IT INFRASTRUCTURE SECURITY ORCHESTRATION

Thesis submitted in partial fulfillment
of the requirements of the degree of

Masters in Science with Specialization in Cyber security

by

Ankit Makwana

Roll No : 03

Gr No : 3511413

Under the Supervision of

Prof. Vishal Badgujar

April 2023

Nagindas Khandwala College,
Malad (West)

(Affiliated to University of Mumbai)

MUMBAI , 400064
MAHARASHTRA
YEAR - 2023

CERTIFICATE

This is to certify that the dissertation entitled **“IT INFRASTRUCTURE SECURITY ORCHESTRATION”** is a bonafide work of “**ANKIT MAKWANA**” **(Roll No: 03 and G.R. No: 3511413)** submitted to the Nagindas Khandwala College(Autonomous), Mumbai in partial fulfillment of the requirement for the award of the degree of **“Masters in Science with Specialization in Cybersecurity”**.

Prof. Vishal Badgujar
Internal-Examiner

Prof.
External Examiner

Supervisor’s Certificate

This is to certify that the dissertation entitled “**IT INFRASTRUCTURE SECURITY ORCHESTRATION”** submitted by **ANKIT MAKWANA, Roll No: 03 and G.R. No: 3511413,** is a record of original work carried out by him under my supervision and guidance in partial fulfillment of the requirements of the degree of **Masters in Science with Specialization in Cybersecurity** at Nagindas Khandwala College(Autonomous),Mumbai 400064 . Neither this dissertation nor any part of it has been submitted earlier for any degree or diploma to any institute or university in India or abroad.

Prof. Vishal Badgujar
Internal-Examiner

Declaration of Originality

I, **Ankit Makwana, Roll No: 03** and **G.R. No: 3511413**, hereby declare that this dissertation entitled "**IT INFRASTRUCTURE SECURITY ORCHESTRATION"** presents my original work carried out as a Master Student of Nagindas Khandwala College(Autonomous),Mumbai 400064. To the best of my knowledge, this dissertation contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of Nagindas Khandwala College(Autonomous), Mumbai or any other institution. Works of other authors cited in this dissertation have been duly acknowledged under the sections "Reference" or "Bibliography". I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

I am fully aware that in case of any non-compliance detected in future, the Academic Council of Nagindas Khandwala College(Autonomous), Mumbai may withdraw the degree awarded to me on the basis of the present dissertation.

Date:

Place:

Ankit Makwana

Acknowledgement

I remain immensely obliged to **Prof. Vishal Badgujar**, for providing me with the idea of this topic, and for his invaluable support in garnering resources for me either by way of information or computers also his guidance and supervision which made this Internship happen.

I would like to say that it has indeed been a fulfilling experience for working out this Internship.

Motilal Oswal Financial Services Limited
CIN : L67190MH2005PLC153397
Regd. Office: Motilal Oswal Tower,
Rahimtullah Sayani Road, Opp. Parel ST Depot,
Prabhadevi, Mumbai – 400025.
Board: +91-22-71934200 / 71934263
Fax: +91 2250362365

Dated 31-Jan-23

To,
Ankit Prakash Makwana
Mumbai

Sub: Internship

Dear *Ankit*,

We are happy to confirm that we will offer you a project on **"Cyber Security**" for period starting from **1-Feb-2023** and ending on **30-Apr-2023**. You will be reporting to **Mrs. Chandrashekar Thangaraj Chettiar.**

This will be on an internship basis and should not be treated as regular employment with our **Motilal Oswal Financial Services Limited**. However, during the internship, all relevant company policies shall be applicable to you.

You will not be paid any stipend for the tenure of your internship.

Warm Regards,
For Motilal Oswal Financial Services Limited

Pragnesh Patel
Senior Vice President– Human Resource

Abstract

The techniques and practices used to secure an organization IT assets against threats such as cyber attacks, data breaches, and authorized access are referred to as IT infrastructure security. A secure IT infrastructure is crucial to an organization capacity to operate successfully, preserve sensitive data, and keep customers and stakeholders trusting. Access restrictions, network security, data encryption, and security monitoring are all examples of IT infrastructure security activities and technology. It include discovering and mitigating vulnerabilities in hardware, software, and network systems, as well as putting in place rules and procedures to guarantee that employees and third-party vendors follow best practices in security. To secure its IT infrastructure, businesses can use a range of tools and technologies, such as firewalls, intrusion detection systems, antivirus software, and vulnerability scanners. They can also develop security policies and training programme to teach staff the value of security and how to recognize and mitigate potential security threats. Continuous monitoring, analysis, and testing are required to discover and remediate vulnerabilities and guarantee that security policies remain effective over time. It also necessitates regular software and system updates and patching to address known vulnerabilities and keep ahead of emerging threats.

Monitoring tools are critical components of every organisation's information technology architecture. These solutions enable IT teams to monitor the performance, availability, and security of their systems and applications in real time, allowing them to discover and resolve issues before they disrupt business operations. Monitoring tools range from simple network monitoring tools to comprehensive analytic platforms that provide in-depth visibility into an organisation's complete IT environment's performance and security. Real-time alerts, performance measurements, historical data analysis, and customisable dashboards and reports are typical characteristics and capabilities of effective monitoring solutions. These technologies enable IT professionals to swiftly identify problems and take corrective action, as well as track trends and patterns to improve overall system reliability.The monitoring tool selected will be determined by an organisation's specific demands and IT environment. Among the most common monitoring tools are Trend Micro Apex one, Sentinel one, Nagios, Zabbix, PRTG, and SolarWinds. Cloud-based monitoring technologies are also growing more common, allowing organisations to scale and adapt more easily

Table of Contents

CHAPTER 1 : INTRODUCTION

1.1] Introduction

IT infrastructure monitoring is the process of tracking and analysing an organisation's IT systems and applications' performance, availability, and security. It entails continuously monitoring and collecting data from various IT infrastructure components like as servers, networks, databases, and applications, and then using that data to discover possible problems, fix difficulties, and optimise system performance.

Effective IT infrastructure monitoring is critical for guaranteeing an organisation's IT environment's dependability and security. It enables IT staff to identify and respond to issues quickly, reducing downtime and service disruptions. It also assists organisations in identifying areas for improvement and optimising their IT infrastructure to increase performance and cost-effectiveness.

IT infrastructure monitoring solutions are required for accurate monitoring. These solutions can provide real-time visibility into the performance and availability of various IT components while also alerting IT employees when problems develop. They can also give historical data analysis and reporting, allowing businesses to find trends and patterns that will help them enhance their IT infrastructure in the future.

Trend Micro Apex One is a comprehensive endpoint security solution designed to safeguard enterprise networks and devices from a variety of cyber attacks. It provides a variety of features and capabilities that assist organisations in preventing, detecting, and responding to cyber assaults and data breaches.

Trend Micro Apex One's primary features include malware protection, web security, firewall protection, device control, data encryption, behavioural analysis, and threat hunting.[1]

Trend Micro is a cybersecurity firm that offers a variety of security solutions such as endpoint protection, network security, and cloud security. Trend Micro's monitoring process varies depending on the product or solution being utilized, but it generally consists of the following steps:

Monitoring begins with a review of network traffic, system logs, and other data sources to identify potential security concerns. This includes keeping an eye out for known malware and vulnerabilities, as well as unusual behaviour that could indicate a new or unknown danger.

Trend Micro's security solutions use a variety of detection techniques, including signature-based detection, behaviour-based detection, and machine learning algorithms, to evaluate whether a possible threat is dangerous

Trend Micro's security solutions analyse threats once they have been detected to identify their severity and impact on the organisation's systems and data.

Response: Depending on the attack's severity and impact, Trend Micro's security solutions may perform a variety of response steps, such as blocking the threat, quarantining infected data, and informing security personnel.

Information: Trend Micro's security solutions provide detailed information on security threats and incidents, including the threat's severity, response actions performed, and suggestions for enhancing the organisation's overall security posture.

SentinelOne is a powerful endpoint security platform that protects against a wide range of cyber threats in real time, including malware, ransomware, fileless assaults, and zero-day exploits. It detects and responds to threats in real time using artificial intelligence and machine learning, rather than signatures or manual updates.

AI-powered threat detection, Autonomous response, Malware prevention, Endpoint detection and response, Ransomware protection, IoT security, and Cloud security are some of SentinelOne's core features. [2]

SentinelOne is an endpoint security technology that detects and responds to attacks in real time across all endpoints in an organisation's network. SentinelOne's monitoring procedure consists of the following steps:

SentinelOne delivers continuous monitoring of all network endpoints, including servers, desktops, laptops, and mobile devices, to detect and mitigate any security risks.

SentinelOne detects known and undiscovered threats in real-time using powerful machine learning and behavioural analysis. To identify potential risks, the platform analyses all system activity, including files, programs, and network connections.

Threat Analysis: When a threat is detected, SentinelOne analyses it automatically to identify its nature, severity, and extent. The platform determines the source of the threat, its potential impact, and the procedures required to mitigate the threat.

SentinelOne provides automated response capabilities to quickly remediate attacks without the need for user interaction. The platform isolates the affected device or system, removes the threat, and returns operations to normal.

SentinelOne delivers thorough data and analytics to assist organisations in understanding their security posture and identifying potential areas for improvement. The platform provides insights on threat behavior, system vulnerabilities, and security policy compliance.

1.2] PROBLEM STATEMENT

Without a mechanism to record and analyse live data, identifying possible faults or patterns affecting the organisation's IT infrastructure becomes difficult. System unavailability, poor performance, security vulnerabilities, and compliance difficulties can all result from a lack of monitoring. To address this issue, the organisation must create a mechanism for recording and analysing the application's live data. This system should enable IT employees to monitor system performance, discover any errors or anomalies, and take appropriate corrective action. Furthermore, frequent data analysis can assist find trends and patterns that can be used to optimise system setups and improve overall performance.The organisation can benefit from developing a system for recording and analysing live data.

The organisation can apply the following methods to address the issue of a lack of a system for recording and analysing live data: Install Monitoring Tools: The organisation can install monitoring tools to track and collect real-time data from all systems. These tools can assist in detecting problems, tracking performance, and identifying potential vulnerabilities. Regular Reporting: To monitor the performance and status of all systems, the organisation can generate regular reports based on live data. These reports can assist in identifying possible problems and taking corrective action before they cause system downtime.

1.3] Aim

The goal of system monitoring in an organization is to guarantee that all networks, systems, and applications are operational and ready for use at all times. The monitoring process entails ongoing observation and evaluation of the operation and condition of the company's IT infrastructure. This is done in order to find any flaws or potential difficulties as soon as possible, enabling the IT personnel to fix them before they cause major disruptions or downtime.

1.4] OBJECTIVE

To Protecting a company's computer systems, networks, and data centres against potential threats and vulnerabilities that could jeopardise their security or interfere with their operations is the goal of IT infrastructure security. The following are the main objectives of IT infrastructure security:

- Confidentiality: Ensuring that private information is kept private and that only authorised personnel can access it.
- Integrity: Ensuring that data is accurate, comprehensive, and unaltered by unauthorised users.
- Availability: Ensuring that essential information and systems are constantly accessible to authorised personnel.
- Compliance: Ensuring that the company conforms with all applicable laws, rules, and standards.

Risk management involves identifying and evaluating potential security risks and vulnerabilities as well as putting the right precautions in place to lessen those risks.

reaction to incidents: Creating and carrying out a successful reaction strategy.

CHAPTER 2 : LITERATURE SURVEY

A Survey of Critical Infrastructure Security by William Hurst, Madjid Merabti, Paul Fergus states that raditionally, securing against environmental threats was the main focus of critical infrastructure protection. However, the emergence of cyber attacks has changed the focus – infrastructures are facing a different danger that has life-threatening consequences and the risk of significant economic losses. Clearly, conventional security techniques are struggling to keep up with the volume of innovative and emerging attacks. Fresh and adaptive infrastructure security solutions are required. .

Safeguarding Cloud Computing Infrastructure: A Security Analysis by Mamdouh Alenezi states that Cloud computing is the provision of hosted resources, comprising software , hardware and processing over the World Wide Web. The advantages of rapid deployment, versatility, low expenses and scalability have led to the widespread use of cloud computing across organizations of all sizes, mostly as a component of the combination/multi-cloud infrastructure structure. While cloud storage offers significant benefits as well as cost-effective alternatives for IT management and expansion, new opportunities and challenges in the context of security vulnerabilities are emerging in this domain. Cloud security, also recognized as cloud computing security

Critical Infrastructure Security by Paul Wagner states that What if a cyber-attack could result in explosions, large scale blackouts, intentional flooding, a nuclear meltdown or nuclear war? Hollywood has provided us with many examples of how hackers could intentionally or unintentionally cause catastrophic failures of critical infrastructure. In 1983's Wargames, a hacker connects to a top-secret computer which is tied into the United States' nuclear arsenal (IMDb, 2020). The 2007 movie Live Free or Die Hard, depicts hackers systematically shutting down the United States Stock Market, disrupting communications and traffic safety, and tampering with other critical infrastructure (IMDb, 2020).

Research Paper on Cyber Security in Cloud Infrastructure by Aniket Ghate states that Cloud computing is predicted to vary the way information technology (IT) is employed and managed better cost efficiency, faster innovation, faster time-tomarket, and therefore the ability to scale Application on Demand (Leighton, 2009). per Gartner, while the hype grew rapidly Released from 2008 and onwards, it's clear that the cloud computing model has undergone a serious change. And the benefits will be significant (Gartner HypeCycle, 2012).

Sr No	Author	Title	Advantages	Disadvantages
1	William Hurst, Madjid Merabti, Paul Fergus	A Survey of Critical Infrastructure Security	The paper provides a comprehensive overview of the various types of critical infrastructure and the threats they face, including physical, cyber, and environmental threats.	While the paper provides a comprehensive overview of critical infrastructure security, it may not cover all possible threats and measures, as the field is constantly evolving and new threats may emerge.
2	Mamdouh Alenezi	Safeguarding Cloud Computing Infrastructure	The paper provides a comprehensive overview of cloud computing security, including the various types of threats and vulnerabilities that can impact cloud computing infrastructure.	The paper focuses on cloud computing security and may not cover all possible threats and vulnerabilities that could impact an organization's overall security posture.
3	Paul Wagner	Critical Infrastructure Security	The paper provides a comprehensive overview of critical infrastructure security, including the various types of critical infrastructure and the threats they face.	The paper does not provide any quantitative analysis, which could limit the ability to measure the effectiveness of different security measures.
4	Aniket Ghate	Research Paper on Cyber Security in Cloud Infrastructure	The paper provides practical advice for organizations to safeguard their cloud infrastructure, including specific security measures that can be implemented.	The paper is largely based on a review of existing literature and may not provide a deep analysis of empirical data, which could limit the conclusions drawn from the study.

CHAPTER 3 : METHEDOLOGY

3.1 REQUIREMNETS

Hardware Used:-

1) Processor: At least a 1 GHz Intel or AMD processor.

2) Memory (RAM): At least 1 GB of RAM (2 GB or more recommended).

3) Hard Disk Space: At least 1.3 GB of available disk space (2.5 GB or more recommended).

4) Display: Minimum 1024 x 768 pixel resolution (Higher resolution recommended).

5) Network Interface: A network interface card (NIC) that supports TCP/IP protocol.

Software and Tools Used:-

1) Trend Micro Apex One

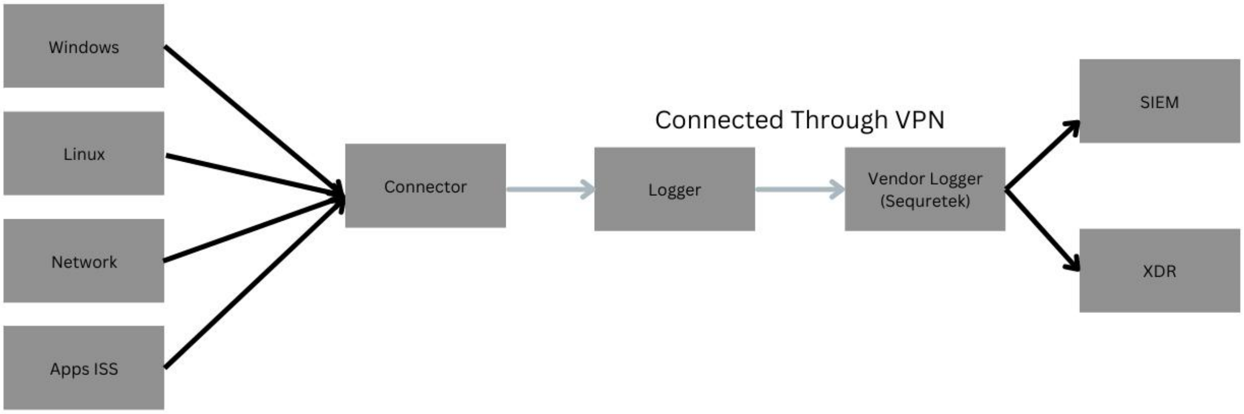
2) Sentinel One

3) Wazuh

3.2 METHEDOLOGY

Overview of Soc

Got an over view of Soc like what does it do and how it gets monitors. Monitoring of SOC is done by a tool name ArcSight which is installed in each and every server which Are present. In Soc mainly logs are monitored and checked weather a device able to generate a log and Monitored it if there is any problem then why is that problem coming along with threat detection.

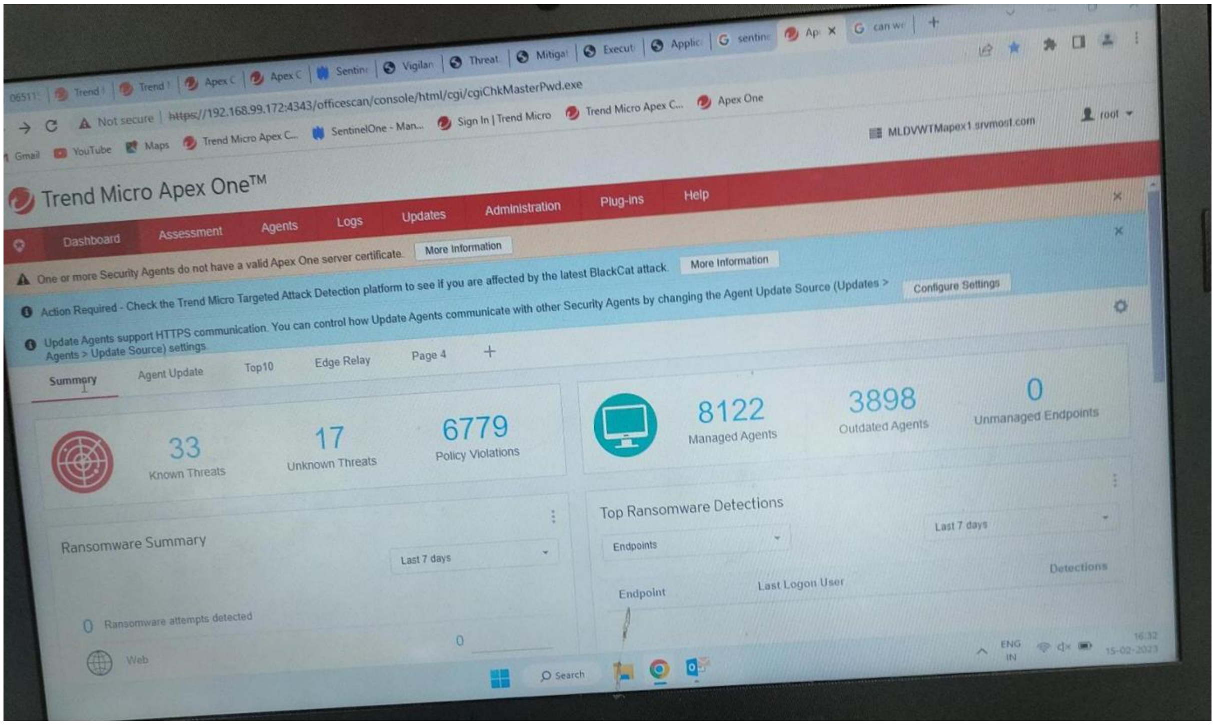


1) Monitoring of Endpoints and Servers

- We monitor Endpoints using Trend micro apex one
- In which we watch Online, Offline System and threats etc are monitored and accordingly a report is Generated
- For Server we use Sentinel One to monitor the servers
- In this we again get the information about the servers like online, offline, risk level etc and accordingly a report is generated.[1]

Trend Micro

Here in this we can see the dashboard of the application from where we monitor the systems



One or more Security Agents do not have a valid Apex One server certificate.

Action Required - Check the Trend Micro Targeted Attack Detection platform to see if you are affected by the latest BlackCat attack.

Update Agents support HTTPS communication. You can control how Update Agents communicate with other Security Agents by changing the Agent Update Source (Updates > Agents > Update Source) settings.

33	17	6779	8122	3898	0
Known Threats	Unknown Threats	Policy Violations	Managed Agents	Outdated Agents	Unmanaged Endpoints

Ransomware Summary

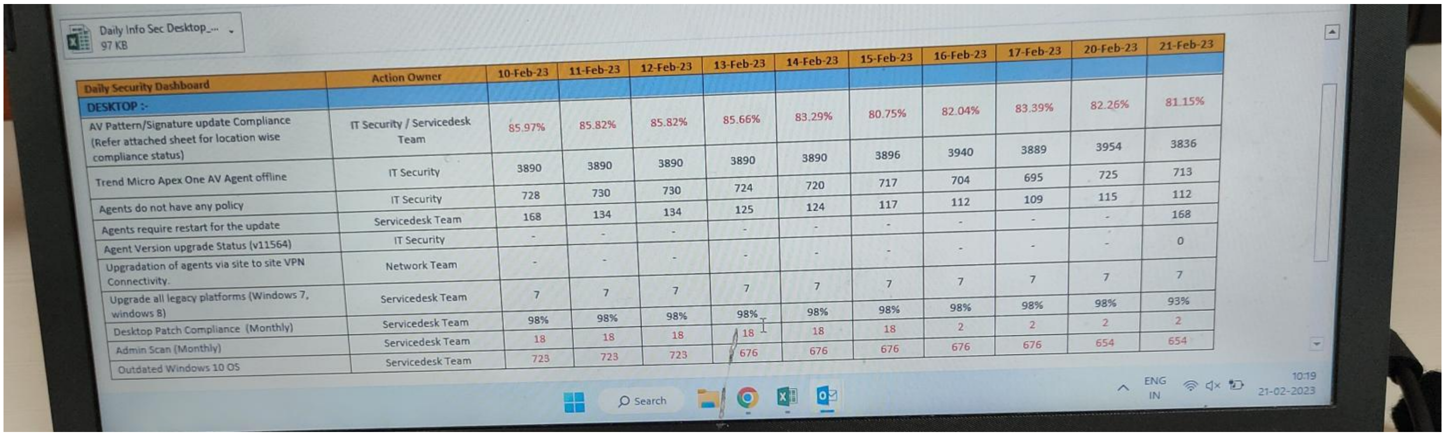
0 Ransomware attempts detected

Web 0

Top Ransomware Detections

Endpoint	Last Logon User	Detections

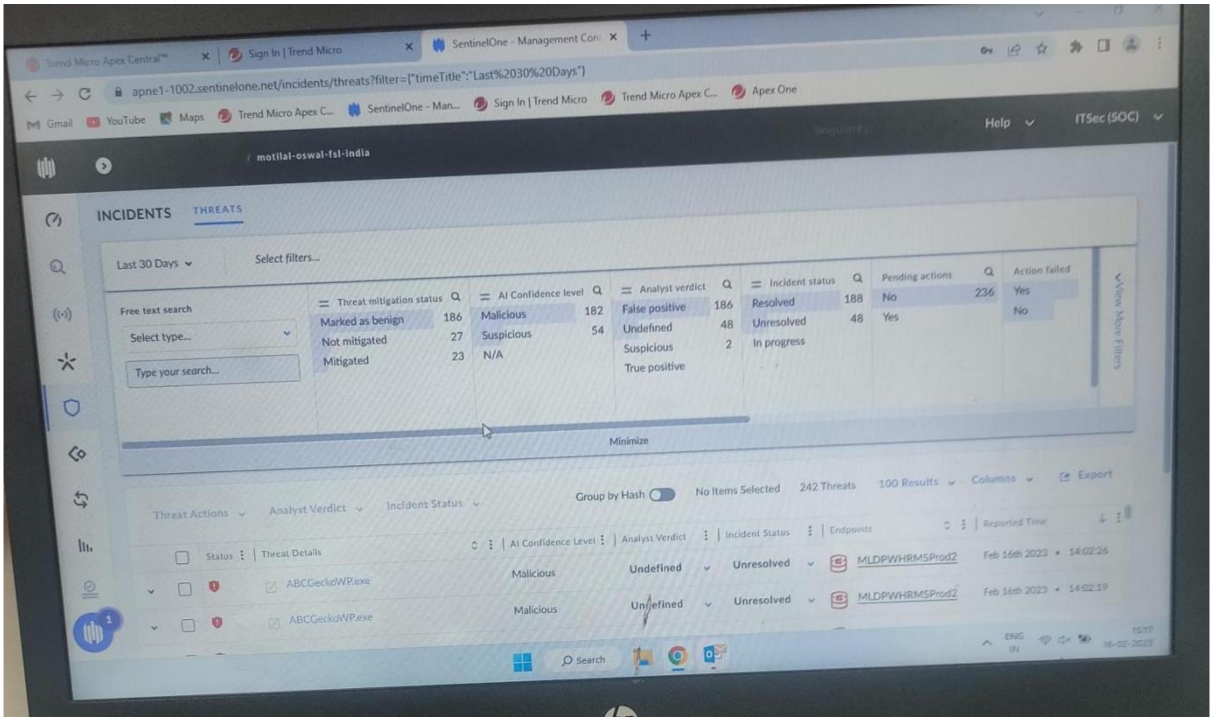
Here I have created a table which contains the details of the systems which are required on daily basis.


Daily Info Sec Desktop_...
97 KB
Search
ENG
IN
10:19
21-02-2023

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

Sentinel One

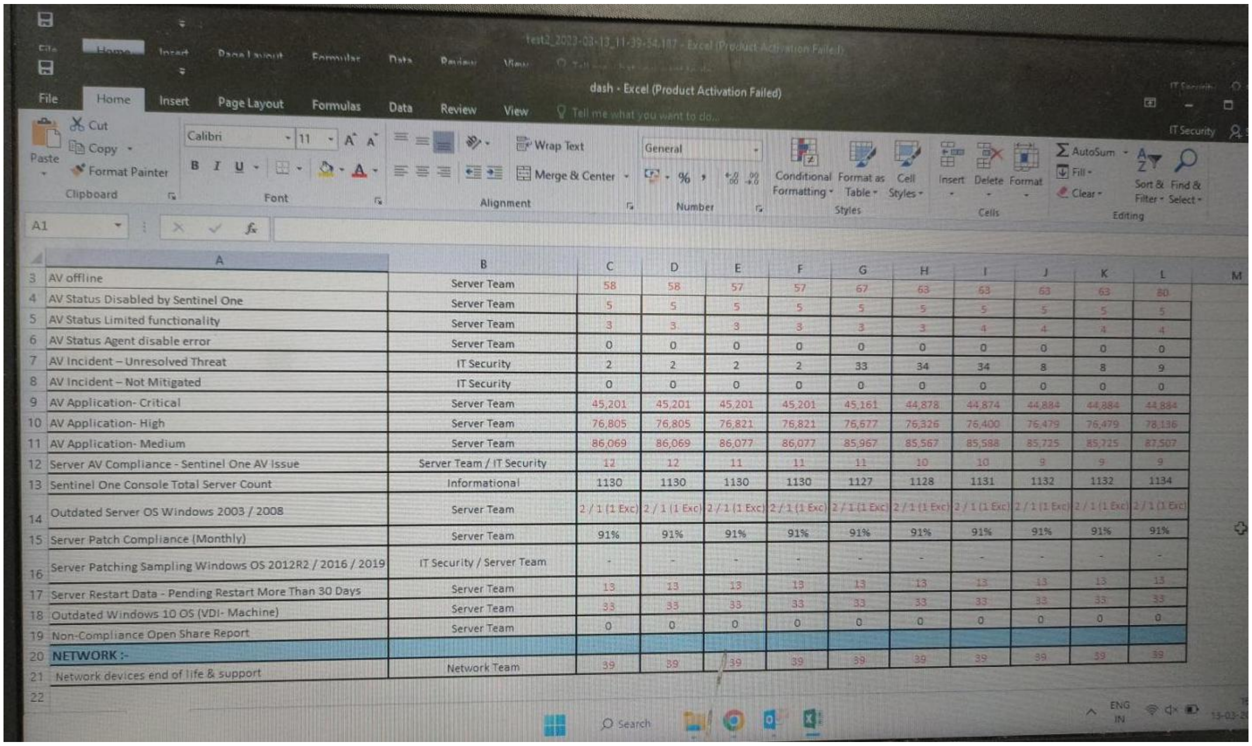
Here in this we can see the dashboard of the application from where we monitor the systems



Threat mitigation status		AI Confidence level		Analyst verdict		Incident status		Pending actions		Action failed
Marked as benign	186	Malicious	182	False positive	186	Resolved	188	No	236	Yes
Not mitigated	27	Suspicious	54	Undefined	48	Unresolved	48	Yes		No
Mitigated	23	N/A		Suspicious	2	In progress				
				True positive						

Status	Threat Details	AI Confidence Level	Analyst Verdict	Incident Status	Endpoints	Reported Time
	ABCGeckoWP.exe	Malicious	Undefined	Unresolved	MLDPWHRMSProd2	Feb 16th 2023 • 14:02:26
	ABCGeckoWP.exe	Malicious	Undefined	Unresolved	MLDPWHRMSProd2	Feb 16th 2023 • 14:02:19

Here I have created a table which contains the details of the systems which are required on daily basis.

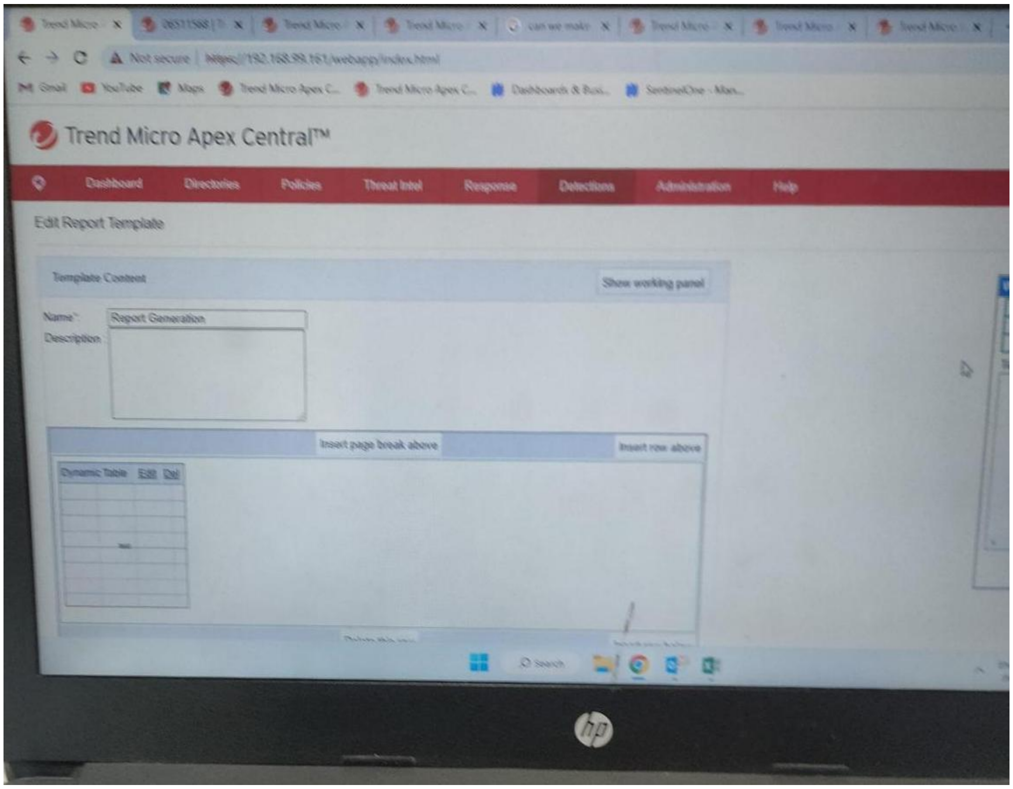


	A	B	C	D	E	F	G	H	I	J	K	L
3	AV offline	Server Team	58	58	57	57	67	63	63	63	63	80
4	AV Status Disabled by Sentinel One	Server Team	5	5	5	5	5	5	5	5	5	5
5	AV Status Limited functionality	Server Team	3	3	3	3	3	3	4	4	4	4
6	AV Status Agent disable error	Server Team	0	0	0	0	0	0	0	0	0	0
7	AV Incident – Unresolved 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	76,326	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												

2) Custom template in Trend

- In this first we need to go in Trend micro apex central
- In central we can see detection in detection we click on report and in report we click on custom Template.
- After that we get a list of templates which are present along with that we get a option of add to create a custom template click on it.
- After that we get few option which we can drag and drop in the selected section there are options Such as dynamic table, static table bar chart etc for my report I used a dynamic table. After that we need to click on edit in dynamic table
- Then we will see a list of folders from which we need to select the folder in order to get data.
- After selecting folder click in next and then we will see a section divided into three part row, colour, Data.
- Along with it we will have option from which we need to drag drop the item which we need to display.
- Then we need to click on save
- After this we need to generate a report.
- Now we need to click on detection in detection we go in one time report
- In one time report we get an option of add click on add then we have to select custom template which we created.
- Then click on next and after some time we will be able to see the report generated according to the custom template.

In the below image I am creating a new custom template to automate the collection of data.



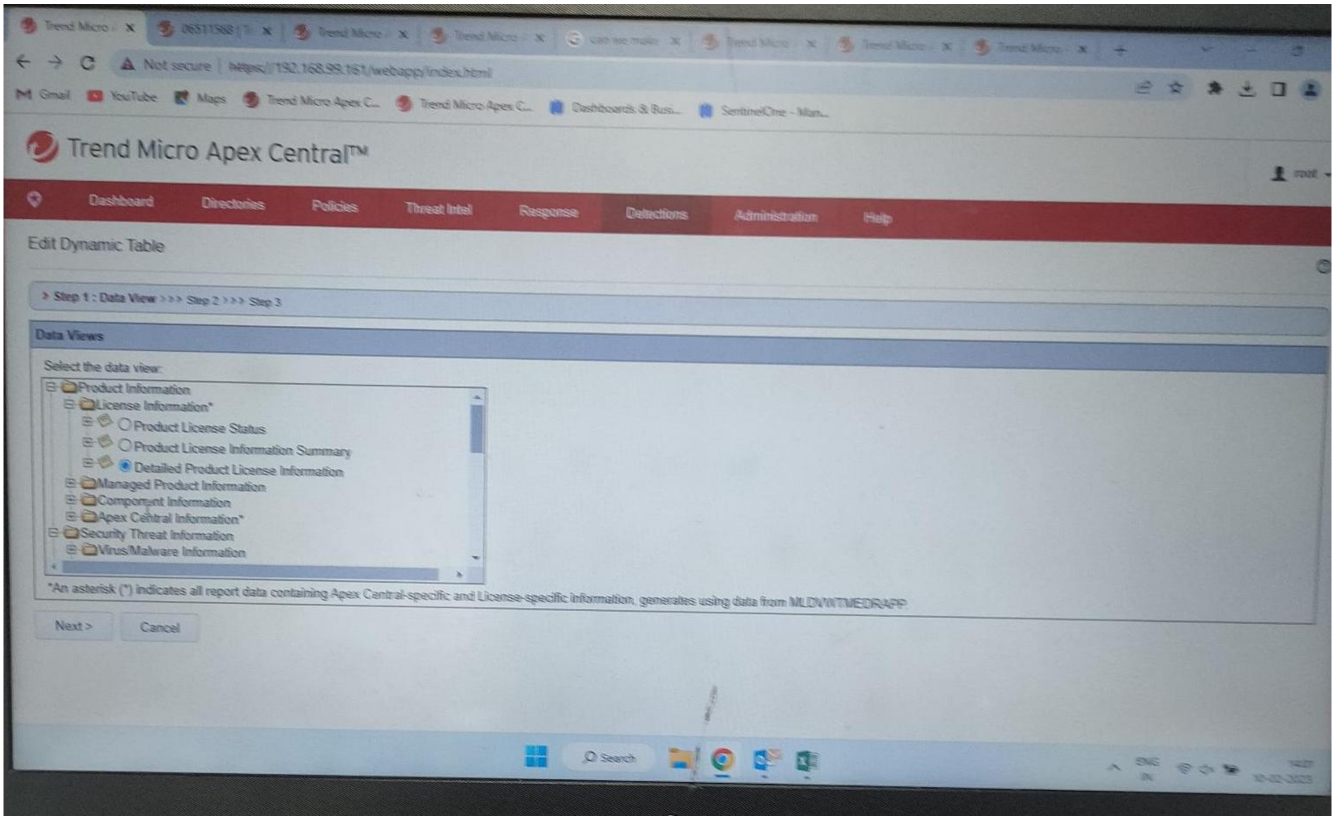
Edit Report Template

Template Content

Name*: Report Generation

Description:

Now I have to select the field which I want to display in the report.



Edit Dynamic Table

> Step 1 : Data View >>> Step 2 >>> Step 3

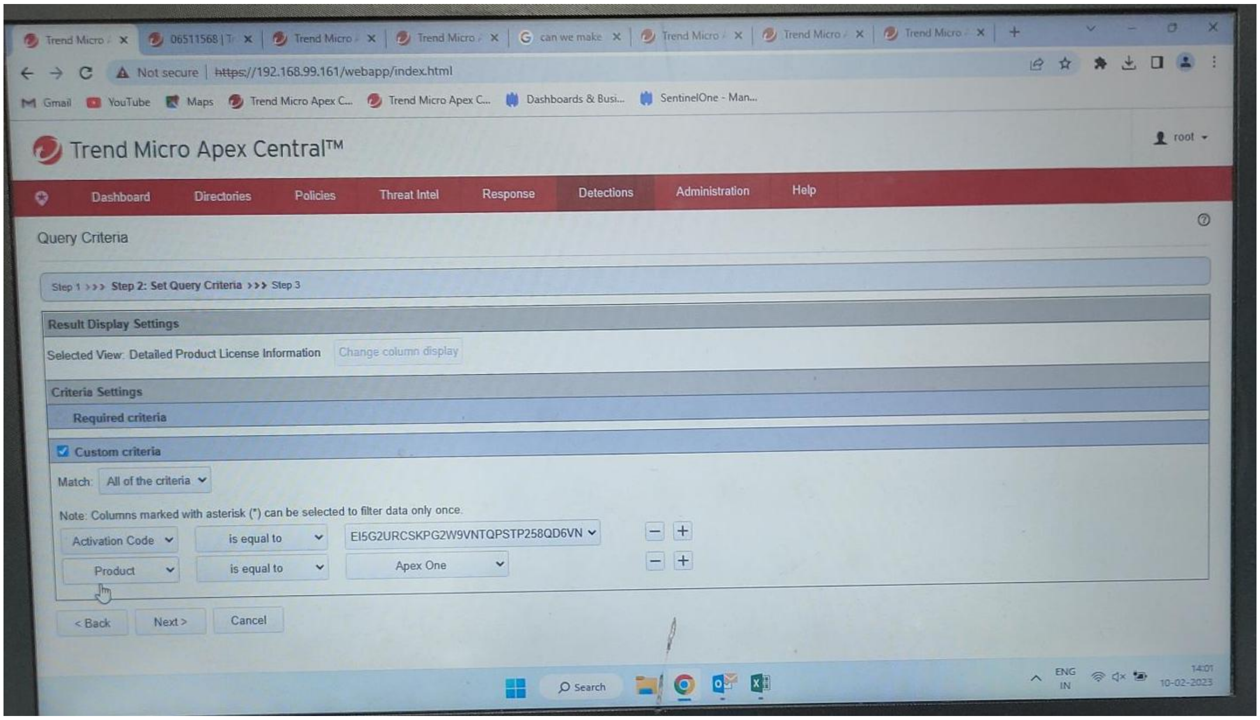
Data Views

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

After selecting field I need to select the criteria.



Query Criteria

Step 1 >>> Step 2: Set Query Criteria >>> Step 3

Result Display Settings

Selected View: Detailed Product License Information Change column display

Criteria Settings

Required criteria

☑ Custom criteria

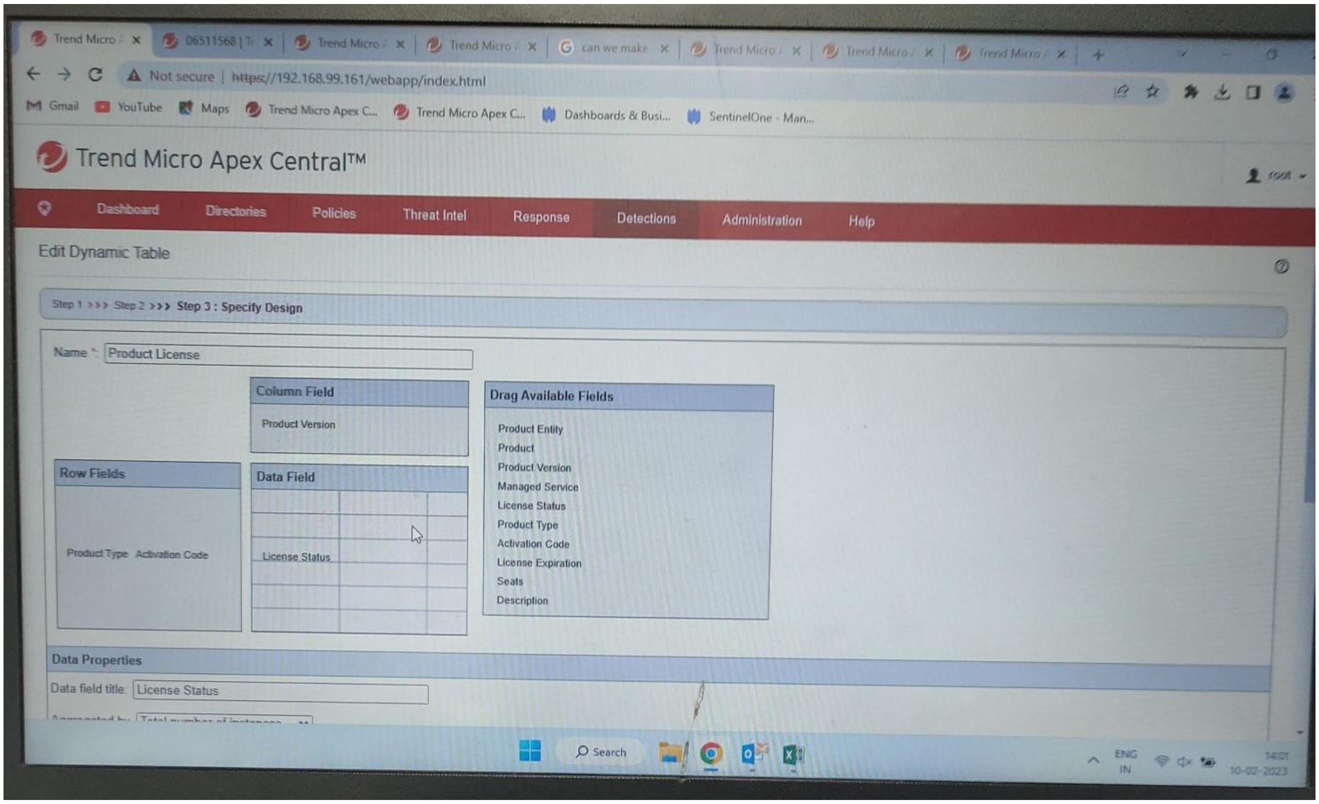
Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Activation Code | is equal to | EI5G2URCSKPG2W9VNTQPSTP258QD6VN

Product | is equal to | Apex One

Now I need to frag and drop the field which I want to display.



Not secure | https://192.168.99.161/webapp/index.html

Edit Dynamic Table

Step 1 >>> Step 2 >>> Step 3 : Specify Design

Name *: Product License

Column Field: Product Version

Row Fields: Product Type Activation Code

Data Field: License Status

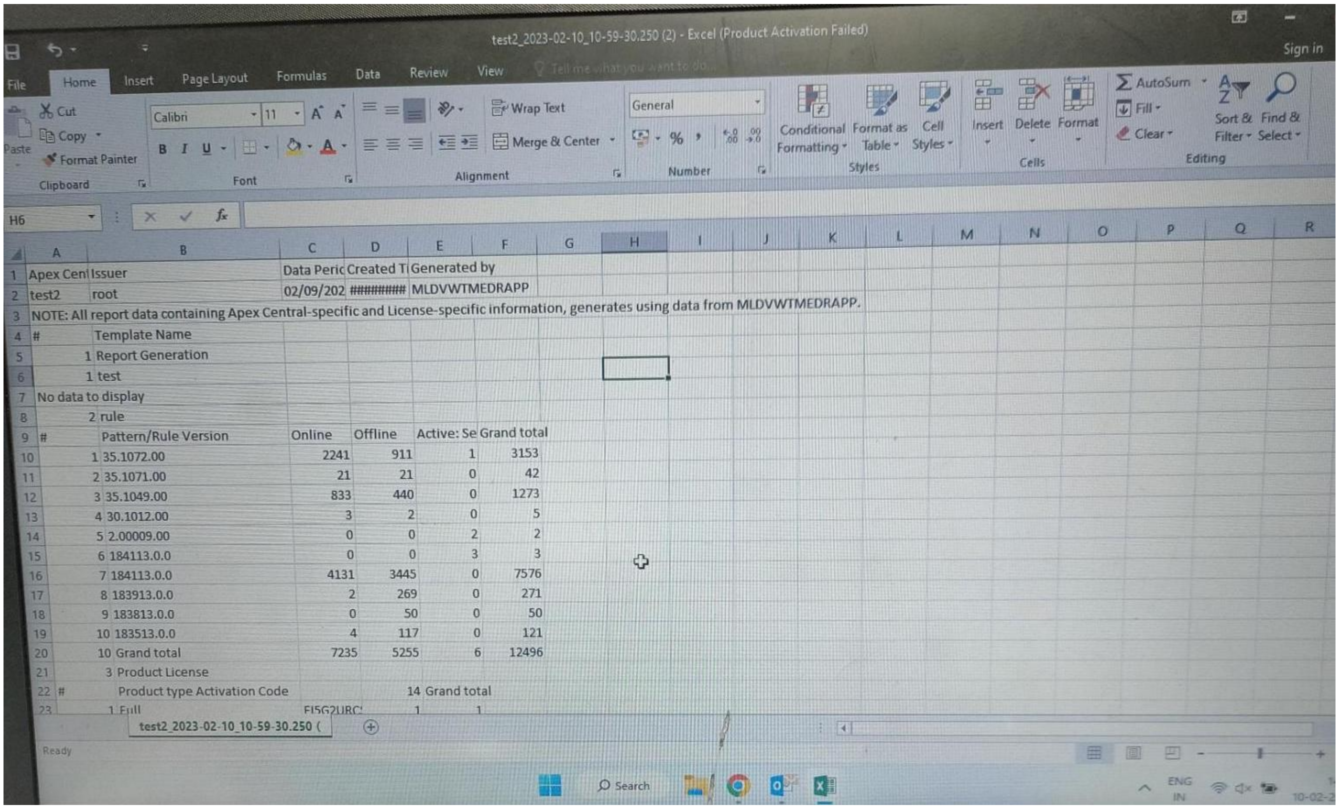
Drag Available Fields:

- Product Entity
- Product
- Product Version
- Managed Service
- License Status
- Product Type
- Activation Code
- License Expiration
- Seats
- Description

Data Properties

Data field title: License Status

Then this is how the final report looks after generating the report.

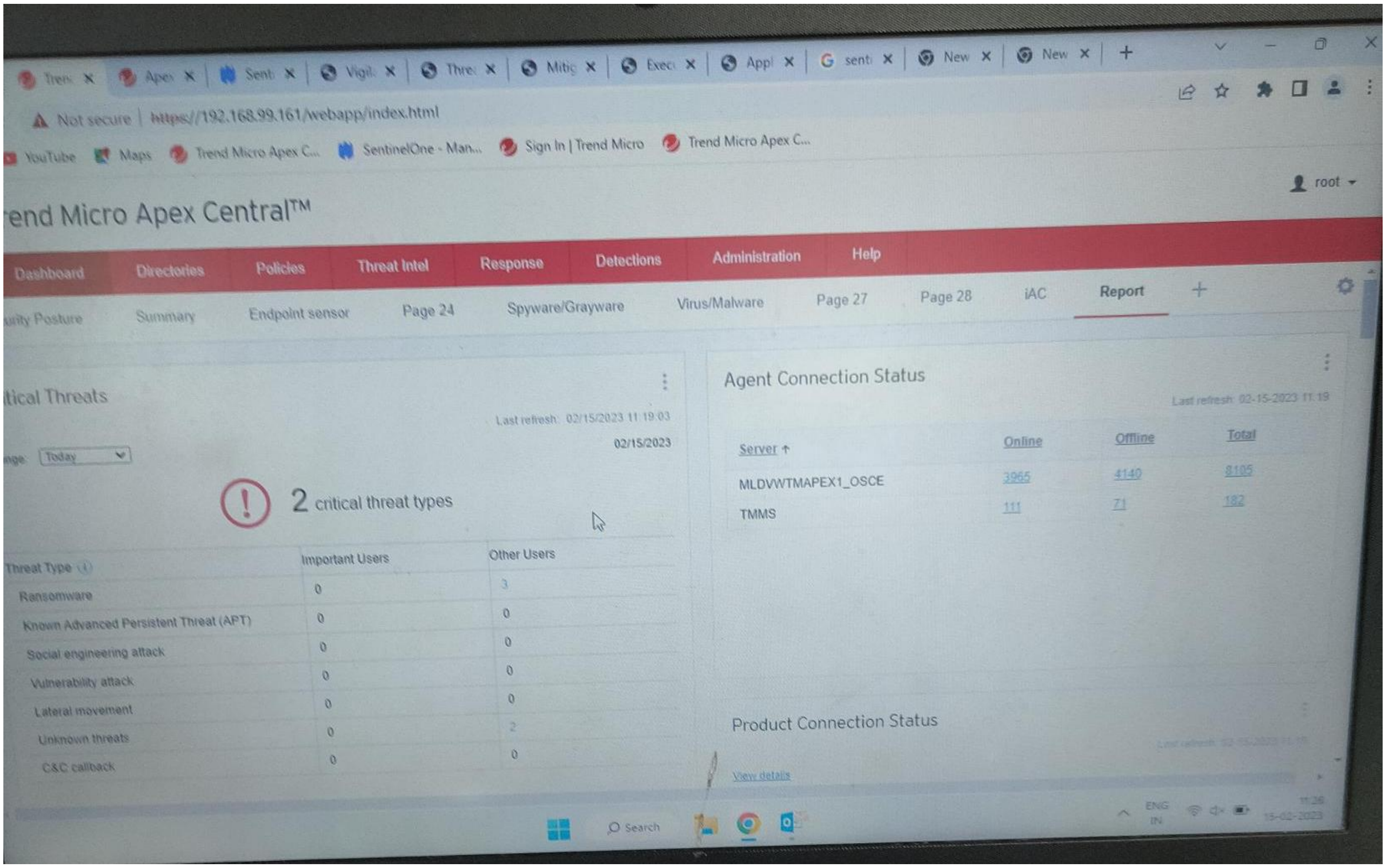


	A	B	C	D	E	F
1	Apex Cen	Issuer	Data Peric	Created Ti	Generated by	
2	test2	root	02/09/202	#########	MLDVWTMEDRAPP	
3	NOTE: All report data containing Apex Central-specific and License-specific information, generates using data from MLDVWTMEDRAPP.					
4	#	Template Name				
5	1	Report Generation				
6	1	test				
7	No data to display					
8	2	rule				
9	#	Pattern/Rule Version	Online	Offline	Active: Se	Grand total
10	1	35.1072.00	2241	911	1	3153
11	2	35.1071.00	21	21	0	42
12	3	35.1049.00	833	440	0	1273
13	4	30.1012.00	3	2	0	5
14	5	2.00009.00	0	0	2	2
15	6	184113.0.0	0	0	3	3
16	7	184113.0.0	4131	3445	0	7576
17	8	183913.0.0	2	269	0	271
18	9	183813.0.0	0	50	0	50
19	10	183513.0.0	4	117	0	121
20	10	Grand total	7235	5255	6	12496
21	3	Product License				
22	#	Product type Activation Code		14	Grand total	
23	1	Full	FI5G2URC!	1	1	

3) Creating a Dashboard In trend Micro

- To create dashboard we need to go and log in to trend me apex central
- In central we can see a tab of dashboard click on it in that we can see a plus icon click on it to create a new dashboard.
- After that we can add widgets to that dashboard by clicking on the setting button on top right of the screen in that we have a option of add widgets click on it. After that we will get a screen where more then 100 widgets are there from which we need to select which all widgets we want in out dashboard.
- After adding the widgets our dashboard is ready and we can see all the data directly.

This is the Dashboard which I created in trend micro.



tical Threats

Last refresh: 02/15/2023 11:19:03

02/15/2023

nge: Today

2 critical threat types

Threat Type	Important Users	Other Users
Ransomware	0	3
Known Advanced Persistent Threat (APT)	0	0
Social engineering attack	0	0
Vulnerability attack	0	0
Lateral movement	0	0
Unknown threats	0	2
C&C callback	0	0

Agent Connection Status

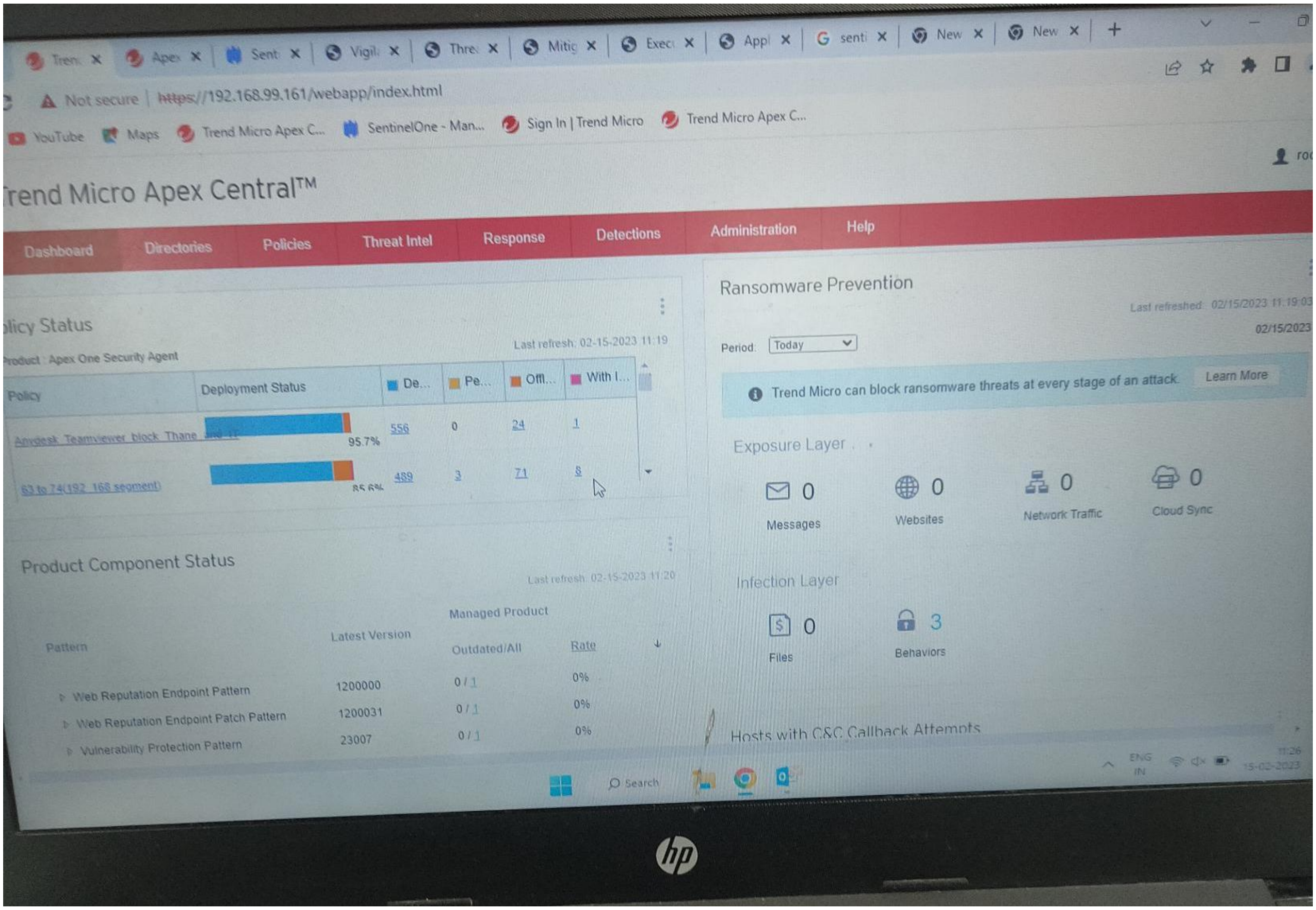
Last refresh: 02-15-2023 11:19

Server ↑	Online	Offline	Total
MLDVWTMAPEX1_OSCE	3965	4140	8105
TMMS	111	71	182

Product Connection Status

View details

In this we are able to check for how many system are online, how many systems have the policies deployed and many more.



licy Status

roduct : Apex One Security Agent

Last refresh: 02-15-2023 11:19

Policy	Deployment Status	De...	Pe...	Offl...	With I...
Anydesk_Teamviewer_block_Thane_and IT	95.7%	556	0	24	1
63 to 74(192_168 segment)	85.6%	489	3	71	8

Product Component Status

Last refresh: 02-15-2023 11:20

Pattern	Latest Version	Managed Product Outdated/All	Rate
Web Reputation Endpoint Pattern	1200000	0 / 1	0%
Web Reputation Endpoint Patch Pattern	1200031	0 / 1	0%
Vulnerability Protection Pattern	23007	0 / 1	0%

Ransomware Prevention

Last refreshed: 02/15/2023 11:19:03

02/15/2023

Period: Today

Trend Micro can block ransomware threats at every stage of an attack. Learn More

Exposure Layer

Messages	Websites	Network Traffic	Cloud Sync
0	0	0	0

Infection Layer

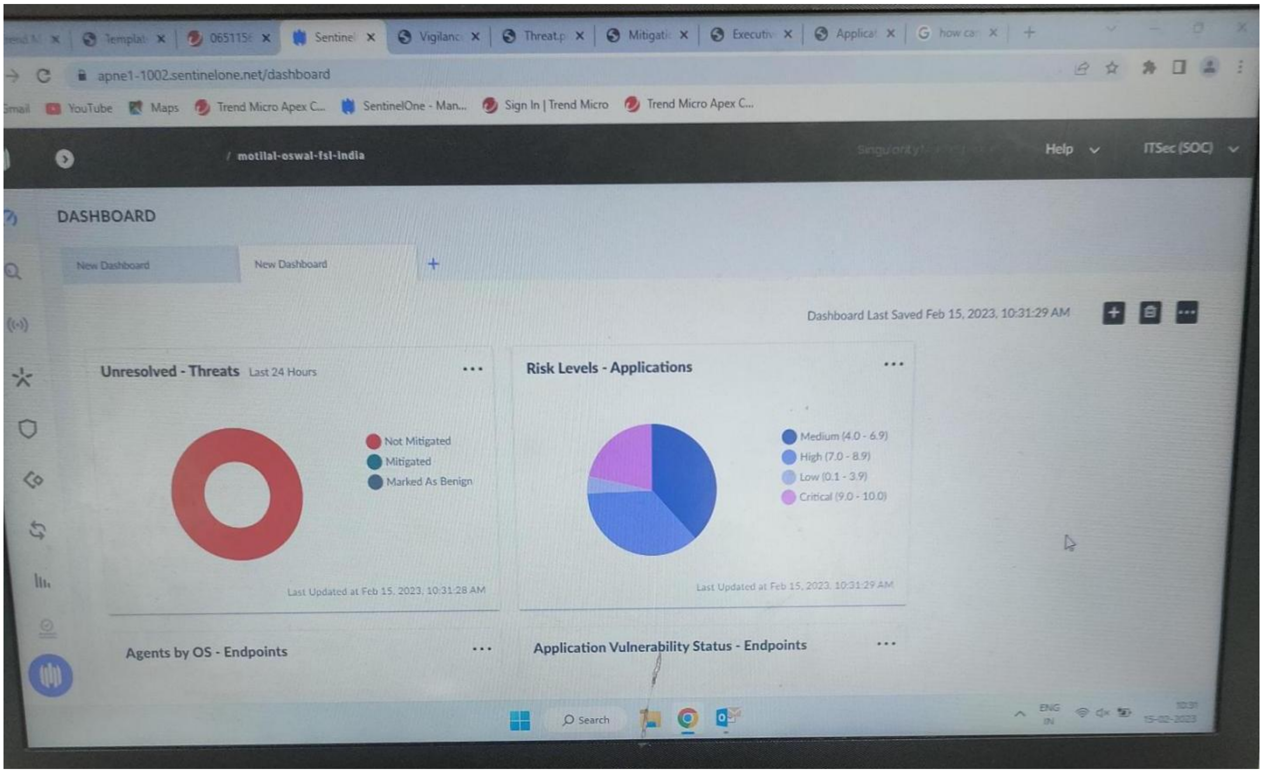
Files	Behaviors
0	3

Hosts with C&C Callback Attempts

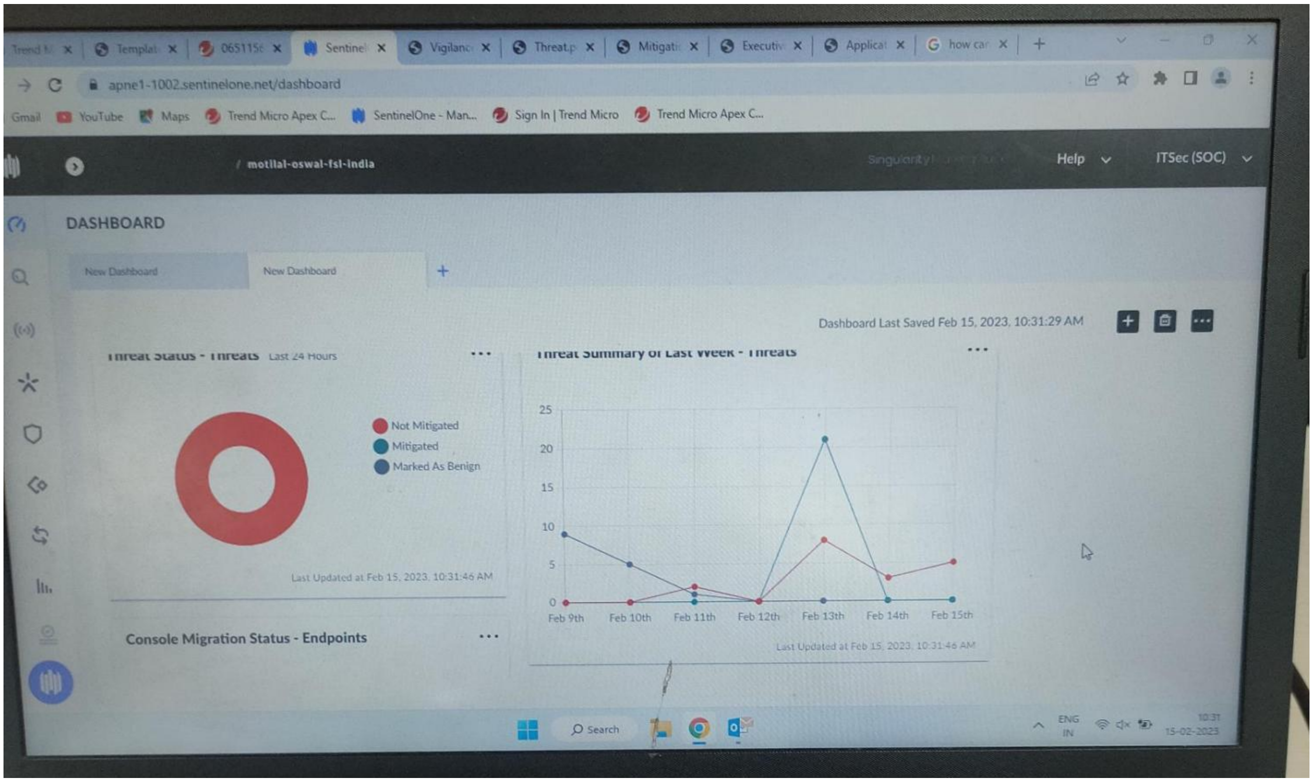
4) Creating a Dash board in Sentinel One

- To create dashboard we need to go and log in to sentinel one
- In sentinel we can see a tab of dashboard click on it we can see a plus icon click on it to create a new dashboard.
- Then we can see a plus option on the top right to ad widgets
- In Widgets we get to see the categories like threats risk endpoints etc in which we need to select which we want and accordingly we will get widgets which we can add.
- After selecting click on save and you will be able to see the widget that you selected on the Dashboard. After adding the widgets our dashboard is ready and we can see all the data directly.[2]

This is the Dashboard which I created in Sentinel One.


apne1-1002.sentinelone.net/dashboard
Gmail YouTube Maps Trend Micro Apex C... SentinelOne - Man... Sign In | Trend Micro Trend Micro Apex C...
/ motilal-oswal-fsl-india
Help
ITSec (SOC)
DASHBOARD
New Dashboard
New Dashboard
Dashboard Last Saved Feb 15, 2023, 10:31:29 AM
Unresolved - Threats Last 24 Hours
Not Mitigated
Mitigated
Marked As Benign
Last Updated at Feb 15, 2023, 10:31:28 AM
Risk Levels - Applications
Medium (4.0 - 6.9)
High (7.0 - 8.9)
Low (0.1 - 3.9)
Critical (9.0 - 10.0)
Last Updated at Feb 15, 2023, 10:31:29 AM
Agents by OS - Endpoints
Application Vulnerability Status - Endpoints
Search
ENG IN
10:31
15-02-2023

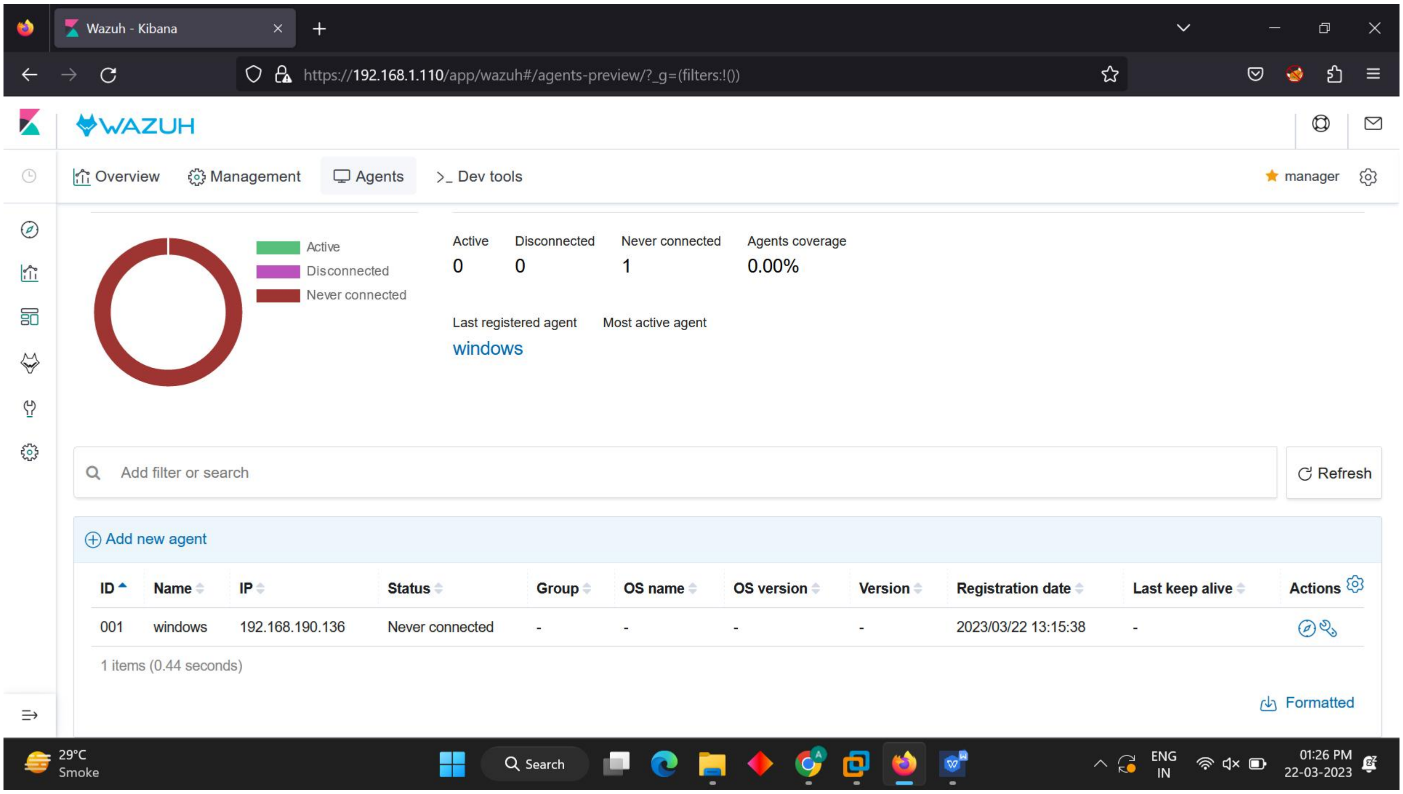
In this we are able to see Agent status, threat detection and many more things.


apne1-1002.sentinelone.net/dashboard
Gmail YouTube Maps Trend Micro Apex C... SentinelOne - Man... Sign In | Trend Micro Trend Micro Apex C...
/ motilal-oswal-fsl-india
Help
ITSec (SOC)
DASHBOARD
New Dashboard
New Dashboard
Dashboard Last Saved Feb 15, 2023, 10:31:29 AM
Threat Status - Threats Last 24 Hours
Not Mitigated
Mitigated
Marked As Benign
Last Updated at Feb 15, 2023, 10:31:46 AM
Threat Summary of Last Week - Threats
25
20
15
10
5
0
Feb 9th
Feb 10th
Feb 11th
Feb 12th
Feb 13th
Feb 14th
Feb 15th
Last Updated at Feb 15, 2023, 10:31:46 AM
Console Migration Status - Endpoints
Search
ENG IN
10:31
15-02-2023

Since I don’t have the allowance to show my work outside my organization so to demonstrate the same this I have created a my own lab set up where I have created Two virtual machine and connect it to the console using a tool called wazuh.[4]

- In this first we need to install Wazuh server on our main system .
- Then we need to configure it with the help of VM ware.
- After that we need to connect systems with wazuh
- To connect we need to install ossec agent on that machine
- Then we need to remote of the wazuh server to add the sytems which we want to scan
- After adding the system we need to run wazuh.

So this is the dashboard of the tool after connecting the system with the console.



Active	Disconnected	Never connected	Agents coverage
0	0	1	0.00%

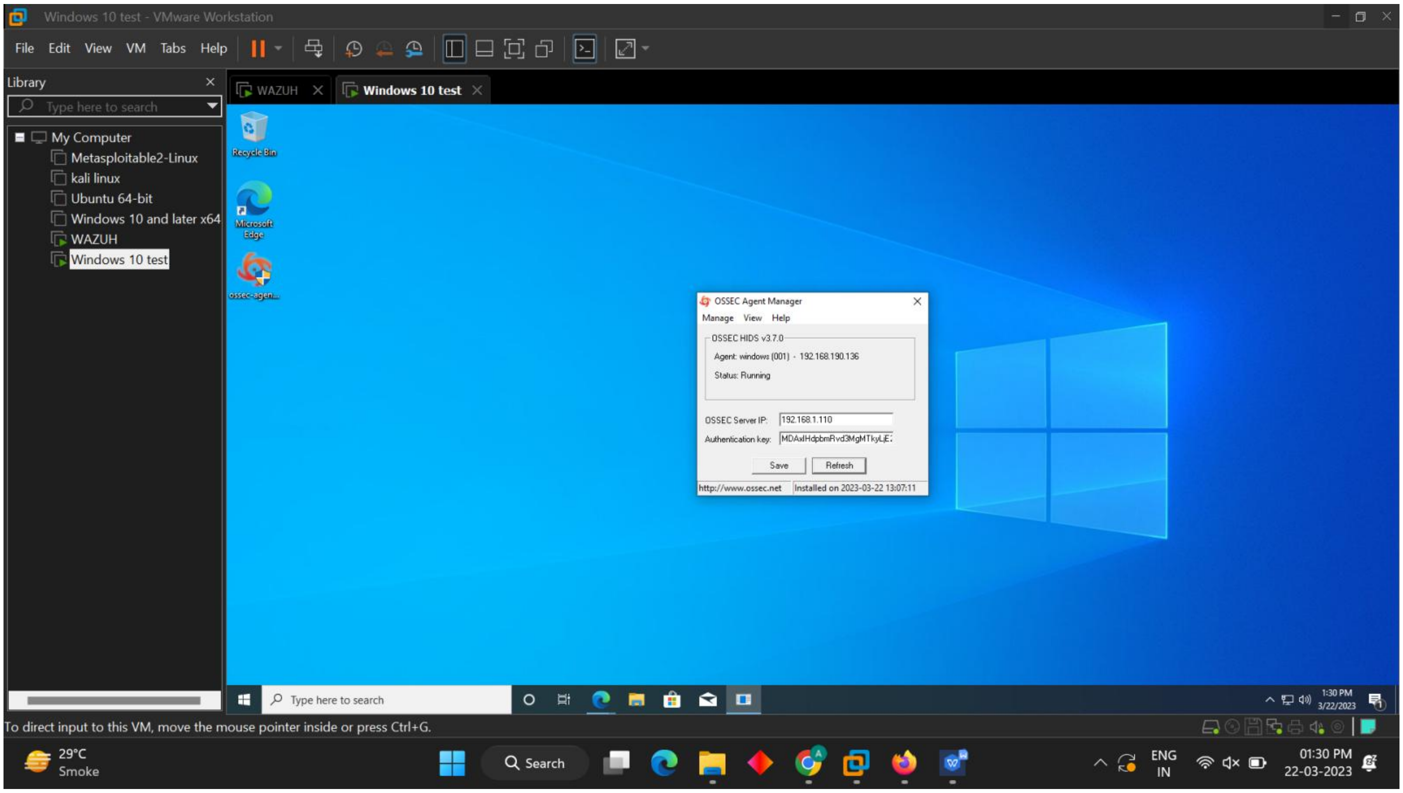
Last registered agent: windows

Most active agent

ID	Name	IP	Status	Group	OS name	OS version	Version	Registration date	Last keep alive	Actions
001	windows	192.168.190.136	Never connected	-	-	-	-	2023/03/22 13:15:38	-	

1 items (0.44 seconds)

This is the virtual system which I have created in which we can see the agent of the tool through which we have connected it with the console.



OSSEC Agent Manager

OSSEC HIDS v3.7.0

Agent: windows (001) - 192.168.190.136

Status: Running

OSSEC Server IP: 192.168.1.110

Authentication key: MDAxIHdpbmRvd3MgMTkyLjE2

http://www.ossec.net | Installed on 2023-03-22 13:07:11

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

CHAPTER 4 : CONCLUSION

In conclusion, IT infrastructure security is a critical component of overall IT security and is essential for protecting an organization's computer systems, networks, and data centers from potential threats and vulnerabilities. Effective IT infrastructure security requires a proactive and ongoing approach to risk management, threat intelligence, and incident response, to identify and mitigate potential security threats and protect against a range of attacks.

By implementing appropriate security controls, such as access controls, network security, endpoint security, data encryption, and backup and disaster recovery planning, organizations can safeguard their critical systems, applications, and data from potential threats and vulnerabilities. This, in turn, helps to maintain business continuity, comply with regulations and standards, and protect against reputational and financial damage.

Overall, IT infrastructure security is a constantly evolving field, with new and sophisticated threats emerging regularly. Organizations must take a proactive approach to IT infrastructure security, continually assessing their security posture, identifying vulnerabilities, and implementing appropriate security controls to protect against potential attacks.

REFERENCES

1) https://www.trendmicro.com/en_us/business.html

2) https://www.sentinelone.com/platform/?utm_content=demo-request&utm_medium=paid-search&utm_source=google-paid&utm_campaign=apj-anz-en-g-s-brand&utm_term=Sentinelone&utm_campaignid=19538119170&gclid=Cj0KCQjwocShBhCOARIsAFVYq0heOg64z-6rXrG2hw96iXW3g-zNPssb4pdEa9-6CCcpLvHDdEbpdzEaAo_kEALw_wcB

3) https://www.techotopia.com/index.php/IT_Infrastructure_Security

4) https://wazuh.com/

5) https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works

6) https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/shift-in-atm-malware-landscape-to-network-based-attacks