Cymulate
Extended Security Posture Management

Testing Security Effectiveness with the MITRE ATT&CK™ Framework

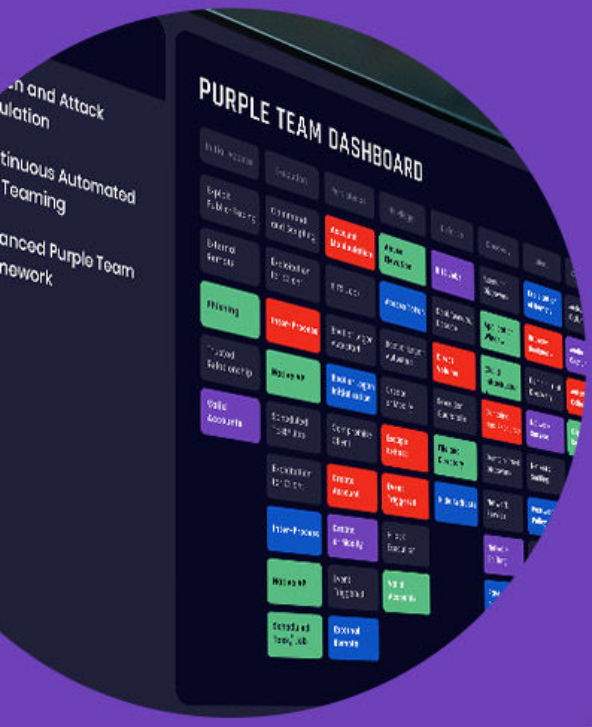


Table of Contents

01 | Modelling Threat Simulations with the MITRE ATT&CK™ Framework

Why MITRE™?

The MITRE ATT&CK™ framework has been gaining traction globally thanks to its comprehensive mapping of adversary tactics and techniques used to infiltrate a network, compromise systems, move laterally and act on malicious threat actor objectives. Across Mac, PC and other platforms, the framework exhaustively covers the full cyber-attack kill chain, from pre-exploitation to exploitation to post- exploitation tactics, techniques, and procedures (TTPs).

Security analysts, researchers, and incident response teams (SOCs) can leverage the tactics enumerated by the framework to test the effectiveness of their security controls and validate that they are operating as expected. Organizations with mature security programs go as far as building their own threat models and running them in their own environment to assess their potential impact.

Limitations of Traditional Threat Modelling

Until recently, this kind of testing of ATT&CK-based techniques, could only be performed in one of several ways.
First, using manual open-source ATT&CK-based tools, security professionals could manually run a list of commands on a target system or server, and verify whether their controls are blocking the simulated attack, alerting on it and logging it appropriately. Another option would be to use automated pen testing software or red teaming tools mapped to MITRE ATT&CK™.
While the latter would be the most effective, these tools often test only certain attack vectors, while failing to simulate the full attack kill chain to emulate the behavior of a multi-vector cyber- attack, or Advanced Persistent Threat (APT). Additionally, they do not necessarily emulate the very latest threats and techniques.

Simulate the Latest Threats with the MITRE ATT&CK™ Framework

With Cymulate's SaaS-based Breach and Attack Simulation (BAS) module, access the best of all worlds:

- Industry-recognized threat modelling using the blocks of the MITRE ATT&CK™ framework
- Simulations of the very latest techniques utilized by current cyber threats, updated daily
- Full attack kill chain coverage, emulating the logical events flow of a multi-vector APT
- Simple wizard-based templates for customizing attack simulations to your needs
- Automation of ATT&CK-based simulations, so you can run them daily, weekly, or wheneve
- Remediation and mitigation guidelines mapped to ATT&CK™ for additional context

Don't Speculate. Cymulate.


Wizard-based ATT&CK templates

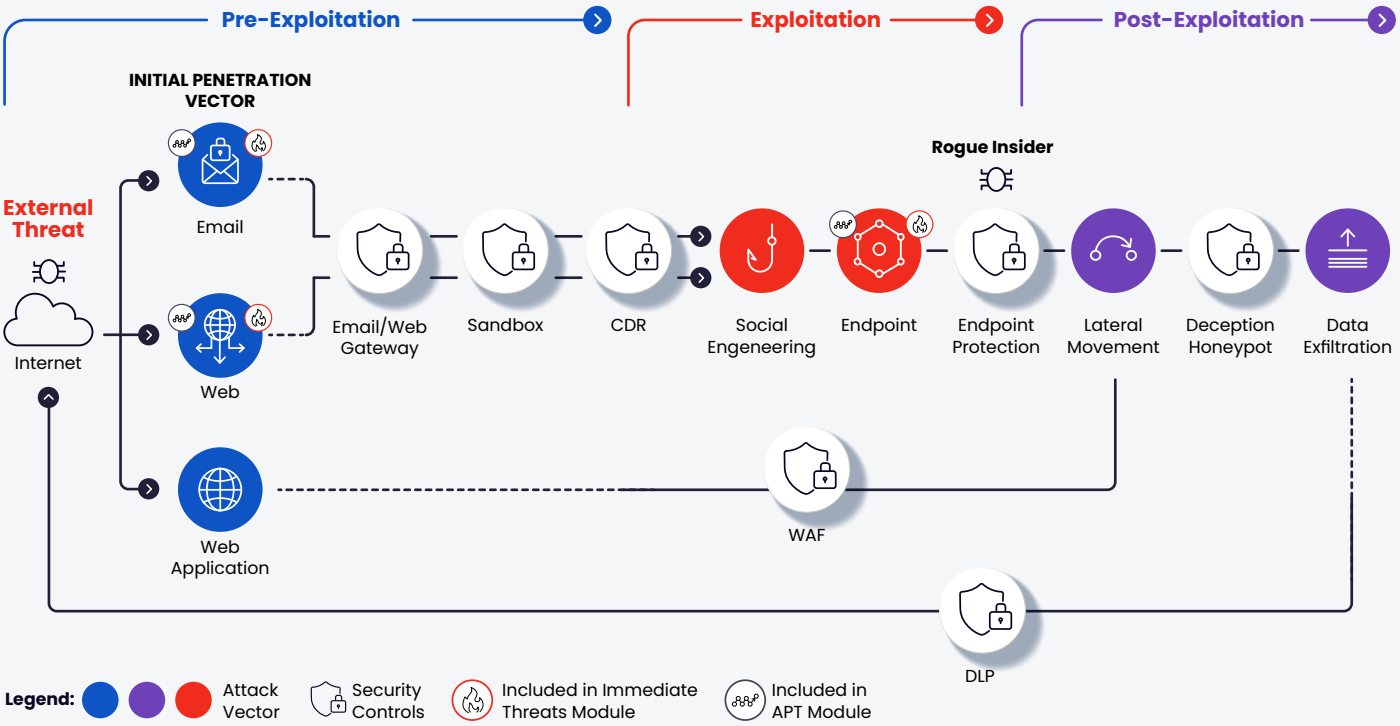

PC or Mac


Test security across the kill chain


Simulate the very latest threats


Deploys seamlessly


Simple to use



Award-Winning Breach and Attack Simulation Technology

Cymulate Extended Security Posture Management approach integrates an award-winning SaaS-based Breach and Attack Simulation (BAS) platform that makes it simple to know and optimize your security posture any time, all the time.

Fully automated and customizable, Cymulate's BAS challenges your security controls against the full attack kill chain with thousands of simulated cyber-attacks, both common and novel.

Testing both internal and external defenses, the attack simulations show you exactly where you're exposed and how to fix it—making security fast, continuous, and part of every-day activities.

Cymulate's BAS module can be run independently or in combination with either or both the Continuous Automated Red Teaming (CART) and the Advanced Purple Teaming Framework.

This solution brief focuses exclusively on the BAS module.

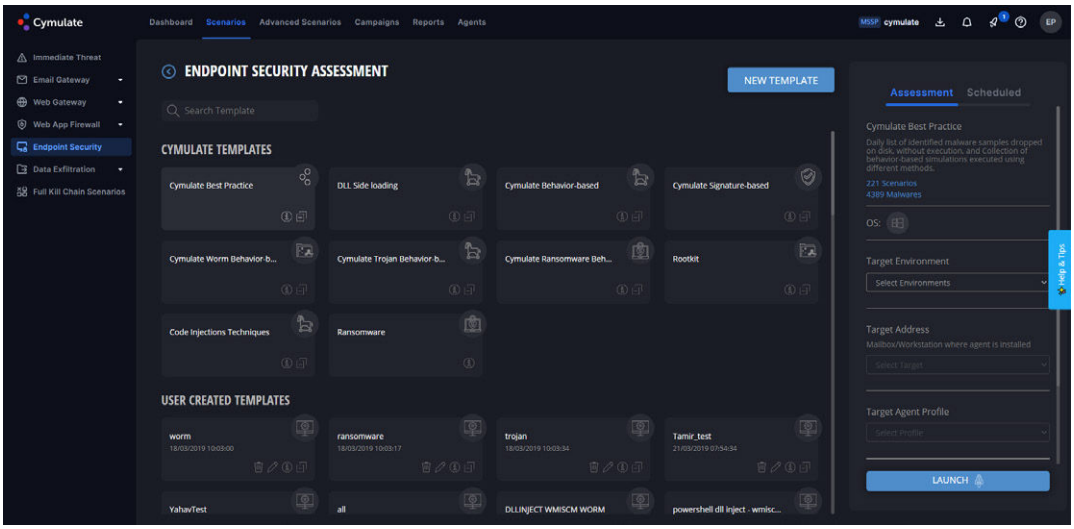
Simulating ATT&CKs™ with Cymulate's BAS Module

Using intuitive wizard-based templates, Cymulate lets you create your own ATT&CKs™-based simulations, by choosing out of over 100 ATT&CK tactics and techniques:

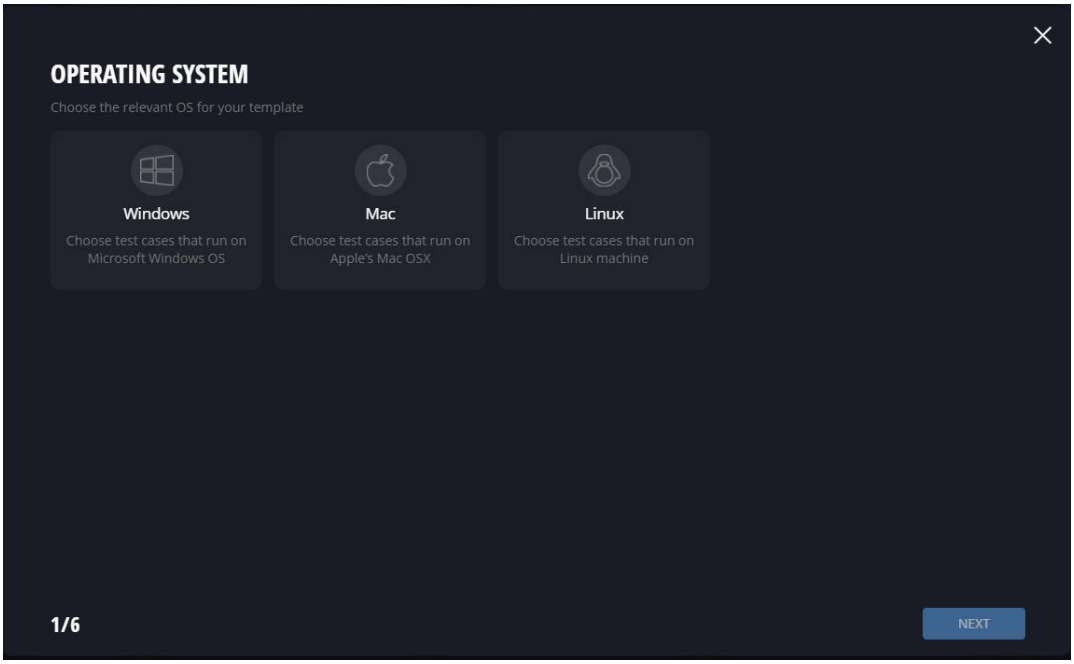
- **Endpoint Security** – Whether on Mac or PC, test the effectiveness of your EPP, EDR, AV and NGAV solutions by crafting your own simulations (see Section 2 below).
- **Email Gateway, Web Gateway, Web App Firewall** – Additional specific module all using similar and easy-to-use flow as the Endpoint Security module described in detail in section 2 below.
- **Full Kill Chain APT** – Emulate the logical flow of a full blown APT by crafting your own ATT&CK-based APT simulation, or by selecting from among APT templates that mimic the modus operandi of well-known APT groups see section3 below).
- **Immediate Threats** – Leveraging Cymulate's Research Lab, the latest threats are uploaded to the platform almost daily, letting you test your security controls against the very latest ransomware, malware, phishing, crypto-miners, and other threats detected in the wild. The threat simulation is mapped to MITRE ATT&CK™ techniques, which can be used to build a custom simulation template (see section 4 below).

02 | Creating an ATT&CK Based Endpoint Security Scenario Template

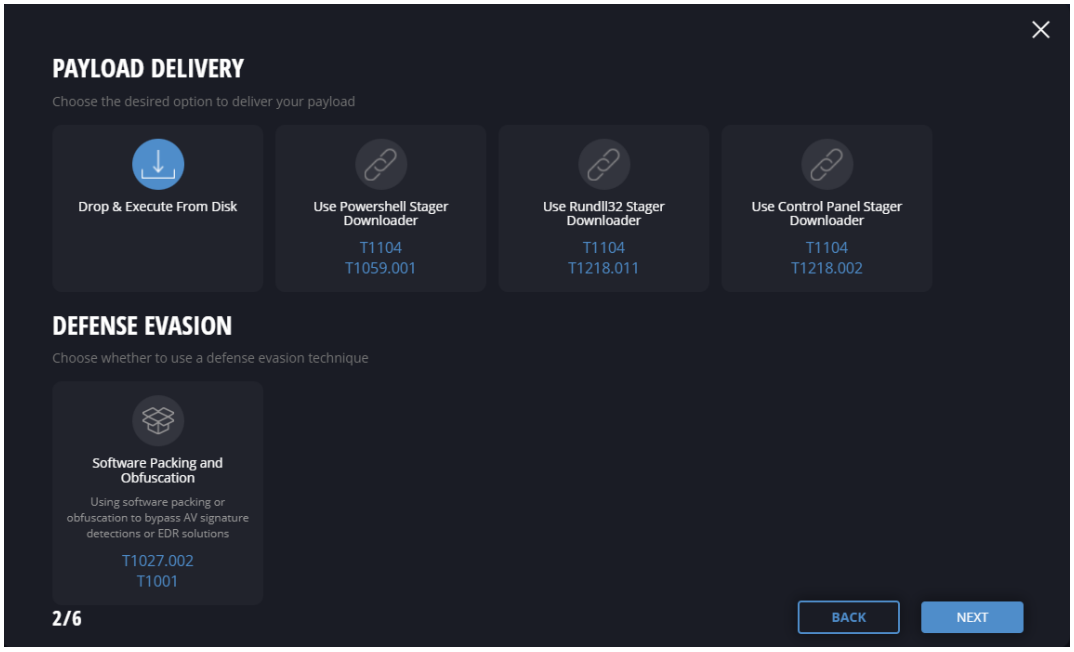
In addition to the out-of-the-box Cymulate templates, you can create customized Endpoint Security templates as follows.



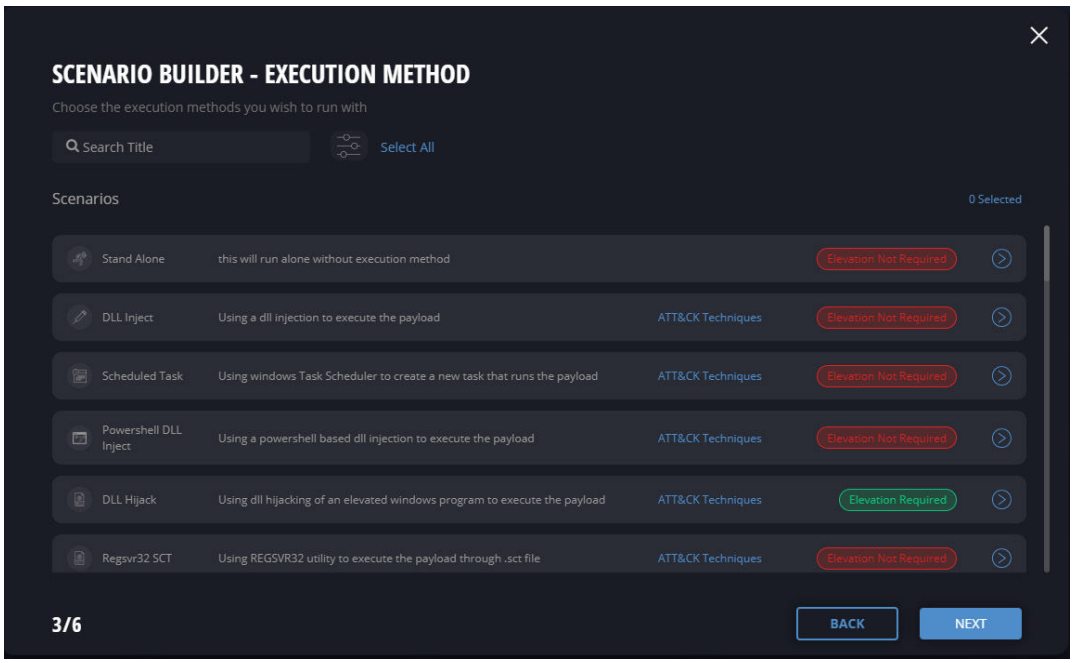
01 From the Scenarios page, Endpoint Security tab, click the **New Template** button.



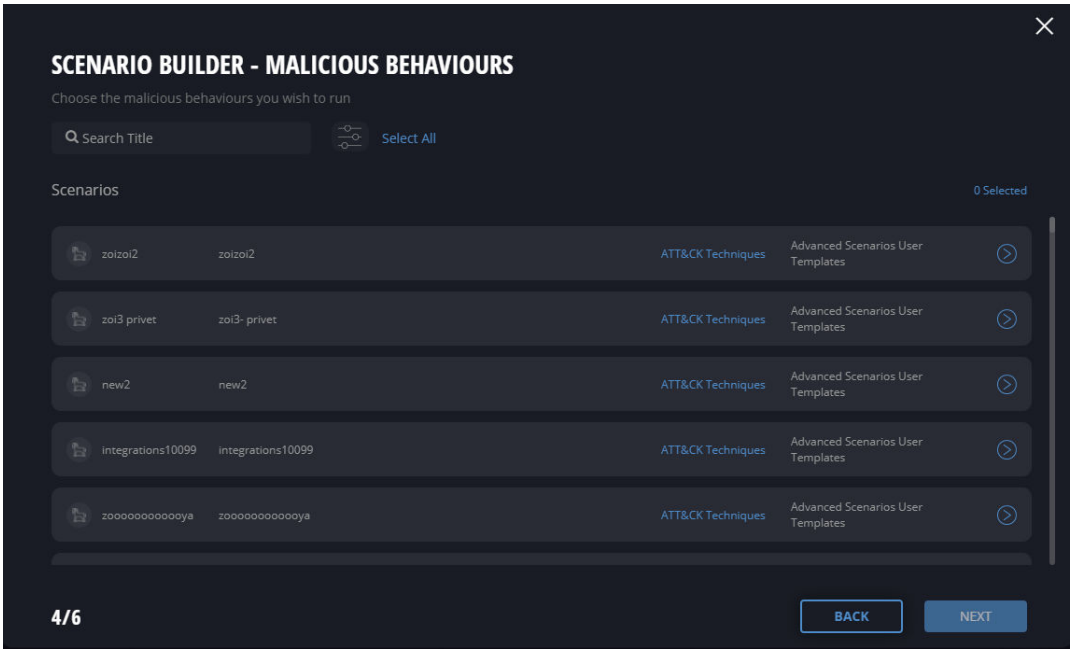
02 Select the Operating system



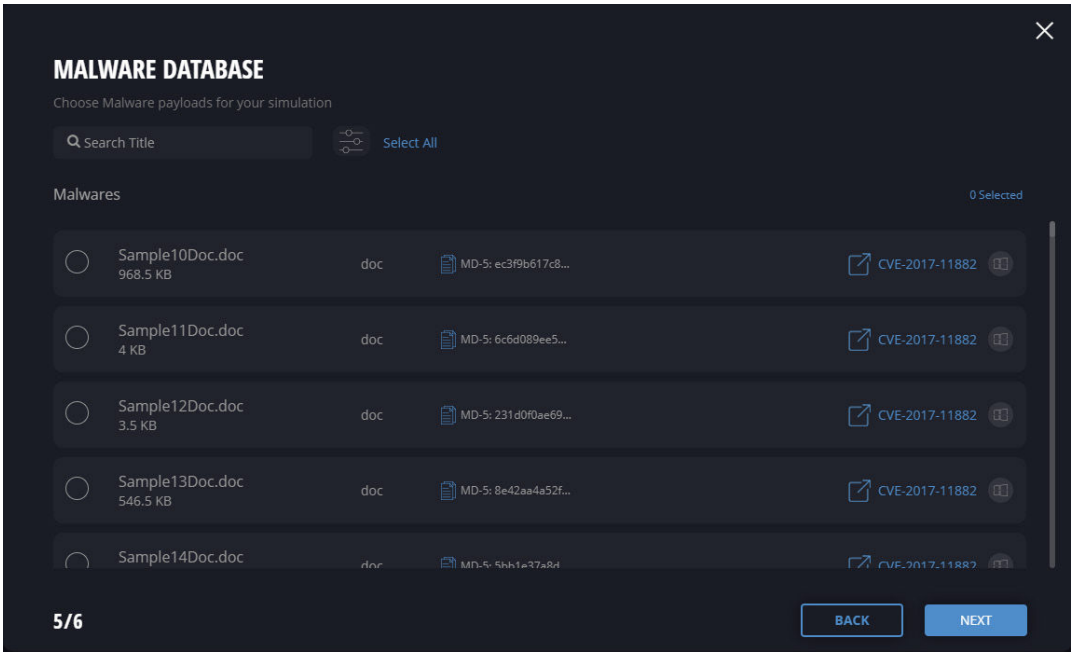
03 Select the payload delivery option and, if needed, the defense evasion technique.



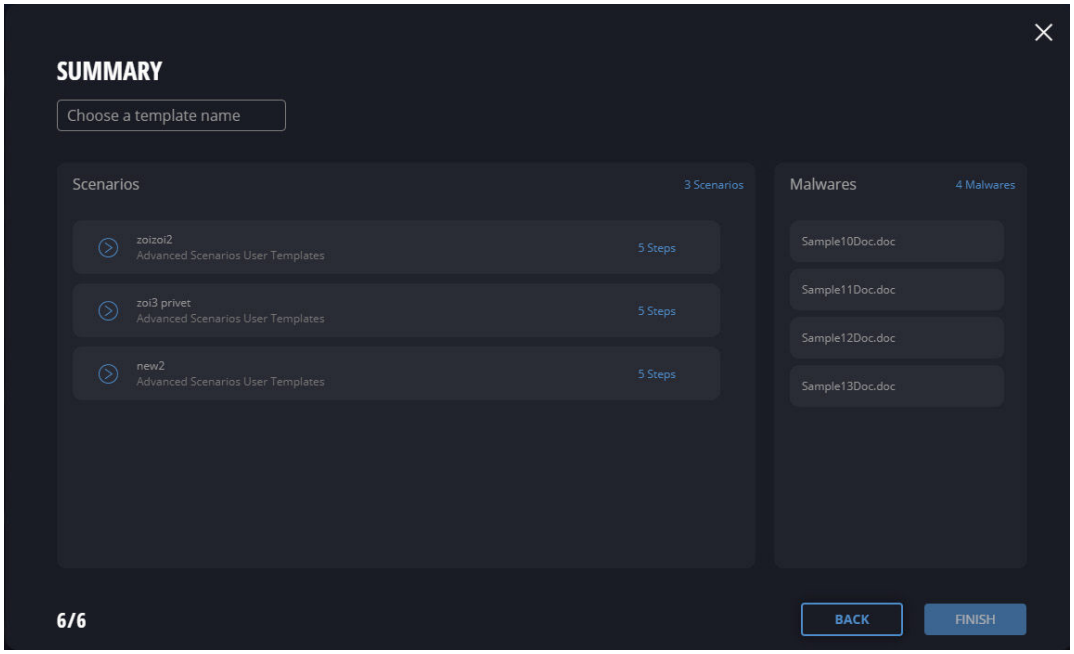
04 Select one or more execution methods to run during the assessment.



05 Select one or more malicious behaviors to run during the assessment.



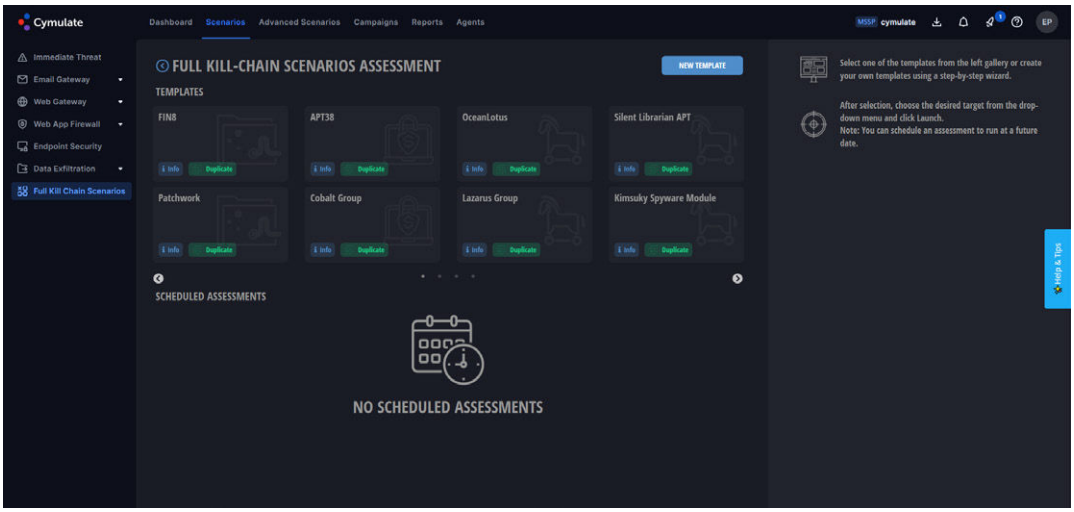
06 Select one or more malware payloads to simulate.



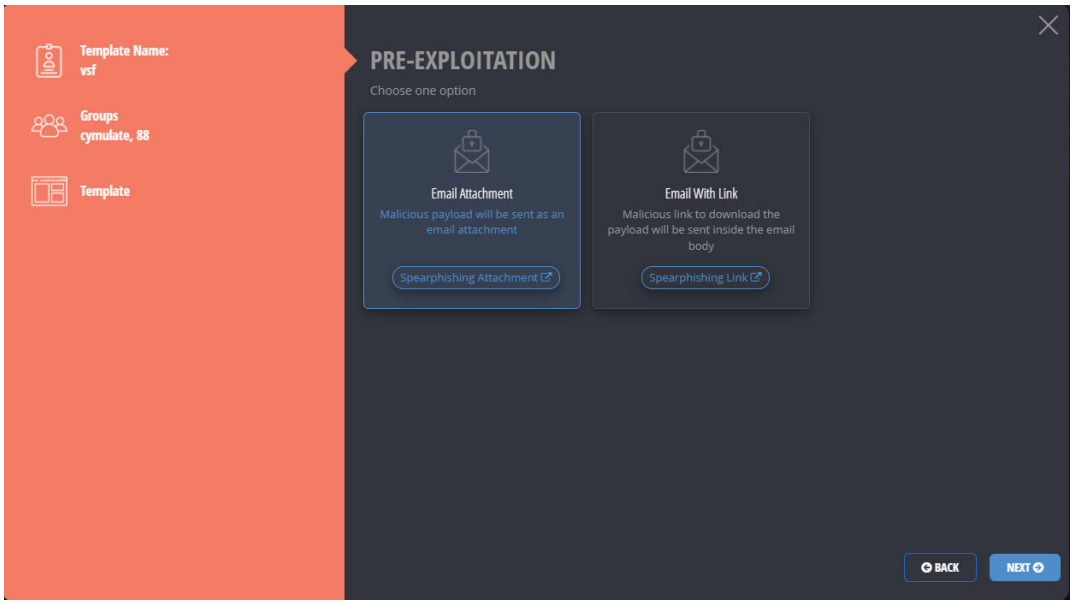
07 Name and save the template.

03 | Creating a Full Kill Chain Scenario Template

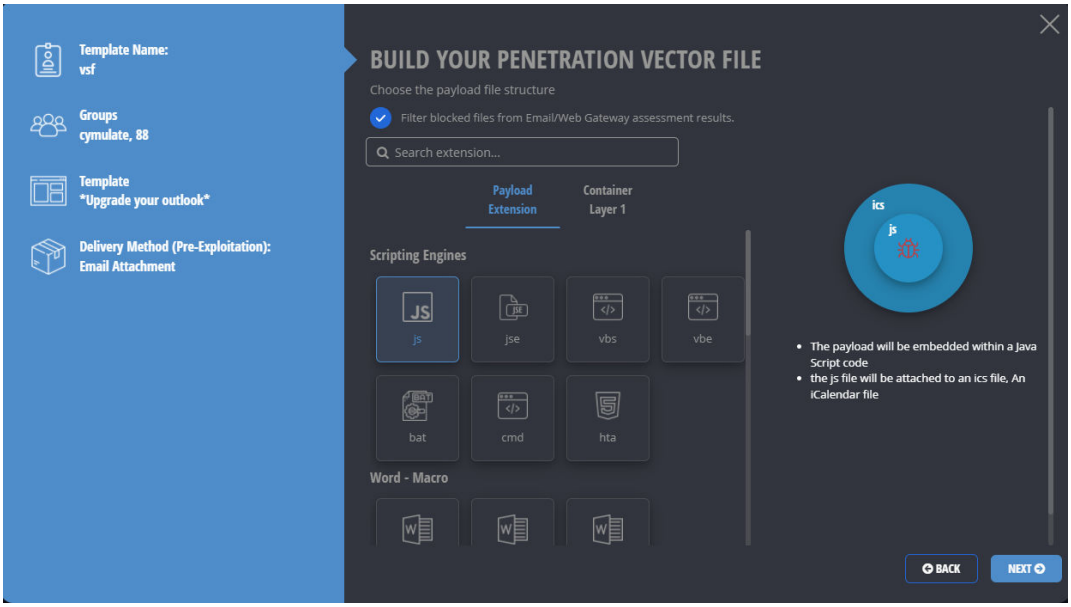
In addition to the out-of-the-box Cymulate templates, you can create customized Full Kill Chain Scenarios templates.



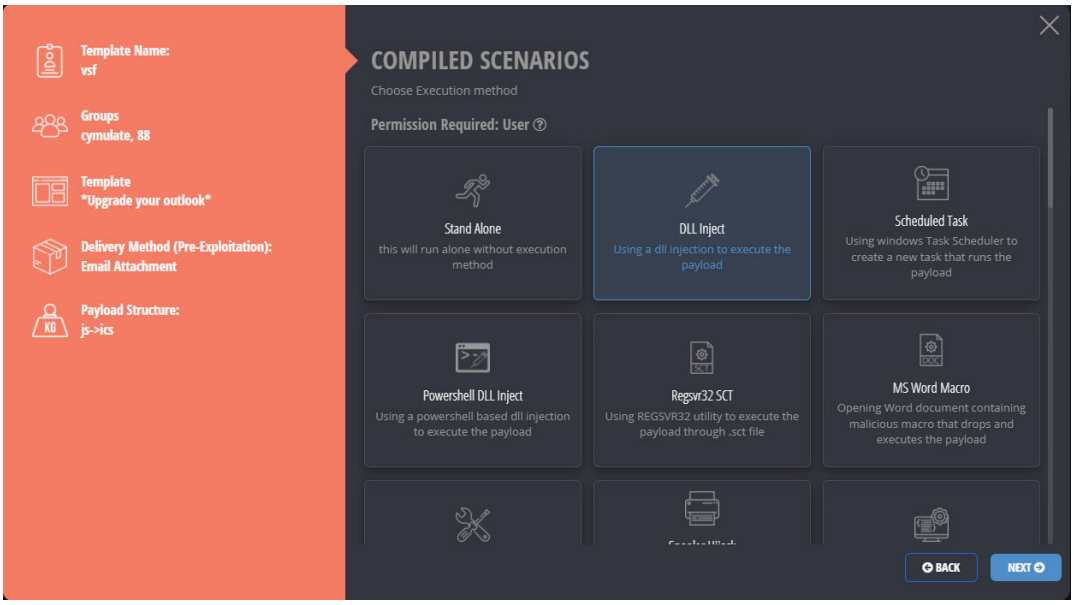
01 From the Scenarios page, **Full Kill Chain Scenarios** tab, click the **New Template** button.



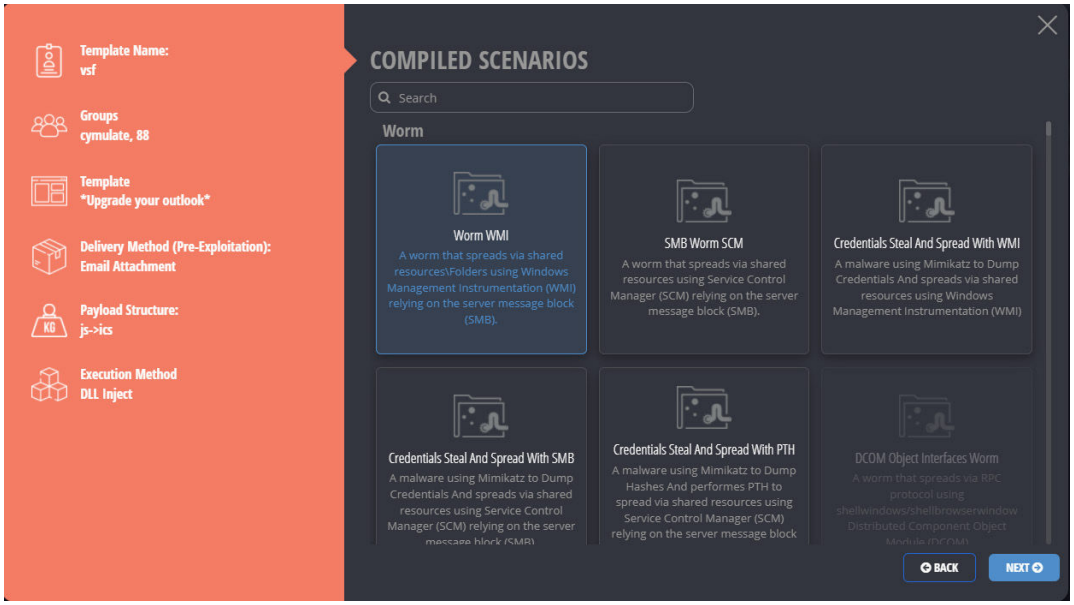
02 After naming the template, select a pre-exploitation payload delivery option.



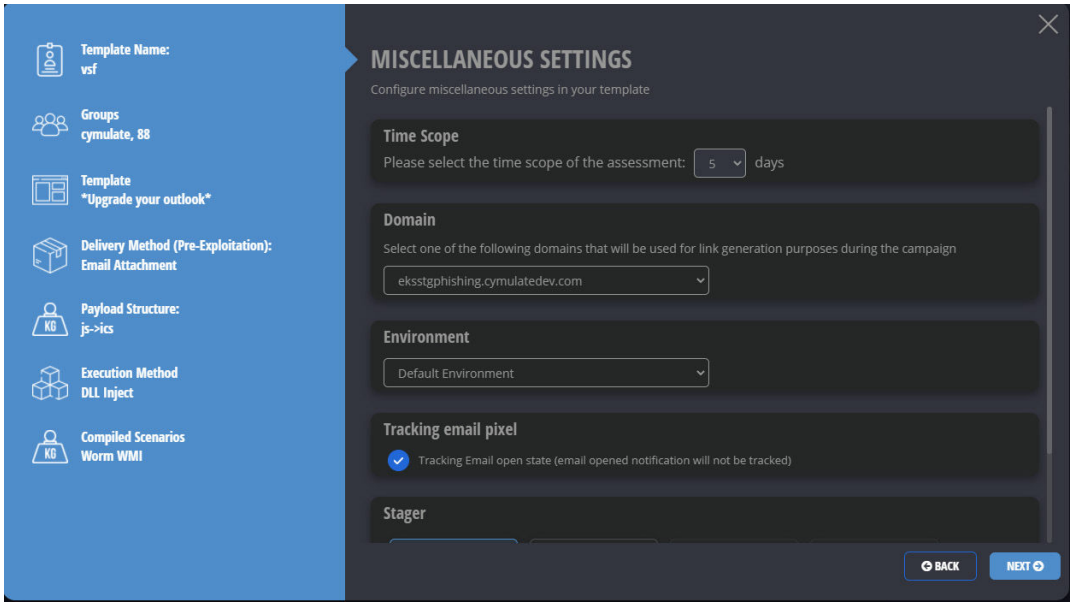
03 Build the penetration vector file (select the payload extension type and define layered containers to further embed the payload).



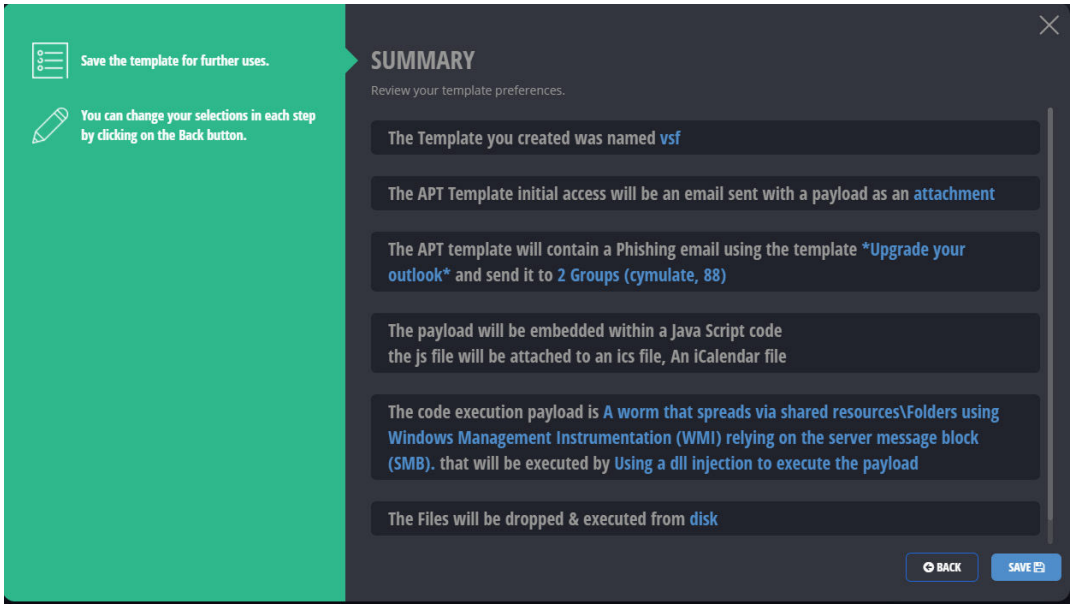
04 Select an execution method (user or administrator level.)



05 Select an attack method from the listed methods (i.e., Ransomware, Worms, Trojans, Lateral Movement, or user- created templates)



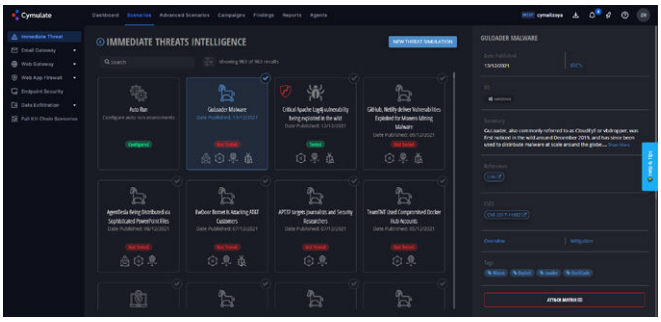
06 Define the miscellaneous settings.



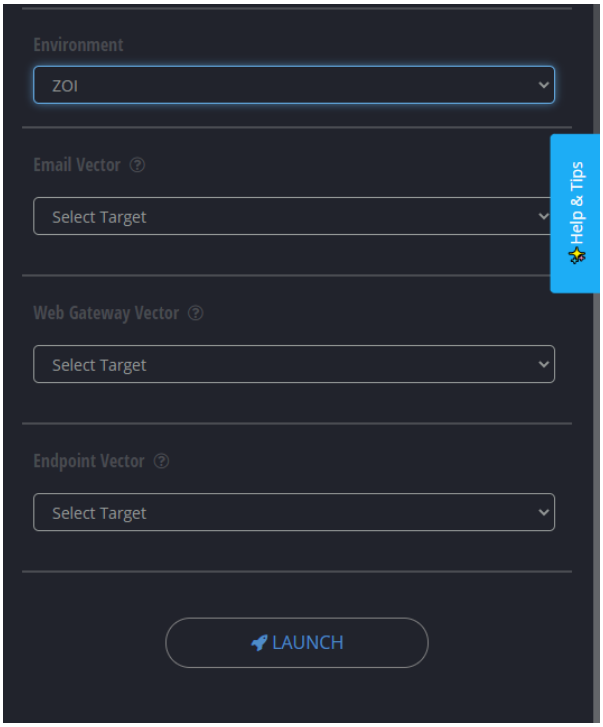
07 Review the template summary and save it. The newly created template is available, editable, deletable and duplicatable in the Full Kill Chain Scenarios page.

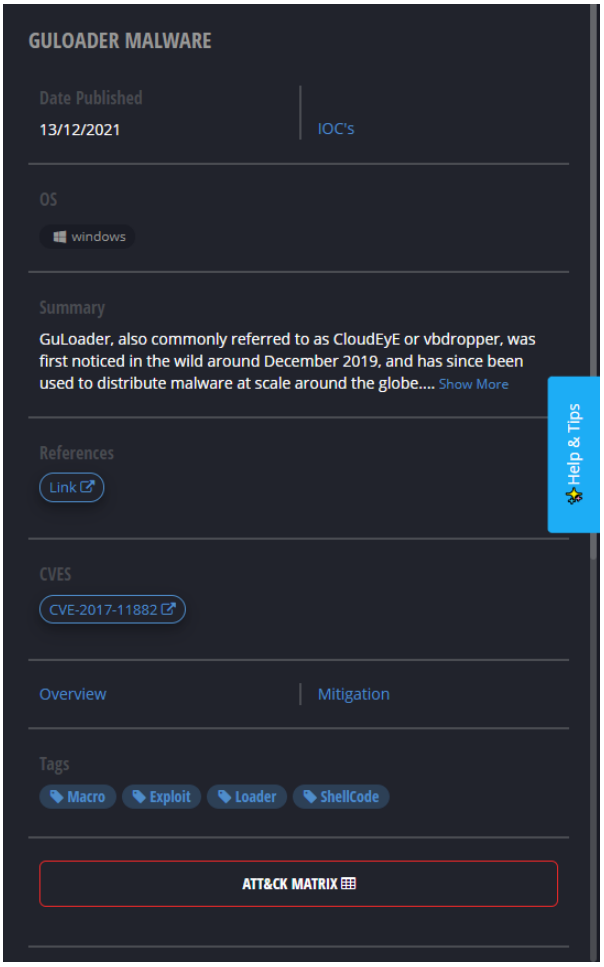
04 Launching Immediate Threats Assessment

You can easily check how resilient to a specific immediate threat your infrastructure at any time, simply by launching the corresponding Immediate Threat Intelligence vector.
Or you can let the Immediate Threat Intelligence module run automatically at all times.



01 In the Scenarios page, go to Immediate Threat and select the **Immediate Threat** for testing.

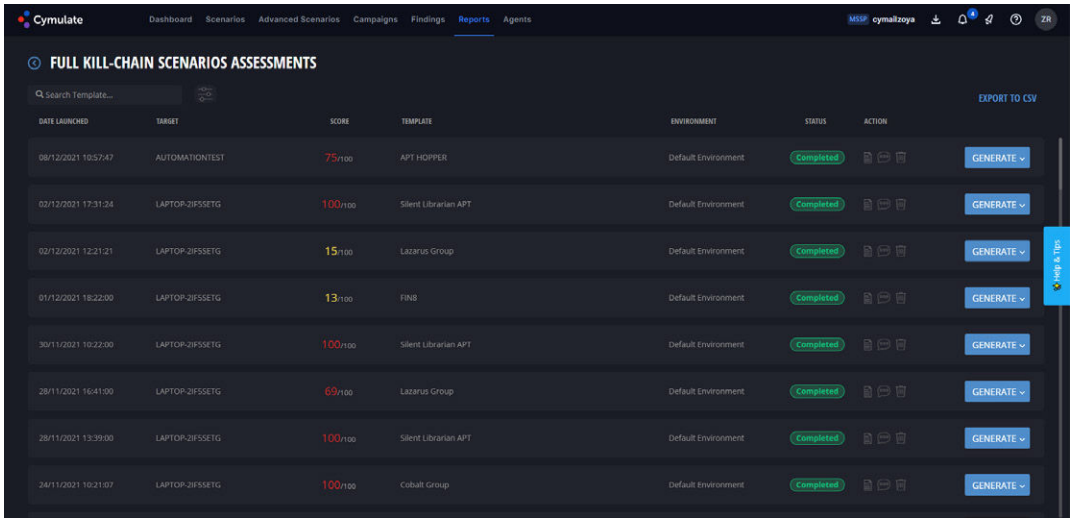




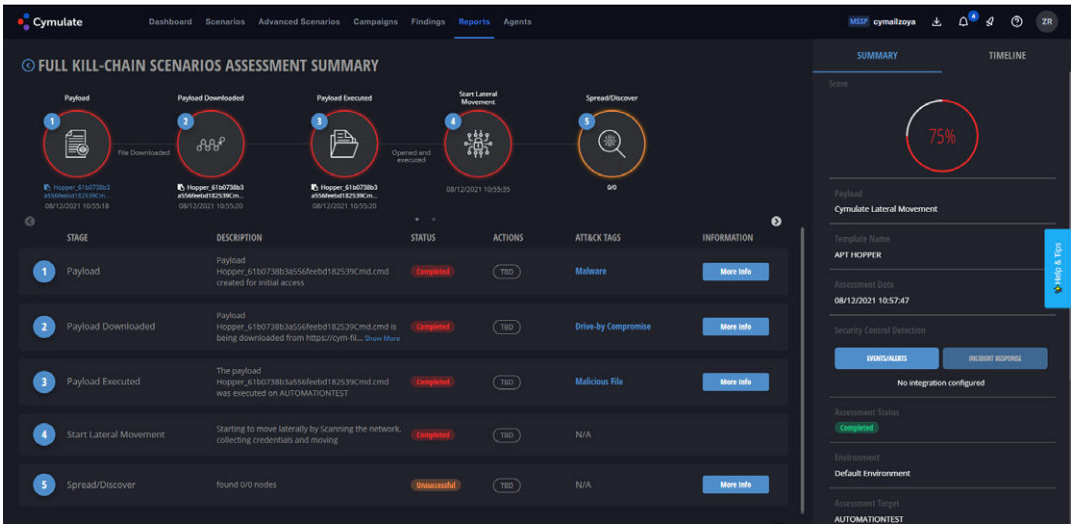
02 From the right pane, you can review:

A. **Date Published** – Date that the threat was published.
B. **IOCs** – Click to view the IOCs for the threat.
C. **OS** - Relevant operating system for the threat.
D. **Summary** – Summary of the threat.
E. **References** – Links to reference articles.
F. **Overview** – Click to view a more detailed overview about the threat.
G. **Mitigation** – Click to view mitigation suggestions to protect against the threat.
H. **ATT&CK Matrix** – Click to view the MITRE & ATT&CK matrix for the threat.

03 Select the targets for the relevant vectors and the integrations and launch the assessment.



04 The launched assessment and its progress will be listed under the reports tab.



05 Access detailed information by clicking the relevant assessment.

Cymulate

05 | Additional Benefits of Security Testing

Security effectiveness testing and attack simulation tools not only deliver immediate visibility into potentially damaging security gaps, they also provide critical insights for strengthening the organization's overall security posture.

They give your security team control over testing so they can make the most informed decisions for tailoring defenses to the organization's most pressing needs.
Additional benefits include:

Security posture at a glance

Get immediate visibility into your cyber-stance across the digital estate—on-demand or continuously without waiting for reports.

Executive and technical stakeholder buy-in

Effectively communicate quantifiable security gaps to the board, executive team, IT staff, and users.

Continuous Optimization

Complement or replace manual and homegrown testing methods with fully automated, repeatable sets of tests that can be run across your infrastructure at any time.

Test effectiveness

Measure the impact of policy changes, software updates, and new or prospective technology purchases to avoid creating vulnerability or opening a gap.

Rationalize security investments

Use objective metrics to benchmark and compare the effectiveness of different security solutions. Prioritize budget allocation and spending based on risk metrics and potential impact.

Validate compliance

Quickly and easily ensure that your organization remains compliant by assessing potential exposure across your infrastructure—without having to wait days or weeks for assessment reports.

KPI metrics

Gain quantifiable benchmarks for an immediate, objective understanding of vulnerabilities and exposure levels. Metrics also provide a way to measure security control performance over time and compare your organization to others in your industry.

Start Your Free Trial

Contact us for a live demo, or get started with a free trial

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632