Cymulate

Technical Guide

Modules

An Overview of Cymulate Technical Modules

4/23/2020

Table of Contents

Modules

Email Gateway

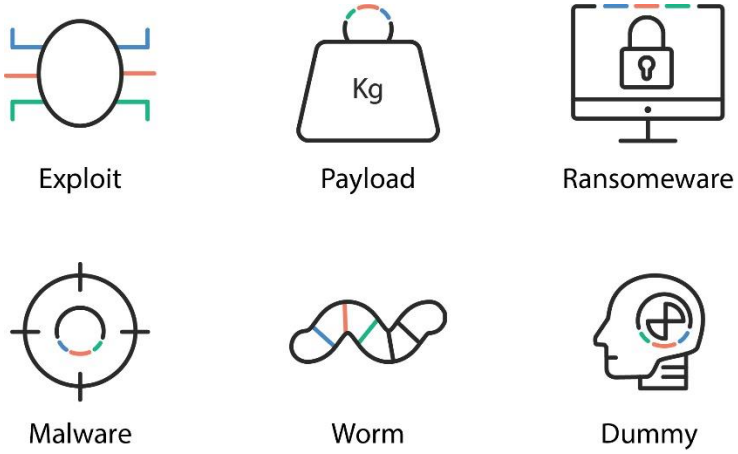
Over 75% of cyberattacks worldwide are originated through the receipt of malicious mail. The number of attacks and targets continue to increase. Malicious email can become dangerous without protecting you and your users from latest identify theft, password and regular scams.

An example scam is a recurring DHL phishing template that notifies victims that a shipment payment is waiting. Behind the link is expected to be a hidden link containing the attacker's malicious content, forming destructive malware. This vendor can be challenged with Cymulate's Mail module. All mail is monitored through transmission to identify and capture unwanted content such as malicious attachment where users receive emails containing malicious content.

Cymulate email assessment helps to improve this experience by reducing the number of attacks that originate via email and help improve email posture for safer everyday use. Its protection aims to block malicious email concerning incoming traffic. The typical architecture of Mail module contains an on-site hardware appliance on the organization network to route inbound and outbound traffic through analysis and filtering.

The email gateway no longer uses the route of detection through installed anti-virus and anti-phishing but uses threat intelligence development to monitor incoming threats. Cymulate email assessment regularly tests email posture improvements.

Cymulate Mail module allows organizations to launch thousands of different attacks containing threats such as:



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

Key features

- Test using one dedicated mailbox which does not affect users or servers in the organization' network.
- All stages of the test are done automatically, including hash comparison of penetrated payloads the deletion of sent emails to the agent once it lands in tested mailbox.
- Detailed reports with mitigation tips based on file type and behavior of penetrated emails.

Web Gateway

Web malware protection is becoming more and more urgent. Websites that profit from extensive traffic are twice as likely to receive large amounts of malware through mainstream networks.

What's the Cyber attacker's objective? It's to tap into your browsers that contain rich data so that they can manipulate or profit from it. This attack vector grows particularly among websites that have larger visitors. In turn, the vector succeeds by increasing the number of browser extension installations that contain web malware on your visiting websites.

This has resulted in its widespread success, with successful malware manipulation of plug-ins such as Flash, Java and Microsoft Silverlight. As estimated, 25% of malware attacks have been located within US and Asia, and 15% in Europe and the Middle East.

As a supportive solution, Cymulate Browsing uses a cyber attack simulation vector to evaluate outbound exposure to malicious or compromised websites. This enables them to test against largely growing databases of malicious websites.

To do this, organization's outbounds are tested using common HTTP/HTTPS protocols. This enables testing against large databases of malicious websites on the web. The results that are delivered help IT security to locate gaps and take preventive measures to reduce outbound attacks.

Cymulate Web Gateway assessment helps stimulates communication of web browsing within the following categories:

Another common form of web malware is to manipulate you into accessing web links which in-turn downloads malicious files through the web browser. Cymulate Web Gateway helps stimulate this with the use of Cymulate Exploit-Kit. The Exploit-Kit locate and exports malicious websites to a text file and uploads them to a Content-Filter security gateway.

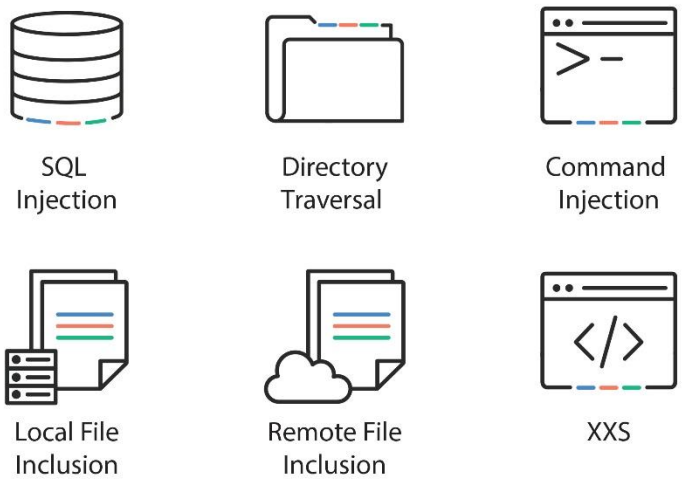
Key features

- Lightweight tests that don't exhaust system resources - a couple of thousand http/s requests downloading small amounts of KBs, in intervals.
- Test using one dedicated workstation which does not affect other users or servers in the organization' network.
- The agent is only approaching the malicious URLs and is not rendering their content.

Web Application Firewall

Web Applications have become a central business component in many organizations, and huge amounts of money and effort are spent protecting these assets. Whereas in the past, IT security teams monitored and defined a small number of enterprise web apps. Today, there is a further need to protect the web backends of many mobile and SaaS applications and other cloud-based solutions. The number of diverse threats continue to increase from advanced malware to web-based application-layer attacks, denial and distributed denial (DoS and DDoS) and security induced usability issues.

One of the main products that is supposed to protect your Web Application is the Web Application Firewall. These products may create a false assumption that your Web Application is immune to security flaws and applicative attacks such as Cross-Site Scripting (XSS), SQL Injection (SQLi) and Cross-Site Request Forgery (CSRF) even if the Web Application code is flawed.



To counter this, the Cymulate WAF platform checks tests your WAF configuration, implementation and features to help stimulate the attacker aiming to bypass your organizations WAF. This ensures that attackers who try to bypass cannot perform malicious actions using these applicative attacks.

Key features

- Challenge WAF against a list containing thousands of payloads signatures.
- Website is crawled and mapped automatically by Cymulate prior to launching the attack.
- Test against different WAF behaviors

Phishing Awareness

Phishing has and continues to be a widespread problem. If you're not aware of phishing, you'll become a victim. Phishing is the most prevalent form of cybercrime and has been for up to eight years. In an instant, companies will lose out on millions of dollars.

An example of a popular attack is the creation of phishing campaigns, an email scam designed to steal personal information of large data and perform malicious tasks.

These risks can be reduced through Cymulate Phishing, a solution that reduces spear-phishing, ransomware and protect CEO fraud. In addition, Cymulate Phishing minimizes malware-related downtime to save money from incident response.

Awareness needs to be heightened to globally ensure that companies do not lose out from phishing attacks. There must be a distinct focus in raising employees' security awareness through simulated phishing campaigns. In addition, IT security within organizations must develop training programs to reinforce vigilante employee behaviors.

Spear phishing uses different templates assigned to the corresponding landing page. Different payloads such as: Links, Attachments and Credential theft are used to fully understand the threats that the employees expose the entire organization.

Key features

- Phishing emails are sent from Cymulate's cloud to a list of emails the customer chooses.
- None of the emails contain real malicious content (ransomware, URLs, worms, etc.).
- Different events are being tracked and updated by Cymulate throughout the campaign.
- Users have full control of templates sent and can create their own using easy builder.

Endpoint Security

Organizations are required to tighten their security parameters to shield from cyberattacks. As part of an Endpoint Security framework, organizations may utilize Antivirus (AV), Endpoint Detection and Response (EDR) or Endpoint Protection Platform (EPP) as part of their defense line. Workstations within a network domain are considered easy entry points for attackers. Where the Endpoint security framework fails to protect user workstations, a cyberattack is more likely.

Outputted reports are developed in a simple format that is easy to understand. Organizations can view security state of each end point and take action to upgrade endpoints. There are mitigations for each threat depending on the type of attack. Endpoint security may be vulnerable towards Operating System (OS) patches and third-party software.

Behavior based scenarios:

Scenarios framework ensures that organizations are able to perform controlled real-ransom and malware attack tests securely and safely. This task ascertains if organization security products are strong enough to protect endpoint nodes.

AV Signature Tests:

AV Signature framework ensures that organizations are able to perform controlled real malware attack tests securely and safely.

Red Team (Atomic commands tagged to Mitre ATT&CK):

Red Team framework contains finely tuned tests performing atomic executions tagged to MITRE ATT&CK framework & tactics, techniques used by threat actors worldwide.

Red Team framework also contains the ability to customize your own attacks – creating your own payloads and commands to be executed directly from the Red Team framework.

Red Team framework will enable every user who wishes to test their detection and response solutions with specific test cases and customized attack scenarios.

Key features

- Basic and advanced scenarios running on a dedicated workstation inside the internal network with no user interaction.
- Simulates real behavior of malwares such as ransomwares, computer worms, trojans and more.
- Test detection against real malwares.
- Contains the ability to test against real APT groups & known malware techniques & tactics based on MITRE ATT&ACK framework.
- Execution of custom commands & payloads created by the organization's Red team.

Lateral Movement

Lateral movement inside a Windows Domain Network is a common penetration scenario. An example scenario are threat actors who use their own logging credentials in web browsers to take advantage.

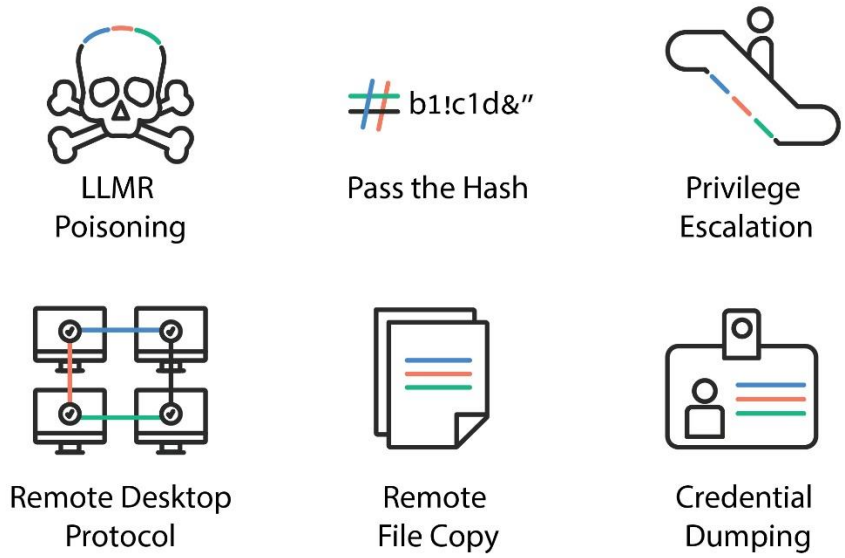
Threat actors become difficult to move laterally within the compromised organization because they use built-in tools from its internal systems to avoid detection. Tools which are not part an organizations security log review process such as Microsoft PowerShell.

Therefore, this makes it difficult for threat actor movement to be detected even if they gain access as an administrator. This therefore makes it easier for threat actors to move deeper into the network.

The problem is there's a lack of man-made methodologies develop to stimulate hacking breach spots. There is, however, one solution that caters for this, known as Cymulate Hopper.

Cymulate Hopper is a sophisticated and efficient algorithm that monitors and access to the network and reveal breaching spots of the organizations Windows Domain Network.

The algorithm identifies potential risk of attack from a Cyber Attack or a threat by simulating a vulnerable workstation to expose its risks using lateral movement methods. This includes:



Each threat has a mitigation strategy to reduce the impact of every discovered threat. This is to reveal the breach spots of the lateral movement inside the Windows Domain Network.

Key features

- Progresses with only 1% CPU usage with zero user interaction.
- No destructive actions such as deletion, encryption, DDOS, etc.
- Abusing OS apps for privilege escalation capabilities.
- Data Assessments – The agent is run on the assessment. A report is then sent via the internal mail system. The platform also accepts uploads of assessment results.

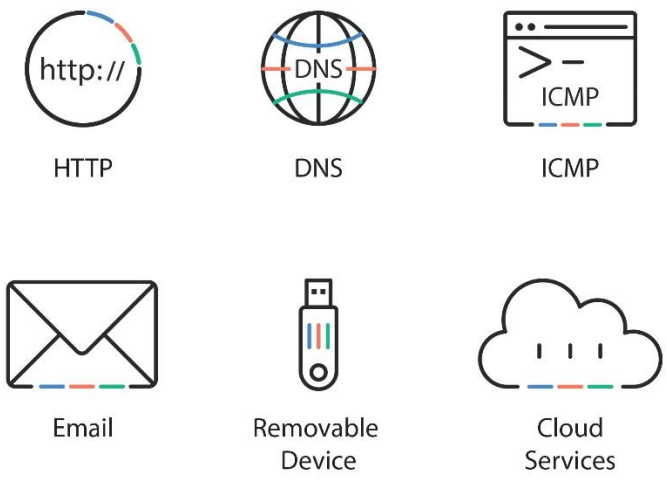
Data Exfiltration

There are an increasing number of laws being passed which put the onus on companies to better safeguard their data. Arguably, the foundation that continues to be followed is the 1974 Privacy Act. Although these regulations are designed to better safeguard your data.

Data breach also has huge financial impact on a company's reputation. There is a heavy reliance on Data Loss Prevention (DLP) laws and products to ensure that critical information cannot stays within organization walls. Each Data Loss Prevention (DLP) product has its own security configurations and implementations and not all businesses should roll-out the same product.

For instance, the Cymulate DLP is a data exfiltration vector that evaluates performance of business solutions that prevent critical information leaving the organization. It allows you to test your outbound flow to keep your main assets in control.

Cymulate attempts to exfiltrate data over the following:



Key features

- Generation of exfiltrated phrases in different file types based on user input.
- Generated phrases information is sent over TLS to Cymulate's cloud.

- Data is stored on a secured designated customer data base at Cymulate's cloud (AWS located at Ireland).

Immediate Threats Intellignece

Counteracting modern cyberthreats requires a 360-degree view of the tactics and tools used by threat actors. Generating this intelligence and identifying the most effective countermeasures requires constant dedication and high levels of expertise. With deep down analysis of each of the threats coming up everyday, we work to support you with the latest threat intelligence from all around the world, helping you to test if you are vulnerable to them and maintain immunity to even previously unseen cyber-attacks.

Key features

- Threat intelligence is actionable - it's timely, provides context, and is able to be understood by the people in charge of making decisions.
- Provide context on indicators of compromise (IoCs) and the tactics, techniques, and procedures (TTPs) of threat actors seen everyday.
- It helps the organization to prepare itself for a future cyberattack knowing the relevant IOCs and TTPs.
- It adds value across security functions for organizations of all sizes.
- Vulnerability management teams can more accurately prioritize the most important vulnerabilities with access to the external insights and context provided by threat intelligence.

Supported modules

- Endpoint Security.
- Web Gateway.
- Email Gateway.
- Integrations:
    - Vulnerability Management
    - SIEM
    - EDR, EPP, AV
    - SOAR, eGRC

Full Kill Chain APT

Full Kill Chain is something you've unlikely to have heard of, unless you have experience as a security professional. The term "kill chain" is a phased model that helps describe stages of an attack to help prevent them. APT is defined as Advanced Persistent Threat. A stealthy computer network where a person or group gains unauthorized access to a network but cannot be detected.

In steps a Full Kill Chain APT, which lists stages within its strategy to help prepare your organization from cybercrime techniques.

Testing Controls Across the Full Kill Chain

APT aims to bypass security controls through the cyber kill chain, from exploitation and post-exploitation. To defend against it, multiple security controls are required. Because one control within the Full Kill Chain sequentially kicks-off the next control within it, security defenses in your organization must protect itself from a full-blown attack.

Instrumenting your Security with APT Simulations

Full Kill-Chain APT Simulation Module is instrumental in effecting your security framework comprehensively. However, it can somewhat become a challenge. The purpose of the module is for organizations to simulate a full-scale API attack by a click of a button and determine security gaps through a single-pane view.

Choose among Templates of High-Profile APTs

Organizations are now able to select identical APT attack templates to mirror real-world APT attacks from espionage cyber groups.

Simulated APT Attack Flow

Attack vectors are sequentially launched and action itself one after the other. This typically begins through a simulated attack on the email or web gateway and through to endpoint security. Some APT templates will test organization network policies and perform tests such as lateral movement, exfiltration of data and testing the effectiveness of DLP controls.

Key features

- Advanced simulation to combine multiple vectors against real APT groups.
- Processed simulation attack from the email gateway or web gateway, followed by endpoint security attack; simulated through lateral movement or exfiltration depending on APT template.
- Fully customize every part of the attack flow and every option available in other modules apart from Immediate Threats.
- Available of Cymulate templates each time a new APT group attack is live.

Defining Your Security Posture

How safe are you? The truth is, it can be fairly difficult to determine if money is not invested into accurate security solutions. These days, there needs to be a guarantee that organizations security is at an acceptable level so that the Head of Security can afford to relax.

Cymulate assessments provides customers with a security posture and exposure level based on their maturity of security solutions and how well they are protected during an assessment.

The total risk score is calculated using an algorithm which takes into consideration the score of each assessment including many aspects such as: Impact probability, difficulty, availability etc. Each module's risk score is calculated using a specific proven risk assessment model such as NIST SP 800-30, CVSS v3.0 and Microsoft's DREAD comprising the risk and probability of each attack method used.

Risk Calculations

Our Solution

Cymulate enables organizations to test their security posture continuously in a number of attack vectors while using real attack methods and payloads. It's attack-simulation platform is a SaaS solution based in AWS/Azure clouds.

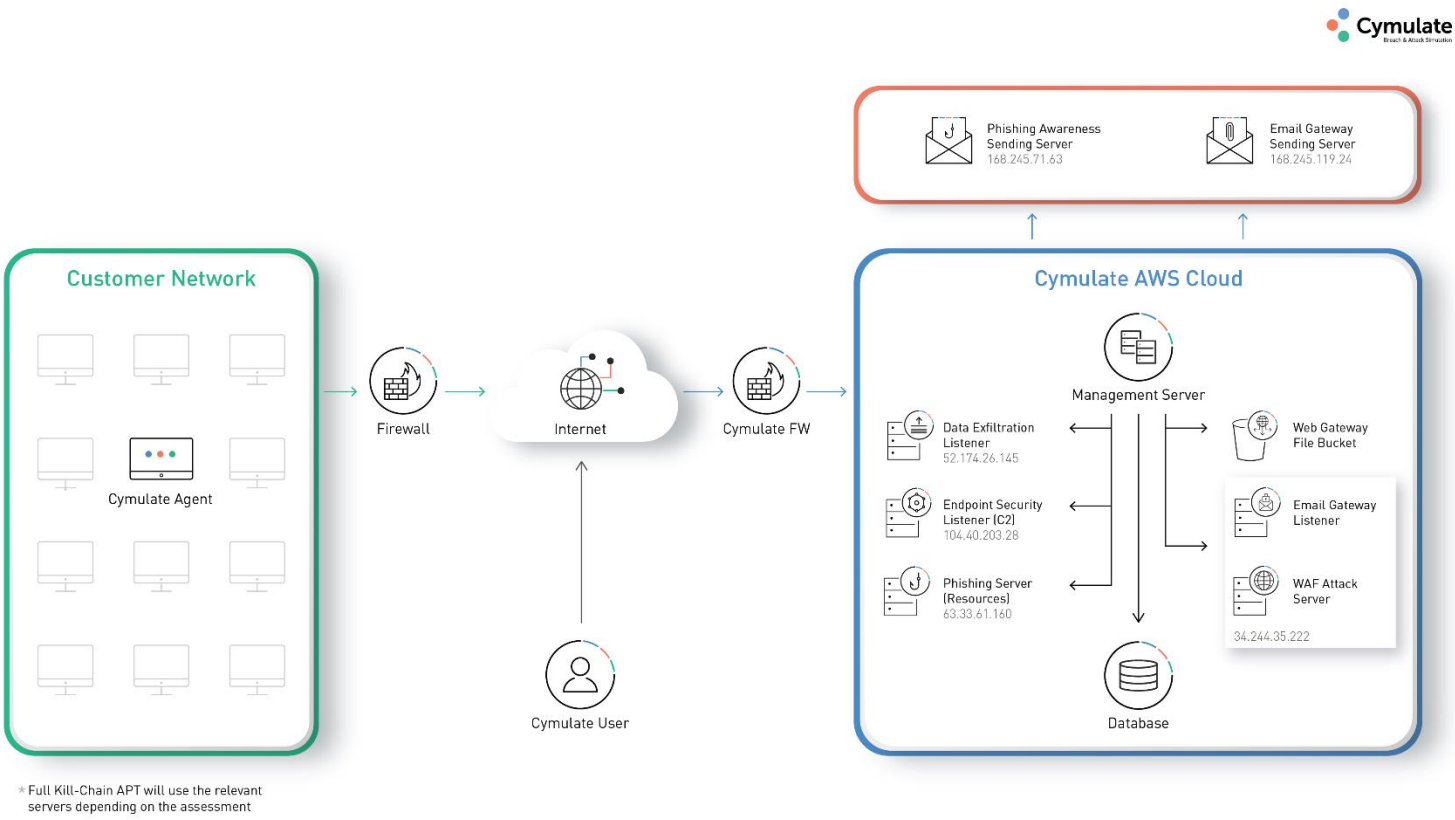
As part of the Cymulate infrastructure, the following additional security measures are implemented:

- **Firewall Security** – As a customer, you would receive individual access to your account by providing a dedicated external IP address. The Firewall is monitored and reviewed periodically for any discrepancies.

- **Application Access Controls** – The Cymulate platform implemented these controls to prevent you from using the platform to access another customer's information. Restriction of access to each customer environment is only permitted to a certain number of users.

Cloud Architecture

Described below are Cymulate's key architecture components and function:



Cymulate Platform

Cymulate provides an easy-to-use web user interface that can accessed from any device connected to the internet: https://app.cymulate.com/

Using the interface, users can create and launch simulations, review results and generate reports.

1. Dashboard

Navigation menu

Navigate to attack vectors' configuration and launch screens, reports section, and action center. The menu provides a comprehensive overview based on scoring rates which indicate a level of imminence of a potential attack incoming. Where the scores out of 100 are low, this indicates it is highly unlikely an attack is forthcoming. Vice versa indicates that an attack is highly likely. You as the user will be able to navigate through each vector to display further information and settings.

Simulations Scores

This section represents a graphical summary of recent Cymulate scores for tested attack vectors. Clicking on each of the scores, will open an additional settings window where baseline can be set.

Attacks Trace

Track recent and running simulations, easy navigation to last reports.

User Menu

The menu allows you to navigate to profile settings, user's management, documentation resources, FAQ and recent activity log.

Alerts feed

Baseline alerts (changes in score), new threats added to the platform, usage reminders.

MSSP* dashboard

Accessing the MSSP dashboard used for managing clients' accounts.

*(*Available only for MSSP users, please refer to the MSSP technical guide for further information).*

Download Center

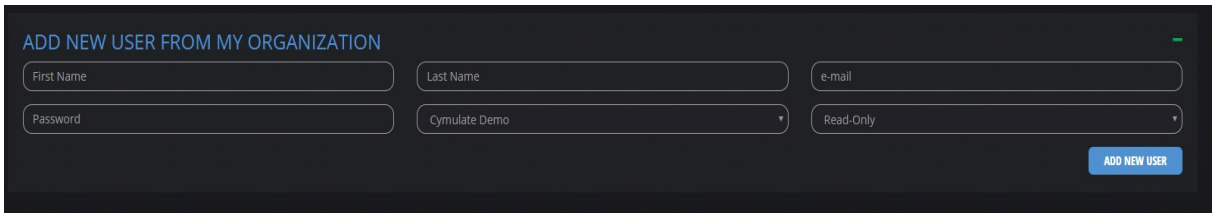
Generated reports available for download.

Agents

Download Cymulate Agent installers.

2. Users Management

To add a new user within your existing account, click on **Users Management** from the **User menu** and fill all required information, as shown below:



The information requested includes First Name, Last Name and Email. All requested fields are mandatory and must be populated. Click on **Add New User** once the user information is populated.

Under **email,** you are able to assign privileges for the created user account.

You can assign the following privileges for each account.

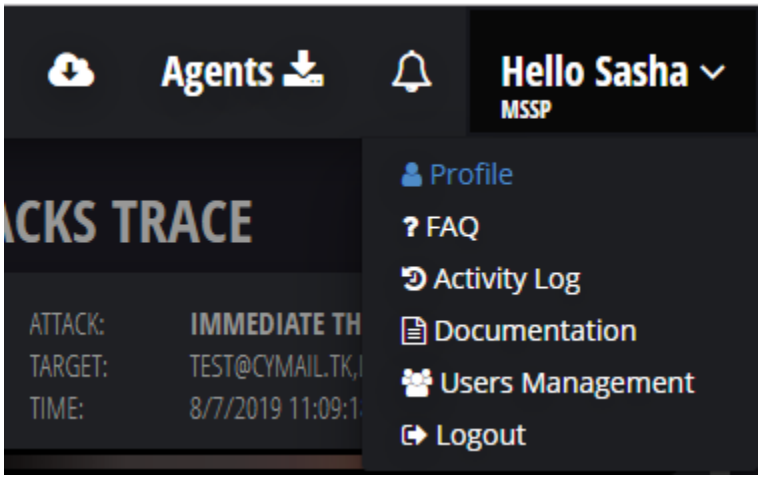
- **Read only** – View results and generate reports.
- **Regular** – Perform assessments, view results and generate reports.
- **Supervisor** – User management (create, delete etc), perform assessments, view results and generate reports.

Depending on the privilege selected, certain restrictions will be applied to areas of the dashboard.

3. Two-Factor Authentication

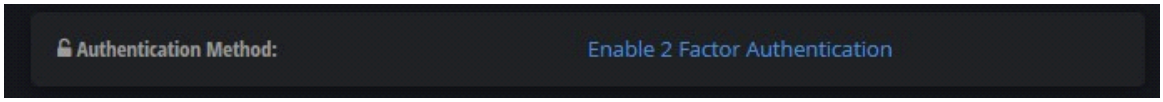
Two Factor Authentication (2FA) is nowadays a very normal form of verification for accessibility purposes. 2FA can be added to access the account.

To do this, **enable** the feature within your user profile under your account.

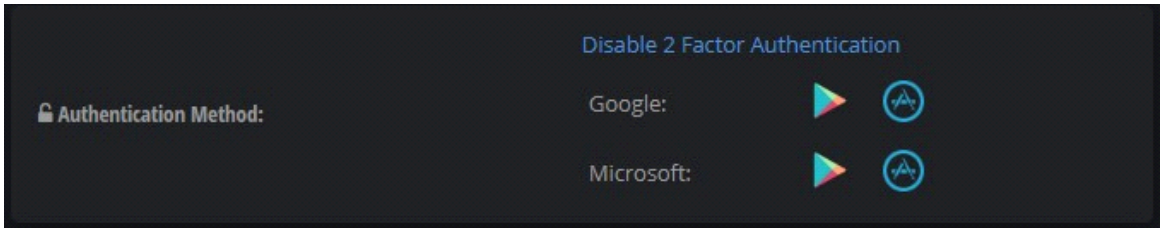


This is shown below:

Scroll down to **Authentication Method** and click on **Enable 2 Factor Authentication.**



Choose which of the 2FA solutions to use **Google** or **Microsoft** authenticator method.



Download the app from the app store to your mobile phone.

Logout of the platform

When attempting to log in again, **scan** the requested QR code and place the code provided into the app for successful entry.

NOTE: This step is one-step authentication and a new code will be required the next time you attempt to log in.

4. Your Security Is Our Security

- The Cymulate platform complies to the following global regulations and platform procedures:

  General Data Protection Regulations (GDPR)
  - ISO 27001
  - ISO 27001
  - ISO 27034
  - NIST 800-53

- Cymulate's platform has been developed using strict secure development life cycle procedures (based on Microsoft Software Development Life Cycle (SDLC)).
- All code modifications are reviewed prior to committing them.
- Cymulate's platform has been assessed through external Penetration Testing in order to validate that no data leaks are possible from one customer to another.
- Each version of the platform is tested prior to being deployed and accessed by our customers.
- The platform is tested for network vulnerabilities periodically.
- The platform is tested for OWASP top 10 vulnerabilities periodically.
- All Cymulate's employees have been reviewed and tested prior to being hired.

5. Data Collection Policy

1. No Sensitive Personal Identifying Information (PII) regarding the customer is kept within Cymulate's platform.
2. As a user, you have full control of reports and can delete data directly from the platform.