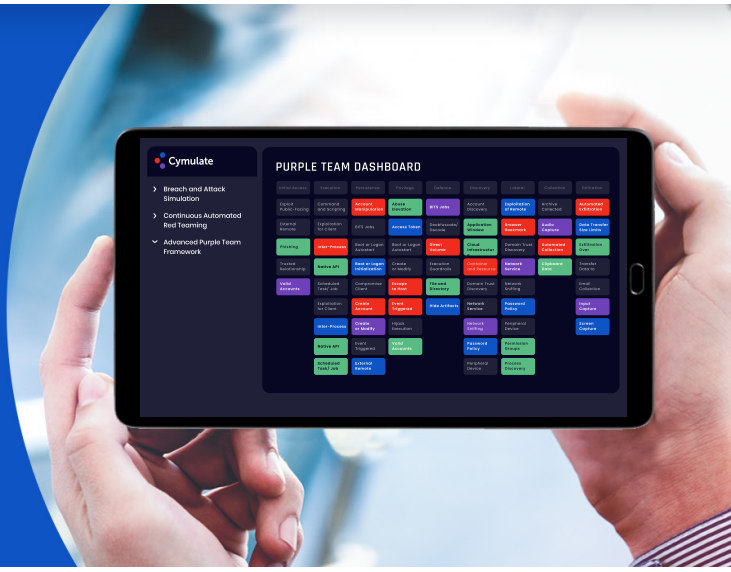
# Purple Team Module Solution Brief

Customized and Automated Security Validation and Assurance




## Introduction

The security of an enterprise is based on threat prevention, detection, and response; and the effective enforcement of the corporate security policy. Threat prevention technologies are common to all types of industries and company sizes; and their efficacy can be validated with out-of-the-box Cymulate security control validation assessments, requiring minimal customization. Organizational security policies, on the other hand will be unique. They include data classification and handling, access controls, segmentation policies, and policies required for regulatory compliance.
Every company's security policy will be different and will require customized validation and assurance procedures. Coupled with the inherent complexity of most validation platforms (such as penetration testing suites); this produces a situation where each validation must be highly customized - even when testing common defensive tools.

Many companies have begun to engage in Purple Team exercises that test their incident response capabilities and their resilience to the Full Kill-Chain of an Advanced Persistent Threat (APT) or a subset of such tactics.

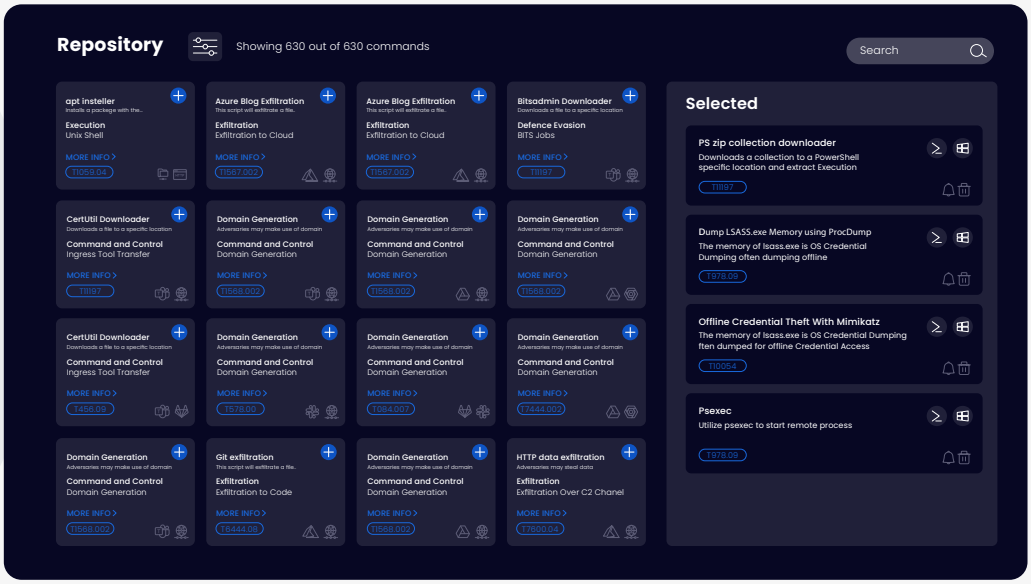
The Cymulate Purple Team module takes BAS customization and automation to the next level to address and support these requirements.
The module enables SOC/Blue Teams with minimal adversarial skills, along with professional Red Teams, and pen-testers to create, store, modify, and execute both simple and sophisticated assessments using custom built or out-of-the-box templates - with the ability to leverage custom payloads and executions where desired - and is fully managed via API and/or a web-based GUI.

| Use Case | Audience | Description |
|---|---|---|
| **Purple teaming** | Blue Team/SOC & Red Team | Adversarial simulations to exercise incident management |
| **Security Assurance Automation / Regression Testing** | Blue Team/SOC | Create and automate assurance procedures (dailies) that ensure changes in IT & security have not impaired security efficacy or policy enforcement |
| **Scaling Expertise** | Red Team | Create, share, and reuse assessment templates, building blocks and resources; leveraging automation for increased operational efficiency |
| **Security validation** | Blue Team/SOC | Measure and track security resilience to APT group Tactics, Techniques, and Procedures (TTPs) codified across the MITRE ATT&CK framework |

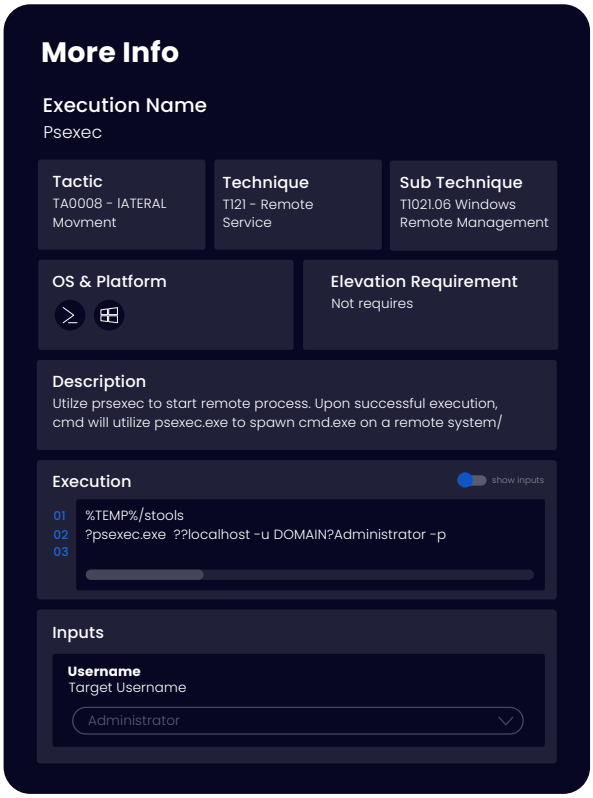
## Template Driven

Assessments are based on templates, and templates are comprised of both built-in executions, payloads, programs, tools, along with custom resources and data sources, as desired.

A template can be a simple set of atomic executions or a complex set of commands along with chained atomic executions.




Executions are aligned to the MITRE ATT&CK framework which is used extensively to leverage the de-facto standard taxonomy it provides.
The execution repository provides extensive coverage of the framework; covering all 12 tactics and all applicable techniques and sub techniques.
Within the Repository are Executions supporting Windows, MacOS, and Linux Operating Systems; and different execution languages such as: PowerShell, Windows Command scripting, bash and other shell scripting, and python - to name just a few.




## Configuring Executions

In order to create true simulation of an attack flow, executions need to be configured for their input, dependencies, success indicators, and outputs.
The Purple Team module provides a comprehensive configuration system to aid in the discovery of what parameters are required and streamline parameter input. The parameters can be entered manually; or they can be chained to receive the output of previous executions or external sources as described below in the example.

## Chaining Executions

In advanced mode the module provides logic to chain executions for both input variables and dependencies using a visual layout editor. For example, a chain could be comprised of the following:

**01.** Dump LSASS using ProcDump to prepare it for Mimikatz.

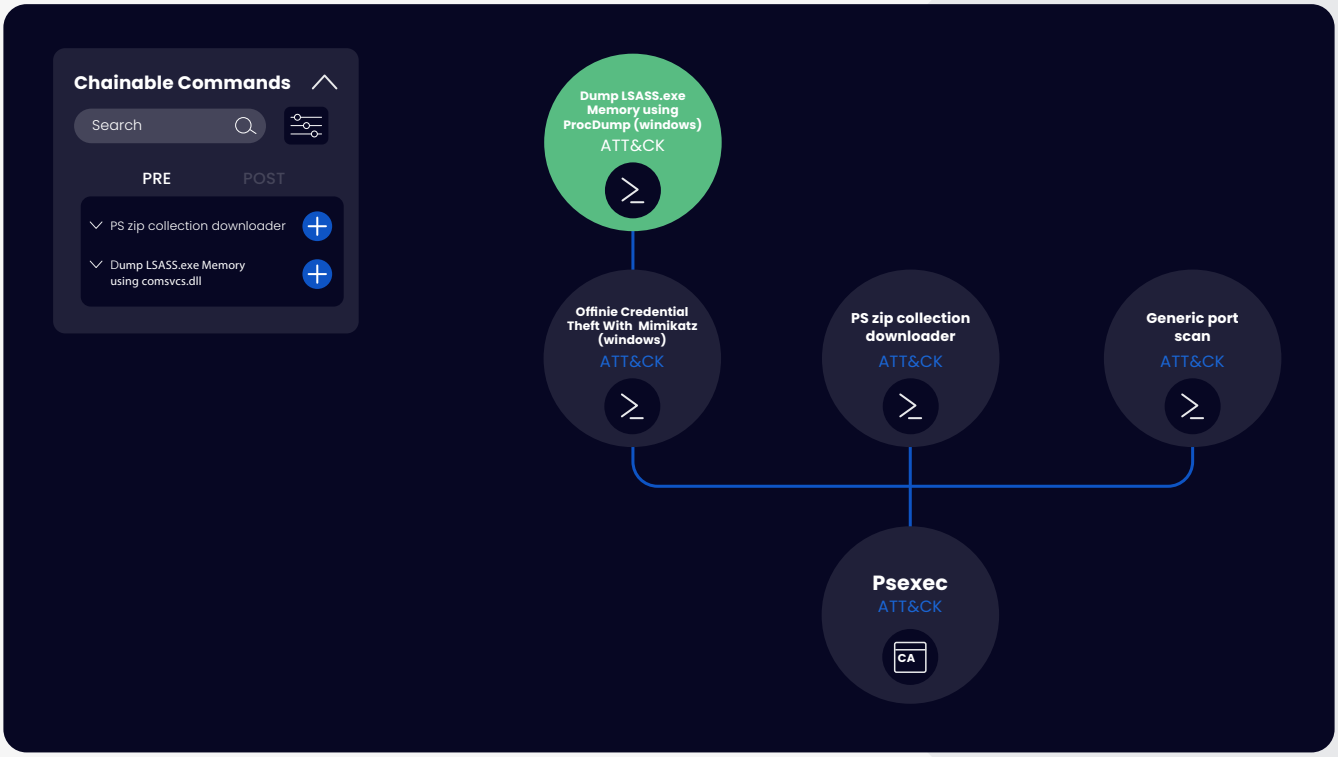
**02.** Use Mimikatz to get credentials (username, password, domain)

**03.** Download PSexec using PS zip collection downloader

**04.** Run a port scan to get the target host and ports

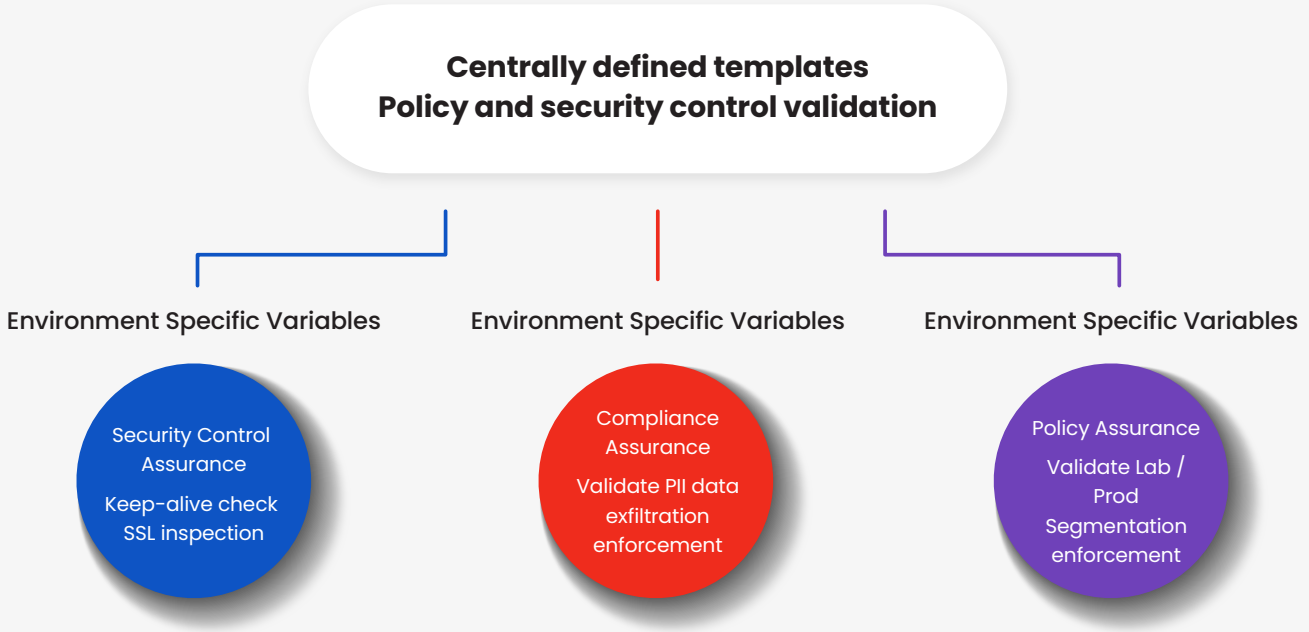
**05.** Use PSexec with all the inputs and dependencies from the previous steps

Templates can be a single chain of executions (such as the example above); but can also link together multiple chained executions to create more sophisticated attacks. The template is then mapped to show its coverage across the MITRE ATT&CK framework and saved for use in assessments (see below).




## Launch an Assessment

An assessment is a single “run” of the process created from a template. The assessment can be modified using the same GUI or API used to create templates to add additional executions or change parameters for this specific run. For example: alerts can be set and environment specific variables can be modified or set if they will not be chained. Additionally, the assessment can be scheduled one-time or set up to be recurring to automate security assurance programs.
Before launch, the assessment is validated for readiness, highlighting for example dependencies or execution pre-requisites that need to be fulfilled.




This model enables a central team to create templates that can then be modified for specific environments, subsidiaries, and geographies as assessments. The same model also serves a security service provider providing automated security validation and assurance services to their customer base.

## Assessment Results

The result of an assessment provides a detailed analysis of success and failure in addition to prescriptive remediation guidance.
The assessments provide visibility so that an organization can know where it is exposed; and evaluate the efficacy of its security controls and configurations. The results are mapped to the MITRE ATT&CK framework and its taxonomy for ease of use by both Blue Teams/SOC groups and Red Teams alike. Integrations with Endpoint Detection and Response (EDR) and Security Incident and Event Management (SIEM) systems provide correlation between executions and the findings of these external tools, to evaluate the effectiveness of their detection capabilities. Integrations with Vulnerability Management systems will provide attack context to better determine the priority and urgency of remediation – allowing teams to focus on remediating exploitable vulnerabilities first.

## Purple Team Dashboard

The Purple Team dashboard provides a high level summary of all assessments so that areas of high risk and exposure to specific techniques can be easily identified and prioritized for remediation.
It includes a histogram that visualizes security drift over time - both for the aggregate results and for each of the MITRE ATT&CK tactics.
The dashboard makes it easy to monitor resilience to specific APT groups and the TTPs they use.
It also provides a similarity analysis to threats found in the wild (based on the Immediate Threats Intelligence module, also found in the Cymulate platform) and a summary of techniques and sub techniques launched, succeeded, and failed.


## Benefits

The Purple Team module brings endless options and scale to everyone in the Security Team; Blue Team groups assessing security controls, SOC groups maintaining a watch over critical systems, and Red Team groups planning and executing attacks. Assessments can be launched in different types of environments and can be deployed on-prem, in cloud environments, or to assess protections for remote worker connectivity.

The module extends automated security visibility and optimization to environments and scenarios that are unique to different organizations, personnel with different job responsibilities, and security professionals of different skill levels.

The benefits of the module extend beyond operational efficiency for both in-house teams and companies that provide Red Team and pen-testing services. It enables large organizations to leverage and scale the expertise of central teams to launch tailored assessments across more geographies and subsidiaries. Assessments can also be replayed to validate lessons learned from previous exercises. The platform can also be used to create and automate recurring assessments that are tailored to security assurance programs and auditing requirements.

| Benefits for security service providers | Benefits for in-house Purple Teams and pen-testers |
|---|---|
| Leverage more personnel effectively and scale your expert resources | Leverage and scale the skills of your central teams and utilize all security employees |
| Differentiate your service offerings with your own customized assessments and automation | Create custom assessments for your company's unique environments and scenarios |
| Create and operationalize customer-specific testing scenarios | Automate security assurance procedures |
| Increase your addressable market with affordable automated assessments | Automate recurring compliance testing mandates |

For service providers, the Purple Team module can make Red Team exercises and pen-testing accessible and achievable to a larger market, where cost is a limiting factor.
Automation will increase the operational efficiency of your experts, enabling them to focus on high value tasks; creating scenarios and templates, analyzing the results of an exercise, and providing guidance to improve incident management and response procedures.

Junior security personnel can run Assessments from Templates created by your experts; freeing the experts from routine tasks and allowing them to focus on higher-value operations.
Enabling service providers to help more organizations be more secure. In-house security teams can perform more Assessments in more areas of the organization with the same number of personnel. Blue Teams and SOC analysts can re-run assessments on their own to confirm successful remediation or to test alterations to security protocols and policies. All levels of expertise can assist in security and compliance testing; leading to more incremental advances, more often, and removing the bottleneck caused by point-in-time testing on an infrequent basis.

## About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their Cybersecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company-and every company-will be.

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

**Start Your Free Trial**

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