IBM Project Report
On
Deployment of Endpoint Detection and Remediation for Secure Financial Applications

Developed By: -
Patel Priyanshu Bansibhai (18162171021)
Soumya Mukherjee (18162171028)
Vyas Nihar Vipul (18162171034)

Guided By:-
Prof. Kunal Garud(Internal)
Mr. Ashwin Thandani (IBM Remote Mentor)

Submitted to
Department of Computer Science & Engineering
Institute of Computer Technology

Year: 2022

CERTIFICATE

This is to certify that the **IBM** Project work entitled **"Deployment of Endpoint Detection and Remediation for Secure financial Applications"** by Patel Priyanshu Bansibhai (18162171021), Soumya Mukherjee (18162171028) and Vyas Nihar Vipul (18162171034) of Ganpat University, towards the partial fulfillment of requirements of the degree of Bachelor of Technology – Computer Science and Engineering, carried out by them in the CSE(CS) Department. The findings contained in this Project have not been submitted in part or full to any other University / Institute for award of any other Degree/Diploma.

Name & Signature of Internal Guide

Name & Signature of Head

Place: ICT - GUNI

Date:

ACKNOWLEDGEMENT

IBM project is a golden opportunity for learning and self- development. We consider ourselves very lucky and honoured to have so many wonderful people lead us through in completion of this project. First and foremost, I would like to thank Dr. Hemal Shah, Principal, ICT, and Prof. Dharmesh Darji , Head, ICT who gave us an opportunity to undertake this project. My grateful thanks to Prof. Kunal Garud, Mr. Ashwin Thandani (IBM Remote Mentor) for their guidance in project work Endpoint Detection and Remediation for a financial application, who despite being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where would have been without his help. CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

Patel Priyanshu Bansibhai (18162171021)
Soumya Mukherjee (18162171028)
Vyas Nihar Vipul (18162171034)

ABSTRACT

In this growing age of technology, every single banking services has stepped towards online platform making it easier for people to access their assets and control their finances. At the very same time, increasing growth in cyber threats has also emerged, risking any application that's online. We are gaining hands-on experience on a industry grade endpoint security and detection tool which provides multiple layers of security along with threat intelligence. This would help us in knowing current industry practices, how they manage endpoints, reporting and a full hand's on experience on the tools.

INDEX

Title **Page No**

CHAPTER: 1 PROJECT BACKGROUND

CHAPTER 1 PROJECT BACKGROUND

Initially this project was supposed to be a coded product which was intended to solve the issue of end point security and remediation for financial applications. First two weeks were planned accordingly, and team started the work.
Upon completion of time, when all data was gathered, we faced some difficulties, such as:

- Unable to find a proper financial application to base our project on.
- Facing an issue with cloud implementation of the project, especially hosting it IBM cloud, since we are limited to one instance for a limited time period whereas this project aims at having 3 different servers to work at once.

On very next day, team had an IBM Mentor meeting, where all the difficulties were presented, and then team got proposed with a change of approach by mentor.
Approach 1: Continue coding the product and try to reduce as much errors possible, but at same time this approach would consume huge amount of time.
Approach 2: Get hands-on experience on industry grade EDR tool, which provides similar solution to the problem statement. This approach was time effective and would help us learn more.

Team thereby chose Approach 2 and entire report is prepared on the basis of Approach 2.

CHAPTER: 2 INTRODUCTION

CHAPTER 2: INTRODUCTION

In this modern epoch every industry is going online and finance industry is no left. In India 41 million transactions per day is happening. Despite spending many millions of rupees on security, financial services organizations continue to be one of the top targets for cybercriminals. The access to the vast amounts of money that the financial industry trades and controls, along with the sensitive personal information they store, continues to make them a prime target. Whilst digital transformation is offering many advantages in driving business forward, it also provides more opportunities for attackers. As well as the increase in number of attacks, the attacks themselves are becoming more complex and targeted, so financial organizations must therefore assume they will be attacked and prepare accordingly.

Endpoint Detection and Response (EDR) can provide real-time detection, identification and response to threats:

Signature-less attacks: unlike conventional solutions like AV, EDR uses AI, machine learning, and behavioural analysis, to detect suspicious behaviour.
File-less attacks: evasive attacks often leverage whitelisted Windows applications to create damage, in a completely file-less fashion so EDR solutions analyze behaviours instead of evaluating files.
Low and slow attacks: EDR solutions aggregate endpoint data and continually analyze it, correlating suspicious individual activities, to then identify a multi-stage attack. This means they can detect “low and slow” attacks which often go undetected.

CHAPTER: 3 PROJECT SCOPE

CHAPTER 3: PROJECT SCOPE

This hand's on experience report is limited to Bitdefender GravityZone Ultra, Comodo Dragon and WithSecure, although brief information about other tools will be given.

CHAPTER: 4 SOFTWARE AND HARDWARE REQUIREMENTS

CHAPTER: 4 SOFTWARE AND HARDWARE REQUIREMENTS

Minimum Hardware Requirements

Processor	I5 2.0 GHz
RAM	8 GB
HDD	40 GB

Table 3.1 Minimum Hardware Requirements

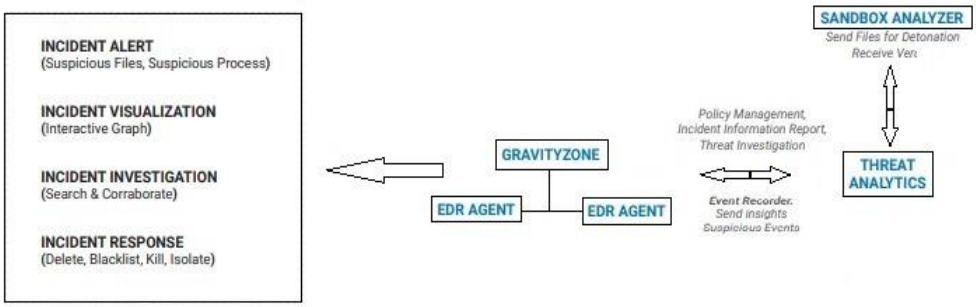
Minimum Software Requirements

Operating System	Any operating system which can support an internet browser.
Programming language	-
Other tools & tech	Internet browser

Table 3.2 Minimum Software Requirements

CHAPTER: 5(A)-PROCESS MODEL (BITDEFENDER

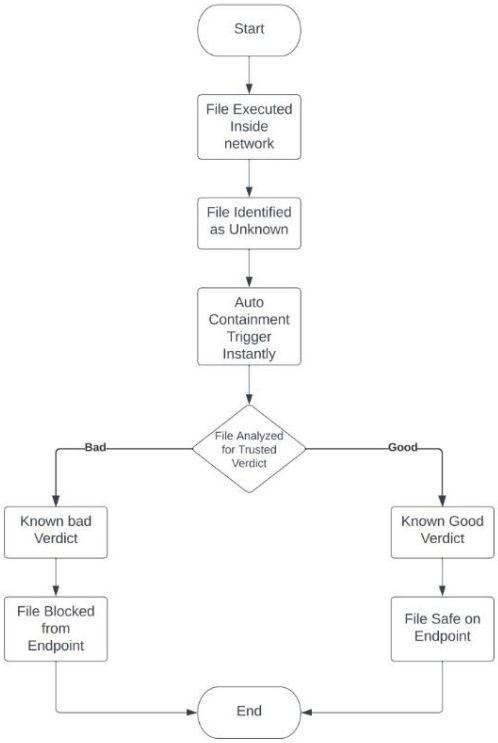
CHAPTER: 5(A)-PROCESS MODEL (BITDEFENDER)



- Once endpoint is connected with panel, any sort of unusual activity detected will create an incident alert.
- Incident alert then will be sent to Gravityzone firewall for further process, from where it will go through policy management, incident information report and threat investigation,
- From threat analytics it goes to sandbox analyser for testing its behaviour and later the report is transferred back to Gravity zone firewall endpoints.
- Finally, it shares the outcome in end user clients and also logs the stuff, and reports it in dashboard.

CHAPTER: 5(B)- PROCESS MODEL (COMODO)

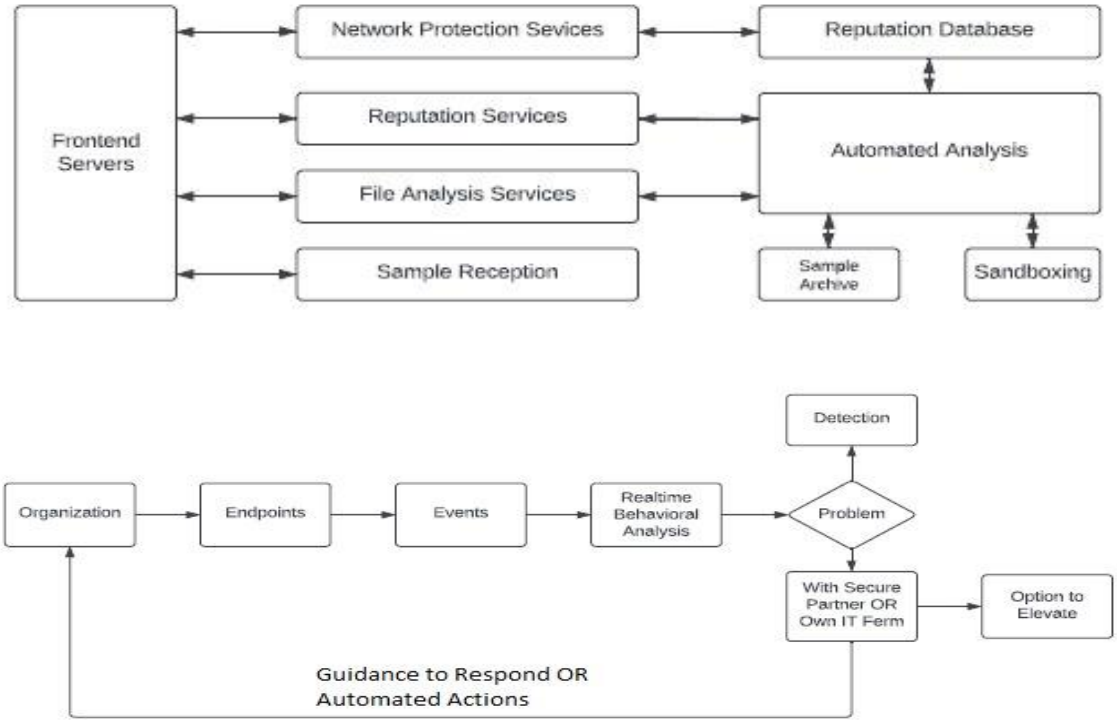
CHAPTER: 5(B)- PROCESS MODEL (COMODO)



- Once a file is executed in client, instantly Comodo client starts observing the file
- If the file gets identified as unknown as in if its sources are unknown or the way of execution if different file gets marked as "unknown threat to system" until it completes execution.
- Auto Containment triggers to control its effect on client meanwhile an analysis on trusted verdict goes on.
- If file appears to be good no harmful effect it gets marked as safe and out from quarantine otherwise it gets wiped out from client.

CHAPTER 5 (C) – PROCESS MODEL (WITHSECURE

CHAPTER 5 (C) – PROCESS MODEL (WITHSECURE)



- WithSecure Client keeps monitoring client devices for any sort of abnormal behaviour or breach of policy or tampering with files.
- In case, any network attack gets detected, Network Protection Service takes care of it, directs the traffic to its Automated Analysis system which then filters out any possible attacks and lets genuine requests pass through without interfering operations.
- File Analysis system takes care of any malicious file being downloaded / found in system, quickly quarantines it and run a full scan on it. Later presents all the malware data on portal and making sure the client is secured.
- One of its highlight features is to elevate an issue to higher ups / admins in an organization if any unwanted events gets triggered apart from automated response system acting on it.

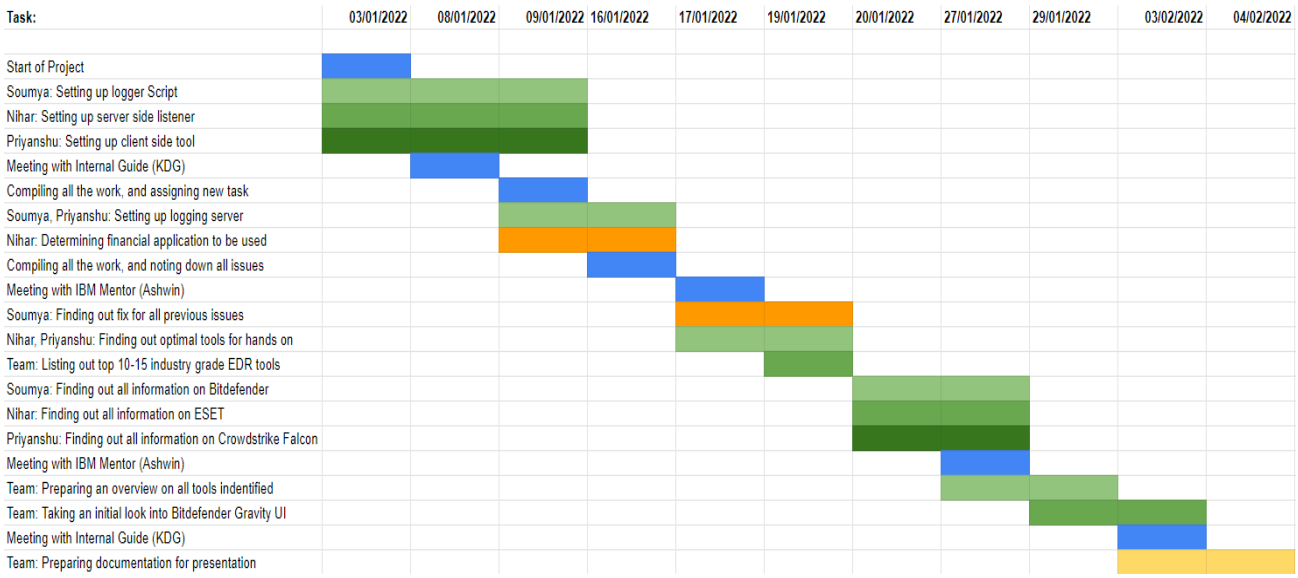
CHAPTER 6 - PROJECT PLAN (TIMELIN

CHAPTER 6 - PROJECT PLAN (TIMELINE)

Task (03/01/2022 – 04/02/2022):

Soumya: Setting up logger Script
Nihar: Setting up server side listener
Priyanshu: Setting up client side tool
Compiling all the work, and assigning new task
Soumya, Priyanshu: Setting up logging server
Nihar: Determining financial application to be used
Compiling all the work, and noting down all issues
Soumya: Finding out fix for all previous issues
Nihar, Priyanshu: Finding out optimal tools for hands on
Team: Listing out top 10-15 industry grade EDR tools
Soumya: Finding out all information on Bitdefender
Nihar: Finding out all information on ESET
Priyanshu: Finding out all information on Crowdstrike Falcon
Team: Preparing an overview on all tools indentified
Team: Taking an initial look into Bitdefender Gravity UI
Team: Preparing documentation for presentation

Timeline:



Task (07/02/2022 – 11/03/2022):

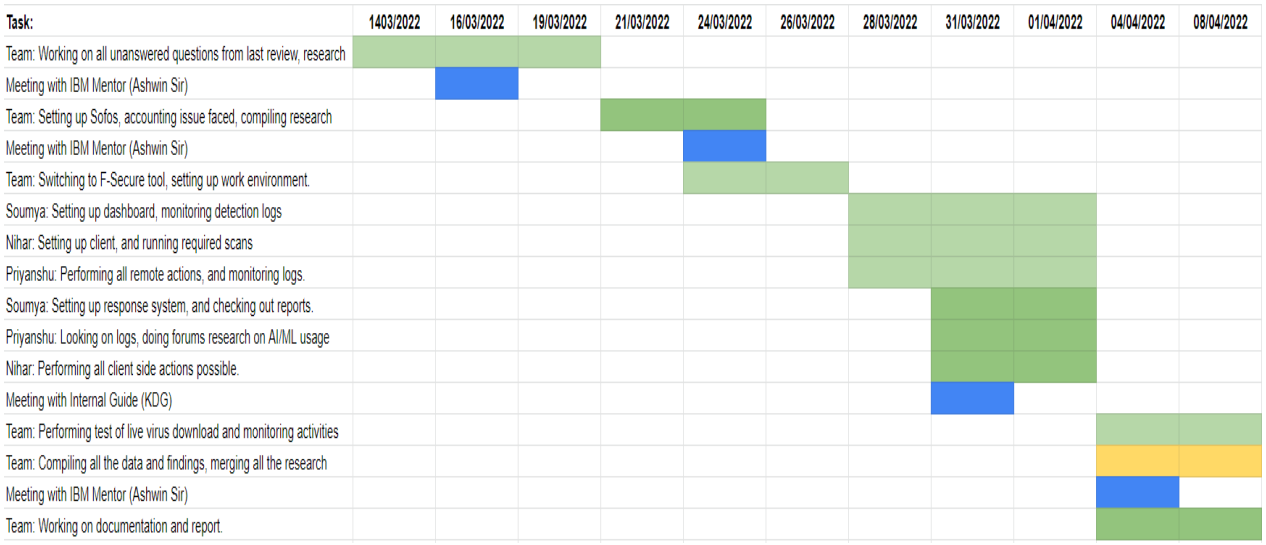
Soumya: Working on sandbox analyzer
Nihar: Working on testing out client side threat protection
Priyanshu: Constantly monitoring logs, reporting & dashboard
Meeting with IBM Mentor (Ashwin Sir)
Team: Compilation of data, and switiching to Comodo
Nihar: Setting up Comodo client, and performing required scans
Priyanshu: Endpoint device profiling, monitoring logs for same.
Soumya: Setting up Comodo control panel, adding users
Team: Compilation of data, and preparring new tasks for next week
Soumya: Working on remote patch management, and antivirus
Nihar: Client auto quarantine file system, threat management
Priyanshu: Remotely performing admin actions on data generated from client.
Meeting with IBM Mentor (Ashwin Sir)
Team: Compilation of findings, working on points given by mentor
Soumya: Testing out Valkyrie an advanced protection layer
Nihar: Checking out security sub systems available for client
Priyanshu: Checking out Application & Device control from panel
Meeting with Internal Guide (KDG)
Meeting with IBM Mentor (Ashwin Sir)
Team: Compilation of all work and properly documenting it
Team: Preparing for a demonstration scenario for review
Team: Working on required documentation
Nihar: Finalising testing and findings on client
Soumya: Finalising findings on Valkyrie and difference b/w both tools
Priyanshu: Finalising findings on all logs and remote actions performed
Meeting with IBM Mentor [LIVE DEMO] (Ashwin Sir)

Timeline:

Task (14/03/2022 – 08/04/2022):

Team: Working on all unanswered questions from last review, research
Meeting with IBM Mentor (Ashwin Sir)
Team: Setting up Sofos, accounting issue faced, compiling research
Meeting with IBM Mentor (Ashwin Sir)
Team: Switching to F-Secure tool, setting up work environment.
Soumya: Setting up dashboard, monitoring detection logs
Nihar: Setting up client, and running required scans
Priyanshu: Performing all remote actions, and monitoring logs.
Soumya: Setting up response system, and checking out reports.
Priyanshu: Looking on logs, doing forums research on AI/ML usage
Nihar: Performing all client-side actions possible.
Meeting with Internal Guide (KDG)
Team: Performing test of live virus download and monitoring activities
Team: Compiling all the data and findings, merging all the research
Meeting with IBM Mentor (Ashwin Sir)
Team: Working on documentation and report.

Timeline:



Basic monthly strategy team was following:
Week 1 - setting up client with dashboard

Week 2 - setting up new rules /policy. Exploring the dashboard and mapping out all the possible logs. Letting the client generate some logs. Includes finding bugs in client / scanning logs.

Week 3 - exploring all client actions, client-based logs, client-based issue/quarantine.

Week 4 - remote operations, cloud sandbox tool, networking tool, contamination, and any new observation tools.

Apart from this week wise data compilation and catching up with new findings are done on weekends.

CHAPTER 7 (A) – DATA GATHERING

- In order to find out best EDR tool with maximum benefits, team did a research on all the available tools currently being used in industry. On base of this research we went with Bitdefender.

- **Features List:**

Features	VMware Cardon Black	Kaspersky EDR	Palo Alto Networks Traps and Cortex	Bitdefender GravityZone Ultra
User Behavioural detection				
Automated Remediation				
Vulnerability monitoring				
Device Control				
Analyst Workflow				
Guided Investigation				
Threat intelligence feed integration				
Custom rules				
Advanced threat hunting				
Unauthenticated device discovery				
Demo	Not Available	Company Demo Only	Company Demo Only	Available
	Hands-on activity	Add on cost	Available on same cost	Not Offered

Features	BlackBerry Cylance	Check Point Sandblast	ESET Enterprise Security	F-secure
User Behavioural detection				
Automated Remediation				
Vulnerability monitoring				
Device Control				
Analyst Workflow				
Guided Investigation				
Threat intelligence feed integration				
Custom rules				
Advanced threat hunting				
Unauthenticated device discovery				
Demo	Company Demo Only	Company Demo Only	Company Demo Only	Available
	Hands-on activity	Add on cost	Available on same cost	Not Offered

Features	SentinelOne	Symantec Endpoint Security Complete	Trend Micro Apex One	Microsoft Defender ATP
User Behavioural detection				
Automated Remediation				
Vulnerability monitoring				
Device Control				
Analyst Workflow				
Guided Investigation				
Threat intelligence feed integration				
Custom rules				
Advanced threat hunting				
Unauthenticated device discovery				
Demo	Company Demo Only	No Demo	Company Demo Only	Only for Microsoft Windows
	Hands-on activity	Add on cost	Available on same cost	Not Offered

Features	McAfee MVISION	CYNET	Cybereason	Comodo Dragon
User Behavioural detection				
Automated Remediation				
Vulnerability monitoring				
Device Control				
Analyst Workflow				
Guided Investigation				
Threat intelligence feed integration				
Custom rules				
Advanced threat hunting				
Unauthenticated device discovery				
Demo	Company Demo Only	No Demo	Company Demo Only	Only for Microsoft Windows
	Hands-on activity	Add on cost	Available on same cost	Not Offered

CHAPTER 7 (B) – OUR FINDINGS

Bitdefender GravityZone Ultra VS Comodo Dragon

Bitdefender and Comodo both use cutting-edge detection technology; however, Bitdefender concentrates on extra features while Comodo maintains a lightweight, streamlined service.

Bitdefender provides protection against a wide range of threats. The Safe File Vault protects you from malware, while the Webcam Shield keeps hackers out of your stream. A Virtual Keyboard and a Password Manager are among the features that help safeguard your passwords. Bitdefender will also scan any new hardware you connect to your device, such as USB devices and external storage, to ensure you don't get infected. Unfortunately, all of these capabilities can cause your smartphone to slow down. While the auto-updates help to mitigate this effect, it remains a significant issue.

While Comodo's extra security capabilities are limited, it does employ unique techniques to enhance its security. Its sandboxing technology places all files in a virtual environment to ensure their security. It also employs cloud-based whitelisting to ensure that no downloads are checked more than they need to be. If it detects a problem, the Application Control locks down your system and only uses apps that are recognized to be safe.

WithSecure

WithSecure Endpoint Security is an AI-powered, cloud-native endpoint protection solution that you can deploy and manage from a single console. It protects your firm from modern threats like ransomware, never-before-seen malware, and zero-day vulnerability exploits by working across all of your endpoints.

From vulnerability management to collaborative protection to endpoint protection, detection, and response, it handles everything from a single security panel. Individual solutions can be employed for specific needs, or all of them can be combined for complete protection. For each attack detected, you'll receive a forensics flow chart that shows the threat's origin (as far as WithSecure can tell) and data for each step taken.

Our findings:

- Client tool seems to be lag free for most parts, have an exceptional detection system which auto detects and quarantines a file keeping the client secure.
- Best part about this tool, is in its dashboard. The in-depth malware analysis it does, giving a flow chart for each attack.
- Auto detects any temp file, downloaded file, files over USB or old malicious files instantly and quarantines them.

So, which one is best?

- Comodo is by far the most practical solution we have tested in terms of its execution and antivirus layers. Although, it makes client slightly lagging because of its own services running.
- BitDefender is by far the best UI, light weight EDR solution we have tested. Gives proper remote controls, executive summary is on point, network discovery, proper contamination of malicious files. Although it’s on a bit expensive side, customer support is not great.
- WithSecure seems to sit right between Comodo and Bitdefender in terms of background performance on client. It has a unique way to show malware analysis from previous scans, client-side monitoring is better and so are the detection logs. Although, it seems to have a lot of features to be locked under full premium mode which makes it sit right in between Comodo and BitDefender.

CHAPTER 7 (C) – COMPARISION

CHAPTER 7 (C) – COMPARISION

Throughout our experience we have gathered all information related to EDR, there performance, impact on client device, threat protection system, etc. After analyzing every observation on all three tools i.e. BitDefender GravityZone Ultra, Comodo Dragon and WithSecure. we came down to the following comparison:

- **Admin web portal, quick glance:**
  Bitdefender has the cleanest and most organized web portal among all three tools. It's UI is user friendly, looks better and has quick response times. Moreover, the executive summary of Bitdefender is better followed by Comodo and then followed by WithSecure.

- **Client Tool and it's functionality:**
  WithSecure offers the lightest Client tool among all three. It's easy to install requires no manual scan to begin with and has a quicker detection. It also allows client to see logs, malware details and check containment files. Where it lacks is giving the client any virtual environment solution to execute any malicious file without flagging it off from system / turning the real time protection off.

  Comodo on other hand is a resource heavy client tool which needs a lot of processing power to run all the services it offers and at the same offers the maximum client options among all three. It gives client a full control over scan logs, quarantine files, options to restore them or remove them completely from server, provides a virtual environment for script execution, automatically runs any slightly malicious script on its safe zone, network discovery and rest all features are similar.

  Bitdefender comes with a heavy client but it's not resource hungry, it's well optimized and sit's right in between WithSecure and comodo in terms of response time, UI, usability and so on.

- **Threat Detection System:**
  Comodo has the best threat detection system among all three, also has a bit of a tendency to false flag non malicious files as malicious. It uses a filebase system to flag files as malicious. It tries to make a similarity index between it's own records and given file, if it gets any match over 5% file gets flagged as malicious or not safe to run on client and gets transferred on virtual environment.

  WithSecure has the next quickest threat detection after comodo (in terms of fraction of seconds) although it has a side effect, WithSecure doesn't flags ZIP files as threat or malware unless they have been scanned separately, which is not the case with other two tools. Threat detection of WithSecure gives a very detailed malware history and study if one wishes to look more in logs.

  BitDefender uses a sandbox analyzer method to counter act with any malicious files, normal file detection is quick and it flags any malicious files enters the system and so on. It doesn't have a detailed malware analysis but offers almost similar threat detection like other tools. It uses it's own client collected data of file activity as detection layer.

  Note: All tools have a great threat detection system deployed which uses AI/ML techniques to filter files and perform automated actions, this comparison is more directed towards finding any difference among three tools we used.

- **Malware Analysis:**
  Being a Cyber Security student, we really wish to know more about a malware or malicious file

that may have entered through the client, in terms of extensive malware analysis and summary, WithSecure is the best one among them, it has a flowchart view which shows the route map of malware, and details like SHA value, hash value, first found, and more details similar to virustotal.com.

Followed by Comodo and Bitdefender both has a better malware analysis, because of there antivirus system which pulls out few details of malicious files from CVE MITRE records.

- **Remote Actions from web portal to clients:**
  Comodo has the maximum remote client actions possible such as remote desktop, remote restart, remote security update, remote package updater, file transfer dashboard etc.

  Bitdefender is second in line with remote features, it allows remote file transfer, basic remote scans, remote restart and remote security update.

  WithSecure has the most limited remote features, it only allows remote restart and remote security updates.

So overall if we have to select one, then it will be Comodo Dragon as it comes with almost every feature one needs from EDR tool, along with its wide features over admin panel and client.

We recommend:
Comodo Dragon > WithSecure > BitDefender GravityZone Ultra

CHAPTER 8 – CHALLENGES FACED

CHAPTER 8 – CHALLENGES FACED

During this entire project, we faced a lot of challenges, below is the list of those with how we passed them and what actions we took.

1. Running an active server for client listeners.

- Initially we were working on coding a tool to perform Endpoint protection and remediation. We faced an issue with linking client with server, since we were not having any server system to hook them up for proper listening mode. Upon few trials it appeared that IBM server or any other server system is off limits.

2. Finding a financial application

- We tried a variety of financial apps, web apps, projects made by various developers but none were actually meeting our requirements for the project. Later we chose to work with Altoro Mutual vulnerable webapp as our financial tool.

3. Change of approach

- It appeared to us that we were spending a lot of time just to figure out some technical issue we were facing such as lack of a proper working server and database system. Plus building an Industry level EDR tool seems to be off the limits for a project to be done in 4 months, upon having a thorough discussion with our Mentors we switched to a different approach were we started taking hand's on experience of Industry grade EDR tools and document our experience.

4. Getting a Trial for EDR tools

- According to our research we got over 30 tools on our watch, upon which of course we picked top 10 to consider working on. So, we started from No. 1 tool and ran into an issue of not getting any remote instant trial option, so we kept switching and applying for trials on multiple tools till we reach No. 4 tool Bitdefender which offered the trial and our project started.

5. Client devices

- Very important part of testing an EDR solution is having a proper client device which can hold all the services one tool has to run and still perform for normal tasks. It was hard for us to setup on entry level laptops we had, hence setting up a client became a challenge as it was continuously spiking the processor usage on devices. We fixed the issue by setting a desktop client with a higher specification, which was then able to handle all the services. Only limitation with this scenario was it can only be reached remotely and one of our team members has to completely dedicate his time on setting up client.

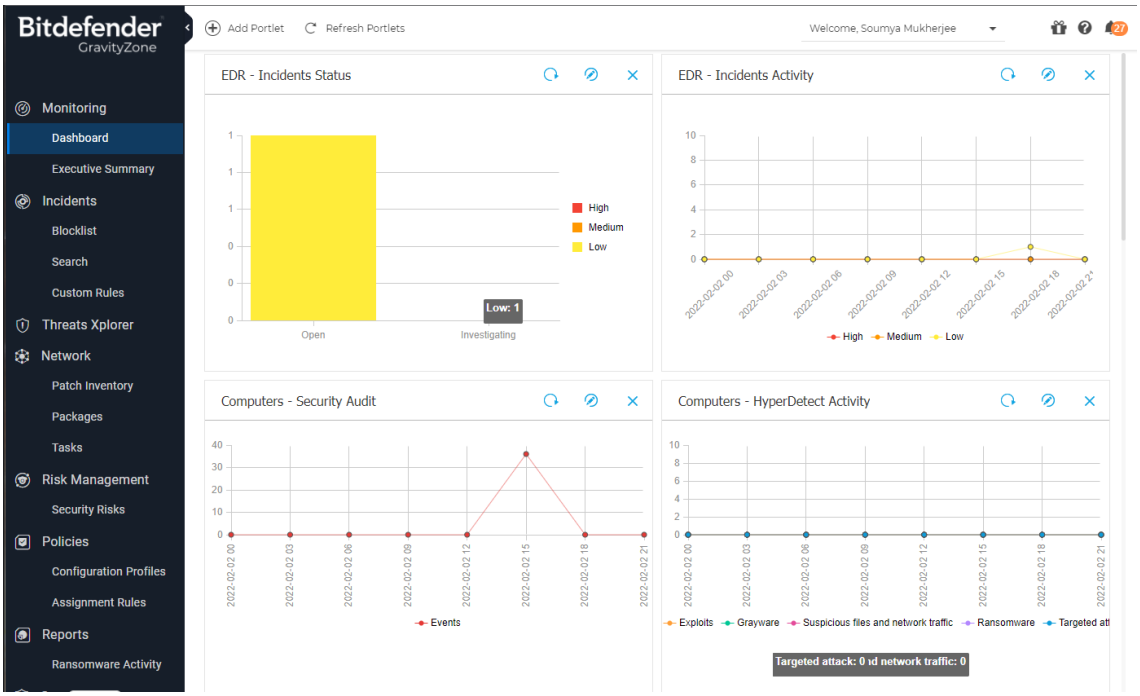
6. Finding technical answers

- When we take hands on experience on readymade industry grade tools, it's really difficult to know how they are actually processing all the background work. Like managing logs, threat detection, remote client handling and so on. We somehow overcame this issue by doing intensive research on their forums, emailing their teams, and web searches to get very detailed information.

CHAPTER 9 (A) – IMPLEMENTATION (BITDEFENDER)

CHAPTER-9 (A) IMPLEMENTATION (BITDEFENDER)

- Initial experience, on start-up you will find dashboard:

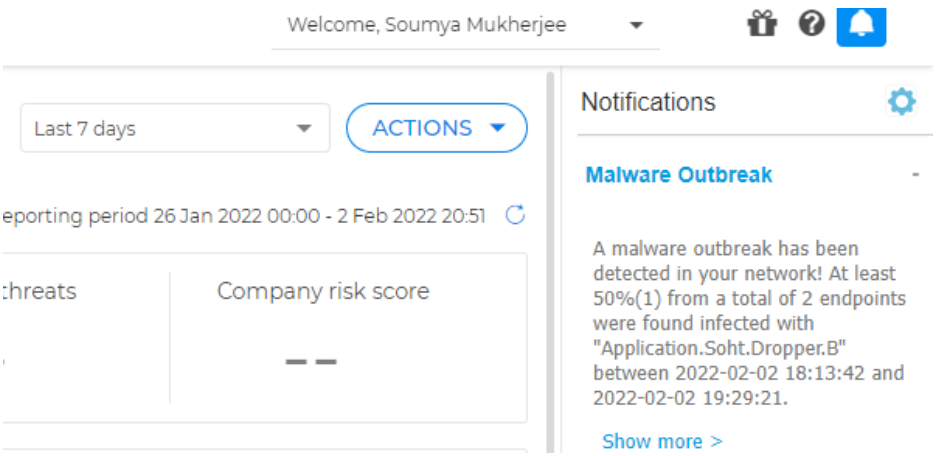


Contains data like:

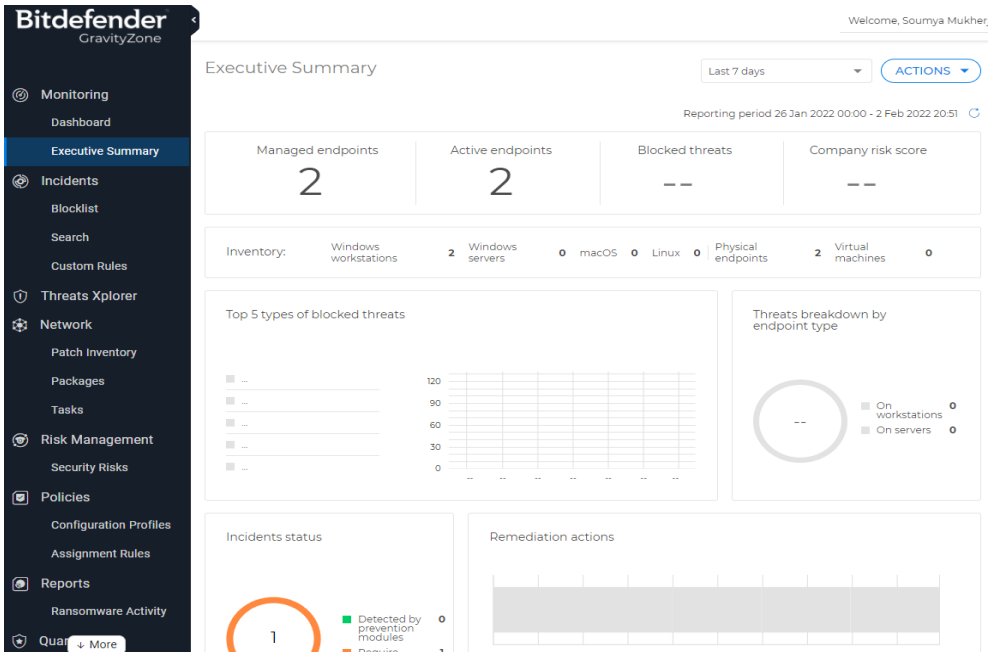
EDR:
Incident Status
Incident Activity

Computers:
Security Audits
HyperDetect Activity

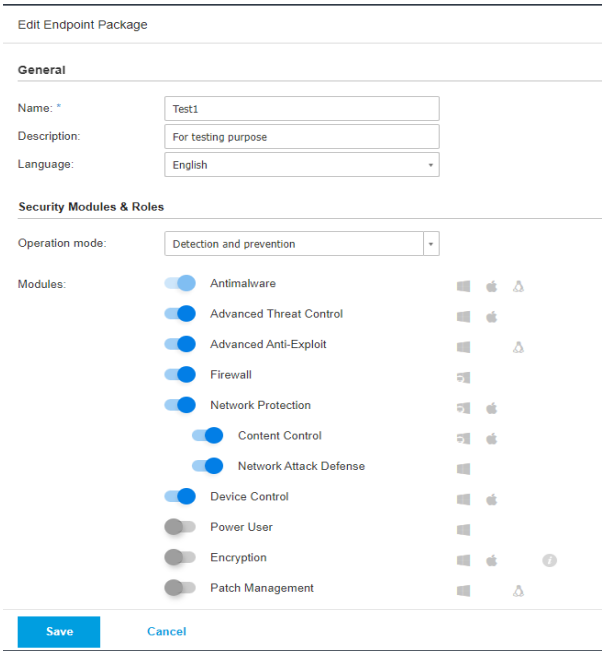
- Up at right side corner, we have user logged in, followed by notification tab, for example: here we have a malware outbreak notification.

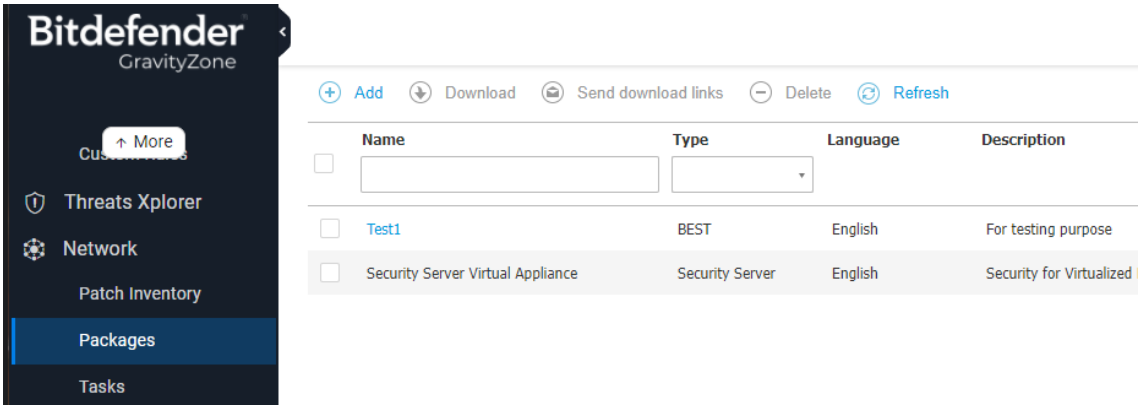


- Next, we have Executive Summary, it contains all data like clients registered, clients active, overall threats detected, top 5 types of threats and so on.

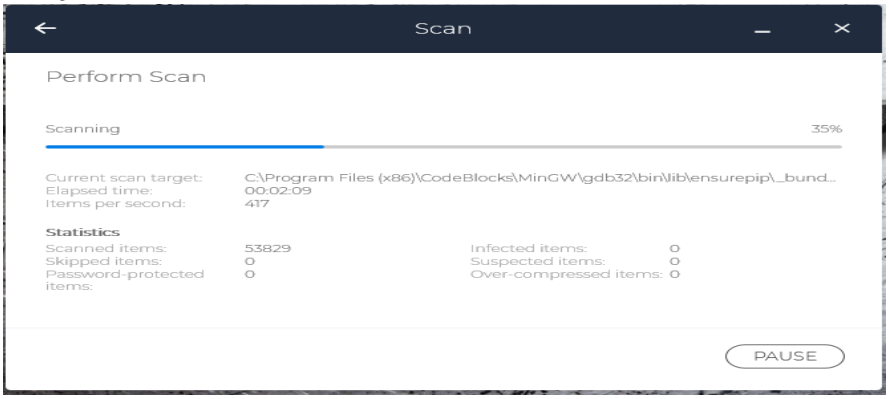


- Setting up clients, it's really easy to setup clients, in Network > Packages tab, one can setup a client package and then share the download link to register the endpoint.

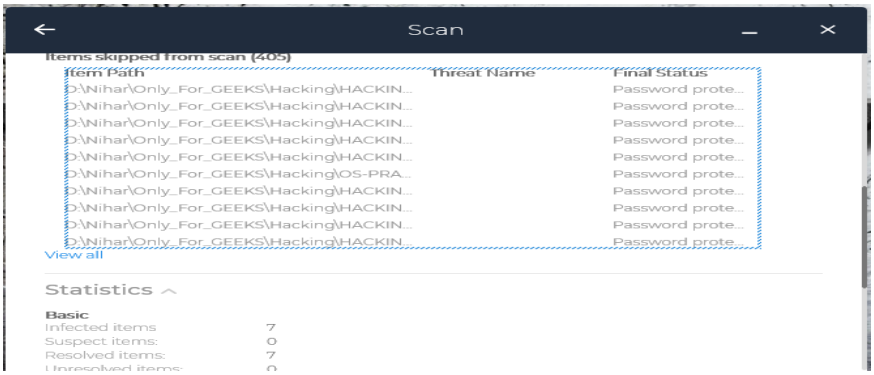




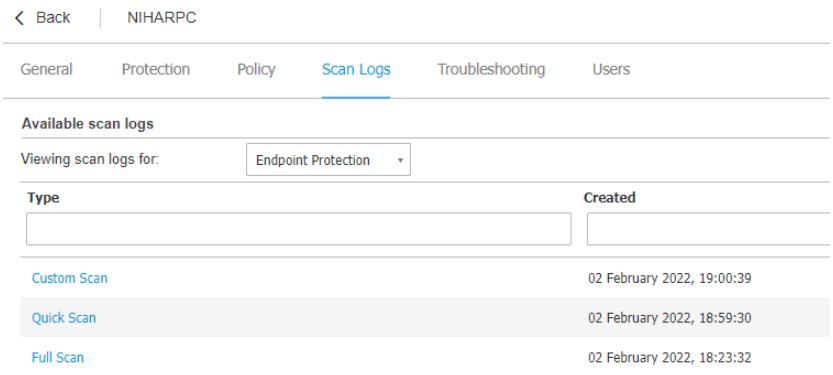
- Once client is ready, perform a full scan to initialize a report, for the endpoint.
- Scan can be a Quick / Custom / Full scan.



- Once a scan is done, the report for same is displayed in client as well as portal

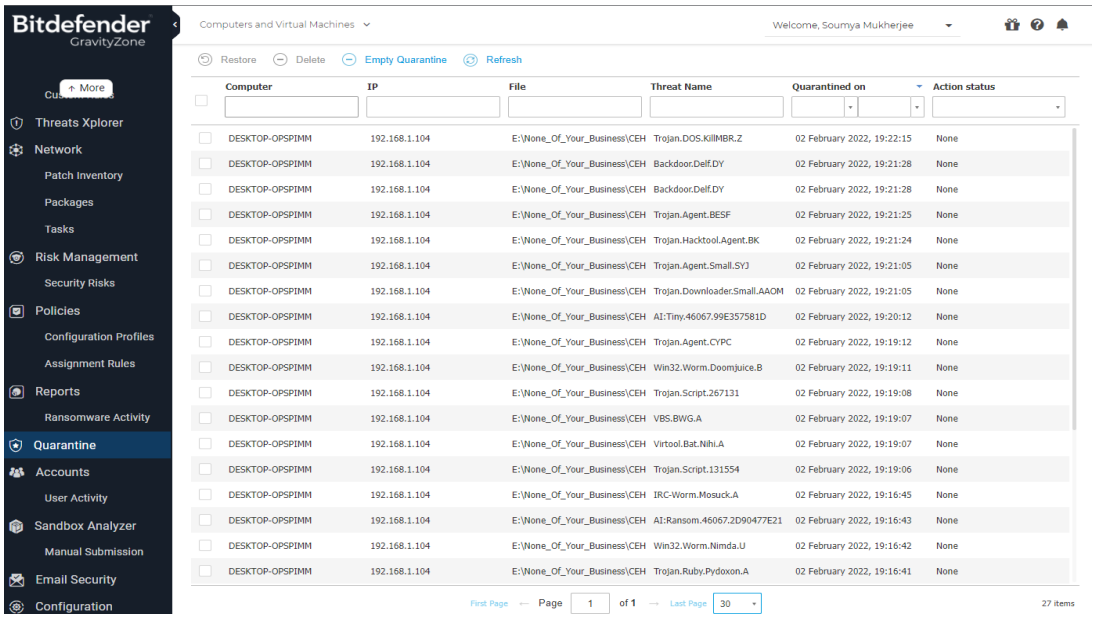


Client Output

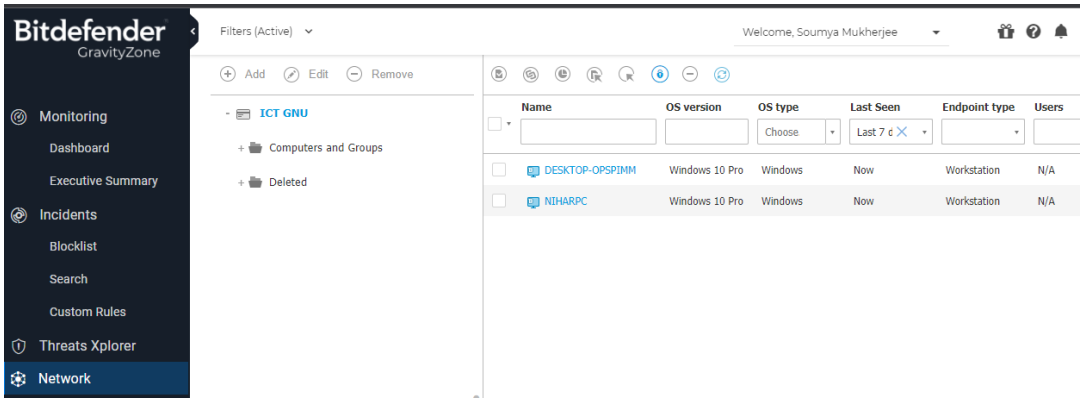


Web Panel Output

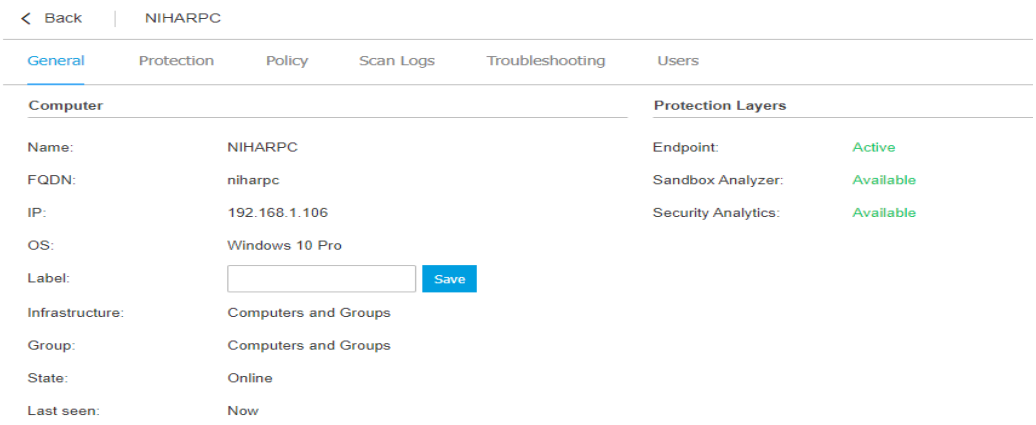
- In case malware files are detected it gets quarantined automatically and can be viewed in web panel.



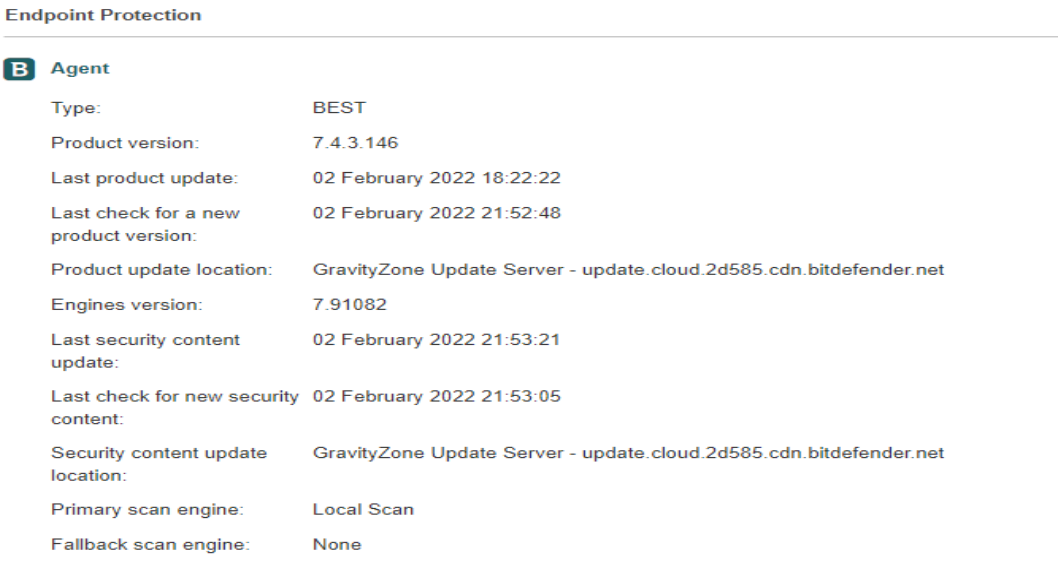
- We can view all the endpoint devices at network tab



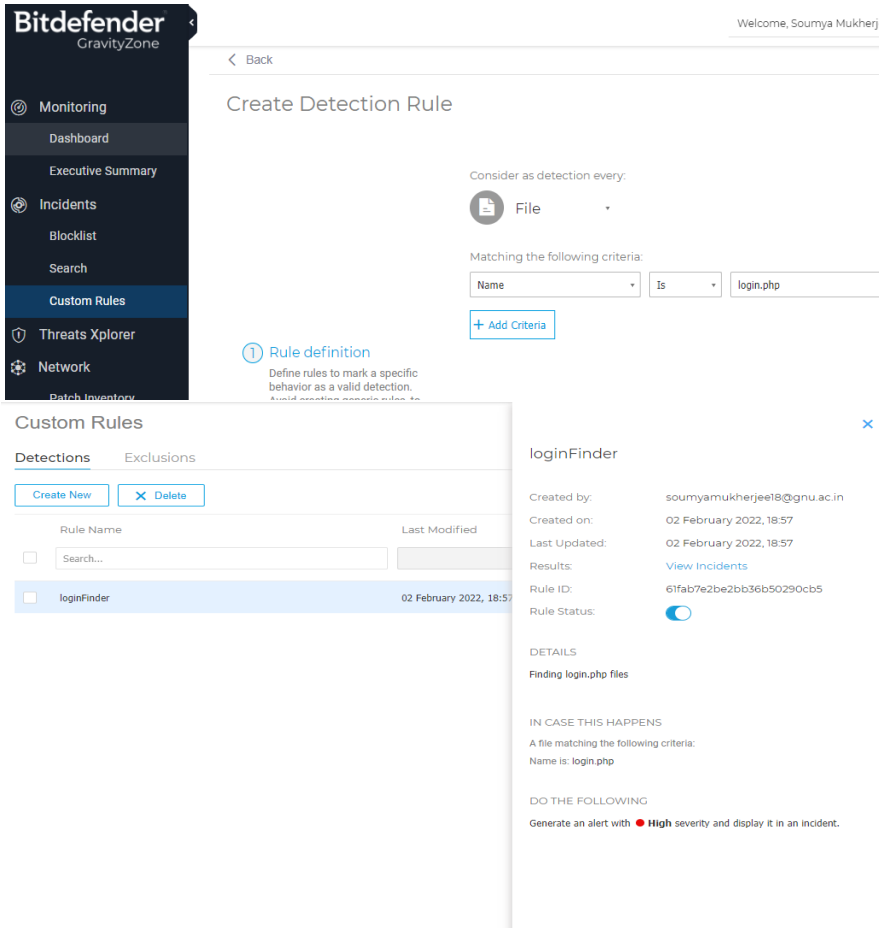
- We can view general information about the computer



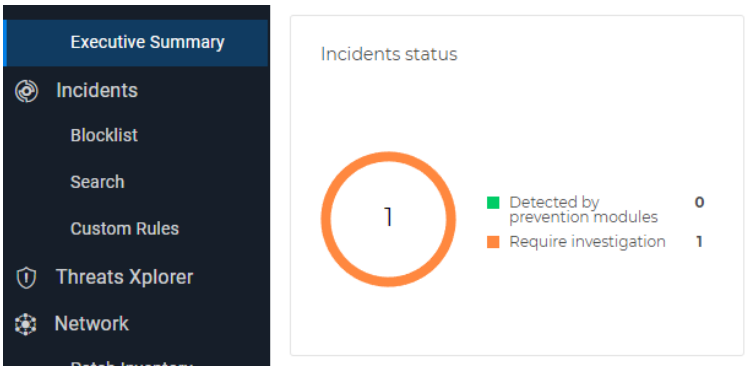
- Followed by information such as updates, version, timestamps, etc.



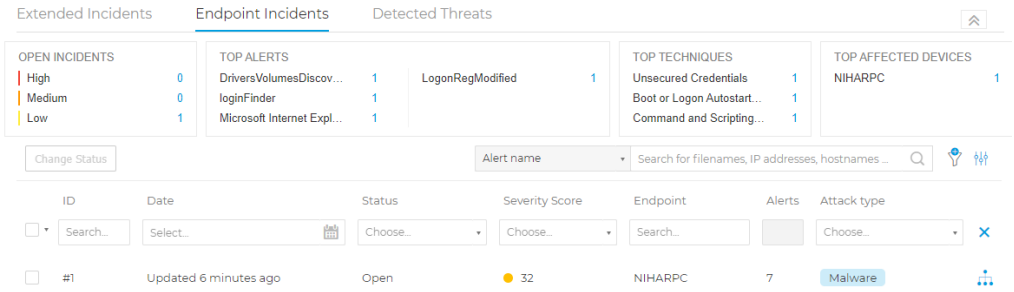
- Next, we create a custom rule, and make it to instantly flag “High” severity if it finds a file with “login.php” name.



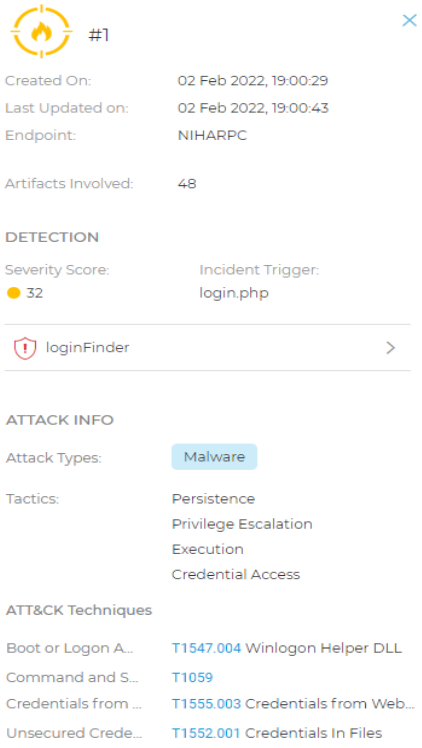
- After a custom scan, we found an Incident notification, stating require investigation.



- Upon checking we find one flag against a file found in one of our endpoint devices.

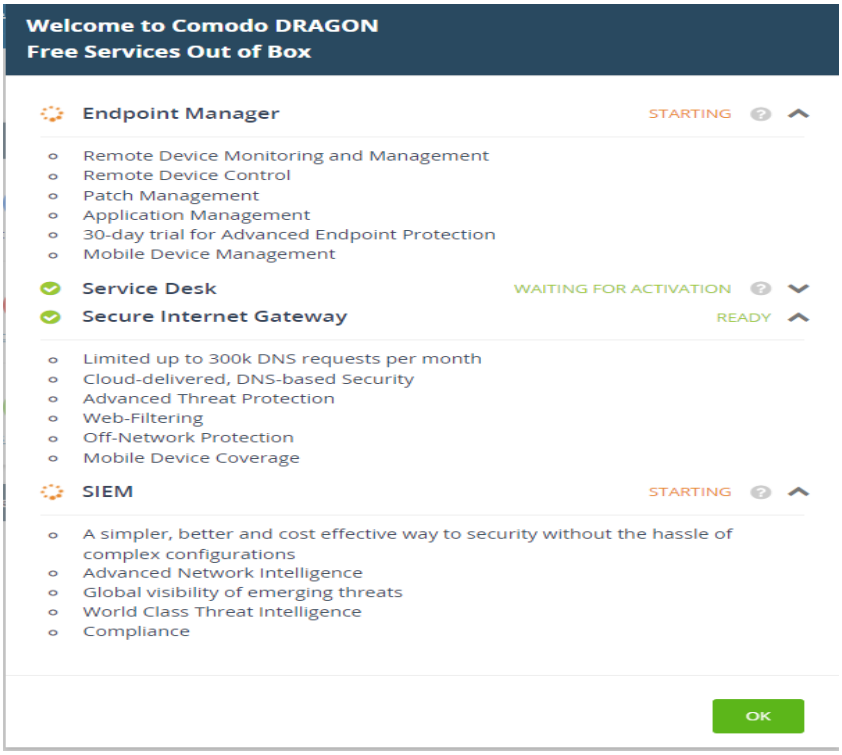


- Malware details:

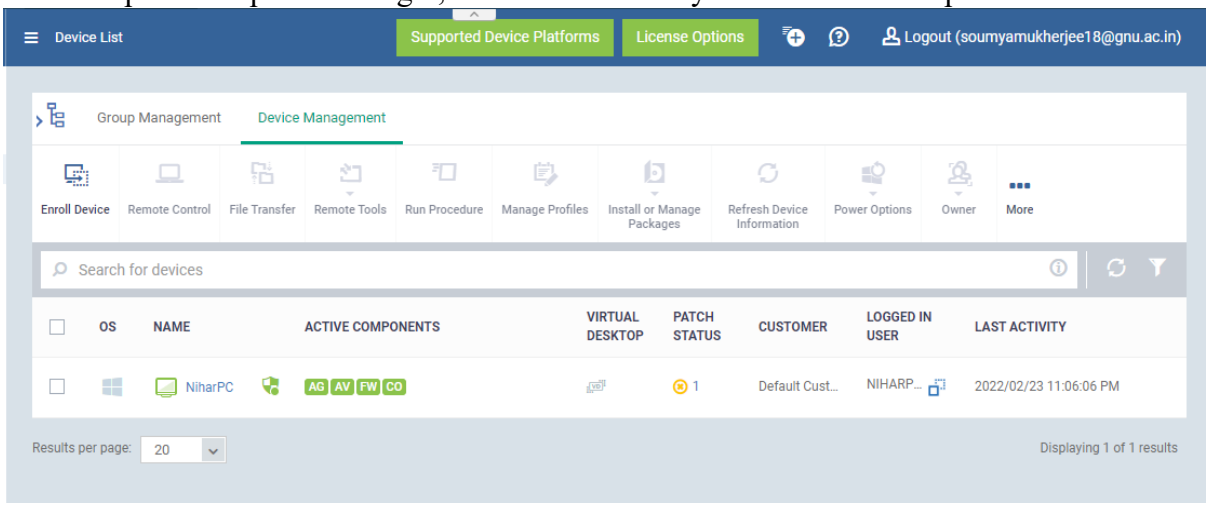


CHAPTER 9 (B) – IMPLEMENTATION (COMODO)

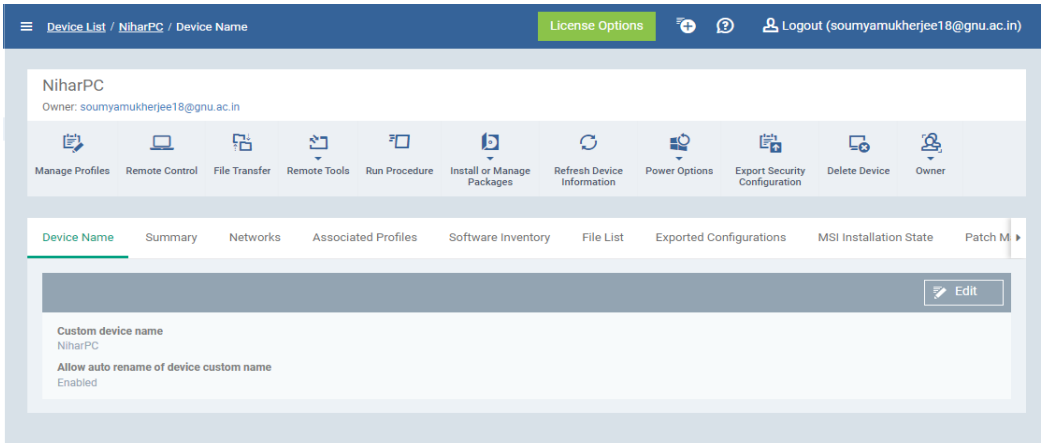
- Setting up comodo client and web portal is really easy. First we will start with web portal, go on their website and request for a free trial, once done login with your account, and you will be greeted with this screen:



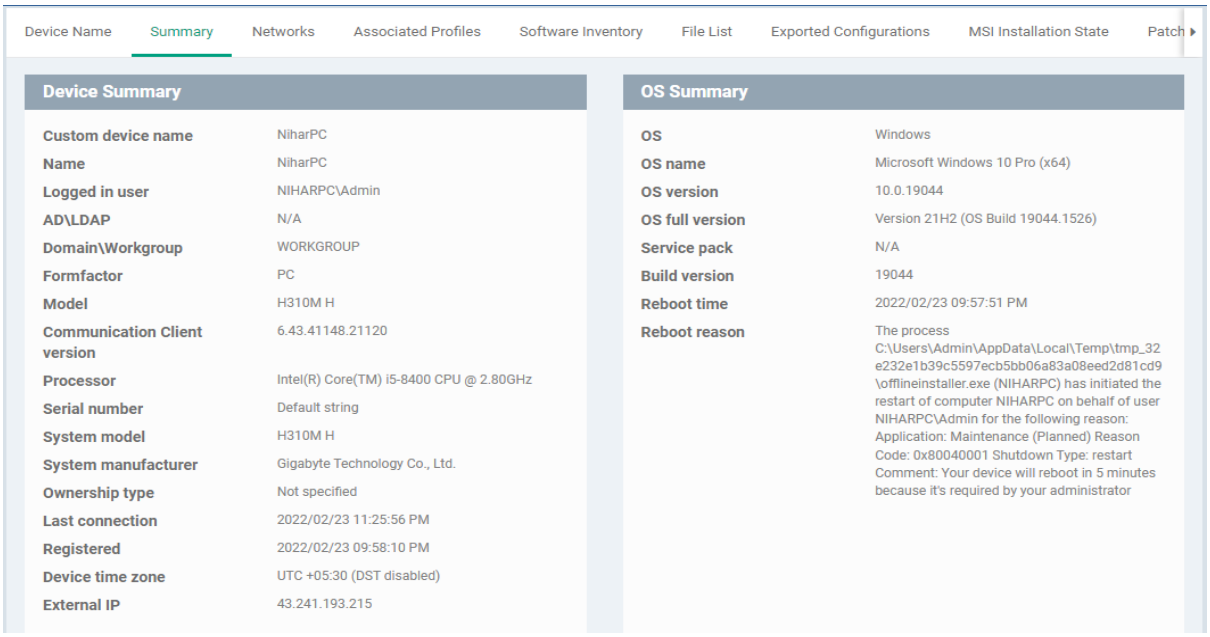
- To set up client, it's easy just need to install package in client and it will setup automatically. Let's explore Endpoint Manager, under Device List you can find all endpoints.



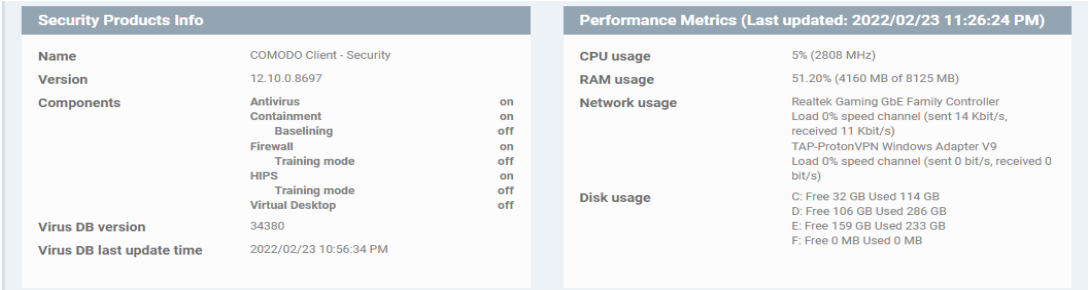
- Details covered under device profiling:
  Device Name:



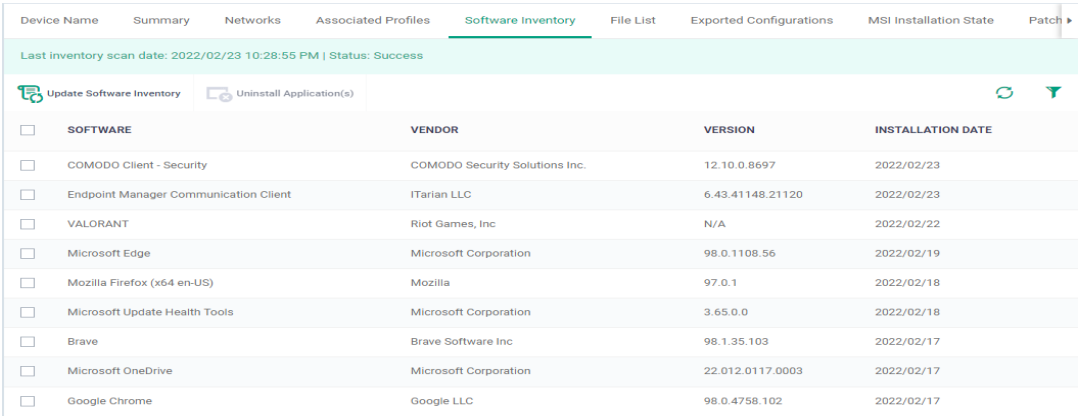
Summarized Info:



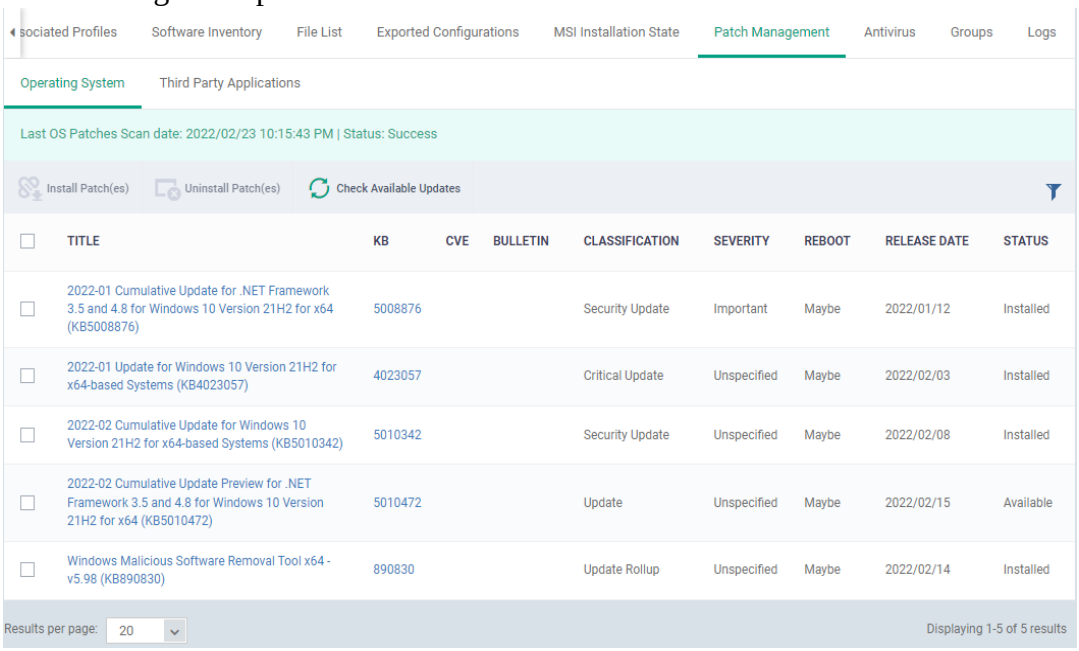
Security Patch Details and information regarding Performance metrics:



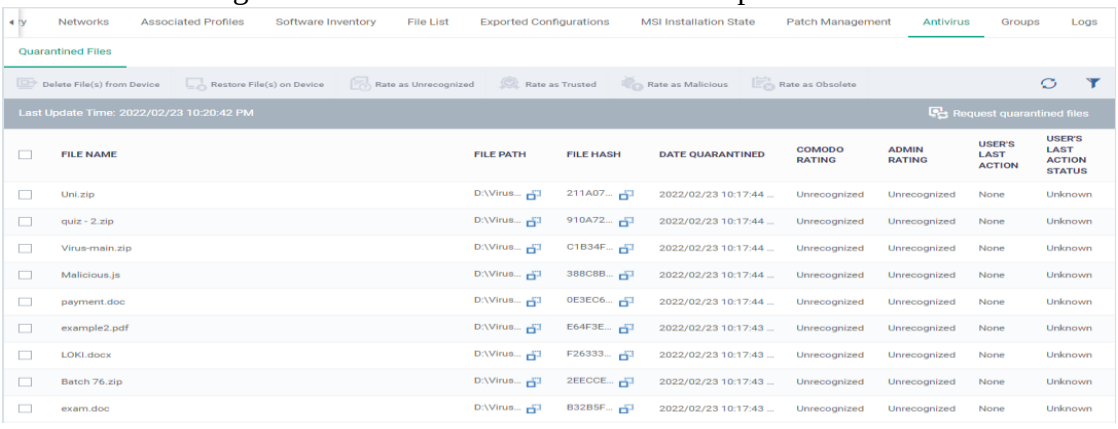
Quick view on all software installed in client:



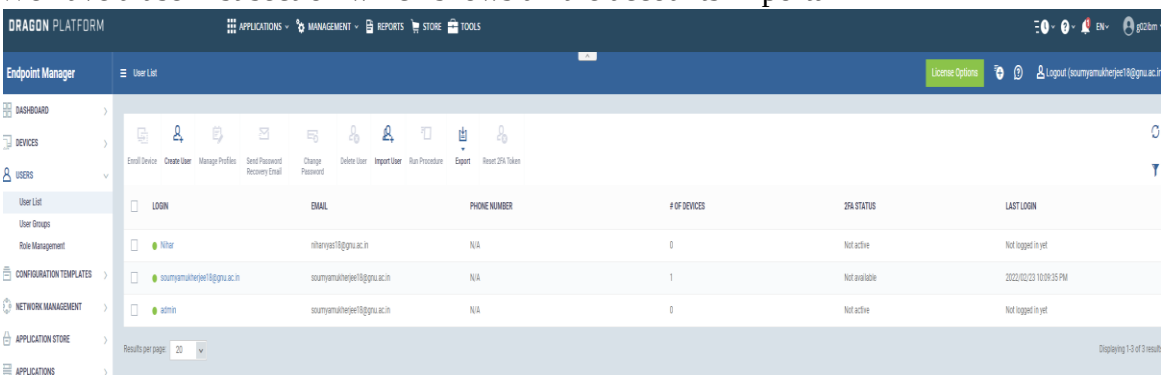
Security Patch running in endpoint:



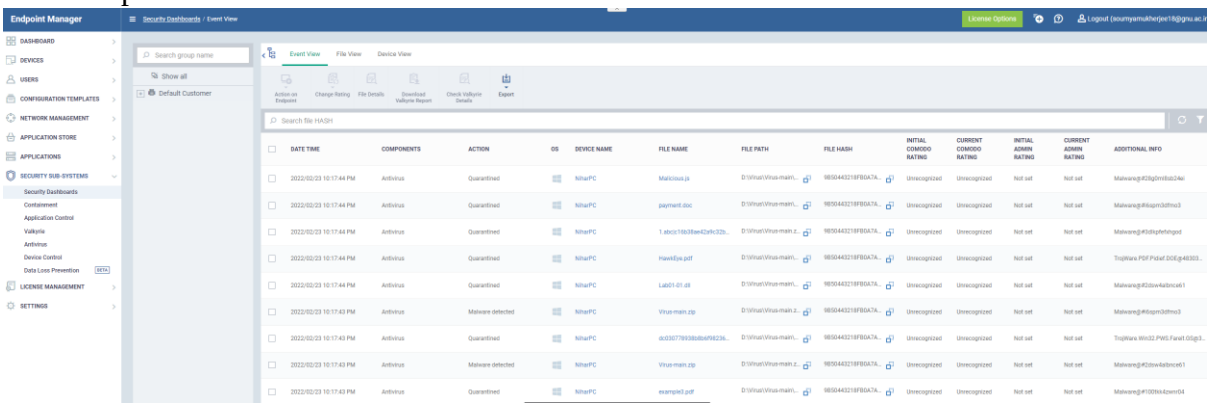
Finally, Antivirus records gathered from client and remote action panel:



- We have a user list section which shows all the accounts in portal

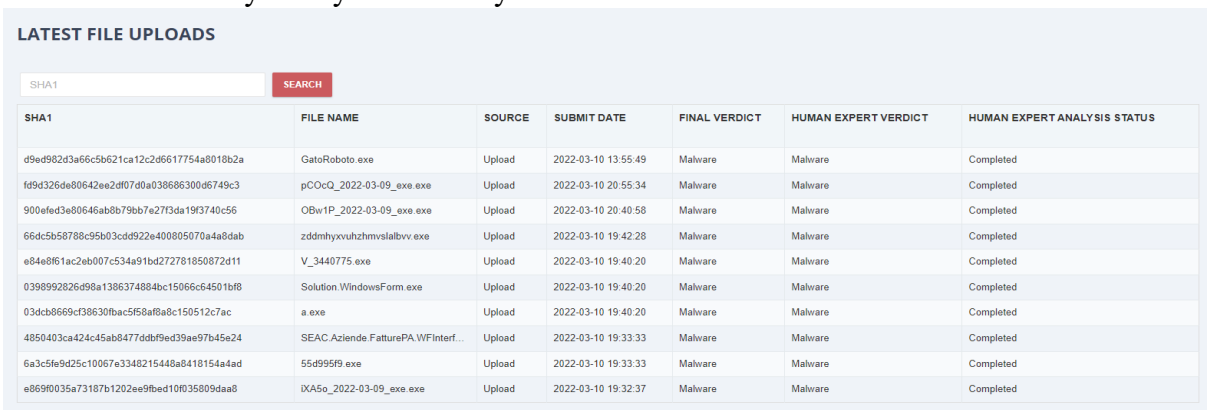


- Security Dashboard gives us the root logs of all sorts of antivirus actions taken on malicious files and endpoint devices.

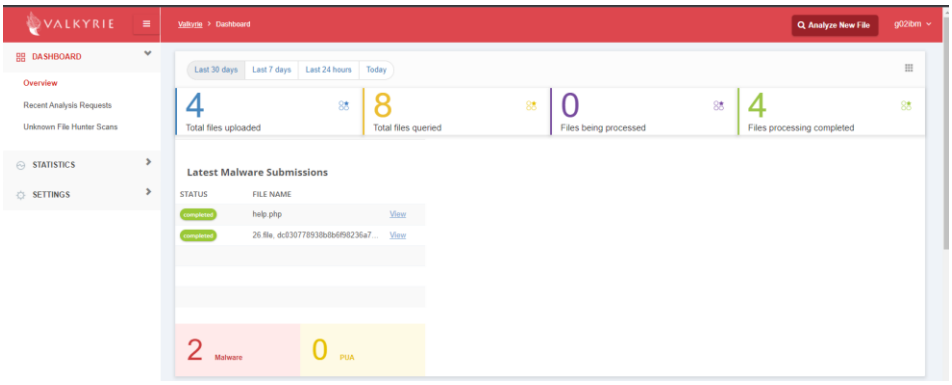


- Web portal has a special tab for Valkyrie logs:

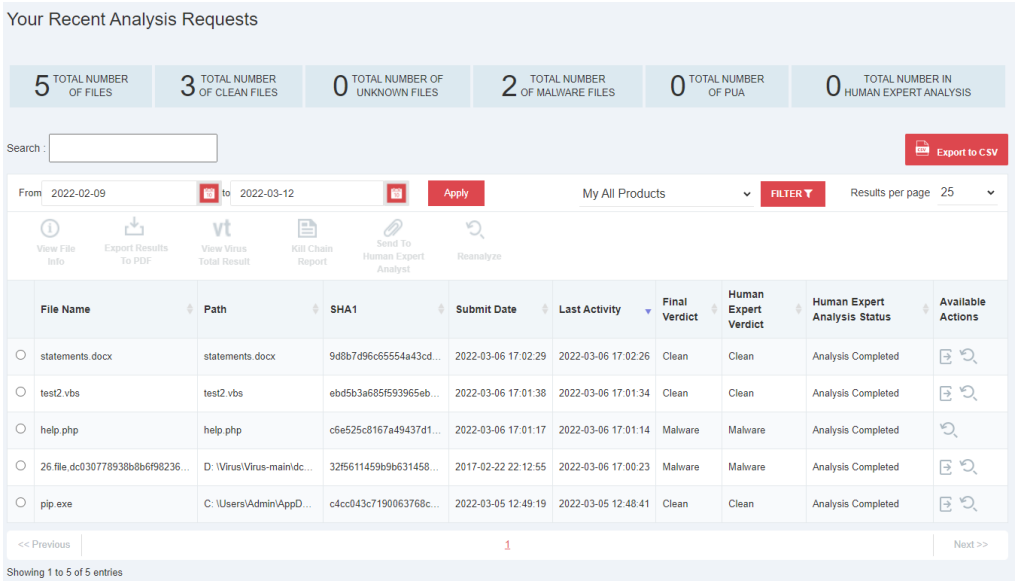
- Advanced security sub system “Valkyrie” dashboard



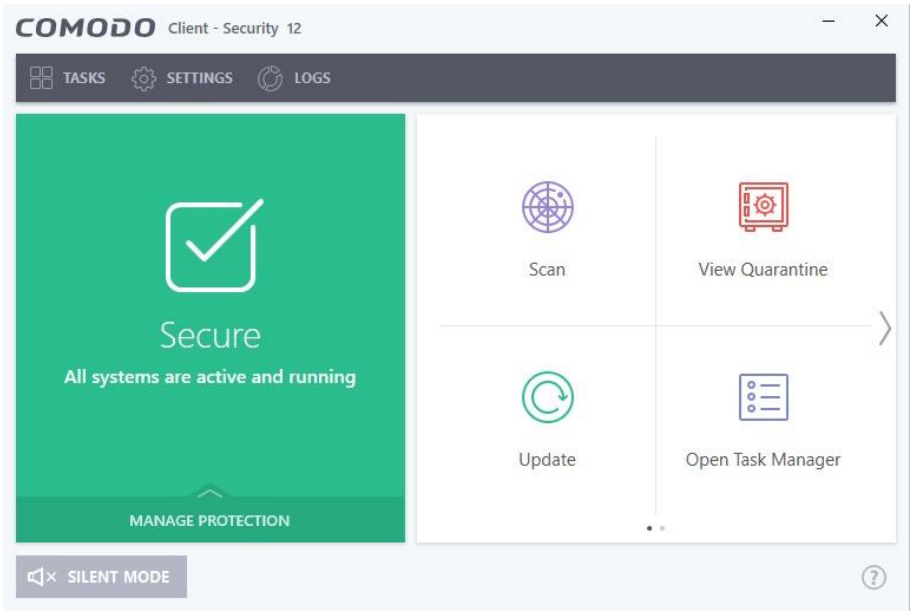
- Overview dashboard:



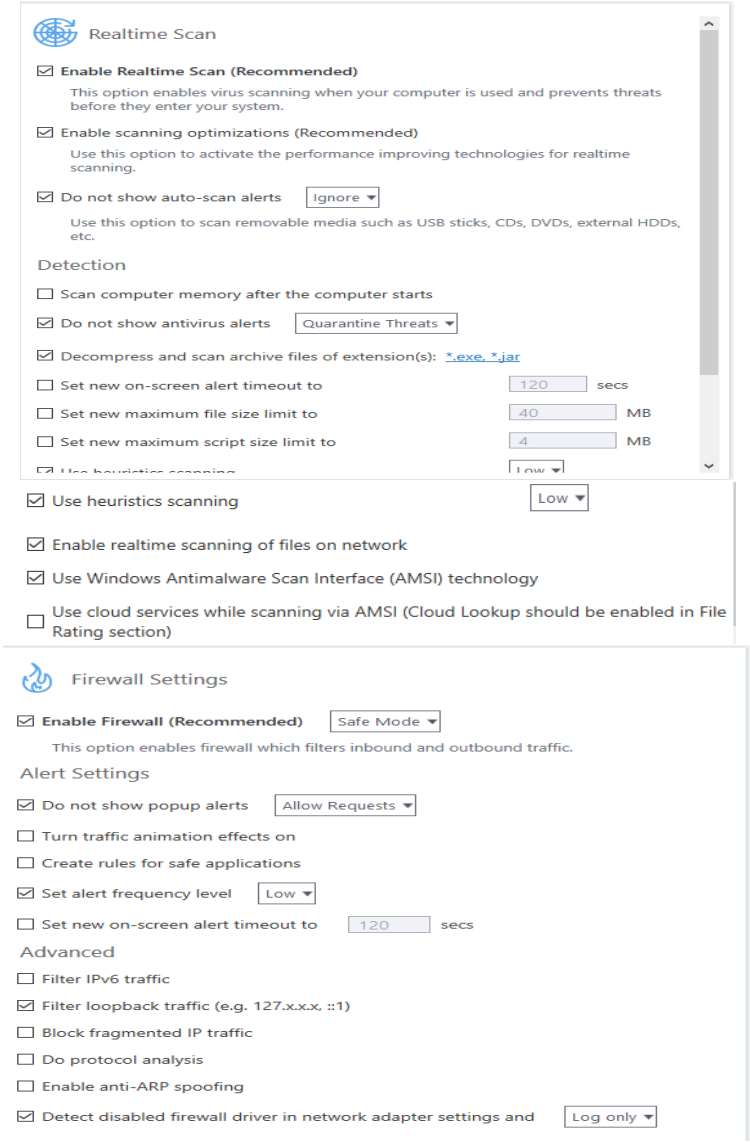
- We can also view recent analysis reports performed in client:



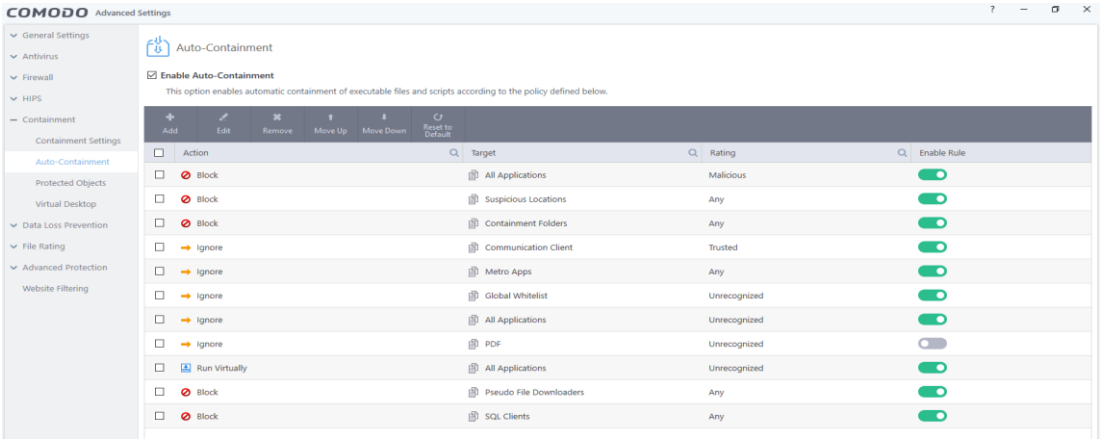
- Client Section: Once installation is done, it runs an automatic scan, following screen is displayed:



- Client comes with advanced settings options one can directly setup in client



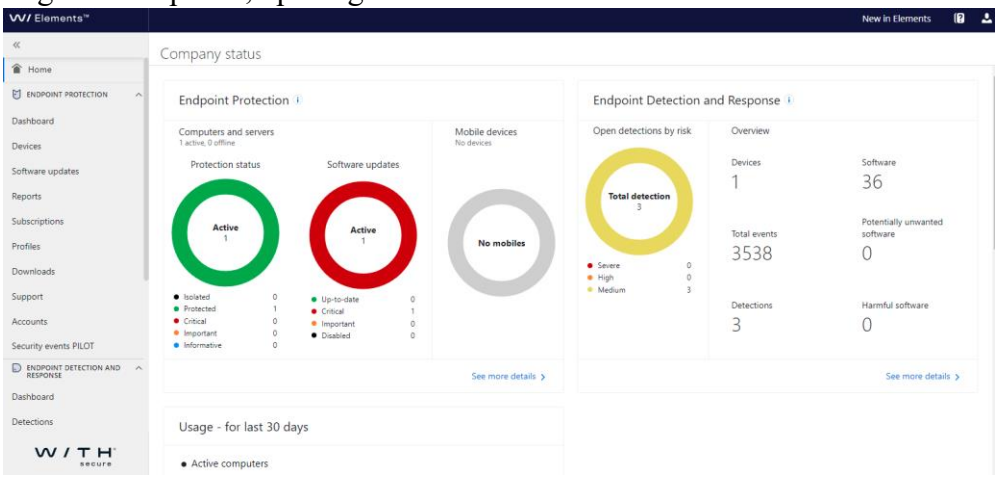
- Comodo client offers auto containment of malicious files along with allowing client logs and client actions on that very endpoint device:



- Manual rulesets and predefined rulesets are all mentioned under HIPS ruleset section so that client doesn't interrupt with normal OS operations.

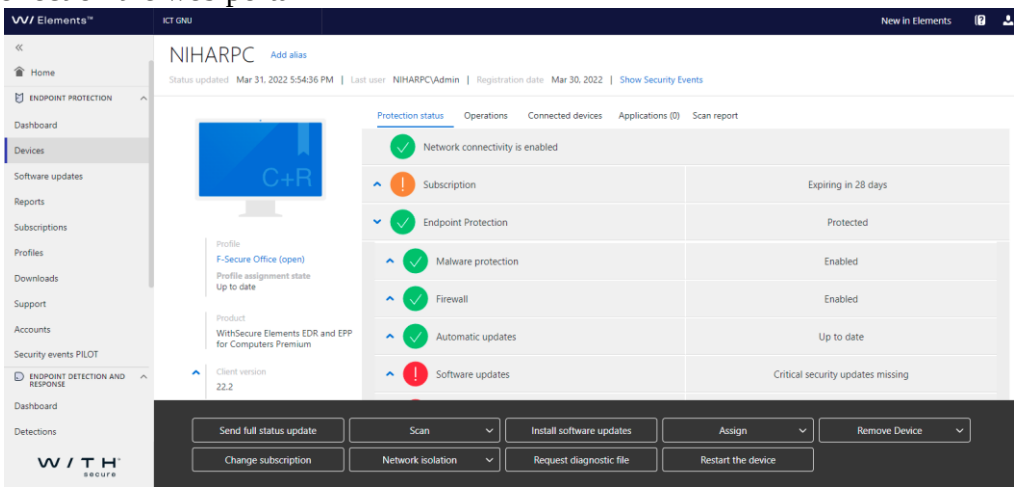
CHAPTER 9 (C) – IMPLEMENTATION (WITHSECURE)

- Initialising the web portal, opening “Dashboard”

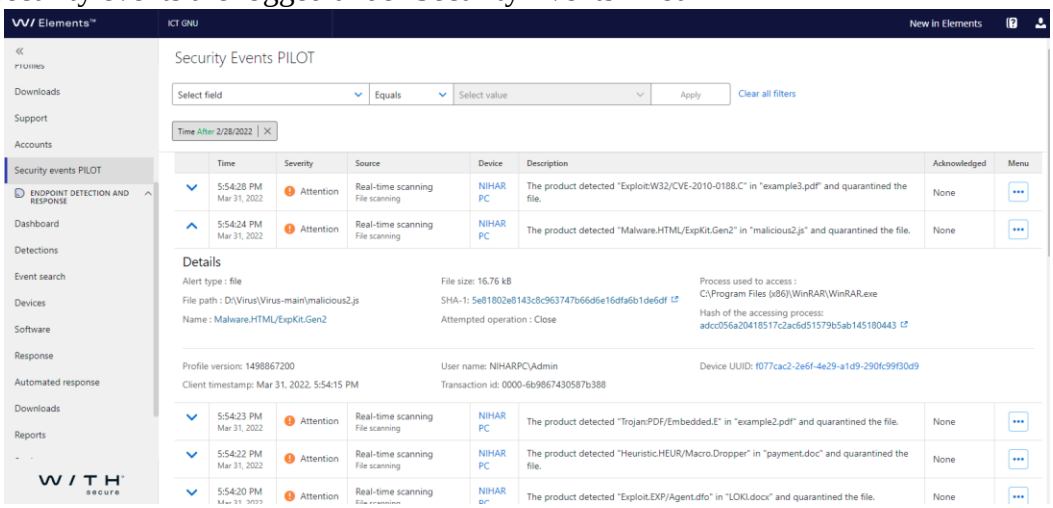


We can view all the endpoints, there security state, software updates, any critical notifications all at one place.

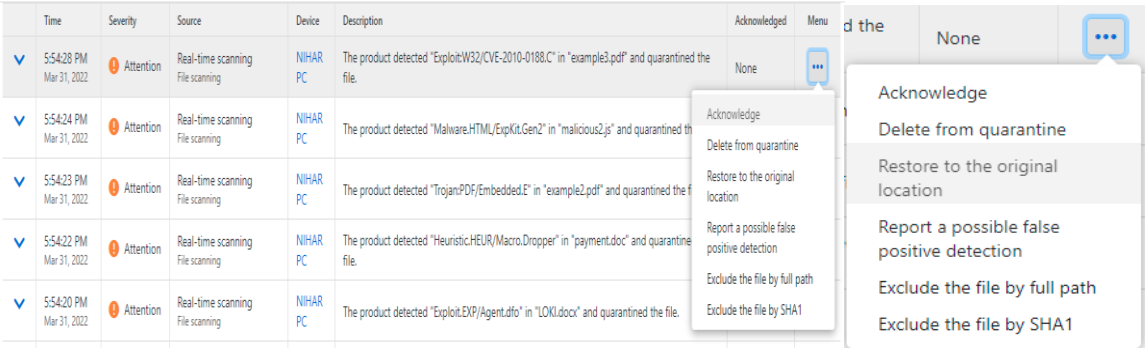
- Adding an endpoint device is easy, just download the package and install it, once done it will auto reflect on the web portal



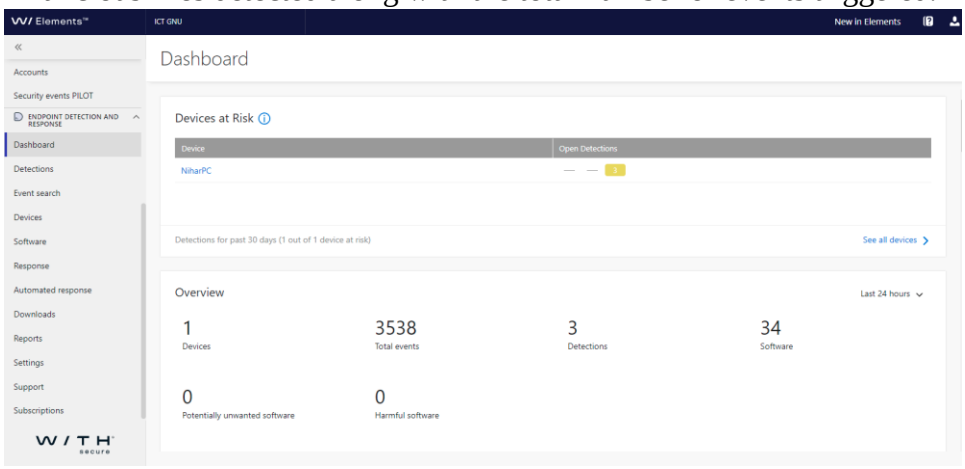
- All security events are logged under Security Events Pilot



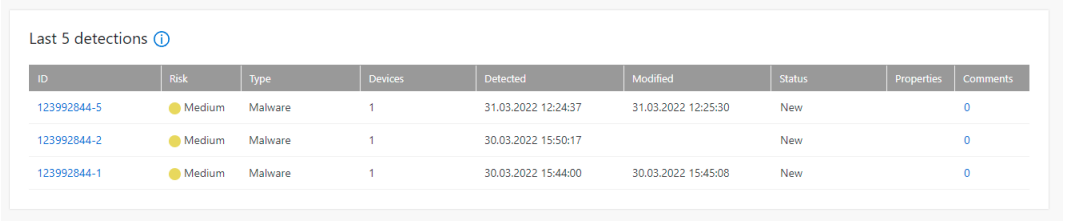
- For example, one file got flagged as malware a.k.a false positive and you wish to restore it, can be simply done by doing the following.



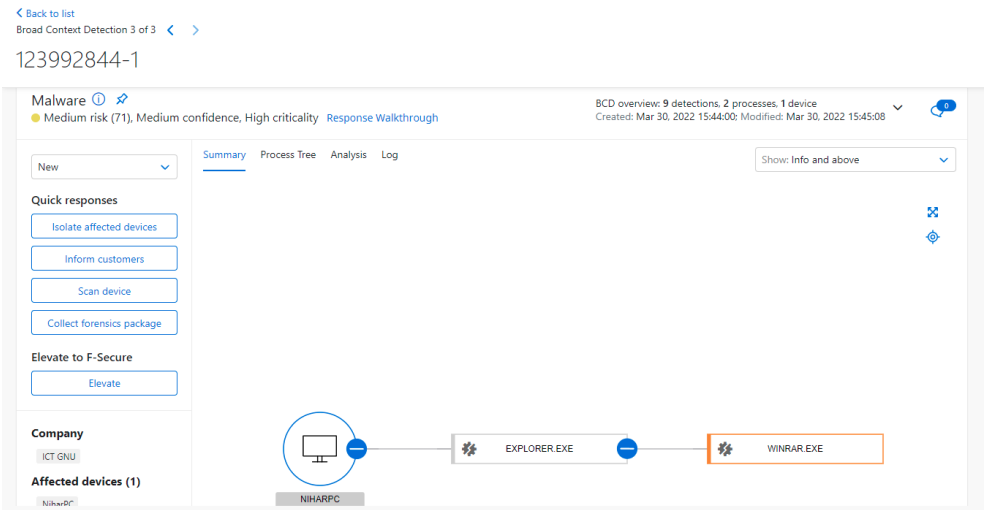
- Detection and Response has a different dashboard to offer, which basically shows total endpoints and total malicious files detected along with the total number of events triggered.



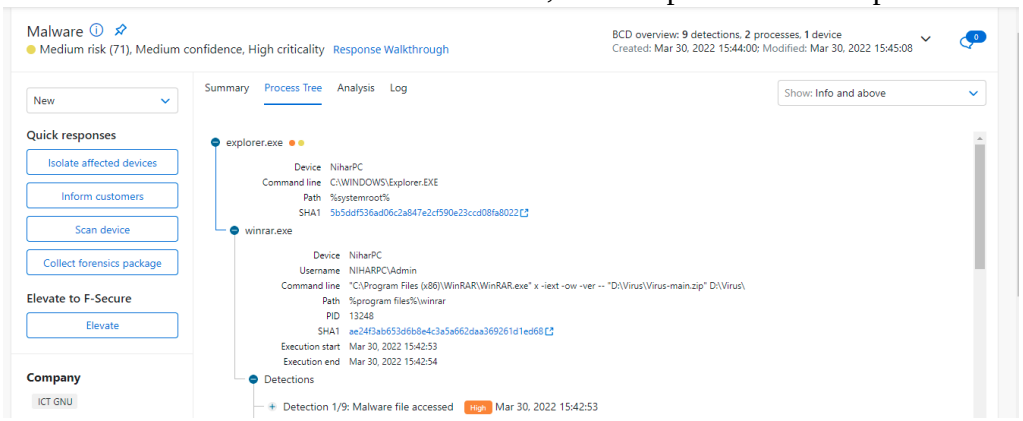
- Detections:



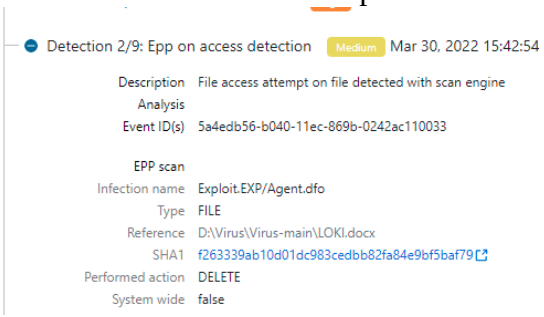
- Now for example, we wish to gather more info on the detected malware, simply click on it.



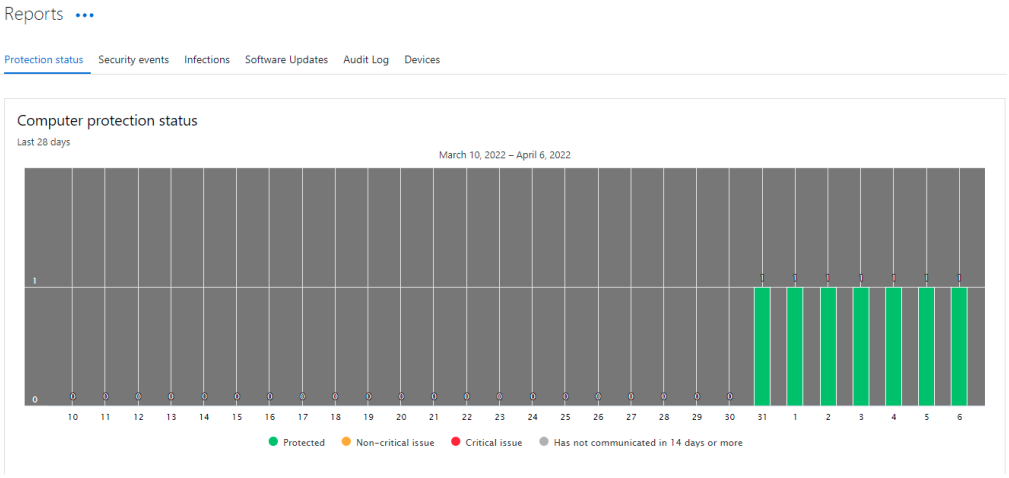
- It gives this nice flowchart view of malware tree, with ample information possible.

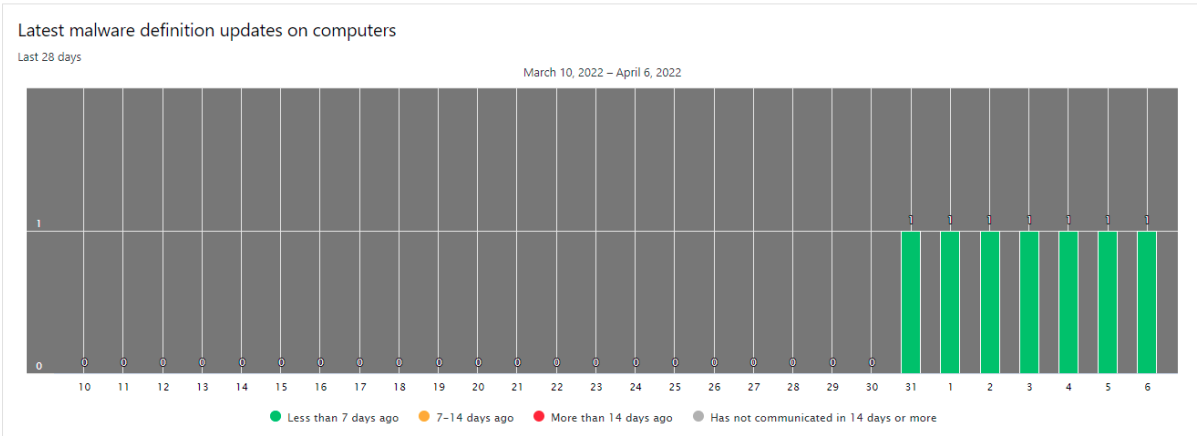


- Followed by, we can also see all the actions performed on each detection:

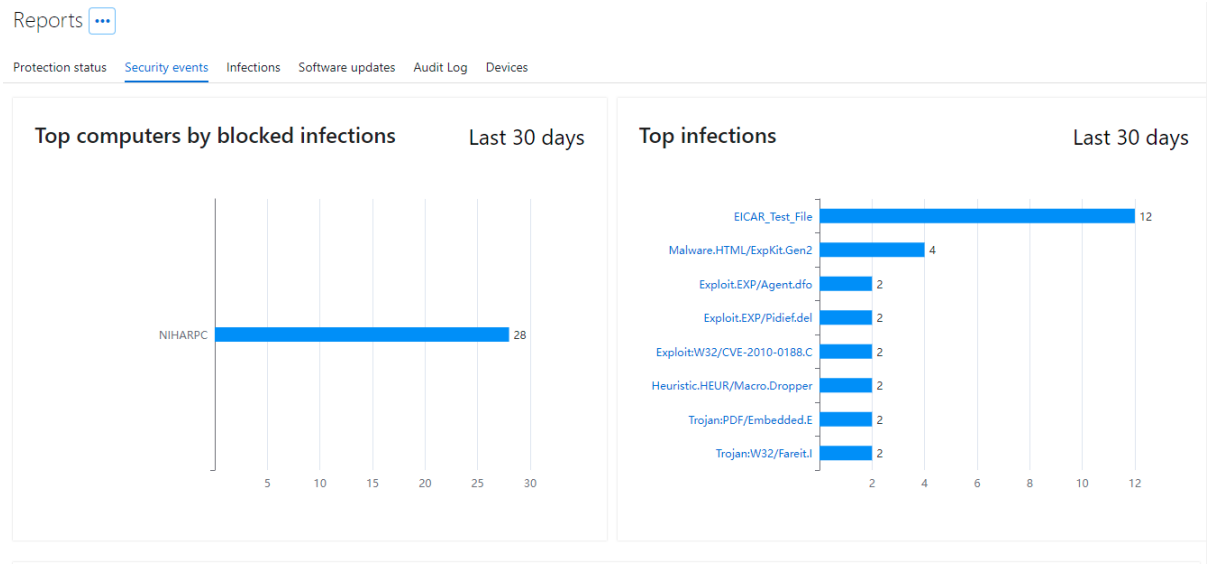


- Report logs for automated actions:

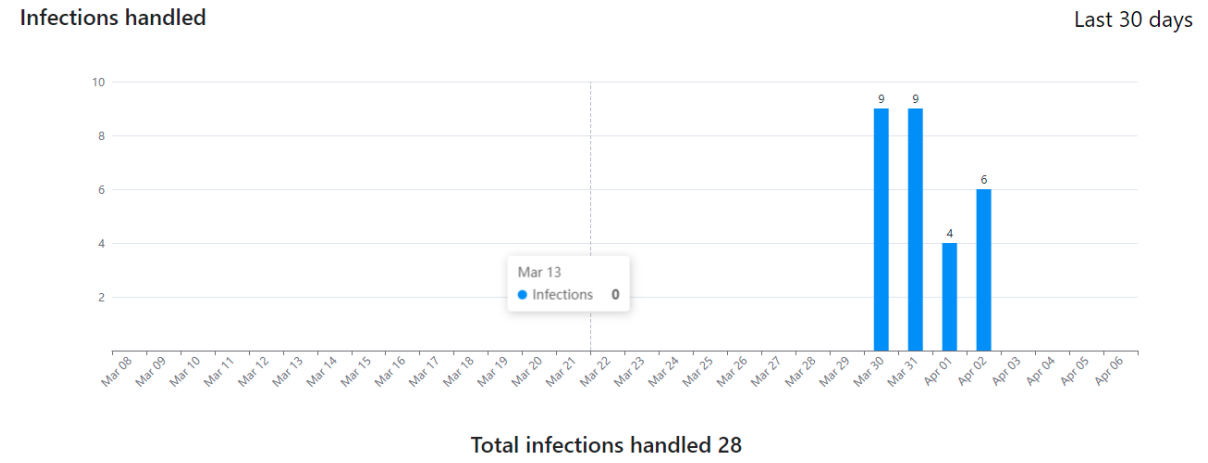




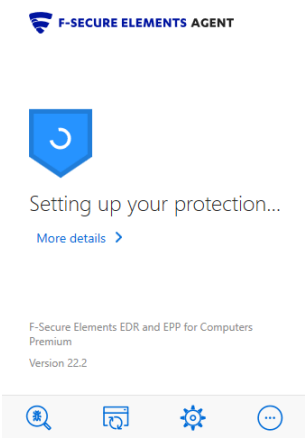
- Quick glace view of which endpoint is getting compromised quicker along with which malware view:



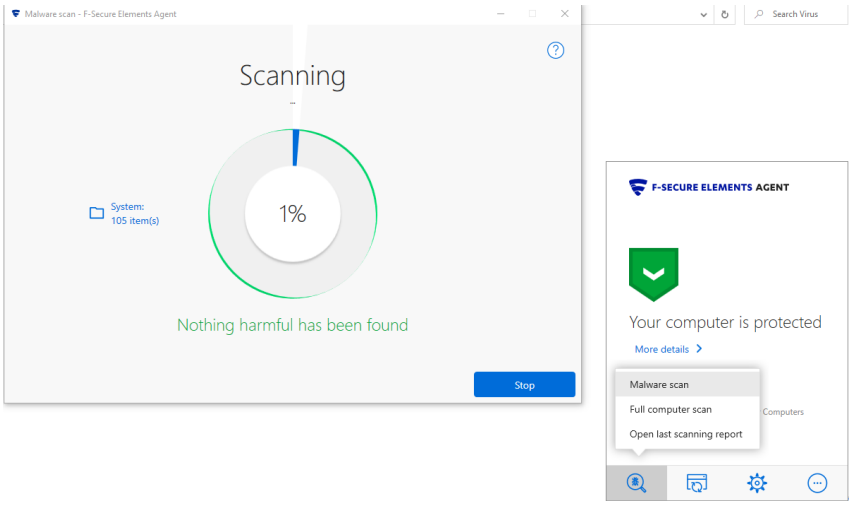
- Graphical representation of data:



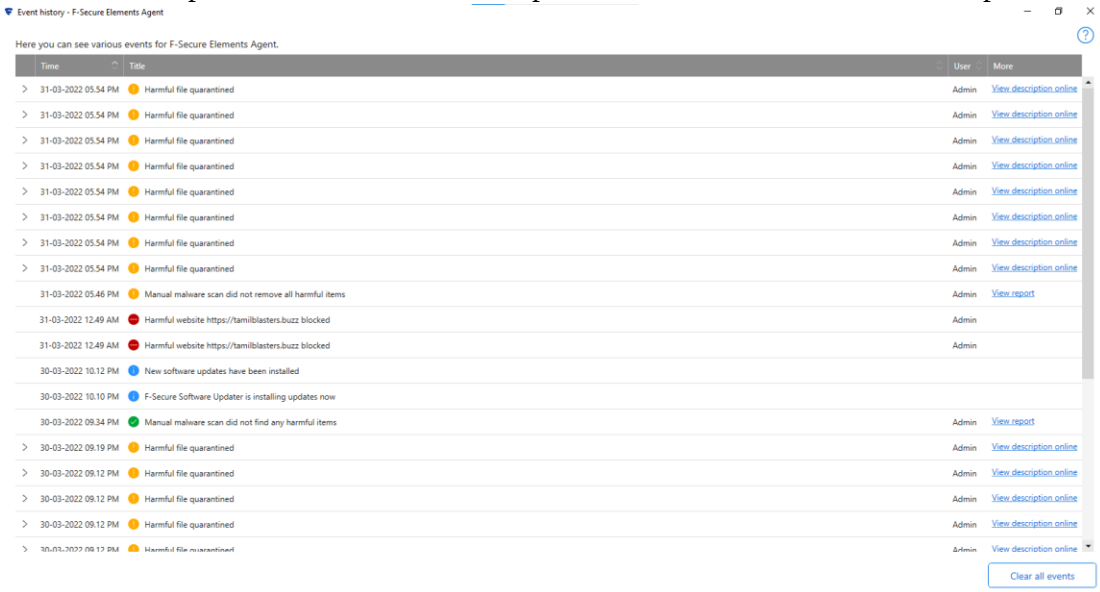
- Client-Side Initialisation:



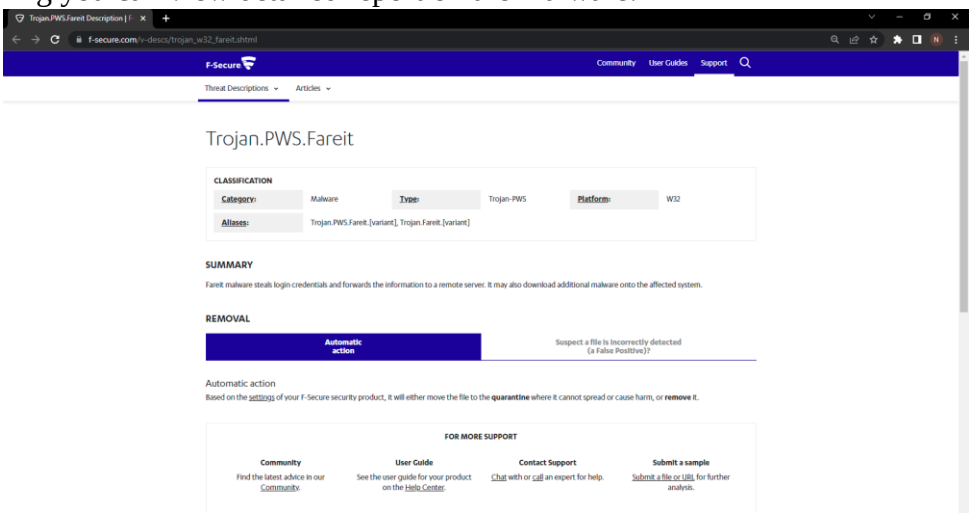
- Running a quick scan to index all the files and look for malicious files.



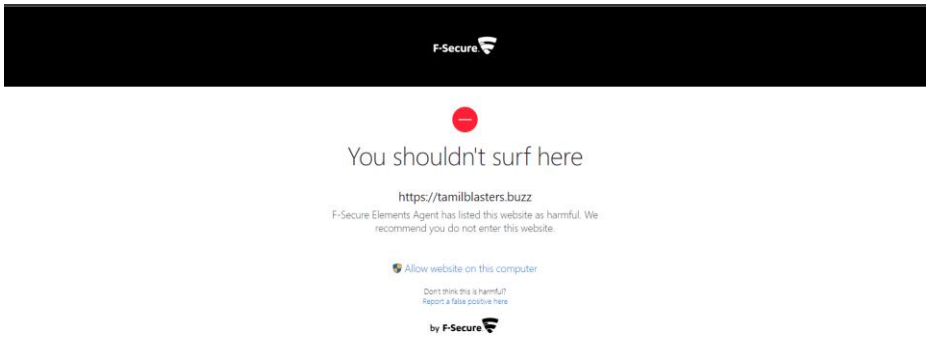
- Once a scan completes it sends a detailed report to client as well as shows it in portal.



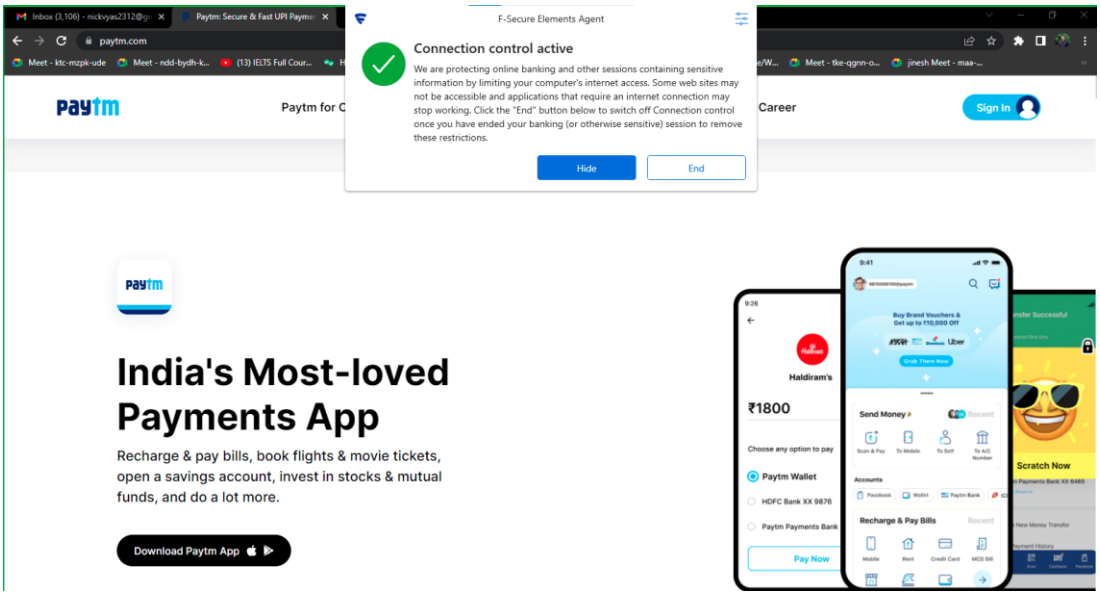
- On clicking you can view detailed report on the malware:



- Client tool also provides malicious link blocker for secure we browsing:



- Key highlight feature making it better for financial applications, it runs a secure antivirus layer once you try to access finance web apps:



CHAPTER 10 – CONCLUSION

CHAPTER 10 – CONCLUSION

Very precise tool in identifying malicious files, automatic detection and action taken upon a scan, client-side devices are monitored for any unusual activity, ease up security, by providing a dashboard and security dashboard with remote actions. Anti-Virus techniques, Valkyrie security sub system and Sandbox Analyzer allows us to run external files in a safe virtual environment. WithSecure detailed malware analysis and quick responsive client makes it easy to know information on detected malwares and securing client.

CHAPTER 11 – REFERENCES

- https://www.crowdstrike.com/endpoint-security-products/falcon-endpoint-protection-enterprise/
- https://www.bitdefender.com
- https://mcaffe.com/security-awareness
- https://github.com/tarcisio-marinho/PayloadIdentifier
- https://platform.comodo.com/
- https://elements.f-secure.com/

G02 IBM Report Final

by Soumya Mukherjee

Submission date: 18-Apr-2022 09:18PM (UTC+0530)
Submission ID: 1811562006
File name: G02_-_IBM_Report_Test_Copy.docx (7.56M)
Word count: 4139
Character count: 21928

CHAPTER: 1 PROJECT BACKGROUND

CHAPTER 1 PROJECT BACKGROUND

Initially this project was supposed to be a coded product which was intended to solve the issue of end point security and remediation for financial applications. First two weeks were planned accordingly, and team started the work.
Upon completion of time, when all data was gathered, we faced some difficulties, such as:

- Unable to find a proper financial application to base our project on.
- Facing an issue with cloud implementation of the project, especially hosting it IBM cloud, since we are limited to one instance for a limited time period whereas this project aims at having 3 different servers to work at once.

On very next day, team had an IBM Mentor meeting, where all the difficulties were presented, and then team got proposed with a change of approach by mentor.
Approach 1: Continue coding the product and try to reduce as much errors possible, but at same time this approach would consume huge amount of time.
Approach 2: Get hands-on experience on industry grade EDR tool, which provides similar solution to the problem statement. This approach was time effective and would help us learn more.

Team thereby chose Approach 2 and entire report is prepared on the basis of Approach 2.

CHAPTER: 2 INTRODUCTION

CHAPTER 2: INTRODUCTION

In this modern epoch every industry is going online and finance industry is no left. In India 41 million transactions per day is happening. Despite spending many millions of rupees on security, financial services organizations continue to be one of the top targets for cybercriminals. The access to the vast amounts of money that the financial industry trades and controls, along with the sensitive personal information they store, continues to make them a prime target. Whilst digital transformation is offering many advantages in driving business forward, it also provides more opportunities for attackers. As well as the increase in number of attacks, the attacks themselves are becoming more complex and targeted, so financial organizations must therefore assume they will be attacked and prepare accordingly.

Endpoint Detection and Response (EDR) can provide real-time detection, identification and response to threats:

Signature-less attacks: unlike conventional solutions like AV, EDR uses AI, machine learning, and behavioural analysis, to detect suspicious behaviour.
File-less attacks: evasive attacks often leverage whitelisted Windows applications to create damage, in a completely file-less fashion so EDR solutions analyze behaviours instead of evaluating files.
Low and slow attacks: EDR solutions aggregate endpoint data and continually analyze it, correlating suspicious individual activities, to then identify a multi-stage attack. This means they can detect "low and slow" attacks which often go undetected.

CHAPTER: 3 PROJECT SCOPE

CHAPTER 3: PROJECT SCOPE

This hand's on experience report is limited to Bitdefender GravityZone Ultra, Comodo Dragon and WithSecure, although brief information about other tools will be given.

CHAPTER: 4 SOFTWARE AND HARDWARE REQUIREMENTS

CHAPTER: 4 SOFTWARE AND HARDWARE REQUIREMENTS

Minimum Hardware Requirements

Processor	I5 2.0 GHz
RAM	8 GB
HDD	40 GB

Table 3.1 Minimum Hardware Requirements

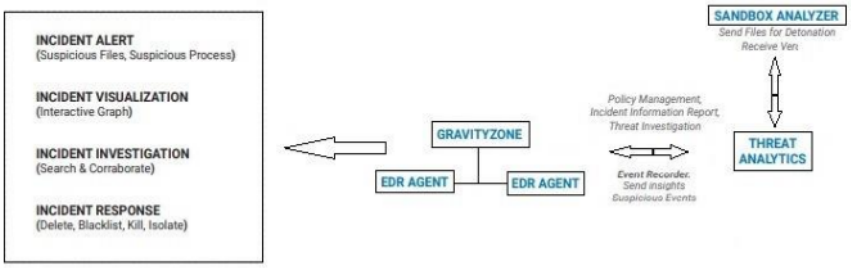
Minimum Software Requirements

Operating System	Any operating system which can support an internet browser.
Programming language	-
Other tools & tech	Internet browser

Table 3.2 Minimum Software Requirements

CHAPTER: 5(A)-PROCESS MODEL (BITDEFENDER

CHAPTER: 5(A)-PROCESS MODEL (BITDEFENDER)



- Once endpoint is connected with panel, any sort of unusual activity detected will create an incident alert.
- Incident alert then will be sent to Gravityzone firewall for further process, from where it will go through policy management, incident information report and threat investigation,
- From threat analytics it goes to sandbox analyser for testing its behaviour and later the report is transferred back to Gravity zone firewall endpoints.
- Finally, it shares the outcome in end user clients and also logs the stuff, and reports it in dashboard.

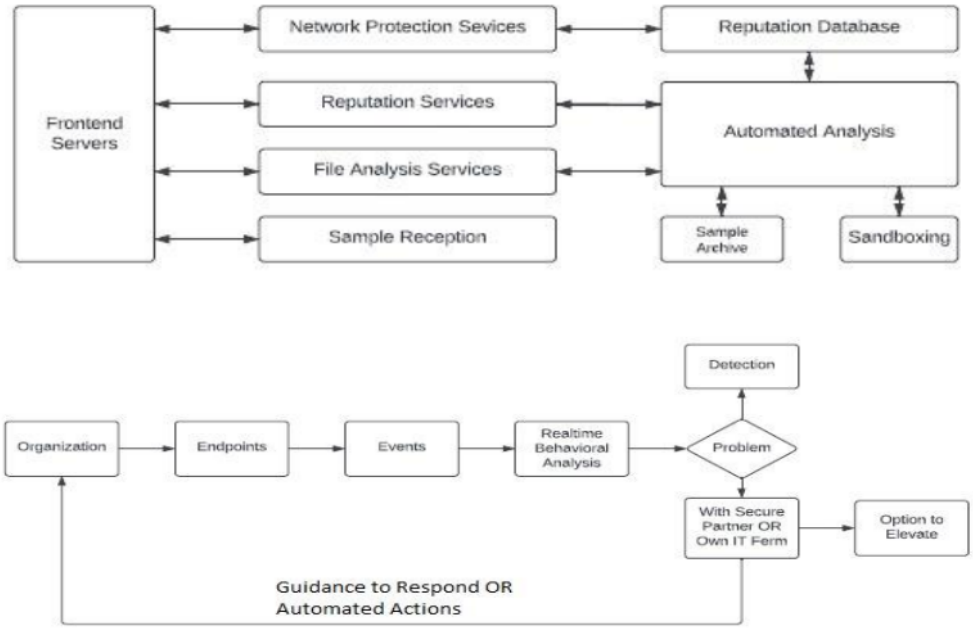
CHAPTER: 5(B)- PROCESS MODEL (COMODO)

CHAPTER: 5(B)- PROCESS MODEL (COMODO)

- Once a file is executed in client, instantly Comodo client starts observing the file
- If the file gets identified as unknown as in if its sources are unknown or the way of execution if different file gets marked as “unknown threat to system” until it completes execution.
- Auto Containment triggers to control its effect on client meanwhile an analysis on trusted verdict goes on.
- If file appears to be good no harmful effect it gets marked as safe and out from quarantine otherwise it gets wiped out from client.

CHAPTER 5 (C) – PROCESS MODEL (WITHSECURE

CHAPTER 5 (C) – PROCESS MODEL (WITHSECURE)



- WithSecure Client keeps monitoring client devices for any sort of abnormal behaviour or breach of policy or tampering with files.
- In case, any network attack gets detected, Network Protection Service takes care of it, directs the traffic to its Automated Analysis system which then filters out any possible attacks and lets genuine requests pass through without interfering operations.
- File Analysis system takes care of any malicious file being downloaded / found in system, quickly quarantines it and run a full scan on it. Later presents all the malware data on portal and making sure the client is secured.
- One of its highlight features is to elevate an issue to higher ups / admins in an organization if any unwanted events gets triggered apart from automated response system acting on it.

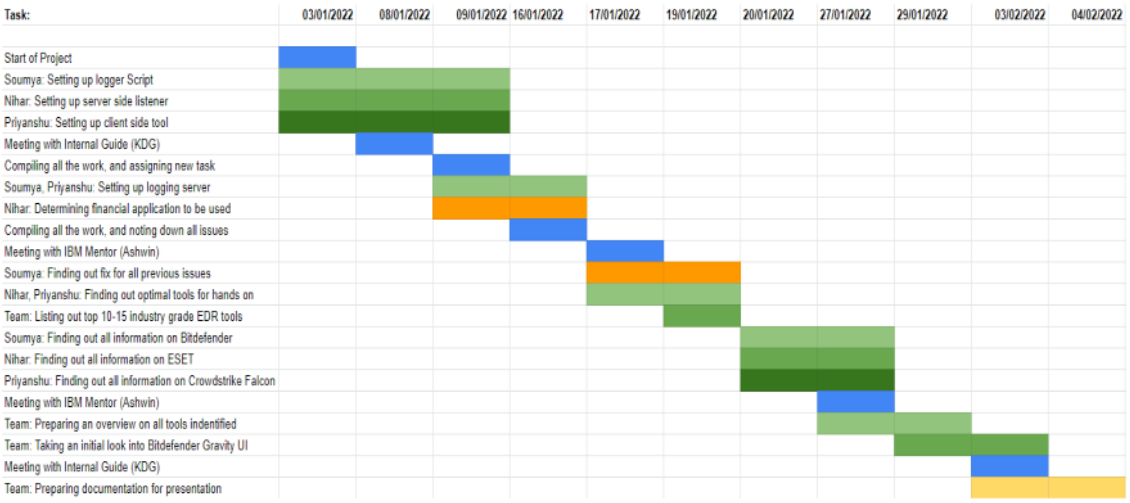
CHAPTER 6 - PROJECT PLAN (TIMELIN

CHAPTER 6 - PROJECT PLAN (TIMELINE)

Task (03/01/2022 – 04/02/2022):

Soumya: Setting up logger Script
Nihar: Setting up server side listener
Priyanshu: Setting up client side tool
Compiling all the work, and assigning new task
Soumya, Priyanshu: Setting up logging server
Nihar: Determining financial application to be used
Compiling all the work, and noting down all issues
Soumya: Finding out fix for all previous issues
Nihar, Priyanshu: Finding out optimal tools for hands on
Team: Listing out top 10-15 industry grade EDR tools
Soumya: Finding out all information on Bitdefender
Nihar: Finding out all information on ESET
Priyanshu: Finding out all information on Crowdstrike Falcon
Team: Preparing an overview on all tools indentified
Team: Taking an initial look into Bitdefender Gravity UI
Team: Preparing documentation for presentation

Timeline:



Task (07/02/2022 – 11/03/2022):

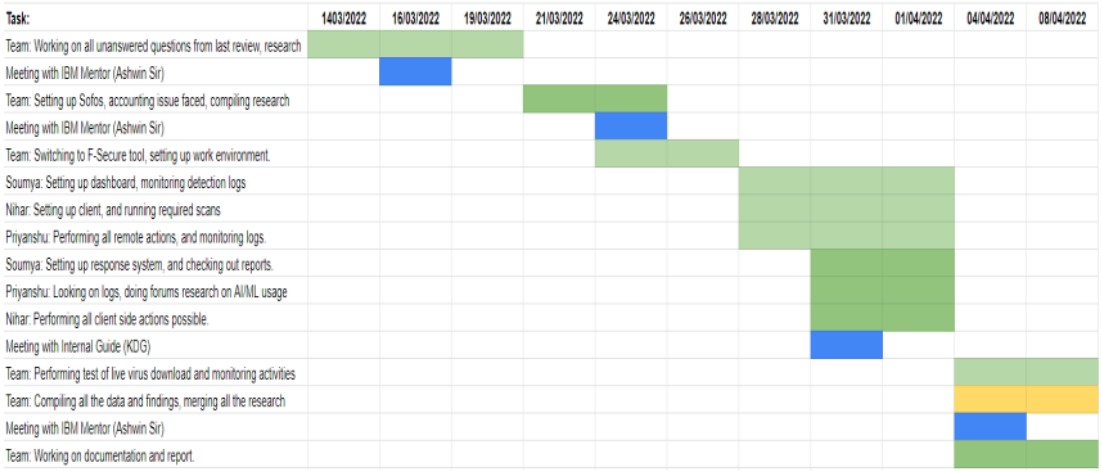
Soumya: Working on sandbox analyzer
Nihar: Working on testing out client side threat protection
Priyanshu: Constantly monitoring logs, reporting & dashboard
Meeting with IBM Mentor (Ashwin Sir)
Team: Compilation of data, and switiching to Comodo
Nihar: Setting up Comodo client, and performing required scans
Priyanshu: Endpoint device profiling, monitoring logs for same.
Soumya: Setting up Comodo control panel, adding users
Team: Compilation of data, and preparring new tasks for next week
Soumya: Working on remote patch management, and antivirus
Nihar: Client auto quarantine file system, threat management
Priyanshu: Remotely performing admin actions on data generated from client
Meeting with IBM Mentor (Ashwin Sir)
Team: Compilation of findings, working on points given by mentor
Soumya: Testing out Valkyrie an advanced protection layer
Nihar: Checking out security sub systems available for client
Priyanshu: Checking out Application & Device control from panel
Meeting with Internal Guide (KDG)
Meeting with IBM Mentor (Ashwin Sir)
Team: Compilation of all work and properly documenting it
Team: Preparing for a demonstration scenario for review
Team: Working on required documentation
Nihar: Finalising testing and findings on client
Soumya: Finalising findings on Valkyrie and difference b/w both tools
Priyanshu: Finalising findings on all logs and remote actions performed
Meeting with IBM Mentor [LIVE DEMO] (Ashwin Sir)

Timeline:

Task (14/03/2022 – 08/04/2022):

Team: Working on all unanswered questions from last review, research
Meeting with IBM Mentor (Ashwin Sir)
Team: Setting up Sofos, accounting issue faced, compiling research
Meeting with IBM Mentor (Ashwin Sir)
Team: Switching to F-Secure tool, setting up work environment.
Soumya: Setting up dashboard, monitoring detection logs
Nihar: Setting up client, and running required scans
Priyanshu: Performing all remote actions, and monitoring logs.
Soumya: Setting up response system, and checking out reports.
Priyanshu: Looking on logs, doing forums research on AI/ML usage
Nihar: Performing all client-side actions possible.
Meeting with Internal Guide (KDG)
Team: Performing test of live virus download and monitoring activities
Team: Compiling all the data and findings, merging all the research
Meeting with IBM Mentor (Ashwin Sir)
Team: Working on documentation and report.

Timeline:



Basic monthly strategy team was following:
Week 1 - setting up client with dashboard

Week 2 - setting up new rules /policy. Exploring the dashboard and mapping out all the possible logs. Letting the client generate some logs. Includes finding bugs in client / scanning logs.

Week 3 - exploring all client actions, client-based logs, client-based issue/quarantine.

Week 4 - remote operations, cloud sandbox tool, networking tool, contamination, and any new observation tools.

Apart from this week wise data compilation and catching up with new findings are done on weekends.

CHAPTER 7 (A) – DATA GATHERING

CHAPTER 7 (A) – DATA GATHERING

- In order to find out best EDR tool with maximum benefits, team did a research on all the available tools currently being used in industry. On base of this research we went with Bitdefender.

- **Features List:**

Features	VMware Cardon Black	Kaspersky EDR	Palo Alto Networks Traps and Cortex	Bitdefender GravityZone Ultra
User Behavioural detection				
Automated Remediation				
Vulnerability monitoring				
Device Control				
Analyst Workflow				
Guided Investigation				
Threat intelligence feed integration				
Custom rules				
Advanced threat hunting				
Unauthenticated device discovery				
Demo	Not Available	Company Demo Only	Company Demo Only	Available
	Hands-on activity	Add on cost	Available on same cost	Not Offered

Features	BlackBerry Cylance	Check Point Sandblast	ESET Enterprise Security	F-secure
User Behavioural detection				
Automated Remediation				
Vulnerability monitoring				
Device Control				
Analyst Workflow				
Guided Investigation				
Threat intelligence feed integration				
Custom rules				
Advanced threat hunting				
Unauthenticated device discovery				
Demo	Company Demo Only	Company Demo Only	Company Demo Only	Available
	Hands-on activity	Add on cost	Available on same cost	Not Offered

Features	SentinelOne	Symantec Endpoint Security Complete	Trend Micro Apex One	Microsoft Defender ATP
User Behavioural detection				
Automated Remediation				
Vulnerability monitoring				
Device Control				
Analyst Workflow				
Guided Investigation				
Threat intelligence feed integration				
Custom rules				
Advanced threat hunting				
Unauthenticated device discovery				
Demo	Company Demo Only	No Demo	Company Demo Only	Only for Microsoft Windows
	Hands-on activity	Add on cost	Available on same cost	Not Offered

Features	McAfee MVISION	CYNET	Cybereason	Comodo Dragon
User Behavioural detection				
Automated Remediation				
Vulnerability monitoring				
Device Control				
Analyst Workflow				
Guided Investigation				
Threat intelligence feed integration				
Custom rules				
Advanced threat hunting				
Unauthenticated device discovery				
Demo	Company Demo Only	No Demo	Company Demo Only	Only for Microsoft Windows
	Hands-on activity	Add on cost	Available on same cost	Not Offered

CHAPTER 7 (B) – OUR FINDINGS

Bitdefender GravityZone Ultra VS Comodo Dragon

Bitdefender and Comodo both use cutting-edge detection technology; however, Bitdefender concentrates on extra features while Comodo maintains a lightweight, streamlined service.

Bitdefender provides protection against a wide range of threats. The Safe File Vault protects you from malware, while the Webcam Shield keeps hackers out of your stream. A Virtual Keyboard and a Password Manager are among the features that help safeguard your passwords. Bitdefender will also scan any new hardware you connect to your device, such as USB devices and external storage, to ensure you don't get infected. Unfortunately, all of these capabilities can cause your smartphone to slow down. While the auto-updates help to mitigate this effect, it remains a significant issue.

While Comodo's extra security capabilities are limited, it does employ unique techniques to enhance its security. Its sandboxing technology places all files in a virtual environment to ensure their security. It also employs cloud-based whitelisting to ensure that no downloads are checked more than they need to be. If it detects a problem, the Application Control locks down your system and only uses apps that are recognized to be safe.

WithSecure

WithSecure Endpoint Security is an AI-powered, cloud-native endpoint protection solution that you can deploy and manage from a single console. It protects your firm from modern threats like ransomware, never-before-seen malware, and zero-day vulnerability exploits by working across all of your endpoints. From vulnerability management to collaborative protection to endpoint protection, detection, and response, it handles everything from a single security panel. Individual solutions can be employed for specific needs, or all of them can be combined for complete protection. For each attack detected, you'll receive a forensics flow chart that shows the threat's origin (as far as WithSecure can tell) and data for each step taken.

Our findings:

- Client tool seems to be lag free for most parts, have an exceptional detection system which auto detects and quarantines a file keeping the client secure.
- Best part about this tool, is in its dashboard. The in-depth malware analysis it does, giving a flow chart for each attack.
- Auto detects any temp file, downloaded file, files over USB or old malicious files instantly and quarantines them.

So, which one is best?

- Comodo is by far the most practical solution we have tested in terms of its execution and antivirus layers. Although, it makes client slightly lagging because of its own services running.
- BitDefender is by far the best UI, light weight EDR solution we have tested. Gives proper remote controls, executive summary is on point, network discovery, proper contamination of malicious files. Although it's on a bit expensive side, customer support is not great.
- WithSecure seems to sit right between Comodo and Bitdefender in terms of background performance on client. It has a unique way to show malware analysis from previous scans, client-side monitoring is better and so are the detection logs. Although, it seems to have a lot of features to be locked under full premium mode which makes it sit right in between Comodo and BitDefender.

CHAPTER 7 (C) – COMPARISION

CHAPTER 7 (C) – COMPARISION

Throughout our experience we have gathered all information related to EDR, there performance, impact on client device, threat protection system, etc. After analyzing every observation on all three tools i.e. BitDefender GravityZone Ultra, Comodo Dragon and WithSecure. we came down to the following comparison:

- **Admin web portal, quick glance:**
  Bitdefender has the cleanest and most organized web portal among all three tools. It's UI is user friendly, looks better and has quick response times. Moreover, the executive summary of Bitdefender is better followed by Comodo and then followed by WithSecure.

- **Client Tool and it's functionality:**
  WithSecure offers the lightest Client tool among all three. It's easy to install requires no manual scan to begin with and has a quicker detection. It also allows client to see logs, malware details and check containment files. Where it lacks is giving the client any virtual environment solution to execute any malicious file without flagging it off from system / turning the real time protection off.

  Comodo on other hand is a resource heavy client tool which needs a lot of processing power to run all the services it offers and at the same offers the maximum client options among all three. It gives client a full control over scan logs, quarantine files, options to restore them or remove them completely from server, provides a virtual environment for script execution, automatically runs any slightly malicious script on its safe zone, network discovery and rest all features are similar.

  Bitdefender comes with a heavy client but it's not resource hungry, it's well optimized and sit's right in between WithSecure and comodo in terms of response time, UI, usability and so on.

- **Threat Detection System:**
  Comodo has the best threat detection system among all three, also has a bit of a tendency to false flag non malicious files as malicious. It uses a filebase system to flag files as malicious. It tries to make a similarity index between it's own records and given file, if it gets any match over 5% file gets flagged as malicious or not safe to run on client and gets transferred on virtual environment.

  WithSecure has the next quickest threat detection after comodo (in terms of fraction of seconds) although it has a side effect, WithSecure doesn't flags ZIP files as threat or malware unless they have been scanned separately, which is not the case with other two tools. Threat detection of WithSecure gives a very detailed malware history and study if one wishes to look more in logs.

  BitDefender uses a sandbox analyzer method to counter act with any malicious files, normal file detection is quick and it flags any malicious files enters the system and so on. It doesn't have a detailed malware analysis but offers almost similar threat detection like other tools. It uses it's own client collected data of file activity as detection layer.

  Note: All tools have a great threat detection system deployed which uses AI/ML techniques to filter files and perform automated actions, this comparison is more directed towards finding any difference among three tools we used.

- **Malware Analysis:**
  Being a Cyber Security student, we really wish to know more about a malware or malicious file

that may have entered through the client, in terms of extensive malware analysis and summary, WithSecure is the best one among them, it has a flowchart view which shows the route map of malware, and details like SHA value, hash value, first found, and more details similar to virustotal.com.

Followed by Comodo and Bitdefender both has a better malware analysis, because of there antivirus system which pulls out few details of malicious files from CVE MITRE records.

- **Remote Actions from web portal to clients:**
  Comodo has the maximum remote client actions possible such as remote desktop, remote restart, remote security update, remote package updater, file transfer dashboard etc.

  Bitdefender is second in line with remote features, it allows remote file transfer, basic remote scans, remote restart and remote security update.

  WithSecure has the most limited remote features, it only allows remote restart and remote security updates.

So overall if we have to select one, then it will be Comodo Dragon as it comes with almost every feature one needs from EDR tool, along with its wide features over admin panel and client.

We recommend:
Comodo Dragon > WithSecure > BitDefender GravityZone Ultra

CHAPTER 8 – CHALLENGES FACED

CHAPTER 8 – CHALLENGES FACED

During this entire project, we faced a lot of challenges, below is the list of those with how we passed them and what actions we took.

1. Running an active server for client listeners.

- Initially we were working on coding a tool to perform Endpoint protection and remediation. We faced an issue with linking client with server, since we were not having any server system to hook them up for proper listening mode. Upon few trials it appeared that IBM server or any other server system is off limits.

2. Finding a financial application

- We tried a variety of financial apps, web apps, projects made by various developers but none were actually meeting our requirements for the project. Later we chose to work with Altoro Mutual vulnerable webapp as our financial tool.

3. Change of approach

- It appeared to us that we were spending a lot of time just to figure out some technical issue we were facing such as lack of a proper working server and database system. Plus building an Industry level EDR tool seems to be off the limits for a project to be done in 4 months, upon having a thorough discussion with our Mentors we switched to a different approach were we started taking hand's on experience of Industry grade EDR tools and document our experience.

4. Getting a Trial for EDR tools

- According to our research we got over 30 tools on our watch, upon which of course we picked top 10 to consider working on. So, we started from No. 1 tool and ran into an issue of not getting any remote instant trial option, so we kept switching and applying for trials on multiple tools till we reach No. 4 tool Bitdefender which offered the trial and our project started.

5. Client devices

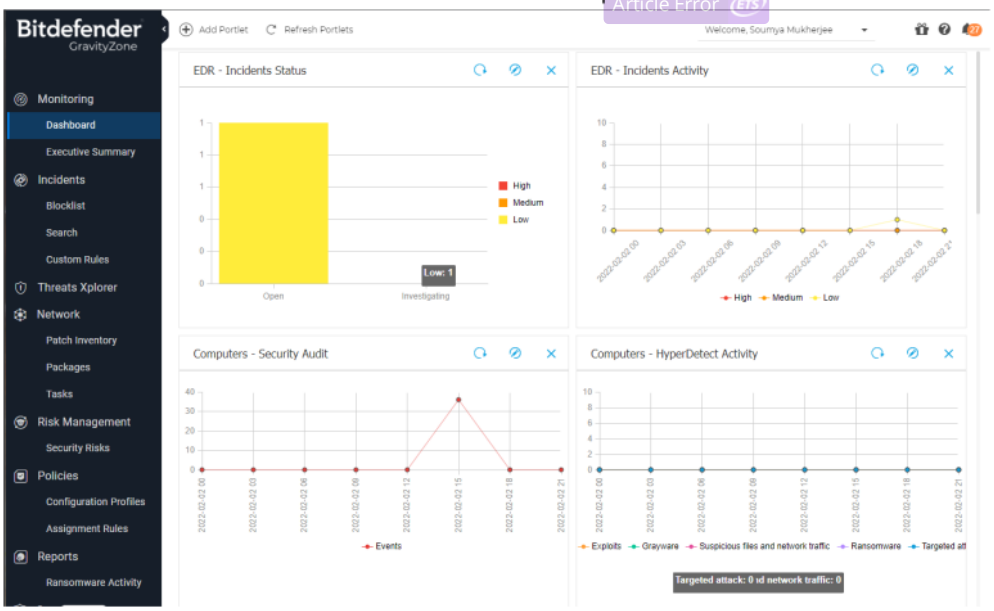
- Very important part of testing an EDR solution is having a proper client device which can hold all the services one tool has to run and still perform for normal tasks. It was hard for us to setup on entry level laptops we had, hence setting up a client became a challenge as it was continuously spiking the processor usage on devices. We fixed the issue by setting a desktop client with a higher specification, which was then able to handle all the services. Only limitation with this scenario was it can only be reached remotely and one of our team members has to completely dedicate his time on setting up client.

6. Finding technical answers

- When we take hands on experience on readymade industry grade tools, it's really difficult to know how they are actually processing all the background work. Like managing logs, threat detection, remote client handling and so on. We somehow overcame this issue by doing intensive research on their forums, emailing their teams, and web searches to get very detailed information.

CHAPTER 9 (A) – IMPLEMENTATION (BITDEFENDER)

- Initial experience, on start-up you will find dashboard:

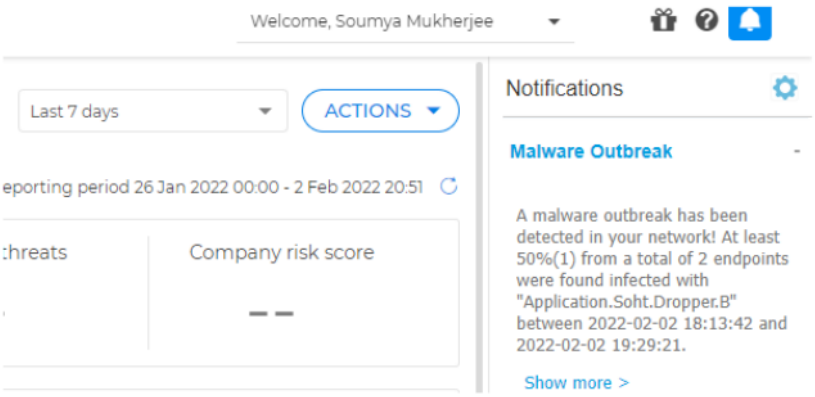


Contains data like:

EDR:
Incident Status
Incident Activity

Computers:
Security Audits
HyperDetect Activity

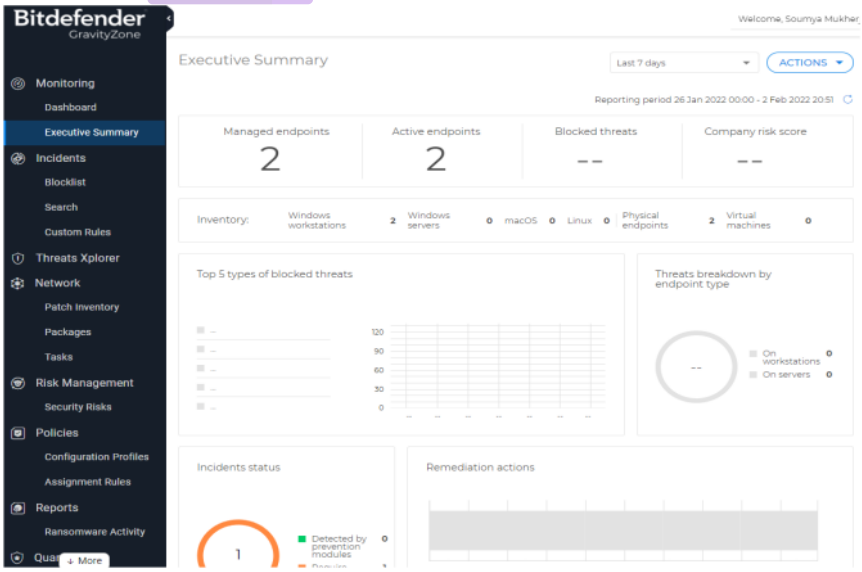
- Up at right side corner, we have user logged in, followed by notification tab, for example: here we have a malware outbreak notification.



- Next, we have Executive Summary, it contains all data like clients registered, clients active, overall threats detected, top 5 types of threats and so on.

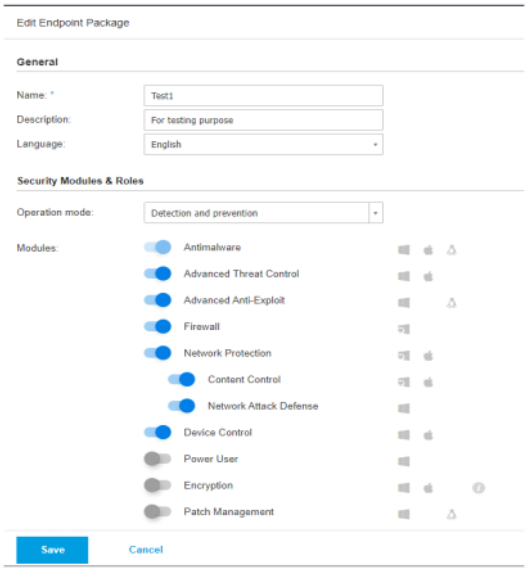
Missing "," ETS

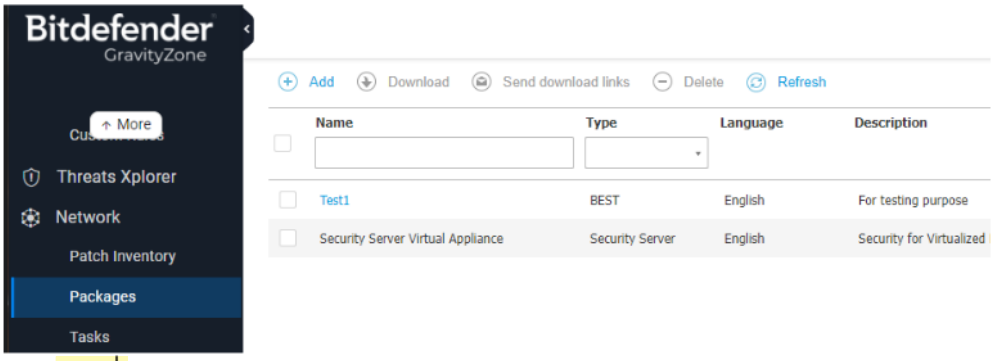
Article Error ETS



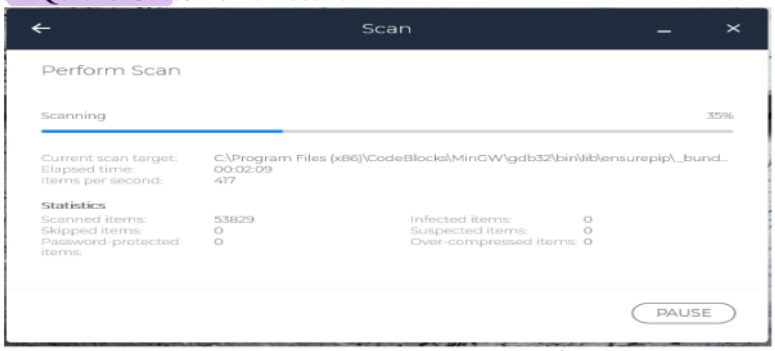
- Setting up clients, it's really easy to setup clients, in Network > Packages tab, one can setup a client package and then share the download link to register the endpoint.

Verb ETS

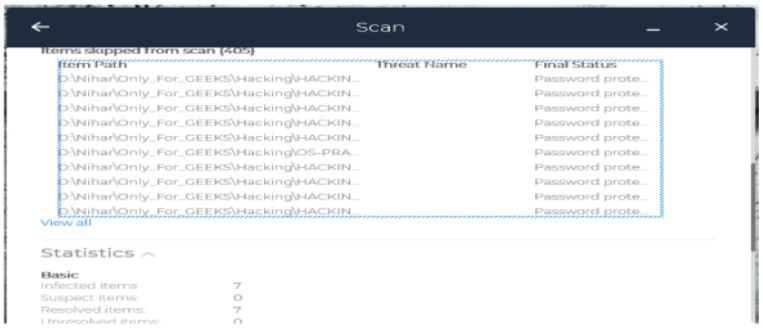




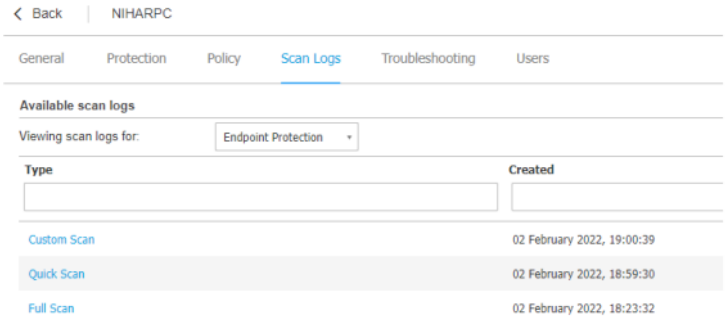
- Once client is ready, perform a full scan to initialize a report, for the endpoint.
- Scan can be a Quick / Custom / Full scan.



- Once a scan is done, the report for same is displayed in client as well as portal

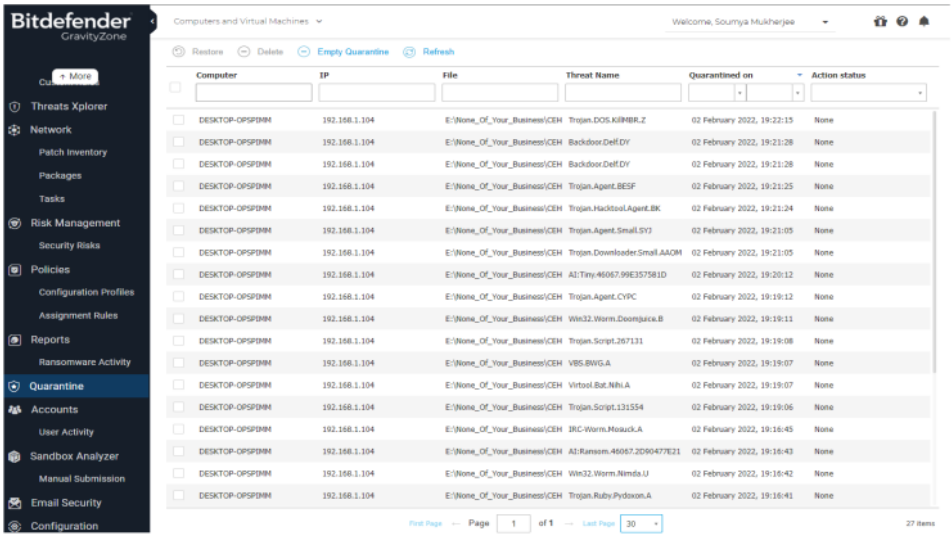


Client Output

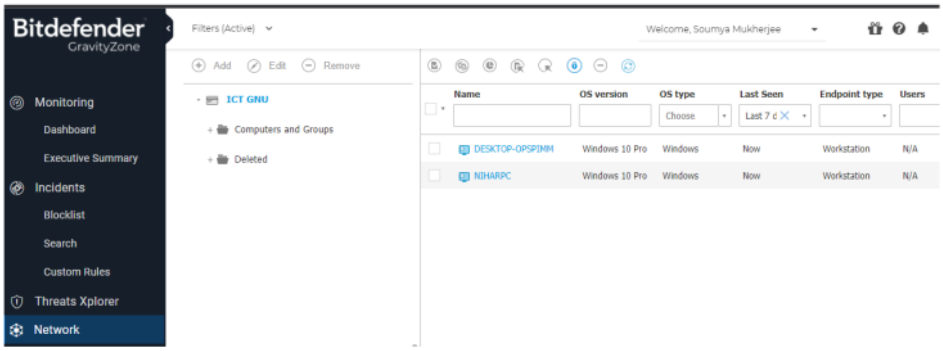


Web Panel Output

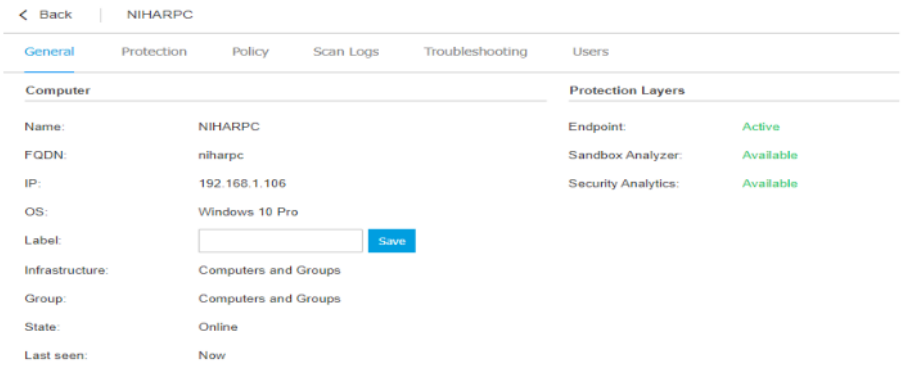
- In case malware files are detected it gets quarantined automatically and can be viewed in web panel.



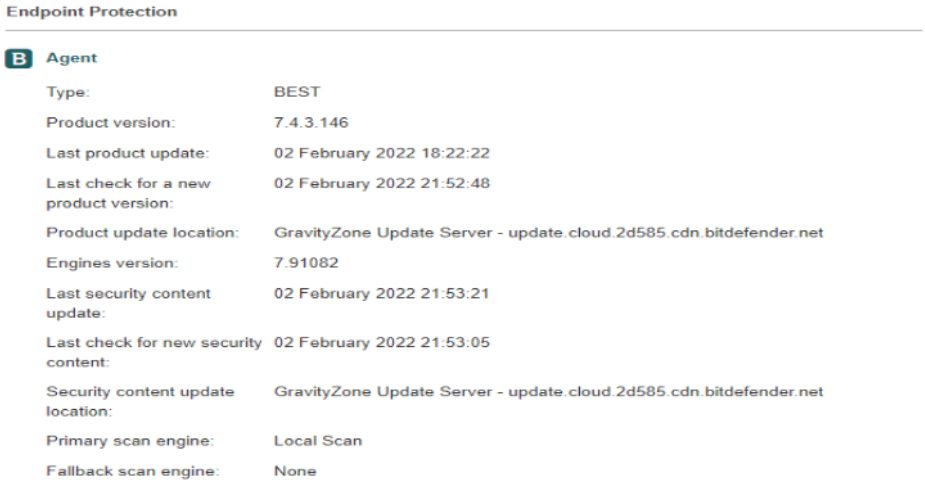
- We can view all the endpoint devices at network tab



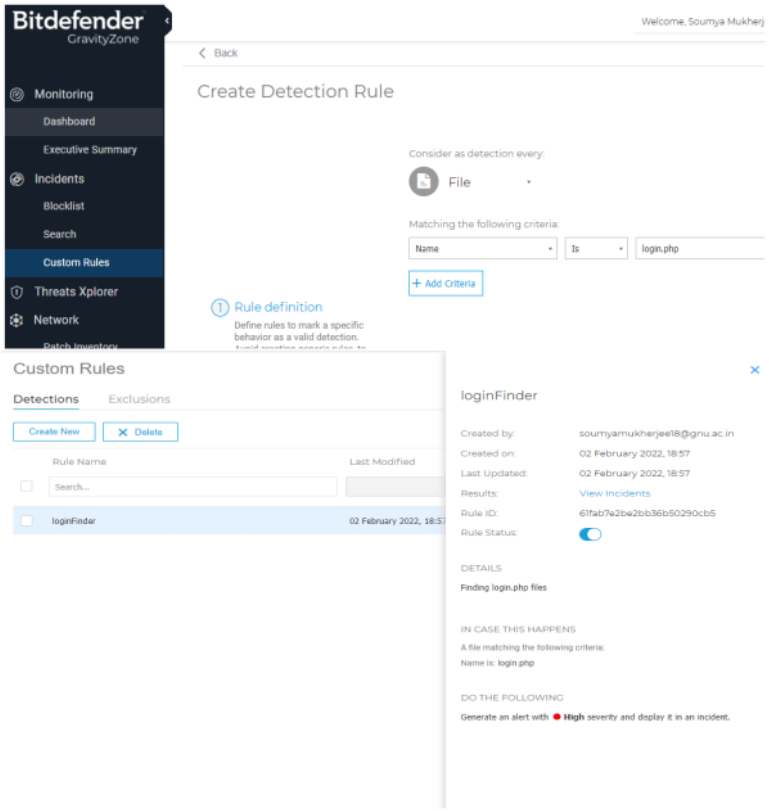
- We can view general information about the computer



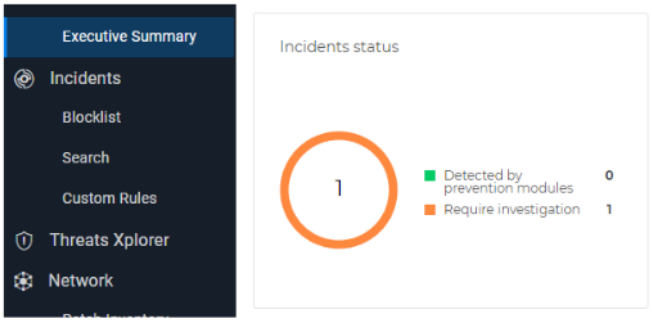
- Followed by information such as updates, version, timestamps, etc.



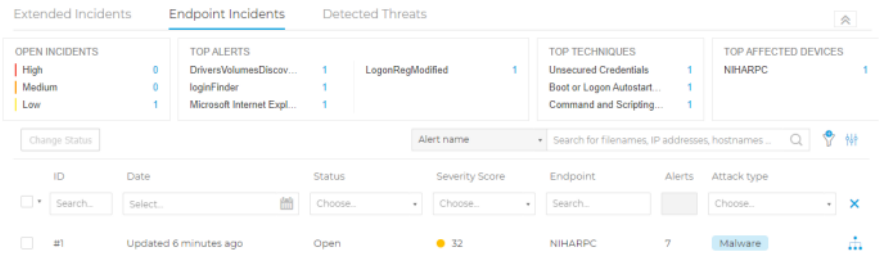
- Next, we create a custom rule, and make it to instantly flag “High” severity if it finds a file with “login.php” name.



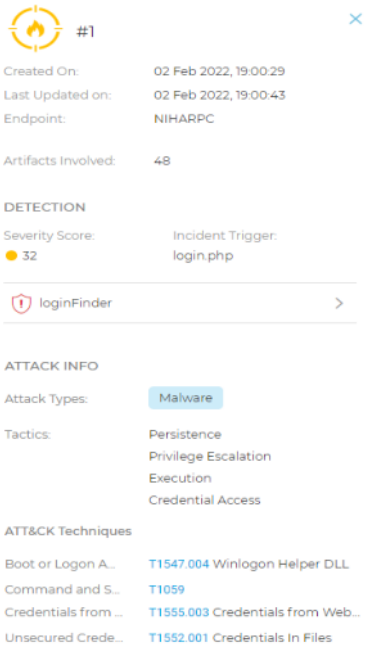
- After a custom scan, we found an Incident notification, stating require investigation.



- Upon checking we find one flag against a file found in one of our endpoint devices.

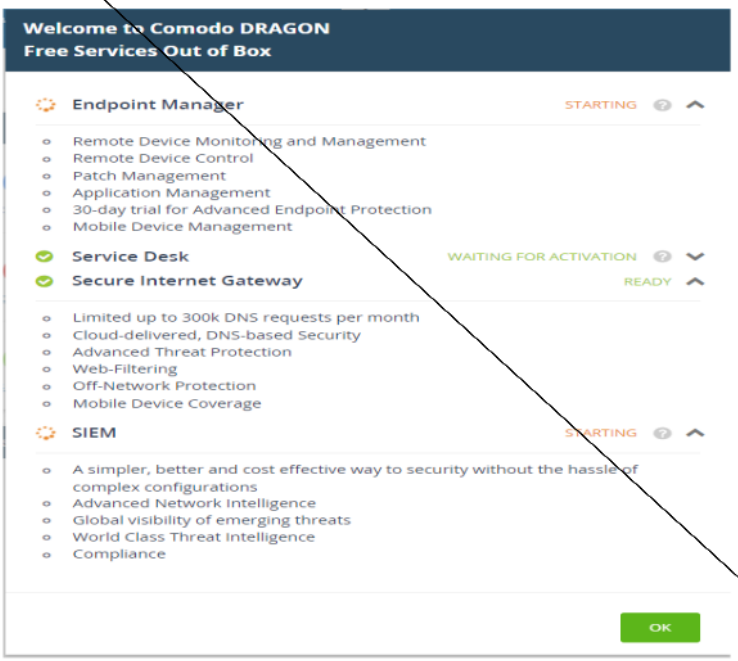


- Malware details:

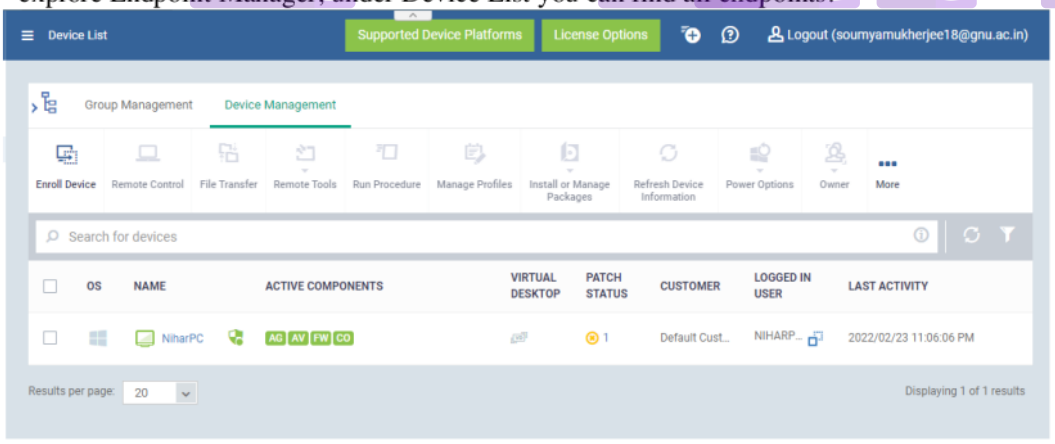


CHAPTER 9 (B) – IMPLEMENTATION (COMODO)

- Setting up comodo client and web portal is really easy. First we will start with web portal, go on their website and request for a free trial, once done login with your account, and you will be greeted with this screen:

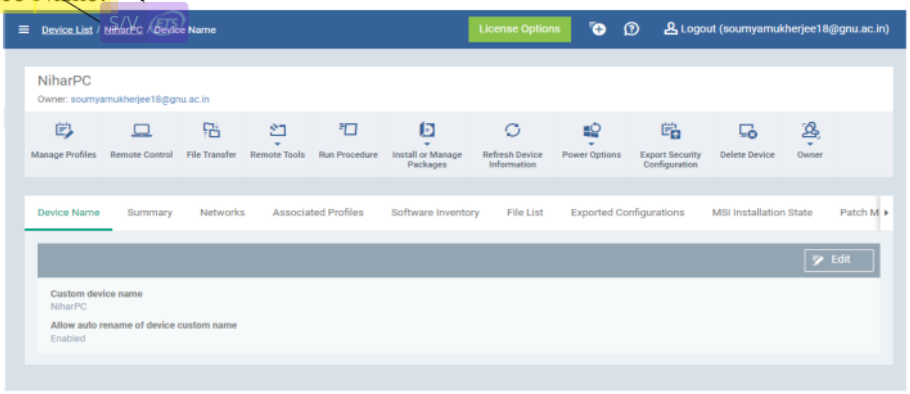


- To set up client, it's easy just need to install package in client and it will setup automatically. Let's explore Endpoint Manager, under Device List you can find all endpoints.

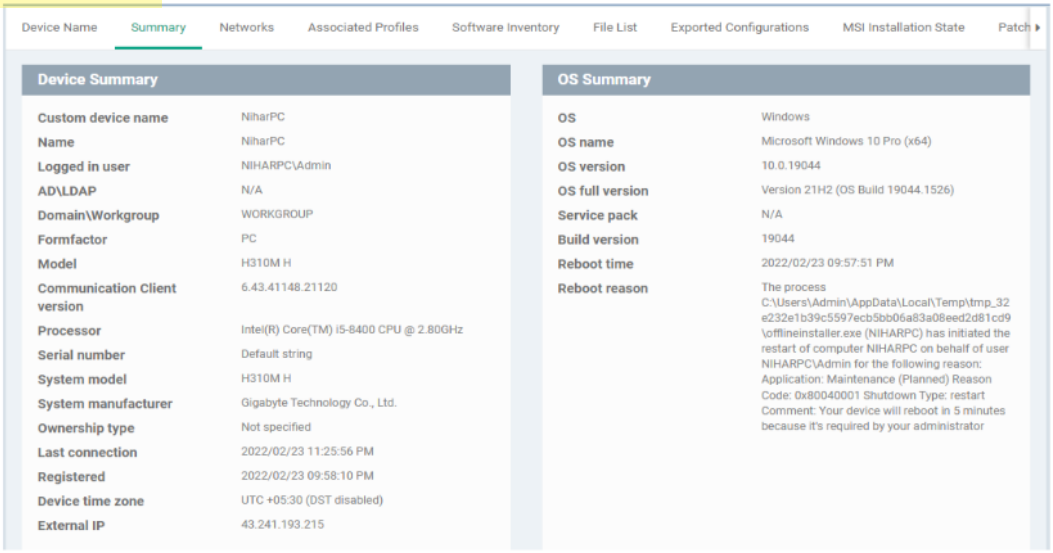


- Details covered under device profiling:

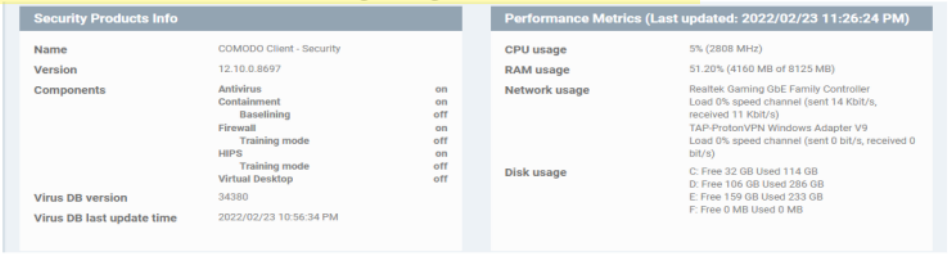
Device Name:



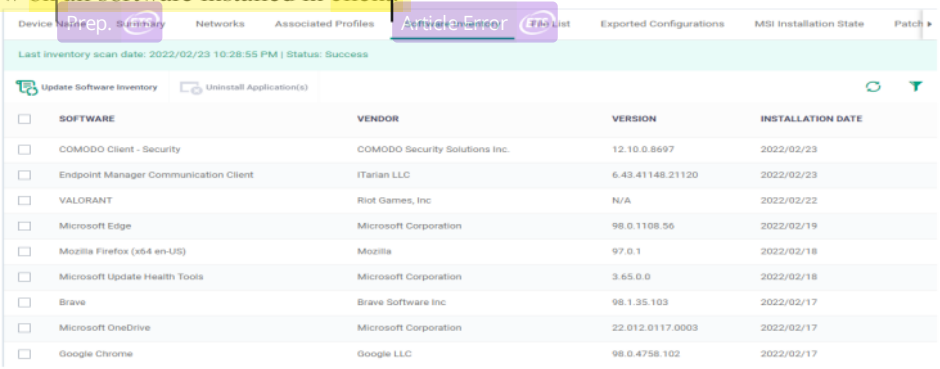
Summarized Info:



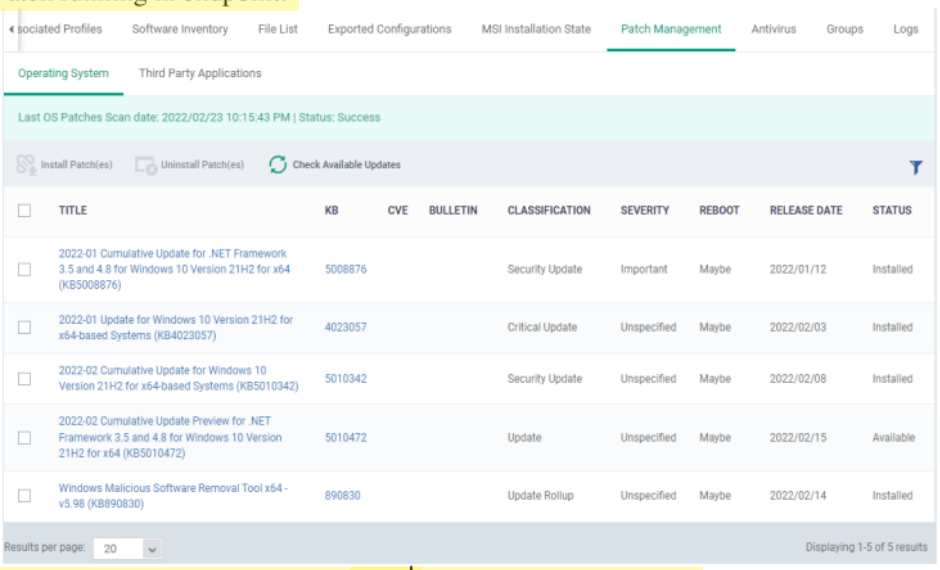
Security Patch Details and information regarding Performance metrics:



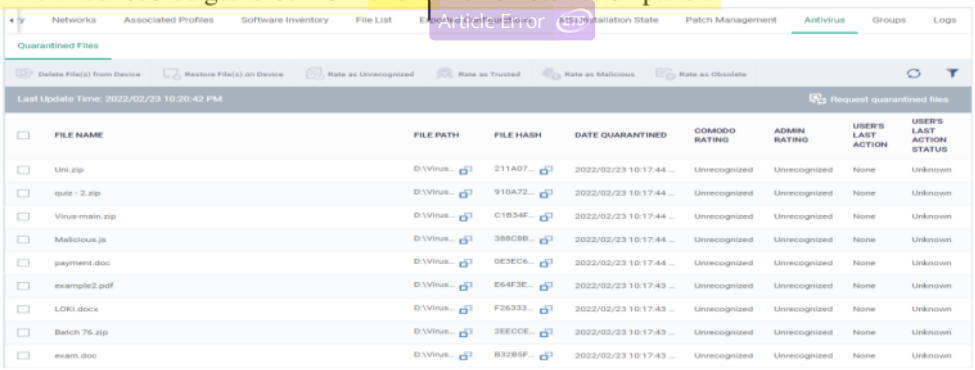
Quick view on all software installed in client:



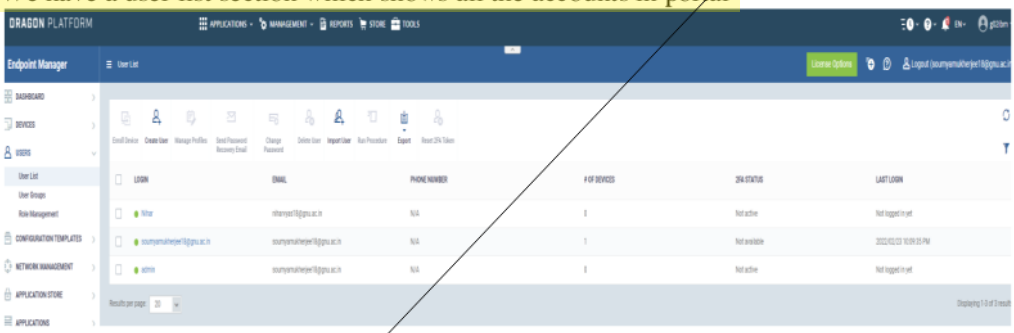
Security Patch running in endpoint:



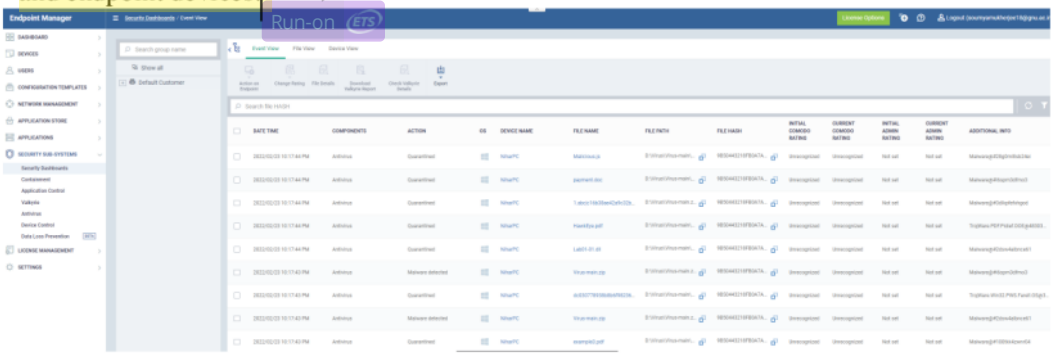
Finally, Antivirus records gathered from client and remote action panel:



- We have a user list section which shows all the accounts in portal

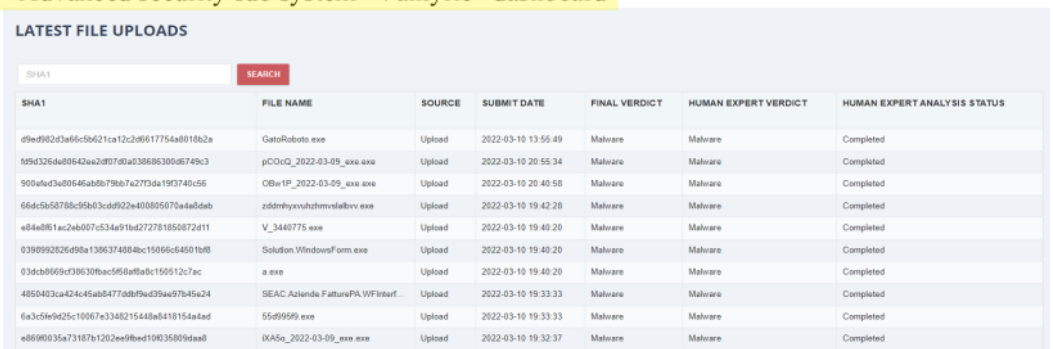


- Security Dashboard gives us the root logs of all sorts of antivirus actions taken on malicious files and endpoint devices.

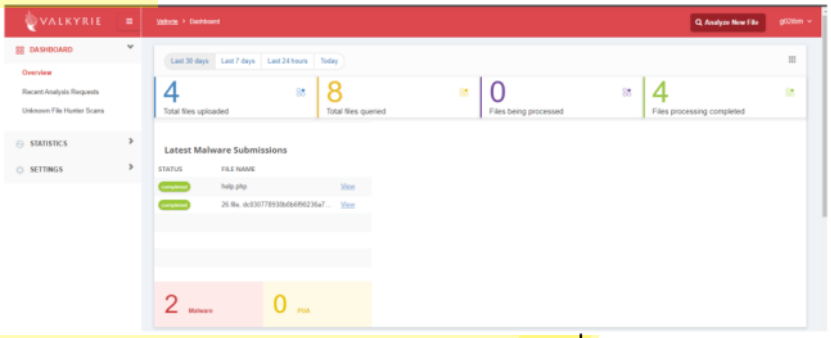


- Web portal has a special tab for Valkyrie logs:

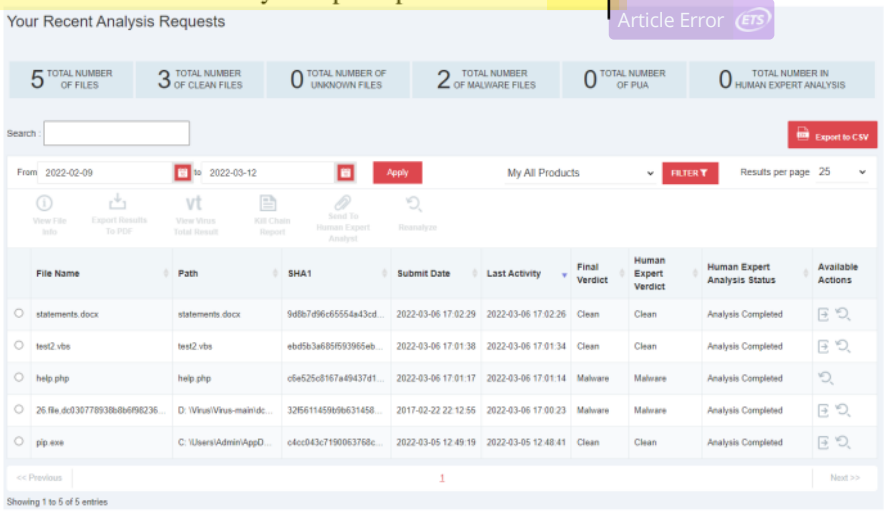
- Advanced security sub system “Valkyrie” dashboard



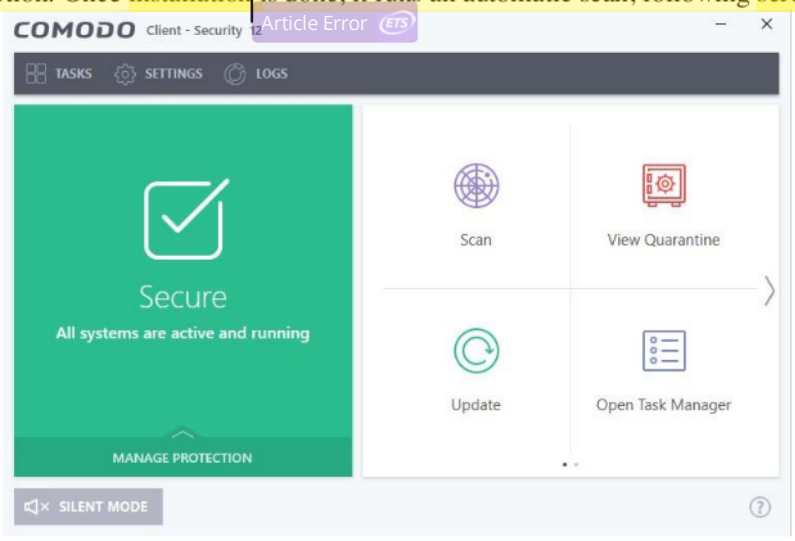
- Overview dashboard:



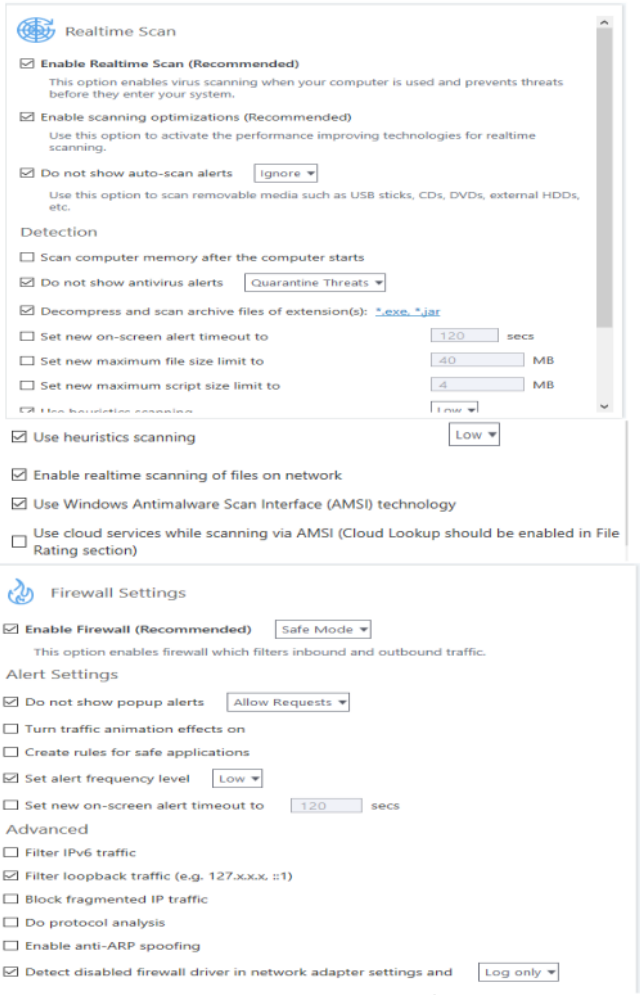
- We can also view recent analysis reports performed in client:



- Client Section: Once installation is done, it runs an automatic scan, following screen is displayed:

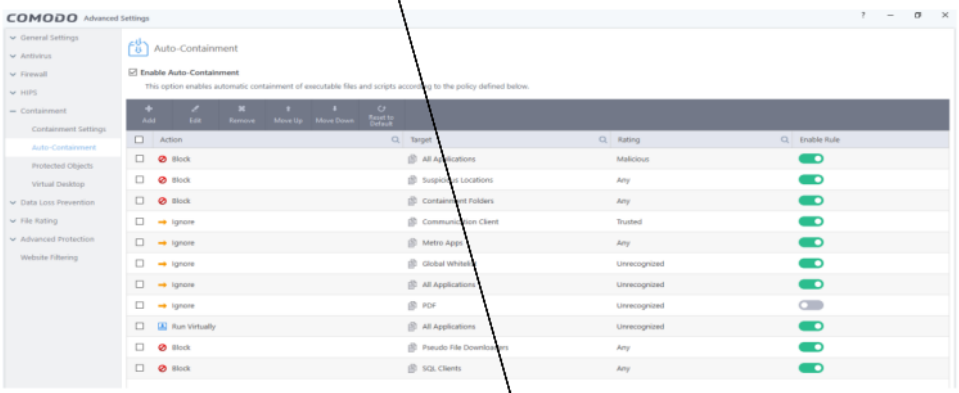


- Client comes with advanced settings options one can directly setup in client



- Comodo client offers auto containment of malicious files along with allowing client logs and client actions on that very endpoint device:

Missing "," ETS



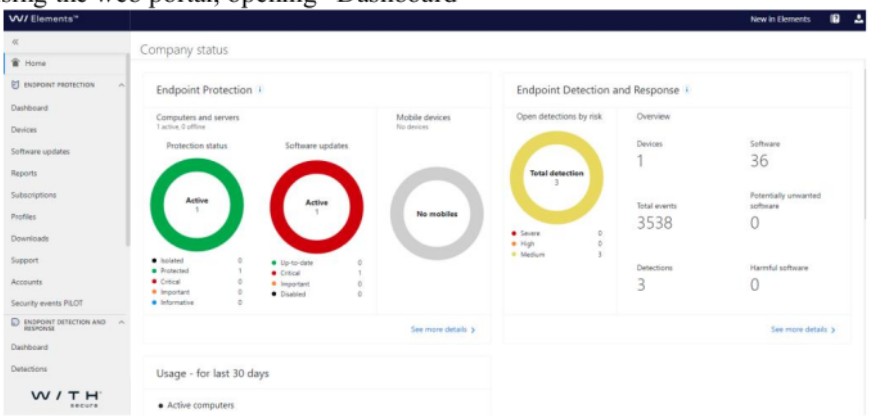
- Manual rulesets and predefined rulesets are all mentioned under HIPS ruleset section so that client doesn't interrupt with normal OS operations.

Sp. ETS
Sp. ETS
Sp. ETS
Garbled ETS


COMODO Advanced Settings
General Settings
Antivirus
Firewall
HIPS
HIPS Settings
HIPS Rules
Rulesets
Protected Objects
HIPS Groups
Containment
Data Loss Prevention
File Rating
Advanced Protection
Website Filtering
Rulesets
The following rulesets are defined on this computer:
Add
Edit
Remove
Ruleset Name
Allowed Application
Windows System Application
Isolated Application
Limited Application

CHAPTER 9 (C) – IMPLEMENTATION (WITHSECURE)

- Initialising the web portal, opening “Dashboard”

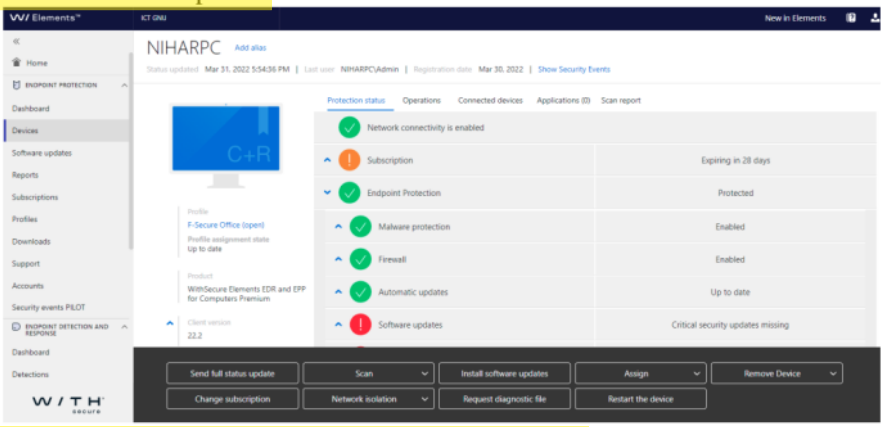


We can view all the endpoints, there security state, software updates, any critical notifications all at one place.

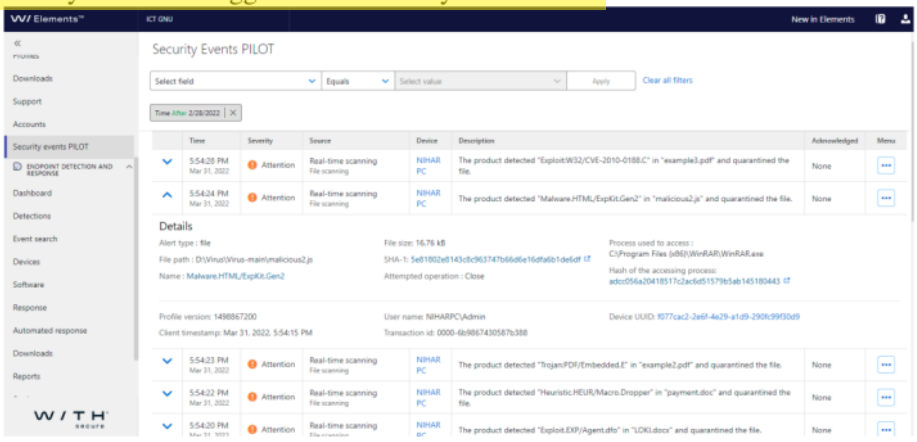
Confused

- Adding an endpoint device is easy, just download the package and install it, once done it will auto reflect on the web portal

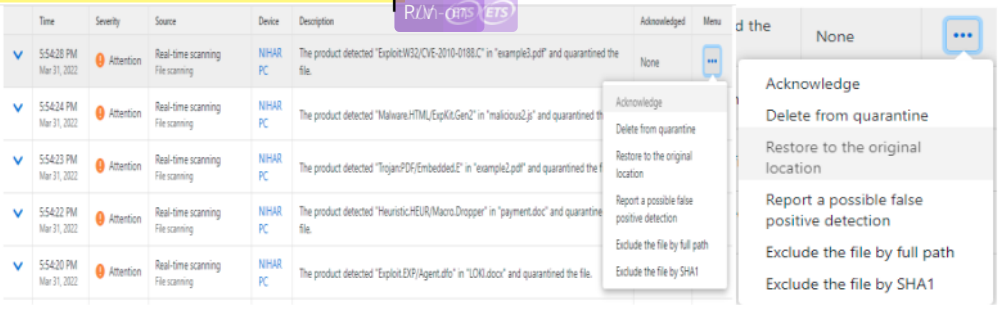
Missing ","



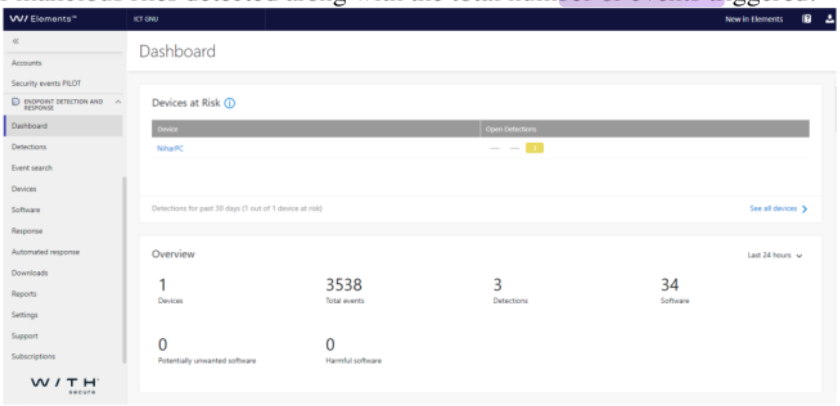
- All security events are logged under Security Events Pilot



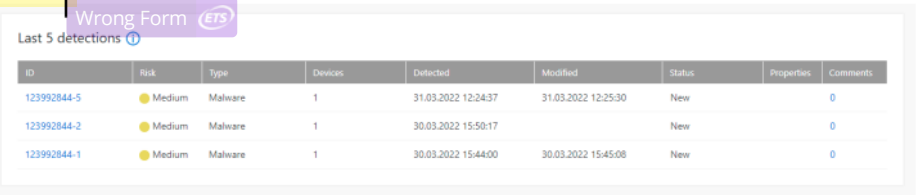
- For example, one file got flagged as malware a.k.a false positive and you wish to restore it, can be simply done by doing the following.



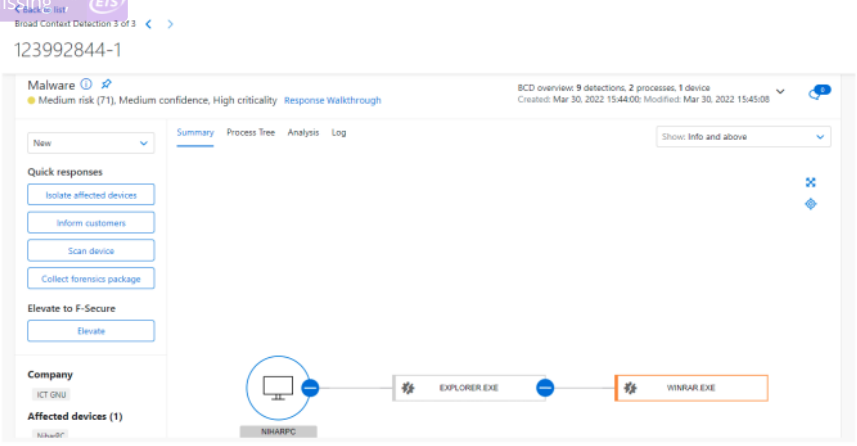
- Detection and Response has a different dashboard to offer, which basically shows total endpoints and total malicious files detected along with the total number of events triggered.



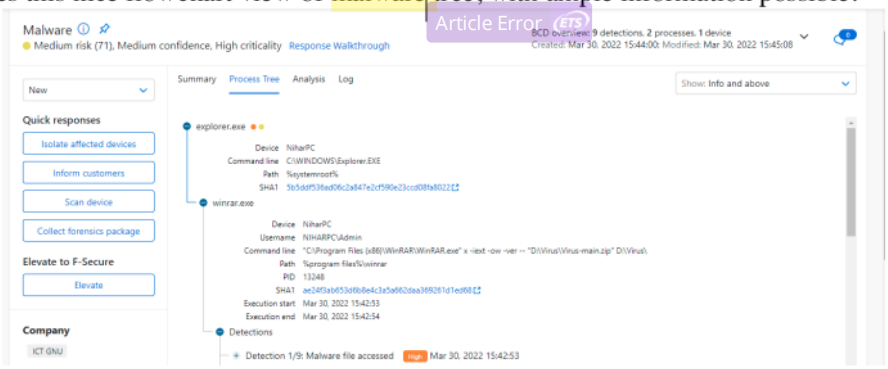
- Detections:



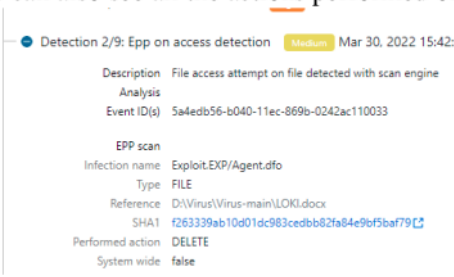
- Now for example, we wish to gather more info on the detected malware, simply click on it.



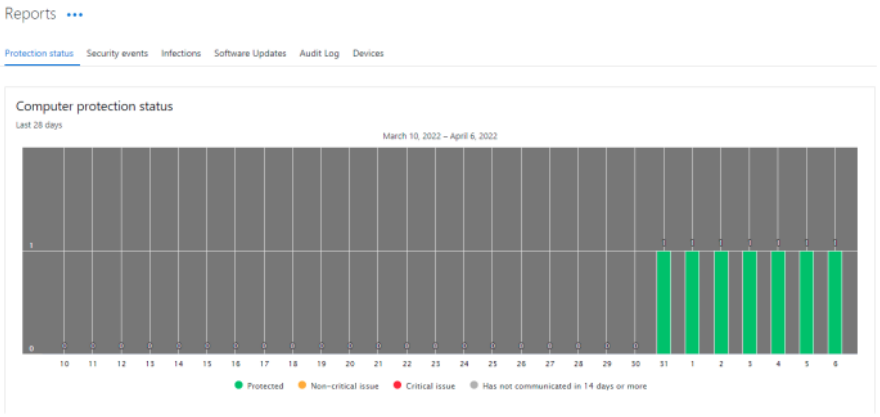
- It gives this nice flowchart view of malware tree, with ample information possible.

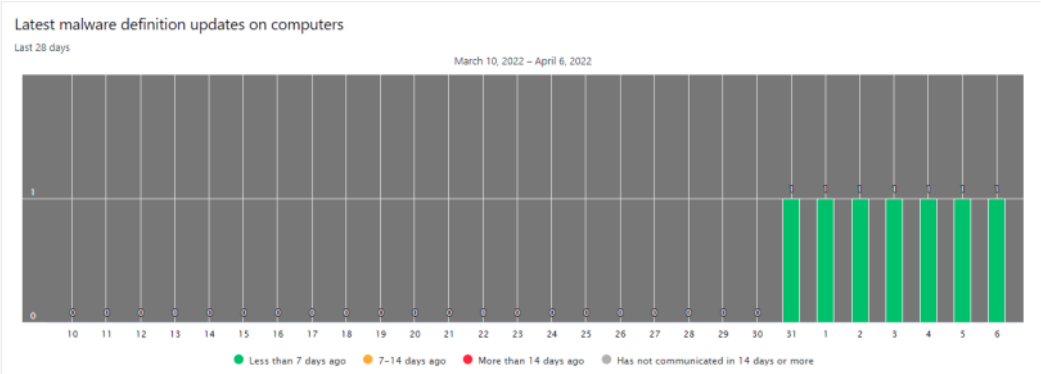


- Followed by, we can also see all the actions performed on each detection:

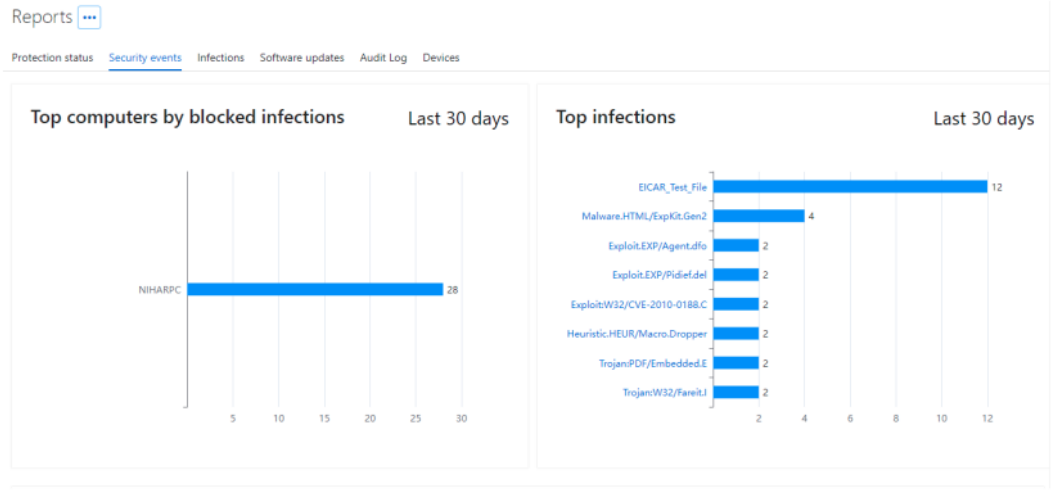


- Report logs for automated actions:

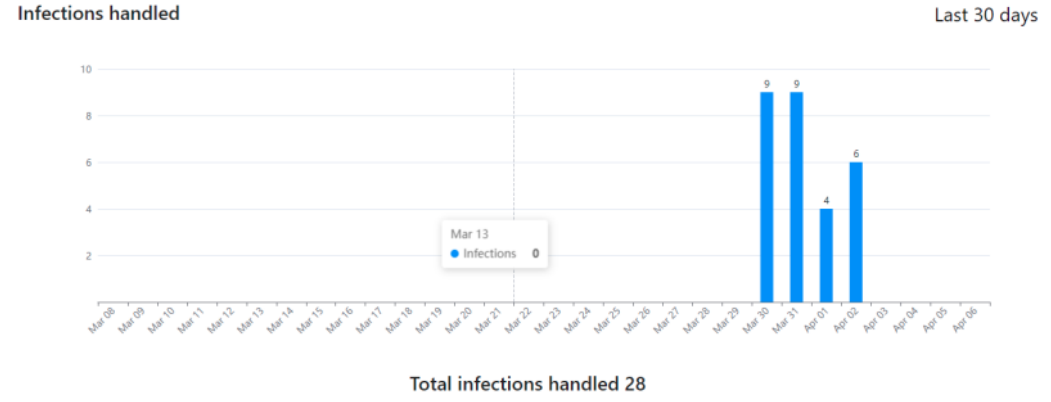




- Quick glace view of which endpoint is getting compromised quicker along with which malware view:

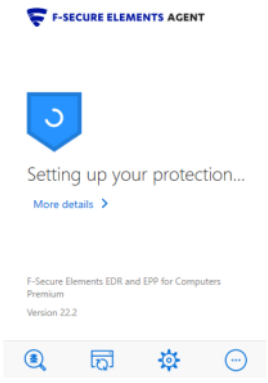


- Graphical representation of data:

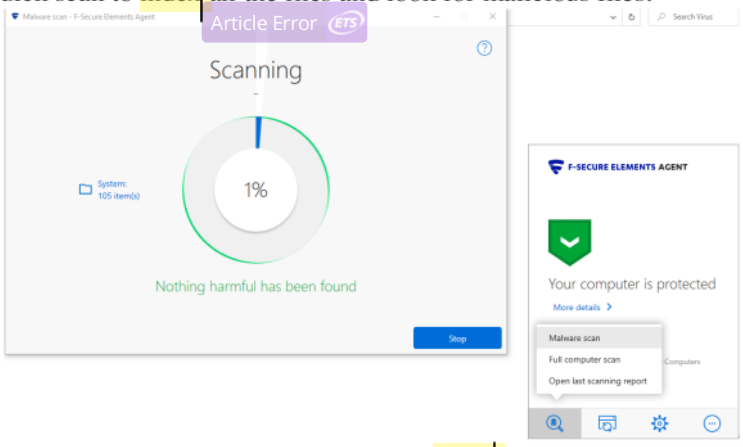


Total infections handled 28

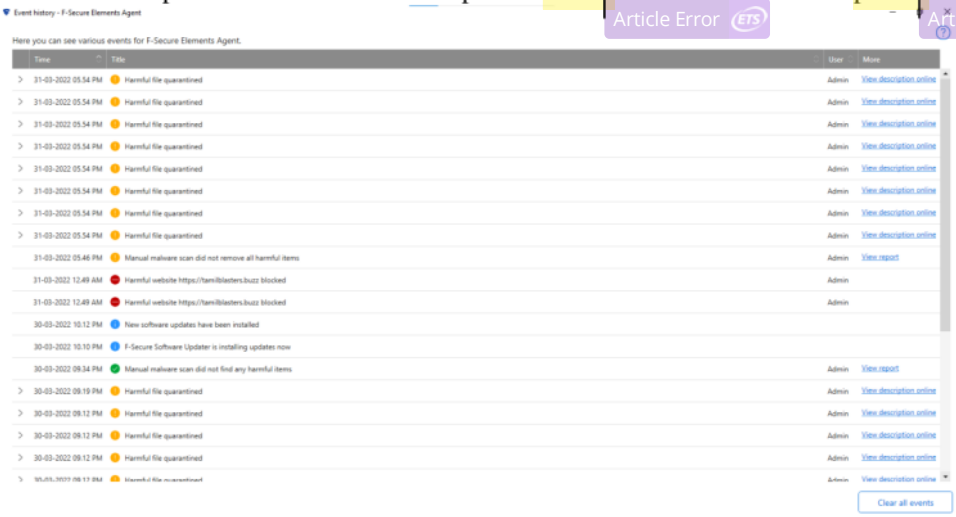
- Client-Side Initialisation:



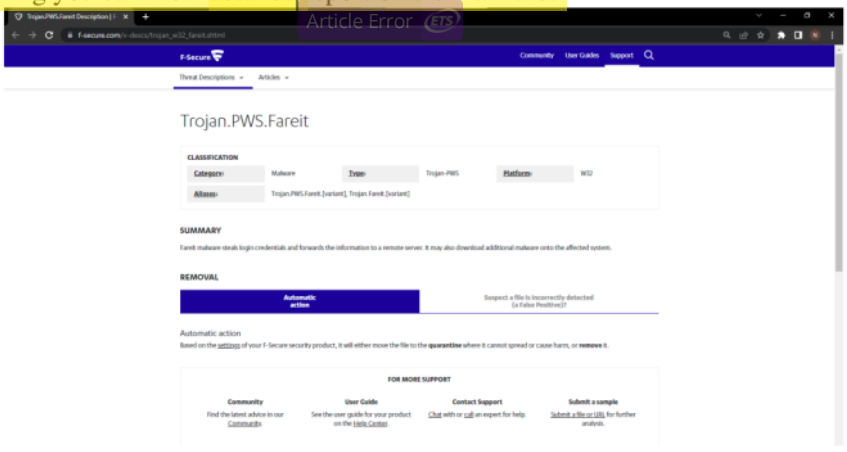
- Running a quick scan to index all the files and look for malicious files.



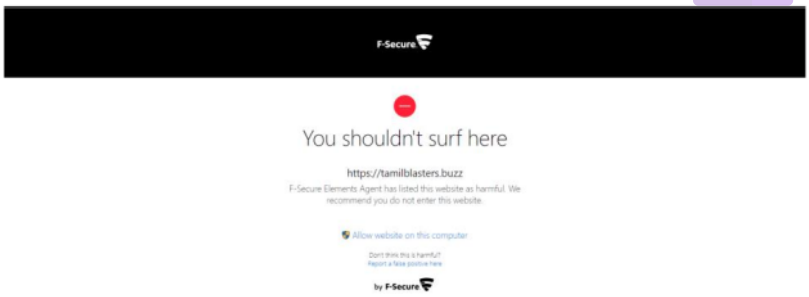
- Once a scan completes it sends a detailed report to client as well as shows it in portal.



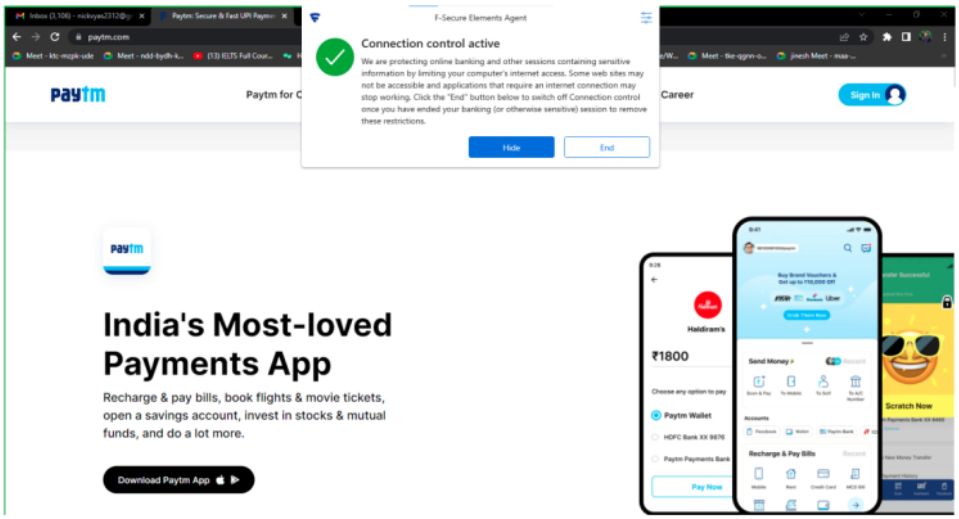
- On clicking you can view detailed report on the malware:



- Client tool also provides malicious link blocker for secure we browsing.



- Key highlight feature making it better for financial applications, it runs a secure antivirus layer once you try to access finance web apps:



CHAPTER 10 – CONCLUSION

CHAPTER 10 – CONCLUSION

Very precise tool in identifying malicious files, automatic detection and action taken upon a scan, client-side devices are monitored for any unusual activity, ease up security, by providing a dashboard and security dashboard with remote actions. Anti-Virus techniques, Valkyrie security sub system and Sandbox Analyzer allows us to run external files in a safe virtual environment. WithSecure detailed malware analysis and quick responsive client makes it easy to know information on detected malwares and securing client.

CHAPTER 11 – REFERENCES

- https://www.crowdstrike.com/endpoint-security-products/falcon-endpoint-protection-enterprise/
- https://www.bitdefender.com
- https://mcaffe.com/security-awareness
- https://github.com/tarcisio-marinho/PayloadIdentifier
- https://platform.comodo.com/
- https://elements.f-secure.com/

G02 IBM Report Final

ORIGINALITY REPORT

4%	3%	0%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	archive.org Internet Source	2%
2	Submitted to Ganpat University Student Paper	1%
3	es.scribd.com Internet Source	<1%
4	www.coursehero.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

G02 IBM Report Final

PAGE 1

PAGE 2

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to remove this article.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Garbled Grammatical or spelling errors make the meaning of this sentence unclear. Proofread the sentence to correct the mistakes.

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **a**.

Article Error You may need to use an article before this word.

PAGE 3

PAGE 4

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Article Error You may need to remove this article.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 5

PAGE 6

Possessive This word may be a plural noun and may not need an apostrophe.

Article Error You may need to use an article before this word.

PAGE 7

PAGE 8

PAGE 9

PAGE 10

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Hyph. You may need to add a hyphen between these two words.

PAGE 11

Dup. You have typed two **identical words** in a row. You may need to delete one of them.

PAGE 12

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 13

PAGE 14

Article Error You may need to use an article before this word.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word.

PAGE 15

PAGE 16

Article Error You may need to use an article before this word. Consider using the article **a**.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

PAGE 17

Prep. You may be using the wrong preposition.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word.

PAGE 18

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word.

PAGE 19

Article Error You may need to use an article before this word. Consider using the article **a**.

Article Error You may need to use an article before this word.

PAGE 20

PAGE 21

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

PAGE 22

PAGE 23

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

Article Error You may need to remove this article.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word. Consider using the article **the**.

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Confused You have used **there** in this sentence. You may need to use **their** instead.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Confused You have used **it's** in this sentence. You may need to use **its** instead.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Missing "," You may need to place a comma after this word.

Confused You have used **it** in this sentence. You may need to use **its** instead.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

PAGE 26

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

Article Error You may need to use an article before this word.

Confused You have used **there** in this sentence. You may need to use **their** instead.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Missing "," You may need to place a comma after this word.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word.

PAGE 27

PAGE 28

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Confused You have used **were** in this sentence. You may need to use **where** instead.

Missing "," You may need to place a comma after this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

Article Error You may need to use an article before this word. Consider using the article **the**.

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word.

PAGE 29

PAGE 30

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

PAGE 31

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

PAGE 32

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

PAGE 33

Article Error You may need to use an article before this word.

PAGE 34

PAGE 35

PAGE 36

PAGE 37

PAGE 38

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **a**.

Article Error You may need to use an article before this word.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

PAGE 39

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

PAGE 40

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 41

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

PAGE 42

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Article Error You may need to use an article before this word.

PAGE 43

Missing "," You may need to place a comma after this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Garbled Grammatical or spelling errors make the meaning of this sentence unclear. Proofread the sentence to correct the mistakes.

PAGE 44

PAGE 45

PAGE 46

Confused You have used **there** in this sentence. You may need to use **their** instead.

Missing "," You may need to place a comma after this word.

PAGE 47

Missing "," You may need to place a comma after this word.

Missing "," You may need to place a comma after this word.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word.

Wrong Form You may have used the wrong form of this word.

Missing "," You may need to place a comma after this word.

PAGE 48

Article Error You may need to use an article before this word.

PAGE 49

PAGE 50

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

PAGE 51

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Article Error You may need to use an article before this word.

PAGE 52

PAGE 53

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 54

PAGE 55