

*PROJECT REPORT*

*On*

**Functioning of SOC including IDS & IPS**

*Submitted by*

**Pragya Rathore (IU1841220041)**

*In fulfillment for the award of the degree*

*Of*

**BACHELOR OF TECHNOLOGY**

*In*

**INFORMATION TECHNOLOGY**



**INSTITUTE OF TECHNOLOGY AND ENGINEERING  
INDUS UNIVERSITY CAMPUS, RANCHARDA, VIA – THALTEJ  
AHMEDABAD – 382115, GUJARAT, INDIA**

WEB: [www.indusuni.ac.in](http://www.indusuni.ac.in)  
APRIL 2022

**PROJECT REPORT**  
**ON**  
**Functioning of SOC including IDS & IPS**

**AT**



In the partial fulfillment of the requirement for the degree of  
Bachelor of Technology  
in  
Information Technology

**PREPARED BY**

Pragya Rathore (IU1841220041)

**UNDER GUIDANCE OF**

**External Guide**

Deepak Bhavsar & Divyesh Vaishnav  
Infoconcept Consulting Pvt. Ltd.  
Ahmedabad

**Internal Guide**

Abhishek Vaghela  
Assistant Professor  
Department of Computer Engineering  
I.T.E, Indus University, Ahmedabad

**SUBMITTED TO**

INSTITUTE OF TECHNOLOGY AND ENGINEERING  
INDUS UNIVERSITY CAMPUS, RANCHARDA, VIA-THALTEJ  
AHMEDABAD-382115, GUJARAT, INDIA

APRIL 2022

## CANDIDATE'S DECLARATION

---

I declare that final semester report entitled “**Functioning of SOC including IDS & IPS**” is my own work conducted under the supervision of the guide **Assistant Prof. Abhishek Vaghela**.

I further declare that to the best of my knowledge, the report for B.Tech final semester does not contain part of the work which has been submitted for the award of B.Tech Degree either in this university or any other university without proper citation.

---

Candidate's Signature

PRAGYA RATHORE (IU1841220041)

---

Guide: Mr. Abhishek Vaghela  
Assistant Professor,  
Department of Computer Engineering,  
Indus Institute of Technology and Engineering  
INDUS UNIVERSITY– Ahmedabad,  
State: Gujarat

**INDUS INSTITUTE OF TECHNOLOGY AND ENGINEERING  
COMPUTER ENGINEERING**

**2021 - 2022**



**CERTIFICATE**

**Date: 19-04-2022**

This is to certify that the project work entitled “**Functioning of SOC including IDS & IPS**” has been carried out by **Pragya Rathore** under my guidance in partial fulfillment of degree of Bachelor of Technology in **INFORMATION TECHNOLOGY (Final Year)** of Indus University, Ahmedabad during the academic year 2021 - 2022.

---

**ABHISHEK VAGHELA**

Assistant Professor  
Department  
Department of Computer Engineering  
I.T.E, Indus University  
Ahmedabad

---

**Dr. SEEMA MAHAJAN**

Head of the  
Department of Computer Engineering  
I.T.E, Indus University  
Ahmedabad

## ACKNOWLEDGEMENT

---

A successful project is a result of fruitful efforts of many people, some directly involved and some indirectly, by providing support and encouragement.

I would like to thank my university faculties for their encouragement & moral support throughout my degree course and express a deep sense of gratitude and respect to my project guide Mr. Abhishek Vaghela who provided immense help and I am really grateful to him for providing necessary suggestions and guidance for the success of this project. He encouraged me to undertake such a great challenging and innovative work. I am grateful to for him guidance, understanding and insightful support in the journey of this project.

I would like to thank my friends for making me more confident, having faith in my strengths and helping me to work on my weaknesses.

Finally, I wouldn't be able to choose Cyber Security field if my parents & my sister didn't believe in me. They were a constant support and I am really glad that they have my back.

## **ABSTRACT**

---

Cyber security can be described as the collective methods, technologies, and processes to help protect the confidentiality, integrity, and availability of computer systems, networks, and data, against cyber-attacks or unauthorized access. The main purpose of cyber security is to protect all organizational assets from both external and internal threats as well as disruptions caused due to natural disasters.

To attain effective cyber security, it is necessary to implement proper technology which gives protection from the incoming attacks. But as we know, nothing is foolproof. So, we need constant monitoring with real time response and incident analysis to be safeguarded from attacks. To make monitoring efficient, we need SIEM tools that collect data from all different data sources and represent it at one place and also provide some features like visual charts to make easy understanding of logs.

The other important aspect of cyber security is to check our own environment with different types of attacks. To make this part automatic we need some tools that will perform breach and attack simulation in our environment without any harm. The user awareness is also very important to make sure the environment is secured. For that some type of simulation should be there to aware the users and identify the phishing or spoofing emails.

# TABLE OF CONTENTS

---

<b>TITLE</b>	<b>PAGE NO.</b>
ACKNOWLEDGEMENT .....	v
ABSTRACT .....	vi
TABLE OF CONTENTS .....	vii
LIST OF FIGURES .....	x
LIST OF TABLES .....	xii
<b>CHAPTER 1 INTRODUCTION.....</b>	<b>1</b>
1.1 PROJECT DESCRIPTION .....	2
1.2 TECHNOLOGY USED .....	2
1.3 PURPOSE.....	3
1.4 SCOPE.....	3
1.5 OBJECTIVE.....	3
<b>CHAPTER 2 DESIGN &amp; CONCEPT .....</b>	<b>5</b>
2.1 WHAT IS SOC? .....	6
2.2 WHAT IS IDS? .....	8
2.3 WHAT IS IPS? .....	9
2.4 ARCHITECTURE FLOWCHART .....	10
<b>CHAPTER 3 PREVENTIVE SECURITY .....</b>	<b>11</b>
3.1 SIEM TOOL .....	12
3.1.1 WAZUH .....	13
3.1.1.1 WAZUH ARCHITECTURE.....	14

3.1.1.2 WAZUH CONFIGURATION / INTEGRATION.....	15
3.2 WEB APPLICATION FIREWALL (WAF) .....	16
3.2.1 IMPERVA WAF .....	17
3.2.1.1 MONITORING WITH IMPERVA .....	17
3.3 ENDPOINT DETECTION & RESPONSE (EDR).....	20
3.3.1 CROWDSTRIKE .....	21
<b>CHAPTER 4 SIMULATION TOOLS .....</b>	<b>24</b>
4.1 BREACH & ATTACK SIMULATION (BAS) TOOL .....	25
4.1.1 INFECTION MONKEY .....	26
4.1.1.1 HOW IT WORKS?.....	26
4.1.1.2 USE CASES .....	27
4.1.1.3 CONFIGURATION .....	28
4.1.1.4 ANALYSIS & REPORT .....	30
4.2 PHISHING SIMULATION TOOL.....	32
4.2.1 GOPHISH.....	33
4.2.1.1 CONFIGURATION .....	33
4.2.1.2 RESULTS .....	35
<b>CHAPTER 5 ENDPOINT SECURITY.....</b>	<b>37</b>
5.1 EMAIL SECURITY .....	38
5.1.1 MICROSOFT 365 DEFENDER .....	39
5.2 CLOUD SECURITY .....	42
5.2.1 NETSKOPE.....	43



<b>CHAPTER 6 CONCLUSION.....</b>	<b>46</b>
6.1 CONCLUSION .....	47
6.2 PROBLEM ENCOUNTERED AND POSSIBLE SOLUTIONS.....	47
6.3 REFERENCES .....	48

## LIST OF FIGURES

---

<b>FIGURE</b>	<b>TITLE</b>	<b>PAGE NO.</b>
Figure 2.1	SOC Features.....	6
Figure 2.2	Client Architecture.....	10
Figure 3.1	SIEM Features.....	12
Figure 3.1.1	Wazuh Features.....	13
Figure 3.1.2	Wazuh Components.....	14
Figure 3.1.3	Wazuh Agents.....	15
Figure 3.1.4	Security Configuration.....	15
Figure 3.1.5	Security Alerts.....	15
Figure 3.2.1	Imperva Traffic Requests.....	17
Figure 3.2.2	Visits by Country / Browser.....	18
Figure 3.2.3	Incidents blocked by rules.....	18
Figure 3.2.4	Threats hitting web application.....	19
Figure 3.2.5	Configured Policies.....	19
Figure 3.2.6	Detailed Incident Log.....	19
Figure 3.3.1	CrowdStrike Detections.....	21
Figure 3.3.2	Quarantined Files.....	22
Figure 3.3.3	Connect to Host.....	22
Figure 3.3.4	Feature of CrowdStrike.....	23
Figure 4.1.1	Flow in Infection Monkey.....	26
Figure 4.1.2	Credentials Leak.....	28
Figure 4.1.3	MITRE ATT&CK Assessment.....	29
Figure 4.1.4	Network Breach.....	29

Figure 4.1.5 Network Breach Map.....	30
Figure 4.1.6 Zero Trust Report.....	30
Figure 4.1.7 Test Findings.....	31
Figure 4.1.8 Attack Results.....	31
Figure 4.2.1 GoPhish Dashboard.....	33
Figure 4.2.2 Sending Profiles.....	34
Figure 4.2.3 Email Templates.....	34
Figure 4.2.4 Landing Pages.....	35
Figure 4.2.5 Recent Phishing Campaigns.....	35
Figure 4.2.6 Results of one campaign.....	35
Figure 4.2.7 Detailed activity of one user.....	36
Figure 5.1.1 Email alerts.....	40
Figure 5.1.2 Quarantined Mails.....	40
Figure 5.1.3 Policies Configured.....	41
Figure 5.1.4 Statistics Report.....	41
Figure 5.2.1 Netskope Compromised Credentials.....	43
Figure 5.2.2 Behavior Analytics.....	44
Figure 5.2.3 Incident Details.....	44
Figure 5.2.4 Users affected by malware.....	45

## LIST OF TABLES

---

Table 1: List of Technologies .....	2
-------------------------------------	---

# **CHAPTER 1**

# **INTRODUCTION**

❖ **PROJECT DESCRIPTION**

❖ **TECHNOLOGIES**

❖ **PROJECT PURPOSE**

❖ **PROJECT SCOPE**

❖ **GOALS AND OBJECTIVES**

## 1.1 PROJECT DESCRIPTION

---

Essentially, my project is divided into sections that are not fully related to one another due to the fact that I worked with various clients, but all aspects are related to cyber security.

To begin, the SIEM tool, Wazuh, must be integrated on a variety of data sources, including Amazon Web Services, Imperva WAF, and New Relic Application Output Tools.

Secondly, I have worked on CrowdStrike EDR, Microsoft 365 Defender. Also, I have explored and completed testing on different tools like Infection Monkey which is a BAS (Breach and Attack Simulation) tool and GoPhish which is a phishing simulation tool.

## 1.2 TECHNOLOGY USED

---

TECHNOLOGY USED	DESCRIPTION
Wazuh	SIEM Tool
Infection Monkey	Breach and Attack Simulation Tool
GoPhish	Phishing Simulation Tool
Microsoft Defender	Email Security Gateway
CrowdStrike	Endpoint Detection & Response
Imperva	Web Application Firewall

Table 1: List of Technologies

## **1.3 PURPOSE**

---

The main purpose is to secure the whole network environment. To prevent attack and give quick and real-time response. The other purpose is to check our own environment's vulnerability against different types of attacks.

The scope of the monitoring and the testing is depending on the agreement with the client that on which environment and accounts they want testing and monitoring.

## **1.4 SCOPE**

---

The scope of the monitoring and the testing is depending on the agreement with the client that on which environment and accounts they want testing and monitoring.

## **1.5 OBJECTIVE**

---

My motivation behind choosing this project and this field, that it never gets boring, requires out-of-the-box thinking and has great growth opportunities. The 'demand & supply' of security professionals is way out of proportion, meaning this is probably the only field of IT which has negative unemployment. And hence, the growing need of securing systems, network and data is giving golden chances to young IT minds.

The main purpose is to secure the whole network environment. To prevent attack and give quick and real-time response. The other purpose is to check our own environment's vulnerability against different types of attacks.

Main objectives are:

- To prevent hackers from hacking the network environment.
- If a hacker exploits any vulnerability and enters in a network then detect, analyze, and take appropriate action to prevent it.
- To monitor all the logs at one place via SIEM tool.
- To find the vulnerabilities present in the current environment against new attacks and after finding we can patch those vulnerabilities.
- To make the employees aware against email fraud by doing a phishing simulation campaign.



## **CHAPTER 2**

# **DESIGN & CONCEPT**

- ❖ **WHAT IS SOC?**
- ❖ **WHAT IS IDS?**
- ❖ **WHAT IS IPS?**
- ❖ **ARCHITECTURE  
FLOWCHART**

## 2.1 WHAT IS SOC?

---

A security operations center (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes.



Figure 2.1: SOC Features

Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work closely with Organizational incident response teams to ensure security issues are addressed quickly upon Discovery.

Also known as information security operations center (ISOC) is a dedicated to a site where enterprise information systems are managed like following:

- Web sites
- Applications
- Databases
- Data centers and servers
- Networks
- Desktops and other endpoints are monitored, assessed (value), and defended

## 2.2 WHAT IS IDS?

---

An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer.

It is a device or software application that monitors a network for malicious activity or policy violations. Any malicious activity or violation is typically reported or collected centrally using a security information and event management system. Some IDS's are capable of responding to detected intrusion upon discovery. These are classified as intrusion prevention systems (IPS).

There is a wide array of IDS, ranging from antivirus software to tiered monitoring systems that follow the traffic of an entire network. The most common classifications are:

- Network intrusion detection systems (NIDS): A system that analyzes incoming network traffic.
- Host-based intrusion detection systems (HIDS): A system that monitors important operating system files.
- Signature-based: detects possible threats by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This terminology originates from antivirus software, which refers to these detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available.
- Anomaly-based: a newer technology designed to detect and adapt to unknown attacks, primarily due to the explosion of malware. This detection method uses machine learning to create a defined model of trustworthy activity, and then compare new behavior against this trust model. While this approach enables the detection of previously unknown attacks, it can suffer from false positives: previously unknown legitimate activity can accidentally be classified as malicious.

## 2.3 WHAT IS IPS?

---

An intrusion prevention system (IPS) is a form of network security that works to detect and prevent identified threats. Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents and capturing information about them.

The IPS reports these events to system administrators and takes preventative action, such as closing access points and configuring firewalls to prevent future attacks. IPS solutions can also be used to identify issues with corporate security policies, deterring employees and network guests from violating the rules these policies contain.

An intrusion prevention system is typically configured to use a number of different approaches to protect the network from unauthorized access. These include:

- **Signature-Based** - The signature-based approach uses predefined signatures of well-known network threats. When an attack is initiated that matches one of these signatures or patterns, the system takes necessary action.
- **Anomaly-Based** - The anomaly-based approach monitors for any abnormal or unexpected behavior on the network. If an anomaly is detected, the system blocks access to the target host immediately.
- **Policy-Based** - This approach requires administrators to configure security policies according to organizational security policies and the network infrastructure. When an activity occurs that violates a security policy, an alert is triggered and sent to the system administrators.

The IPS performs real-time packet inspection, deeply inspecting every packet that travels across the network. If any malicious or suspicious packets are detected, the IPS will carry out one of the following actions:

- Terminate the TCP session that has been exploited and block the offending source IP address or user account from accessing any application, target hosts or other network resources unethically.
- Reprogram or reconfigure the firewall to prevent a similar attack occurring in the future.

- Remove or replace any malicious content that remains on the network following an attack. This is done by repackaging payloads, removing header information and removing any infected attachments from file or email servers.

## 2.4 ARCHITECTURE FLOWCHART

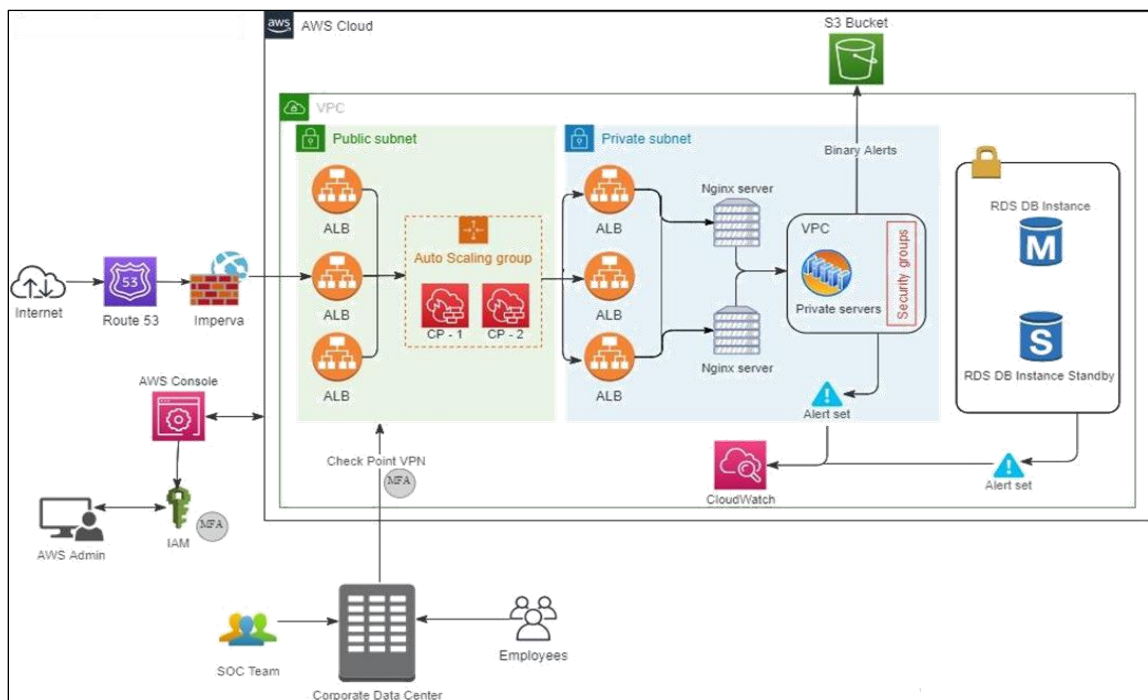


Figure 2.2: Client Architecture

## **CHAPTER 3**

# **PREVENTIVE SECURITY**

- ❖ **SECURITY INFORMATION &  
EVENT MANAGEMENT**
- ❖ **WEB APPLICATION  
FIREWALL**
- ❖ **ENDPOINT DETECTION &  
RESPONSE**

### 3.1 SIEM TOOL

---

Security Information and Event Management (SIEM) is a software product focused on the security of systems. It is a combination of security information management (SIM) and security event management (SEM) tools. This combination allows you to do real-time analysis and offline analysis with persisted data that you can retain for a long time.

Everything starts with data collection, and that's where SIM comes into play. Depending on the specific tool you use, you can actively move data or upload data on demand to a centralized place. Choosing one tool over another will determine whether you are doing real-time analysis or forensic analysis using data from the past. Once you load data, you can perform searches for troubleshooting and create reports and visualizations to make sense of the collected data.

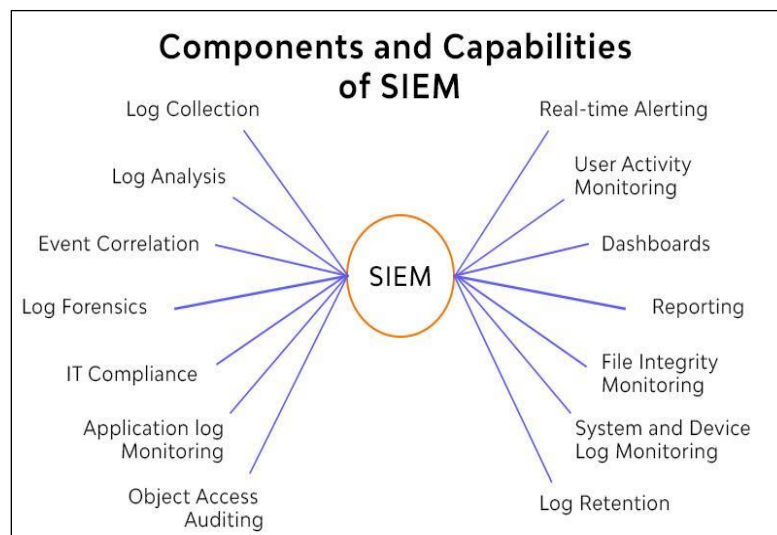


Figure 3.1: SIEM Features

Things then get interesting when SEM comes to the table. After you have identified patterns in the data, you can correlate the data to automate notifications and actions based on the rules you define. For example, you can set it to trigger an alert because there are too many 404 errors. By looking at the logs, you can then correlate the requests to see that someone is trying to find a hole in your system.



### 3.1.1 WAZUH

Wazuh is a free and open-source platform for threat detection, security monitoring, incident response and regulatory compliance. It can be used to monitor endpoints, cloud services and containers, and to aggregate and analyze data from external sources<sup>[1]</sup>. Wazuh provides the following capabilities:

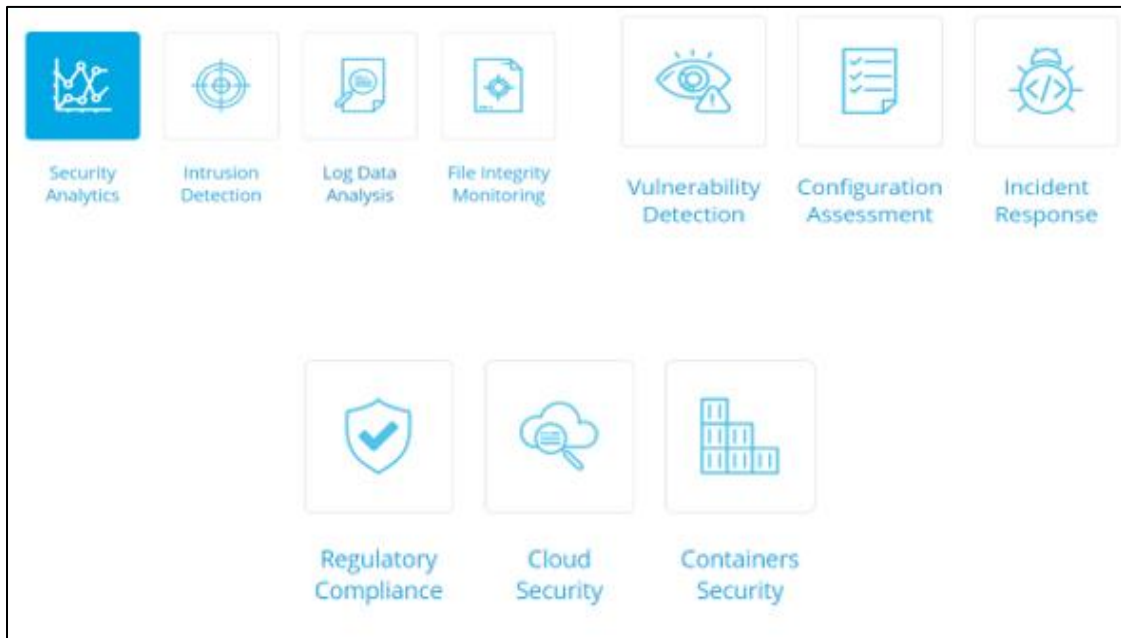


Figure 3.1.1: Wazuh Features

### 3.1.1.1 WAZUH ARCHITECTURE

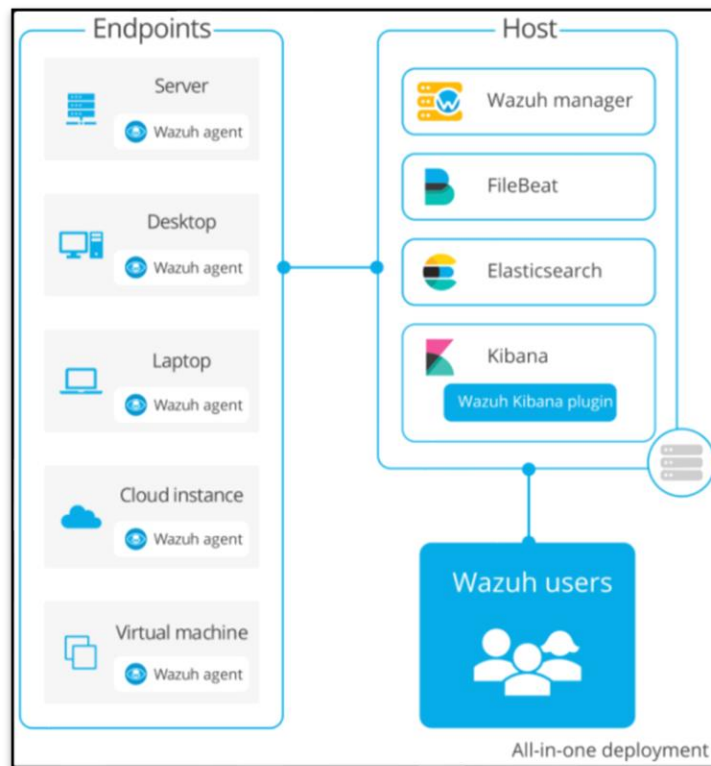


Figure 3.1.2: Wazuh Components

- Wazuh Manager is used for analyzing the data received from the agents.
- File beat is a lightweight shipper for forwarding and centralizing log data.
- Elasticsearch allows you to store, search, and analyze huge volumes of data quickly and in near real-time and give back answers in milliseconds.
- Kibana is an open-source data visualization & exploration tool used for log and time-series analytics.

### 3.1.1.2 WAZUH CONFIGURATION / INTEGRATION

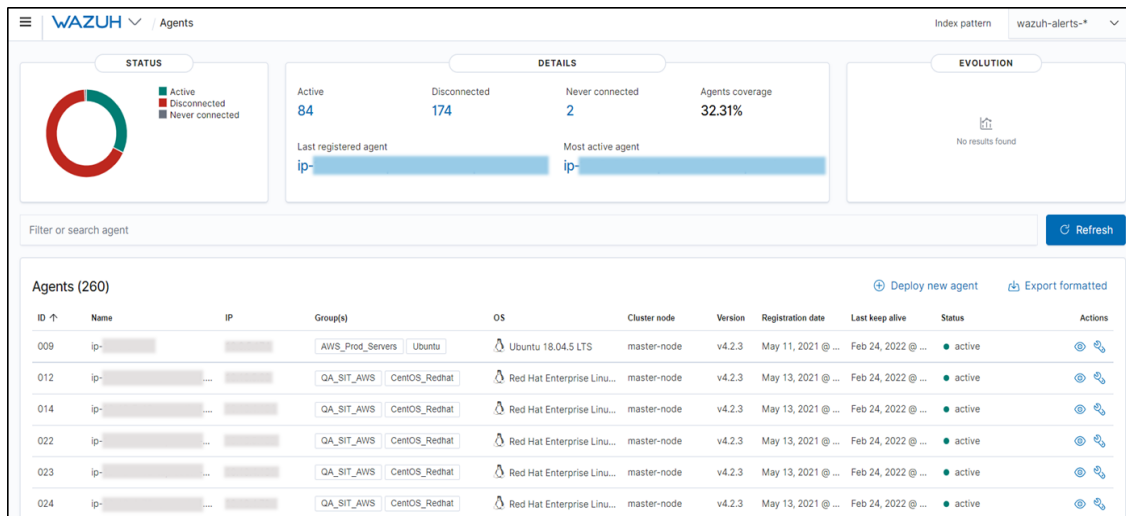


Figure 3.1.3: Wazuh Agents

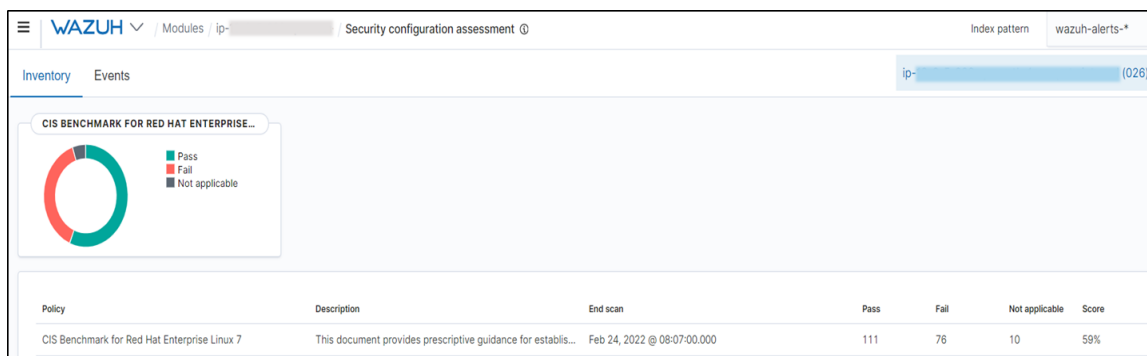


Figure 3.1.4: Security Configuration

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Apr 5, 2022 @ 09:30:06.118	278	ip-...ap-south-1.compute.internal	T1169	Privilege Escalation	Successful sudo to ROOT executed.	3	5402
> Apr 5, 2022 @ 09:30:06.116	278	ip-...ap-south-1.compute.internal			PAM: Login session closed.	3	5502
> Apr 5, 2022 @ 09:30:06.112	278	ip-...ap-south-1.compute.internal	T1169	Privilege Escalation	Successful sudo to ROOT executed.	3	5402
> Apr 5, 2022 @ 09:30:06.106	278	ip-...ap-south-1.compute.internal	T1169	Privilege Escalation	Successful sudo to ROOT executed.	3	5402
> Apr 5, 2022 @ 09:30:06.102	278	ip-...ap-south-1.compute.internal	T1169	Privilege Escalation	Successful sudo to ROOT executed.	3	5402
> Apr 5, 2022 @ 09:30:06.101	278	ip-...ap-south-1.compute.internal			PAM: Login session closed.	3	5502

Figure 3.1.5: Security Alerts

## 3.2 WEB APPLICATION FIREWALL (WAF)

---

A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.

A WAF is a protocol layer 7 defense (in the OSI model) and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors.

By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine's identity by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server.

A WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS attack, rate limiting can be quickly implemented by modifying WAF policies.

### 3.2.1 IMPERVA WAF

Imperva WAF is a key component of a comprehensive Web Application and API Protection (WAAP) stack that secures from edge to database, so the traffic you receive is only the traffic you want <sup>[2]</sup>.

WAF Gateway continuously adapts to evolving threats, mitigates the risk of online data breaches, prevents account takeover, and addresses regulatory compliance requirements such as PCI DSS 6.6. Imperva WAF Gateway is a key component of Imperva's market-leading, full stack application security solution which brings defense-in-depth to a new level.

Imperva WAF integrates with most of the leading Security Information and Event Management (SIEM) systems such as Splunk and others. It exports events as syslog messages. Events generated by Imperva WAF are intuitively indexed and easily searchable for quick incident response.

#### 3.2.1.1 MONITORING WITH IMPERVA



Figure 3.2.1: Traffic requests

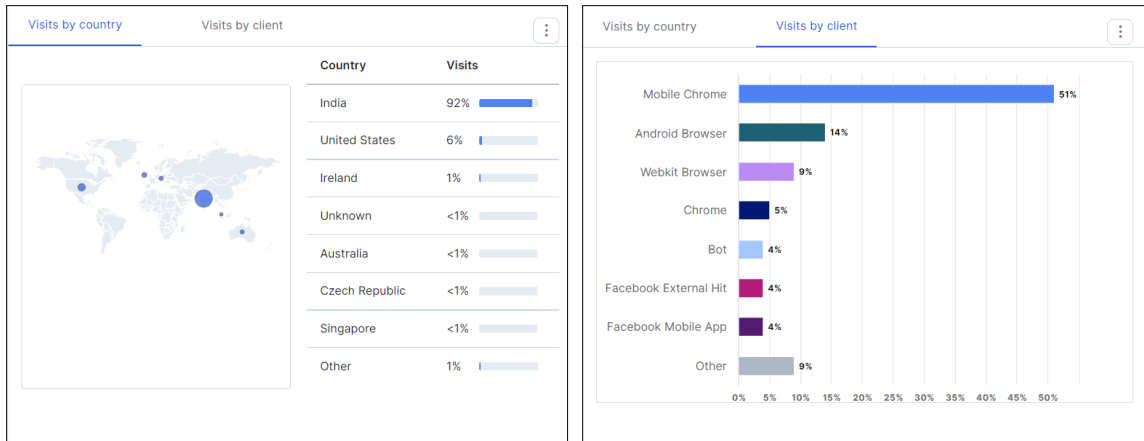


Figure 3.8: Visits by country / client browser

Security settings		
<a href="#">WAF policies</a> <a href="#">Security rules</a> <a href="#">View settings</a>		
Type	Sessions	Current setting
<a href="#">SQL Injection</a>	1	Block IP
<a href="#">Cross Site Scripting</a>	1	Block IP
<a href="#">Illegal Resource Access</a>	10	Block IP
<a href="#">Bot Access Control</a>	546	Block Request
<a href="#">DDoS</a>	0	Automatic
<a href="#">Backdoor Protection</a>	0	Protected
<a href="#">Remote File Inclusion</a>	0	Alert Only
<a href="#">API Specification Violation</a>	0	View settings in API Security

Figure 3.2.2: Incidents blocked by rules

Security settings		
WAF policies	Security rules	<a href="#">View settings</a>
Rule name	Hits	Action
Blocking Attacks (1041049)	20	Raise alert
Country Code Block (1323038)	10	Block request
Block Anonymous Proxy and T...	3	Block request
Anti Scraper Policy SBI (10410...	3	Block request
Blocking Web Attacks (1041048)	0	Block request
Privacy Policy (1688743)	0	Block IP

Figure 3.2.3: Threat hitting web application

Priority	Name (ID)	Description	Hits (Last 7 days)	Status
Security				
	Country Code Block (1578939)	If: CountryCode == BE   CountryCode == KW   CountryCode == NL   CountryCode == GB   CountryCode == RU   CountryCode == TR Then: Block Request		Enabled
	Anti Scraper Policy (1578940)	If: NumOnSession > 40 & Rate > (get-page-ip;20) & ClientType != Browser;SearchBot;SiteHelper Then: Block Request		Enabled
	Blocking Web Attacks (1578941)	If: ClientType == VulnerabilityScanner;DDoSBot;ClickBot;CommentSpamBot;SpamBot;Worm Then: Block Request		Enabled
	Blocking Attacks (1578942)	If: Attack == Yes & Attack == Yes Then: Alert		Enabled
	Blocked IP (1578944)	If: ClientIP == 74.125.212.201 & ClientIP == 74.125.212.205 & ClientIP == 74.125.212.199 & ClientIP == 74.125.212.203 & ClientIP == 74.125.212.207 & ClientIP == 74.125.212.209 Then: Block Request		Enabled
	BOB Private Access Connect (1578949)	If: URL contains "/connect/getUserDetailsStageWise" & ClientIP != 182.75.147.198 Then: Block IP		Enabled
	Website blockage (1578994)	If: ClientIP != 106.77.95.16 & ClientIP != 49.34.118.139 & ClientIP != 42.106.13.252 & ClientIP != 27.61.174.67 & ClientIP != 49.36.84.82 & ClientIP != 49.36.101.70 & ClientIP != 27.61.171.150 & ClientIP != 157.32.65.15 & ClientIP != 27.61.218.37 & ClientIP != 103.81.92.46 & ClientIP != 27.61.225.235 & ClientIP != 49.36.95.196 Then: Block IP		Disabled
	Block Anonymous Proxy and TOR (1676798)	If: IPList == 1;14;16 Then: Block Request		Enabled

Figure 3.2.4: Configured Policies

Client Type	Hacking Tool	Time	23 Feb 2022, 21:16:42	Hits	1	
Client App	python-requests	Session...	689000660038824312	HTTP	1.1	
Entry Page	git/con...	Country	Lithuania	Cookies	not supported	
Method	GET	Source IP				
User Agent	python-requests/2.27.1	Policy ID	331805			
Blocked Country		Illegal Resource Access (1)		More Details ^		
Request ID	Type	URL	Method	Action		
176116538471944334	Illegal Resource Access	https://.../...	GET	Blocked		

Figure 3.2.5: Detailed Incident Log

### 3.3 ENDPOINT DETECTION & RESPONSE (EDR)

---

Endpoint security is the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns. Endpoint security systems protect these endpoints on a network or in the cloud from cybersecurity threats. Endpoint security has evolved from traditional antivirus software to providing comprehensive protection from sophisticated malware and evolving zero-day threats.

Endpoint detection and response (EDR), also known as endpoint threat detection and response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. The term referred to emerging security systems that detect and investigate malicious activity on hosts and endpoints, with a high degree of automation to help security teams rapidly identify and react to threats.

The primary functions of an EDR security system are to:

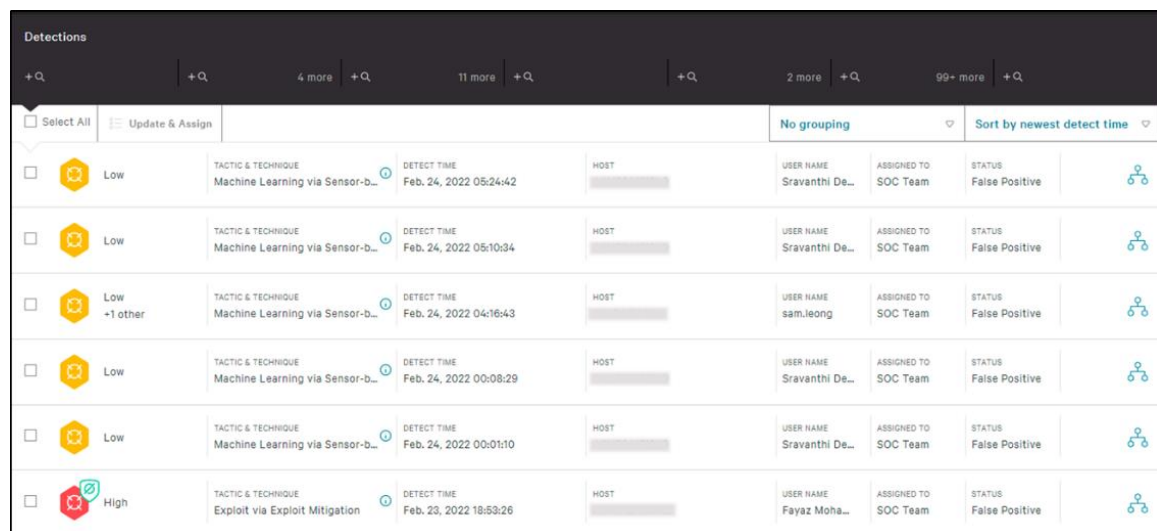
- Monitor and collect activity data from endpoints that could indicate a threat
- Analyze this data to identify threat patterns
- Automatically respond to identified threats to remove or contain them, and notify security personnel
- Forensics and analysis tools to research identified threats and search for suspicious activities



### 3.3.1 CROWDSTRIKE

CrowdStrike is a leader in cloud-delivered, next-generation services for endpoint protection, threat intelligence, and response. The CrowdStrike Falcon platform stops breaches by preventing and responding to all types of attacks—both malware and malware-free. The company has revolutionized endpoint protection by combining next-generation anti-virus technology with endpoint detection and response, coupled with a 24/7 managed hunting service, all delivered via the cloud in a single integrated solution. Falcon uses the patented CrowdStrike Threat Graph to analyze and correlate billions of events in real time, providing complete protection and five-second visibility across all endpoints <sup>[3]</sup>.

In CrowdStrike, the agent which installed on endpoint system collects all the logs and see all the activity. Whenever it finds any suspicious / malicious activity or process running it shows it in CrowdStrike Detection section as shown in below snapshot. We can collect all the information related to that system and activity from there <sup>[4]</sup>.



Detections							
+ Q. + Q. 4 more + Q. 11 more + Q. + Q. 2 more + Q. 99+ more + Q.							
<input type="checkbox"/> Select All <input type="checkbox"/> Update & Assign		No grouping		Sort by newest detect time			
<input type="checkbox"/>	Low	TACTIC & TECHNIQUE Machine Learning via Sensor-b...	DETECT TIME Feb. 24, 2022 05:24:42	HOST	USER NAME Sravanthi De...	ASSIGNED TO SOC Team	STATUS False Positive
<input type="checkbox"/>	Low	TACTIC & TECHNIQUE Machine Learning via Sensor-b...	DETECT TIME Feb. 24, 2022 05:10:34	HOST	USER NAME Sravanthi De...	ASSIGNED TO SOC Team	STATUS False Positive
<input type="checkbox"/>	Low +1 other	TACTIC & TECHNIQUE Machine Learning via Sensor-b...	DETECT TIME Feb. 24, 2022 04:16:43	HOST	USER NAME sam.leong	ASSIGNED TO SOC Team	STATUS False Positive
<input type="checkbox"/>	Low	TACTIC & TECHNIQUE Machine Learning via Sensor-b...	DETECT TIME Feb. 24, 2022 00:08:29	HOST	USER NAME Sravanthi De...	ASSIGNED TO SOC Team	STATUS False Positive
<input type="checkbox"/>	Low	TACTIC & TECHNIQUE Machine Learning via Sensor-b...	DETECT TIME Feb. 24, 2022 00:01:10	HOST	USER NAME Sravanthi De...	ASSIGNED TO SOC Team	STATUS False Positive
<input type="checkbox"/>	High	TACTIC & TECHNIQUE Exploit via Exploit Mitigation	DETECT TIME Feb. 23, 2022 18:53:26	HOST	USER NAME Fayaz Moha...	ASSIGNED TO SOC Team	STATUS False Positive

Figure 3.3.1: Detections

When the CrowdStrike finds any critical file or software running in the endpoint system it automatically quarantines that file by itself and shows it in Quarantine Files section. After the analysis of that file, we can manually delete or release that file.

Quarantined Files							
<input type="checkbox"/> Selected 0 of 61 <input type="button" value="Release"/> <input type="button" value="Delete"/> <input type="button" value="Undo Release"/>							
Date of Quarantine	File Name	Hostname	AV Detections	User	Status	Actions	
Feb. 21, 2022 19:05:27	O16Setup.exe, O16Setup.exe		41	maulesh.patel	Deleted		
Feb. 21, 2022 13:04:37	webCom.exe		0	Sushma.C	Deleted		
Feb. 15, 2022 12:49:20	Unlocker1-9-2.exe		28	raish.saiyed	Deleted		
Feb. 11, 2022 09:57:29	DeltaTB.exe		29	Fayaz Mohammed	Deleted		
Feb. 9, 2022 21:28:00	Jianying_pro_2_6_0_7223...		50	user	Deleted		
Feb. 8, 2022 19:06:15	N74-FULL-x86.exe		3	nishit.marvania	Deleted		
Feb. 7, 2022 15:28:35	ArchiSteamFarm.exe		0	Sam	Deleted		
<input type="checkbox"/> Feb. 6, 2022 22:40:45	Launcher.exe		0	Vincent.Ippolito	Released		

Figure 3.3.2: Quarantine files

While the analysis of the incident if we stuck anywhere and we want to know the exact location or working of that file we can directly connect to that host by the feature called **Connect to host** provided by CrowdStrike. Here we get the command line interface of that system so we can run any command or any scripts. Using this feature, we can directly remove malicious file even without knowledge of the user.

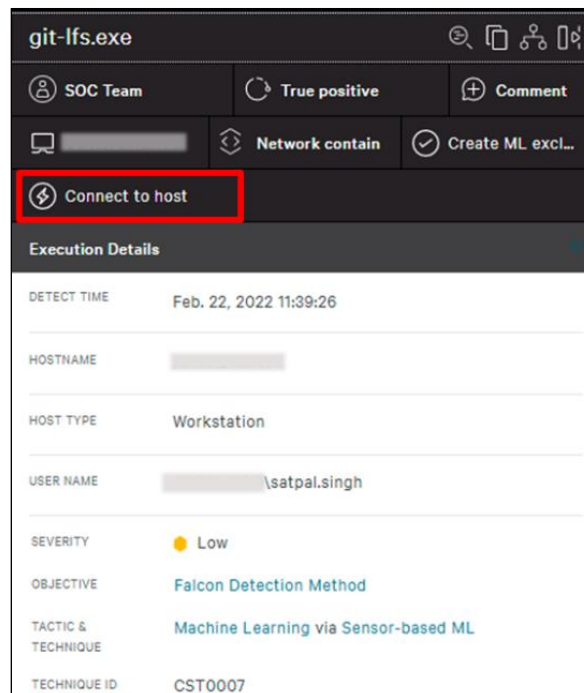


Figure 3.3.3: Connect to Host

Here we also get the feature of Kill the specific process if we do not want to connect to host. After clicking on the kill process feature immediately it will kill the suspicious process. So, by this we can stop spreading further infection in the system. And if in case we are not sure about the file being malware or not and if we want to analyze more about it there is one feature called Prepare file for download. By this feature we can download that suspicious file in safe environment and analyze it in our way.

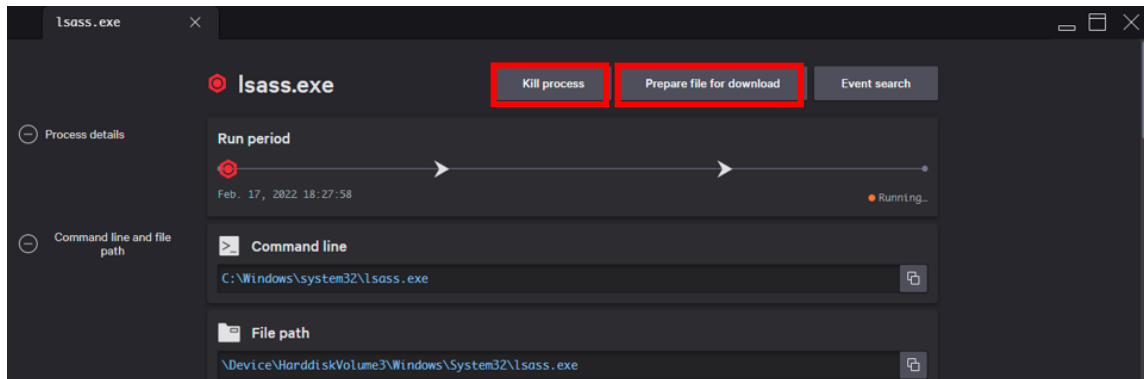


Figure 3.3.4: Feature of CrowdStrike

# **CHAPTER 4**

## **SIMULATION TOOLS**

- ❖ **BREACH & ATTACK  
SIMULATION TOOL**
- ❖ **PHISHING  
SIMULATION TOOL**

## 4.1 BREACH & ATTACK SIMULATION (BAS) TOOL

---

Threat emulators are tools or sets of scripts that emulate cyber-attacks or malicious behavior. Specifically, threat emulators can launch single procedure attacks or give one the ability to create multi-step attacks, while the resulting attacks may be known or unknown cyber-attacks. The motivations for using threat emulators are various: cutting costs of penetration testing activities by having smaller red teams, performing automated security audits in organizations, creating baseline tests for security tools in development, supplying penetration testers with another tool in their arsenal, etc.

In this project, we review various open-source threat emulators and perform qualitative and quantitative comparison between them. We focus on tactics and techniques from MITRE ATT&CK matrix, and check if they can be performed and tested with the reviewed emulators. We develop a comprehensive methodology for the evaluation and comparison of threat emulators with respect to general features such as prerequisites, attack manipulation, clean up and more.

Once the all testing done in all different environments, a team can choose the best threat emulator for their needs without checking and trying them all.

### 4.1.1 INFECTION MONKEY

The Infection Monkey is an open-source breach and attack simulation tool for testing a data center's resiliency to perimeter breaches and internal server infection. Infection Monkey will help you validate existing security solutions and will provide a view of the internal network from an attacker's perspective.

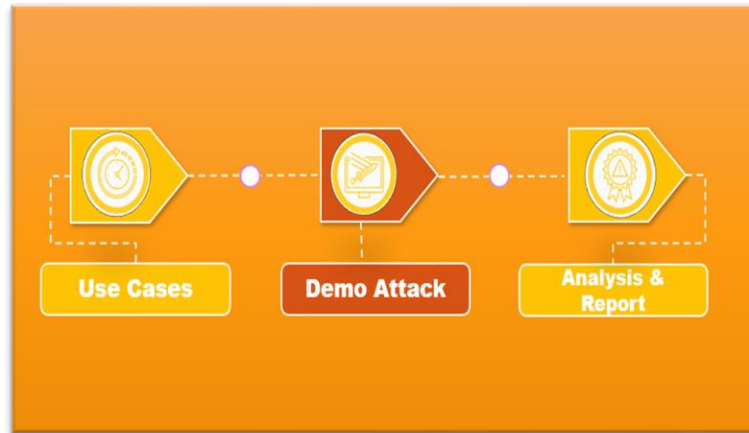


Figure 4.1.1: Flow in Infection Monkey

#### 4.1.1.1 HOW IT WORKS?

Architecturally, Infection Monkey is comprised of two components:

- i. Monkey Agent (Monkey for short) - a safe, worm-like binary program which scans, propagates and simulates attack techniques on the local network.
- ii. Monkey Island Server (Island for short) - a C&C web server which provides a GUI for users and interacts with the Monkey Agents.

The user can run the Monkey Agent on the Island server machine or distribute Monkey Agent binaries on the network manually. Based on the configuration parameters, Monkey Agents scan, propagate and simulate an attacker's behaviour on the local network. All the information gathered about the network is aggregated in the Island Server and displayed once all Monkey Agents are finished <sup>[5]</sup>.

#### 4.1.1.2 USE CASES

- i. Zero Trust assessment: See where you stand in your Zero Trust journey.
  - The Infection Monkey can automatically evaluate your readiness across the different Zero Trust Extended Framework principles. You can additionally scan your cloud infrastructure's compliance to Zero Trust principles using Scout Suite integration.
- ii. MITRE ATT&CK: assessment Assess your network security detection and prevention capabilities.
  - The Infection Monkey can simulate various ATT&CK techniques on the network. Use it to assess your security solutions' detection and prevention capabilities. The Infection Monkey will help you find which ATT&CK techniques go unnoticed and provide specific details along with suggested mitigations.
  - Network Breach: Simulate an internal network breach and assess the potential impact.
  - Infection Monkey will help you assess the impact of a future breach by attempting to propagate within your internal network using service vulnerabilities, brute-forcing and other safe exploiters.
- iii. Network Segmentation: Verify your network is properly segmented.
  - Segmentation is a method of creating secure zones in data centres and cloud deployments. It allows organizations to isolate workloads from one another and secure them individually, typically using policies. Segmentation is key to protecting your network. It can reduce the network's attack surface and minimize the damage caused during a breach.
  - You can use the Infection Monkey's cross-segment traffic feature to verify that your network segmentation configuration is adequate. This way, you can ensure that, even if a bad actor breaches your defenses, they cannot move laterally between segments.

- iv. Credentials Leak Assess the impact of a successful phishing attack, insider threat, or other form of credential's leak.
- Numerous attack techniques (from phishing to dumpster diving) might result in a credential leak. The Infection Monkey can help you assess the impact of stolen credentials by automatically searching where bad actors can reuse these credentials in your network.

#### 4.1.1.3 CONFIGURATION

**Infection Monkey**

1. Run Monkey Island Server ✓  
 2. Run Monkey ✓  
 3. Infection Map ✓  
 4. Security Reports ✓  
 Start Over

**Configuration**

Log

Powered by  
 Guardicore  
 License

Infection Monkey Version: 3.10.0

### Credentials

#### Exploit password list

List of password to use on exploits using credentials

Password1!	↑	↓	×
1234	↑	↓	×
password	↑	↓	×
12345678	↑	↓	×
+			

#### Exploit user list

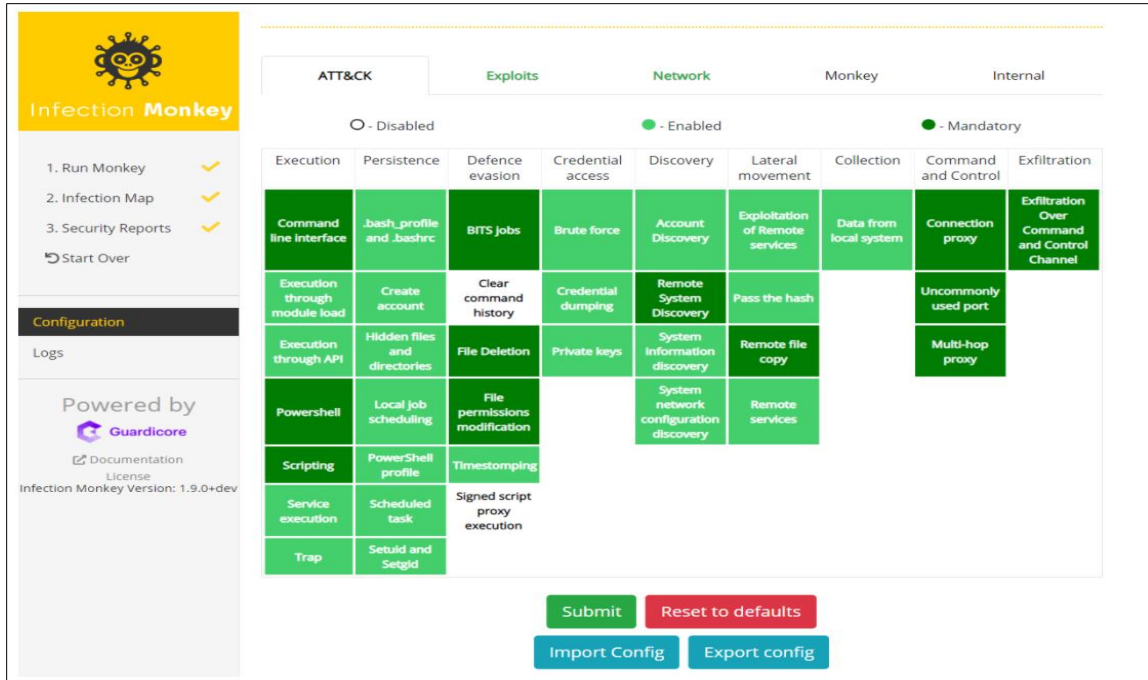
List of usernames to use on exploits using credentials

Administrator	↑	↓	×
root	↑	↓	×
user	↑	↓	×
+			

Submit Reset to defaults  
 Import Config Export config

Figure 4.1.2: Credentials Leak





**Infection Monkey**

- Run Monkey ✓
- Infection Map ✓
- Security Reports ✓
- Start Over

**Configuration**

Logs

Powered by **Guardicore**

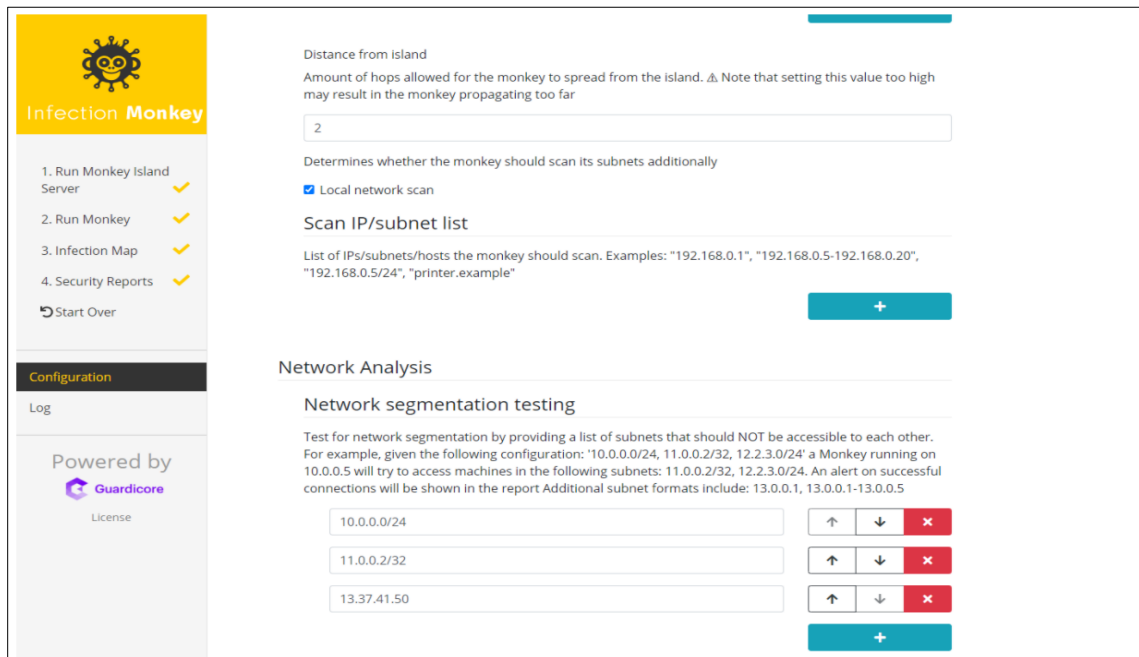
Documentation License  
Infection Monkey Version: 1.9.0+dev

ATT&CK			Exploits	Network	Monkey	Internal		
○ - Disabled			● - Enabled			● - Mandatory		
Execution	Persistence	Defence evasion	Credential access	Discovery	Lateral movement	Collection	Command and Control	Exfiltration
Command line interface	.bash_profile and .bashrc	BITS jobs	Brute force	Account Discovery	Exploitation of Remote services	Data from local system	Connection proxy	Exfiltration Over Command and Control Channel
Execution through module load	Create account	Clear command history	Credential dumping	Remote System Discovery	Pass the hash		Uncommonly used port	
Execution through API	Hidden files and directories	File Deletion	Private keys	System Information discovery	Remote file copy		Multi-hop proxy	
Powershell	Local job scheduling	File permissions modification		System network configuration discovery	Remote services			
Scripting	PowerShell profile	Timestomping						
Service execution	Scheduled task	Signed script proxy execution						
Trap	Setuid and Setgid							

Submit Reset to defaults

Import Config Export config

Figure 4.1.3: MITRE ATT&amp;CK Assessment



**Infection Monkey**

- Run Monkey Island Server ✓
- Run Monkey ✓
- Infection Map ✓
- Security Reports ✓
- Start Over

**Configuration**

Log

Powered by **Guardicore**

License

Distance from Island  
Amount of hops allowed for the monkey to spread from the island. ⚠ Note that setting this value too high may result in the monkey propagating too far

2

Determines whether the monkey should scan its subnets additionally

☒ Local network scan

Scan IP/subnet list

List of IPs/subnets/hosts the monkey should scan. Examples: "192.168.0.1", "192.168.0.5-192.168.0.20", "192.168.0.5/24", "printer.example"

+

**Network Analysis**

**Network segmentation testing**

Test for network segmentation by providing a list of subnets that should NOT be accessible to each other. For example, given the following configuration: '10.0.0.0/24, 11.0.0.2/32, 12.2.3.0/24' a Monkey running on 10.0.0.5 will try to access machines in the following subnets: 11.0.0.2/32, 12.2.3.0/24. An alert on successful connections will be shown in the report Additional subnet formats include: 13.0.0.1, 13.0.0.1-13.0.0.5

10.0.0.0/24

11.0.0.2/32

13.37.41.50

↑ ↓ ×

↑ ↓ ×

↑ ↓ ×

+

Figure 4.1.4: Network Breach

- Check infection map and security report to see how far monkey managed to propagate in the network and which vulnerabilities it used in doing so. If you left post breach actions selected, you should also check ATT&CK and Zero Trust reports.

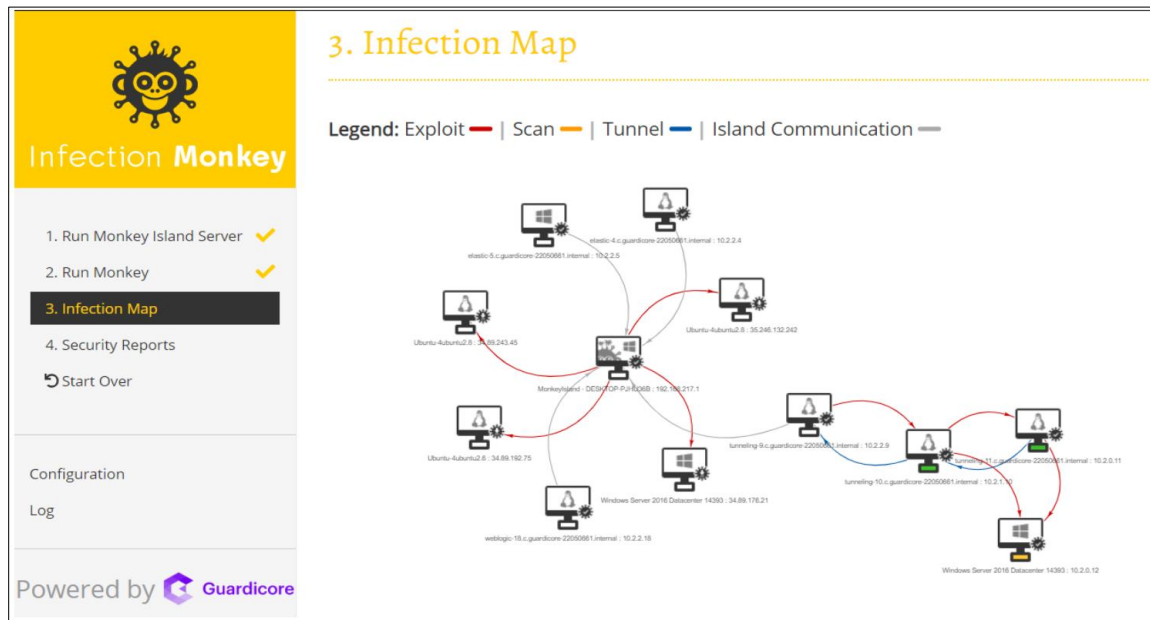


Figure 4.1.5: Network Breach Map

#### 4.1.1.4 ANALYSIS & REPORT

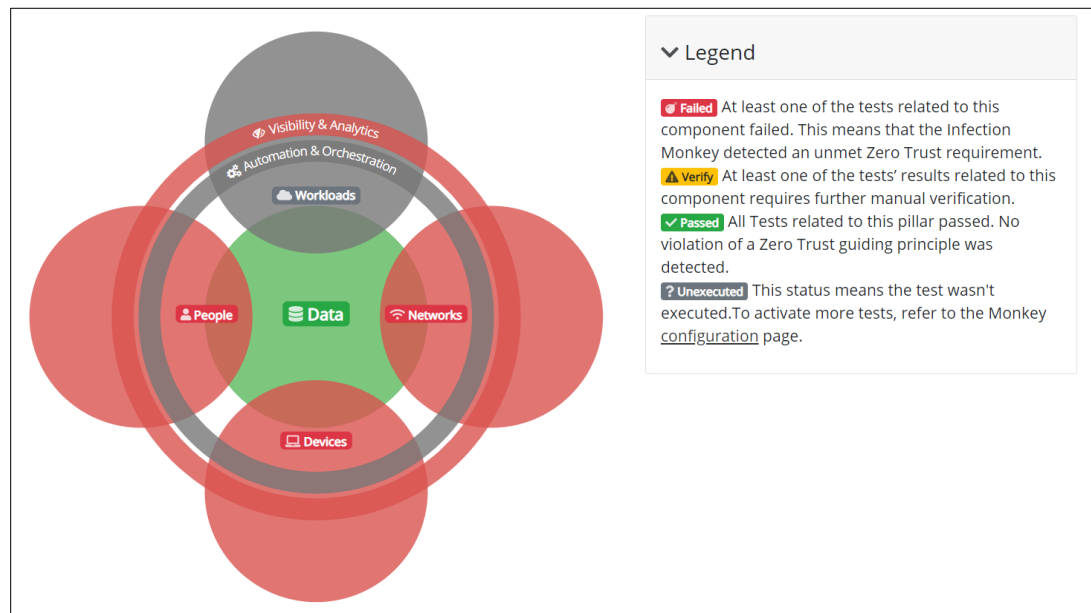


Figure 4.1.6: Zero Trust Report

Failed tests' findings		
Finding	Events	Pillars
Monkey didn't find ANY active endpoint security processes. Install and activate anti-virus software on endpoints.	Events 0	Devices
Monkey caused a new user to access the network. Your network policies are too permissive - restrict them to MAC only.	Events 9+	People Networks Visibility & Analytics
Verify tests' findings		
Finding	Events	Pillars
Monkey performed malicious actions in the network. Check SOC logs and alerts.	Events 9+	Networks Visibility & Analytics
Passed tests' findings		
Finding	Events	Pillars
Monkey didn't find open HTTP servers. If you have such servers, look for alerts that indicate attempts to access them.	Events 9+	Data
Monkey didn't find open Elasticsearch instances. If you have such instances, look for alerts that indicate attempts to access them.	Events 9+	Data
Monkey didn't manage to exploit an endpoint.	Events 9+	Devices
Monkey wasn't able to cause a new user to access the network.	Events 4	People Networks Visibility & Analytics
Monkey found active endpoint security processes. Check their logs to see if Monkey was a security concern.	Events 4	Devices

Figure 4.1.7: Test Findings

This report shows information about **Mitre ATT&CK™** techniques used by Infection Monkey.

● - Disabled     
 ● - Not attempted     
 ● - Tried (but failed)     
 ● - Successfully used

Execution	Persistence	Defence evasion	Credential access	Discovery	Lateral movement	Collection	Command and Control	Exfiltration
Command line interface	.bash_profile and .bashrc	BITS jobs	Brute force	Remote System Discovery	Exploitation of Remote services	Data from local system	Connection proxy	Exfiltration Over Command and Control Channel
Execution through module load	Create account	File Deletion	Credential dumping	System information discovery	Pass the hash		Uncommonly used port	
Execution through API	Hidden files and directories	File permissions modification	Private keys	System network configuration discovery	Remote file copy		Multi-hop proxy	
Powershell	Local job scheduling				Remote services			
Scripting	PowerShell profile							
Service execution	Scheduled task							
Trap	Setuid and Setgid							

Figure 4.1.8: Attack Result

## 4.2 PHISHING SIMULATION TOOL

---

Cybercriminals use phishing, the fraudulent attempt to obtain sensitive information such as credit card details and login credentials, by disguising as a trustworthy organization or reputable person in an email communication. Phishing emails are also used to distribute malware and spyware through links or attachments that can steal information and perform other malicious tasks.

Phishing simulation guards your business against social-engineering threats by training your employees to identify and report them. Phishing is popular with cybercriminals because it enables them to steal financial and personal information by exploiting human behavior.

Due to the fact that just one mistake by one employee clicking on one link could result in fraud, a data breach, huge costs, and damage the company's reputation, user security awareness is now widespread; employers are educating workers about the latest attack techniques and testing them with phishing simulations to help protect their businesses against cybercrimes.

Anti-phishing and security training solutions show employees the different types of attacks, how to recognize the subtle clues and report suspicious emails to your IT department.

Phishing simulation helps employees recognize, avoid, and report potential threats that can compromise critical business data and systems, including phishing, malware, [ransomware](#), and spyware. As a part of user security awareness, phishing simulation training provides employees with the information they need to understand the dangers of social engineering, detect potential attacks, and take the appropriate actions to protect your business with security best practices.

## 4.2.1 GOPHISH

GoPhish is a powerful, open-source phishing framework that makes it easy to test your organization's exposure to phishing.

GoPhish is a phishing framework that makes the simulation of real-world phishing attacks dead simple. The idea behind GoPhish is simple – make industry-grade phishing training available to everyone <sup>[6][7]</sup>.

“Available” in this case means two things:

- i. Affordable – GoPhish is open-source software that is completely free for anyone to use.
- ii. Accessible – GoPhish is written in the Go programming language. This has the benefit that GoPhish releases are compiled binaries with no dependencies. In a nutshell, this makes installation as simple as "download and run"!

### 4.2.1.1 CONFIGURATION

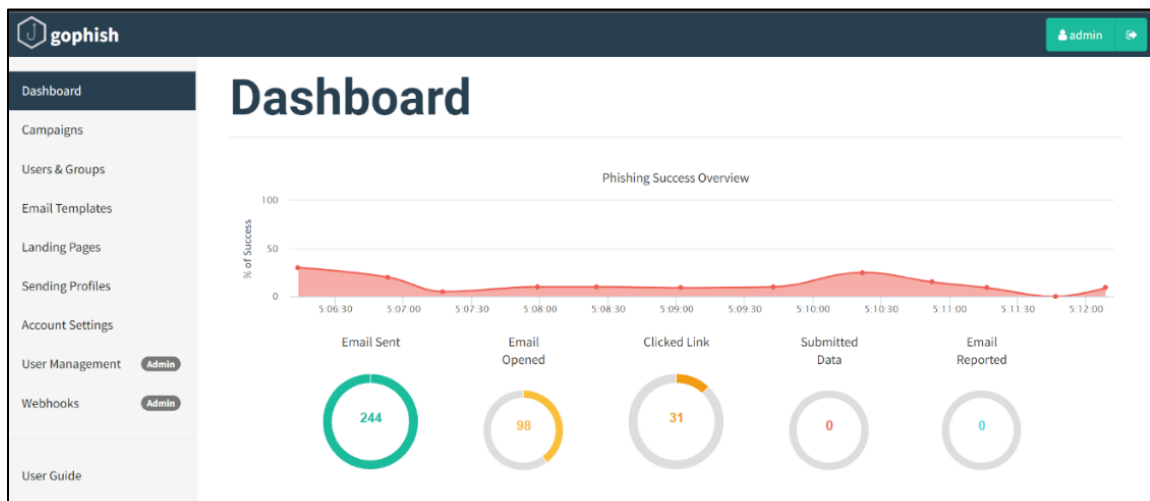


Figure 4.2.1: Dashboard

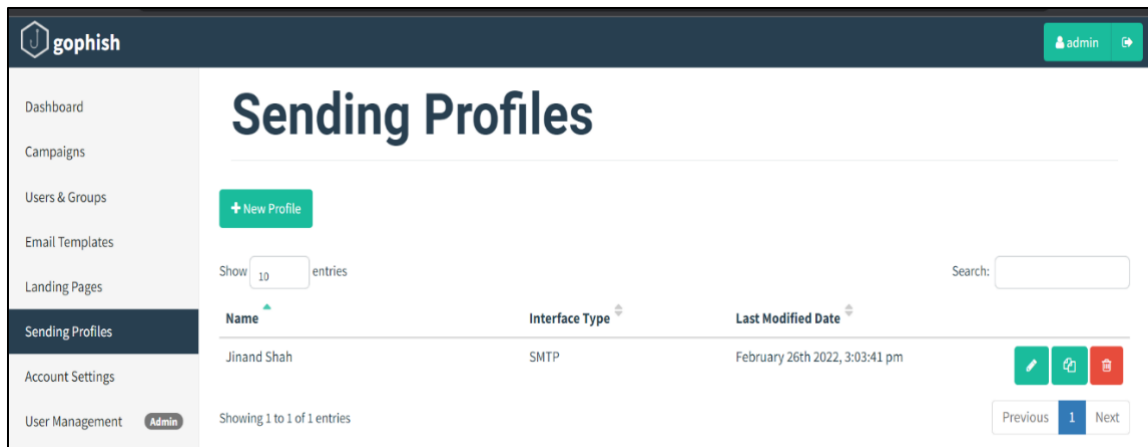


Figure 4.2.2: Sending Profiles

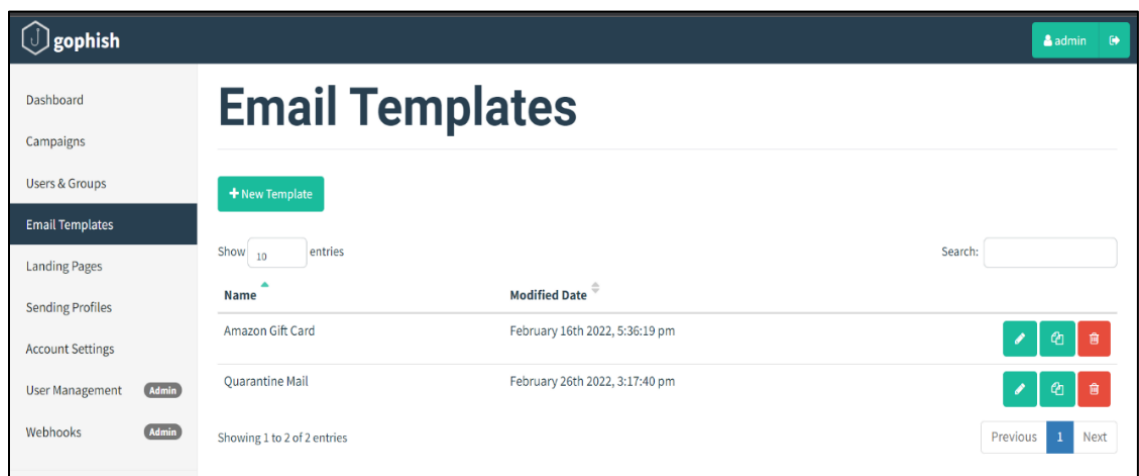


Figure 4.2.3: Email Templates

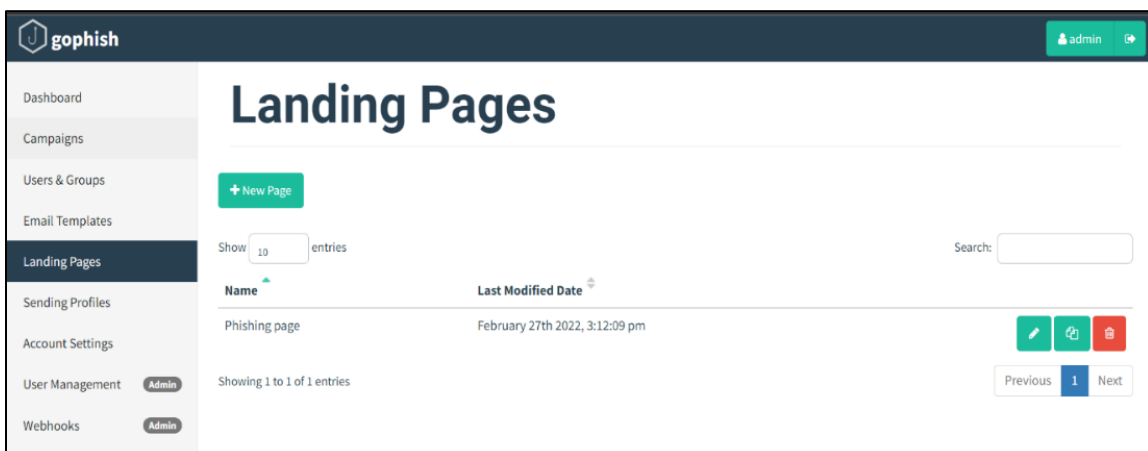


Figure 4.2.4: Landing Pages

### 4.2.1.2 RESULTS

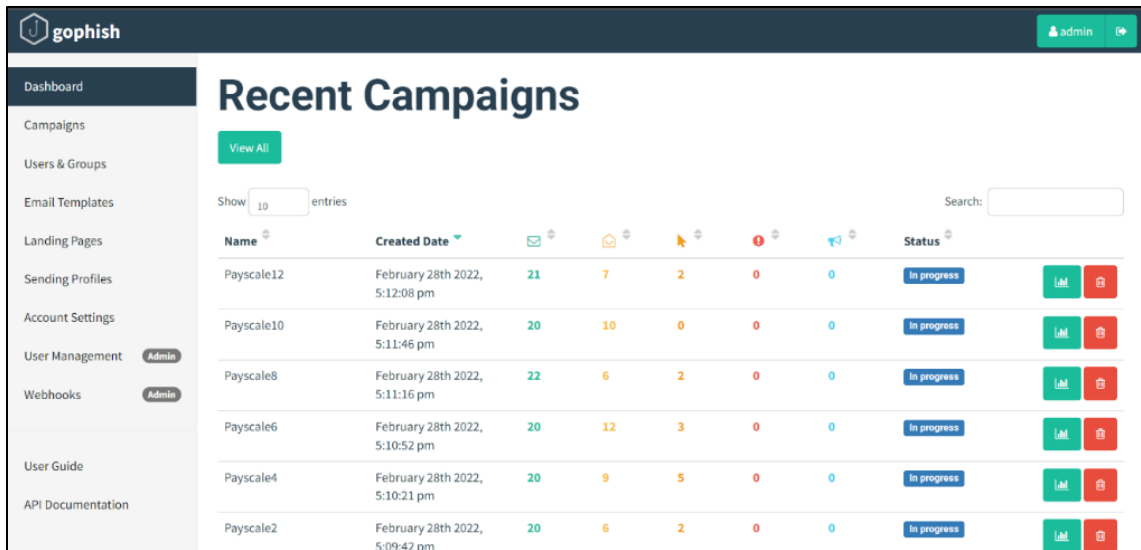


Figure 4.2.5: Recent Phishing Campaigns

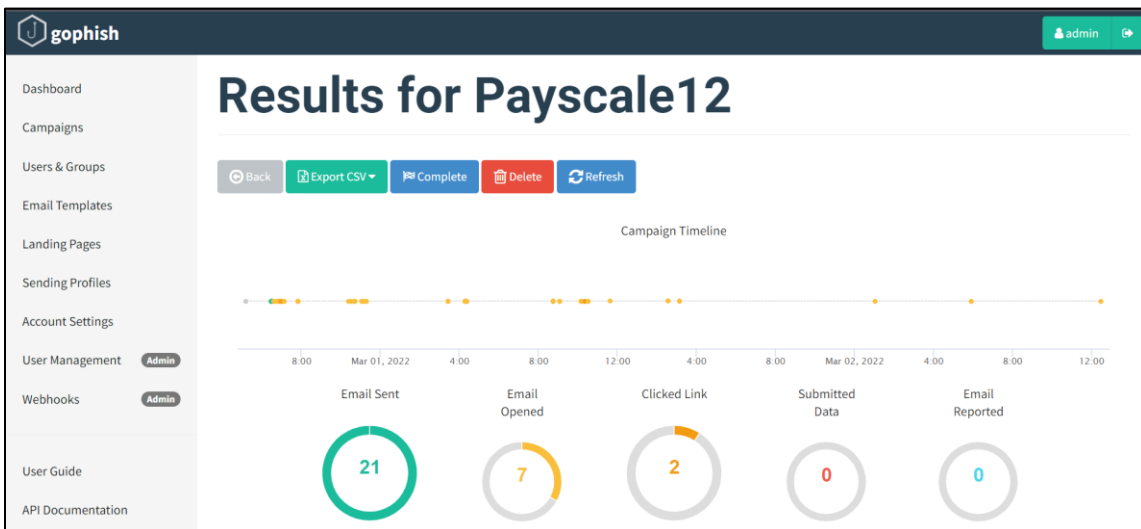


Figure 4.2.6: Results of one campaign

The screenshot displays the Gophish web interface. On the left is a sidebar menu with options: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management (with an 'Admin' button), Webhooks (with an 'Admin' button), User Guide, and API Documentation. The main content area is titled 'Details' and shows a table of users. The first user listed is Kalash Shah, with email kalash.shah@onlinepsbloans.com and status 'Email Opened'. Below the table is a 'Timeline for Kalash Shah' section, which includes the email and result ID, followed by a vertical timeline of events: Campaign Created (Feb 28th 2022 5:10:52 pm), Email Sent (Feb 28th 2022 6:15:08 pm), and five Email Opened events (March 1st 2022 9:57:39 am, March 1st 2022 10:08:40 am, March 1st 2022 1:35:11 pm, March 2nd 2022 8:52:40 am, and March 3rd 2022 8:11:06 am).

First Name	Last Name	Email	Position	Status	Reported
Kalash	Shah	kalash.shah@onlinepsbloans.com		Email Opened	

**Timeline for Kalash Shah**  
 Email: kalash.shah@onlinepsbloans.com  
 Result ID: mGDtrvSA

- Campaign Created February 28th 2022 5:10:52 pm
- Email Sent February 28th 2022 6:15:08 pm
- Email Opened March 1st 2022 9:57:39 am
- Email Opened March 1st 2022 10:08:40 am
- Email Opened March 1st 2022 1:35:11 pm
- Email Opened March 2nd 2022 8:52:40 am
- Email Opened March 3rd 2022 8:11:06 am

Figure 4.2.7: Details of one user



\

# **CHAPTER 5**

# **ENDPOINT SECURITY**

❖ **EMAIL SECURITY**

❖ **CLOUD SECURITY**

## **5.1 EMAIL SECURITY**

---

Email security is the term for any procedure that protects email content and accounts against unauthorized access. Email service providers have email security measures in place to secure client accounts and information from hackers.

Email is popular with hackers as a tool for spreading malware, spam, and phishing attacks. They use deceptive messages to trick recipients into sharing sensitive information, resulting in identity theft. They lure people into opening attachments or clicking hyperlinks that install malware (such as email viruses) on the user's device. Email is also a main entry point for attackers looking to access an enterprise network and breach valuable company data.

### 5.1.1 MICROSOFT 365 DEFENDER

Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

With the integrated Microsoft 365 Defender solution, security professionals can stitch together the threat signals that each of these products receive and determine the full scope and impact of the threat; how it entered the environment, what it's affected, and how it's currently impacting the organization. Microsoft 365 Defender takes automatic action to prevent or stop the attack and self-heal affected mailboxes, endpoints, and user identities [8].

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools. Defender for Office 365 includes:

- Threat protection policies: Define threat-protection policies to set the appropriate level of protection for your organization.
- Reports: View real-time reports to monitor Defender for Office 365 performance in your organization.
- Threat investigation and response capabilities: Use leading-edge tools to investigate, understand, simulate, and prevent threats.
- Automated investigation and response capabilities: Save time and effort investigating and mitigating threats.

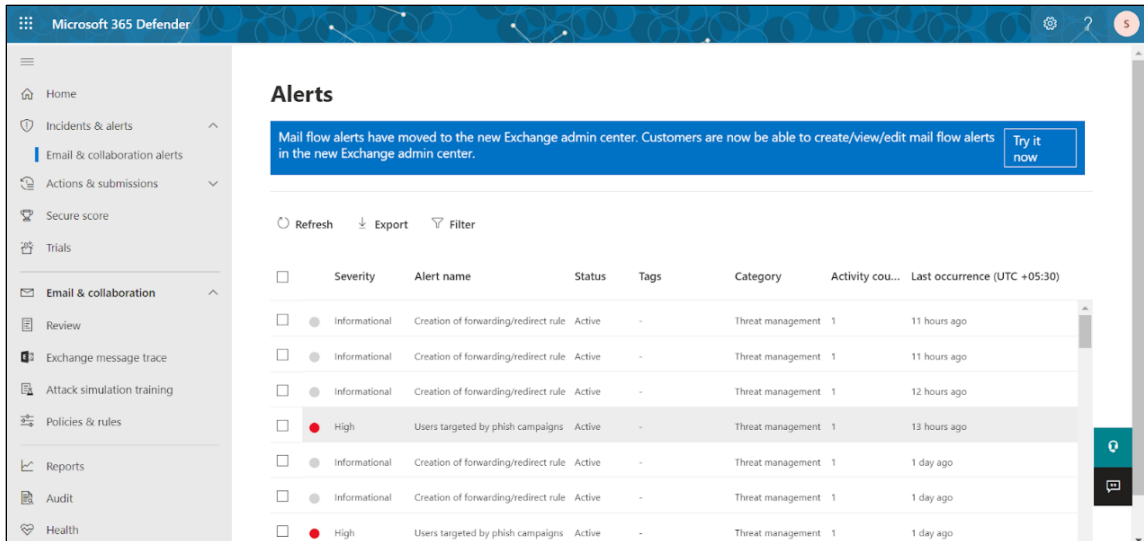


Figure 5.1.1: Email alerts

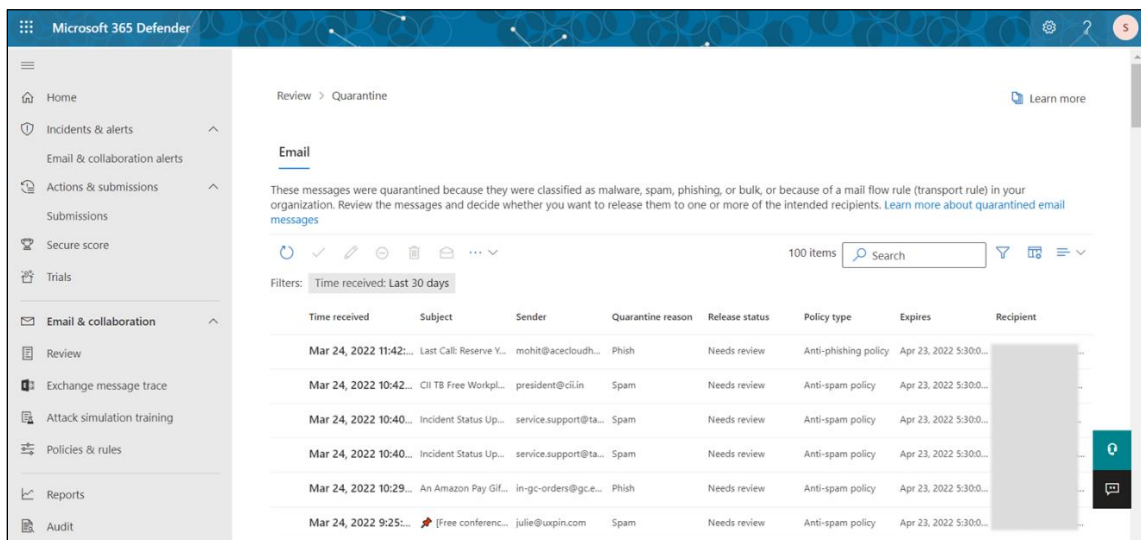


Figure 5.1.2: Quarantined mails

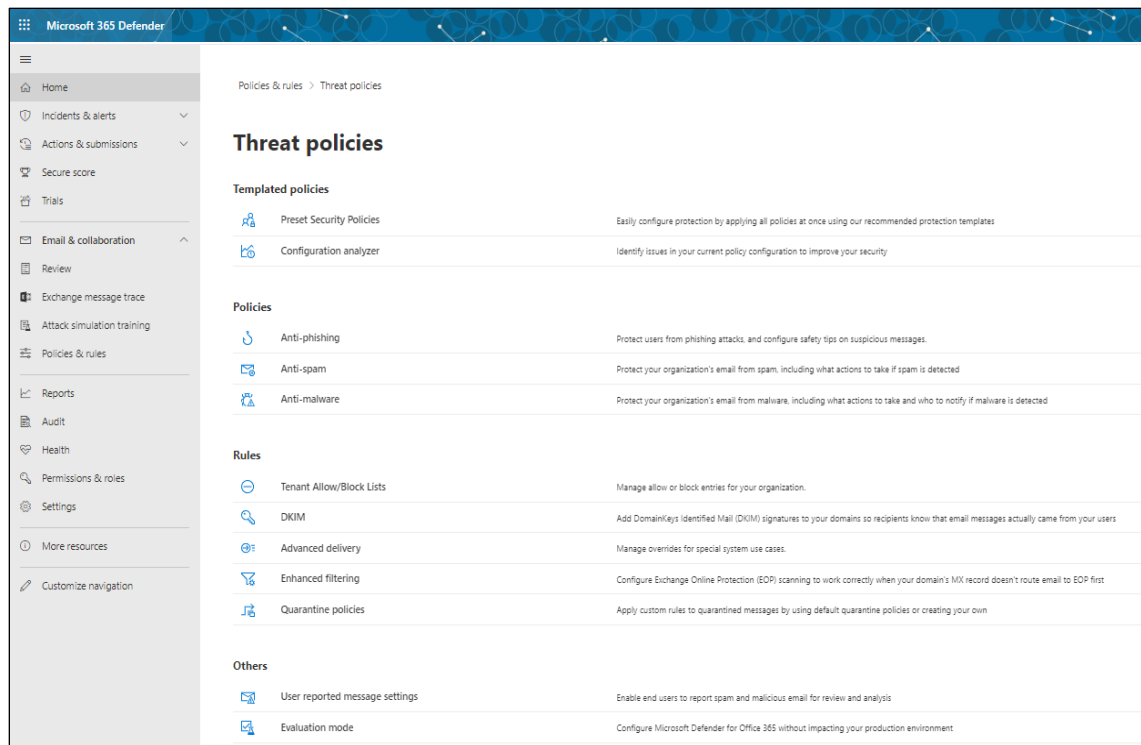


Figure 5.1.3: Policies configured

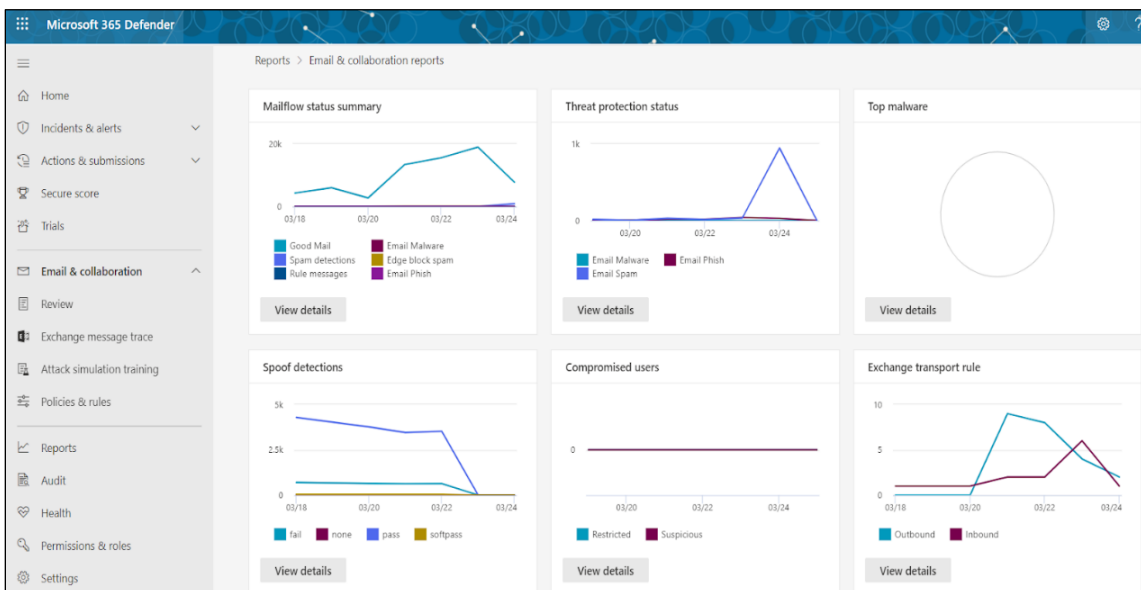


Figure 5.1.4: Statistics report

## **5.2 CLOUD SECURITY**

---

Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security.

Cloud security is a set of control-based safeguards and technology protection designed to protect resources stored online from leakage, theft, or data loss.

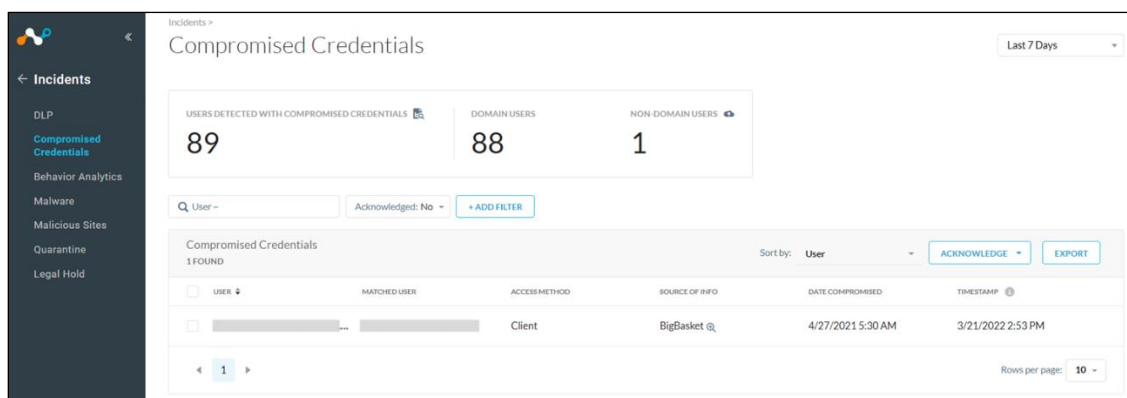
Protection encompasses cloud infrastructure, applications, and data from threats. Security applications operate as software in the cloud using a Software as a Service (SaaS) model.

## 5.2.1 NETSKOPE

Netskope Security Cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device.

The rapid adoption of cloud apps, services, and mobile devices has resulted in data going to places where traditional security technology is blind. Netskope takes a data-centric approach to cloud security, following data everywhere it goes. From data created and exposed in the cloud to data going to unmanaged cloud apps and personal devices, Netskope protects data and users everywhere<sup>[9]</sup>.

Cloud usage dominates the web, with cloud services making up the majority of enterprise web traffic. Securing this environment, without slowing down the business, demands a new security model based on contextual knowledge of the cloud. Netskope enables you to take advantage of intimate, contextual understanding of the cloud to apply effective security controls that enable you to safely use the cloud and web.



The screenshot displays the 'Compromised Credentials' section in the Netskope Security Cloud interface. The left sidebar shows navigation options: Incidents, DLP, Compromised Credentials (selected), Behavior Analytics, Malware, Malicious Sites, Quarantine, and Legal Hold. The main content area shows a summary of compromised credentials: 89 users detected with compromised credentials, 88 domain users, and 1 non-domain user. Below this, there is a search bar for 'User' and a filter for 'Acknowledged: No'. A table lists the compromised credentials, with one entry found. The table columns are: USER, MATCHED USER, ACCESS METHOD, SOURCE OF INFO, DATE COMPROMISED, and TIMESTAMP. The entry shows a user with a masked name, accessed via 'Client' from 'BigBasket @', on 4/27/2021 5:30 AM, with a timestamp of 3/21/2022 2:53 PM. The interface also includes a 'Sort by: User' dropdown, 'ACKNOWLEDGE', and 'EXPORT' buttons. The bottom right corner shows 'Rows per page: 10'.

USER	MATCHED USER	ACCESS METHOD	SOURCE OF INFO	DATE COMPROMISED	TIMESTAMP
[REDACTED]	[REDACTED]	Client	BigBasket @	4/27/2021 5:30 AM	3/21/2022 2:53 PM

Figure 5.2.1: Compromised Credentials

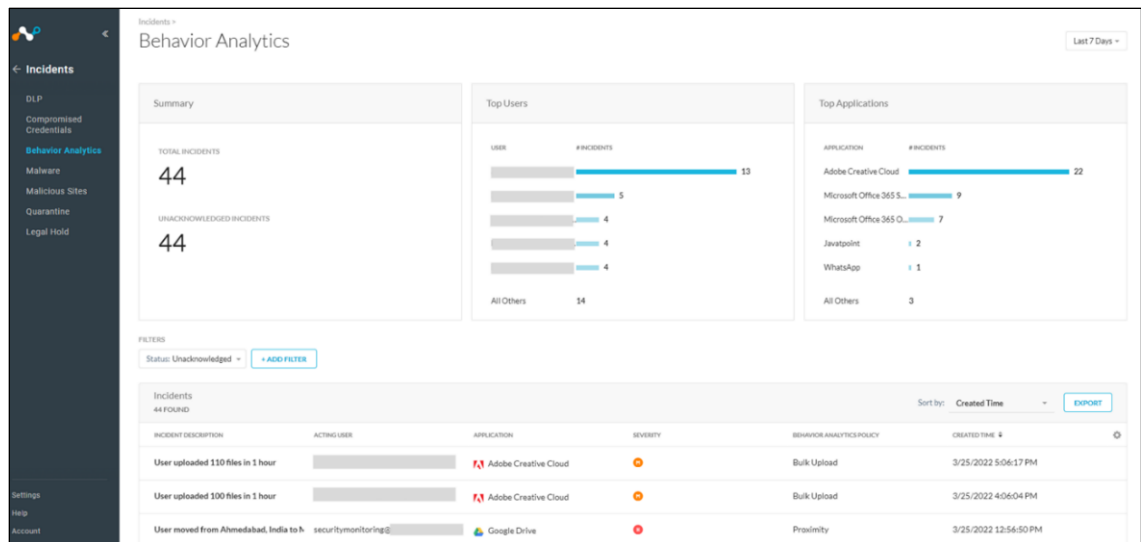


Figure 5.2.2: Behavior analytics

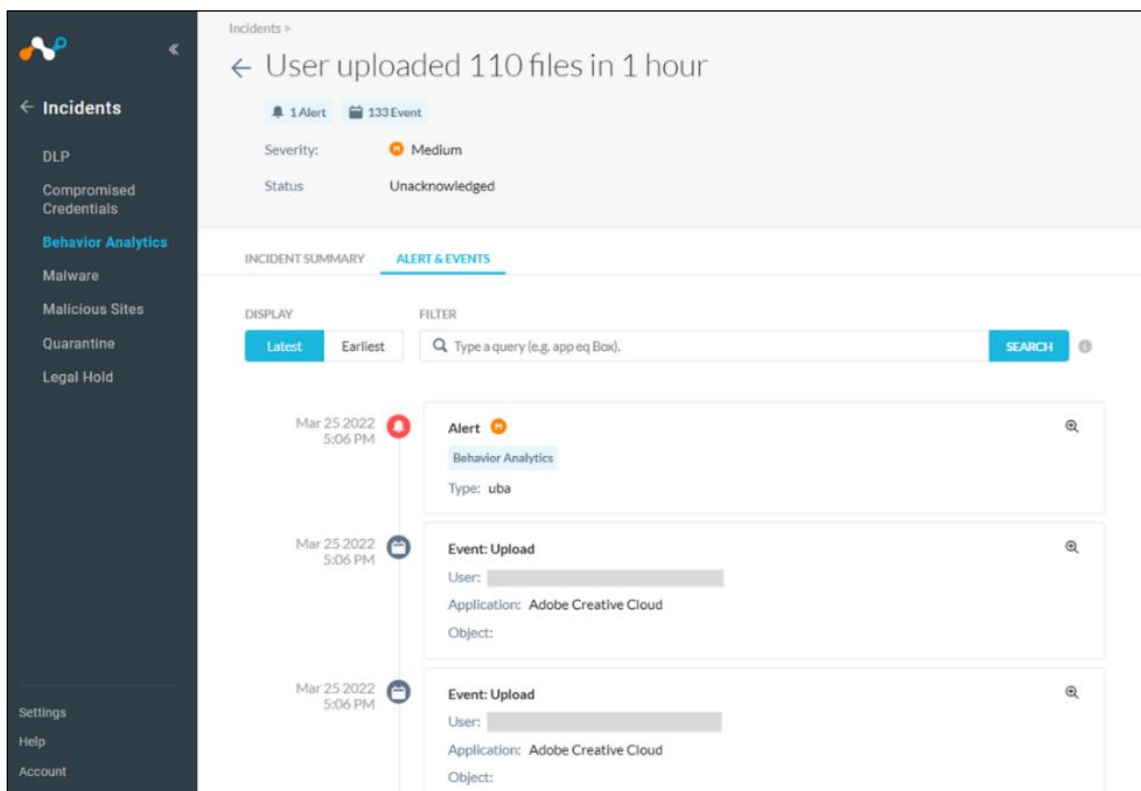


Figure 5.2.3: Incident details



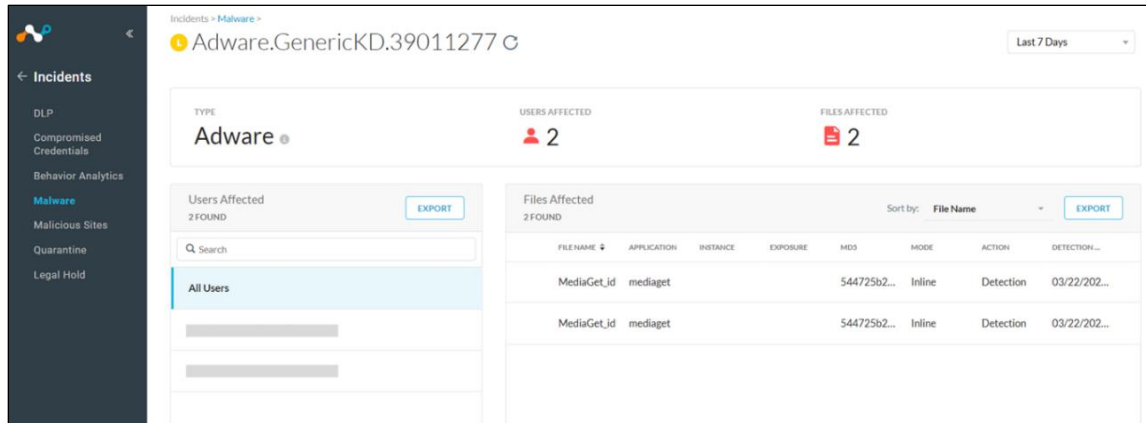


Figure 5.2.4: Users affected by malware

# **CHAPTER 6**

# **CONCLUSION**

- ❖ **CONCLUSION**
- ❖ **PROBLEMS FACED**
- ❖ **REFERENCES**

## 6.1 CONCLUSION

---

The project is very helpful for the beginners in the field of Cyber Security. By this project, one can understand the whole working flow of security in an organization. Also, the use of different tools can automate so many manual processes and make it easy and effortless for the security personnel. And by using simulation tools, we can assess our environment security by our own.

The importance of this project is to secure the organization environment from a hacker. By implementing the proper technology and software we can stop the attacker from entering our network and stealing our sensitive data. SIEM tool is helpful for constant monitoring, other simulation tools are useful for assessing the security of an organization and increase user awareness for the possible incoming attacks. I have successfully implemented and tested all the tools and got the client-side experience by working on client-side projects.

## 6.2 PROBLEM ENCOUNTERED AND POSSIBLE SOLUTIONS

---

*Problem:* I have faced many issues while installing Wazuh agent in the system as it did not reflect to the Wazuh server.

*Solution:* I had to do everything from the start by proper IP configuration.

*Problem:* While the testing of Infection Monkey is going on, I couldn't test it on the system in the other network, as the public IP is not assigned on AWS server.

*Solution:* I had done the tunneling and assigned the public IP to AWS instance so that I can access it from the outside of network.

## 6.3 REFERENCES

---

1. <https://documentation.wazuh.com/current/index.html>
2. <https://docs.imperva.com/>
3. <https://www.crowdstrike.com/blog/tech-center/>
4. <https://www.crowdstrike.com/resources/case-studies/>
5. <https://www.guardicore.com/infectionmonkey/>
6. <https://docs.getgophish.com/user-guide/getting-started>
7. <https://www.techrepublic.com/article/how-to-run-a-phishing-attack-simulation-with-gophish/>
8. <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/?view=o365-worldwide>
9. <https://docs.netskope.com/>