

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



Institute of
Computer
Technology

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
<u>CHAPTER 1: PROJECT BACKGROUND</u>	01-02
<u>CHAPTER 2: INTRODUCTION</u>	03-04
<u>CHAPTER 3: PROJECT SCOPE</u>	05-06
<u>CHAPTER 4: SYSTEM REQUIREMENTS</u>	07-08
<u>CHAPTER 5: PROCESS MODEL</u>	09-14
<u>5.1 PROCESS MODEL (BITDEFENDER)</u>	10
<u>5.2 PROCESS MODEL (COMODO)</u>	12
<u>5.3 PROCESS MODEL (WITHSECURE)</u>	14
<u>CHAPTER 6: PROJECT PLAN</u>	15-19
<u>CHAPTER 7: DATA GATHERING & FINDINGS</u>	20-26
<u>7.1 DATA GATHERING</u>	21
<u>7.2 FINDINGS</u>	23
<u>7.3 COMPARISION</u>	25
<u>CHAPTER 8: CHALANGES FACED</u>	27-28
<u>CHAPTER 9: IMPLEMENTATIONS</u>	29-51
<u>9.1 IMPLEMENTATIONS OF BITDEFENDER</u>	29
<u>9.2 IMPLEMENTATIONS OF COMODO</u>	36
<u>9.3 IMPLEMENTATIONS OF WITHSECURE</u>	45
<u>CHAPTER 10: CONCLUSION</u>	52-53
<u>CHAPTER 11: REFERNCES</u>	54-55

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

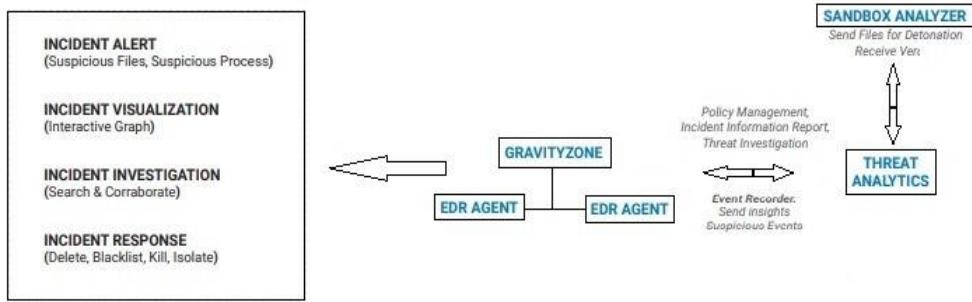
Minimum Software Requirements

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

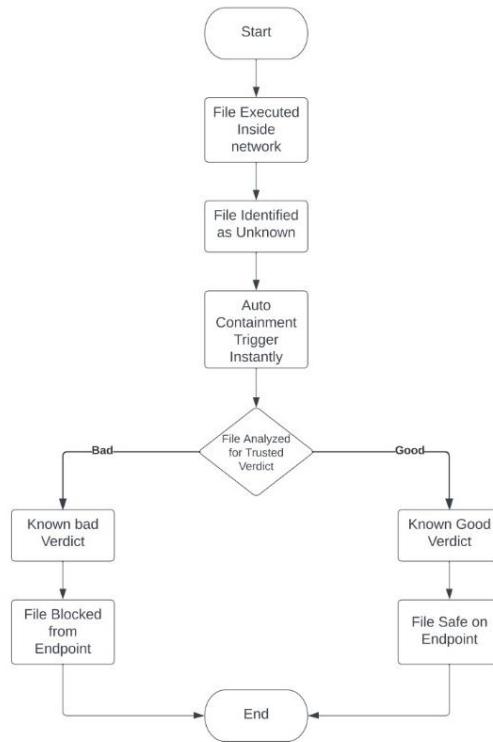
CHAPTER: 5(A)-PROCESS MODEL (BITDEFENDER)



- 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)

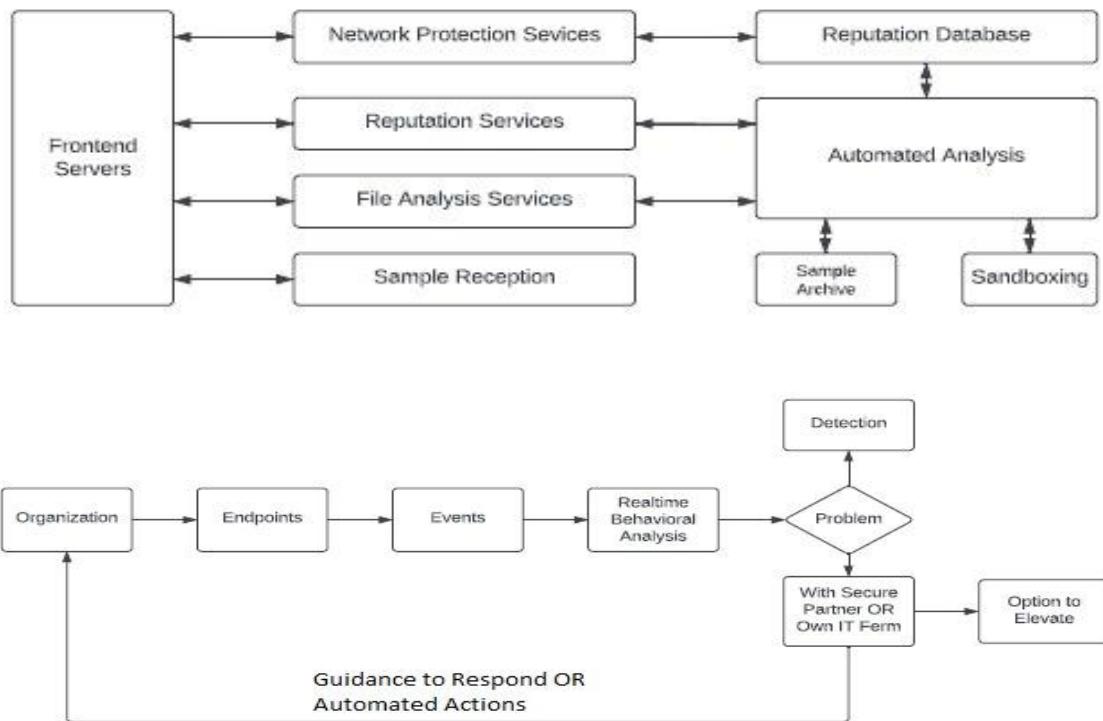
CHAPTER: 5(B)- PROCESS MODEL (COMODO)



- 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.

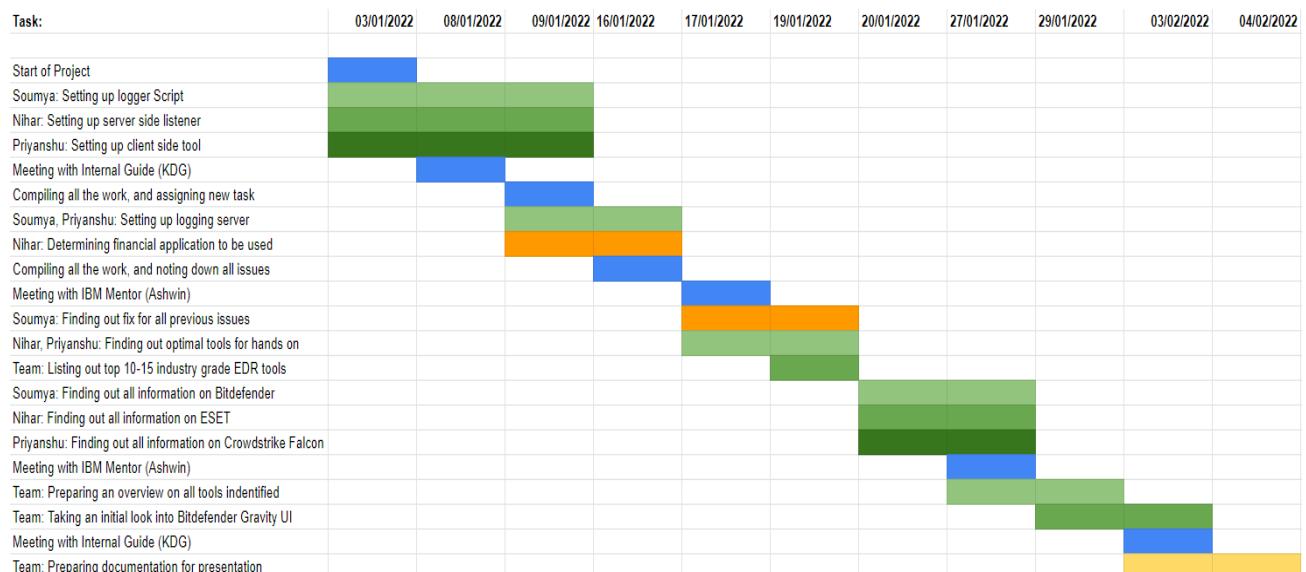
CHAPTER 6 - PROJECT PLAN (TIMELIN

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 switching 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 preparing 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:	07/02/2022	11/02/2022	12/02/2022	14/02/2022	18/02/2022	19/02/2022	21/02/2022	25/02/2022	26/02/2022
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)									
Compilation of data, and switching 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									
Compilation of data, and preparing 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)									
Compilation of findings, working on points given by mentor									
Task:	28/02/2022	03/03/2022	04/03/2022	05/03/2022	07/03/2022	11/03/2022			
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 (KG)									
Meeting with IBM Mentor (Ashwin Sir)									
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									

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 (KG)
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:

Task:	14/03/2022	16/03/2022	19/03/2022	21/03/2022	24/03/2022	26/03/2022	28/03/2022	31/03/2022	01/04/2022	04/04/2022	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 (KDQ)											
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.											

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 Carbon 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

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 their 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 where 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.

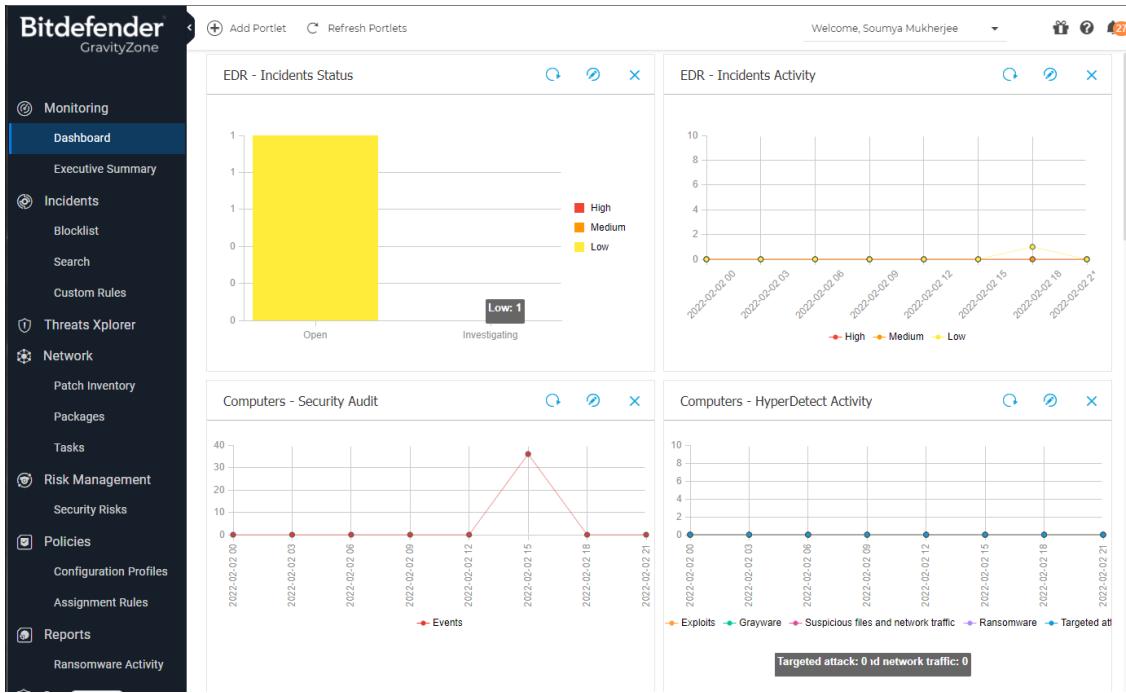
6. Finding technical answers

- 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.

Welcome, Soumya Mukherjee

Last 7 days ACTIONS

Reporting period 26 Jan 2022 00:00 - 2 Feb 2022 20:51

Threats Company risk score

Malware Outbreak

A malware outbreak has been detected in your network! At least 50%(1) from a total of 2 endpoints were found infected with "Application.Soht.Dropper.B" between 2022-02-02 18:13:42 and 2022-02-02 19:29:21.

Show more >

- 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.

Welcome, Soumya Mukherjee

Executive Summary Last 7 days ACTIONS

Reporting period 26 Jan 2022 00:00 - 2 Feb 2022 20:51

Managed endpoints	Active endpoints	Blocked threats	Company risk score
2	2	--	--

Inventory: Windows workstations 2 Windows servers 0 macOS 0 Linux 0 Physical endpoints 2 Virtual machines 0

Top 5 types of blocked threats

Incidents status: 1

Remediation actions

Threats breakdown by endpoint type

- 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.

Edit Endpoint Package

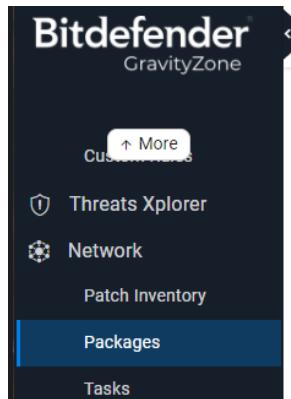
General

Name:	Test1
Description:	For testing purpose
Language:	English

Security Modules & Roles

Operation mode:	Detection and prevention
Modules:	<input checked="" type="checkbox"/> Antimalware <input checked="" type="checkbox"/> Advanced Threat Control <input checked="" type="checkbox"/> Advanced Anti-Exploit <input checked="" type="checkbox"/> Firewall <input checked="" type="checkbox"/> Network Protection <input checked="" type="checkbox"/> Content Control <input checked="" type="checkbox"/> Network Attack Defense <input checked="" type="checkbox"/> Device Control <input type="checkbox"/> Power User <input type="checkbox"/> Encryption <input type="checkbox"/> Patch Management

Buttons: Save | Cancel



Bitdefender GravityZone

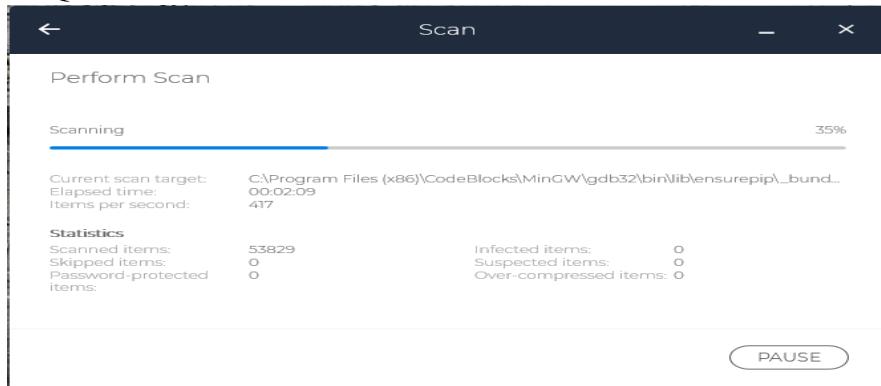
Custom contexts ↑ More

- Threats Xplorer
- Network
- Patch Inventory
- Packages**
- Tasks

Add Download Send download links Delete Refresh

Name	Type	Language	Description
Test1	BEST	English	For testing purpose
Security Server Virtual Appliance	Security Server	English	Security for Virtualized

- 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

Available scan logs	
Viewing scan logs for:	Endpoint Protection ▾
Type	Created
<input type="text"/>	<input type="text"/>
Custom Scan	02 February 2022, 19:00:39
Quick Scan	02 February 2022, 18:59:30
Full Scan	02 February 2022, 18:23:32

Web Panel Output

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

Computers and Virtual Machines							Welcome, Soumya Mukherjee
	Computer	IP	File	Threat Name	Quarantined on	Action status	Action
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Trojan.DOS.KillMBR.Z	02 February 2022, 19:22:15	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Backdoor.Delf.DY	02 February 2022, 19:21:28	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Backdoor.Delf.DY	02 February 2022, 19:21:28	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Trojan.Agent.BESF	02 February 2022, 19:21:25	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Trojan.Hacktool.Agent.BK	02 February 2022, 19:21:24	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Trojan.Agent.Small.SY	02 February 2022, 19:21:05	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	TrojanDownloader.Small.AAQO	02 February 2022, 19:21:05	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	AI:Tiny:46067.99E357581D	02 February 2022, 19:20:12	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Trojan.Agent.CYPC	02 February 2022, 19:19:12	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Win32.Worm.DoomJuice.B	02 February 2022, 19:19:11	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Trojan.Script.267131	02 February 2022, 19:19:08	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	VBS.BWG.A	02 February 2022, 19:19:07	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Virtool.Bz.Nihia	02 February 2022, 19:19:07	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Trojan.Script.131554	02 February 2022, 19:19:06	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	IRC-Worm.Mosuck.A	02 February 2022, 19:16:45	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	AI:Ransom:46067.2D90477E21	02 February 2022, 19:16:43	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Win32.Worm.Nimda.U	02 February 2022, 19:16:42	None	
<input type="checkbox"/>	DESKTOP-OPSPIMM	192.168.1.104	E:\None\Of_Your_Business\CEH	Trojan.Ruby.Pydoxon.A	02 February 2022, 19:16:41	None	

- We can view all the endpoint devices at network tab

Name	OS version	OS type	Last Seen	Endpoint type	Users
DESKTOP-OPSPIMM	Windows 10 Pro	Windows	Now	Workstation	N/A
NIHARPC	Windows 10 Pro	Windows	Now	Workstation	N/A

- We can view general information about the computer

General	Protection	Policy	Scan Logs	Troubleshooting	Users	
Computer	Protection Layers					
Name: NIHARPC	Endpoint:	Active				
FQDN: niharpc	Sandbox Analyzer:	Available				
IP: 192.168.1.106	Security Analytics:	Available				
OS: Windows 10 Pro						
Label: <input type="text"/>	Save					
Infrastructure: Computers and Groups						
Group: Computers and Groups						
State: Online						
Last seen: Now						

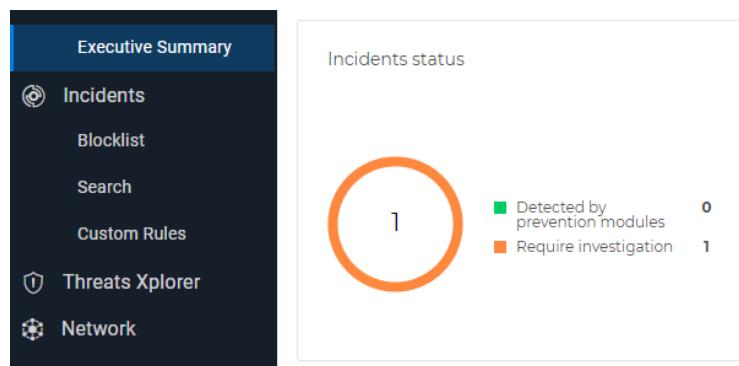
- Followed by information such as updates, version, timestamps, etc.

Endpoint Protection	
Agent	
Type:	BEST
Product version:	7.4.3.146
Last product update:	02 February 2022 18:22:22
Last check for a new product version:	02 February 2022 21:52:48
Product update location:	GravityZone Update Server - update.cloud.2d585.cdn.bitdefender.net
Engines version:	7.91082
Last security content update:	02 February 2022 21:53:21
Last check for new security content:	02 February 2022 21:53:05
Security content update location:	GravityZone Update Server - update.cloud.2d585.cdn.bitdefender.net
Primary scan engine:	Local Scan
Fallback scan engine:	None

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

The screenshot shows the Bitdefender GravityZone interface. On the left, a sidebar menu includes Monitoring, Incidents, Custom Rules (selected), Threats Xplorer, and Network. The main area is titled "Create Detection Rule". It shows a search bar for "Name" set to "Is" "login.php". Below it, a section titled "① Rule definition" says "Define rules to mark a specific behavior as a valid detection." A table lists a single rule: "loginFinder" created by soumyamukherjee18@gnu.ac.in on 02 February 2022, 18:57. The rule ID is 6fab7e2be2bb36b50290cb5 and it is active. To the right, a detailed view of the "loginFinder" rule is shown, including its creation details, results (View Incidents), and a "DO THE FOLLOWING" section where an alert is generated with High severity.

- 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.

Extended Incidents Endpoint Incidents Detected Threats

OPEN INCIDENTS		TOP ALERTS		TOP TECHNIQUES		TOP AFFECTED DEVICES	
High	0	DriversVolumesDiscov...	1	LogonRegModified	1	Unsecured Credentials	1
Medium	0	loginFinder	1	Boot or Logon Autostart...	1	Command and Scripting...	1
Low	1	Microsoft Internet Expl...					
Change Status		Alert name: <input type="text"/> Search		Search for filenames, IP addresses, hostnames... Search		Help	Print
ID	Date	Status	Severity Score	Endpoint	Alerts	Attack type	
<input type="checkbox"/> #1	Updated 6 minutes ago	Open	● 32	NIHARPC	7	Malware	More

➤ Malware details:

#1

Created On: 02 Feb 2022, 19:00:29
 Last Updated on: 02 Feb 2022, 19:00:43
 Endpoint: NIHARPC
 Artifacts Involved: 48

DETECTION

Severity Score: ● 32 Incident Trigger: login.php

[! loginFinder >](#)

ATTACK INFO

Attack Types: [Malware](#)

Tactics: Persistence
 Privilege Escalation
 Execution
 Credential Access

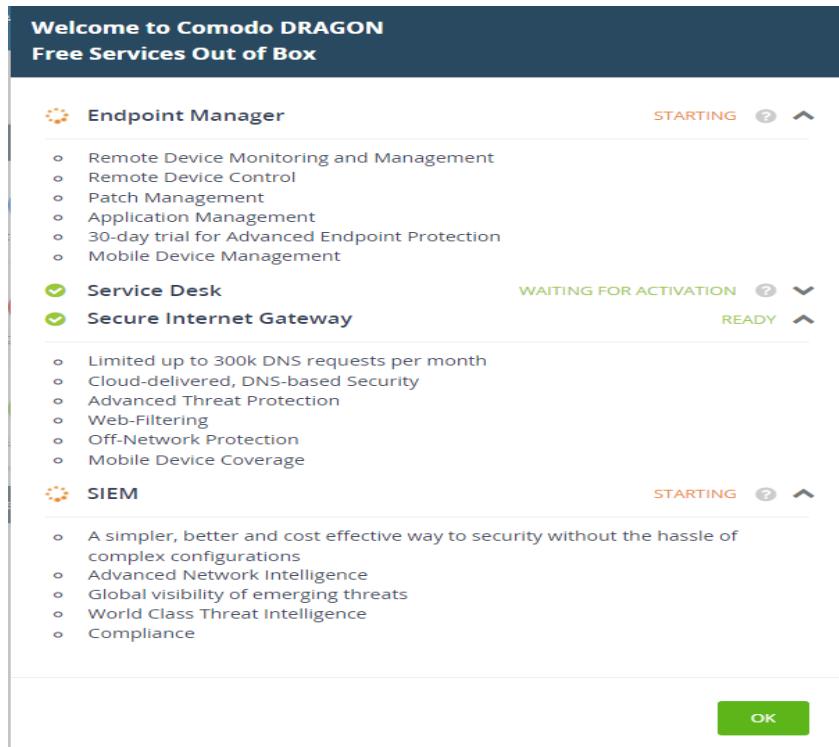
ATT&CK Techniques

Boot or Logon A...	T1547.004 Winlogon Helper DLL
Command and S...	T1059
Credentials from ...	T1555.003 Credentials from Web...
Unsecured Crede...	T1552.001 Credentials In Files

CHAPTER 9 (B) – IMPLEMENTATION (COMODO)

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.

The screenshot shows the "Device List" section of the Comodo interface. The top navigation bar includes "Device List", "Supported Device Platforms", "License Options", and a user dropdown. The main area has tabs for "Group Management" and "Device Management", with "Device Management" selected. Below is a toolbar with icons for Enroll Device, Remote Control, File Transfer, Remote Tools, Run Procedure, Manage Profiles, Install or Manage Packages, Refresh Device Information, Power Options, Owner, and More. A search bar says "Search for devices". The main table displays device information:

OS	NAME	ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LOGGED IN USER	LAST ACTIVITY
Windows	NiharPC	AG AV FW CO	1	1	Default Cust...	NIHARPC	2022/02/23 11:06:06 PM

At the bottom, there are buttons for "Results per page:" (set to 20) and "Displaying 1 of 1 results".

- Details covered under device profiling:

Device Name:

Summarized Info:

Device Name	Summary	Networks	Associated Profiles	Software Inventory	File List	Exported Configurations	MSI Installation State	Patch ▶																																																		
Device Summary <table border="1"> <tr><td>Custom device name</td><td>NiharPC</td></tr> <tr><td>Name</td><td>NiharPC</td></tr> <tr><td>Logged in user</td><td>NIHARPC\Admin</td></tr> <tr><td>AD\LDAP</td><td>N/A</td></tr> <tr><td>Domain\Workgroup</td><td>WORKGROUP</td></tr> <tr><td>Formfactor</td><td>PC</td></tr> <tr><td>Model</td><td>H310M H</td></tr> <tr><td>Communication Client version</td><td>6.43.41148.21120</td></tr> <tr><td>Processor</td><td>Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz</td></tr> <tr><td>Serial number</td><td>Default string</td></tr> <tr><td>System model</td><td>H310M H</td></tr> <tr><td>System manufacturer</td><td>Gigabyte Technology Co., Ltd.</td></tr> <tr><td>Ownership type</td><td>Not specified</td></tr> <tr><td>Last connection</td><td>2022/02/23 11:25:56 PM</td></tr> <tr><td>Registered</td><td>2022/02/23 09:58:10 PM</td></tr> <tr><td>Device time zone</td><td>UTC +05:30 (DST disabled)</td></tr> <tr><td>External IP</td><td>43.241.193.215</td></tr> </table>			Custom device name	NiharPC	Name	NiharPC	Logged in user	NIHARPC\Admin	AD\LDAP	N/A	Domain\Workgroup	WORKGROUP	Formfactor	PC	Model	H310M H	Communication Client version	6.43.41148.21120	Processor	Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz	Serial number	Default string	System model	H310M H	System manufacturer	Gigabyte Technology Co., Ltd.	Ownership type	Not specified	Last connection	2022/02/23 11:25:56 PM	Registered	2022/02/23 09:58:10 PM	Device time zone	UTC +05:30 (DST disabled)	External IP	43.241.193.215	OS Summary <table border="1"> <tr><td>OS</td><td>Windows</td></tr> <tr><td>OS name</td><td>Microsoft Windows 10 Pro (x64)</td></tr> <tr><td>OS version</td><td>10.0.19044</td></tr> <tr><td>OS full version</td><td>Version 21H2 (OS Build 19044.1526)</td></tr> <tr><td>Service pack</td><td>N/A</td></tr> <tr><td>Build version</td><td>19044</td></tr> <tr><td>Reboot time</td><td>2022/02/23 09:57:51 PM</td></tr> <tr><td>Reboot reason</td><td>The process C:\Users\Admin\AppData\Local\Temp_32e232e1b39c5597ecb5bb06a83a08eed2d81cd9\offlineinstaller.exe (NIHARPC) has initiated the restart of computer NIHARPC on behalf of user NIHARPC\Admin for the following reason: Application: Maintenance (Planned) Reason Code: 0x80040001 Shutdown Type: restart Comment: Your device will reboot in 5 minutes because it's required by your administrator</td></tr> </table>						OS	Windows	OS name	Microsoft Windows 10 Pro (x64)	OS version	10.0.19044	OS full version	Version 21H2 (OS Build 19044.1526)	Service pack	N/A	Build version	19044	Reboot time	2022/02/23 09:57:51 PM	Reboot reason	The process C:\Users\Admin\AppData\Local\Temp_32e232e1b39c5597ecb5bb06a83a08eed2d81cd9\offlineinstaller.exe (NIHARPC) has initiated the restart of computer NIHARPC on behalf of user NIHARPC\Admin for the following reason: Application: Maintenance (Planned) Reason Code: 0x80040001 Shutdown Type: restart Comment: Your device will reboot in 5 minutes because it's required by your administrator
Custom device name	NiharPC																																																									
Name	NiharPC																																																									
Logged in user	NIHARPC\Admin																																																									
AD\LDAP	N/A																																																									
Domain\Workgroup	WORKGROUP																																																									
Formfactor	PC																																																									
Model	H310M H																																																									
Communication Client version	6.43.41148.21120																																																									
Processor	Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz																																																									
Serial number	Default string																																																									
System model	H310M H																																																									
System manufacturer	Gigabyte Technology Co., Ltd.																																																									
Ownership type	Not specified																																																									
Last connection	2022/02/23 11:25:56 PM																																																									
Registered	2022/02/23 09:58:10 PM																																																									
Device time zone	UTC +05:30 (DST disabled)																																																									
External IP	43.241.193.215																																																									
OS	Windows																																																									
OS name	Microsoft Windows 10 Pro (x64)																																																									
OS version	10.0.19044																																																									
OS full version	Version 21H2 (OS Build 19044.1526)																																																									
Service pack	N/A																																																									
Build version	19044																																																									
Reboot time	2022/02/23 09:57:51 PM																																																									
Reboot reason	The process C:\Users\Admin\AppData\Local\Temp_32e232e1b39c5597ecb5bb06a83a08eed2d81cd9\offlineinstaller.exe (NIHARPC) has initiated the restart of computer NIHARPC on behalf of user NIHARPC\Admin for the following reason: Application: Maintenance (Planned) Reason Code: 0x80040001 Shutdown Type: restart Comment: Your device will reboot in 5 minutes because it's required by your administrator																																																									

Security Patch Details and information regarding Performance metrics:

Security Products Info		Performance Metrics (Last updated: 2022/02/23 11:26:24 PM)		
Name	COMODO Client - Security	CPU usage	5% (2808 MHz)	
Version	12.10.0.8697	RAM usage	51.20% (4160 MB of 8125 MB)	
Components	Antivirus Containment Baselining Firewall Training mode HIPS Training mode Virtual Desktop	Network usage	Realtek Gaming GbE Family Controller Load 0% speed channel (sent 14 Kbit/s, received 1 Kbit/s) TAP-ProtonVPN Windows Adapter V9 Load 0% speed channel (sent 0 bit/s, received 0 bit/s)	
Virus DB version	34380	Disk usage	C: Free 32 GB Used 114 GB D: Free 106 GB Used 286 GB E: Free 159 GB Used 233 GB F: Free 0 MB Used 0 MB	
Virus DB last update time	2022/02/23 10:56:34 PM			

Quick view on all software installed in client:

Device Name	Summary	Networks	Associated Profiles	Software Inventory	File List	Exported Configurations	MSI Installation State	Patch
Last inventory scan date: 2022/02/23 10:28:55 PM Status: Success								
	Update Software Inventory							
□ SOFTWARE	VENDOR	VERSION	INSTALLATION DATE					
□ COMODO Client - Security	COMODO Security Solutions Inc.	12.10.0.8697	2022/02/23					
□ Endpoint Manager Communication Client	ITarian LLC	6.43.41148.21120	2022/02/23					
□ VALORANT	Riot Games, Inc	N/A	2022/02/22					
□ Microsoft Edge	Microsoft Corporation	98.0.1108.56	2022/02/19					
□ Mozilla Firefox (x64 en-US)	Mozilla	97.0.1	2022/02/18					
□ Microsoft Update Health Tools	Microsoft Corporation	3.65.0.0	2022/02/18					
□ Brave	Brave Software Inc	98.1.35.103	2022/02/17					
□ Microsoft OneDrive	Microsoft Corporation	22.012.0117.0003	2022/02/17					
□ Google Chrome	Google LLC	98.0.4758.102	2022/02/17					

Security Patch running in endpoint:

Associated Profiles	Software Inventory	File List	Exported Configurations	MSI Installation State	Patch Management	Antivirus	Groups	Logs
Operating System Third Party Applications								
Last OS Patches Scan date: 2022/02/23 10:15:43 PM Status: Success								
□ TITLE	KB	CVE	BULLETIN	CLASSIFICATION	SEVERITY	REBOOT	RELEASE DATE	STATUS
□ 2022-01 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H2 for x64 (KB5008876)	5008876			Security Update	Important	Maybe	2022/01/12	Installed
□ 2022-01 Update for Windows 10 Version 21H2 for x64-based Systems (KB4023057)	4023057			Critical Update	Unspecified	Maybe	2022/02/03	Installed
□ 2022-02 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5010342)	5010342			Security Update	Unspecified	Maybe	2022/02/08	Installed
□ 2022-02 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H2 for x64 (KB5010472)	5010472			Update	Unspecified	Maybe	2022/02/15	Available
□ Windows Malicious Software Removal Tool x64 - v5.98 (KB890830)	890830			Update Rollup	Unspecified	Maybe	2022/02/14	Installed

Results per page: 20

Displaying 1-5 of 5 results

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

Networks	Associated Profiles	Software Inventory	File List	Exported Configurations	MSI Installation State	Patch Management	Antivirus	Groups	Logs
Quarantined Files									
Last Update Time: 2022/02/23 10:20:42 PM									
□ FILE NAME	FILE PATH	FILE HASH	DATE QUARANTINED	COMODO RATING	ADMIN RATING	USER'S LAST ACTION	USER'S LAST ACTION STATUS		
□ Uni.zip	D:\Virus...	211A07...	2022/02/23 10:17:44 ...	Unrecognized	Unrecognized	None	Unknown		
□ quiz - 2.zip	D:\Virus...	910A72...	2022/02/23 10:17:44 ...	Unrecognized	Unrecognized	None	Unknown		
□ Virus-main.zip	D:\Virus...	C1B34F...	2022/02/23 10:17:44 ...	Unrecognized	Unrecognized	None	Unknown		
□ Malicious.js	D:\Virus...	388C8B...	2022/02/23 10:17:44 ...	Unrecognized	Unrecognized	None	Unknown		
□ payment.doc	D:\Virus...	0E3EC0...	2022/02/23 10:17:44 ...	Unrecognized	Unrecognized	None	Unknown		
□ example2.pdf	D:\Virus...	E64F3E...	2022/02/23 10:17:43 ...	Unrecognized	Unrecognized	None	Unknown		
□ LOKI.docx	D:\Virus...	F26333...	2022/02/23 10:17:43 ...	Unrecognized	Unrecognized	None	Unknown		
□ Batch 76.zip	D:\Virus...	2EECCE...	2022/02/23 10:17:43 ...	Unrecognized	Unrecognized	None	Unknown		
□ exam.doc	D:\Virus...	B32BSF...	2022/02/23 10:17:43 ...	Unrecognized	Unrecognized	None	Unknown		

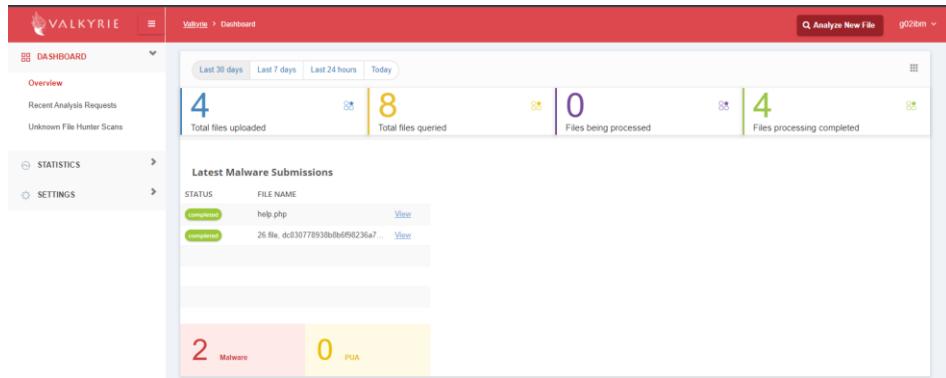
- We have a user list section which shows all the accounts in portal

- 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

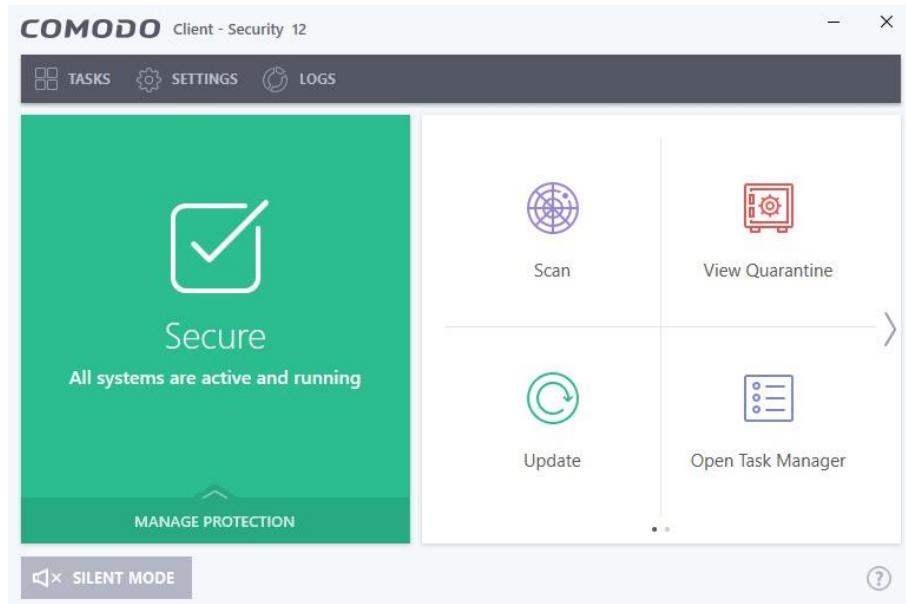
➤ Overview dashboard:



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

Your Recent Analysis Requests					
5 TOTAL NUMBER OF FILES	3 TOTAL NUMBER OF CLEAN FILES	0 TOTAL NUMBER OF UNKNOWN FILES	2 TOTAL NUMBER OF MALWARE FILES	0 TOTAL NUMBER OF PUA	0 TOTAL NUMBER IN HUMAN EXPERT ANALYSIS
Search : <input type="text"/>					
From 2022-02-09	To 2022-03-12	<input type="button" value="Apply"/>	My All Products	<input type="button" value="FILTER"/>	Results per page 25
<input type="button" value="View File Info"/>	<input type="button" value="Export Results To PDF"/>	<input type="button" value="View Virus Total Result"/>	<input type="button" value="Kill Chain Report"/>	<input type="button" value="Send To Human Expert Analyst"/>	<input type="button" value="Reanalyze"/>
File Name	Path	SHA1	Submit Date	Last Activity	Final Verdict
statements.docx	statements.docx	9d8b7d96c65554a43cd...	2022-03-06 17:02:29	2022-03-06 17:02:26	Clean
test2.vbs	test2.vbs	ebd5b3a685f593965eb...	2022-03-06 17:01:38	2022-03-06 17:01:34	Clean
help.php	help.php	c6e525c8167a49437d1...	2022-03-06 17:01:17	2022-03-06 17:01:14	Malware
26 file_dc030778938b8b6f98236a...	D:\Virus\Virus-main\dc...	32f5611459b9b631458...	2017-02-22 22:12:55	2022-03-06 17:00:23	Malware
pip.exe	C:\Users\Admin\AppData\Local\Temp\pip_..._00000000000000000000000000000000	c4cc043c7190063768c...	2022-03-05 12:49:19	2022-03-05 12:48:41	Clean

➤ 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

Realtime Scan

- Enable Realtime Scan (Recommended)**
This option enables virus scanning when your computer is used and prevents threats before they enter your system.
- Enable scanning optimizations (Recommended)**
Use this option to activate the performance improving technologies for realtime scanning.
- Do not show auto-scan alerts**
- Scan computer memory after the computer starts**
- Do not show antivirus alerts**
- Decompress and scan archive files of extension(s): *.exe, *.jar**
- Set new on-screen alert timeout to** secs
- Set new maximum file size limit to** MB
- Set new maximum script size limit to** MB
- Use heuristic scanning**
- Use heuristics scanning**
- Enable realtime scanning of files on network**
- Use Windows Antimalware Scan Interface (AMSI) technology**
- Use cloud services while scanning via AMSI (Cloud Lookup should be enabled in File Rating section)**

Firewall Settings

- Enable Firewall (Recommended)**
- This option enables firewall which filters inbound and outbound traffic.
- Alert Settings**
 - Do not show popup alerts**
 - Turn traffic animation effects on**
 - Create rules for safe applications**
 - Set alert frequency level**
 - Set new on-screen alert timeout to** secs
- Advanced**
 - Filter IPv6 traffic**
 - Filter loopback traffic (e.g. 127.x.x.x, ::1)**
 - Block fragmented IP traffic**
 - Do protocol analysis**
 - Enable anti-ARP spoofing**
 - Detect disabled firewall driver in network adapter settings and**

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

Auto-Containment

This option enables automatic containment of executable files and scripts according to the policy defined below.

Action	Target	Rating	Enable Rule
Block	All Applications	Malicious	<input checked="" type="checkbox"/>
Block	Suspicious Locations	Any	<input checked="" type="checkbox"/>
Block	Containment Folders	Any	<input checked="" type="checkbox"/>
Ignore	Communication Client	Trusted	<input checked="" type="checkbox"/>
Ignore	Metro Apps	Any	<input checked="" type="checkbox"/>
Ignore	Global Whitelist	Unrecognized	<input checked="" type="checkbox"/>
Ignore	All Applications	Unrecognized	<input checked="" type="checkbox"/>
Ignore	PDF	Unrecognized	<input type="checkbox"/>
Run Virtually	All Applications	Unrecognized	<input checked="" type="checkbox"/>
Block	Pseudo File Downloaders	Any	<input checked="" type="checkbox"/>
Block	SQL Clients	Any	<input checked="" type="checkbox"/>

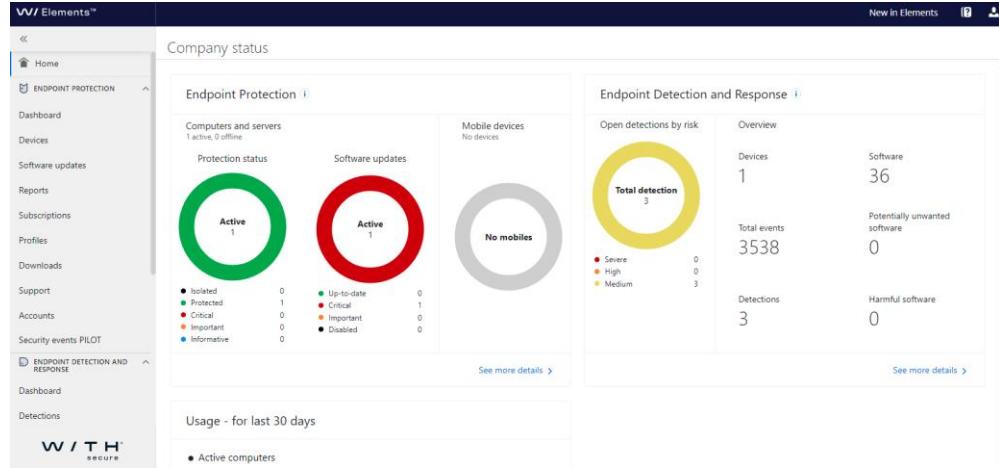
- Manual rulesets and predefined rulesets are all mentioned under HIPS ruleset section so that client doesn't interrupt with normal OS operations.



CHAPTER 9 (C) – IMPLEMENTATION (WITHSECURE)

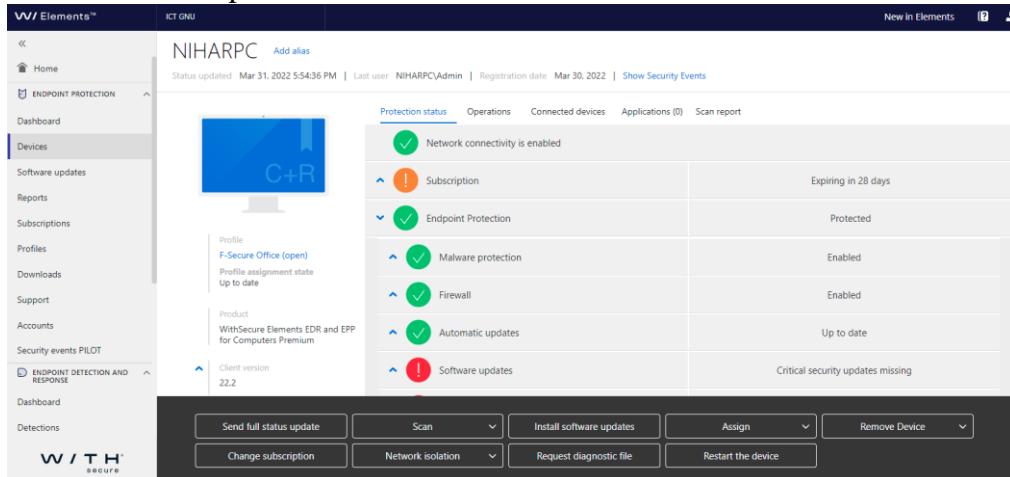
CHAPTER-9 (C) IMPLEMENTATION (WITHSECURE)

- Initialising the web portal, opening “Dashboard”

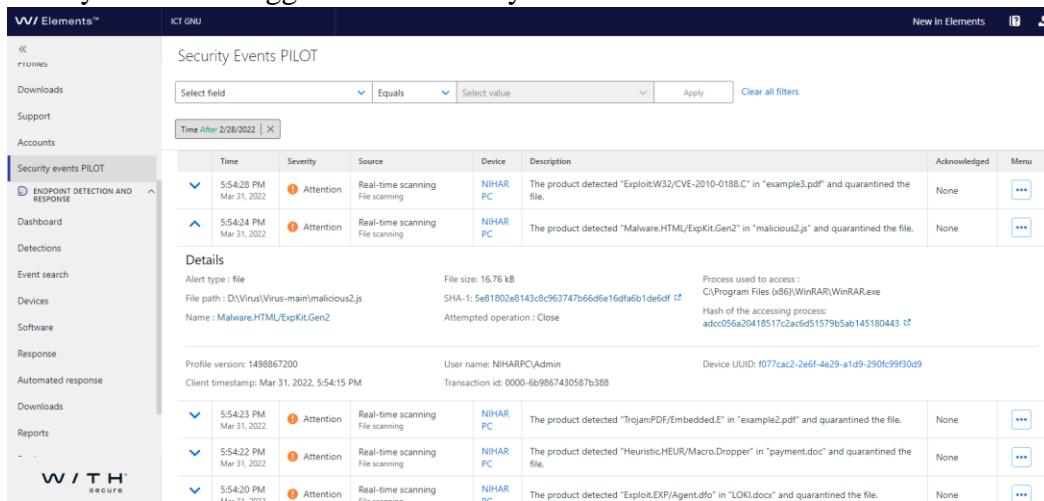


We can view all the endpoints, their security state, software updates, any critical notifications all at one place.

- 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.

Time	Severity	Source	Device	Description	Acknowledged	Menu
5:54:28 PM Mar 31, 2022	Attention	Real-time scanning File scanning	NIHAR PC	The product detected "Exploit:W32/CVE-2010-0188.C" in "example3.pdf" and quarantined the file.	None	
5:54:24 PM Mar 31, 2022	Attention	Real-time scanning File scanning	NIHAR PC	The product detected "Malware.HTML/ExpKit.Gen2" in "malicious2.js" and quarantined the file.	None	
5:54:23 PM Mar 31, 2022	Attention	Real-time scanning File scanning	NIHAR PC	The product detected "Trojan:PDF/Embedded.E" in "example2.pdf" and quarantined the file.	None	
5:54:22 PM Mar 31, 2022	Attention	Real-time scanning File scanning	NIHAR PC	The product detected "Heuristic:HEUR/Macro.Dropper" in "payment.doc" and quarantined the file.	None	
5:54:20 PM Mar 31, 2022	Attention	Real-time scanning File scanning	NIHAR PC	The product detected "Exploit.EXE/Agent.dfo" in "LOKI.docx" and quarantined the file.	None	

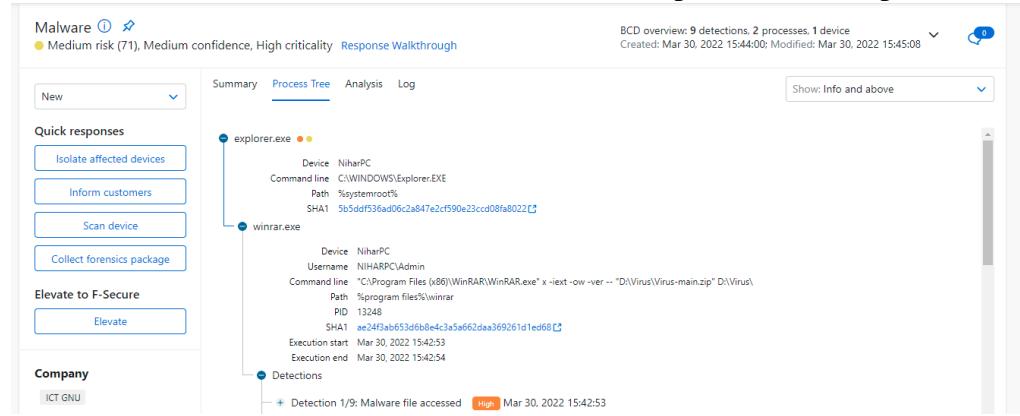
- Detection and Response has a different dashboard to offer, which basically shows total endpoints and total malicious files detected along with the total number of events triggered.

- Detections:

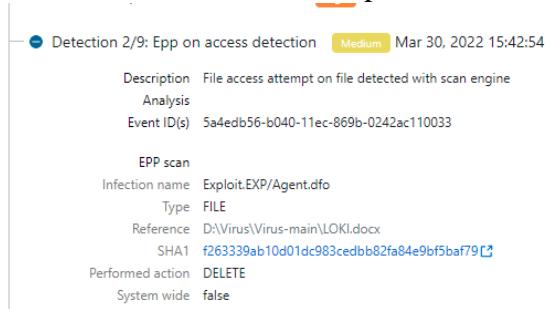
ID	Risk	Type	Devices	Detected	Modified	Status	Properties	Comments
123992844-5	Medium	Malware	1	31.03.2022 12:24:37	31.03.2022 12:25:30	New	0	
123992844-2	Medium	Malware	1	30.03.2022 15:50:17		New	0	
123992844-1	Medium	Malware	1	30.03.2022 15:44:00	30.03.2022 15:45:08	New	0	

- 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:

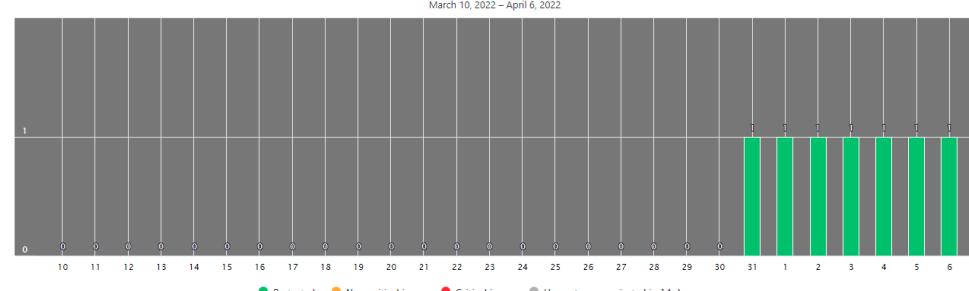
Reports ...

[Protection status](#) [Security events](#) [Infections](#) [Software Updates](#) [Audit Log](#) [Devices](#)

Computer protection status

Last 28 days

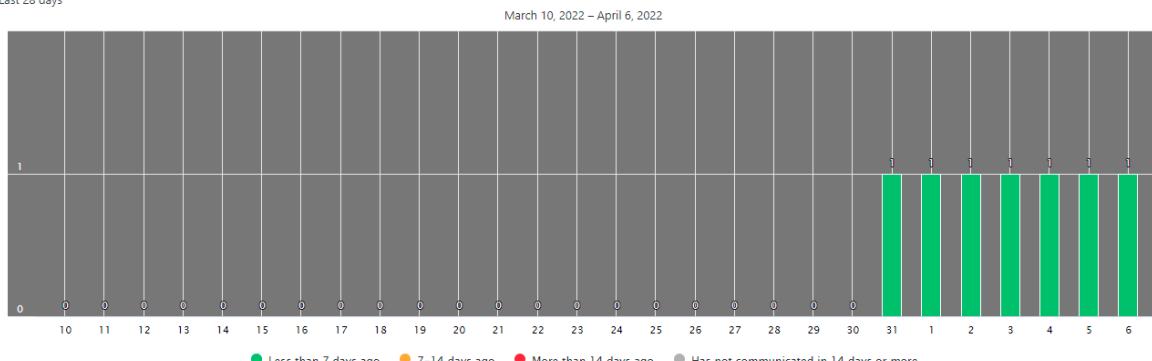
March 10, 2022 – April 6, 2022



Latest malware definition updates on computers

Last 28 days

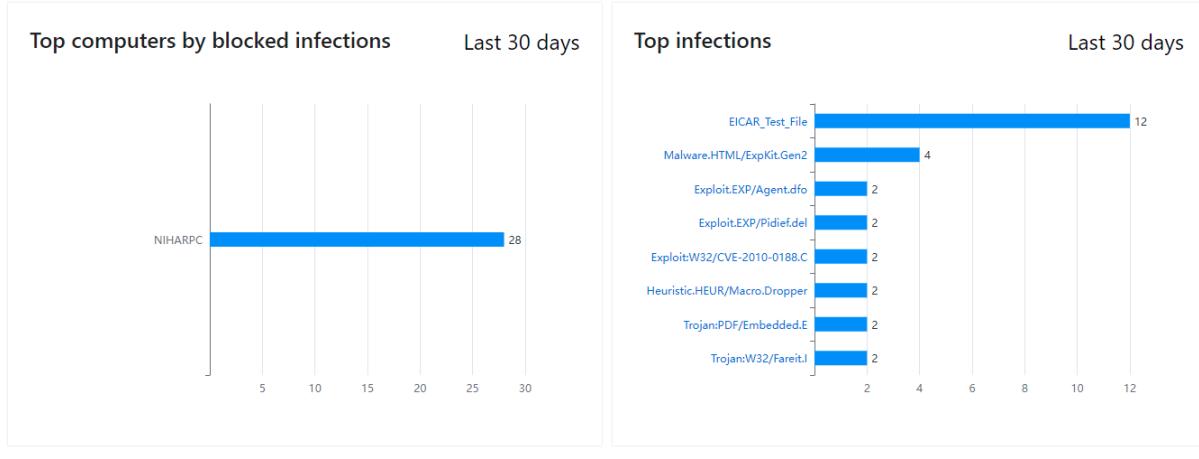
March 10, 2022 – April 6, 2022



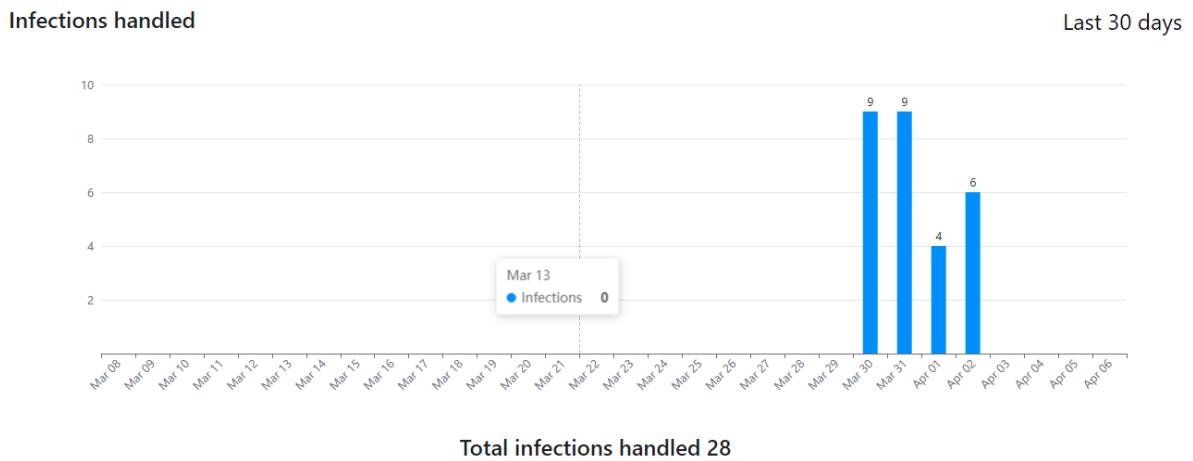
- Quick glace view of which endpoint is getting compromised quicker along with which malware view:

Reports ...

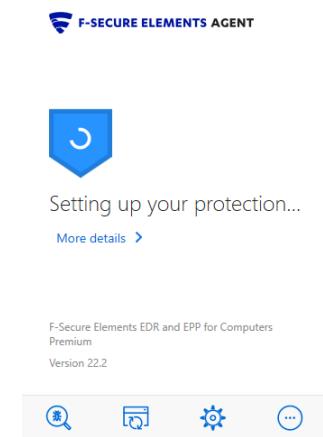
Protection status Security events Infections Software updates Audit Log Devices



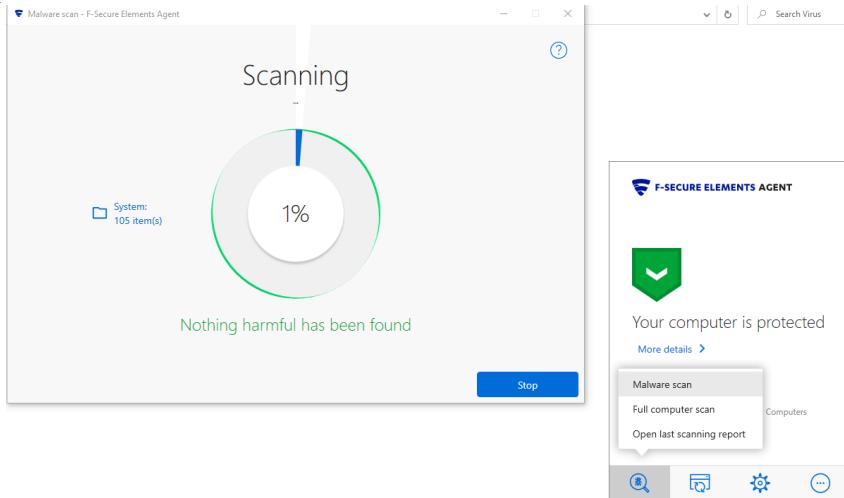
- Graphical representation of data:



- Client-Side Initialisation:



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



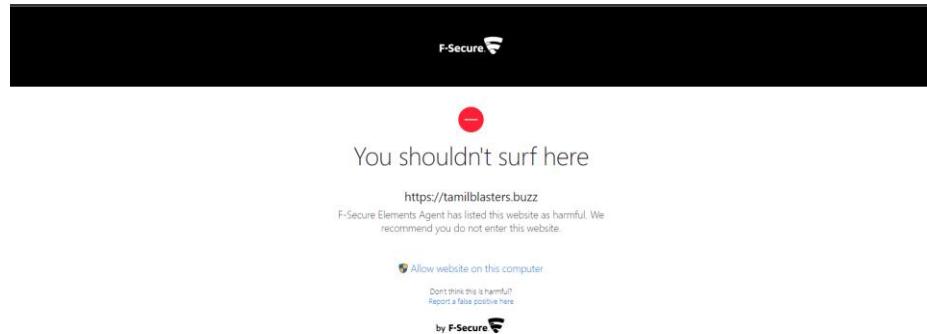
- Once a scan completes it sends a detailed report to client as well as shows it in portal.

Time	Title	User	Action
31-03-2022 05.54 PM	Harmful file quarantined	Admin	View description online
31-03-2022 05.54 PM	Harmful file quarantined	Admin	View description online
31-03-2022 05.54 PM	Harmful file quarantined	Admin	View description online
31-03-2022 05.54 PM	Harmful file quarantined	Admin	View description online
31-03-2022 05.54 PM	Harmful file quarantined	Admin	View description online
31-03-2022 05.54 PM	Harmful file quarantined	Admin	View description online
31-03-2022 05.54 PM	Harmful file quarantined	Admin	View description online
31-03-2022 05.54 PM	Harmful file quarantined	Admin	View description online
31-03-2022 05.54 PM	Harmful file quarantined	Admin	View description online
31-03-2022 05.46 PM	Manual malware scan did not remove all harmful items	Admin	View report
31-03-2022 12.49 AM	Harmful website https://tamilblasters.buzz blocked	Admin	
31-03-2022 12.49 AM	Harmful website https://tamilblasters.buzz blocked	Admin	
30-03-2022 10.12 PM	New software updates have been installed	Admin	
30-03-2022 10.10 PM	F-Secure Software Updater is installing updates now	Admin	
30-03-2022 09.34 PM	Manual malware scan did not find any harmful items	Admin	View report
30-03-2022 09.19 PM	Harmful file quarantined	Admin	View description online
30-03-2022 09.12 PM	Harmful file quarantined	Admin	View description online
30-03-2022 09.12 PM	Harmful file quarantined	Admin	View description online
30-03-2022 09.12 PM	Harmful file quarantined	Admin	View description online
30-03-2022 09.12 PM	Harmful file quarantined	Admin	View description online

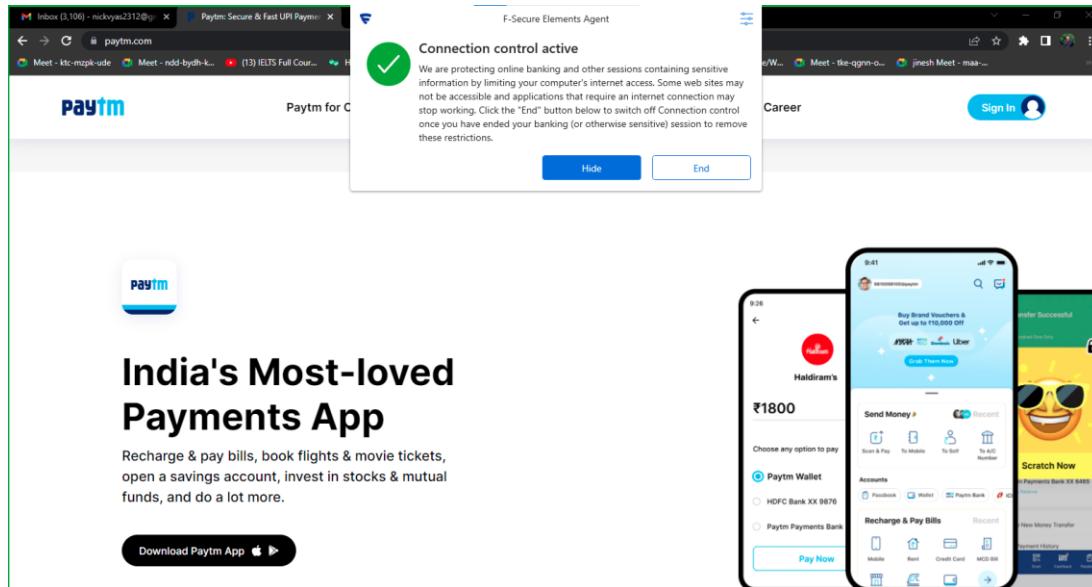
- On clicking you can view detailed report on the malware:

CLASSIFICATION			
Category:	Malware	Type:	Trojan-PWS
Aliases:	Trojan.PWS.Fareit [variant], Trojan.Fareit,[variant]		
SUMMARY			
Fareit malware steals login credentials and forwards the information to a remote server. It may also download additional malware onto the affected system.			
REMOVAL			
Automatic action		Suspect a file is incorrectly detected (a False Positive?)	
Automatic action Based on the settings of your F-Secure security product, it will either move the file to the quarantine where it cannot spread or cause harm, or remove it.			
FOR MORE SUPPORT			
Community	User Guide	Contact Support	Submit a sample
Find the latest advice in our Community .	See the user guide for your product on the Help Center .	Chat with or call an expert for help.	Submit a file or URL for further analysis.

- Client tool also provides malicious link blocker for secure web 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

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

3

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.

Missing ":" 

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.

Wrong Article 

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.

Article Error 

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.

2

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

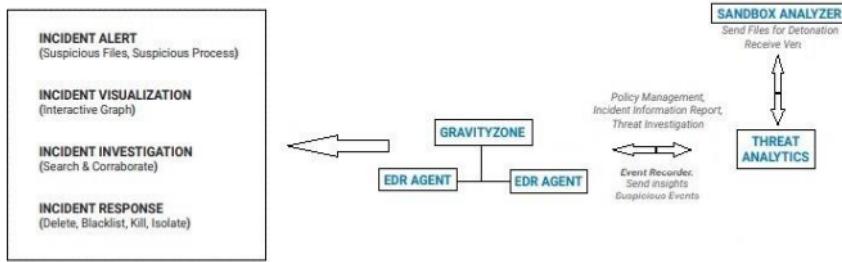
Minimum Software Requirements

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

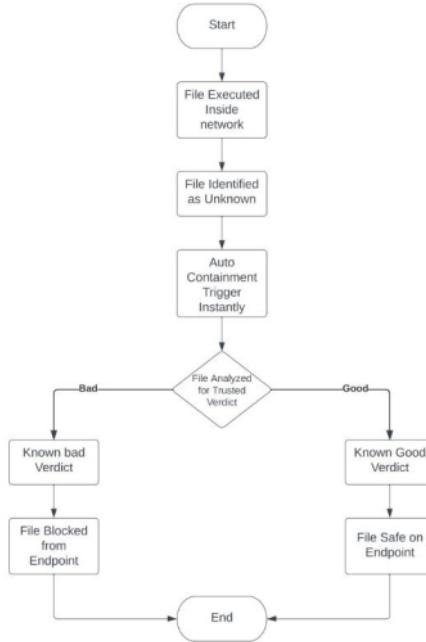
CHAPTER: 5(A)-PROCESS MODEL (BITDEFENDER)



- Once endpoint is connected with panel, any sort of unusual activity detected will create an incident alert. Article Error (ETS)
- 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. Article Error (ETS)

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

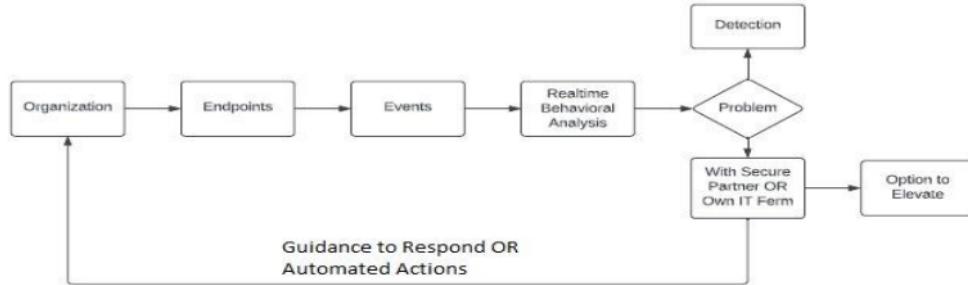
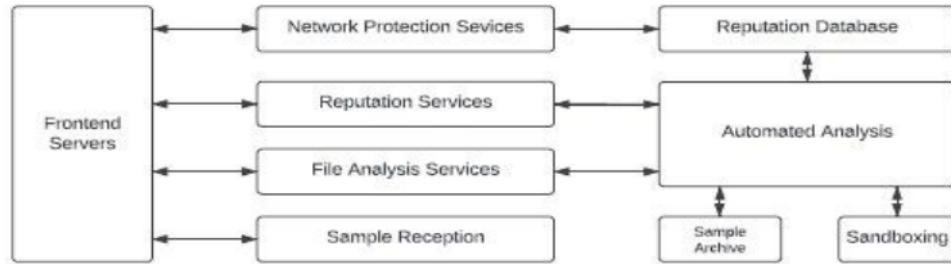
CHAPTER: 5(B)- PROCESS MODEL (COMODO)



- 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.

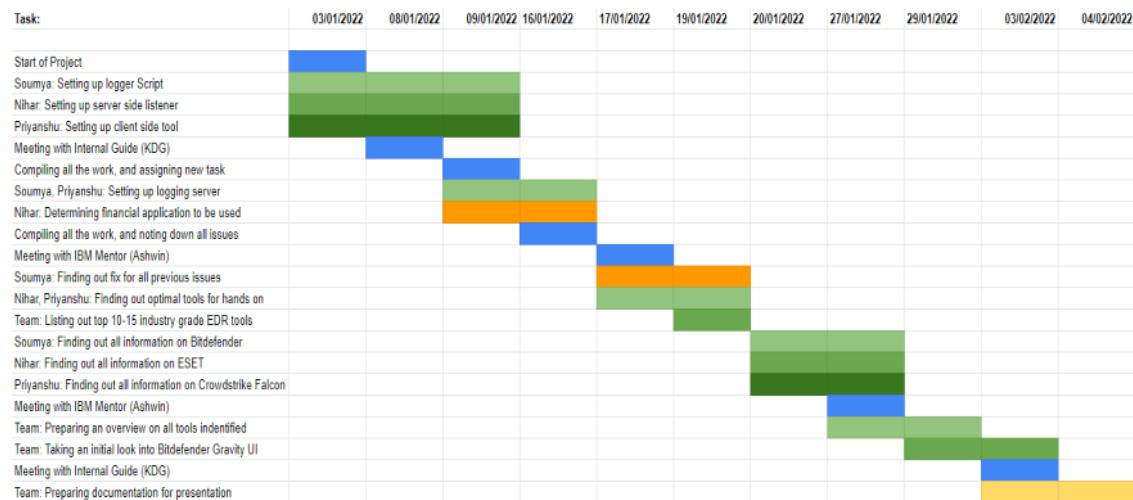
CHAPTER 6 - PROJECT PLAN (TIMELIN

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 identified
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 switching 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 preparing 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 (KG)	
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:	07/02/2022	11/02/2022	12/02/2022	14/02/2022	18/02/2022	19/02/2022	21/02/2022	25/02/2022	26/02/2022
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)									
Compilation of data, and switching 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									
Compilation of data, and preparing 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)									
Compilation of findings, working on points given by mentor									
Task:	28/02/2022	03/03/2022	04/03/2022	05/03/2022	07/03/2022	11/03/2022			
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 (KG)									
Meeting with IBM Mentor (Ashwin Sir)									
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									

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 Article Error (ETS)
Nihar: Setting up client and running required scans Article Error (ETS)
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 Proofread (ETS)
Nihar: Performing all client-side actions possible.
Meeting with Internal Guide (KG)
Team: Performing test of live virus download and monitoring activities Article Error (ETS)
Team: Compiling all the data and findings, merging all the research
Meeting with IBM Mentor (Ashwin Sir)
Team: Working on documentation and report.

Timeline:

Task:	14/03/2022	16/03/2022	19/03/2022	21/03/2022	24/03/2022	26/03/2022	28/03/2022	31/03/2022	01/04/2022	04/04/2022	08/04/2022
Team: Working on all unanswered questions from last review, research											
Meeting with IBM Mentor (Ashwin Sir)											
Team: Setting up Sotios, 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.											

Basic monthly strategy team was following:

Week 1 - setting up client with dashboard

Article Error 

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.

Article Error 

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

4

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.

Article Error (ETS)

➤ Features List:

Features	VMware Carbon 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

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.

Article Error (ETS)

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.

Article Error (ETS)

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.

Sp. (ETS)

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, lightweight 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.

Article Error (ETS)

CHAPTER 7 (C) – COMPARISION

CHAPTER 7 (C) – COMPARISON

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

Sp. (ETS)

Run-on (ETS)

➤ 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 its 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.

Article Error (ETS)

Article Error (ETS)

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 its own client collected data of file activity as detection layer.

Confused (ETS)

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

Run-on (ETS)

➤ 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.

Run-on 

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.

Confused

➤ **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.

Article Error 

Sp. 

Missing "," 

S/V 

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

S/V 

Article Error 

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

S/V 

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.

Article Error 

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.

Sp. 

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. Confused 

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 until we reach No. 4 tool Bitdefender which offered the trial and our project started.

Run-on 

Proofread 

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.

Prep. 

Article Error 

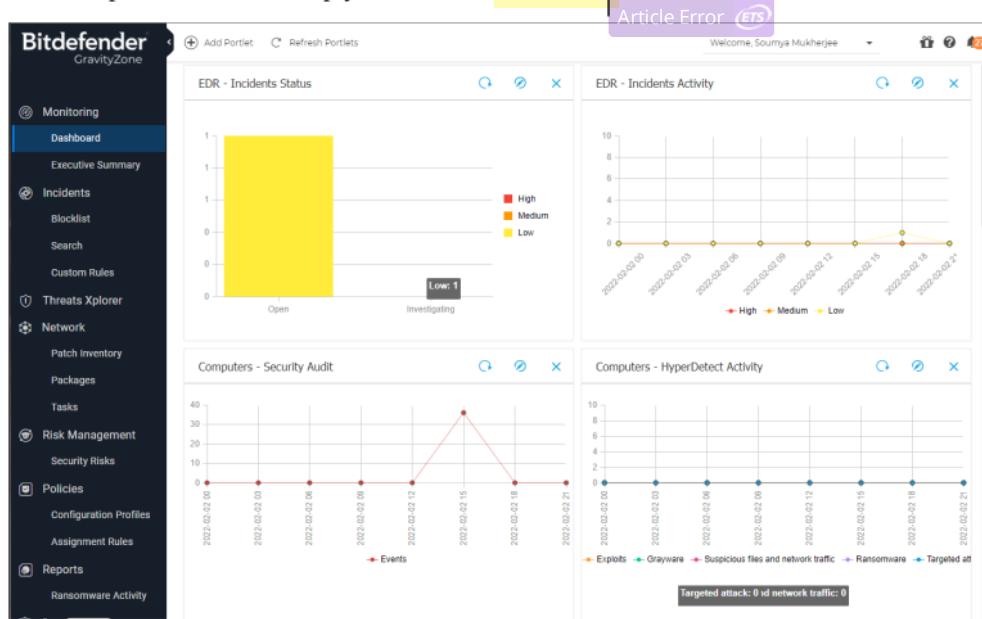
6. Finding technical answers

- 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.

Welcome, Soumya Mukherjee

Last 7 days ACTIONS ▾

Reporting period 26 Jan 2022 00:00 - 2 Feb 2022 20:51

Threats Company risk score

Malware Outbreak

A malware outbreak has been detected in your network! At least 50%(1) from a total of 2 endpoints were found infected with "Application.Sohf.Dropper.B" between 2022-02-02 18:13:42 and 2022-02-02 19:29:21.

Show more >

- 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.

Welcome, Soumya Mukherjee

Executive Summary Last 7 days ACTIONS ▾

Reporting period 26 Jan 2022 00:00 - 2 Feb 2022 20:51

Managed endpoints	Active endpoints	Blocked threats	Company risk score
2	2	--	--

Inventory: Windows workstations 2 Windows servers 0 macOS 0 Linux 0 Physical endpoints 2 Virtual machines 0

Top 5 types of blocked threats

Type	Count
1	120
2	90
3	60
4	30
5	0

Incidents status

Remediation actions

Threats breakdown by endpoint type

On workstations 0
On servers 0

- 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.

Edit Endpoint Package

General

Name:	Test1
Description:	For testing purpose
Language:	English

Security Modules & Roles

Operation mode:	Detection and prevention
Modules:	<input checked="" type="checkbox"/> Antimalware <input checked="" type="checkbox"/> Advanced Threat Control <input checked="" type="checkbox"/> Advanced Anti-Exploit <input checked="" type="checkbox"/> Firewall <input checked="" type="checkbox"/> Network Protection <input checked="" type="checkbox"/> Content Control <input checked="" type="checkbox"/> Network Attack Defense <input checked="" type="checkbox"/> Device Control <input type="checkbox"/> Power User <input type="checkbox"/> Encryption <input type="checkbox"/> Patch Management

Buttons: Save, Cancel

Bitdefender GravityZone

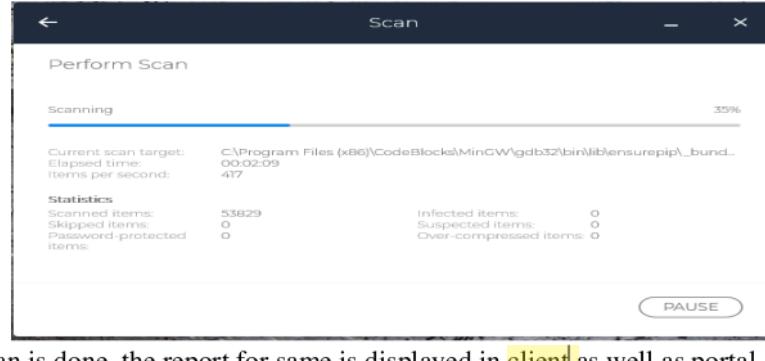
CUSTOMER SUPPORT More

- Threats Xplorer
- Network
- Patch Inventory
- Packages**
- Tasks

Add Download Send download links Delete Refresh

Name	Type	Language	Description
Test1	BEST	English	For testing purpose
Security Server Virtual Appliance	Security Server	English	Security for Virtualized

- 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 Article Error (ETS)

Client Output

Available scan logs	
Type	Created
Custom Scan	02 February 2022, 19:00:39
Quick Scan	02 February 2022, 18:59:30
Full Scan	02 February 2022, 18:23:32

Web Panel Output

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

Computers and Virtual Machines						Welcome, Soumya Mukherjee	
	Restore	Delete	Empty Quarantine	Refresh			
Computer	IP	File	Threat Name	Quarantined on	Action	Status	
<input type="checkbox"/>							
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Trojan.DOS.KILLMBR.Z	02 February 2022, 19:22:15		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Backdoor.Delf.DY	02 February 2022, 19:21:28		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Backdoor.Delf.DY	02 February 2022, 19:21:28		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Trojan.Agent.BSF	02 February 2022, 19:21:25		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Trojan.Hacktool.Agent.BK	02 February 2022, 19:21:24		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Trojan.Agent.Small.SY	02 February 2022, 19:21:05		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_TrojanDownloader.Small.JAO.M	02 February 2022, 19:21:05		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_AltTiny46097.9ME357581D	02 February 2022, 19:20:12		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Trojan.Agent.CYPC	02 February 2022, 19:19:12		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Win32.Worm.DoomJarka.B	02 February 2022, 19:19:11		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Trojan.Script.197111	02 February 2022, 19:19:08		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_VBS.BWVG.A	02 February 2022, 19:19:07		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_VirutBot.Nhi.A	02 February 2022, 19:19:07		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Trojan.Script.131554	02 February 2022, 19:19:06		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_IRC-Worm.Nosuck.Z	02 February 2022, 19:18:45		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Alt-Ransom46097.2D90477E21	02 February 2022, 19:18:43		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Win32.Worm.Nimda.U	02 February 2022, 19:18:42		None	
<input type="checkbox"/>	DESKTOP-OPSPDMN	192.168.1.104	E:\None\Of_Your_Business\CEH_Trojan.Ruby.Pydon.A	02 February 2022, 19:18:41		None	

- We can view all the endpoint devices at network tab

- We can view general information about the computer

Computer		Protection Layers	
Name:	NIHARPC	Endpoint:	Active
FQDN:	niharpc	Sandbox Analyzer:	Available
IP:	192.168.1.106	Security Analytics:	Available
OS:	Windows 10 Pro		
Label:	<input type="text"/>	Save	
Infrastructure:	Computers and Groups		
Group:	Computers and Groups		
State:	Online		
Last seen:	Now		

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

Agent	
Type:	BEST
Product version:	7.4.3.146
Last product update:	02 February 2022 18:22:22
Last check for a new product version:	02 February 2022 21:52:48
Product update location:	GravityZone Update Server - update.cloud.2d585.cdn.bitdefender.net
Engines version:	7.91082
Last security content update:	02 February 2022 21:53:21
Last check for new security content:	02 February 2022 21:53:05
Security content update location:	GravityZone Update Server - update.cloud.2d585.cdn.bitdefender.net
Primary scan engine:	Local Scan
Fallback scan engine:	None

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

The screenshot shows the Bitdefender GravityZone interface. On the left, a sidebar menu includes options like Monitoring, Dashboard, Executive Summary, Incidents, Blocklist, Search, Custom Rules (which is selected), Threats Xplorer, and Network. The main area is titled 'Create Detection Rule' with a sub-section 'Rule definition'. It asks 'Consider as detection every:' and has a 'File' icon selected. Below it, 'Matching the following criteria:' is set to 'Name Is login.php'. A 'Rule definition' section explains defining rules to mark specific behavior as valid detections. The right side shows a detailed view of the 'loginFinder' rule, which was created by soumyamukherjee18@gnu.ac.in on 02 February 2022, 18:57, last updated on the same date. The rule ID is 6fab7e2be2bb36b50290cb6 and it is active. The 'DETAILS' section specifies finding 'login.php files'. The 'IN CASE THIS HAPPENS' section states 'A file matching the following criteria: Name is: login.php'. The 'DO THE FOLLOWING' section says 'Generate an alert with **High** severity and display it in an incident.'.

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

The screenshot shows the 'Executive Summary' page. The sidebar menu is identical to the previous screen. The main area is titled 'Incidents status' and shows a summary: '1' incidents, all of which are circled in orange. Below this, there are two categories: 'Detected by prevention modules' (0) and 'Require investigation' (1).

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

Extended Incidents Endpoint Incidents Detected Threats

OPEN INCIDENTS		TOP ALERTS		TOP TECHNIQUES		TOP AFFECTED DEVICES	
High	0	DriversVolumesDiscov...	1	LogonRegModified	1	Unsecured Credentials	1
Medium	0	loginFinder	1	Boot or Logon Autostart...	1	NIHARPC	1
Low	1	Microsoft Internet Expl...	1	Command and Scripting...	1		

Change Status Alert name: Search for filenames, IP addresses, hostnames...

ID	Date	Status	Severity Score	Endpoint	Alerts	Attack type
#1	Updated 6 minutes ago	Open	32	NIHARPC	7	Malware

➤ Malware details:

 #1

Created On: 02 Feb 2022, 19:00:29
Last Updated on: 02 Feb 2022, 19:00:43
Endpoint: NIHARPC
Artifacts Involved: 48

DETECTION
Severity Score: 32 Incident Trigger: login.php

 loginFinder >

ATTACK INFO
Attack Types: Malware
Tactics: Persistence, Privilege Escalation, Execution, Credential Access

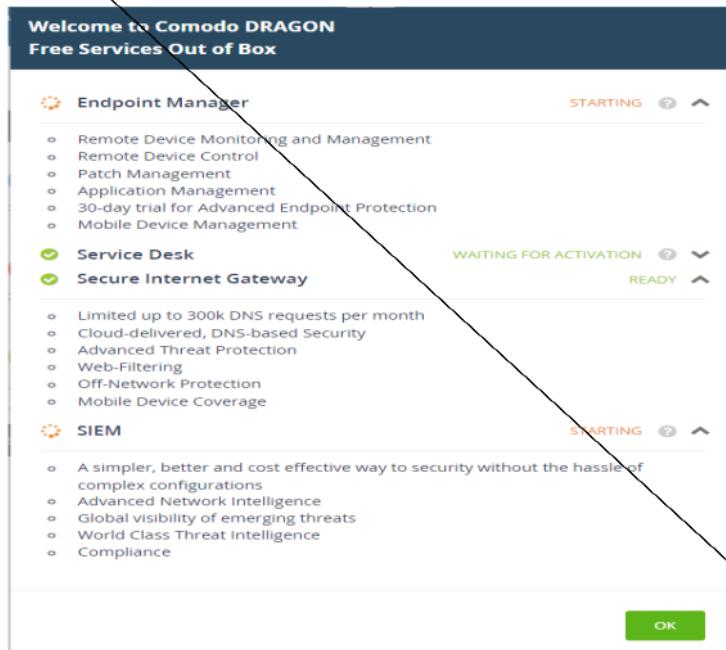
ATT&CK Techniques

Boot or Logon A...	T1547.004 Winlogon Helper DLL
Command and S...	T1059
Credentials from ...	T1555.003 Credentials from Web...
Unsecured Crede...	T1552.001 Credentials In Files

CHAPTER 9 (B) – IMPLEMENTATION (COMODO)

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.

The screenshot shows the "Device List" section of the Comodo web portal. The top navigation bar includes "Device List", "Supported Device Platforms", "License Options", and a "Logout" link. The main area displays a table of devices with columns: OS, NAME, ACTIVE COMPONENTS, VIRTUAL DESKTOP, PATCH STATUS, CUSTOMER, LOGGED IN USER, and LAST ACTIVITY. A single row is visible for "NiharPC". The table includes various icons for device status and management. At the bottom, there are pagination controls and a message indicating 1 result.

OS	NAME	ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LOGGED IN USER	LAST ACTIVITY
	NiharPC	AG AV FW CO		1	Default Cust...	NIHARPC	2022/02/23 11:06:06 PM

- Details covered under device profiling:

Device Name:

Summarized Info:

Device Name	Summary	Networks	Associated Profiles	Software Inventory	File List	Exported Configurations	MSI Installation State	Patch M...
Device Summary					OS Summary			
Custom device name: NiharPC Name: NiharPC Logged in user: NIHARPC\Admin AD\LDAP: N/A Domain\Workgroup: WORKGROUP Formfactor: PC Model: H310M H Communication Client version: 6.43.41148.21120 Processor: Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz Serial number: Default string System model: H310M H System manufacturer: Gigabyte Technology Co., Ltd. Ownership type: Not specified Last connection: 2022/02/23 11:25:56 PM Registered: 2022/02/23 09:58:10 PM Device time zone: UTC +05:30 (DST disabled) External IP: 43.241.193.215				OS: Windows OS name: Microsoft Windows 10 Pro (x64) OS version: 10.0.19044 OS full version: Version 21H2 (OS Build 19044.1526) Service pack: N/A Build version: 19044 Reboot time: 2022/02/23 09:57:51 PM Reboot reason: The process C:\Users\Admin\AppData\Local\Temp\tmp_32e32e1b39c5597ecbb6a83a08eed2d81cd9\offlineinstaller.exe (NIHARPC) has initiated the restart of computer NIHARPC on behalf of user NIHARPC\Admin for the following reason: Application: Maintenance (Planned) Reason Code: 0x80040001 Shutdown Type: restart Comment: Your device will reboot in 5 minutes because it's required by your administrator				

Security Patch Details and information regarding Performance metrics:

Security Products Info		Performance Metrics (Last updated: 2022/02/23 11:26:24 PM)	
Name	COMODO Client - Security	CPU usage	5% (2808 MHz)
Version	12.10.0.8697	RAM usage	51.20% (4160 MB of 8125 MB)
Components	Antivirus: on Containment: on Baselining: off Firewall: on Training mode: off HIPS: on Training mode: off Virtual Desktop: off	Network usage	Realtek Gaming GbE Family Controller: Load 0% speed channel (sent 14 Kbit/s, received 11 Kbit/s) TAP-ProtonVPN Windows Adapter V9: Load 0% speed channel (sent 0 bit/s, received 0 bit/s)
Virus DB version	34380	Disk usage	C: Free 32 GB Used 114 GB D: Free 106 GB Used 286 GB E: Free 159 GB Used 233 GB F: Free 0 MB Used 0 MB
Virus DB last update time	2022/02/23 10:56:34 PM		

Quick view on all software installed in client:

Software	Vendor	Version	Installation Date
COMODO Client - Security	COMODO Security Solutions Inc.	12.10.0.8697	2022/02/23
Endpoint Manager Communication Client	ITarian LLC	6.43.41148.21120	2022/02/23
VALORANT	Riot Games, Inc	N/A	2022/02/22
Microsoft Edge	Microsoft Corporation	98.0.1108.56	2022/02/19
Mozilla Firefox (x64 en-US)	Mozilla	97.0.1	2022/02/18
Microsoft Update Health Tools	Microsoft Corporation	3.65.0.0	2022/02/18
Brave	Brave Software Inc.	98.1.35.103	2022/02/17
Microsoft OneDrive	Microsoft Corporation	22.012.0117.0003	2022/02/17
Google Chrome	Google LLC	98.0.4758.102	2022/02/17

Security Patch running in endpoint:

Title	KB	CVE	Bulletin	Classification	Severity	Reboot	Release Date	Status
2022-01 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H2 for x64 (KB5008876)	5008876			Security Update	Important	Maybe	2022/01/12	Installed
2022-01 Update for Windows 10 Version 21H2 for x64-based Systems (KB4023057)	4023057			Critical Update	Unspecified	Maybe	2022/02/03	Installed
2022-02 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5010342)	5010342			Security Update	Unspecified	Maybe	2022/02/08	Installed
2022-02 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H2 for x64 (KB5010472)	5010472			Update	Unspecified	Maybe	2022/02/15	Available
Windows Malicious Software Removal Tool x64 - v5.98 (KB890830)	890830			Update Rollup	Unspecified	Maybe	2022/02/14	Installed

Results per page: 20

Displaying 1-5 of 5 results

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

FILE NAME	FILE PATH	FILE HASH	DATE QUARANTINED	COMODO RATING	ADMIN RATING	USER'S LAST ACTION	USER'S LAST ACTION STATUS
Uni.zip	D:\Virus\	211A67...	2022/02/23 10:17:44...	Unrecognized	Unrecognized	None	Unknown
quiz - 2.zip	D:\Virus\	910A72...	2022/02/23 10:17:44...	Unrecognized	Unrecognized	None	Unknown
Virus-main.zip	D:\Virus\	C1B34C...	2022/02/23 10:17:44...	Unrecognized	Unrecognized	None	Unknown
Malicious.js	D:\Virus\	38BCB8...	2022/02/23 10:17:44...	Unrecognized	Unrecognized	None	Unknown
payment.doc	D:\Virus\	0E3EC6...	2022/02/23 10:17:44...	Unrecognized	Unrecognized	None	Unknown
example2.pdf	D:\Virus\	E64F3E...	2022/02/23 10:17:43...	Unrecognized	Unrecognized	None	Unknown
LOKI.docx	D:\Virus\	F26333...	2022/02/23 10:17:43...	Unrecognized	Unrecognized	None	Unknown
Batch 76.zip	D:\Virus\	2EECCE...	2022/02/23 10:17:43...	Unrecognized	Unrecognized	None	Unknown
exam.doc	D:\Virus\	B32B8F...	2022/02/23 10:17:43...	Unrecognized	Unrecognized	None	Unknown

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

LOGIN	EMAIL	PHONE NUMBER	# OF DEVICES	STATUS	LAST LOGIN
rishabh	rishabh@gnu.ac.in	N/A	1	Not active	Not logged in yet
soumyamukherjee	soumyamukherjee@gnu.ac.in	N/A	1	Not available	2022/02/23 10:59:21 PM
srujan	srujan@gnu.ac.in	N/A	1	Not active	Not logged in yet

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

DATE/TIME	COMPONENTS	ACTION	DEVICE NAME	FILE NAME	FILE PATH	FILE HASH	INITIAL COMODO RATING	CURRENT COMODO RATING	INITIAL AVP RATING	CURRENT AVP RATING	ADDITIONAL INFO
2022/02/23 10:17:44 PM	Antivirus	Guaranteed	MinIPC	Maxwell	E:\test\maxwell	00000000000000000000000000000000	Unrecognized	Unrecognized	Not set	Not set	Malware@P@MinIPC
2022/02/23 10:17:44 PM	Antivirus	Guaranteed	MinIPC	payment.xls	E:\test\payment.xls	00000000000000000000000000000000	Unrecognized	Unrecognized	Not set	Not set	Malware@P@MinIPC001
2022/02/23 10:17:44 PM	Antivirus	Guaranteed	MinIPC	1000_1000_00000000000000000000000000000000	E:\test\1000_1000_00000000000000000000000000000000	00000000000000000000000000000000	Unrecognized	Unrecognized	Not set	Not set	Malware@P@MinIPC002
2022/02/23 10:17:44 PM	Antivirus	Guaranteed	MinIPC	Maxwell.xls	E:\test\maxwell.xls	00000000000000000000000000000000	Unrecognized	Unrecognized	Not set	Not set	Trojan/MS02.P@MinIPC003
2022/02/23 10:17:44 PM	Antivirus	Guaranteed	MinIPC	1001_01_01.xls	E:\test\1001_01_01.xls	00000000000000000000000000000000	Unrecognized	Unrecognized	Not set	Not set	Malware@P@MinIPC004
2022/02/23 10:17:44 PM	Antivirus	Guaranteed	MinIPC	Maxwell.xls	E:\test\maxwell.xls	00000000000000000000000000000000	Unrecognized	Unrecognized	Not set	Not set	Malware@P@MinIPC005
2022/02/23 10:17:44 PM	Antivirus	Guaranteed	MinIPC	Maxwell.xls	E:\test\maxwell.xls	00000000000000000000000000000000	Unrecognized	Unrecognized	Not set	Not set	Trojan/MS02.P@MinIPC006
2022/02/23 10:17:44 PM	Antivirus	Guaranteed	MinIPC	Maxwell.xls	E:\test\maxwell.xls	00000000000000000000000000000000	Unrecognized	Unrecognized	Not set	Not set	Malware@P@MinIPC007
2022/02/23 10:17:44 PM	Antivirus	Guaranteed	MinIPC	Maxwell.xls	E:\test\maxwell.xls	00000000000000000000000000000000	Unrecognized	Unrecognized	Not set	Not set	Malware@P@MinIPC008

- Web portal has a special tab for Valkyrie logs:

FILE NAME	FILE PATH	SHA1	FILE RATING	FIRST SEEN DATE BY COMODO
pip.exe	C:\Users\Admin\AppData\Local\Programs\Python\Python39\pip.exe	c4cc043c7190063768c941e31eeb1348fc5e317	Clean	2022/03/05 12:49:19 PM
0c030778938b0b6f982...	D:\Virus\ Virus-man\0c030778938b0b6f98236a...	32f561149b9063145895926f949d8ce7ac79	Malware	2017/02/22 10:12:55 PM

- Advanced security sub system “Valkyrie” dashboard

SHA1	FILE NAME	SOURCE	SUBMIT DATE	FINAL VERDICT	HUMAN EXPERT VERDICT	HUMAN EXPERT ANALYSIS STATUS
09ed982d3a66c5b621ca12c2d6617754a018b2a	GatoRoboto.exe	Upload	2022-03-10 13:55:49	Malware	Malware	Completed
f95d326da0642a2c2df07d0a0a3868300d6749c3	pCCoQ_2022-03-09_exxe.exe	Upload	2022-03-10 20:55:34	Malware	Malware	Completed
500efd3a0645ab8b79b7a27f3da193740:c56	CBerIP_2022-03-09_exxe.exe	Upload	2022-03-10 20:40:58	Malware	Malware	Completed
6fd5b58786c59b3cd922e400950704ad5db	zddmhyvxxzhzmrlabvv.exe	Upload	2022-03-10 19:42:28	Malware	Malware	Completed
e84ed061ac2eb007c534a91bd27781850872d11	V_3440775.exe	Upload	2022-03-10 19:40:20	Malware	Malware	Completed
0399952826d98fa1396374084bc15066c64501bf8	Solution.WindowsForm.exe	Upload	2022-03-10 19:40:20	Malware	Malware	Completed
03dcbb0693c39630bac595a8fb8c159512c7ac	a.exe	Upload	2022-03-10 19:40:20	Malware	Malware	Completed
4850403ca424c45ab8477d8df9a039aa97b45a24	SEAC.Azienda.FatturePA.WFInterf...	Upload	2022-03-10 19:33:33	Malware	Malware	Completed
633cfef925c510607e348d15448a8518154a4d	55d99599.exe	Upload	2022-03-10 19:33:33	Malware	Malware	Completed
e8696035a73187b1202ee9bfed104035609dxa0	IXA5x_2022-03-09_exxe.exe	Upload	2022-03-10 19:32:37	Malware	Malware	Completed

➤ Overview dashboard:

The screenshot shows the VALKYRIE dashboard with the following statistics:

- Total files uploaded: 4
- Total files queued: 8
- Files being processed: 0
- Files processing completed: 4
- Latest Malware Submissions:

STATUS	FILE NAME
Infected	help.php
Infected	26 file.dcf3077893b8b6f9823...
- Malware count: 2
- PUA count: 0

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

The screenshot shows the client's analysis interface with the following summary:

- TOTAL NUMBER OF FILES: 5
- TOTAL NUMBER OF CLEAN FILES: 3
- TOTAL NUMBER OF UNKNOWN FILES: 0
- TOTAL NUMBER OF MALWARE FILES: 2
- TOTAL NUMBER OF PUA: 0
- TOTAL NUMBER IN HUMAN EXPERT ANALYSIS: 0

Recent analysis requests table:

File Name	Path	SHA1	Submit Date	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Available Actions
statements.docx	statements.docx	9d8b7d9c65554a43cd...	2022-03-06 17:02:29	2022-03-06 17:02:26	Clean	Clean	Analysis Completed	View File Info Export Results To PDF
test2.vbs	test2.vbs	ebd5b3a695f93965eb...	2022-03-06 17:01:38	2022-03-06 17:01:34	Clean	Clean	Analysis Completed	View File Info Export Results To PDF
help.php	help.php	c5e525cb167a49437d1...	2022-03-06 17:01:17	2022-03-06 17:01:14	Malware	Malware	Analysis Completed	View File Info Export Results To PDF
26 file.dcf3077893b8b6f9823...	D:\Virus\Virus-main\dc...	32f611459fb631458...	2017-02-22 22:12:55	2022-03-06 17:00:23	Malware	Malware	Analysis Completed	View File Info Export Results To PDF
pip.exe	C:\Users\Admin\AppData\Local\Temp\pip...	e4cc043c7190063768c...	2022-03-05 12:49:19	2022-03-05 12:48:41	Clean	Clean	Analysis Completed	View File Info Export Results To PDF

Showing 1 to 5 of 5 entries

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

The screenshot shows the COMODO Client - Security interface with the following status:

- Secure
- All systems are active and running
- MANAGE PROTECTION
- SILENT MODE

Right-hand sidebar options:

- Scan
- View Quarantine
- Update
- Open Task Manager

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

Realtime Scan

- Enable Realtime Scan (Recommended)**
This option enables virus scanning when your computer is used and prevents threats before they enter your system.
- Enable scanning optimizations (Recommended)**
Use this option to activate the performance improving technologies for realtime scanning.
- Do not show auto-scan alerts**
- Use this option to scan removable media such as USB sticks, CDs, DVDs, external HDDs, etc.
- Detection**
 - Scan computer memory after the computer starts
 - Do not show antivirus alerts
 - Decompress and scan archive files of extension(s): *.exe, *.jar
 - Set new on-screen alert timeout to secs
 - Set new maximum file size limit to MB
 - Set new maximum script size limit to MB
 - Use heuristic scanning
 - Enable realtime scanning of files on network
 - Use Windows Antimalware Scan Interface (AMSI) technology
 - Use cloud services while scanning via AMSI (Cloud Lookup should be enabled in File Rating section)

Firewall Settings

- Enable Firewall (Recommended)**
- This option enables firewall which filters inbound and outbound traffic.
- Alert Settings**
 - Do not show popup alerts
 - Turn traffic animation effects on
 - Create rules for safe applications
 - Set alert frequency level
 - Set new on-screen alert timeout to secs
- Advanced**
 - Filter IPv6 traffic
 - Filter loopback traffic (e.g. 127.x.x.x, ::1)
 - Block fragmented IP traffic
 - Do protocol analysis
 - Enable anti-ARP spoofing
 - Detect disabled firewall driver in network adapter settings and

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

COMODO Advanced Settings

- Auto-Containment**
This option enables automatic containment of executable files and scripts according to the policy defined below.

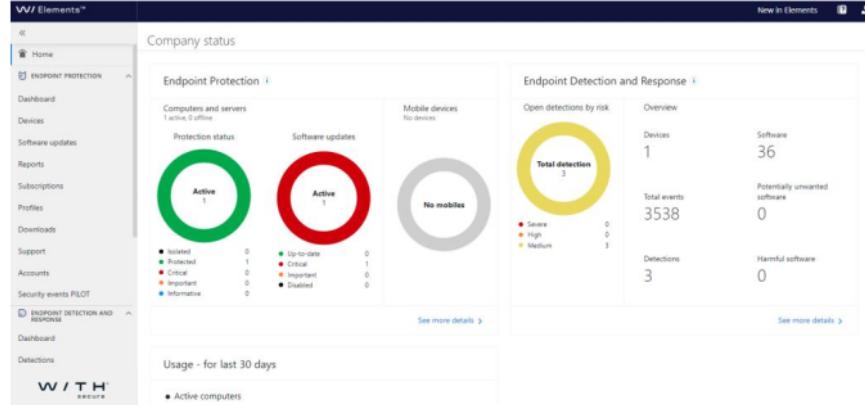
Action	Target	Rating	Enable Rule
Block	All Applications	Malicious	<input checked="" type="checkbox"/>
Block	Suspicious Locations	Any	<input checked="" type="checkbox"/>
Block	Containment Folders	Any	<input checked="" type="checkbox"/>
Ignore	Communication Client	Trusted	<input checked="" type="checkbox"/>
Ignore	Metro Apps	Any	<input checked="" type="checkbox"/>
Ignore	Global Whitelist	Unrecognized	<input checked="" type="checkbox"/>
Ignore	All Applications	Unrecognized	<input checked="" type="checkbox"/>
Ignore	All Applications	Unrecognized	<input checked="" type="checkbox"/>
Run Virtually	Pseudo File Downloaders	Any	<input checked="" type="checkbox"/>
Block	SQL Clients	Any	<input checked="" type="checkbox"/>
Block	Garbled	Sp. (ETS)	<input checked="" type="checkbox"/>

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



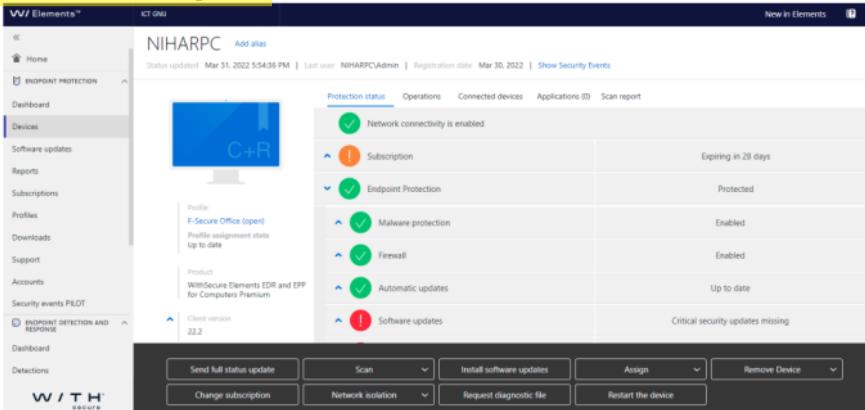
CHAPTER 9 (C) – IMPLEMENTATION (WITHSECURE)

- Initialising the web portal, opening “Dashboard”

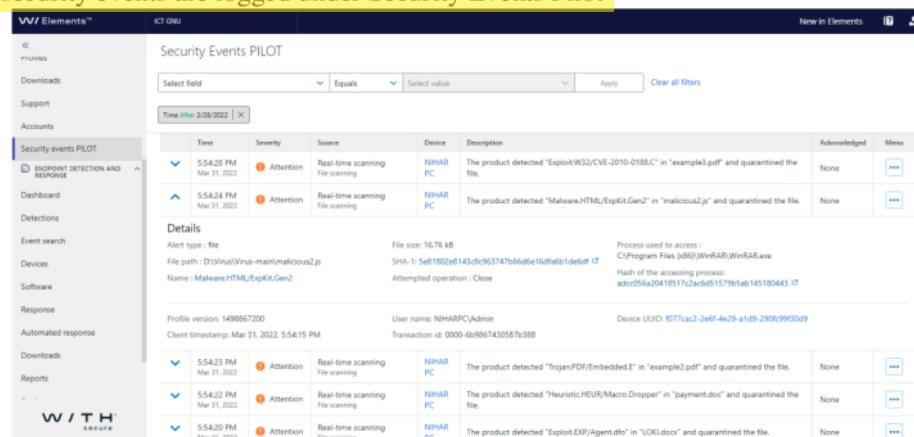


We can view all the endpoints, their security state, software updates, any critical notifications all at one place.

- 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

Time	Severity	Source	Device	Description	Acknowledged	Menu
5:54:28 PM Mar 31, 2022	Attention	Real-time scanning File scanning	NIHAR PC	The product detected "Exploit:W32/CVE-2010-0188.C" in "example3.pdf" and quarantined the file.	None	⋮
5:54:24 PM Mar 31, 2022	Attention	Real-time scanning File scanning	NIHAR PC	The product detected "Malware:HTML/ExpKit.GenZ" in "malicious2.js" and quarantined the file.	None	⋮
5:54:23 PM Mar 31, 2022	Attention	Real-time scanning File scanning	NIHAR PC	The product detected "Trojan:PDF/Embedded.E" in "example2.pdf" and quarantined the file.	None	⋮
5:54:22 PM Mar 31, 2022	Attention	Real-time scanning File scanning	NIHAR PC	The product detected "Heuristic:HEUR/Macro.Dropper" in "payment.doc" and quarantined the file.	None	⋮
5:54:20 PM Mar 31, 2022	Attention	Real-time scanning File scanning	NIHAR PC	The product detected "Exploit:DIF/Agent.dfo" in "LOKI.docx" and quarantined the file.	None	⋮

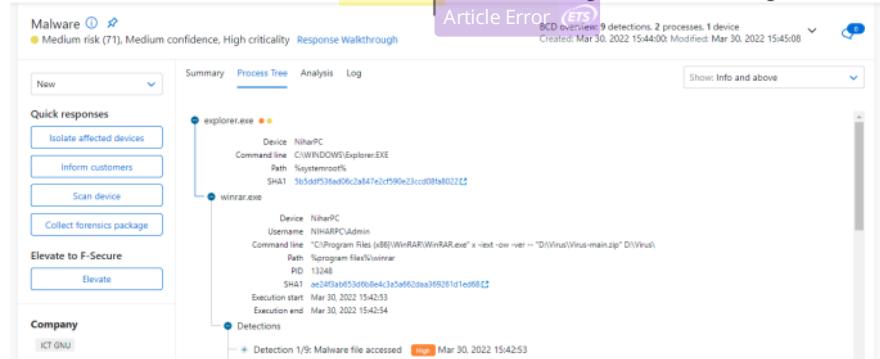
- Detection and Response has a different dashboard to offer, which basically shows total endpoints and total malicious files detected along with the total number of events triggered.

Detections:

ID	Risk	Type	Devices	Detected	Modified	Status	Properties	Comments
123992844-5	Medium	Malware	1	31.03.2022 12:24:37	31.03.2022 12:25:30	New	0	
123992844-2	Medium	Malware	1	30.03.2022 15:50:17		New	0	
123992844-1	Medium	Malware	1	30.03.2022 15:44:00	30.03.2022 15:45:08	New	0	

- 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:

Detection 2/9: Epp on access detection [Medium] Mar 30, 2022 15:42:54

Description: File access attempt on file detected with scan engine

Analysis

Event ID(s): 5a4edb56-b040-11ec-869b-0242ac110033

EPP scan

Infection name: Exploit.EXP/Agent.dfo

Type: FILE

Reference: D:\Virus\Virus-main\LOKI.docx

SHA1: f263339ab10d01dc983cedbb82fa84e9bf5ba79

Performed action: DELETE

System wide: false

- Report logs for automated actions:

Reports ...

Protection status Security events Infections Software Updates Audit Log Devices

Computer protection status

Last 28 days

March 10, 2022 – April 6, 2022

Protected Non-critical issue Critical issue Has not communicated in 14 days or more

Latest malware definition updates on computers

Last 28 days

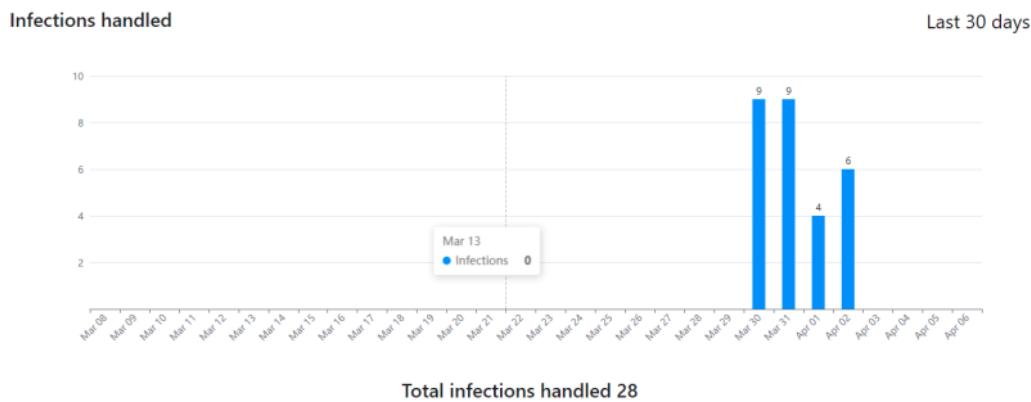
March 10, 2022 – April 6, 2022

Less than 7 days ago 7-14 days ago More than 14 days ago Has not communicated in 14 days or more

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



- Graphical representation of data:



- Client-Side Initialisation:

F-SECURE ELEMENTS AGENT



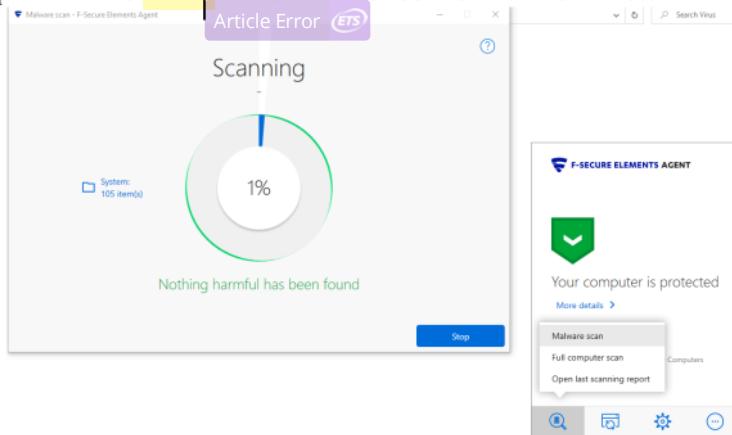
Setting up your protection...

[More details >](#)

F-Secure Elements EDR and EPP for Computers
Premium
Version 22.2



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



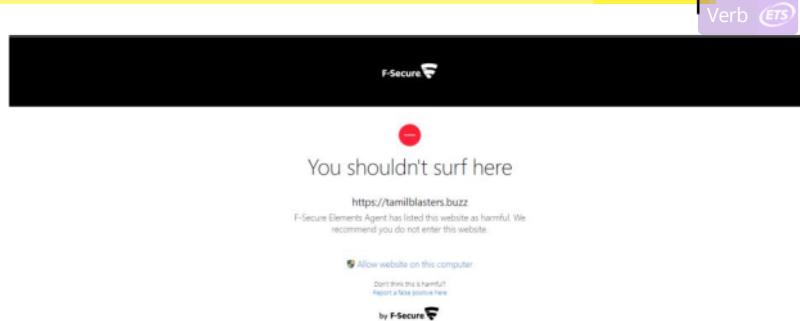
- Once a scan completes it sends a detailed report to client as well as shows it in portal.

The image displays two side-by-side screenshots. On the left is the 'Event History - F-Secure Elements Agent' page, which lists various events such as 'Harmful file quarantined' and 'Harmful website blocked'. On the right is a detailed 'Threat Description' for 'Trojan.PWS.Fareit', showing classification (Category: Malware, Type: Trojan-PWS, Platform: Win), summary (steals login credentials), removal (Automatic action: Quarantine file), and support links for Community, User Guide, Contact Support, and Submit a sample.

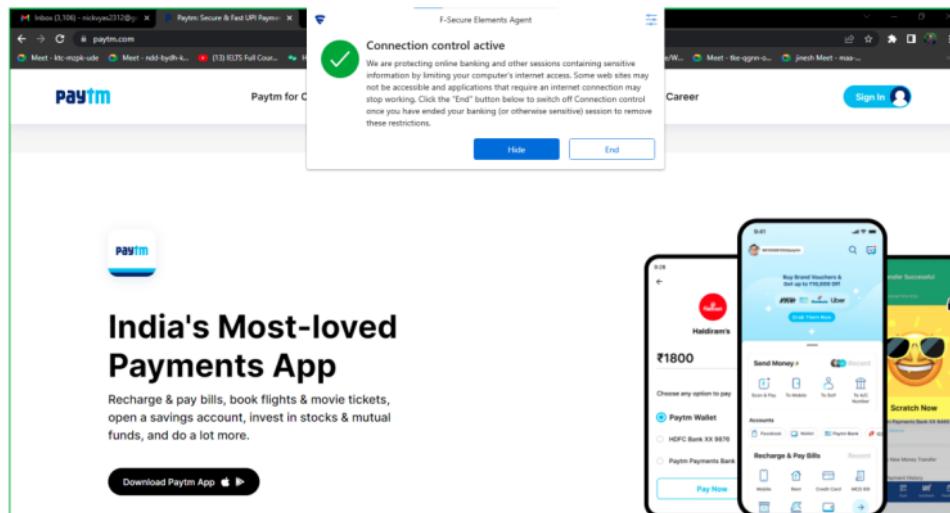
- On clicking you can view detailed report on the malware:

This screenshot provides a detailed view of the threat description for 'Trojan.PWS.Fareit'. It includes sections for Classification (Category: Malware, Type: Trojan-PWS, Platform: Win), Summary (steals login credentials), Removal (Automatic action: Quarantine file), and a 'FOR MORE SUPPORT' section with links to Community, User Guide, Contact Support, and Submit a sample.

- Client tool also provides malicious link blocker for secure web 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.

Sp. (ETS)

CHAPTER 11 – REFERENCES

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



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 bibliography On

Exclude matches Off

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.



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.



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.



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.



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



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**.



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.



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.



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.



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.



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.



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.



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.

PAGE 24

PAGE 25



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.



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.



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**.



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. 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.



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.



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