183913.0.0 0 0 0 0 0 0 271 271
8 183813.0.0 0 0 0 0 0 50 0 50
9 183513.0.0 0 0 0 0 121 0 0 121
10 183313.0.0 0 0 0 1 0 0 0 1
10 Grand total 10734 1278 0 1 121 50 313 12497
7 Product status
Connection Status 9.8 9.7 14 12 Grand total
1 Online 71 1 4112 3 4187
2 Offline 3 0 3073 5 3081
3 Active: Service is working 0 0 1 0 1
3 Grand total 74 1 7186 8 7269
8 virus pattern
Pattern/Rule Virus/Malware 18.243.00 Grand total
1 Virus Pattern Possible 11 11
test2_2023-02-10_10-59-30.250 (
Search

Demo

- For demo i have used an open source SIEM tool called Wazuh.

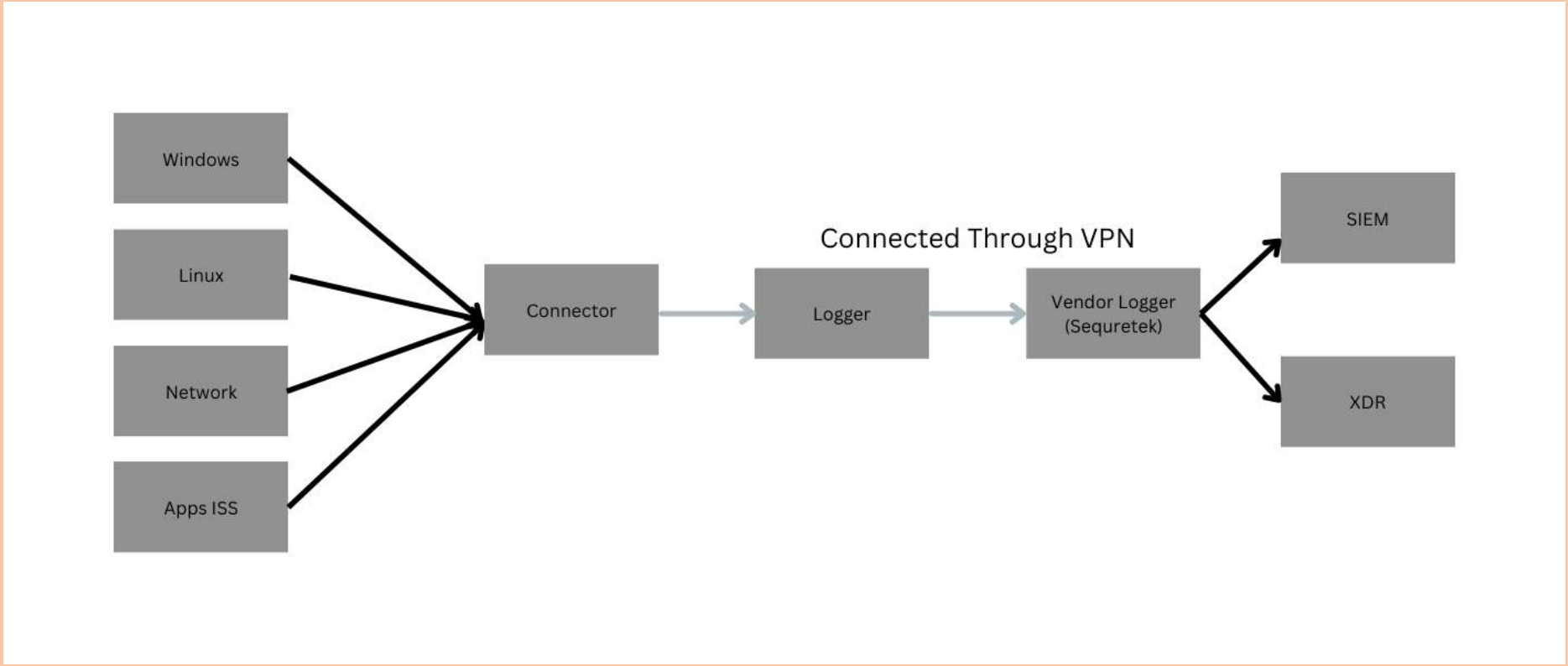



Wazuh - Kibana
https://192.168.1.110/app/wazuh#/overview/?_g=(filters:!())&tabView=panels&_a=(columns:!(_source),filters:!(('$state':(
WAZUH
Overview
Management
Agents
>_ Dev tools
manager
Total
8
Level 12 or above alerts
0
Authentication failure
0
Authentication success
3
Alert level evolution
3
5
Count
timestamp per 30 minutes
Alerts
Alerts
timestamp per 30 minutes
Top 5 agents
Top 5 rule groups
Agents status
29°C
Smoke
Search
ENG
IN
01:28 PM
22-03-2023


Windows 10 test - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2-Linux
kali linux
Ubuntu 64-bit
Windows 10 and later x64
WAZUH
Windows 10 test
WAZUH
Windows 10 test
Recycle Bin
Microsoft Edge
ossec-agen...
OSSEC Agent Manager
Manage View Help
OSSEC HIDS v3.7.0
Agent: windows (001) - 192.168.190.136
Status: Running
OSSEC Server IP: 192.168.1.110
Authentication key:
Save
Refresh
http://www.ossec.net
Installed on 2023-03-22 13:07:11
Type here to search
1:30 PM
3/22/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
29°C
Smoke
Search
ENG
IN
01:30 PM
22-03-2023

SOC Working

- Worked with Soc team and got an overview of SOC.



THANK YOU