



# TECHNICAL GUIDE AND USER MANUAL

## MODULES

An Overview of Cytomate Technical Modules

# 1. CONTENTS

Modules .....	6
I. WEB SECURITY .....	6
1. Technical Details of Web Security .....	6
1.1. The Importance of Web Security: Statistics Speak .....	6
1.2. The Harmful Effects of Web Security Gaps .....	6
1.3. Introducing Cytomate Web Security - The Solution to Web Security Challenges .....	6
1.4. Benefits of Cytomate Web Security .....	7
2. User Manual of Web Security .....	7
Scope of Manual .....	7
Definitions .....	7
2.1. Web reconnaissance .....	7
2.2. Web assessment .....	8
2.3. Web Mitigations .....	8
3. Cytomate Web Security Solution .....	8
3.1. Overview .....	9
3.2. Web Recon .....	11
3.2.1. Domain Verification .....	11
3.2.2. Automated Web Recon .....	13
3.2.3. Manual Web Recon .....	13
3.3. Web Assessment .....	14
3.3.1. Scheduling Assessment .....	16
3.4. Web Reports .....	17
3.4.1. Column Detail .....	18
3.4.2. View Report .....	18
3.5. Web Report Summary .....	19
3.5.1. Summary .....	19
3.5.2. CVEs .....	21
3.5.3. Misconfigurations .....	22
3.5.4. Sensitive Information .....	23
3.5.5. Exposed Panel .....	24
3.5.6. Web Mitigations .....	25
3.6. Scheduled Assessment .....	26
II. WAF SECURITY .....	27
1. Technical Details of WAF Security .....	27
1.1. The Importance of WAF: Statistics Speak .....	27



1.2.	Introducing Cytomate WAF Security: The Solution to Web Security Challenges .....	27
1.3.	Benefits of Cytomate WAF Security .....	29
2.	User Manual of WAF Security.....	29
	Scope of the Manual .....	29
	Definitions .....	29
2.1.	Web Application Firewall (WAF).....	29
2.2.	WAF Assessment .....	29
2.3.	WAF Mitigations.....	30
3.	Advanced WAF Assessment.....	30
3.1.	Hardware and Software Requirements .....	30
3.1.1.	Domain Verification .....	30
3.2.	Cytomate WAF Security Solution .....	30
3.2.1.	Overview.....	31
3.2.2.	Assessment.....	33
3.2.3.	Reports .....	38
3.2.3.4.4.1.	Columns Details.....	46
3.2.4.	Schedule Assessment (WAF).....	47
III.	EMAIL GATEWAY .....	48
1.	Technical Detail of Email Gateway.....	48
1.1.	The Importance of Email Gateway .....	48
1.2.	Introducing Cytomate Email Gateway: The Solution to Email Gateway Challenges .....	48
1.3.	Benefits of Email Gateway.....	49
2.	User Manual of Email Gateway .....	50
	Scope of the Manual .....	50
	Definitions .....	50
2.1.	Email gateway (Security) .....	50
2.2.	Cytomate Agent .....	50
2.3.	Mitigation .....	50
3.	Cytomate Email Gateway Assessment.....	50
4.	Hardware and Software Requirements .....	51
4.1.	Cytomate Agent installation.....	51
4.2.	Domain Verification.....	51
4.3.	Features and Functionalities .....	51
5.	Cytomate Breach+ Email Gateway Security Solution.....	51
5.1.	Overview .....	53
5.2.	Assessment.....	54
5.2.1.	Domain verification .....	54





5.2.2.	Email Gateway Security Testing Setup.....	56
5.2.3.	Steps to Start an Assessment .....	57
5.2.4.	Steps to Start (Schedule) an Assessment.....	59
5.3.	Reports .....	62
5.3.1.	Columns Details .....	63
5.3.2.	Viewing the Assessment Report .....	63
5.3.3.	Behavior (Payload) report.....	64
5.3.4.	Mitigations.....	66
5.4.	Scheduled Assessments .....	66
IV.	ENDPOINT SECURITY .....	67
1.	Technical Detail of Endpoint Security .....	67
1.1.	The Importance of Endpoint Security.....	67
1.2.	Introducing Breach+ Endpoint Security: The Solution to Endpoint Security Challenges	68
1.3.	Benefits of Breach+ Endpoint Security .....	69
2.	User Manual of Endpoint Security .....	70
	Scope of the Manual .....	70
	Definitions .....	70
2.1.	Endpoint (Security).....	70
2.2.	Cytomate Agent .....	70
2.3.	Cytomate Breach+ .....	70
3.	Endpoint Security Assessment.....	70
3.1.	Breach+ Endpoint Security Assessment .....	71
3.2.	Breach+ Endpoint Security Assessment & MITRE ATT&CK Tactics.....	71
4.	Hardware and Software Requirements .....	72
4.1.	Breach+ Agent .....	72
5.	Features and Functionalities.....	72
5.1.	Breach+ Endpoint Security Solution .....	72
5.1.1.	Assessments .....	78
5.1.2.	Reports .....	82
5.2.	Breach+ Campaign Security Assessment .....	92
5.2.1.	Campaign Overview.....	92
5.2.2.	Campaign Assessments .....	93
5.2.3.	Campaign Reports .....	95
5.3.	Breach+ ATT&CK Maps .....	100
V.	NETWORK SECURITY.....	102
1.	Technical Detail of Network Security.....	102





1.1.	Performance Evaluation of Security Controls.....	103
1.2.	Use of Packet Capture (PCAP) Replay.....	103
1.3.	Real-World Malware Traffic Simulation .....	103
1.4.	Comprehensive Testing of Inline Security .....	103
1.5.	Detection and Prevention Analysis.....	103
1.6.	Mitigation Recommendations and Prescriptive Guidance .....	103
1.7.	Provision of IoCs and Vendor-Specific Mitigations.....	103
VI.	INTEGRATIONS .....	104
VII.	TEMPLATES.....	106
VIII.	ANALYTICS .....	112

## Modules

### I. WEB SECURITY

#### 1. Technical Details of Web Security

In today's digital age, web security has become crucial for organizations. With the increasing reliance on the internet and web-based applications, the threat landscape has become more complex, and cybercriminals are becoming more sophisticated. Web security involves protecting an organization's web infrastructure from attacks, vulnerabilities, and other threats that can cause damage to its reputation, financial loss, and legal liabilities.

##### 1.1. The Importance of Web Security: Statistics Speak

According to a report by Positive Technologies, web applications accounted for 17% of all cyber-attacks in 2020 <sup>[1]</sup>. Similarly, a report by Imperva indicates that web application attacks particularly DoS attacks increased by 82% on the application layer <sup>[2]</sup>. These statistics highlight the importance of web security for organizations.

##### 1.2. The Harmful Effects of Web Security Gaps

A web security gap can lead to various harmful effects, including data breaches, loss of sensitive information, financial loss, and legal liabilities. Data breaches can be catastrophic for organizations, leading to reputation loss, customer trust, and legal penalties. In addition, web security gaps can allow cybercriminals to gain unauthorized access to an organization's web infrastructure, leading to the installation of malware, ransomware, and other harmful software.

##### 1.3. Introducing Cytomate Web Security - The Solution to Web Security Challenges

Cytomate's assessment tool assigns different security levels ranging from low to critical to assess the security status of these websites. By leveraging an expansive database of Common Vulnerabilities and Exposures (CVEs), misconfigurations, vulnerabilities, directory traversals, arbitrary file reads, sensitive information, DOM\_XSS, network, subdomain takeover, exposed panels, and miscellaneous risks, Cytomate empowers users to proactively test their web domains for potential vulnerabilities. With its comprehensive approach to web security assessments, Cytomate is a valuable tool for organizations seeking to protect themselves from the ever-increasing risk of web-based attacks.



## Web Assessment

## Web Recon

Cytomate Detects abnormalities like some of these are:

- i. **CVEs:** (Common Vulnerabilities and Exposures) are publicly disclosed security vulnerabilities found in software, hardware, or firmware.
- ii. **Misconfigurations:** refer to errors or oversights in the configuration of software, systems, or applications that can lead to security vulnerabilities.
- iii. **Subdomain takeovers:** occurs when an attacker gains control of a subdomain that is no longer in use or is misconfigured, allowing them to host malicious content or launch attacks.
- iv. **Exposed panels:** refer to administrative interfaces or control panels that are accessible over the internet and not properly secured, allowing unauthorized access to data.
- v. **Sensitive information:** refers to data that, if disclosed or compromised, could result in significant harm to individuals or organizations.

#### 1.4. Benefits of Cytomate Web Security

- i. Provides a detailed breakdown of the severity counts of attacks discovered.
- ii. Provides actionable mitigations against discovered vulnerabilities and threats.
- iii. Discovers leaked sensitive information about the company and guides how to protect it.
- iv. Performs a detailed assessment of an organization's web security posture.

Web security is critical for organizations in today's digital age, and Cytomate Web Security provides an effective solution to web security challenges. With its powerful features and ability to detect and report on web-based threats, vulnerabilities, and abnormalities, it is a must-have for any organization that wants to protect its web infrastructure.

## 2. User Manual of Web Security

### Scope of Manual

This section aims to explain the functionality of Cytomate Breach+ Web Security, and its ability to protect web application assets by identifying vulnerabilities. Furthermore, we will delineate the essential hardware and software prerequisites that must be fulfilled for the proper utilization of Cytomate Breach+ Web Security on your computer.

### Definitions

#### 2.1. Web reconnaissance

In Cytomate, Web Recon performs the passive enumeration and discovery of sub-domains

from diverse sources, followed by the detection of installed solutions and services along with their respective versions in each subdomain. This analysis helps us to narrow down or shortlist the use cases for web assessment. Additionally, we perform both active and passive discovery of endpoints to further evaluate and identify potential vulnerabilities and possible attacks.

## 2.2. Web assessment

Comprehensive test cases are triggered against the targeted web domains, with both immediate and scheduled assessments available to ensure continuous monitoring and mitigation of security risks. Our platform is designed to evaluate all test cases and assessments in a sophisticated, and controlled manner, ensuring complete security throughout the process. Web assessment will be executed to expose these most occurring security loopholes like misconfigurations, OWASP Top10 vulnerabilities, subdomain takeovers, exposed panels, and default logins.

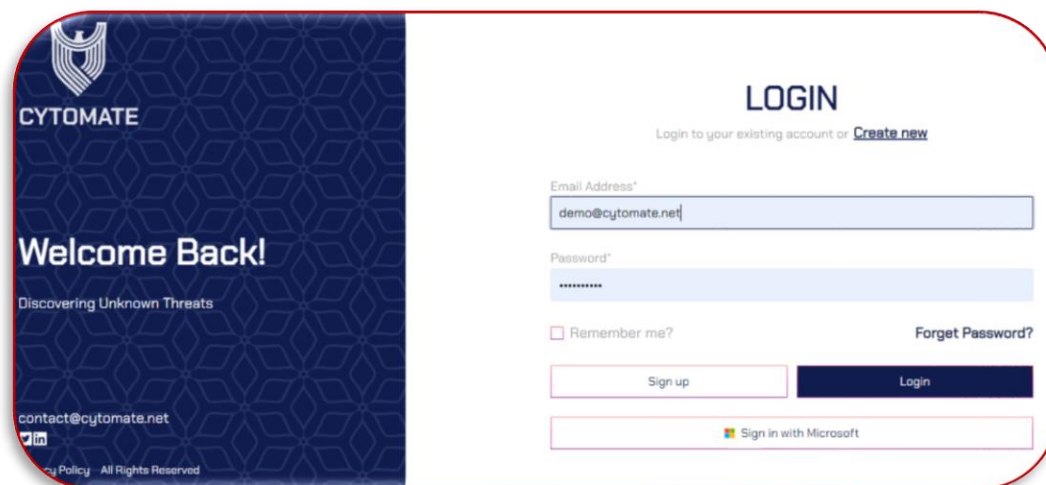
## 2.3. Web Mitigations

Cytomate Breach+ recommends implementing suitable mitigation measures for web security, such as updating web security protocols and adding supplementary security controls to enhance its resilience against threats.

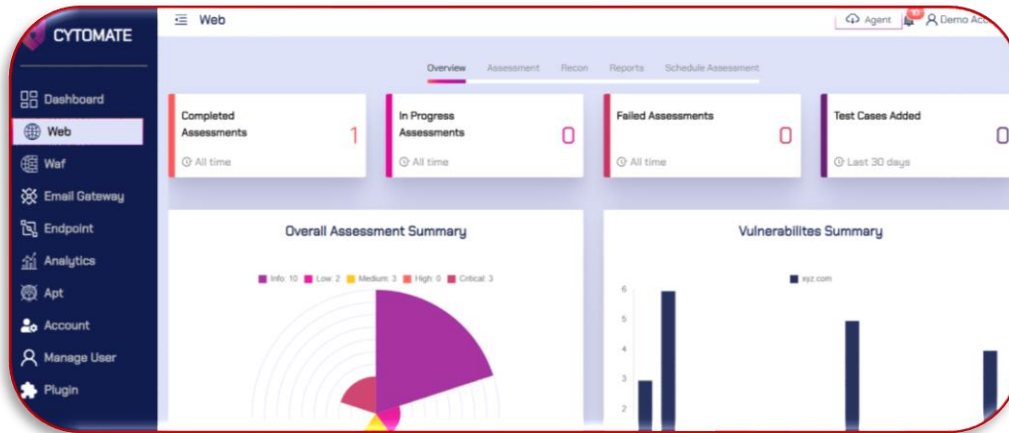
## 3. Cytomate Web Security Solution

To start a web assessment on a web domain, follow these steps:

1. Please access the Cytomate Breach+ portal by visiting <https://apt.cytomate.net/> and using the Google Chrome web browser for optimal performance.
2. Afterward, input your login credentials and proceed to click the "Login" button to gain access to the Cytomate Breach+ dashboard. Thank you.

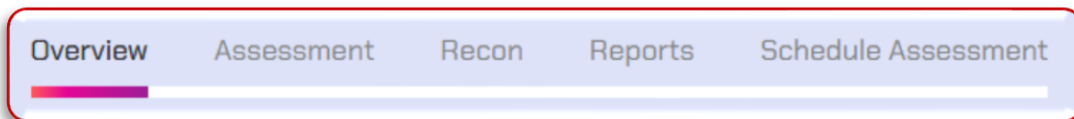


3. To access the dedicated dashboard for Web Security Assessments, please navigate to the side menu and click on the **"Web"** option. This will direct you to the appropriate dashboard.



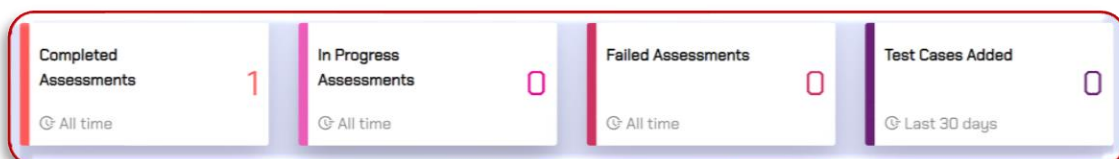
### 3.1. Overview

1. There are five distinct tabs located at the top of the dashboard, each presenting exclusive functionalities and features.
2. The current tab in use is labeled **"Overview"** which showcases a graphical representation of web assessment details through the utilization of widgets and graphs.



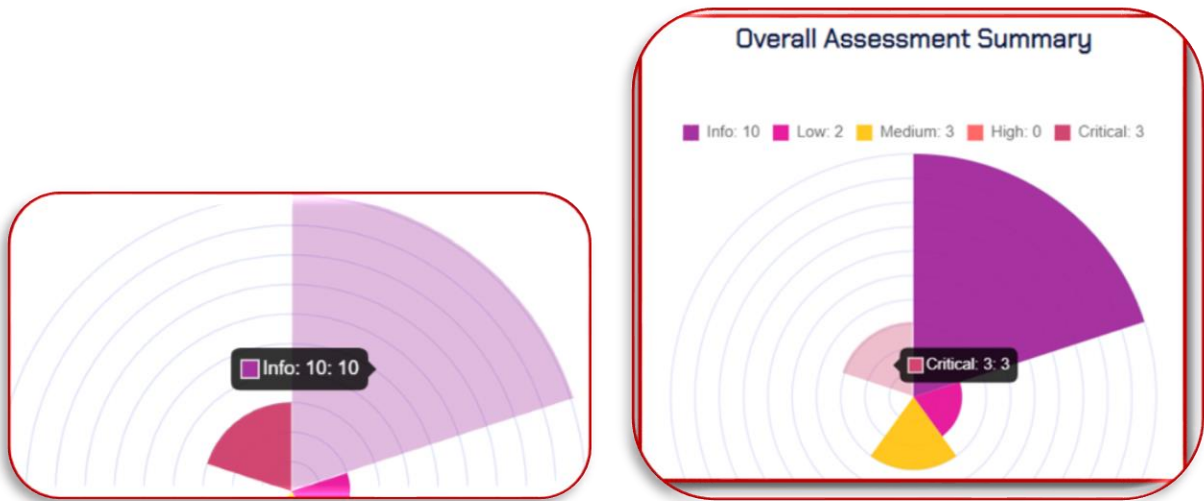
Within the **"Overview"** tab, there exist four primary widgets that present an expedited view of web assessment details. These widgets consist of the following:

- i. **Completed Assessments:** This widget displays information regarding the total number of assessments that have been completed by the user since the account's creation.
- ii. **In Progress Assessments:** This widget presents the total number of assessments that are currently in progress by the user since the account's inception.
- iii. **Failed Assessments:** This widget provides information concerning the total number of assessments that have failed since the account's creation.
- iv. **Test Cases Added:** This widget highlights the total number of test cases that have been added by Cytomate for user utilization in assessments.



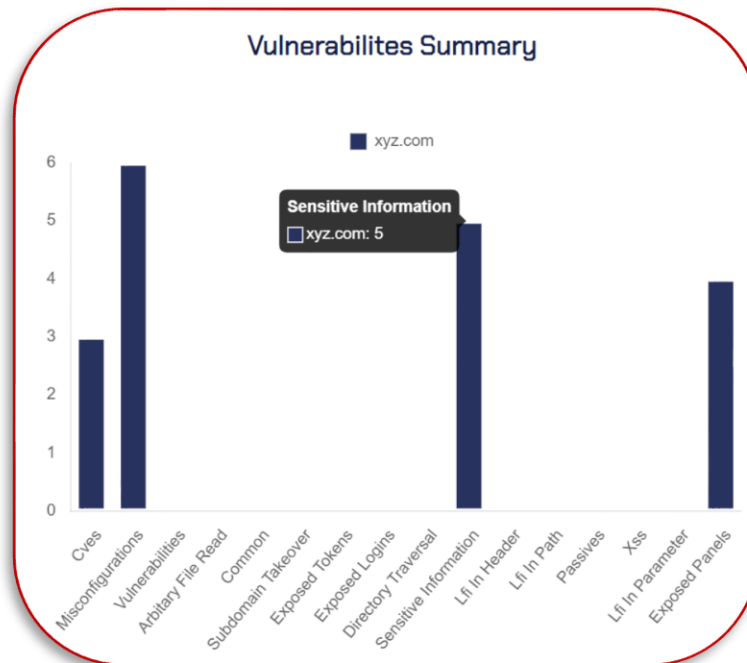
**Overall Assessment Summary:** This graph featured in the Web dashboard presents a comprehensive visualization of the overall security measurements identified through web assessments.

- The chart provides an in-depth analysis of all vulnerabilities with their relevant security measures from informative to critical.
- By hovering the cursor over the shaded area, you can see the category and details against each assessment.



**Vulnerabilities Summary graph:** This chart provides an elaborate breakdown of various vulnerabilities, which are categorized as "CVEs, misconfigurations, arbitrary file read, common, subdomain takeover, exposed tokens, exposed logins, directory traversal, sensitive information, LFI in the header, LFI in the path, DOM XSS, and exposed panels".

- Moreover, hovering the cursor over the chart bars enables the viewer to observe the total number of vulnerabilities found in the relevant category against the provided web domain for an assessment.



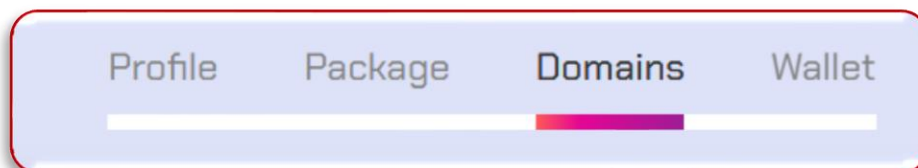
## 3.2. Web Recon

Before starting the Web Recon, the user needs to ensure the verification of the web domain by using these steps– domain verification, automated and manual recon process.

### 3.2.1. Domain Verification

It is necessary to first verify the domain before starting a recon or assessment on a targeted domain. The verification method involves triggering the recon process through the verification of the web domain.

- To start a domain verification, verify the web domain by clicking the **"Accounts"** option from the side panel and selecting **"Domains"**.



- A domain will appear in the table below with the **"Verified"** column set to "false".



Search	Q	Refresh	+ Add	Delete
Domain	Verified	Key	Action	
xyz.com	true	hTEYkN7S	Verify	

< 1 > 6 / page

- iii. Subsequently, add the web domain of your organization for verification by clicking the "Add" button.

Add Domain

cytomate.net

Add Domain

- iv. To verify the domain, copy the key from the "Key" column and paste it into the domain's DNS as a TXT record.
- v. Once your domain registrar publishes your verification code (which may take the time up to 72 hours to propagate worldwide, although it typically takes a few hours), click on the "Verify" button to check if the TXT record exists.
- vi. If the record is found, the "Verified" column will be set to "true" and we'll know you are the owner of your domain.

Verified

false

true



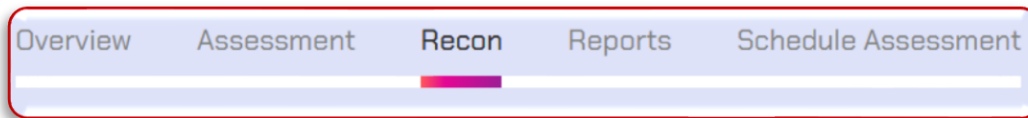
### 3.2.2. Automated Web Recon

When the domain verification process will complete then the automated Recon will start.

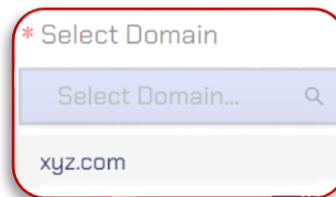
### 3.2.3. Manual Web Recon

Initiating the Web recon process involves the following steps:

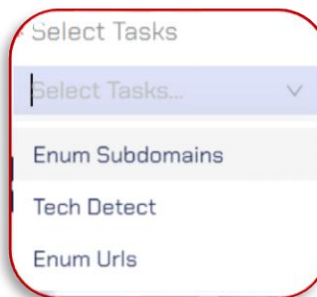
1. Navigate to the **"Web"** option located in the navigation bar.
2. To start the manual Web Recon, navigate to the **"Web"** option in the navbar, then select the **"Recon"** option within the **"Dashboard"** section.



3. Select the web domain (verified) to start the Recon service against it.



4. Furthermore, in the next selection you have options to select the Recon options in a singular manner or through a selection of multiple tasks simultaneously on a specific web domain, as per your requirement.



In the aforementioned tasks, each task has its functionalities and relevant features:

- i. **Subdomain Enumeration:** To execute a subdomain enumeration on a web domain, select the **"Enum Subdomain"** option from the dropdown list located against the targeted web domain, followed by clicking the **"Start Assessment"** button.

\* Select Tasks

Select Tasks...

Enum Subdomains

- ii. **Technology detection:** To identify web technology utilized by a specific web domain, select the **"Tech Detect"** option from the dropdown list located against the web domain and click the **"Start Assessment"** button.

Tech Detect

- iii. **URLs Enumeration:** To enumerate web domain URLs associated with your web domain, choose the **"Enum Urls"** option and click the **"Start Assessment"** button.

Enum Urls

5. You can choose test cases altogether and click on the **"Start Recon"** button to start the Recon against the targeted web domain.

Perform Web Recon

\* Select Domain

xyz.com

\* Select Tasks

Enum Subdomains x

Start Recon

6. Wait for the pop-up notification that indicates the assessment has been started successfully.

Successfully created recon history

### 3.3. Web Assessment

Web assessment services offer organizations the chance to assess the security of their Web domain against the latest web-based threats. This evaluation encompasses the testing of

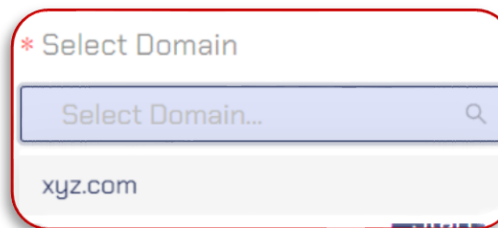
potential vulnerabilities related to CVEs, misconfigurations, exposed panels, sensitive information leakage, DOM XSS, subdomain takeover, exposed logins, and exposed tokens. By utilizing these assessment services, organizations can effectively identify potential security vulnerabilities within their Web domain and take necessary actions to enhance their overall security posture through mitigations.

**Note:** The Web Recon process should always be performed on the targeted web domain before starting the web assessment. It is important to ensure that the Web Recon process is completed before commencing the web assessment.

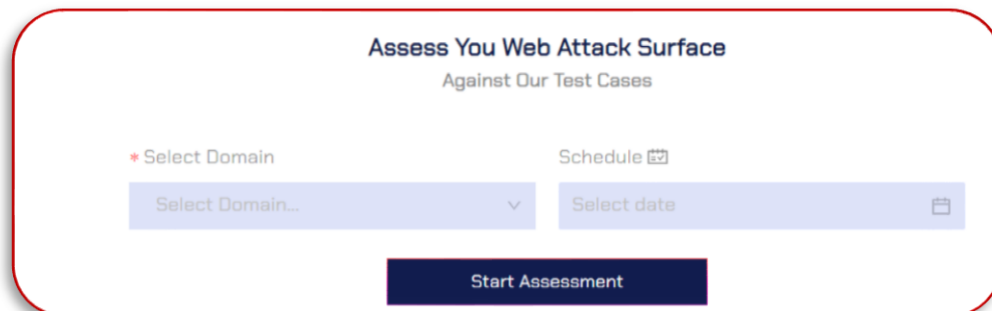
1. To start the assessment, first navigate to the **"Assessment"** tab in the dashboard menu within the Web Module.



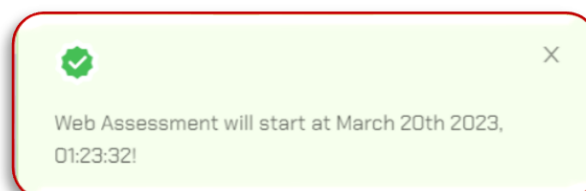
2. To start a web assessment, you need to select the **(verified) web domain** through the aforementioned steps in Recon via the **"Select Domain"** option.



3. Then to start the Assessment, just click the **"Start Assessment"** button.

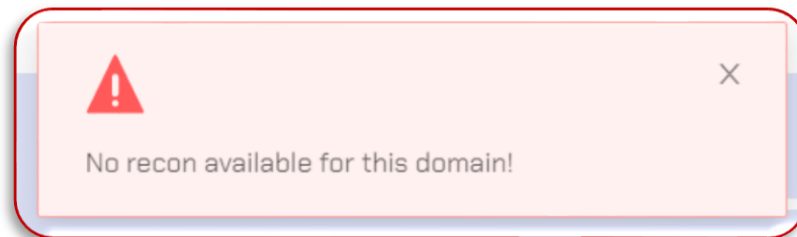


4. After starting the assessment, wait for the pop-up notification that indicates that the assessment has been started.



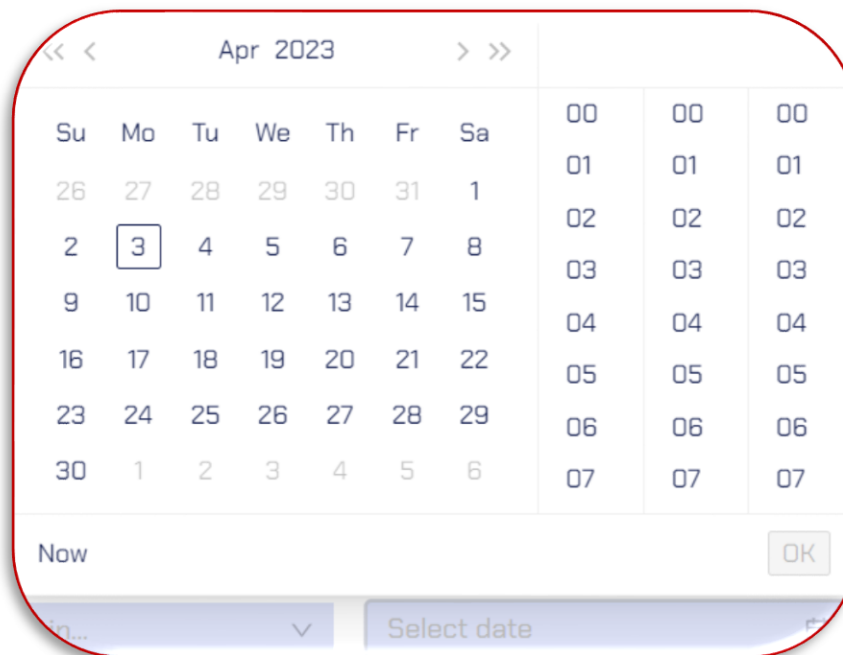
**Error Response:** If a web assessment is executed without adhering to the essential procedures of web reconnaissance and web domain verification, an **"Error message"** will be displayed.

**Note:** It is imperative to ensure the completion of web recon before assessment by ensuring the web domain verification before initiating the web recon process.

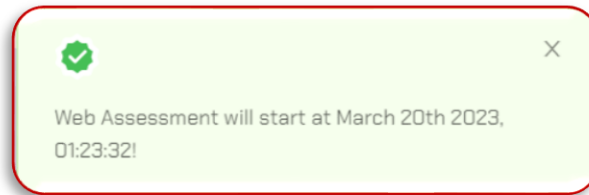


### 3.3.1. Scheduling Assessment

1. To schedule an assessment for later, follow the above mentioned steps as well as select the entire date and time from the given calendar, and time chart and hit the **"Start Assessment"** button.

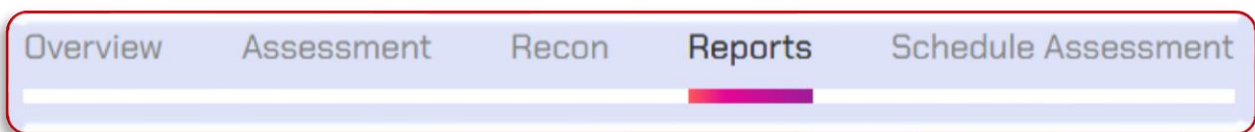


2. Wait for the pop-up notification indicating the successful schedule of the web assessment.

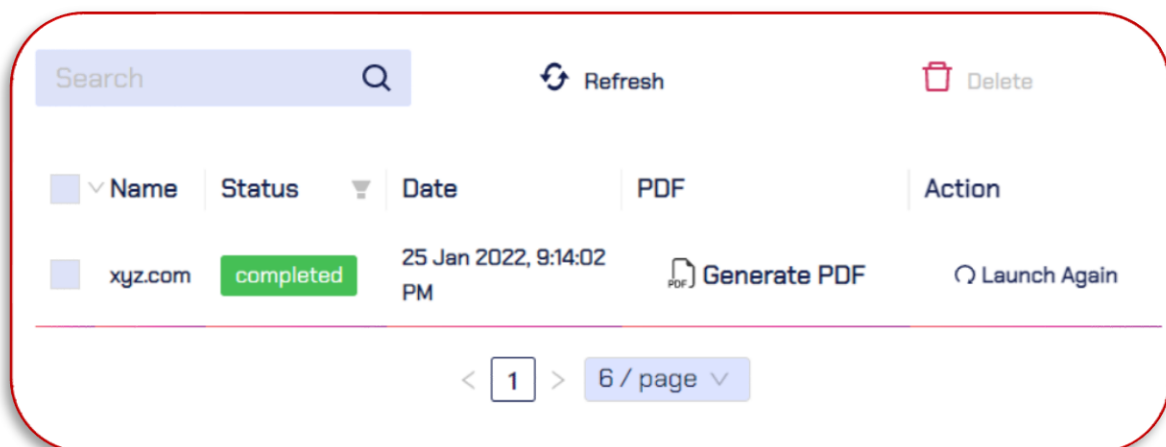


### 3.4. Web Reports

Within the **"Web"** module, there is a designated tab named **"Reports"** that offers comprehensive insights into all assessments conducted, whether normal or scheduled. This tab presents a detailed overview of assessment results, allowing for thorough analysis and evaluation. By utilizing this feature, users can gain a more comprehensive understanding of their assessments and make informed decisions based on the results.



1. Here, users are presented with a list of all assessments conducted, accompanied by their respective names and relevant details.
2. Users can view a detailed report of any assessment by clicking on the name of the desired report. This process enables users to thoroughly analyze assessment results and make informed decisions based on the information presented.



3. A recently generated report will be visible, indicating the status and time of generation. Click on **"Generate PDF"** to obtain a comprehensive report.

A rectangular button with a red border and a light blue background. It contains a PDF icon and the text "Generate PDF".

4. If you wish to execute the assessment again, simply click "Launch Again".

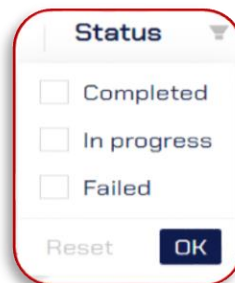
A rectangular button with a red border and a light blue background. It contains a circular arrow icon and the text "Launch Again".

5. The generated report will include all the identified findings such as CVEs, misconfigurations, vulnerabilities, subdomain takeovers, logins, directory traversals, sensitive information, etc.

#### 3.4.1. Column Detail

This section contains the same columns as the "Assessments" tab, except for the following:

- i. **Name Column:** This column displays information about the web domain that was selected by the user to run the Web assessment.
- ii. **Status Column:** This column displays information about the status of the assessment whether it is completed, in progress, or failed.



- iii. **Date Column:** This column displays the date and time when the assessment started.
- iv. **PDF column:** This column allows the user to download a PDF report of the assessment only after it has been completed successfully.
- v. **Action Column:** This column allows the user to relaunch the same assessment.
- vi. **Delete:** Allows the user to delete anything within Web assessment that is typically not available until you select any assessment.
- vii. **Refresh:** Can be used to refresh the report in case of issues while loading.

#### 3.4.2. View Report

1. After PDF report generation, it will automatically create and save in the designated "Download" folder.
2. The report will be named "Web" for easy identification.





3. To access the report, simply navigate to the "Download" folder and locate the "Web" file.

REPORT	
Domain: xyz.com	
Assessment Date: January 25th 2022, 4:14:02 pm +00:00	
Status: completed	
SUMMARY	
SEVERITY COUNT	
Info Count	10
Low Count	2
Medium Count	3
High Count	0
Critical Count	3

ABNORMALITIES	
Cves	3
Misconfigurations	6
Vulnerabilities	0
Arbitrary File Read	0
Common	0
Subdomain Takeover	0
Exposed Tokens	0
Exposed Logins	0
Directory Traversal	0
Sensitive Information	5
Lfi In Header	0
Lfi In Path	0
Passives	0
Xss	0
Lfi In Parameter	0
Exposed Panels	4

### 3.5. Web Report Summary

To view the detailed report summary within the report tab against a particular domain available in assessment history. Follow these steps:

- i. Click on a web domain in the Report list to view its complete assessment summary.

xyz.com

- ii. You will be able to see the overall detailed assessment summary. Which is further categorized into the following components.

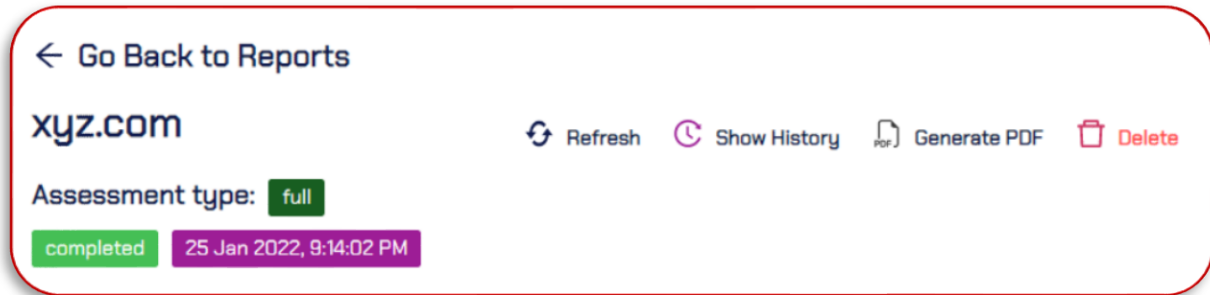
#### 3.5.1. Summary

The purpose of this document is to provide a comprehensive summary of web threats, which includes **CVEs**, **misconfigurations**, **vulnerabilities**, **subdomain takeovers**, **exposed panels**, and **default logins**.



The report summary covers a range of listed tasks and presents a detailed summary of vulnerabilities found in the web assessment with different techniques and an overview of the overall vulnerability's summary.

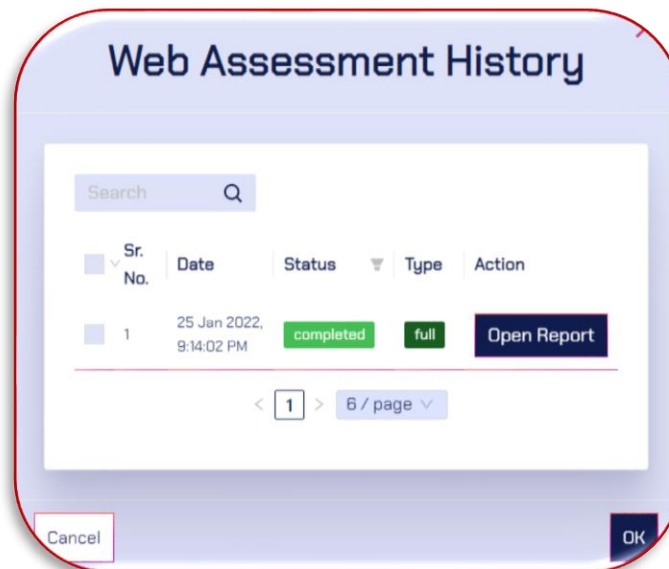
1. On top of the page the selected domain will appear and also appears the assessment status, date, and time with the assessment execution path.



This assessment aims to provide Web domains with relevant information regarding vulnerabilities arising from various misconfigurations in the Web domain.

You can take the following actions with the overall assessment summary.

- i. **Refresh:** can be used to refresh the report in case of issues while loading.
- ii. **Show history:** display the history of all assessments that are to be done so far.

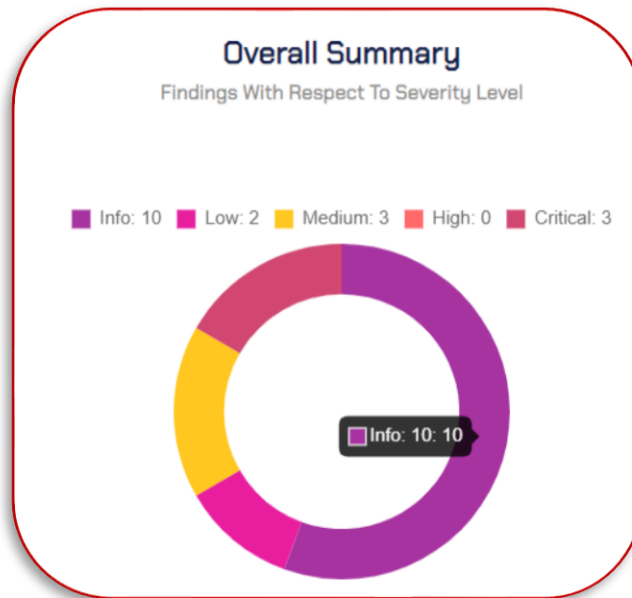


- iii. **Generate PDF:** this allows the user to download the report in PDF format.
- iv. **Delete:** allows the user to delete the report.

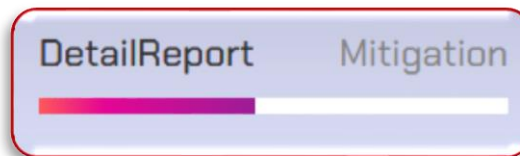
**Overall Summary:** This donut shape graph displays all security levels utilized through vulnerabilities to determine their severity levels, which diverge from **Info** (as informative



vulnerabilities), **Low, Medium, High, and Critical** (severe level).



2. Now Navigate to the “**Detail Report**” tab, to determine the details of the report.



### 3.5.2. CVEs

If a CVE is identified and matches with the already-known CVEs, it will be displayed along with its associated severity level, which can be categorized as informative, low, medium, or critical.

- Type:** Display the type of CVE found against the web domain in assessment.
- Severity:** Determine their severity levels, which diverge from **Info** (as informative vulnerabilities), **Low, Medium, High, and Critical** (severe level).
- Details:** Description of the CVE exploitation and remediation.
- Found On:** Platform where the CVE was found during the assessment.
- Single Test Run:** Execution routine as if you want to restart the assessment.



Misconfigurations					
Vulnerabilities					
Common					
Subdomain_takeover					
Expos					
Search					
Type	Severity	Url	Details	Found On	Single Test Run
CVE-2021-27905	critical	http://mmevdi.xyz.com/solr/error_video_converter/replication/?command=fetchindex&masterUrl=https://example.com	--	--	Start Again
CVE-2021-27905	critical	http://orcl-wbctr-int.xyz.com/solr/emp_offers/replication/?command=fetchindex&masterUrl=https://example.com	--	--	Start Again
CVE-2021-27905	critical	http://cities.xyz.com/solr/dynaForms/replication/?command=fetchindex&masterUrl=https://example.com	--	--	Start Again

### 3.5.3. Misconfigurations

Misconfigurations can result from incorrect or suboptimal configurations, leaving systems susceptible to exploitation by malicious actors.

- Type:** Display the type of misconfiguration found in vulnerabilities.
- Severity:** Determine their severity levels, which diverge from **Info** (as informative vulnerabilities), **Low**, **Medium**, **High**, and **Critical** (severe level).
- URL:** Reference of URL where misconfiguration was found during assessment against a web domain.
- Details:** Description of the misconfiguration found and its remediation.
- Found On:** Platform where the misconfiguration was found during the assessment.
- Single Test Run:** Execution routine as if you want to restart the assessment.
- For Example,** Cytomate offers a facility to list all identified misconfigurations, including but not limited to "front-page-misconfigurations" and "internal-ip-disclosure".





Misconfigurations Vulnerabilities Common Subdomain_takeover Exposi						
Search						
Type	Severity	Url	Details	Found On	Single Test Run	
front-page-misconfig	info	http://bps.xyz.com/_vti_inf.html	--	--	Start Again	
front-page-misconfig	info	http://bps.xyz.com/_vti_pvt/service.cnf	--	--	Start Again	
front-page-misconfig	info	https://bps.xyz.com/_vti_inf.html	--	--	Start Again	
front-page-misconfig	info	https://bps.xyz.com/_vti_pvt/service.cnf	--	--	Start Again	
iis-internal-ip-disclosure	info	https://autodiscover.xyz.com	--	--	Start Again	
iis-internal-ip-disclosure	info	https://mail.xyz.com	--	--	Start Again	

### 3.5.4. Sensitive Information

It helps in finding the exposure of an organization's sensitive information that may cause harm to security controls and leave a huge impact on the reputation of that organization.

- Type:** Display the type of sensitive information found in vulnerabilities.
- Severity:** Determine their severity levels, which diverge from **Info** (as informative vulnerabilities), **Low**, **Medium**, **High**, and **Critical** (severe level).
- URL:** Reference of URL where misconfiguration was found during assessment against a web domain.
- Details:** Description of the information exploitation and remediation.
- Found On:** Platform where the information is found during the assessment.
- Single Test Run:** Execution routine as if you want to restart the assessment.
- For Example,** Web assessment reports list all possible points where SI disclosure may occur, including but not limited to "exposed-share-point-list" and "thumb-db-disclosure".





Sensitive_information						
Search						
Type	Severity	Url	Details	Found On	Single Test Run	
exposed-sharepoint-list	low	<a href="https://bps.xyz.com/_vti_bin/lists.asmx?WSDL">https://bps.xyz.com/_vti_bin/lists.asmx?WSDL</a>	--	--	Start Again	
exposed-authentication-asmx	low	<a href="https://bps.xyz.com/_vti_bin/Authentication.asmx?op=Mode">https://bps.xyz.com/_vti_bin/Authentication.asmx?op=Mode</a>	--	--	Start Again	
thumbs-db-disclosure	info	<a href="http://gcc.xyz.com/Thumbs.db">http://gcc.xyz.com/Thumbs.db</a>	--	--	Start Again	
thumbs-db-disclosure	info	<a href="http://kids.xyz.com/Thumbs.db">http://kids.xyz.com/Thumbs.db</a>	--	--	Start Again	
thumbs-db-disclosure	info	<a href="http://aljaiza.xyz.com/Thumbs.db">http://aljaiza.xyz.com/Thumbs.db</a>	--	--	Start Again	

### 3.5.5. Exposed Panel

When access controls are limited to username and password combinations alone, it becomes significantly easier for attackers to breach the site.

- Type:** Display the type of sensitive information found in vulnerabilities.
- Severity:** Determine their severity levels, which diverge from **Info** (as informative vulnerabilities), **Low, Medium, High, and Critical** (severe level).
- URL:** Reference of URL where misconfiguration was found during assessment against a web domain.
- Details:** Description of the information exploitation and remediation.
- Found On:** Platform where the information is found during the assessment.
- Single Test Run:** Execution routine as if you want to restart the assessment.
- For Example:** To mitigate these risks, Cytomate identifies all vulnerabilities found in exposed panels, such as "solr-exposure" and "microsoft-exchange-panel", and categorizes them based on their associated severity levels.



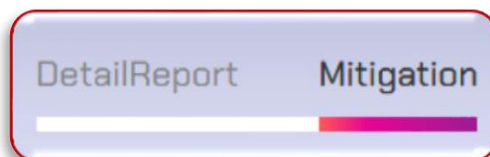


Arbitrary_file_read Sensitive_information Dom_xss Network Exposed_panels ...						
Search						
Type	Severity	Url	Details	Found On	Single Test Run	
solr-exposure	medium	http://bp.xyz.com/solr/	--	--	Start Again	
solr-exposure	medium	http://mmevdi.xyz.com/solr/	--	--	Start Again	
solr-exposure	medium	http://orcl-wbctr-int.xyz.com/solr/	--	--	Start Again	
microsoft-exchange-panel	info	https://autodiscover.xyz.com/owa/auth/logon.aspx?replaceCurrent=1&url=https://autodiscover.xyz.com/ecp	--	--	Start Again	

### 3.5.6. Web Mitigations

After identifying all web domain weaknesses, Cytomate suggests appropriate mitigations related to the web domain to address the vulnerabilities with their relevant security measurement and patch them.

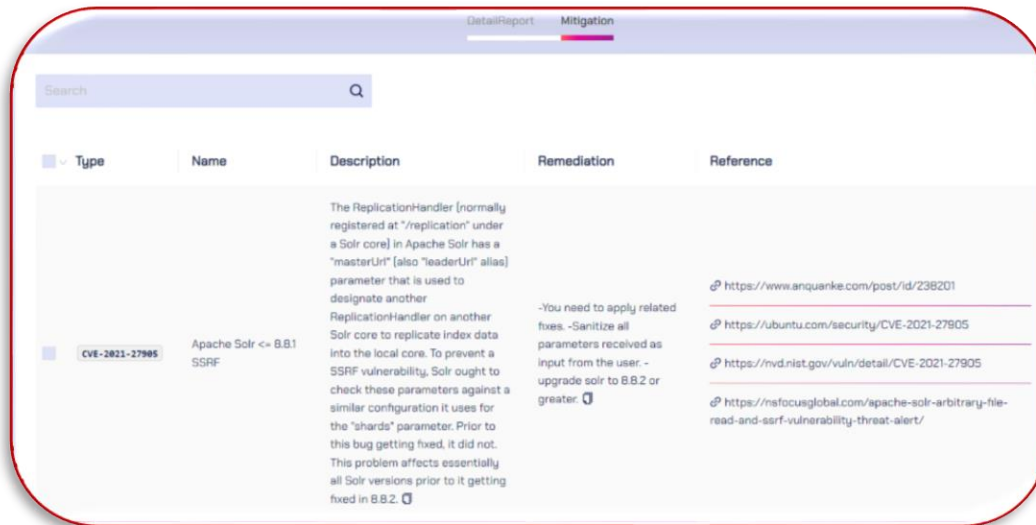
- Navigate to the “Mitigation” tab within the summary page.



- Type:** Display all types of vulnerabilities found in the web domain with mitigations to patch them.
- Name:** Display the name of the vulnerability found to mitigate it.
- Description:** Details of the found vulnerabilities from breach to security remediation.
- Remediation:** Method to patch the vulnerability to exploit the loophole.
- Reference:** URL that is being utilized to find the vulnerability in the provided web domain.



- vii. **For example**, if an extension vulnerability is found on Microsoft Front Page, it will suggest suitable remediation strategies along with descriptions and references to guide organizations in taking proactive measures as mentioned below.



Type	Name	Description	Remediation	Reference
CVE-2021-27905	Apache Solr <= 8.8.1 SSRF	The ReplicationHandler (normally registered at "/replication" under a Solr core) in Apache Solr has a "masterUri" (also "leaderUri" alias) parameter that is used to designate another ReplicationHandler on another Solr core to replicate index data into the local core. To prevent a SSRF vulnerability, Solr ought to check these parameters against a similar configuration it uses for the "shards" parameter. Prior to this bug getting fixed, it did not. This problem affects essentially all Solr versions prior to it getting fixed in 8.8.2.	-You need to apply related fixes. -Sanitize all parameters received as input from the user. -upgrade solr to 8.8.2 or greater.	<a href="https://www.anquanke.com/post/id/238201">https://www.anquanke.com/post/id/238201</a> <a href="https://ubuntu.com/security/CVE-2021-27905">https://ubuntu.com/security/CVE-2021-27905</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-27905">https://nvd.nist.gov/vuln/detail/CVE-2021-27905</a> <a href="https://msfocusglobal.com/apache-solr-arbitrary-file-read-and-ssrf-vulnerability-threat-alert/">https://msfocusglobal.com/apache-solr-arbitrary-file-read-and-ssrf-vulnerability-threat-alert/</a>

### 3.6. Scheduled Assessment

The list of scheduled assessments displays complete details of the domain, including the domain name, date, and time.

1. Navigate to the **"Scheduled Assessments"** tab located in the **"Web"** sub-menu to view all scheduled assessments.



2. The scheduled assessment will appear with the status of **"Scheduled"** and it will trigger automatically at the scheduled time and date.

## II. WAF SECURITY

### 1. Technical Details of WAF Security

Web application firewalls (WAFs) are critical tools for organizations to protect their web applications from various cyber threats, such as SQL injection, cross-site scripting, and distributed denial-of-service (DDoS) attacks. However, a recent study found that 99% of web application attacks still exploit known vulnerabilities, highlighting the importance of having a strong WAF in place.

#### 1.1. The Importance of WAF: Statistics Speak

According to a report by Cybersecurity Ventures, cybercrime will cost the world \$10.5 trillion annually by 2025 <sup>[3]</sup>. Moreover, 90% of businesses experienced at least one cyber-attack in the last year, and 59% of organizations had to deal with an application layer attack in the same period <sup>[4]</sup>.

A WAF helps protect web applications from such attacks and provides an additional layer of security to prevent malicious traffic from reaching the application server. Failure to secure web applications can result in financial loss, reputational damage, and legal liability.

#### 1.2. Introducing Cytomate WAF Security: The Solution to Web Security Challenges

Cytomate WAF solution is a unique solution that helps organizations assess their WAF's effectiveness against various payloads, including cross-site scripting and SQL injection attacks. Using Cytomate's WAF solution, organizations can simulate attacks and test their WAFs' resilience against different threat vectors, including payloads that are designed to bypass WAFs. The Open Web Application Security Project (OWASP) Top vulnerabilities are a list of the most common and critical web application security risks. Here is the list of OWASP's Top vulnerabilities:

- i. **Injection:** Injection vulnerabilities occur when untrusted user input is sent to an interpreter as part of a command or query, allowing attackers to execute unintended commands or access unauthorized data.



- ii. **Cross-Site Scripting (XSS):** XSS vulnerabilities occur when an application includes untrusted data in a web page without proper validation or escaping, allowing attackers to execute malicious scripts in a victim's browser.



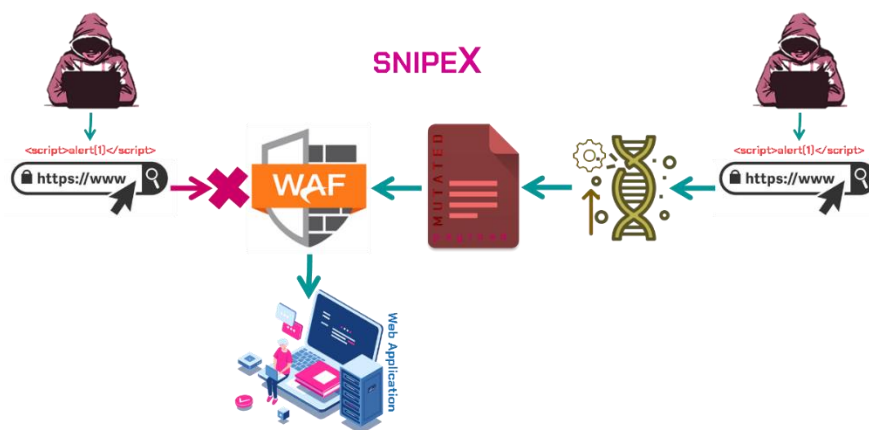
- iii. **Directory Traversal:** Directory Traversal is a type of attack where an attacker can access files and directories outside of the web root directory on a vulnerable server.



- iv. **Command Injection (CMDI)** is a security vulnerability that allows attackers to execute arbitrary commands on a vulnerable system by injecting malicious commands through an application or system that does not properly validate user input.



- v. **SNIPEx Integration:** Cytomate WAF solution integrates with the SNIPEx system, which uses AI and machine learning algorithms to generate payloads that are specifically designed to bypass WAFs. By testing your WAF against these payloads, you can ensure that your WAF is capable of detecting and blocking the most advanced attacks, including those that are specifically crafted to evade traditional security measures.



**Using Components with Known Vulnerabilities:** Using components with known vulnerabilities occurs when an application uses third-party components that are known to have security vulnerabilities, allowing attackers to exploit those vulnerabilities to gain access to the application or system.

Cytomate's WAF solution provides a comprehensive report on the WAF's efficacy, identifying any vulnerabilities or gaps that may exist.





### 1.3. Benefits of Cytomate WAF Security

- i. Comprehensive Testing: Cytomate WAF solution tests the organization's WAF against a broad range of threat vectors, including payloads, and spoofed headers.
- ii. Intelligent Reporting: The platform provides a detailed report on the effectiveness of the organization's WAF.
- iii. Scalable and Automated: Cytomate WAF solution is a scalable and automated solution, enabling organizations to schedule tests at their convenience and receive comprehensive reports automatically.

Web application attacks continue to be a major threat to organizations worldwide, and a WAF is a critical tool to mitigate such threats. Cytomate WAF solution is a unique solution that provides comprehensive testing and intelligent reporting to help organizations assess their WAF's effectiveness against various threats. With its custom payloads, scalability, and automation capabilities, Cytomate WAF solution is an ideal solution for organizations of all sizes and industries.

## 2. User Manual of WAF Security

### Scope of the Manual

In this section, we aim to explain the significance of Cytomate Breach+ WAF Security and how it can serve as a defense against potential Web Application Firewall (WAF) threats. Additionally, we will provide an overview of the essential hardware and software prerequisites that are required to utilize Cytomate Breach+ WAF Security to its full potential.

### Definitions

#### 2.1. Web Application Firewall (WAF)

A WAF monitors and filters incoming and outgoing traffic between a web application and the internet and blocks malicious traffic before it reaches the web application. In today's business landscape, web applications have emerged as a key component of numerous organizations, demanding significant resources like (WAFs) to safeguard these digital assets.

However, as the internet evolves, the number and scope of threats also continue to escalate, encompassing everything from complex malware to targeted application-layer attacks, distributed denial of service (DoS/DDoS) strikes, to security-induced usability issues.

#### 2.2. WAF Assessment

To counteract these threats, most organizations invest in Web Application Firewalls, which sometimes provide a false sense of security and leave organizations open to



exploitation. To address this problem, Cytomate has developed an advanced WAF assessment tool that evaluates the configuration, implementation, and features of your WAF to identify web application attacks like XSS, SQLi, LFI, CMDi, and many other injection attacks and misconfigurations that may expose your organization to cyberattacks.

Our state-of-the-art simulation techniques simulate an attacker attempting to bypass the WAF, infiltrate the web application firewall, and launch destructive attacks like mining sensitive information, damaging data, and redirecting users to infected sites.

### 2.3. WAF Mitigations

Cytomate Breach+ suggests appropriate mitigations related to the WAF, updates WAF security, and adds more rules to harden WAF.

## 3. Advanced WAF Assessment

Advanced WAF assessment is a process that evaluates and tests the security controls of a Web Application Firewall to protect a Web application against various threats and malicious traffic. The WAF assessment service provider organizations the opportunity to evaluate the security of their Web Application Firewall (WAF) against the latest web-based threats. This includes testing for potential vulnerabilities related to abused SSL ciphers, abused DNS history, basic payloads, obfuscated basic payloads, advanced payloads, known payloads, and SnipeX payloads.

### 3.1. Hardware and Software Requirements

To use Cytomate WAF Security Solution, the following hardware and software requirements must be met:

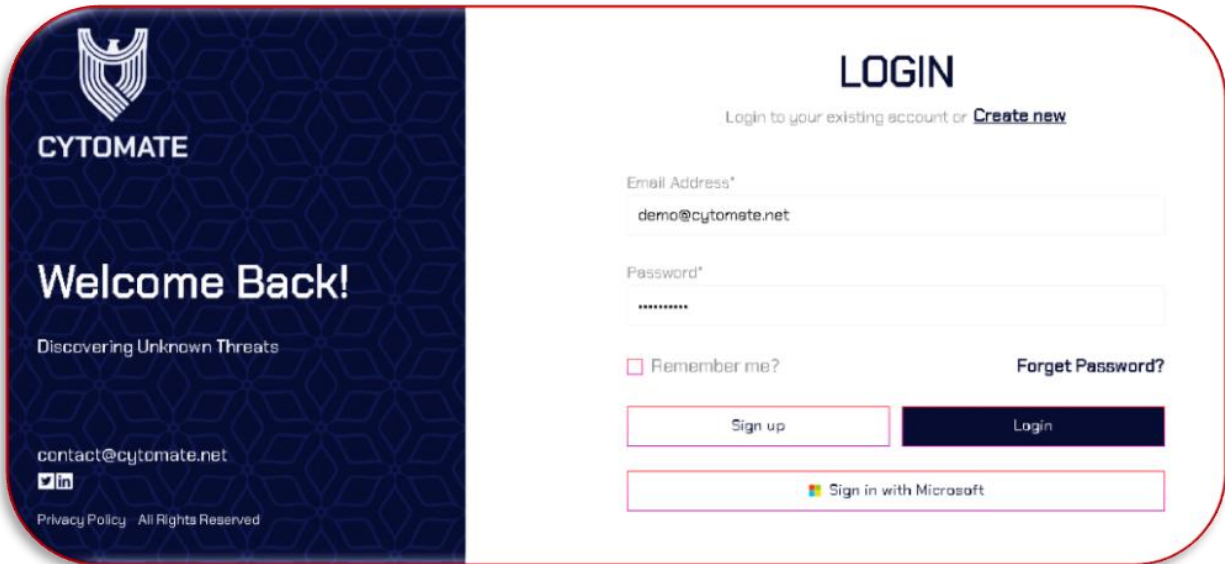
#### 3.1.1. Domain Verification

Cytomate WAF assessment required a verified domain. Domain verification steps are described in the “**Assessment**” part.

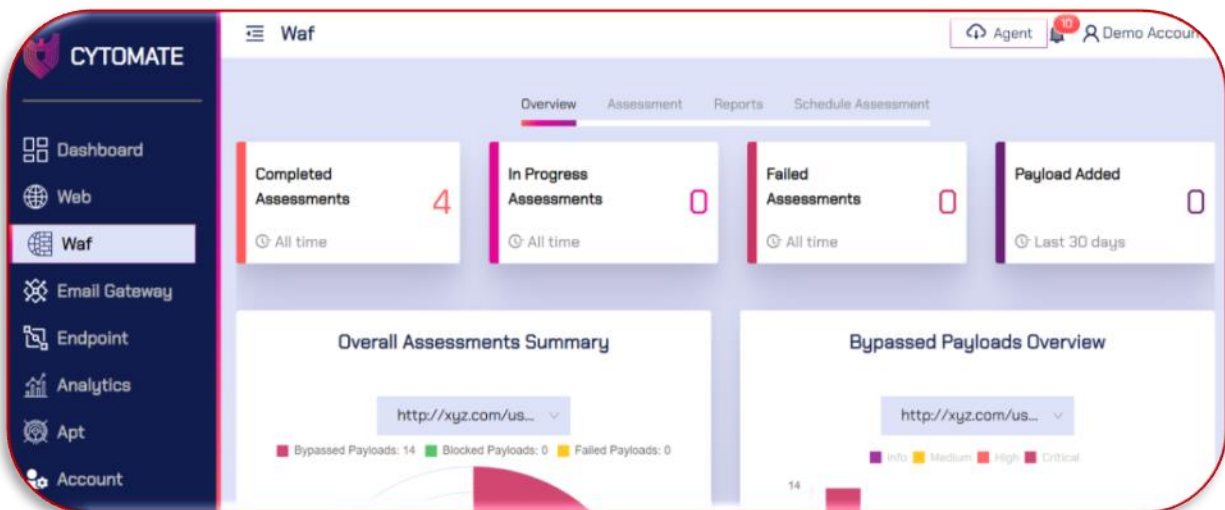
### 3.2. Cytomate WAF Security Solution

To start the WAF assessment follow the simple steps as follows:

1. Access the Cytomate Breach+ portal <https://apt.cytomate.net/>.
2. Login through credentials (enter username and password) to access Cytomate Breach+ Dashboard.

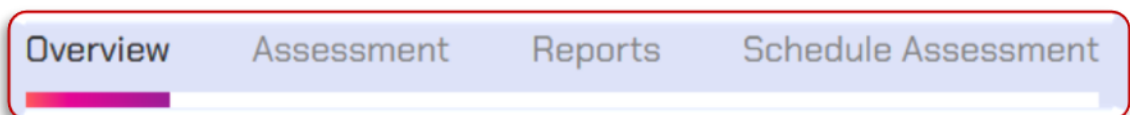


3. Navigate to the “WAF” module to access its functionalities and features.



### 3.2.1. Overview

Within the WAF module, there are four different tabs, each of them offering unique functionalities and features.



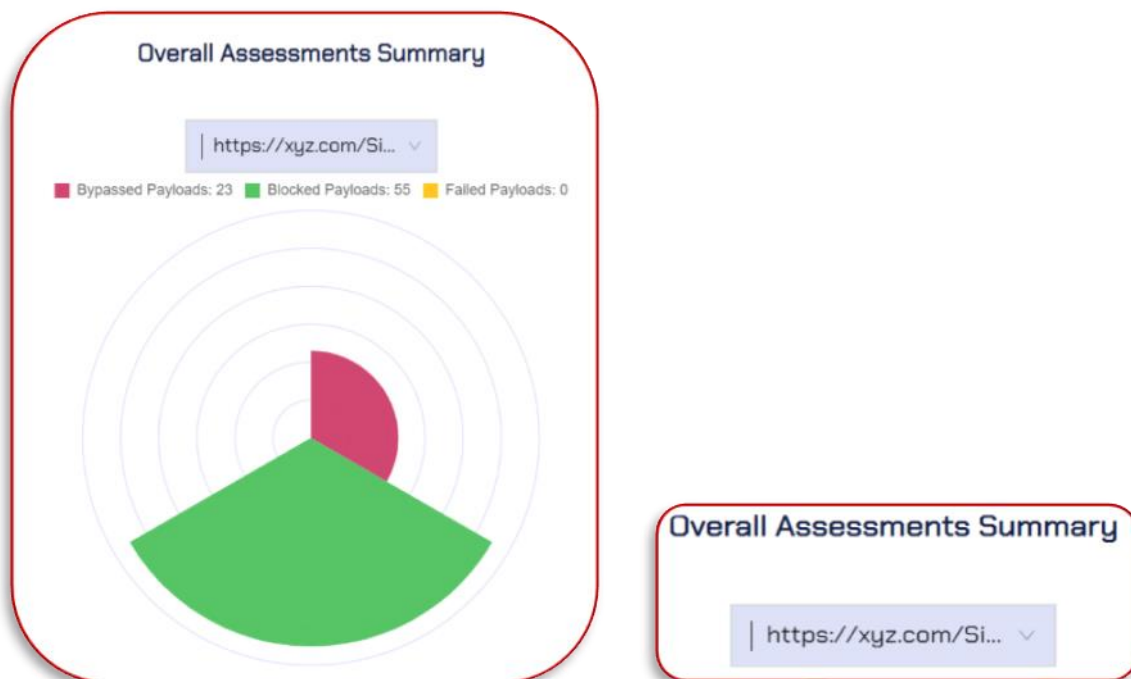
In the overview tab, four widgets provide a quick review of the WAF assessment and an overview of WAF assessment details in the form of graphs. These widgets include:

- Completed Assessments:** This widget contains information on how many total assessments have been completed by users since the account was created.

- ii. **In progress Assessments:** This widget displays how many assessments by the user are currently in progress since the account was created.
- iii. **Failed Assessments:** This widget contains information on how many total assessments have failed since the account was created.
- iv. **Payloads added:** This widget contains information on how many new payloads have been added by Cytomate within the last 30 days that can be used for WAF assessments by the user.



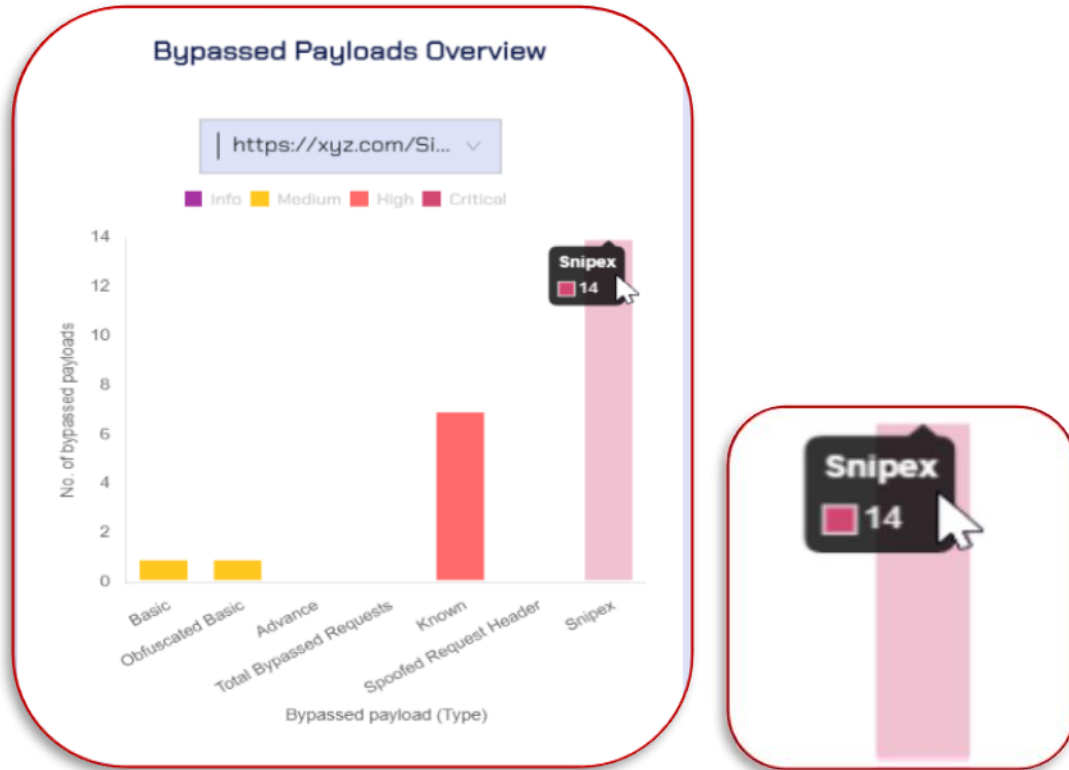
**Overall Assessment:** This Rose Chart displays the overall security weaknesses detected in the WAF and provides a detailed overview of all payloads used by users and shows statistics about payloads that Bypassed, Blocked, and Failed out of all available payloads. You can choose the URL from the list to view the details.



**Bypassed Payload Overview:** This graph provides a detailed breakdown of various payloads, which are further categorized as “Basic, Obfuscated Basic, Advanced, Bypassed Requests, and Known Requests, out of the total number of sent requests”.

- i. Additionally, the section includes information on spoofed request headers and AI-based payloads.
- ii. Select the URL to view the statistics.

- iii. This chart visualizes the number of Bypassed payloads against different payload categories basic, obfuscated, and SnipeX payloads, etc.
- iv. You can hover on the wedges to see the total number of payloads against that particular category.



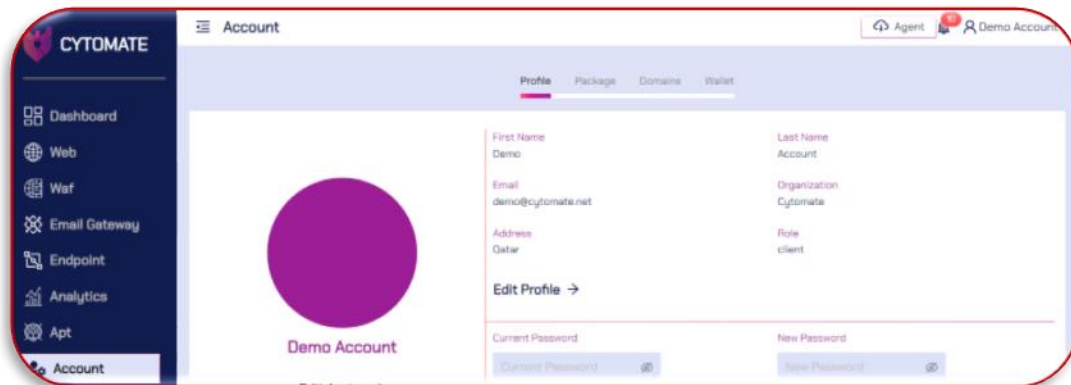
This comprehensive display of information makes a clear understanding of the security vulnerabilities present and enables users to take the necessary steps to strengthen the security of their Web application firewall.

### 3.2.2. Assessment

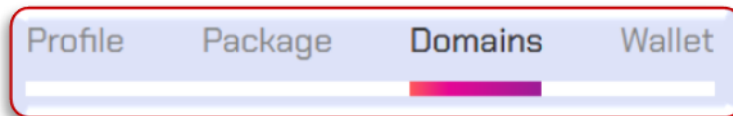
#### 3.2.2.1. Domain Verification Steps

To run the assessment, it is essential to provide a verified domain. If the targeted domain is not verified yet, you should follow these steps to verify it.

1. Navigate to the **"Accounts"** option from the side panel.



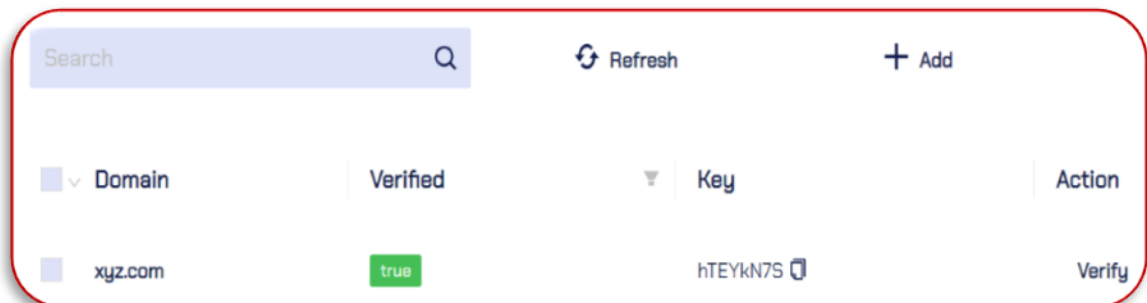
- Click the “Domains” tab.



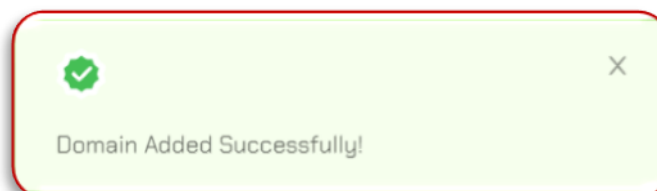
- Click the “Add” icon to add a new domain.



- Enter the required web domain and proceed to the next step click “Add Domain”.



- Wait for the prompt that indicates the domain has been added successfully.



6. To verify the domain, copy the key from the **"Key"** column and paste it into the domain's DNS as a TXT record.
7. Once your domain registrar publishes your verification code (which may take the time up to 72 hours to propagate worldwide, although it typically takes a few hours), click on the **"Verify"** button to check if the TXT record exists.
8. If the record is found, the **"Verified"** column will be set to **"true"** and we'll know you are the owner of your domain.

**Verified**

false

true

#### 3.2.2.1.1. Column Details

- i. **Domain Column:** This column contains the name of the domain which are successfully verified or being verified.
- ii. **Verified Column:** This column contains the verification status against the domain.
- iii. **Key Column:** This column contains a verification key of this domain.
- iv. **Action Column:** This column contains the actions against the particular domain whether these are verified or pending.

#### 3.2.2.1.2. Steps to start an assessment

1. To start the assessment, first navigate to the **"Assessment"** tab within the WAF module.

Overview
Assessment
Reports
Schedule Assessment

2. Interested parties need to provide the URL with a parameter by accessing the **"Select URL"** option.

\* Select Url

http://xyz.com/?search=

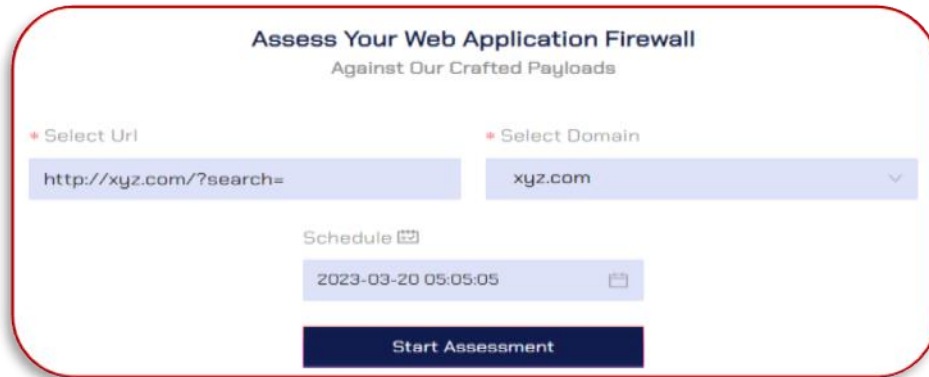
3. Add the verified web domain via the **"Select Domain"** option.



\* Select Domain

xyz.com


4. Click the "Start Assessment" button.\




**Assess Your Web Application Firewall**  
Against Our Crafted Payloads

\* Select Url      \* Select Domain

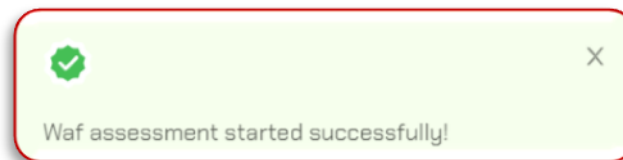
http://xyz.com/?search=      xyz.com

Schedule 

2023-03-20 05:05:05 

**Start Assessment**

5. When you will hit the "Start Assessment" button wait for the pop-up notification that indicates the assessment has been started successfully.



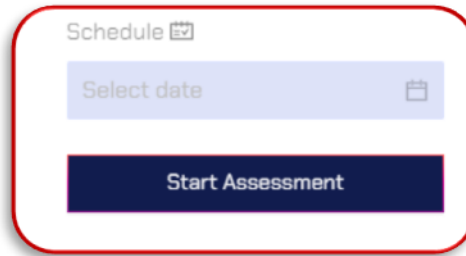
### 3.2.2.1.3. Steps to start (Schedule) an Assessment

The client can **schedule an assessment** to begin at a later time if you prefer not to initiate the assessment immediately. Cytomate WAF assessment module provides the convenience of scheduling assessments on domains according to an organization's specific needs. By scheduling assessments in advance, ensure that you have conducted assessments at a time that minimizes disruption to your daily activities.

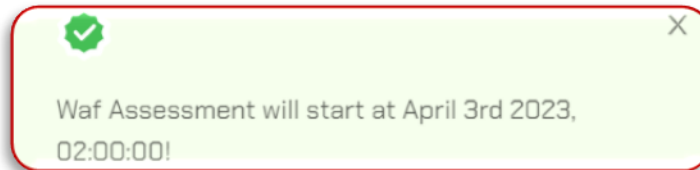
To schedule an assessment, the user must follow these steps:

- i. To schedule a WAF assessment, simply follow all the above-mentioned steps to start an immediate assessment.
- ii. Choose the targeted Domain and URL with the parameter.
- iii. An additional step you need to follow. Set the date and time and press the "**Start Assessment**" button to schedule the WAF assessment for later execution.



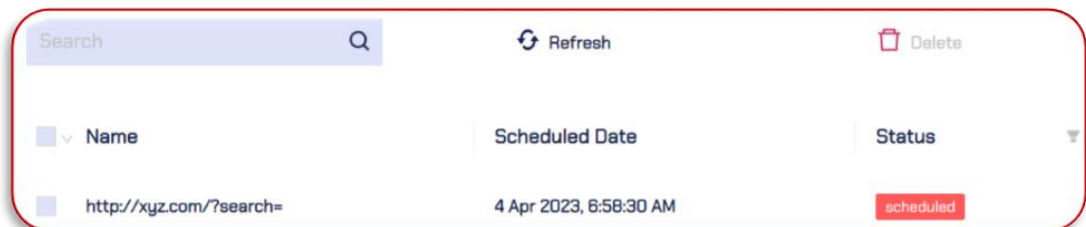


- iv. Wait for a pop-up notification that indicates the assessment has been scheduled successfully.



**Note:** It is mandatory to provide both URLs with parameters and targeted domains to start the WAF assessment.

- v. The scheduled assessment will appear in scheduled assessments with the status of "Scheduled" and it will trigger automatically at the selected time.



Name	Scheduled Date	Status
http://xyz.com/?search=	4 Apr 2023, 6:58:30 AM	scheduled

- vi. To schedule an assessment for a later time or date, follow the above steps but select the desired date and time from the calendar.

#### 3.2.2.1.4. Columns Details

- iii. **Name Column:** This column contains the URL with a parameter it indicates the specific endpoint upon which the assessment is going to start according to the scheduled date and time.
- iv. **Scheduled Date Column:** This column contains the date and time for assessment.
- v. **Status Column:** This column contains the assessment status which is possibly completed, scheduled, and failed.

☐ Completed
 ☐ Scheduled
 ☐ Failed

Reset
 OK

### 3.2.3. Reports

The "WAF" module contains a tab called "Reports" that provides you with detailed information on all assessments, including both normal and scheduled assessments. This tab allows you to view and analyze the results of your assessments in a more detailed manner. The resulting report will comprise a comprehensive overview of all findings identified during the assessment. These findings will include potential vulnerabilities related to abused SSL ciphers, abused DNS history, basic payloads, obfuscated basic payloads, advanced payloads, known payloads, spoofed request headers, SnipeX, and other relevant issues that may have been identified.

Upon the successful completion of the WAF assessment on the selected URL, you can generate a report.

1. Navigate to the "Reports" tab within the WAF module to access the generated report.



2. A recently generated report will be visible, indicating the status and time of assessment.

Name	Status	Date
https://xyz.com/SiteSearch.aspx?BusinessUnitID=6516txtSearch=	completed	2 Mar 2023, 6:24:33 PM
<div>           &lt;           1           &gt;           6 / page         </div>		

3. Click on "Generate PDF" to obtain a comprehensive report.



4. If you wish to execute the assessment again, simply click "Launch Again" assessment will be started again.



Search

Q

Refresh

Delete

▼

Name

Status

Date

PDF

Action

▼

https://xyz.com/SiteSearch.aspx?BusinessUnitID=6518txtSearch=

completed

2 Mar 2023, 6:24:33 PM

Generate PDF

Launch Again

<

1

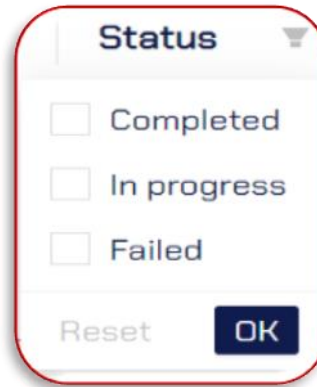
>

6 / page

### 3.2.3.1. Columns details

This section contains the same columns as the "Assessments" tab, except for the following:

- i. **Name Column:** This column displays information about the URL that was selected by the user to run the WAF assessment on a specific domain.
- ii. **Status Column:** This column displays information about the status of the assessment, including:
  - a. **Completed:** This means that the assessment started by the user has been completed, and the user can view the detailed report.
  - b. **In progress:** This means that the assessment is currently being performed.
  - c. **Failed:** This means that an error occurred either on the server side or on the endpoint, but it does not necessarily mean that the exploit failed to perform its functions. The developers will be notified, and they will investigate and resolve the issue.

A modal window titled "Status" with a dropdown arrow. It contains three checkboxes: "Completed", "In progress", and "Failed". At the bottom, there are "Reset" and "OK" buttons.

Status	
<input type="checkbox"/>	Completed
<input type="checkbox"/>	In progress
<input type="checkbox"/>	Failed
Reset OK	

- iii. **Date Column:** This column displays the date and time when the assessment started.
- iv. **PDF column:** This column allows the user to download a PDF report of the assessment only after it has been completed.
- v. **Action Column:** This column allows the user to relaunch the same assessment.
- vi. **Delete:** Allows the user to delete anything within the WAF assessment.
- vii. **Refresh:** Can be used to refresh the report in case of issues while loading.

#### 3.2.3.2. Viewing the Assessment (PDF) Report

1. After PDF report generation, it will automatically create and save in the designated "Download" folder.
2. The report will be named "Waf.Pdf" for easy identification.
3. To access the report, simply navigate to the "Download" folder and locate the "Waf.Pdf" file. Double-click on the file to open it and view the report.





Cytomate	
REPORT	
Origin: https://xyz.com	
Path: /SiteSearch.aspx	
Search: ?BusinessUnitID=651&txtSearch=	
Assessment Date: March 2nd 2023, 1:24:33 pm +00:00	
Status: completed	
OVERALL SUMMARY	
Total Requests	78
Total Bypassed Requests	23
Total Blocked Requests	55
Total Failed Requests	0
INDIVIDUAL TESTS SUMMARY	
Abused Dns History	
BASIC	
Total Requests	14
Total Bypassed Requests	1
Total Blocked Requests	13
Total Failed Requests	0
OBFUSCATED BASIC	
Total Requests	16
Total Bypassed Requests	1
Total Blocked Requests	15
Total Failed Requests	0
ADVANCE	
Total Requests	0
Total Bypassed Requests	0
Total Blocked Requests	0
Total Failed Requests	0
TOTAL BYPASSED REQUESTS	
Total Requests	0
Total Bypassed Requests	0
Total Blocked Requests	0
Total Failed Requests	0

### 3.2.3.3. Behavior (Payload) report

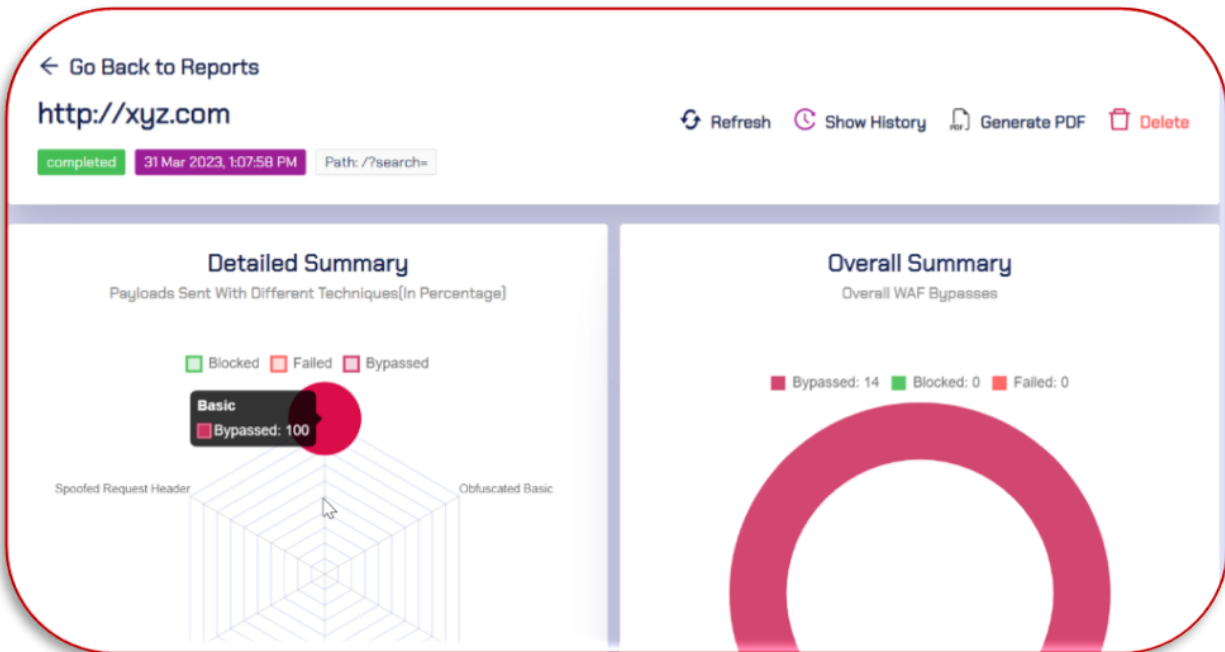
To view the detailed report summary, the user must perform the following steps:

1. Click on a URL to view its complete assessment summary.



2. It will open a new window that displays a detailed report of the payload behavior.





- At the top of the report, there is a navigation button that allows the user to go back to the "All Reports" page.

← Go Back to Reports

- Following the navigation button, there are action buttons alongside the behavior name that serve different purposes, as explained below:

Refresh Show History Generate PDF Delete

- Show History:** this allows the user to view all previous assessments that were done using this exploit. Click the "Open Report" option to view the assessment report.

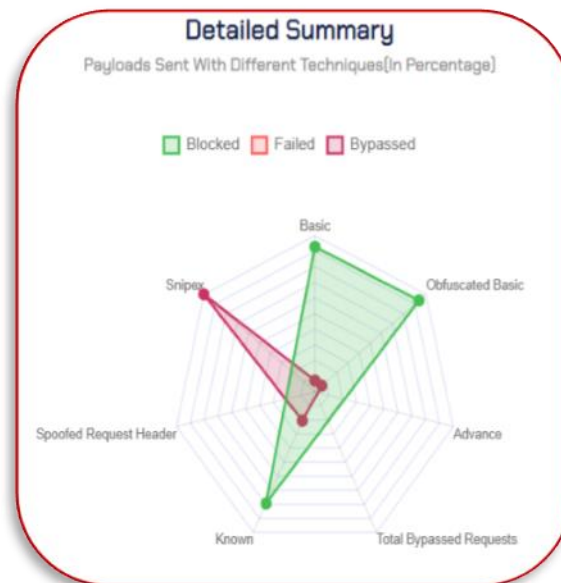
WAF Assessment History				
Sr. No.	Date	Status	Action	
1	31 Mar 2023, 1:07:58 PM	completed	Open Report	
2	20 Mar 2023, 5:05:07 AM	completed	Open Report	

- Generate PDF:** this allows the user to download the report in PDF format.
- Delete:** allows the user to delete any item.

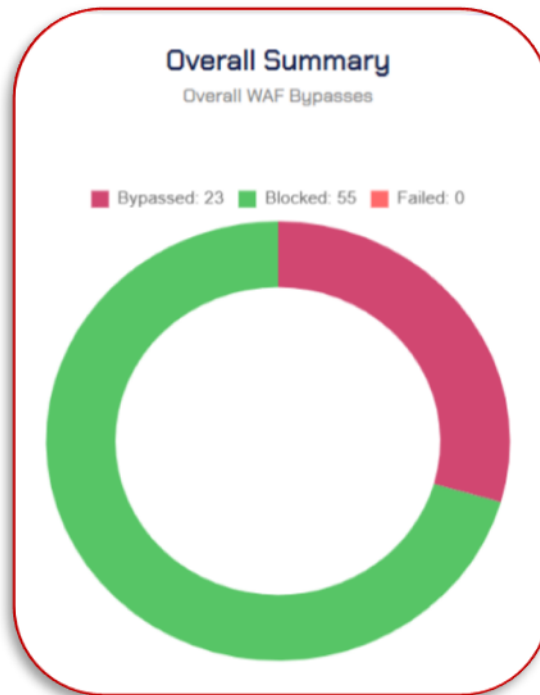
6. Below the action button, there is a detailed assessment section that includes information about the status of the assessment, the date and time when the assessment started, the path that was used for the assessment, and the type of exploit used for the assessment.



7. The next section is the Detailed Summary and overall summary.
  - i. **Detailed summary:** In this graph, multiple payloads with different techniques with their responses are visualized such as bypassed, blocked, and failed which can be useful to mitigate vulnerabilities.



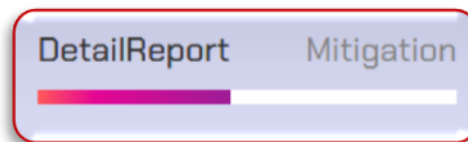
- ii. **Overall Summary:** This Donut shape graph displays the overall blocked, bypassed, and failed payloads.



While moving down on the same page further two tabs are available providing more details:

#### 3.2.3.4. Detail Report

1. Navigate to the “Detail Report” tab.



2. Following payload categories are available:

##### 3.2.3.4.1. Basic Payloads

- i. During the basic payload testing phase, the assessment will transmit the simple payloads to the WAF in their unaltered state, to generate a generic response.
- ii. The objective of this phase is to observe the WAF's response and assess how WAF reacts to a specific payload applied to a particular URL endpoint.
- iii. It should be noted that many of the payloads used in this phase are malicious in nature and will likely be blocked by the WAF.



DetailReport

Mitigation

Abused\_ssl\_cipher

Abused\_dns\_history

Basic

Obfuscated\_basic

Advance

Known

Spoofed\_request\_header

Snipex

Search

Q

Type	Payload	Status	Status Code
sql	* OR 1 = 1 --	Blocked	403
sql	T ORDER BY 1--	Blocked	403
sql	UNION ALL SELECT 1,2,3,4,5--	Blocked	403
xss	<div onpointerover=alert(1)>MOVE HERE</div>	Blocked	403
xss	<img src=x onerror=alert(1)>	Blocked	403
xss	<script>alert(1)</script>	Blocked	403

<

1

2

3

>

6 / page

#### 3.2.3.4.2. Known Payloads

- In this phase, known payloads will send to the WAF during the assessment.
- These are the payloads collected from an open source shared by the hackers on daily basis.
- They can be categorized based on their level of complexity and sophistication, ranging from basic payloads that require little knowledge or skill to advanced payloads that are specifically crafted to bypass complex security measures.

Basic	Type	Payload	Status	Status Code
Obfuscated_basic	xss	<a href=")6Tab;abTab;6Tab;asc6NewLine;ri6Tab;pt6colon;w006T\u006C\u0065\u0072\u00748ipar,t his[document][cookie]6rpar;">X</a>	Bypassed	200
Advance	xss	<--<img/src=" onerror=confirm">-->	Blocked	403
Known	xss	%22--%3E%3C/style%3E%3C/script%3E%3Cscript%3Eshadowlabs(0x00045)%3C/script%3E	Blocked	403
Spoofed_request_header	xss	<script>eval(atob(decodeURIComponent("payload")))//	Blocked	403
Snipex	xss	"><img/src/onerror=alert(1)>	Blocked	403
	xss	<svg/onload=6#976#1086#1016#1146#001166#406#416#x2f6#x2f	Blocked	403

#### 3.2.3.4.3. Obfuscate Payloads

- In this phase, the obfuscated payloads will be used during the assessment.

- ii. These basic WAF-blocked payloads will be intentionally obfuscated to generate mutated payloads with different encoding and decoding patterns, which obscure the original payload.

Basic	Type	Original Payload	Payload	Status	Status Code	Encoded Obfuscation
Obfuscated_basic	XSS	<--<img/src="onerror=confirm">-->	%253C--%2560%253Cimg%252Fsrc%2530%2560%252Onerror%2530confirm%2560%2560%253E%2520--%2521%253E	Blocked	403	double_url_encode
Advance	XSS	<--<img/src="onerror=confirm">-->	<--<img/SRc=" onERroR=confirm">-->	Blocked	403	upper_and_lower_case
Known	XSS	<--<img/src="onerror=confirm">-->	%C0%BC--%C0%BCimg/src="onerror=confirm"%C0%BE--%C0%BE	Blocked	403	utf_8_encode
Spoofted_request_header	XSS	<--<img/src="onerror=confirm">-->	<!--><--<img/src=" onerror=confirm">-->-->	Blocked	403	inside_comments
Snipex	XSS	<--<img/src="onerror=confirm">-->	<noscript><p title="</noscript><--<img/src="onerror=confirm">-->">	Blocked	403	noscript_tag_mutation
	XSS	%22--%3E%3C/style%3E%3C/script%3E%3Cscript%3Eshadowlabs[0x00045]%3C/script%3E	%2527%252522--%25253E%25253C%252Fstyle%25253E%25253C%252Fscript%25253E%25253Cscript%25253Eshadowlabs%2520x00045%2520%25253C%252Fscript%25253E	Blocked	200	double_url_encode

1
2
3
6 / page

#### 3.2.3.4.4. SnipeX Payloads

- i. In this phase, AI-Based mutated payloads will send through requests that have been mutated by a Reinforcement Learning based system with multiple types of mutations, encodings, and decoding schemes, to blur the effect of the original payload.

Abused_ssl_cipher	Search			
Abused_dns_history				
Basic	Type	Payload	Status	Status Code
Obfuscated_basic	XSS	<B#<B>< /"/"/"->"/" #wT3vG2 < /"/"/"/"/"-></Script><image SrcSet="K "; OnError=confirm"/>	Bypassed	200
Advance	XSS	<B#<B>< /"/"/"/"->"/" #ahZcVZ <svg </onload =>{ _=>prompt_[""]}~/>/B/"; +%"00	Bypassed	200
Known	XSS	<B#<B>< /"/"/"/"->"/" #jL4cAZ <script/><a/src-data="<a[B].some(confirm)/>/B/"; +%"00	Bypassed	200
Spoofed_request_header	XSS	<B#<B>< /"/"/"/"->"/" #hQ8cH4 <input/onmouseover="javaSCRIPT\$colon:confirm\$ipar;\$rpar"/>/B/"; +%"	Bypassed	200
Snipex	XSS	<B#<B>< /"/"/"/"->"/" #vD2eR14 <w="/*>"/>ondblclick="<[confirm"]>~/B/"; +%"00	Bypassed	200
	XSS	<B#<B>< /"/"/"/"->"/" #kFSuQ16 ><svg/onload=alert[document.domain]/>/B/"; +%"00	Bypassed	200

#### 3.2.3.4.4.1. Columns Details

Against payload following details are available:

- i. **Type:** it provides information about the payload category.
- ii. **Original Payload:** it displays the original payloads sent to the WAF without applying any obfuscation technique.
- iii. **Payload:** it displays the payload that is obfuscated through different techniques.

- iv. **Status:** it displays the status of the payload after applying a payload whether it is blocked or bypassed by WAF.
- v. **Status Code:** It displays the response status code that indicates the request was successfully sent if the status code is 200.
- vi. **Encoded Obfuscation:** it displays the obfuscation technique category applied to the mutated payload.

▼ Type ▼	Original Payload	Payload	Status ▼	Status Code ▼	Encoded Obfuscation
----------	------------------	---------	----------	---------------	---------------------

#### 3.2.3.4.5. WAF Mitigations

Cytomate identifies WAF weaknesses and suggests appropriate mitigations related to the WAF, updates WAF security and adds more rules to harden WAF. Also, it suggests suitable remediation strategies with descriptions to guide WAF vendors in taking proactive measures.

- i. Navigate to the "Mitigation" tab within the summary page.



- ii. **Strategy:** it displays which strategy should be followed against a particular misconfiguration.
- iii. **Description:** it shows a detailed description of the strategy to implement in WAF against misconfiguration and defines new rules.

▼ Strategy	Description
Add Rules/Signature	Add Rules/Signatures of bypassed payloads in WAF at your endpoint to prevent these payloads from bypassing this endpoint again in future.

#### 3.2.4. Schedule Assessment (WAF)

1. Navigate to the "Scheduled Assessments" tab located in the "WAF" sub-menu to view all scheduled assessments.



2. The scheduled assessment will appear with the status and time. It will trigger

automatically at the scheduled date and time.

□	Name	Scheduled Date	Status	▼
□	http://xyz.com/?search=	3 Apr 2023, 2:00:00 AM	scheduled	

### III. EMAIL GATEWAY

#### 1. Technical Detail of Email Gateway

The number of cyberattacks is a growing concern, with over 75% of such attacks being initiated through the receipt of malicious emails. As the number of targets and attacks continues to increase, it is imperative to protect against potential identity theft, password scams, and other forms of regular fraudulent activities that can cause significant harm.

##### 1.1. The Importance of Email Gateway

Malicious files, particularly office documents, are often used by cybercriminals as a first step to gaining access to an organization's network. These files may contain various types of email scams, such as phishing and business email compromise (BEC) scams. For instance, a common phishing scam involves sending an email that appears to be from a reputable organization, such as a bank or an online shopping website, and requesting the recipient to provide sensitive information such as login credentials or credit card numbers.

These emails may also contain a link to a fake website that resembles the legitimate one, tricking the victim into entering their personal information, which is then captured by the attacker. Similarly, a BEC scam involves an attacker impersonating an executive or a vendor and requesting the recipient to transfer funds to a fraudulent account. These scams may be disguised as legitimate office documents, such as invoices or purchase orders, and can be difficult to detect.

##### 1.2. Introducing Cytomate Email Gateway: The Solution to Email Gateway Challenges

Cytomate Email Gateway is an advanced security solution that helps organizations to assess the resilience of their email gateway security controls. As email remains one of the primary means of communication for businesses, it is a critical attack vector for cybercriminals. The assessment uses advanced techniques to emulate real-world attack scenarios. The

assessment includes a comprehensive analysis of the email security architecture, including the identification of email security gaps, vulnerabilities, and potential threats.

It helps to evaluate the organization's response to these simulated attacks, assessing the effectiveness of the email gateway security controls. The results of the assessment are presented in a detailed report, which includes an overview of the email gateway security controls, a description of the simulated attacks, an analysis of the results, and recommendations for improving the email gateway security controls. The report also provides insights into the organization's overall security posture.



Payloads



Malware Attack



Ransomware Attack

These threats are being hidden with different run-time file formats (Penetration Vectors) to bypass common security products such as Mail Relay, Sanitize Solutions, and Sandbox. Mitigation recommendations are also offered by Cytomate for each threat that has been discovered depending on the category and prevention vector.

### 1.3. Benefits of Email Gateway

- i. Test using one dedicated mailbox which does not affect users or systems in the organization's network.
- ii. Email gateway assessment automatically runs in stages; first Cytomate email assessment module will send an email with malicious contents, then the Cytomate agent will access and open emails, download attachments for static analysis, and then report to the server.
- iii. All stages of the test are done automatically, including the hash comparison of penetrated payloads and the deletion of sent emails to the agent once it lands in the tested mailbox.
- iv. Testing can be performed on a regular basis to monitor the threats continuously by selecting individual or multiple test cases to execute on a targeted email gateway.
- v. By scheduling assessments in advance, ensure that you have conducted the assessment at a time that minimizes disruption to your daily activities.
- vi. Based on the identified findings and associated risks, Cytomate also offers suggestions for actionable mitigations that organizations can implement to avoid potential threats.
- vii. Detailed reports with mitigation tips based on file type and behavior of penetrated emails.

## 2. User Manual of Email Gateway

### Scope of the Manual

In this section, we aim to explain the significance of Cytomate Breach+ Email Gateway Security and how it can serve as a defense against potential email-based threats. Additionally, we will provide an overview of the essential hardware and software prerequisites that are required to utilize Cytomate Breach+ Email Gateway Security to its full potential.

### Definitions

#### 2.1. Email gateway (Security)

An email gateway is a type of email server that protects an organization or user's internal email servers. This server acts as a gateway through which every incoming and outgoing email passes. All the security solutions that are typically implemented at the email gateway level include features such as content filtering, antivirus scanning, encryption, and authentication mechanisms to ensure the safety and integrity of email communication.

#### 2.2. Cytomate Agent

Cytomate relies on a lightweight agent known as the "BreachPlusAgent" to evaluate the security of the email gateway. You can choose the operating system "Windows or Linux" for the system agent which enables communication with Cytomate Breach+.

#### 2.3. Mitigation

Cytomate Breach+ suggests appropriate mitigations related to the email gateway security, updating email security and adding more security controls to keep it safe from threats.

## 3. Cytomate Email Gateway Assessment

Cytomate offers an email gateway assessment that assesses your organizational email gateway security and identifies all the associated threats. It is a process that evaluates and tests the security controls of the email gateway to protect your organizational email security posture. As email gateways use a combination of technologies, including spam filters, antivirus software, content filtering, encryption, and authentication mechanisms to protect email communications. This service allows organizations to launch a diverse range of simulated malicious emails containing threats such as ransomware, payloads, exploits, malware, worms, and dummy files.

The entire email gateway security assessment process is performed securely and confidentially, with the utmost consideration for the privacy of the client organization. The results of the

assessment are then used to provide actionable mitigations to protect against the weaker security areas.

## 4. Hardware and Software Requirements

To use Cytomate Email Gateway Security Solution, the following hardware and software requirements must be met:

### 4.1. Cytomate Agent installation

The solution includes a lightweight agent that is installed on the system and communicates with the Cytomate Breach+. This agent is used by Cytomate to test corporate email gateway security controls and identify any vulnerabilities or weaknesses in the security defenses.

1. To download and install the agent on your system, please refer to the **Agent installation guide**.
2. This guide provides detailed instructions on how to install and configure the agent to start using the Email gateway security solution.

### 4.2. Domain Verification

Cytomate email gateway assessment required a verified domain. Domain verification steps are described in the “**Assessment**” part in this document.

### 4.3. Features and Functionalities

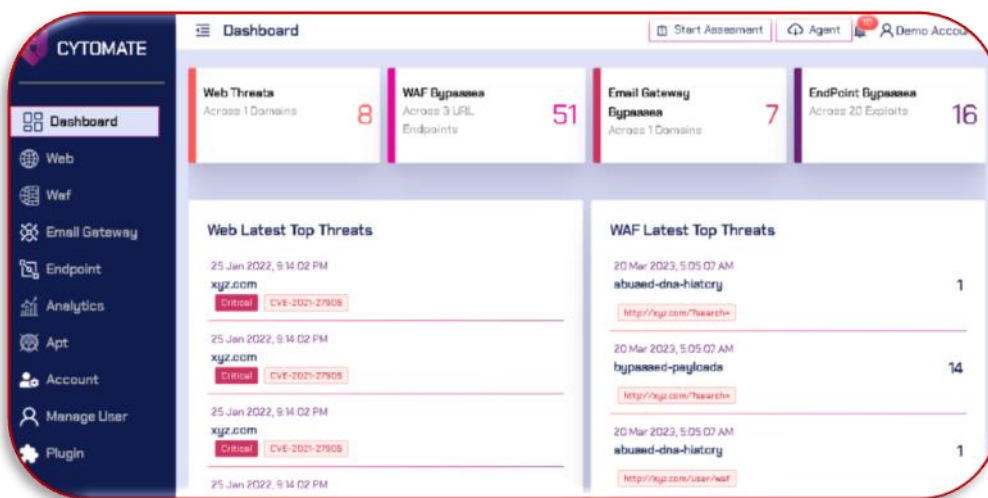
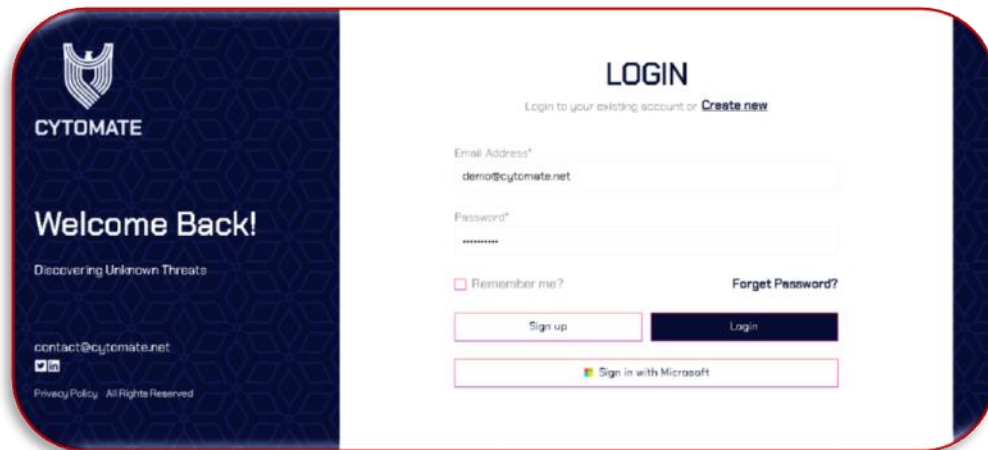
This section provides an interactive demonstration of Breach+ Email Gateway Security solution features and functionalities. Through the use of screenshots and step-by-step instructions, users can learn how to effectively use the solution to protect their Email gateway security. By the end of this section, users will have a thorough understanding of how to use Breach+ Email Gateway Security solution to enhance email protection against potential threats.

## 5. Cytomate Breach+ Email Gateway Security Solution

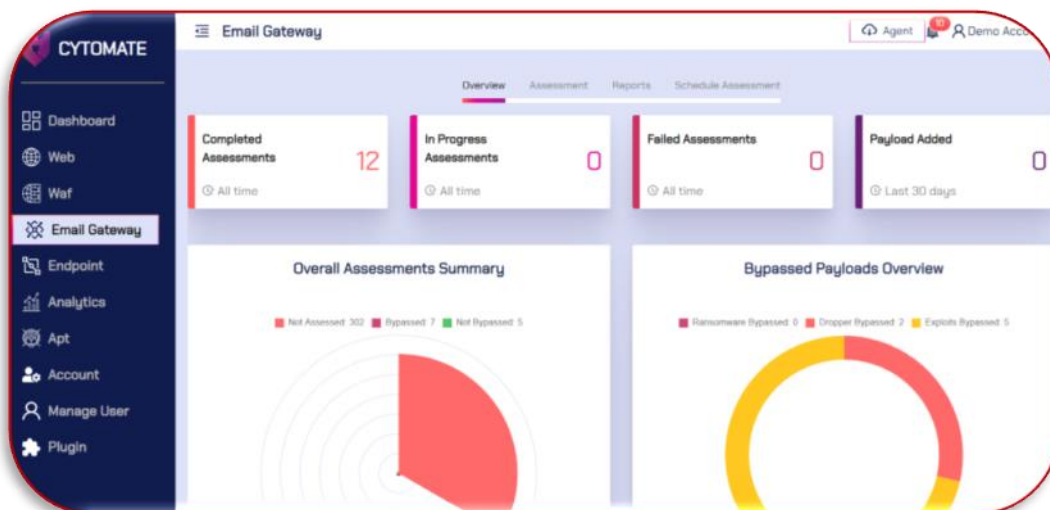
To start an Email gateway assessment following steps should be followed:

1. Go to the Cytomate Breach+ portal at <https://apt.cytomate.net/>.
2. Login through username and password and click “**Login**” to access the main Dashboard.





- Navigate to the “Email Gateway” module from the side menu to access the email gateway dashboard.





## 5.1. Overview

At the top of the dashboard, you will find four different tabs, each offering unique functionalities and features. The currently active tab is "Overview," which displays an overview of the endpoint assessment details in the form of widgets and graphs.

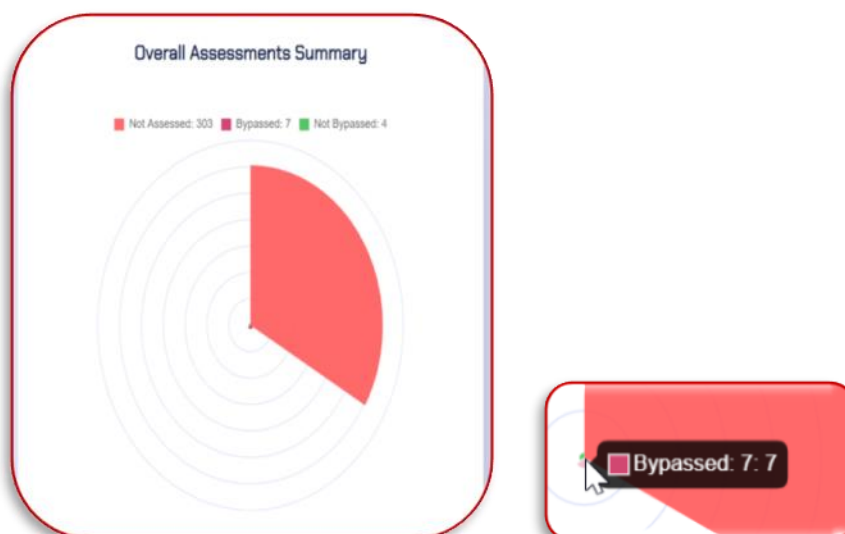


In the "Overview" tab, there are four top widgets that provide a quick view of the Email Gateway assessment details. These widgets include:

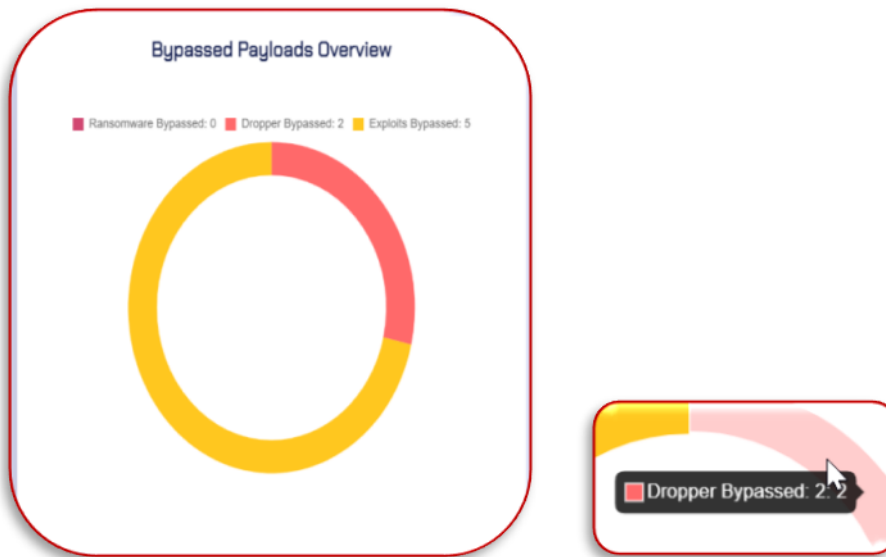
- Completed Assessments:** This widget contains information on how many total assessments have been completed by the user since the account was created.
- In Progress Assessments:** This widget displays how many assessments by the user are currently in progress since the account was created.
- Failed Assessments:** This widget contains information on how many total assessments have failed since the account was created.
- Payload Added:** This widget contains information on how many new payloads have been added by Cytomate that can be used for assessments by the user.



**Overall Assessment Summary:** This interactive Rose-shaped chart provides the summary of all payloads used by the client and shows statistics about the "Not Assessed", "Bypassed" and "Not Bypassed" payloads out among all test cases.



**Bypassed payloads Overview:** This Pie Donut graph displayed the overview of all bypassed payloads used by the client. It represents various bypassed payloads like “Ransomware Bypassed”, “Dropper Bypassed” and “Exploit Bypassed” with their total number.



By hovering over the chart bars, users can see information on the counts of each tactic's bypassed payloads.

## 5.2. Assessment

The “**Assessment**” tab within the email gateway module allows clients to evaluate the effectiveness of their Email Gateway security by conducting an assessment through the Cytomate Email Gateway module. An email gateway assessment that assesses your organizational email and identifies all the associated threats to protect email communications.

### 5.2.1. Domain verification

To run the assessment, it is essential to provide a verified email. If the targeted email is not verified yet, you should follow these steps to verify it.

1. Navigate to the “**Accounts**” option from the side panel.
2. There are four tabs on top of the page.
3. Navigate to the “**Domain**” tab and then click the “**Add**” icon to add a new domain.



4. Enter the required email address and proceed to the next step click “**Add Domain**”.

Add Domain

cytomate.net

Add Domain

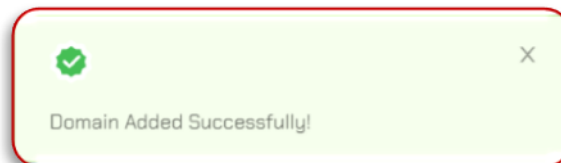
Search

Refresh

+ Add

Domain	Verified	Key	Action
xyz.com	true	hTEYkN7S	Verify

5. Wait for the prompt that indicates the domain has been added successfully.



6. To verify the domain, copy the key from the **"Key"** column and paste it into the domain's DNS as a TXT record.
7. Once your domain registrar publishes your verification code (which may take the time up to 72 hours to propagate worldwide, although it typically takes a few hours), click on the **"Verify"** button to check if the TXT record exists.
8. If the record is found, the **"Verified"** column will be set to **"true"** and we'll know you are the owner of your domain.

Verified

false

true

9. Once the domain verification process is completed, then all associated emails will be verified immediately.

#### 5.2.1.1. Column details

- i. **Domain Column:** This column contains the name of the domain which is successfully verified or being verified.



- ii. **Verified Column:** This column contains the verification status against the domain.
- iii. **Key Column:** This column contains a verification key of this domain.
- iv. **Action Column:** This column contains the actions against the particular domain whether these are verified or pending.

### 5.2.2. Email Gateway Security Testing Setup

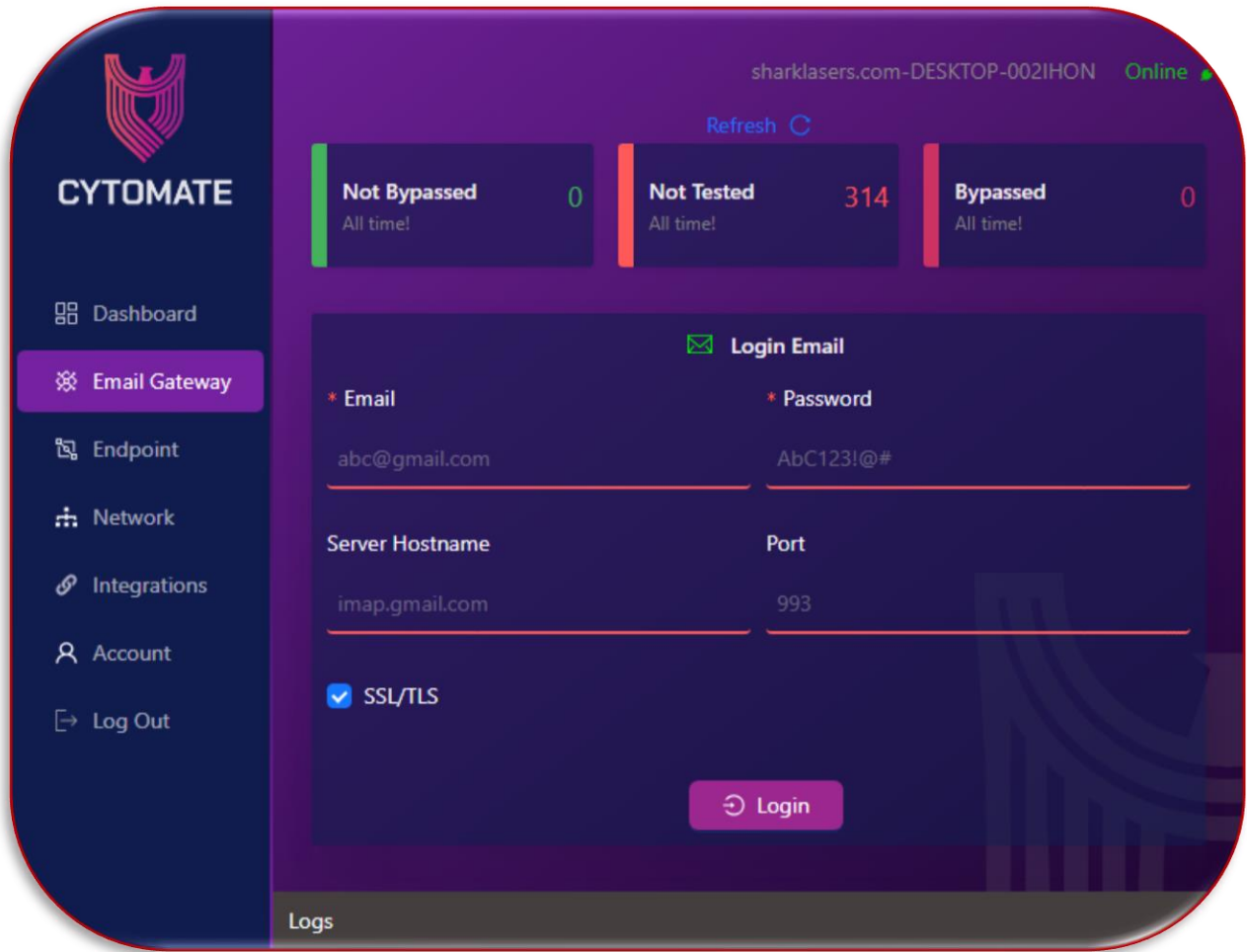
To access the email gateway component, you must integrate the agent with your email gateway through the login process. A successful login requires the addition of your organization:

- Email
- Password
- Server Hostname (Optional but required in some scenarios)
- Port

Once successfully logged in, the Breach+ agent automatically establishes a connection with the client's email server using the IMAP protocol. Subsequently, it retrieves emails from the inbox and checks for the presence of specific extensions. This automated process ensures a seamless assessment of the email content for enhanced security measures.

On the email gateway user interface, it will also provide information about the email gateway exploits which is not tested. also tells how many exploits successfully bypassed your email gateway defenses and how many were effectively blocked.





Once the agent is logged in to the testing email. You can launch assessments from the Breach+ webapp.

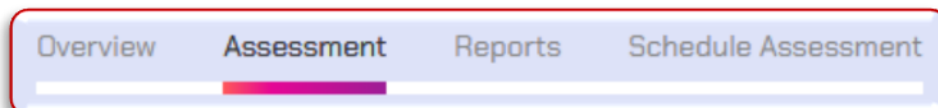
### 5.2.3. Steps to Start an Assessment

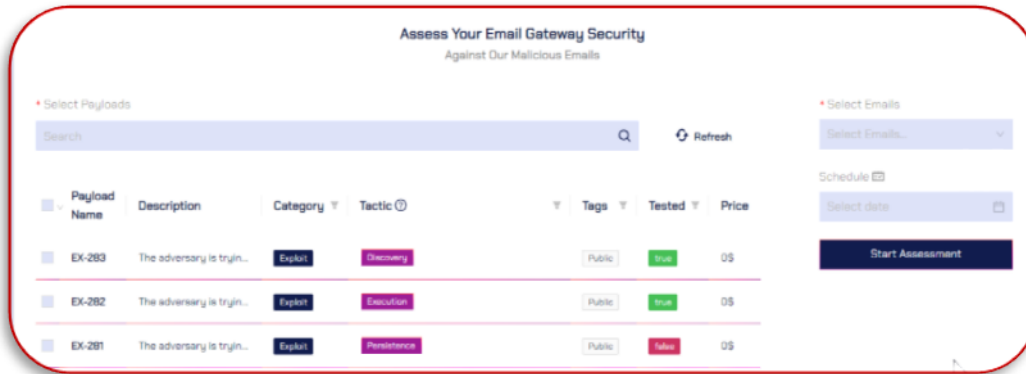
**Note:** Before conducting an email assessment, it is important to ensure that these three necessary steps have already been completed.

- i. Domain verification
- ii. Agent installation
- iii. Testing Email Login from Agent (e.g. [cytomate@YOUR\\_DOMAIN.com](mailto:cytomate@YOUR_DOMAIN.com))

To start an email assessment user must perform the following steps:

1. First navigate to the “**Assessment**” tab within the Email Gateway module.





**Assess Your Email Gateway Security**  
Against Our Malicious Emails

**\* Select Payloads**

Search Refresh

Payload Name	Description	Category	Tactic	Tags	Tested	Price
EX-283	The adversary is tryin...	Exploit	Discovery	Public	True	0\$
EX-282	The adversary is tryin...	Exploit	Execution	Public	True	0\$
EX-281	The adversary is tryin...	Exploit	Persistence	Public	False	0\$

**\* Select Emails**

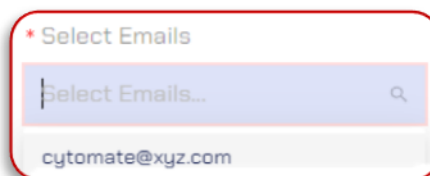
Select Emails...

Schedule 📅

Select date 📅

**Start Assessment**

2. Enter the (**verified**) Email by accessing the "Select Email" option. Follow the pattern of email which is visible as a hint.

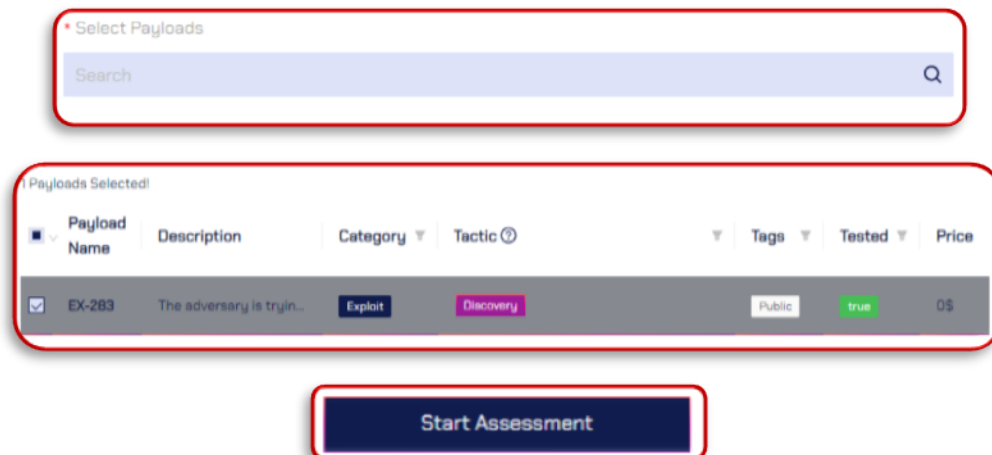


**\* Select Emails**

Select Emails... 🔍

cytomate@xyz.com

3. Choose payload then click the "**Start Assessment**" button to immediately execute it. You can select the available payloads executed by previous assessments or you can provide a new payload.



**\* Select Payloads**

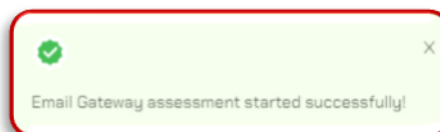
Search 🔍

**Payloads Selected:**

Payload Name	Description	Category	Tactic	Tags	Tested	Price
<input checked="" type="checkbox"/> EX-283	The adversary is tryin...	Exploit	Discovery	Public	True	0\$

**Start Assessment**

4. Wait for the pop-up notification that indicates the assessment started successfully.



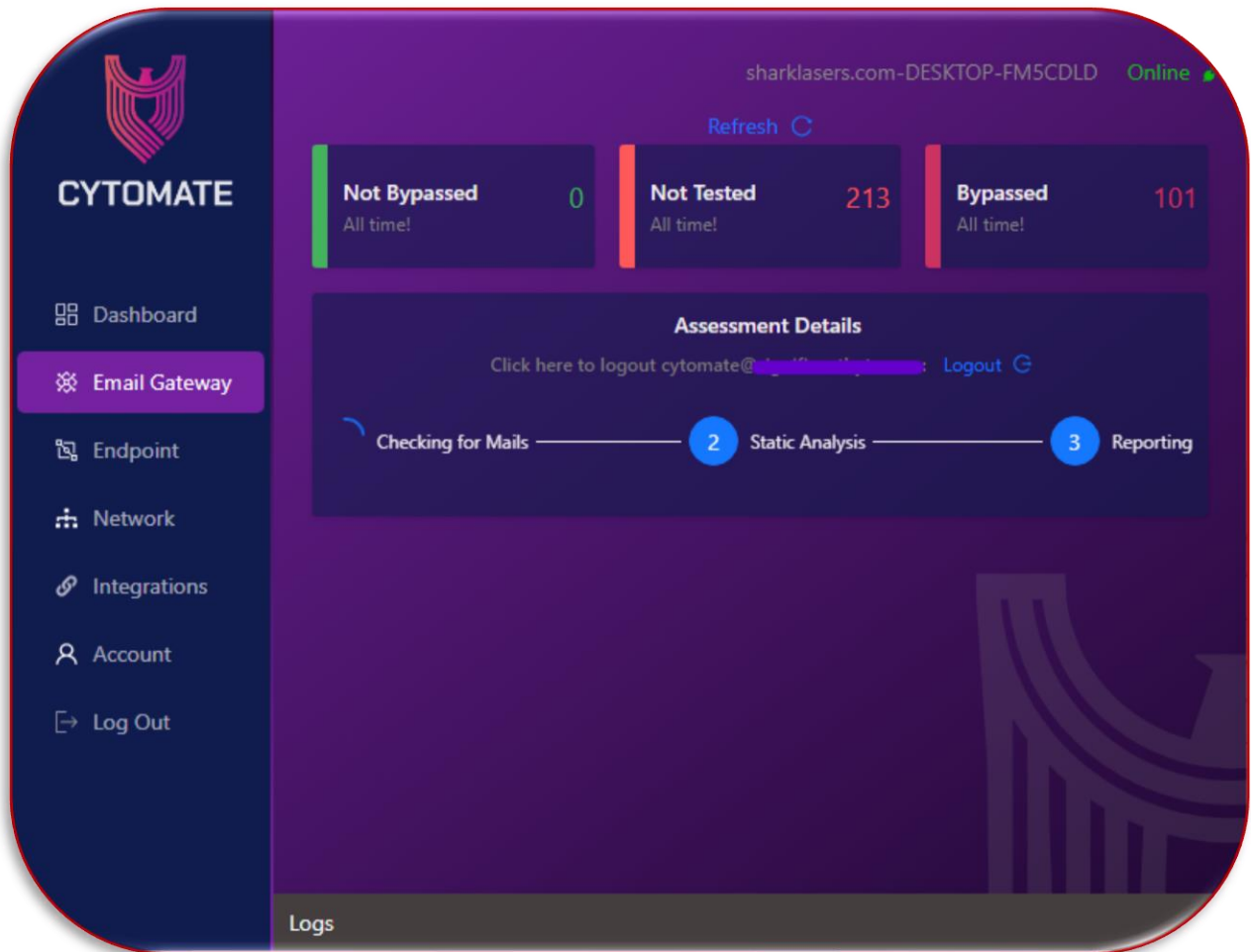
✓

Email Gateway assessment started successfully!

✕

5. On the Breach+ agent, if it is online, the assessment would start immediately. It does 3 main tasks:
  - Check for emails.

- Check for static analysis.
- Report



#### 5.2.4. Steps to Start (Schedule) an Assessment

The client can **schedule an assessment** to begin at a later time if you prefer not to initiate the assessment immediately. Cytomate Breach+ Email Gateway provides the convenience of scheduling assessments on domains according to an organization's specific needs. By scheduling assessments in advance, ensure that you have conducted assessments at a time that minimizes disruption to your daily activities.

To schedule an assessment, the user must follow these steps:

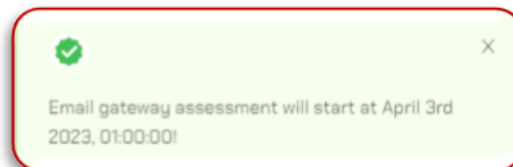
- To schedule an email assessment, simply follow all the above-mentioned steps to start an immediate assessment.
- Choose the targeted email and select the payload you want to use.
- An additional step you need to follow. Set the date and time and press the **“Start Assessment”** button to schedule an email assessment for later execution.

Schedule

Select date

Start Assessment

- iv. Wait for a pop-up notification that indicates the assessment has been scheduled.



- v. The scheduled assessment will appear with the status of **"Scheduled"** and it will trigger automatically at the selected time.
- vi. To schedule an assessment for a later time or date, follow the above steps but select the desired date and time from the calendar.

Name	Scheduled Date	Status	Details
xyz.com	3 Apr 2023, 1:00:00 AM	scheduled	

- vii. For more details, click the "Eye" option to check your scheduled Assessment details.

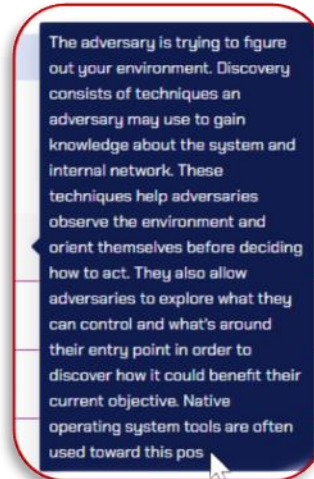
Email Gateway Assessment Details		
Sr. No.	File Name	Category
1	EX-283	exploit

1 / page

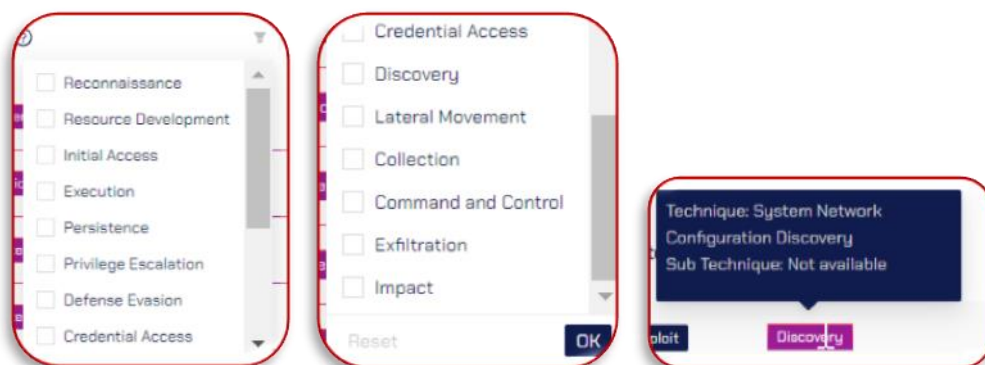
#### 5.2.4.1. Columns Details

- Payloads Column:** This column contains the name of executed payloads.
- Description column:** This column contains the description of each exploit and it can be seen by hovering the cursor over the details.



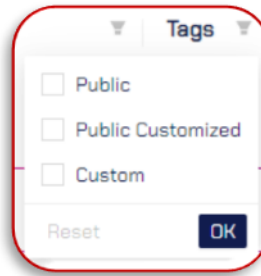


- iii. **Category Column:** This column infers the category of the exploit that can be any out of the given below list. Further, it also allows applying filters to select exploits based on these categories:
- Exploit** A program or technique used to take advantage of a vulnerability in a system, software, or application to gain unauthorized access or execute malicious code.
  - Ransomware:** A type of malware that encrypts a user's files or system and demands payment in exchange for restoring access to the affected data.
  - Dropper:** A type of malware, drops and executes the additional malware onto the victim's system once executed successfully on the targeted system.
- iv. **Tactics Column:** This column contains information about the tactic, technique, and sub-technique of each exploit that can be seen by hovering over the cursor on the tactic name. Further Tactic Filter allows filtering out exploits based on MITRE tactics and then selecting from those exploits.



- v. **Tags column:** Contains information about payload tags. Users can apply filters to select payloads based on three tag categories: Public, Public Customized, and Custom.
- Public:** Payloads collected from the internet for static analysis without being executed by Breach+.

- b. **Custom:** Highly advanced and sophisticated payloads developed by the Breach+ team.



- vi. **Tested Column:** Allows users to filter payloads based on whether they have been used (**True**) or not used (**False**) in previous assessments.
- vii. **Price Colum:** This column displays the price of each payload used by the client.

### 5.3. Reports

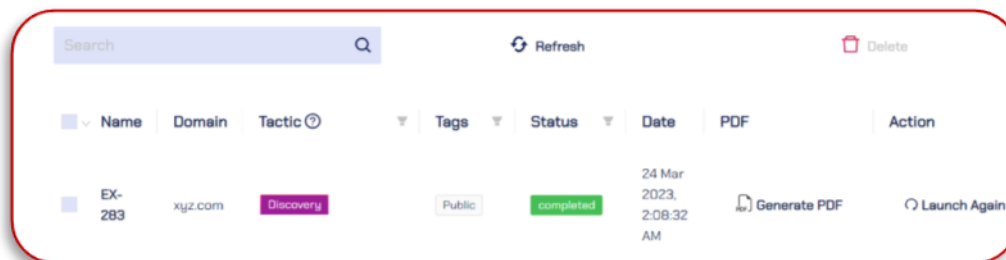
The "Email Gateway" contains a tab called "Reports" that provides you with detailed information on all assessments, including both normal and scheduled assessments. This tab allows you to view and analyze the results of your assessments in a more detailed manner.

To assess the report of your email assessment following steps should be followed:

1. Navigate to the "**Reports**" panel to access the generated report.



2. Generated report will be visible, indicating the status and time of generation.



3. Click on "**Generate PDF**" to obtain a comprehensive report.



4. If you want to execute the assessment again, click "**Launch Again**" Assessment will be restarted on the targeted email.

 Launch Again

### 5.3.1. Columns Details

- i. **Name Column:** This column displays information about the payload that was selected by the user to run an assessment on a specific domain. In other words, it indicates which payload the assessment was performed on.
- ii. **Domain Column:** This column displays information about the domain that was given by the user to run an assessment.
- iii. **Tactics Column:** This column contains information about the tactic, technique, and sub-technique of each exploit. Further Tactic Filter allows filtering out payloads based on MITRE tactics and then selecting from those exploits.
- iv. **Status Column:** This column displays information about the status of the assessment, including:
  - a. **Completed:** This means that the assessment started by the user has been completed, and the user can view the detailed report.
  - b. **In progress:** This means that the assessment is currently being performed.
  - c. **Failed:** This means that an error occurred either on the server side or on the email gateway, but it does not necessarily mean that the payloads failed to perform their functions. The developers will be notified, and they will investigate and resolve the issue.
- v. **Date Column:** This column displays the date and time when the assessment was started.
- vi. **PDF column:** This column allows the user to download a PDF report of the assessment only after it has been completed.
- vii. **Action Column:** This column allows the user to relaunch the same assessment.

### 5.3.2. Viewing the Assessment Report

To see the report of the assessment, users must perform the following steps:

1. Select the “Report” tab.

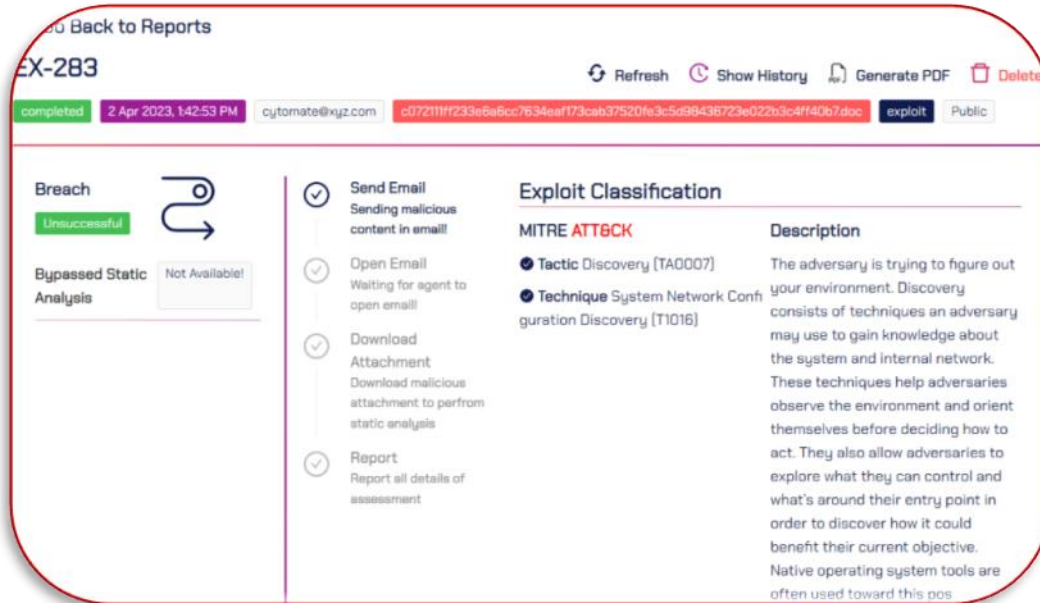
Name	Domain	Tactic	Tags	Status	Date	PDF	Action
EX-289	xgi.com	Discovery	Public	Completed	2 Apr 2023, 142:53 PM	 Generate PDF	 Launch Again
EX-282	xgi.com	Evaluation	Public	Completed	27 Mar 2023, 4:50:20 PM	 Generate PDF	 Launch Again

2. In the report section, locate the name of the exploit or behavior in that you wish to view a detailed report.
3. Click on the name of the payload for further details.



### 5.3.3. Behavior (Payload) report

1. It will open a new window that displays a detailed report of the exploit behavior.



2. At the top of the report, there is a navigation button that allows the user to go back to the "All Reports" page.

← Go Back to Reports

3. Following the navigation button, there are action buttons alongside the behavior name that serve different purposes, as explained below:



- i. **Show History:** this allows the user to view all previous assessments that were done using this exploit. Click the "Open Report" option to view the assessment report.



- ii. **Generate PDF:** this allows the user to download the report in PDF format.
- iii. **Delete:** allows the user to delete any item they wish.



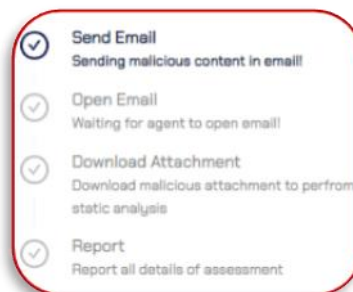
4. Below the action button, there is a detailed assessment section that includes information about the status of the assessment, the date and time when the assessment started, the email that was used for the assessment, and the type of exploit used for the assessment.



5. The next section is the breach status, which shows the status of analyses. Possible statuses are:
  - i. **Successful:** if the analysis was successful.
  - ii. **Un Successful:** if any of the analyses, either static or dynamic, failed.
  - iii. **Not Available:** It means the payloads didn't bypass the security controls or the exploit did not work correctly



6. The center of the window displays the "Server Tasks List," which shows the stages of assessment. These are:
  - i. **Send Email** means the server is collecting the malicious contents from emails to analyze the behaviors or compiling them.
  - ii. **Open Email:** the server is sending the request and waiting for an agent to open the email.
  - iii. **Download Attachment:** it means the server is wrapping up the malicious attachment to perform static analysis and cleaning the environment on both the email gateway and server.
  - iv. **Report:** server is waiting for an agent to report the details the of assessment.



7. On the right side of the window, the Exploit Classification based on the MITRE ATT&CK framework is shown, containing information about the tactic and technique of the exploit, along with a brief description.



#### Exploit Classification

MITRE **ATT&CK**

- ✔ **Tactic** Discovery (TA0007)
- ✔ **Technique** System Network Configuration Discovery (T1016)

### 5.3.4. Mitigations

Based on the identified findings and associated risks, Breach+ also offers suggestions for actionable mitigations that organizations can implement to avoid potential threats. This report provides valuable guidance for organizations to ensure they have a comprehensive understanding of the risks they face and the measures they can take to protect against them.

1. Navigate to the “Mitigation” tab

Mitigation

Strategy	Category	Description	Effectiveness	Mitigate Code Execution	Mitigate Network Propagation	Mitigate Data Exfiltration
Disable or control macros in Microsoft Office files	Attachment Filtering	An increase in the use of macros in Microsoft Office files being used as a malware delivery vector has been observed. These macros are written in the Visual Basic for Applications (VBA) programming language, a feature built into Microsoft Office applications. Macros are commonly used for task automation; however, adversaries are also using macros to perform a variety of malicious activities including the download and execution of malware on the host computer. Organizations should configure Microsoft Office to disable all macros by default and only run macros vetted as trustworthy and placed in 'trusted locations' which typical low-privileged users can't write to.	Very High	true	false	false

### 5.4. Scheduled Assessments

1. Navigate to the “Scheduled Assessment” tab located in the “Email Gateway” sub-menu to view all scheduled assessments.

Overview Assessment Reports **Schedule Assessment**

Search

Refresh

Delete

<div><div></div></div> Name	Scheduled Date	Status	<div><div></div></div> Details
<div><div></div></div> xyz.com	3 Apr 2023, 1:00:00 AM	<div>scheduled</div>	<div><div></div></div>

2. To view additional details about a specific assessment, click on the "Eye" icon located in the "Details" column. A pop-up window will appear with information about the selected exploits for the assessment.



3. The following actions can be performed on the selected assessments:
  - i. **Delete:** If a scheduled assessment is no longer needed, select the assessment by checkbox and click the delete button to remove it from the list.

## IV. ENDPOINT SECURITY

### 1. Technical Detail of Endpoint Security

In today's digital landscape, organizations face a growing threat of cyberattacks, making it imperative for them to implement robust security measures to protect their sensitive data. An Endpoint Security framework, comprising of Antivirus (AV), Endpoint Detection and Response (EDR), or Endpoint Protection Platform (EPP), can serve as a powerful defense line against malicious actors. However, user workstations within a network domain can serve as easy entry points for attackers, and in cases where the Endpoint Security framework falls short, the likelihood of a successful cyberattack increase.

#### 1.1. The Importance of Endpoint Security

For instance, a common endpoint security threat is a ransomware attack, where attackers use malicious software to encrypt an organization's data and demand a ransom in exchange for the decryption key. Breach+ offers a framework as Endpoint Security module. This module ensures organizations can perform controlled real-ransomware, Trojan Horse, worms, spyware, adware, virus, botnet, rootkit, and other malware attack tests securely and safely.

## 1.2. Introducing Breach+ Endpoint Security: The Solution to Endpoint Security Challenges

This task determines if organization security products are strong enough to protect endpoint nodes. It can also consider signature-based antivirus detection. After the assessment completion, the reports are generated in a simple format that is easy to understand. Organizations can view the security state of each endpoint and take action to upgrade endpoints. Endpoint security may be vulnerable to OS (operating system) patches and third-party software. There are many types of malwares, each designed to achieve different malicious goals. Here are some common types of malwares:

- i. **Virus:** A virus is a malicious program that replicates itself and infects other programs or files on a computer.



- ii. **Worm:** A worm is a self-replicating malware that spreads through networks and can cause widespread damage.



- iii. **Trojan:** A Trojan is a type of malware that disguises itself as legitimate software but is designed to harm a computer system or steal data.



- iv. **Spyware:** Spyware is a type of malware that collects information about a user's activity without their knowledge or consent.





- v. **Rootkit:** A rootkit is a type of malware that allows an attacker to maintain unauthorized access to a computer system while hiding their presence from detection.



- vi. **Botnet:** A botnet is a network of infected computers controlled by a central server, often used to carry out distributed denial of service (DDoS) attacks or spam campaigns.



Upon completion of the assessment, the generated reports are presented in a concise and understandable format. These reports offer organizations an overview of the security state of each endpoint and enable them to take proactive measures to address any security issues. In addition, the reports provide specific mitigations for each identified threat, based on the type of attack detected.

While Endpoint Security frameworks are essential for protecting against cyber threats, they may be vulnerable to exploitation via OS patches and third-party software. Mitigations can help in Regular and timely updates of these components, coupled with hard security protocols, and enhance the overall security posture of an organization.



Windows Agent



Linux Agent

### 1.3. Benefits of Breach+ Endpoint Security

- i. Basic and advanced scenarios running on a dedicated workstation inside the internal network with no user interaction.
- ii. Mimicking real behavior of malware such as ransomware, computer worms, and Trojans.
- iii. Breach+ agent cleans all remaining “malicious” content once the assessment is over.
- iv. Use custom and undetectable exploits to determine if the endpoint security can detect and prevent simulated attacks.
- v. No execution is done in case of Public malware.

Execution of custom commands mapped to MITRE ATT&CK tactics. This comprehensive framework emulates real-world attacks and tests the effectiveness of endpoint security controls.



## 2. User Manual of Endpoint Security

### Scope of the Manual

In this section, we will explain what Cytomate Breach+ Endpoint Security is and how it can protect your computer if you are using Windows or Linux operating systems. We will also outline the necessary hardware and software requirements that you need to have on your computer to use Breach+ Endpoint Security properly.

### Definitions

#### 2.1. Endpoint (Security)

The devices or machines on which the Cytomate Breach+ Agent is installed and actively run test cases. The agent provides continuous evaluation of the security status of each endpoint, generating alerts and notifications when any security risks are detected.

#### 2.2. Cytomate Agent

Cytomate Breach+ relies on a lightweight agent known as the "BreachPlusAgent" to evaluate the security of the email gateway. You can choose the operating system "Windows or Linux" for the system agent which enables communication with Cytomate Breach+.

#### 2.3. Cytomate Breach+

Cytomate Breach+ is a Breach and Attack Simulation (BAS) solution that emulates, assesses, and validates the most recent attack tactics used by Advanced Persistent Threats (APTs) and other hostile groups.

## 3. Endpoint Security Assessment

Endpoint Security Assessment is a critical process that evaluates and tests the security controls of computer networks to protect against various cyber threats. By performing an endpoint security assessment, organizations can identify vulnerabilities and weaknesses in their security infrastructure and implement necessary measures to secure

their networks.

### **3.1. Breach+ Endpoint Security Assessment**

Breach+ Endpoint Security solution is a comprehensive security solution that offers advanced features to protect against different types of malwares, ransomware, worms, and trojans. The solution includes endpoint security assessment, which allows organizations to deploy and run real ransomware, Trojans, worms, and viruses on a dedicated endpoint in a controlled and safe manner. This comprehensive testing covers all aspects of endpoint security, including virus detection, known vulnerabilities detection, and behavioral changes detection.

### **3.2. Breach+ Endpoint Security Assessment & MITRE ATT&CK Tactics**

Breach+ Endpoint Security solution provides advanced security features to protect against various malware, ransomware, worms, and trojans. The solution also offers endpoint security assessment using the MITRE ATT&CK tactics to evaluate the strength of the corporate endpoint security controls.

The MITRE ATT&CK tactics provide a comprehensive framework to simulate real-world attacks and test the effectiveness of endpoint security controls. Breach+ endpoint module uses these tactics, which include but are not limited to Initial Access, Persistence, Lateral Movement, Defense Evasion, Collection, Privilege Escalation, Credential Access, Reconnaissance, Discovery, Command and Control, Execution, and Impact. The module also uses custom and undetected exploits to determine if the endpoint security can detect and prevent the simulated attacks.

The entire endpoint security assessment process is performed in a secure and confidential manner, with utmost consideration of the privacy of the client organization. The results of the assessment are then used to provide actionable mitigations to protect against the weaker security areas.

Breach+ endpoint module employs various techniques beyond the MITRE ATT&CK tactics to test endpoint security controls and identify any vulnerabilities or weaknesses in the security defenses. This approach enables the solution to provide comprehensive endpoint security assessment and ensure that the organization's endpoints are secure from potential threats.

By using the MITRE ATT&CK tactics, along with other techniques, Breach+ Endpoint Security solution provides a comprehensive and reliable endpoint security assessment to help organizations identify and address potential security gaps in their endpoint security defenses.

## 4. Hardware and Software Requirements

To use Breach+ Endpoint Security solution, the following hardware and software requirements must be met:

### 4.1. Breach+ Agent

The solution includes a lightweight agent that is installed on the endpoint and communicates with the Breach+. This agent is used by breach+ to test corporate endpoint security controls and identify any vulnerabilities or weaknesses in the security defenses.

To download and install the agent, please refer to the agent installation guide. This guide provides detailed instructions on how to install and configure the agent to start using the endpoint security solution.

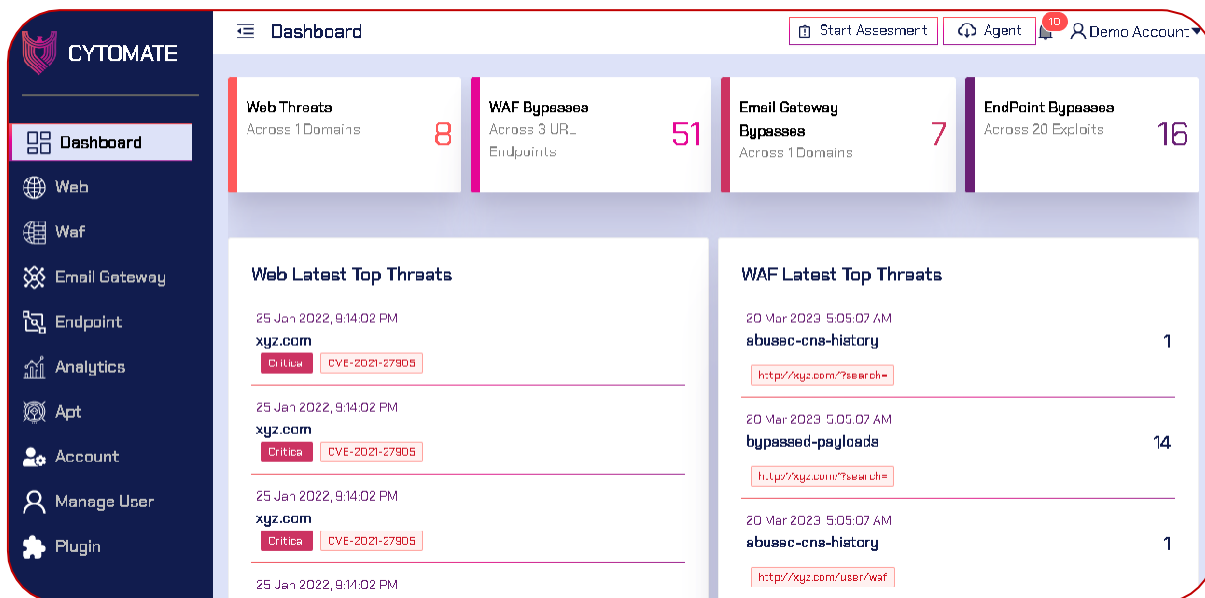
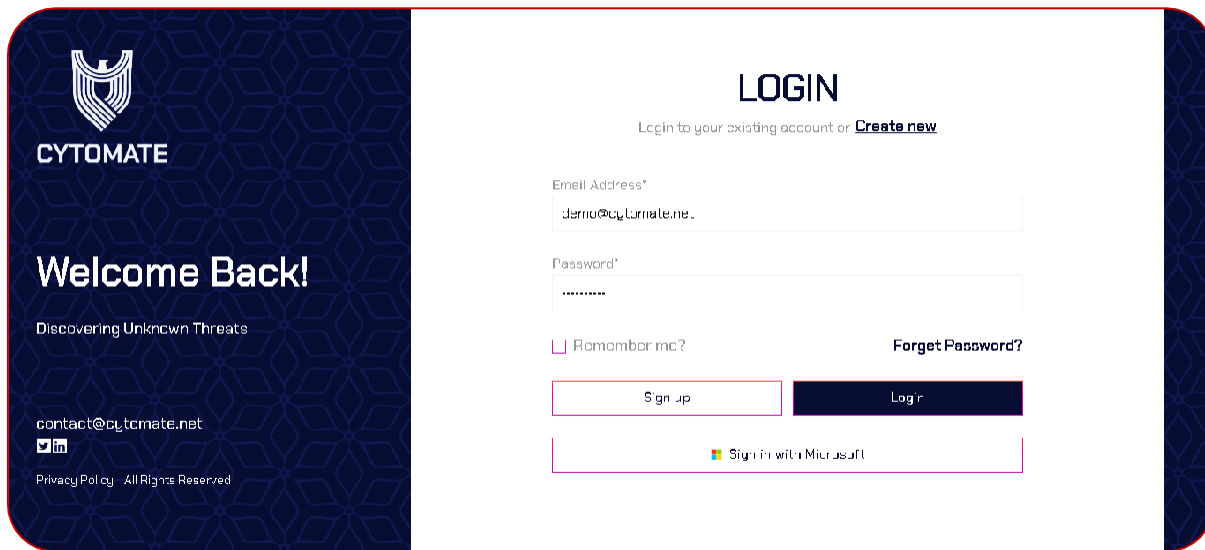
## 5. Features and Functionalities

This section provides an interactive demonstration of breach+ Endpoint Security solution features and functionalities. Through the use of screenshots and step-by-step instructions, users can learn how to effectively use the solution to protect their endpoints. By the end of this section, users will have a thorough understanding of how to use breach+ Endpoint Security solution to enhance endpoint protection against potential threats.

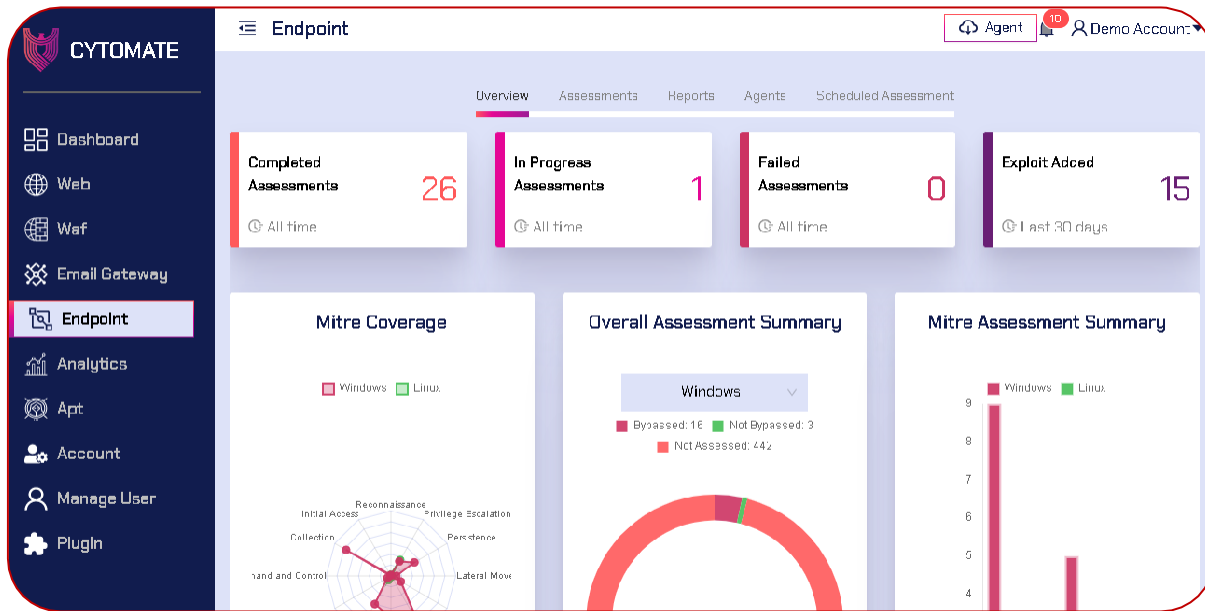
### 5.1. Breach+ Endpoint Security Solution

To start using the Breach+ Endpoint Security Solution, follow these steps:

- i. Go to the Breach+ portal at <https://apt.cytomate.net/> (Use Google Chrome for the best experience.)
- ii. Enter your credentials and click "Login" to access the Breach+ dashboard.



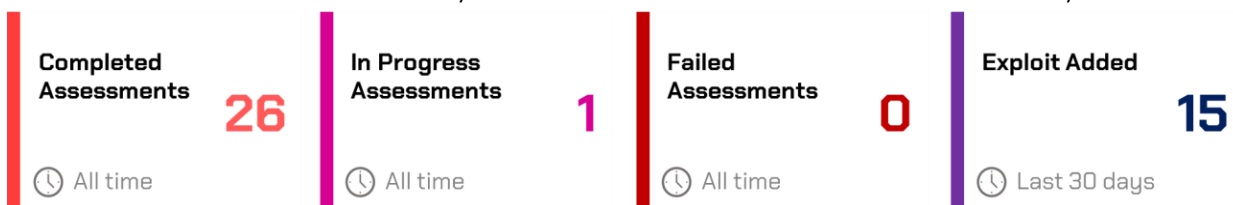
- iii. Click on “Endpoint” from the side menu to open the dedicated dashboard for Endpoint Security Assessments.



- vi. At the top of the dashboard, you will find five different tabs, each offering unique functionalities and features. The current active tab is "Overview," which displays an overview of the endpoint assessment details in the form of widgets and graphs.

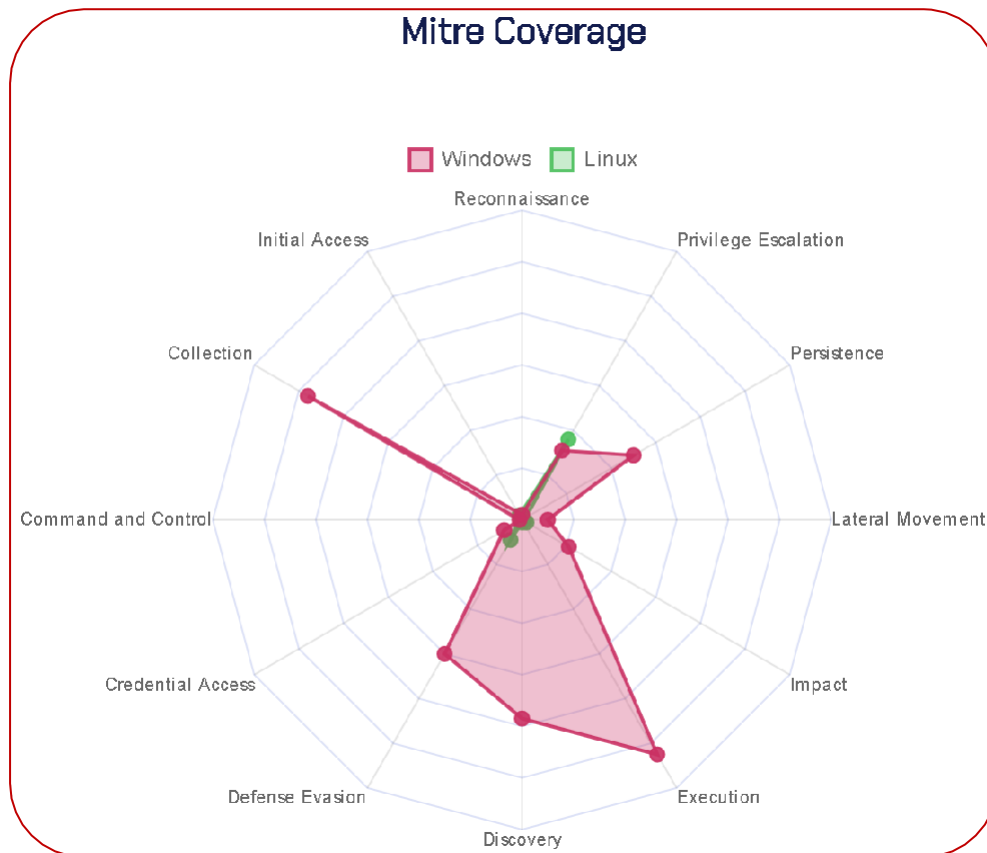


- vii. In the "Overview" tab, there are four top widgets that provide a quick view of the endpoint assessment details. These widgets include:
- **Completed Assessments:** This widget contains information on how many total assessments have been successfully completed by the user since the account was created.
  - **In Progress Assessments:** This widget displays how many assessments by the user are currently in progress since the account was created.
  - **Failed Assessments:** This widget contains information on how many total assessments have failed since the account was created.
  - **Exploit Added:** This widget contains information on how many new exploits have been added by Breach+ that can be used for assessments by the user.

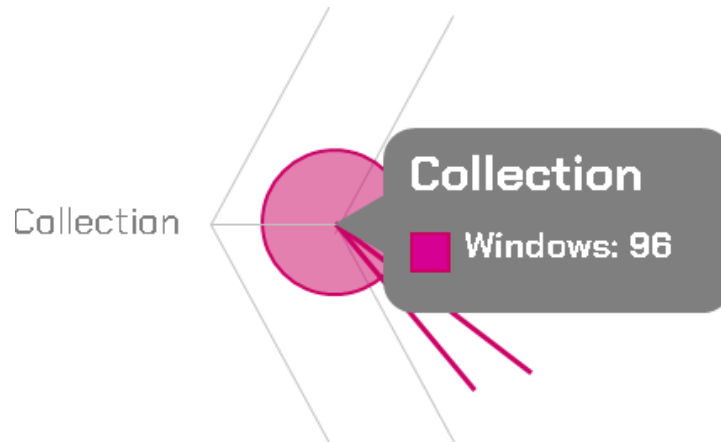


viii. After the widgets section, three interactive graphs are displayed to provide detailed information. These graphs are explained below:

- **MITRE Coverage:** This interactive radar graph displays the number of total exploits developed by breach+ for both Linux and Windows operating systems based on the Tactics of MITRE ATT&CK Framework



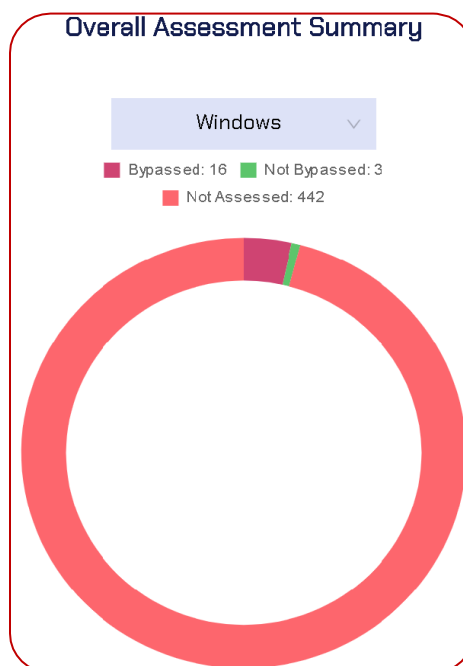
- The dots on the graph represent the number of exploits in the respective tactic and operating system, which can be viewed by hovering the cursor over them.



- ii. Moreover, users can apply filters to the graphs based on the operating system using toggle buttons displayed as legends on the graph.



- **Overall Assessment Summary:** This Pie Doughnut graph displays the overall summary of all exploits used by the client and shows statistics about exploits that Bypassed, Not Bypassed, and Not Assessed out of all available exploits.

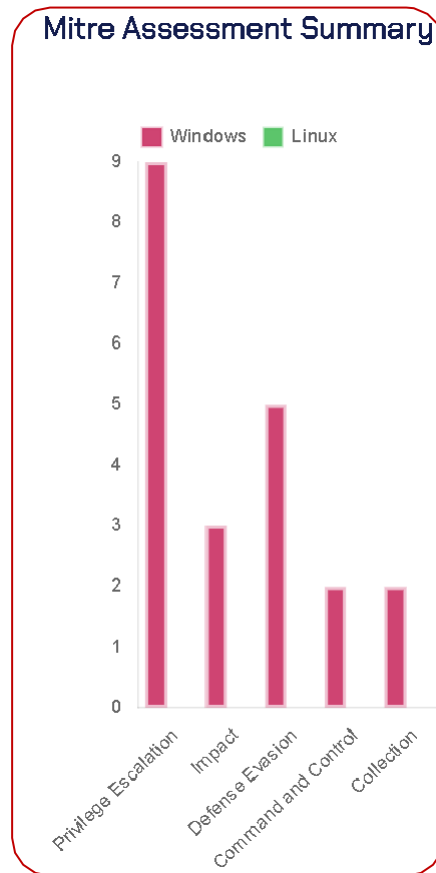




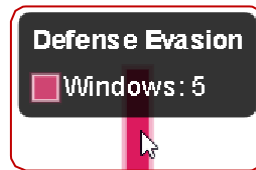
- i. Green Color indicates that client's endpoint security defenses successfully defended against those exploits, while red color shows the number of exploits that bypassed the security defenses and hence marked as danger.
- ii. A filter is available at the top of the graph, allowing users to see the statistics for the operating system of their choice, such as Windows or Linux.



- iii. **MITRE Assessment Summary:** This chart presents a comprehensive display of successful exploits that have bypassed the Windows or Linux operating systems, based on the Mitre Tactics.



- iv. By hovering over the chart bars, users can see information on the counts of each tactic's bypassed exploits.

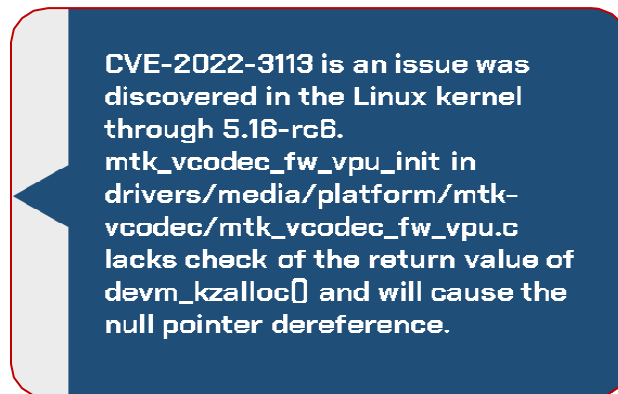


### 5.1.1. Assessments

The "Assessments" tab within the Endpoint module allows clients to evaluate the effectiveness of their Endpoint Security Controls by conducting assessments using breach+ exploits.

#### 1. Column Details

- A. **Name Column:** This column contains the name of each exploit also known as behavior.



- B. **Description Column:** This column contains the description of each exploit, and it can be seen by hovering the cursor over the details.
- C. **Tactic Column:** This column contains information about the tactic, technique and sub-technique of each exploit that can be seen by hovering over the cursor on the tactic name. Further, the Tactic Filter allows filtering out exploits based on MITRE tactics and then selecting from those exploits.



The screenshot shows a web interface with a list of categories on the left and a selected category on the right. The categories on the left are: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, and Credential Access. The 'Defense Evasion' category is selected, and a tooltip is displayed next to it. The tooltip contains the text: 'Technique: Exploitation for Privilege Escalation' and 'Sub Technique: Not available'. The selected category 'Privilege Escalation' is highlighted in a pink box on the right.

D. **Category Column:** This column infers about the category of the exploit that can beany out of the given below list. Further, it also allows applying filters to select exploits based on these categories:

- **Exploit:** A program or technique used to take advantage of a vulnerability in a system, software, or application to gain unauthorized access or execute malicious code.
- **Ransomware:** A type of malware that encrypts a user's files or system anddemands payment in exchange for restoring access to the affected data.
- **Backdoor:** A hidden and unauthorized means of accessing a computer system or network, often used by hackers to gain control of a compromisedsystem.
- **Worm:** A type of malware that replicates itself to spread across networksand infect other computers, often causing damage or disrupting normalsystem operations.
- **RAT (Remote Access Trojan):** A type of malware that provides unauthorizedaccess to a victim's computer, allowing an attacker to take control of the system and perform various malicious activities.
- **Keylogger:** A type of software that records every keystroke made by a user,including passwords and sensitive data, often used by attackers to stealconfidential information.



Category

☐ exploit
☐ ransomware
☐ backdoor
☐ worm
☐ RAT
☐ keylogger

Reset
OK

- E. **Platform Column:** Displays the operating system, such as Linux or Windows, on which an exploit will run. Allows users to apply filters to select exploits for specific OS types.
- F. **Tags Column:** Contains information about exploit tags. Users can apply filters to select exploits based on three tag categories: Public, Public Customized, and Custom.
- Public: Exploits collected from the internet for static analysis without being executed by Breach+.
  - Custom: Highly advanced and sophisticated exploits developed by the Breach+ team.
- G. **Tested Column:** Allows users to filter exploits based on whether they have been used (True) or not used (False) in previous assessments.
- H. **Price Column:** Displays the price of each exploit

## 2. Steps to Start (Schedule) an Assessment

To initiate assessments, users must perform the following steps:

- Navigate to the "Assessments" tab in the "Endpoint" module.

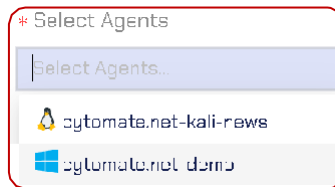
Overview
Assessments
Reports
Agents
Scheduled Assessment

\* Select Exploits

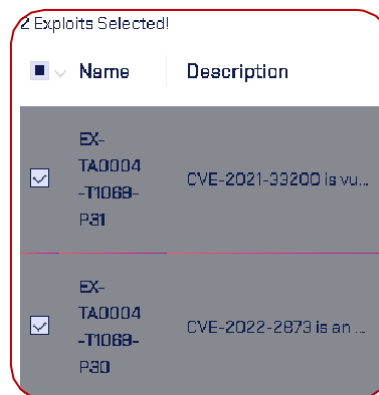
Search
Refresh

Name	Description	Tactic	Category	Platform	Tags	Tested	Price
EX-TA0004-11068-Pg1	CVE-2021-33200 is vul...	Privilege Escalation	Exploit		Custom	false	1\$

- Select the agent(s) installed on the endpoints that require assessment.



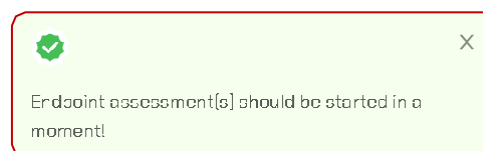
- Choose the desired exploits by selecting the checkboxes next to each exploit or using the search field to locate specific exploits.
  - Note:** Exploits can only be selected after selecting the agent(s). Filters can also be applied to select exploits. To select all exploits, check the checkbox on the left side of "Name".



- Click the "Start Assessment" button to begin the assessment process.



- Wait for a pop-up notification that indicates the assessment has started.



- To schedule an assessment for a later time or date, follow the above steps but select the desired date and time from the calendar.



2 Exploits Selected

Name	Description
EX-TA0004-T1068-P31	CVE-2021-33200 is vulner...

\* Select Agents

+ 1 ...

Start Assessment

Schedule

2023-03-19 15:31:51

Mar 2023

Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

Now

OK

- Wait for a pop-up message indicating the successful scheduling of the assessment.

Endpoint assessment will start at March 31st 2023, 15:37:19!

### 5.1.2. Reports

The "Endpoint" contains a tab called "Reports" that provides you with detailed information on all assessments, including both normal and scheduled assessments. This tab allows you to view and analyze the results of your assessments in a more detailed manner.

To access the Reports section, simply navigate to the "Endpoint" tab and click on the "Reports" sub-tab. From here, you can view a list of all assessments, including their names and relevant information. To view the detailed report of any assessment, simply click on the name of the report.

Once you click on the report name, a new page will open, displaying the detailed report for the selected assessment. This report will provide you with in-depth information about the assessment, including any relevant data, graphs, and other visual aids.

Name	Description	Agent	Tactic	Status	Date	PDF	Action
80-TA0005-T1055-S005-P1	This is a malware that...	Uemen Sikander	Defense Evasion	completed	7 Mar 2023, 10:18:14 PM	Generate PDF	Launch Again





## 1. Column Details

This section contains the same columns as the "Assessments" tab, with the exception of the following:

- A. **Agent Column:** This column displays information about the agent that was selected by the user to run an assessment on a specific endpoint. In other words, it indicates which endpoint the assessment was performed on.
- B. **Status Column:** This column displays information about the status of the assessment, including:
  - Completed: This means that the assessment started by the user has been successfully completed, and the user can view the detailed report.
  - In progress: This means that the assessment is currently being performed.
  - Failed: This means that an error occurred either on the server side or on the endpoint, but it does not necessarily mean that the exploit failed to perform its functions. The developers will be notified, and they will investigate and resolve the issue.
- C. **Date Column:** This column displays the date and time when the assessment was started.
- D. **PDF column:** This column allows the user to download a PDF report of the assessment only after it has been successfully completed.
- E. **Action Column:** This column allows the user to relaunch the same assessment.

## 2. Viewing the Assessment Report

To see the report of assessment, users must perform the following steps:

- Select the "Reports" tab

<input type="checkbox"/> Name	Description	Agent	Tactic	Status	Date	PDF	Action
<input type="checkbox"/> 80-TA0005-T1055-5005-P1	This is a malware that...	Uman Silkander	Defense Evasion	completed	7 Mar 2023, 10:18:14 PM	Generate PDF	Launch Again

- In the Reports section, locate the Name of the exploit or behavior that you wish to view a detailed report for.
- Click on the Name of the exploit for a detailed report.





### 3. Behavior (exploit) Report

[Go Back to Reports](#)

**BD-TA0005-T1055-S005-P1**
Refresh
Show History
Generate PDF
Delete

Completed
7 Mar 2023, 10:10:14 PM
Agent: Usman S'kander
backdoor
Custom

**Breach**  
Successful

**Bypassed Static Analysis**  
Successful

**Bypassed Dynamic Analysis**  
Successful

Pre Attack  
Preparing attack arsenal.

C2  
Starting c2 listener.

Agent  
Waiting for agent to execute attack.

Post Attack  
Wrapping attack and cleaning environment.

**Exploit Classification**

MITRE ATT&CK	Description
<b>Tactic:</b> Defense Evasion (TA0005)	This is a malware that injects malicious shellcode into legitimate processes using
<b>Technique:</b> Process Injection (T1055)	Callback Function
<b>Sub-technique:</b> Thread Local Storage (S005)	

- It will open a new window that displays a detailed report of the behavior.
- At the top of the report, there is a navigation button that allows the user to go back to the "All Reports" page.

[Go Back to Reports](#)

- Following the navigation button, there are action buttons alongside the behavior name that serve different purposes, as explained below:

Behavior (exploit) name
To refresh the report
To delete report

**BD-TA0005-T1055-S005-P1**
Refresh
Show History
Generate PDF
Delete

To see history of assessment
To get pdf report

- Show History: allows the user to view all previous assessments that were done using this exploit.





## Endpoint Assessment History

<input type="checkbox"/>	Sr. No.	Date	Status	Action
<input type="checkbox"/>	1	7 Mar 2023, 10:18:14 PM	completed	<a href="#">Open Report</a>

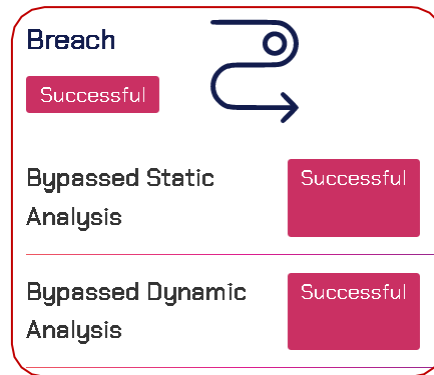
< 1 > 6 / page ▾

- b. **Generate PDF:** allows the user to download the report in PDF format.
- c. **Delete:** allows the user to delete any item they wish, anywhere in Breach+ Endpoint.
- d. **Refresh:** can be used to refresh the report in case of issues while loading.
- Below the action buttons, there is a detailed assessment section that includes information about the status of the assessment, the date and time when the assessment started, the agent name, the type of exploit used for assessment, and the tag.

completed	7 Mar 2023, 10:18:14 PM	Agent: Usman Sikander	backdoor	Custom
-----------	-------------------------	-----------------------	----------	--------

- The next section is the breach status, which shows the status of analyses. Possible statuses are:
  - a. **Successful:** if the analysis was successful.
  - b. **Unsuccessful:** if any of the analysis, either static or dynamic, failed.
  - c. **Not Available:** It means the exploits didn't bypass the security controls or the exploit did not work correctly.





- The center of the window displays the "Server Tasks List," which shows the stages of assessment. These are:
  - a. Pre-Attack: it means the server is collecting the exploit from the collection of behaviors or compiling it.
  - b. Agent: the server is sending that exploit to the selected agent.
  - c. Post-Attack: it means the server is wrapping up the attack and cleaning the environment on both endpoint and server.



- On the right side of the window, the Exploit Classification based on the MITRE ATT&CK framework is shown, containing information about the tactic, technique, and sub-technique of the exploit, along with a brief description.



## Exploit Classification

### MITRE **ATT&CK**

- ✓ **Tactic:** Defense Evasion [TA0005]
- ✓ **Technique:** Process Injection [T1055]
- ✓ **Sub\_technique:** Thread Local Storage [S005]

### Description

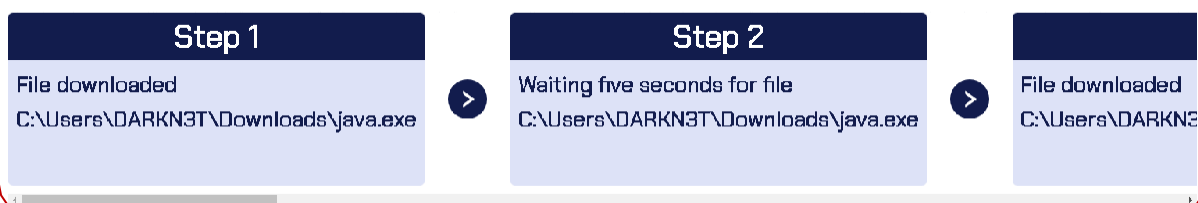
This is a malware that injects malicious shellcode into legitimate processes using Callback Function

## 4. Attack Path

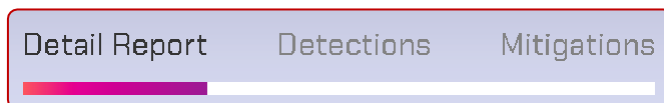
The Attack Path refers to the sequence of steps taken by an exploit to successfully execute.

- The Detailed Attack Path provides a step-by-step account of the exploit's actions, from its initial download to its successful execution.

### Exploit Attack Path



- Following the Attack Path section, the user can access a sub-menu that provides additional details such as a comprehensive report, instructions for detecting the exploit, and effective mitigation strategies to counter such malicious behavior.



## 5. Detailed Report

In addition to the exploit report, a detailed JSON version of the report is also provided to users for further analysis. The detailed report includes actionable intelligence, and evidence of successful execution of the exploit on the targeted endpoint.





## 6. Evidence

- The left window provides users with detailed evidence, such as any commands that the exploit was expected to run, and their respective responses.
- If the exploit was aimed at downloading a malicious file from the internet, the path of the file is provided, among other details.
  - a. Note: these details may vary from exploit to exploit based on its nature and behavior.

### Evidence

- command: systeminfo
- output: systeminfo Host Name: DESKTOP-79P1C73  
OS Name: Microsoft Windows 10 Pro OS Version: 10.0.19045 N/A Build 19045 OS Manufacturer: Microsoft Corporation OS Configuration: Standalone Workstation OS Build Type: Multiprocessor Free Registered Owner: DARKN3T Registered Organization: Product ID: 00330-80000-00000-AA188 Original Install Date: 11/24/2022, 4:38:46 PM

## 7. Report JSON View

- Users can find a detailed report of the exploit in JSON format on the right side window after evidence. Clicking on the copy button against each key allows users to easily copy the values of the keys. The full report can be copied using the copy icon present on the first line of the report.



### Report Json View

```

{
  "Report": {
    "dynamic_analysis_bypassed": true,
    "metasploit_session_created": true,
    "overall_bypassed": true,
    "trace_file": {
      "attack_index": 0,
      "file_path": "C:\\Users\\DARKN3T\\Downloads\\golden-jerboa-from-hell...",
      "static_analysis_bypassed": true
    }
  }
}

```

## 8. Detection

- This sub-tab provides actionable details on how to detect a particular exploitor behavior.

Detail Report **Detections** Mitigations

Strategy	Description
Mitre	Windows API calls such as CreateRemoteThread, SuspendThread/SetThreadContext/ResumeThread, and those that can be used to modify memory within another process, such as VirtualAllocEx/WriteProcessMemory, may be used for this technique.
Process monitoring	Process monitoring is a minimum requirement for reliably detecting Process Injection. Even though injection can be invisible to some forms of process monitoring, the effects of the injection become harder to miss once you compare process behaviors against expected functionality.

## 9. Mitigations

- This tab appears only if the exploit successfully bypasses the security controls, and the breach result is "Successful." It contains steps and guidelines that the user must follow as a remedy or threat mitigation solution to mitigate the exploit and protect the endpoint from further exploitation in



the future.

Detail Report   Detections   Mitigations

Strategy	Description
Mitra	Install anti-malware with heuristics capabilities or endpoint detection and response (EDR) products. These products use API hooking to detect Windows API calls commonly used by malware authors. Combined with heuristics and machine learning, they have the capability to detect suspicious process injections and alert the user as it happens.
Application control	Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts. An appropriately configured implementation of application control helps to prevent the undesired execution of software regardless of whether the software was downloaded from a website, clicked on as an email attachment or introduced via CD/DVD/USB removable storage media. A very basic implementation to mitigate some unsophisticated malware from running involves using application control or filesystem permissions to block execution from user profile directories. Such directories include %AppData%, %LocalAppData%, their subdirectories, as well as %TEMP%.

## 10. Agents

- Next tab in sub-menu of endpoint is “Agent” that contains information about all of the installed agents by the user on the endpoints.

Overview   Assessments   Reports   Agents   Scheduled Assessment

- To rename the agent, select agent from the list of agents and click on the “Edit” button.

Name	Mac Address	Platform	Created On	Modify
cytomate.net-DESKTOP-KOUVV35	8C1845B082A9		21 Mar 2023, 1:12:38 AM	<button>Edit</button>

- A pop-up window will appear where you can change the name. Click on the Update button to apply the changes.





### Edit Agent

\* Name

cytomate.net-demo

\* Mac Address

8C1645B0B2A9

\* System Name

DESKTOP-KOUVV35

Platform

Windows

Update

- Finally, the updated agent name will be visible under the "Agents" tab and on the agent itself.

	cytomate.net-demo	8C1645B0B2A9		21 Mar 2023, 1:12:39 AM	Edit
--	-------------------	--------------	--	-------------------------	------

## 11. Scheduled Assessments

- Navigate to the "Scheduled Assessments" tab located in the "Endpoint" sub-menu to view all scheduled assessments.

Overview

Assessments

Reports

Agents

Scheduled Assessment

▼

Name

Scheduled Date

Status

▼

Details

1 assessments scheduled across 1 agents

31 Mar 2023, 3:37:19 PM

scheduled

2 assessments scheduled across 1 agents

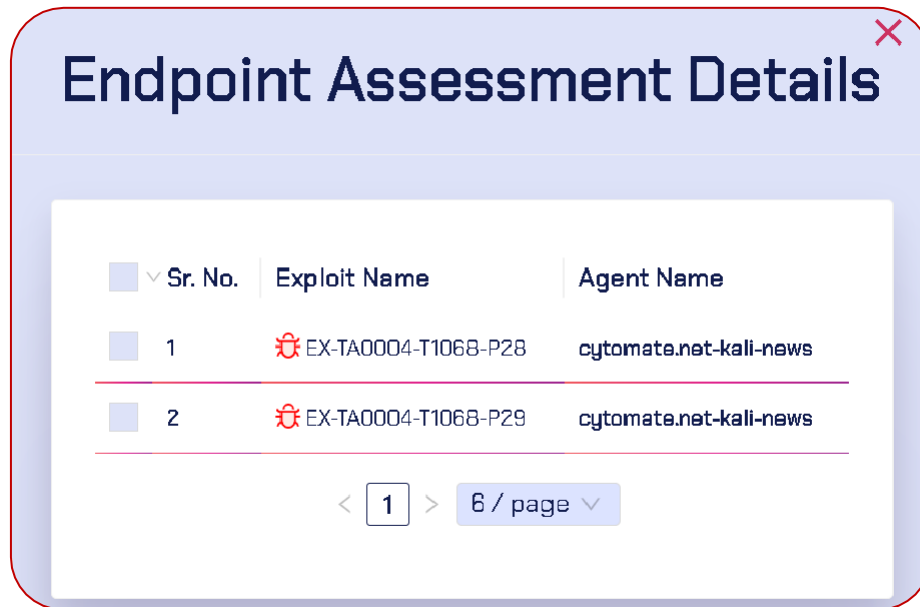
31 Mar 2023, 4:12:34 PM

scheduled

- To view additional details about a specific assessment, click on the "Eye" icon



located in the "Details" column. A pop-up window will appear with information about the selected exploits for the assessment.



- The following actions can be performed on the selected assessments:
  - Delete: If a scheduled assessment is no longer needed, select the assessment by checkbox and click the delete button to remove it from the list.

Refresh: Click the refresh button to update the assessments list and view any new scheduled assessments.

## 5.2. Breach+ Campaign Security Assessment

### 5.2.1. Campaign Overview

#### Definition:

Campaigns are basically a sequence of malware behaviors or test-cases that have been extracted from a real-world malware sample.

Malware analysis is a critical component of our services. Our team uses advances tools and techniques to dissect malicious code and determine its intended behavior. By understanding the TTPs used by the malware, we can identify the specific techniques that the attackers have used to compromise a system, exfiltrate data, or otherwise achieve their objectives. The main purpose of malware analysis is to uncover latest attack paths from malware-in-the-wild which we recreate



into safe **test-cases** that we call “**behaviors**” to emulate the whole malware and check the response of organization’s security architecture. Our TTP extraction process involves identifying various tactics used by the attackers and the techniques and procedures that they use to execute those tactics. By understanding the TTPs used by specific malware variant or attack group, we can develop effective countermeasures to protect our clients from future attacks.

Breach+ Lab analyzes latest malware-in-the-wild. We have a TTP extraction process, which include dividing the sample’s malicious behavior into multiple TTPs each mapped on MITRE ATT&CK. Once all the TTPs have been extracted from the sample, our team of malware developers recreate those TTPs using the exact way as used by malware for example: using the same API calls, or same way of coding and even using the same language it is written in. All these behaviors are then added as a **campaign** in sequence making a whole APT.

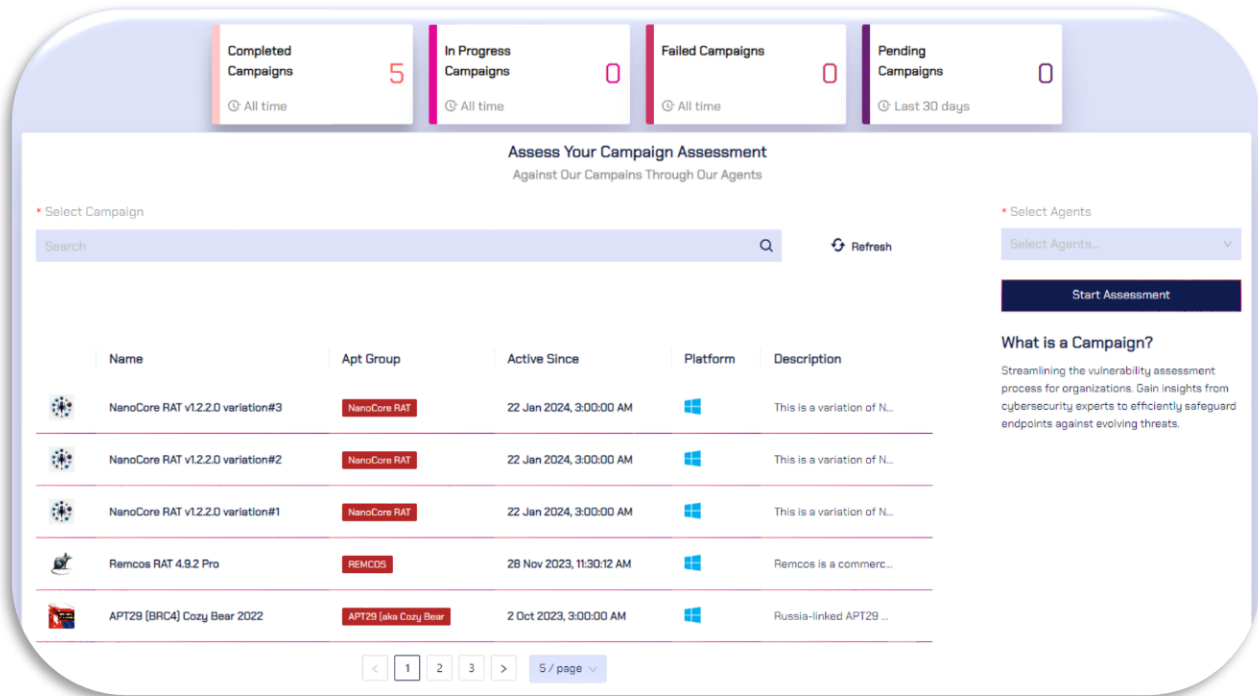
### 5.2.2. Campaign Assessments

To start using the Breach+ Campaign Security Assessment, follow these steps:

- i. Go to the Breach+ portal at <https://apt.cytomate.net/> (Use Google Chrome for the best experience.)
- ii. Enter your credentials and click "Login" to access the Breach+ dashboard.
- iii. Go to the campaigns tab on the side bar



- iv. It has a similar interface as in Endpoint assessments tab.



**Completed Campaigns** 5  
⌚ All time

**In Progress Campaigns** 0  
⌚ All time

**Failed Campaigns** 0  
⌚ All time

**Pending Campaigns** 0  
⌚ Last 30 days

**Assess Your Campaign Assessment**  
Against Our Campaigns Through Our Agents

\* Select Campaign

Search

Name	Apt Group	Active Since	Platform	Description
NanoCore RAT v1.2.2.0 variation#3	NanoCore RAT	22 Jan 2024, 3:00:00 AM	Windows	This is a variation of N...
NanoCore RAT v1.2.2.0 variation#2	NanoCore RAT	22 Jan 2024, 3:00:00 AM	Windows	This is a variation of N...
NanoCore RAT v1.2.2.0 variation#1	NanoCore RAT	22 Jan 2024, 3:00:00 AM	Windows	This is a variation of N...
Remcos RAT 4.9.2 Pro	REMCOS	28 Nov 2023, 11:30:12 AM	Windows	Remcos is a commerc...
APT29 (BRC4) Cozy Bear 2022	APT29 (aka Cozy Bear)	2 Oct 2023, 3:00:00 AM	Windows	Russia-linked APT29 ...

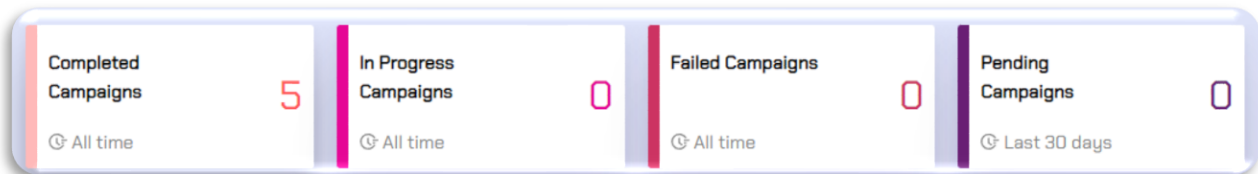
< 1 2 3 > 5 / page

\* Select Agents

Select Agents...

**What is a Campaign?**  
Streamlining the vulnerability assessment process for organizations. Gain insights from cybersecurity experts to efficiently safeguard endpoints against evolving threats.

- v. You will see the overview above. It shows all the campaigns that are completed, in progress, pending or failed



**Completed Campaigns** 5  
⌚ All time

**In Progress Campaigns** 0  
⌚ All time

**Failed Campaigns** 0  
⌚ All time

**Pending Campaigns** 0  
⌚ Last 30 days

- vi. Starting campaign assessment is very similar to starting simple Endpoint assessment. You will select the agent first









\* Select Agents

Select Agents...

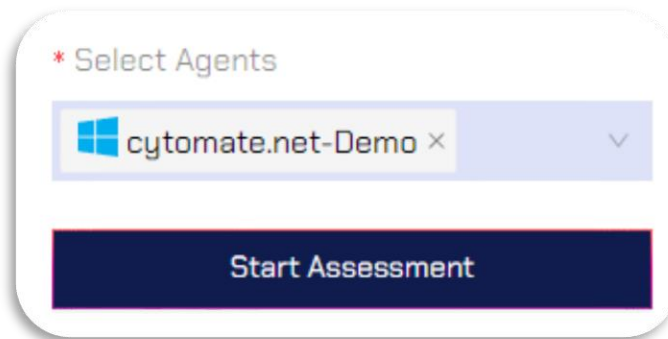
- cytomate.net-Demo
- cytomate.net-DESKTOP-UUAC3ID
- cytomate.net-kali-news
- cytomate.net-demo

- vii. Once the agent is selected, you can select the Malware campaigns that you want to test

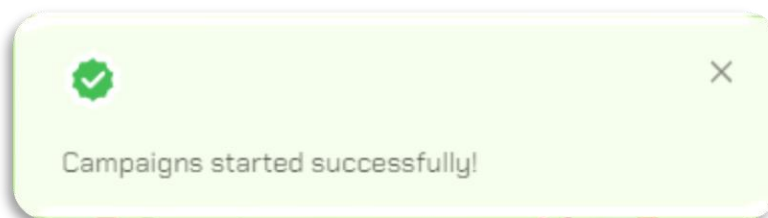
Campaign(s) Selected!

<input type="checkbox"/>	Name	Apt Group	Active Since	Platform	Description
<input checked="" type="checkbox"/>	 NanoCore RAT v1.2.2.0 variation#3	NanoCore RAT	22 Jan 2024, 3:00:00 AM		This is a variation of N...
<input type="checkbox"/>	 NanoCore RAT v1.2.2.0 variation#2	NanoCore RAT	22 Jan 2024, 3:00:00 AM		This is a variation of N...
<input type="checkbox"/>	 NanoCore RAT v1.2.2.0 variation#1	NanoCore RAT	22 Jan 2024, 3:00:00 AM		This is a variation of N...
<input checked="" type="checkbox"/>	 Remcos RAT 4.9.2 Pro	REMCOS	28 Nov 2023, 11:30:12 AM		Remcos is a commerc...
<input type="checkbox"/>	 APT29 (BRC4) Cozy Bear 2022	APT29 (aka Cozy Bear	2 Oct 2023, 3:00:00 AM		Russia-linked APT29 ...

- viii. After selecting the desired campaigns for assessment. You can start the assessment immediately by clicking on the **“Start Assessment”** button



- ix. Wait for the Notification to confirm that the assessment has been started








### 5.2.3. Campaign Reports

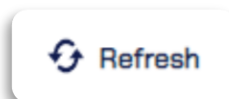
- i. To check on campaign reports. Go to the tab of Reports under Campaign tab



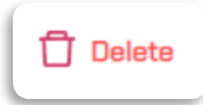
- ii. Here you can see the overall summary of all the campaigns you have assessed. The summary includes:
- Name of Campaign
  - Description of Campaign
  - Agent against which it was tested
  - Status of the campaign
    - completed**: Successfully completed
    - in progress**: It is currently being assessed
    - pending**: It is preparing for the assessment but hasn't started yet
  - Date on which it was assessed
  - Actions that define:
    - Launch assessment again
    - Generate PDF Report

Icon	Name	Description	Agent	Status	Date	Actions
	NanoCore RAT v1.2.2.0 variation#3	This is a variation of N...	cytomate.net-Demo	in progress	29 Jan 2024, 10:02:05 AM	<a href="#">Generate PDF</a> <a href="#">Launch Again</a>
	Remcos RAT 4.9.2 Pro	Remcos is a commerc...	cytomate.net-Demo	in progress	29 Jan 2024, 10:02:05 AM	<a href="#">Generate PDF</a> <a href="#">Launch Again</a>
	APT29 (BRC4) Cozy Bear 2022	Russia-linked APT29 ...	cytomate.net-THEPUNISHER	completed Partially Breached	2 Oct 2023, 2:20:57 PM	<a href="#">Generate PDF</a> <a href="#">Launch Again</a>
	NanoCore RAT v1.2.2.0	NanoCore RAT is a pot...	Win11	completed Partially Breached	24 Sep 2023, 3:59:53 PM	<a href="#">Generate PDF</a> <a href="#">Launch Again</a>
	MAR-10158513.r1v1 – SamSam Ransomware	This campaign fully e...	cytomate.net-THEPUNISHER	completed Breached	18 Sep 2023, 1:30:16 PM	<a href="#">Generate PDF</a> <a href="#">Launch Again</a>

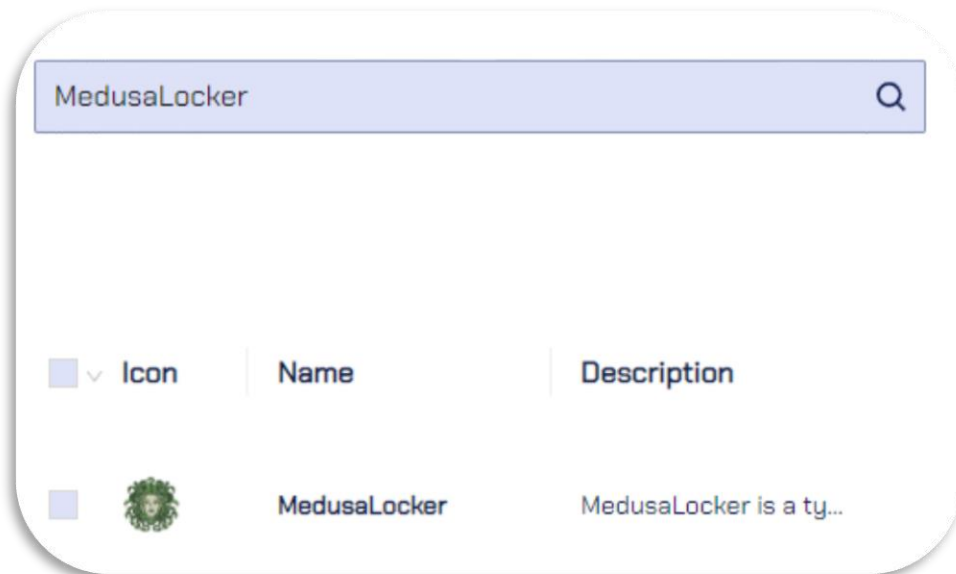
- iii. From this tab, you can Refresh the tab to get updated status



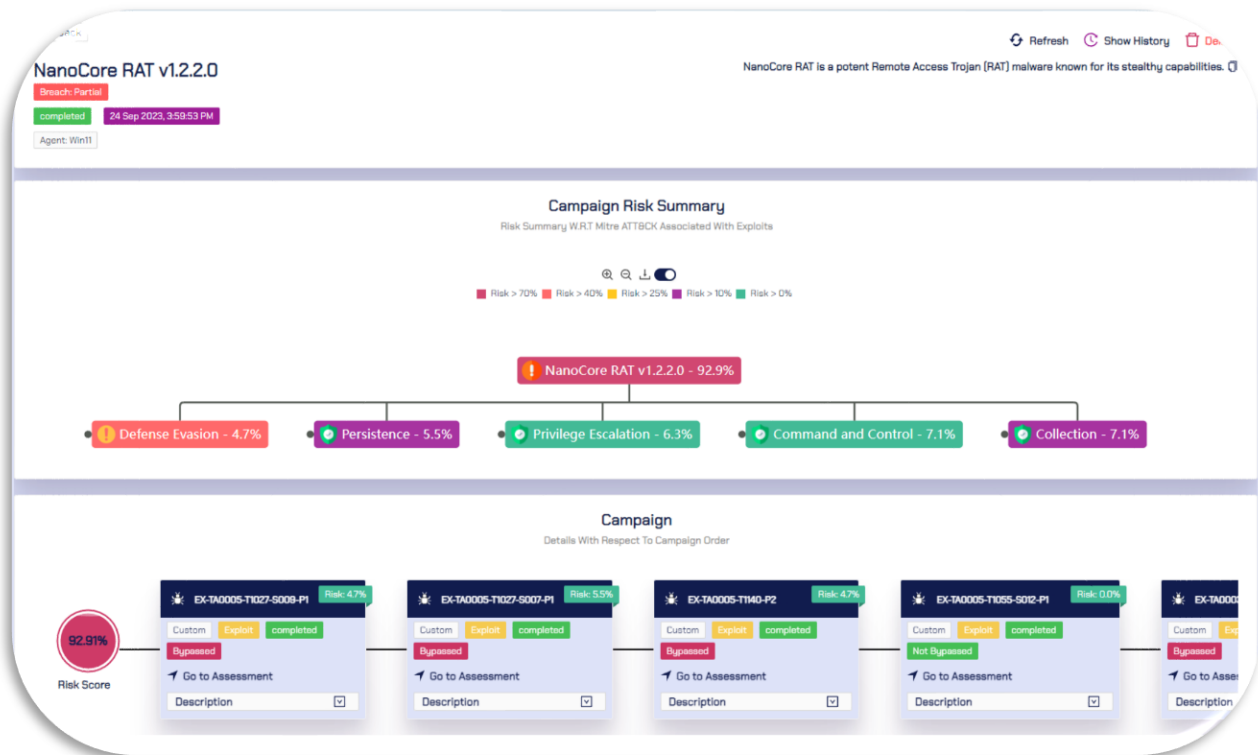
- iv. From this tab, you can select any campaigns and delete



- v. From this tab, you can search for any specific campaigns



- vi. To view detailed reports of Campaigns. Click on any campaign



vii. The campaign report contains following key information:

1. Breach:

- Successful: Every TTP is breached
- Partial: Some of the test cases have been breached and some of them have been prevented
- Unsuccessful: Every TTP has been prevented

**Breach: Partial**

2. Status:

- completed
- failed
- in progress
- pending

**completed**

3. Date

**5 Oct 2023, 11:00:13 AM**

#### 4. Agent

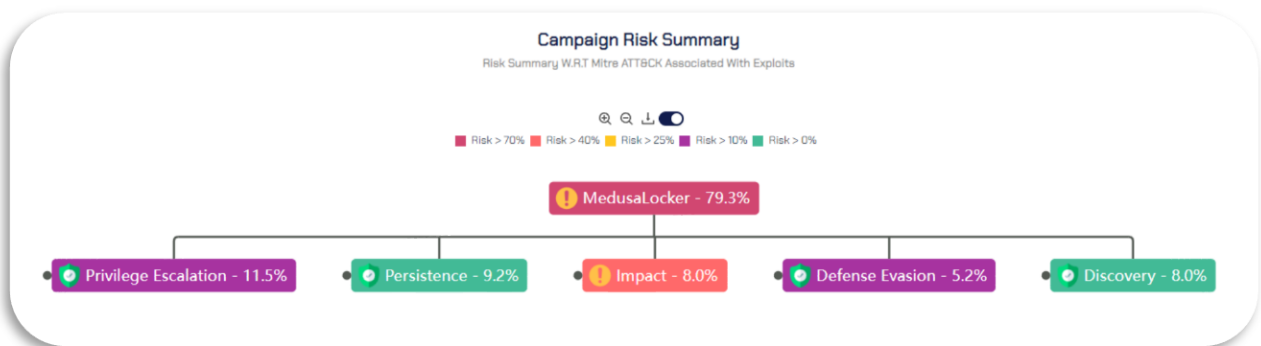
Agent: testcytotate

#### 5. Description

MedusaLocker is a type of ransomware that encrypts victims' files and demands a ransom.

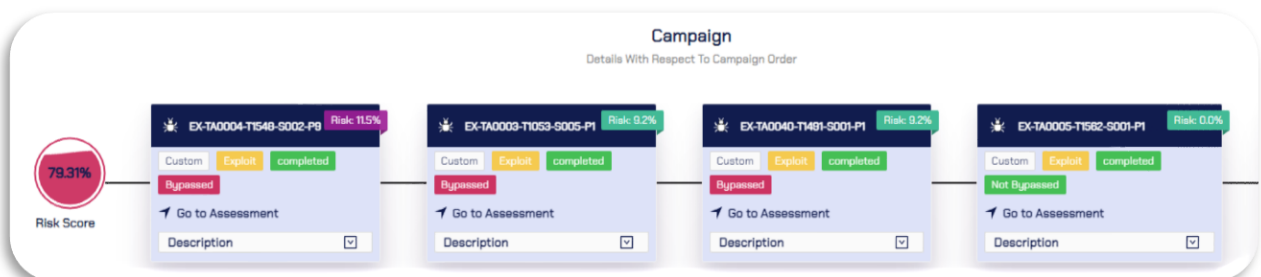
#### 6. Campaign Risk Summary

- Overall Risk
- Risk for every MITRE Tactic

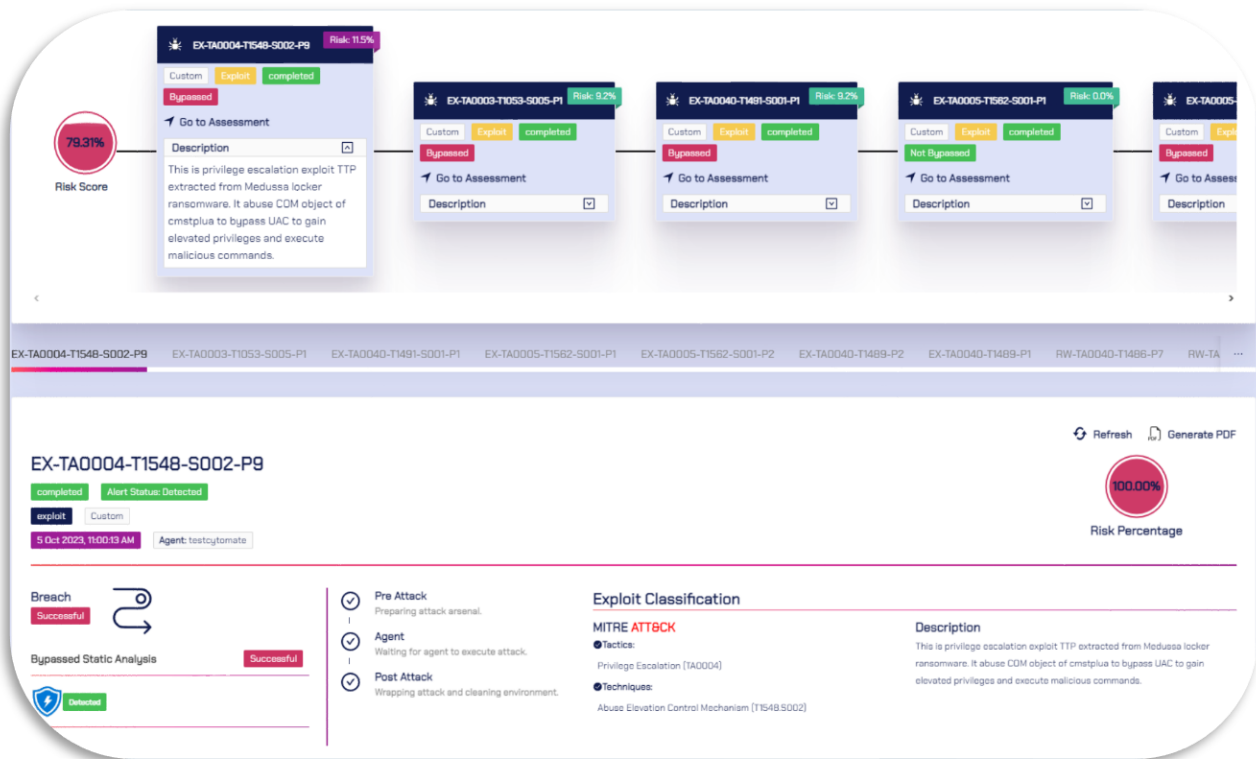


#### 7. Campaign test cases

- Test case ID
- Test case description
- Test case status
- Test case category
- Test case risk
- Test case Breach

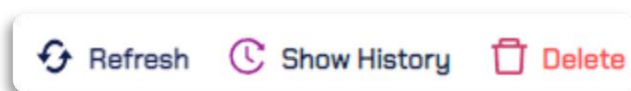


- Campaign test case Reports can be viewed individually. The test case report is similar to the Endpoint Reports that have been explained in the section of [Behavior \(exploit\) Report](#)



ix. There are a few other options available in the campaign reports on the top right corner:

1. **Refresh**: refresh the reports
2. **Show History**: show previous assessments
3. **Delete**: delete campaign report



### 5.3. Breach+ ATT&CK Maps

Breach+ ATT&CK Maps is a feature that shows an overview of all endpoint & email gateway assessments mapped on **MITRE ATT&CK** framework matrix. The ATT&CK Maps also provides a heat map of assessments by organizing the results of assessments in a way that gives the user a perspective of which TTPs are hot and which are cold in their security architecture by assigned relevant colors.

- i. To open ATT&CK Maps, go to the respective tab from side bar





ii. The heat map is displayed on the ATT&CK Maps tab

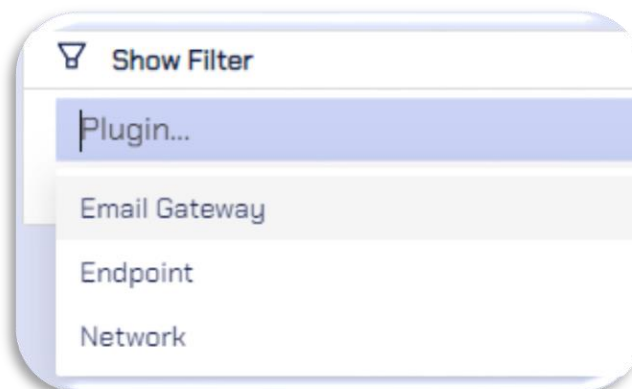


iii. On the ATT&CK Maps, every TTP is displayed according to the following color combination:

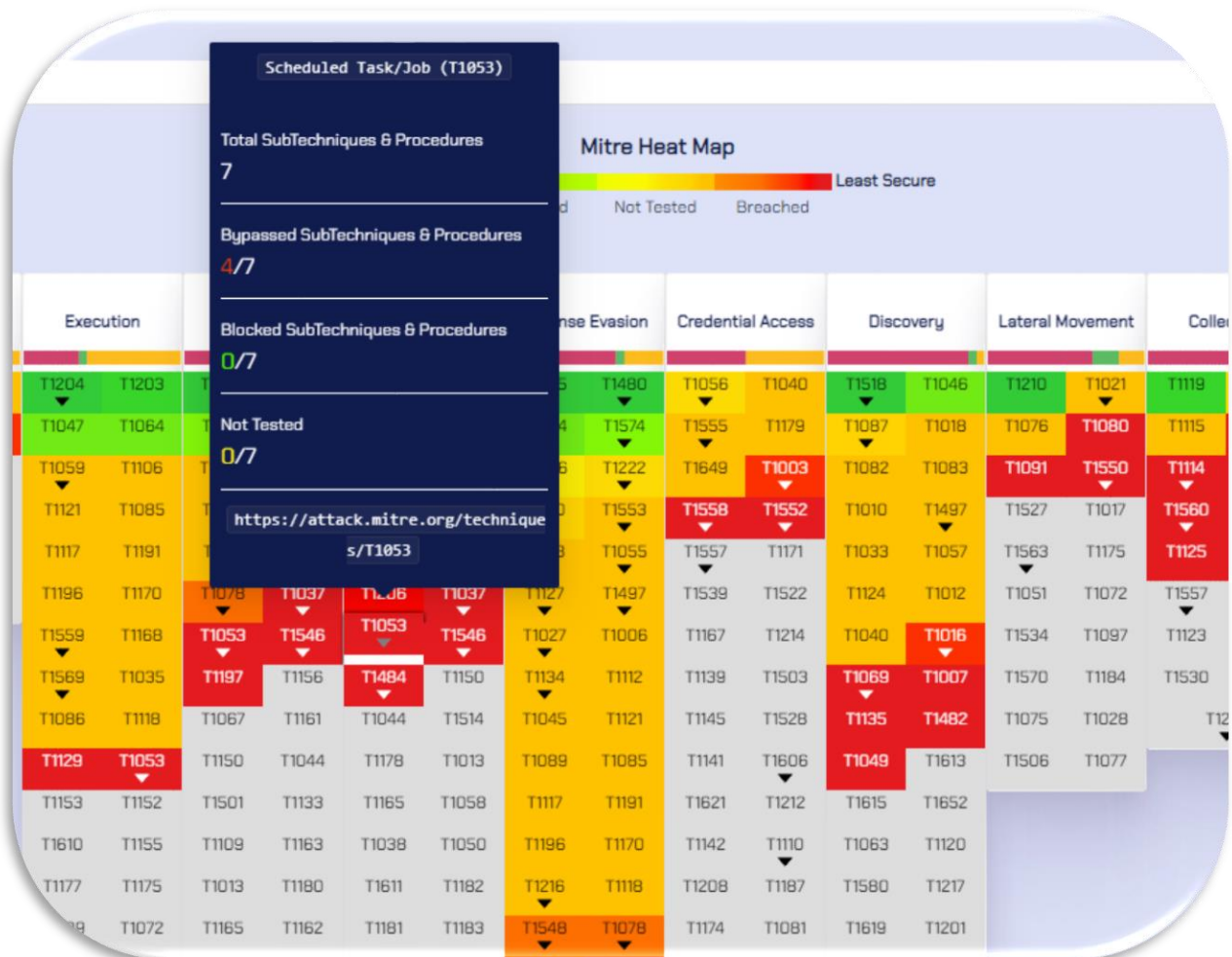
1. **Green:** Most Secure
2. **Red:** Least Secure
3. **Grey:** Not Tested

iv. The ATT&CK Maps could be filtered through 3 components:

1. Endpoint & Campaigns
2. Email Gateway
3. Network



- v. If you hover on a specific TTP, it will show detailed information about that TTP like how many of these TTPs are available or bypassed or prevented.



## V. NETWORK SECURITY

### 1. Technical Detail of Network Security

The Breach+ Network Control Validation module is a sophisticated tool designed for enhancing cybersecurity measures, particularly focusing on the efficiency and effectiveness of network-deployed security controls. This module is tailored for organizations that have invested in next-generation firewalls (NGFWs) and other similar advanced security technologies. Here's a detailed explanation of its features and functionalities:

## 1.1. Performance Evaluation of Security Controls

The primary function of this module is to assess the performance of security controls that have been deployed within a network. This is crucial for organizations to ensure that their investments in security technologies like NGFWs are yielding the desired protective outcomes.

## 1.2. Use of Packet Capture (PCAP) Replay

A key feature of this module is its ability to replay traffic using PCAP. PCAP is a data packet capture format that records network traffic. The module replays this recorded traffic between a target and attacking assets.

## 1.3. Real-World Malware Traffic Simulation

The traffic replayed is not just any traffic; it includes real-world malware traffic. This means the module simulates actual malicious traffic patterns and behaviors seen in real cyberattack scenarios. This provides a more realistic and challenging test environment for the network's security controls.

## 1.4. Comprehensive Testing of Inline Security

By replaying whole PCAPs, the module thoroughly checks the inline security measures. 'Inline security' refers to security controls that are placed directly in the path of network traffic, actively analyzing, and making decisions about the traffic in real-time. This comprehensive testing is crucial for identifying any weaknesses or gaps in the security setup.

## 1.5. Detection and Prevention Analysis

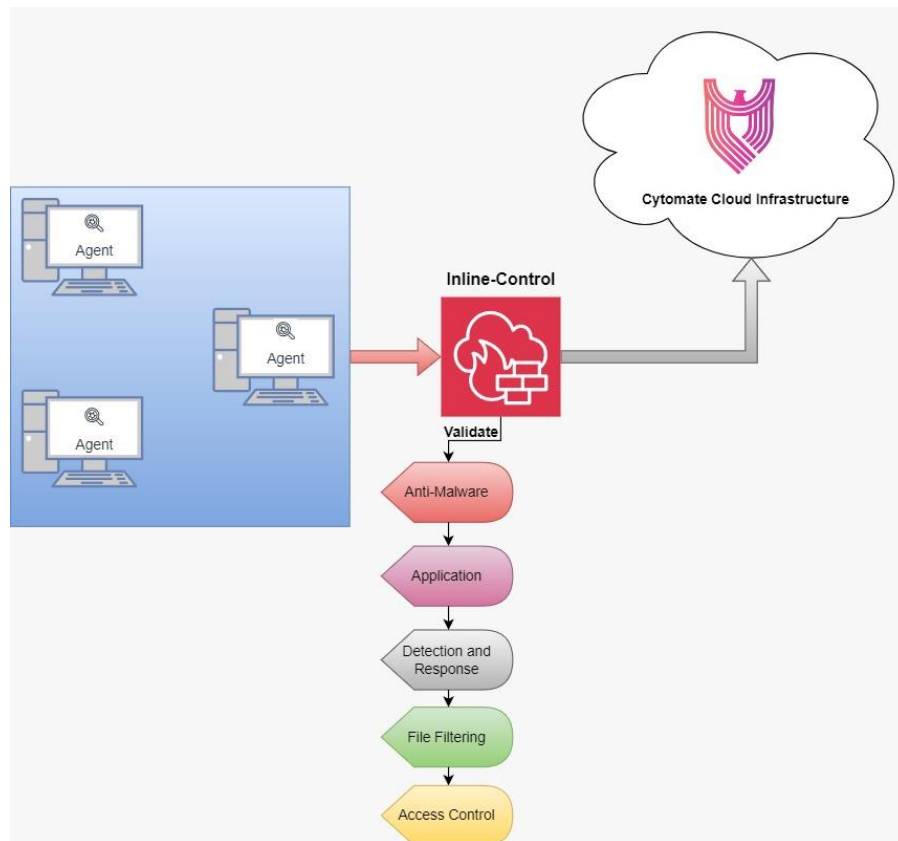
The module not only tests whether the in-line security controls can detect an attack but also if they can prevent it. This dual capability is essential for a robust security posture, as detection without prevention may not be sufficient to thwart sophisticated cyber threats.

## 1.6. Mitigation Recommendations and Prescriptive Guidance

Post analysis, the module provides clear mitigation recommendation options. This includes prescriptive guidance on how to improve the security posture. Such recommendations are crucial for organizations to understand the necessary steps needed to enhance their defenses against identified vulnerabilities.

## 1.7. Provision of IoCs and Vendor-Specific Mitigations

Cytomate also provides Indicators of Compromise (IoCs) and vendor-specific mitigation strategies.

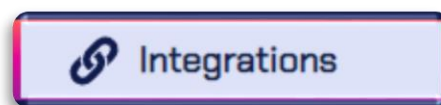


*Network Component*

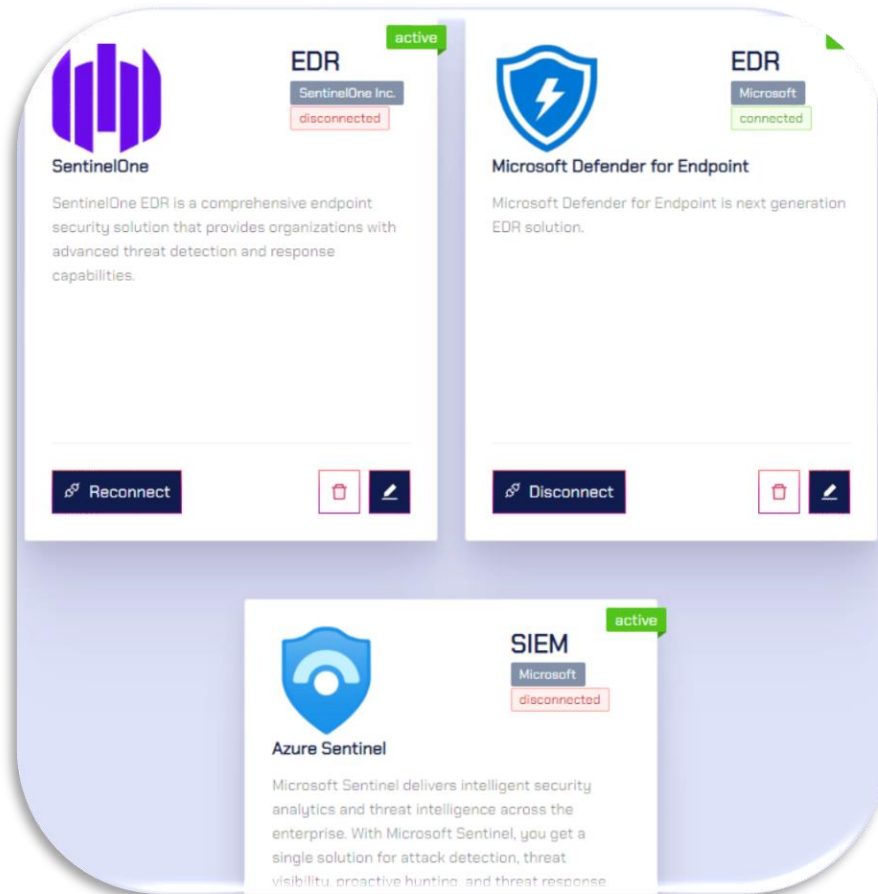
## VI. INTEGRATIONS

The Integration Manager Module is a critical component of a comprehensive security solution designed to streamline and enhance the integration of multiple security controls with a Breach and Attack Simulation (BAS) product. Its primary purpose is to facilitate the quick retrieval and analysis of alerts and logs generated by various security controls following each security assessment conducted by the BAS product. This module acts as a central hub, ensuring seamless communication and interoperability between diverse security tools and the BAS solution.

- i. To visit integrations module, go to the Integrations tab from side bar



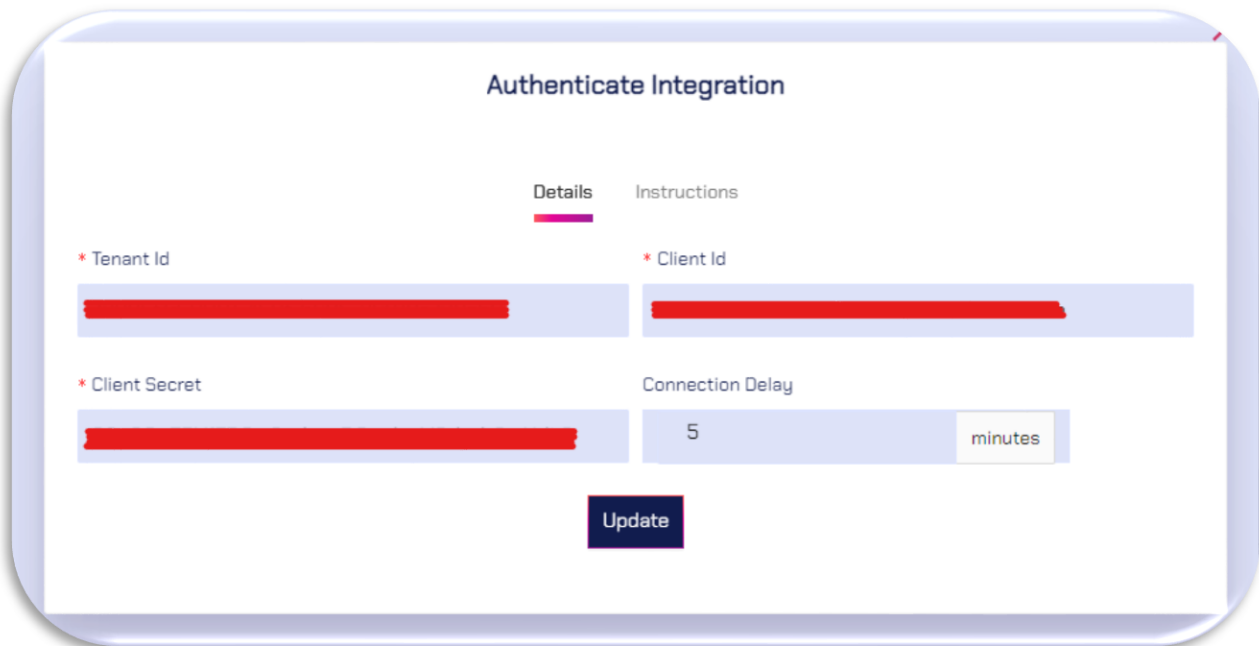
- ii. We have a few of **EDR** and **SIEM** integration currently available in the **INTEGRATIONS** module



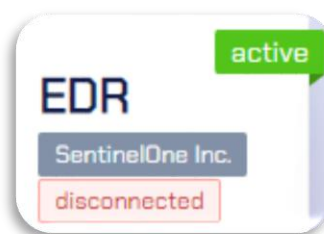
- iii. To connect with the integrations, there is a connect & reconnect button available on the integration card.



- iv. You can **edit** and insert the required detailed in each integration to connect it with breach+ account.



- v. The status of Integrations shows if they are active and either connected or disconnected to the security solutions.



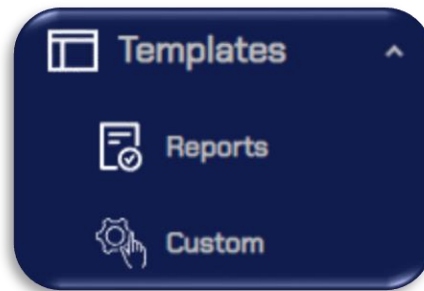
- vi. Apart from these, any other integrations could also be added within a week's notice provided with the documentation of the security control and its APIs.

## VII. TEMPLATES

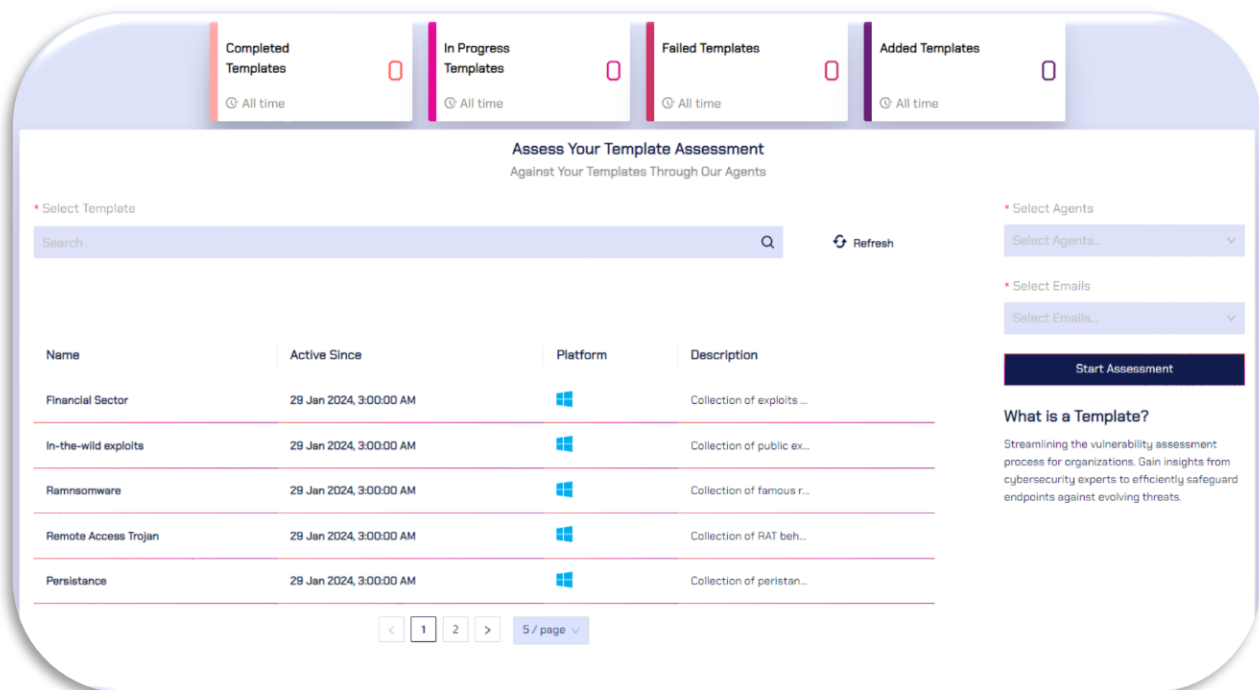
The Testing Templates suite is a meticulously curated collection of malware combinations, organized to serve specific cybersecurity testing purposes. Each template is tailored to address distinct security challenges, making it a versatile tool for comprehensive threat assessments. For instance, the **Privilege Escalation** template is a compilation of exploits sourced from our threat library, all strategically chosen to achieve privilege escalation within diverse system environments. This template aids cybersecurity professionals in assessing and fortifying the resilience of systems against potential unauthorized access or privileges scenarios. On the other hand, the **Financial Sector** template is a specialized set of malware bundles, precision-engineered to target vulnerabilities commonly found in financial institutions. This template allows security teams in the

financial sector to simulate and evaluate their defenses against threats specifically tailored to their industry. These templates not only streamline the testing process but also empower organizations to proactively identify and remediate vulnerabilities within their unique threat landscape, thereby bolstering overall cybersecurity resilience.

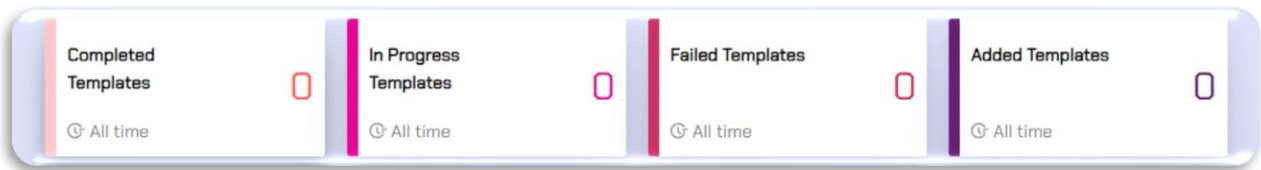
- i. To open templates, go to the templates tab in side bar



- ii. In the templates tab, there are multiple templates created by our security team. These templates are regularly updated and posted here



- iii. On the overview, we have:
  - i. Complete Templates
  - ii. In Progress Templates
  - iii. Failed Templates
  - iv. Added Templates



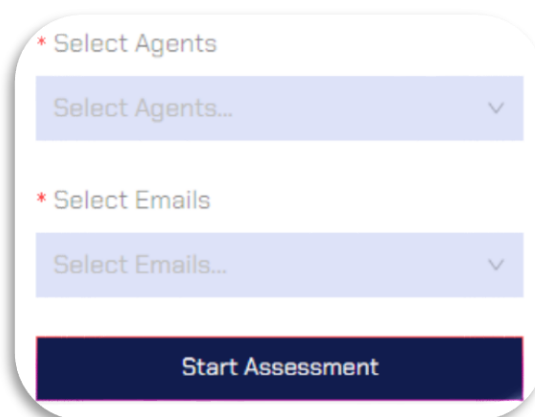
- iv. On the search bar, you can search for a specific template



\* Select Template

Search

- v. To launch a template assessment, select an **agent** and **email address** on which the assessments would be launched



\* Select Agents

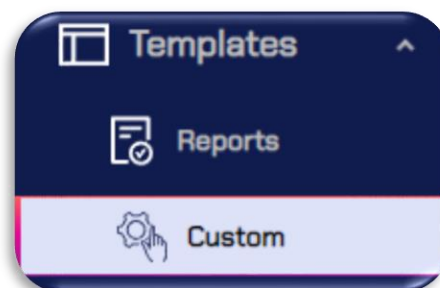
Select Agents...

\* Select Emails

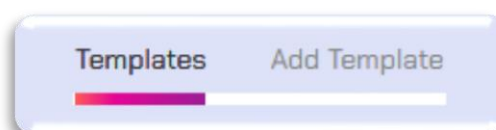
Select Emails...

Start Assessment

- vi. You can also create custom templates, go to the Custom tab under Templates.



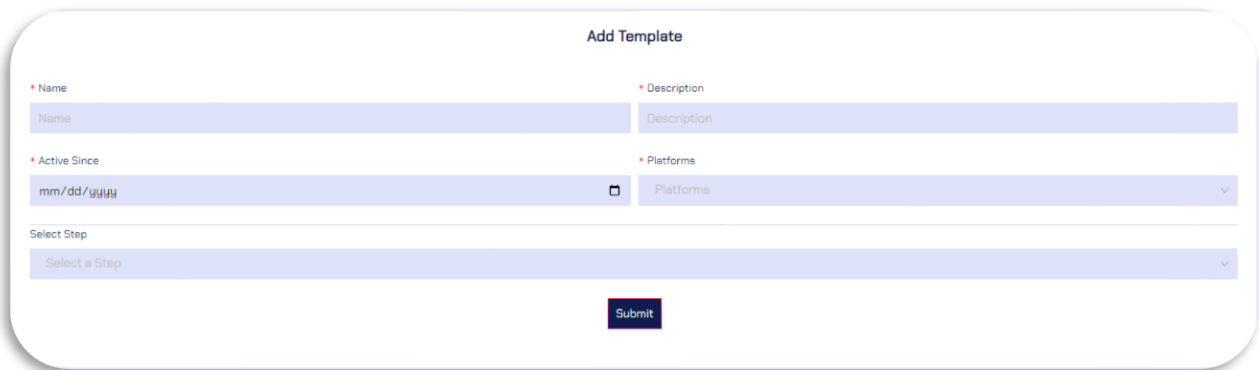
- vii. Go to the **Add Template** tab



Templates Add Template



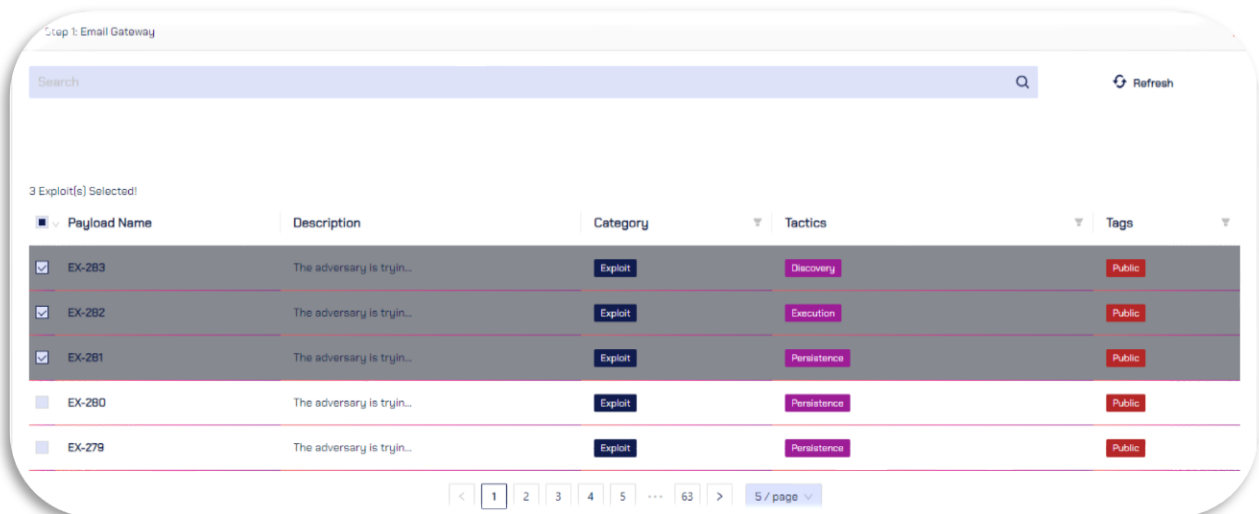
- viii. You can fill templates as per your need. In the custom templates, you can also combine multiple components like:
- Email Gateway Assessment
  - Endpoint Assessments
  - Campaign Assessments



The 'Add Template' form contains the following fields:

- Name:** A text input field.
- Description:** A text input field.
- Active Since:** A date input field with a placeholder 'mm/dd/yyyy' and a calendar icon.
- Platforms:** A dropdown menu with 'Platforms' as the selected option.
- Select Step:** A dropdown menu with 'Select a Step' as the selected option.
- Submit:** A blue button at the bottom right.

- ix. In the Select Step option, you can choose assessments from 3 different components:
- Email Gateway:** Select the malicious attachments and links for email gateway assessments.

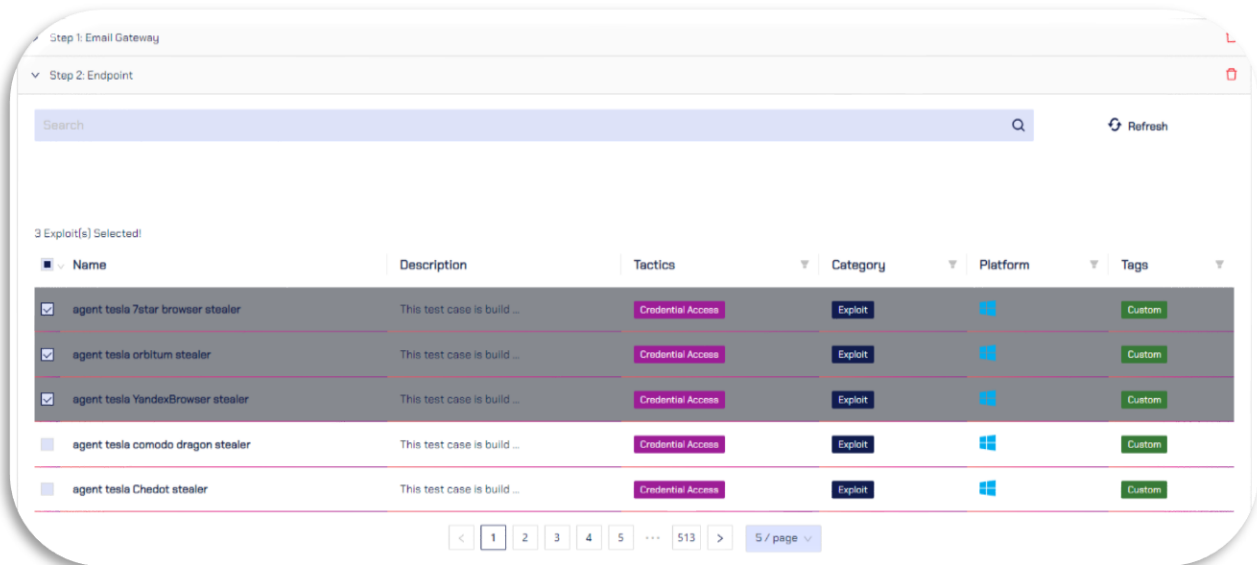


The interface shows 'Step 1: Email Gateway' with a search bar and a 'Refresh' button. Below the search bar, it indicates '3 Exploit(s) Selected!'. The table below lists the selected exploits:

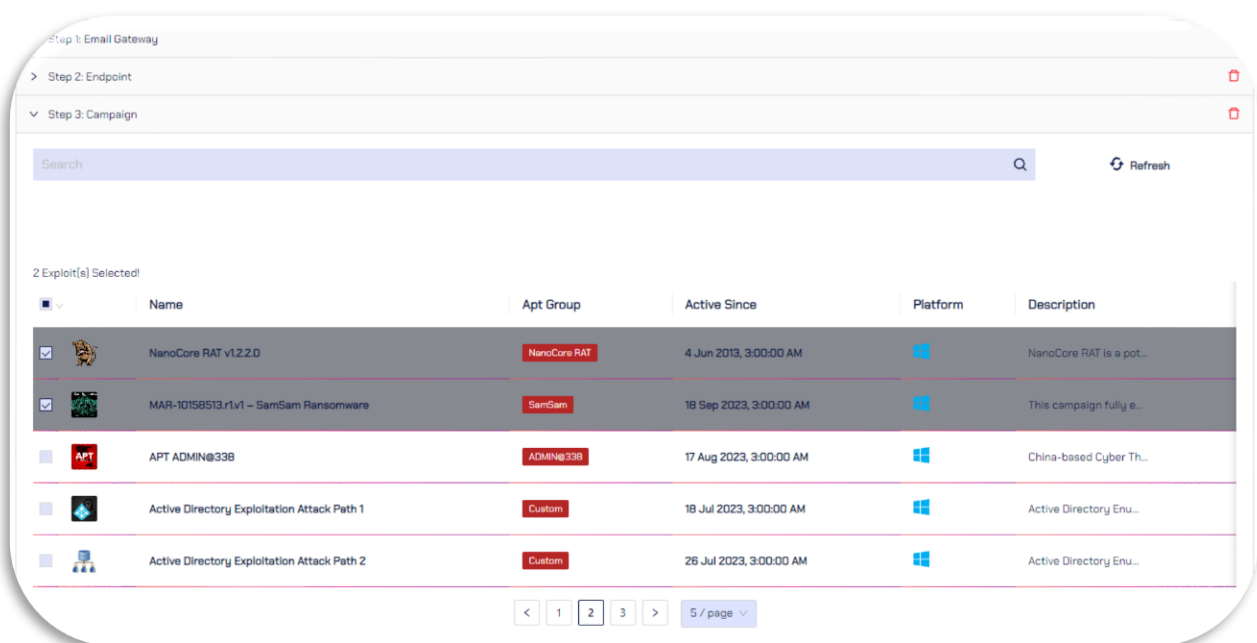
Payload Name	Description	Category	Tactics	Tags
<input checked="" type="checkbox"/> EX-283	The adversary is tryin...	Exploit	Discovery	Public
<input checked="" type="checkbox"/> EX-282	The adversary is tryin...	Exploit	Execution	Public
<input checked="" type="checkbox"/> EX-281	The adversary is tryin...	Exploit	Persistence	Public
<input type="checkbox"/> EX-280	The adversary is tryin...	Exploit	Persistence	Public
<input type="checkbox"/> EX-279	The adversary is tryin...	Exploit	Persistence	Public

At the bottom, there is a pagination bar showing '5 / page' and a list of page numbers (1, 2, 3, 4, 5, ..., 63).

- Endpoint:** In the endpoint section, the threat library of endpoint will be provided from which a user can select different types of malicious test cases or behaviors.



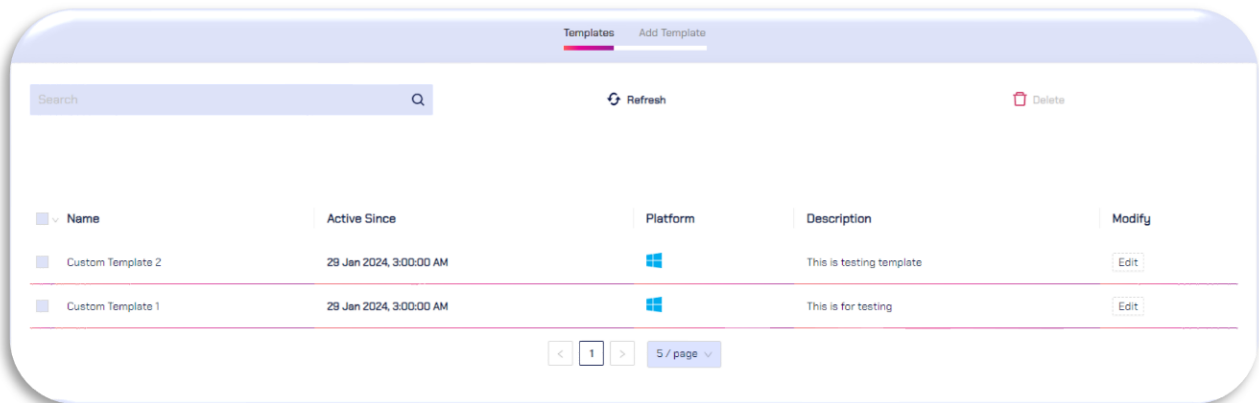
3. Campaign: From the campaigns step, a user can include different campaigns available in breach+.



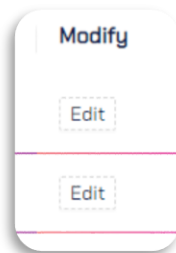
- x. Combining all these steps a custom template could be created by the user itself from the “Add Template” menu.

Submit

- xi. Once the custom templates are created, they will appear in custom templates tab and user can launch these assessments from main templates tab



- xii. User can also modify these assessments from Edit menu



- xiii. Once the templates are successfully created, they will appear on the main template window to launch templates assessments

Name	Active Since	Platform	Description
Custom Template 2	29 Jan 2024, 3:00:00 AM	Windows	This is testing template
Custom Template 1	29 Jan 2024, 3:00:00 AM	Windows	This is for testing
Financial Sector	29 Jan 2024, 3:00:00 AM	Windows	Collection of exploits ...
In-the-wild exploits	29 Jan 2024, 3:00:00 AM	Windows	Collection of public ex...
Ramnsomware	29 Jan 2024, 3:00:00 AM	Windows	Collection of famous r...

## VIII. ANALYTICS

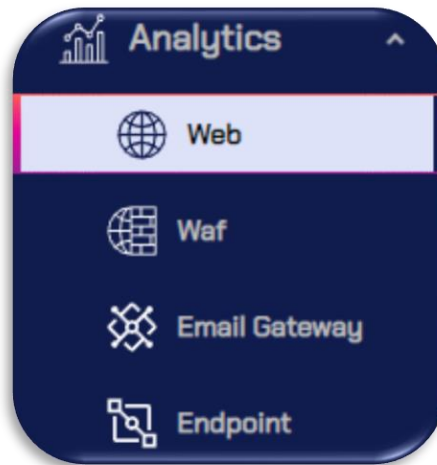
Cytomate's Breach+ incorporates robust analytics across four main components, each tailored to scrutinize distinct facets of an organization's cybersecurity posture. In the case of WEB analytics, the focus lies on identifying potential vulnerabilities, misconfigurations, and malicious payloads within web applications. The BAS product employs advanced scanning techniques to assess web assets, providing insights into weaknesses that could be exploited by attackers. Similarly, WAF analytics centers around evaluating the effectiveness of Web Application Firewalls, analyzing how well they mitigate specific types of payloads.

On the other hand, Email Gateway analytics delve into the risk landscape associated with email communication. The product assesses the effectiveness of email gateways in detecting and preventing phishing attempts, malware-laden attachments, and other email-borne threats. The risk calculations in this context are based on real-world test cases, often mapped onto the MITRE ATT&CK framework, ensuring a comprehensive evaluation of an organization's email security posture.

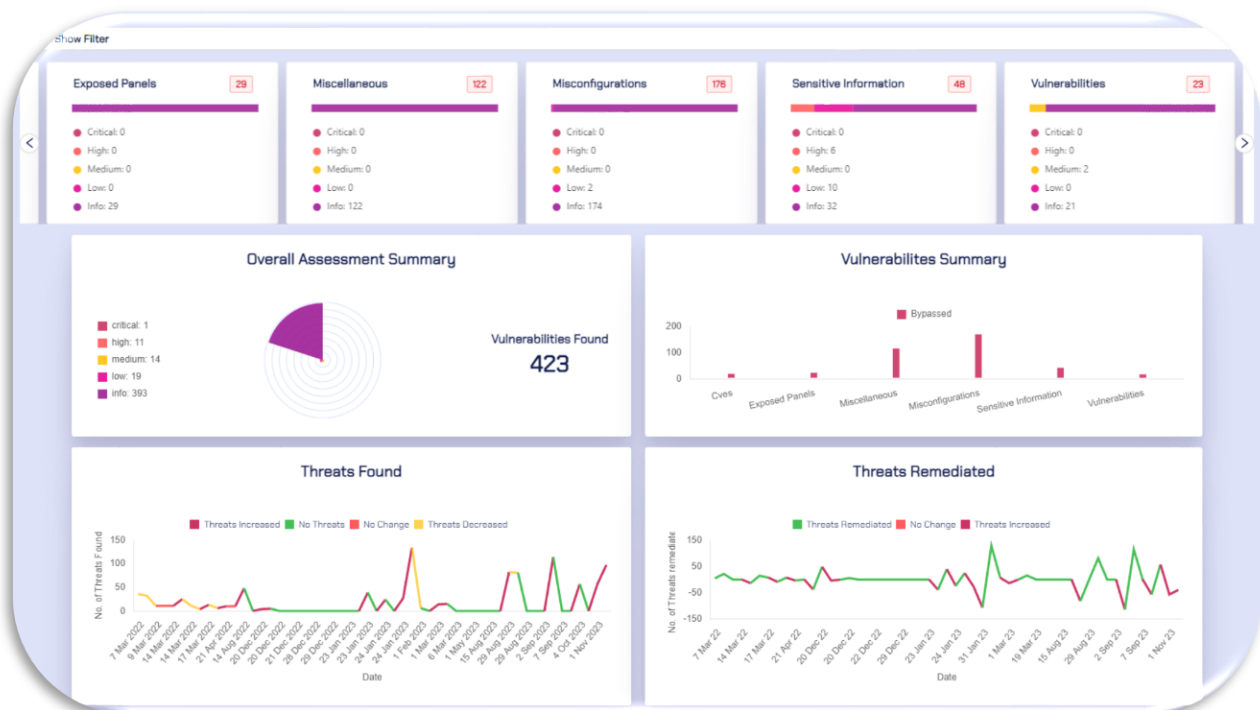
Endpoint analytics focus on evaluating the security posture of individual devices within the network. Through the execution of simulated attack scenarios, the BAS product gauges the endpoint's ability to detect and respond to various threat vectors. Risk calculations in this domain are intricately tied to the MITRE ATT&CK framework, allowing for a nuanced assessment of an endpoint's resilience against known attack techniques.

By leveraging these analytics across WEB, WAF, Email Gateway, and Endpoint components, breach+ provides a holistic view of an organization's security posture. This approach not only identifies specific vulnerabilities or weaknesses but also quantifies the overall risk by aligning assessments with the MITRE ATT&CK framework, offering a sophisticated and comprehensive understanding of potential security threats and vulnerabilities within the tested environment. This information empowers cybersecurity teams to prioritize remediation efforts and fortify their defenses against real-world cyber threats effectively.

- i. To see Analytics, go to the Analytics Tab on the side bar.

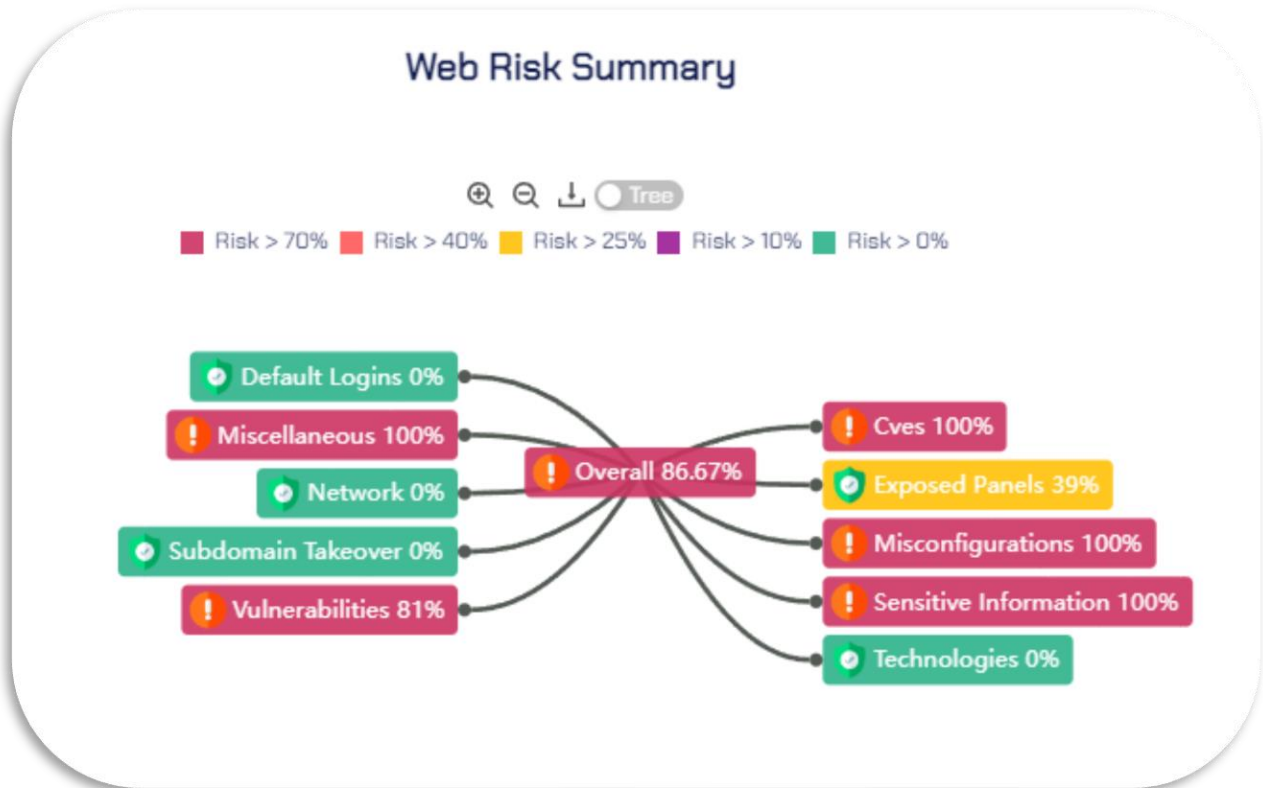


- ii. First analytics component shows WEB. In WEB analytics, we have different categories of problems:
- Exposed Panels
  - Miscellaneous
  - Misconfigurations
  - Sensitive Information
  - Vulnerabilities
  - CVEs

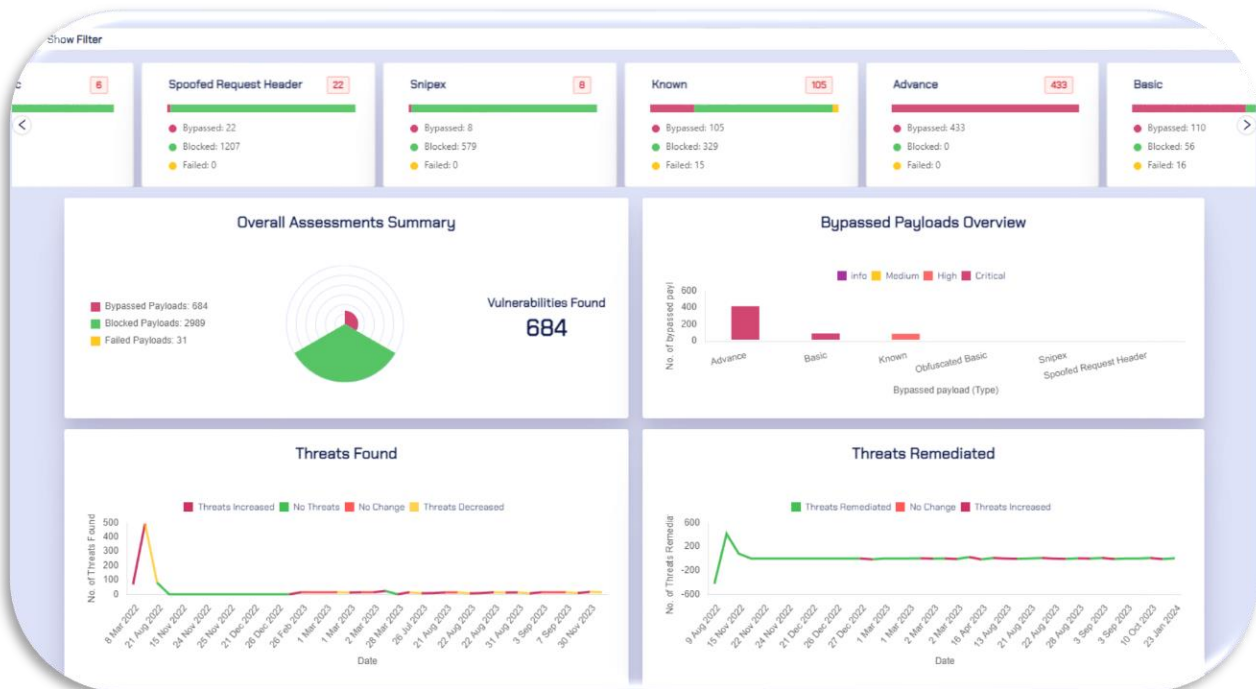


- iii. We have overall assessment summary which shows how many vulnerabilities have been found along with their severity level each color coded.

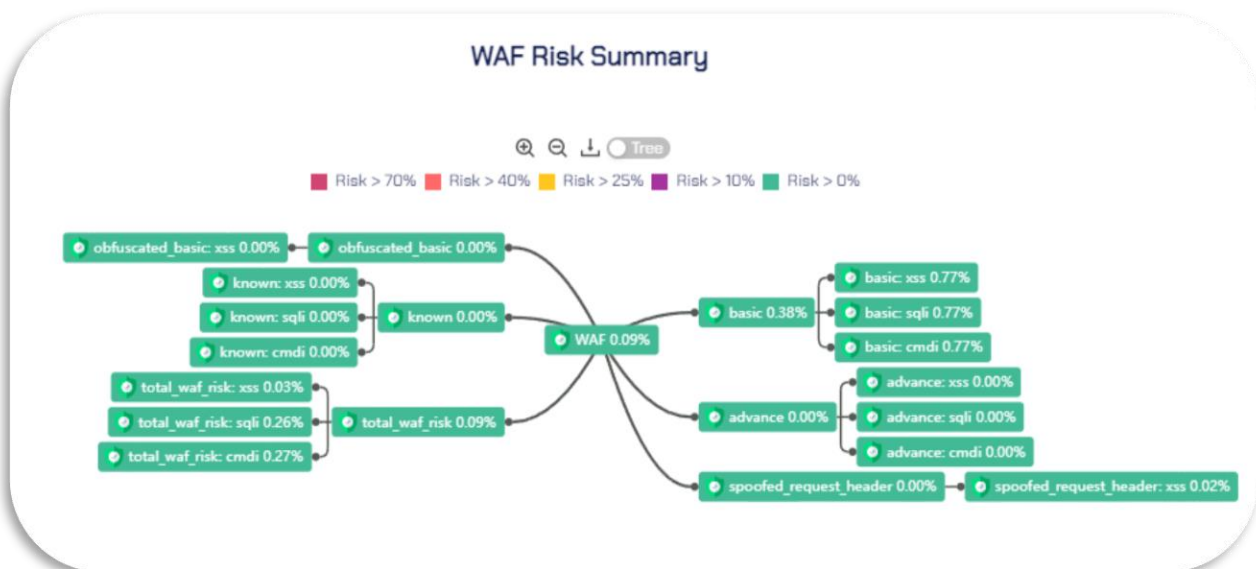
- iv. Other graphs show, real-time view of how many Threats have been found during each day and how many of those threats are remediated
- v. We also have overall risk summary graph which shows risk score across all categories and their overall risk



- vi. Next, we have WAF Analytics, which are similar to WEB analytics. However, here instead of WEB categories, we have WAF payload categories and their overall risk.



vii. Similarly, WAF overall risk summary contains the type of WAF payloads



viii. In case of Email gateway, the analytics categories are based on MITRE ATT&CK framework



ix. The overall risk summary is also based on MITRE ATT&CK



x. Similar to email gateway, the **ENDPOINT** Analytics are also based on MITRE ATT&CK framework. It contains Tactics from MITRE as categories and overall risk summary is also based on the MITRE Tactics



