Cymulate

Web Gateway

Solution Brief

Securing Your Web Gateway

Cymulate's Web Gateway vector validates your organization's web security controls. This vector challenges the controls that protect employees from both accessing and downloading malware from malicious and compromised websites.

Attack Vector Overview

Malicious and compromised web sites are commonly used by cyber-criminals to gain a foothold or steal information. These include web sites that infect browsers with drive-by downloads and phishing web sites that mimic legitimate sites to steal user credentials. A growing proportion of web sites use HTTPS encryption to convey a false sense of security to the end-user.

Cymulate's Web Gateway vector simulates an employee accessing malicious websites.
The tests are performed over HTTP and HTTPS by the Cymulate agent to validate the effectiveness of the organization's web security from a controlled endpoint on the production network.

Continuous Testing

The security assessments are performed against a large, continuously growing database of malicious websites that are updated daily for both inbound and outbound vectors. Continuous testing verifies that web security controls are set up correctly and maintained at optimal effectiveness.

How It Works

Test Setup –The Web Gateway tests for both inbound and outbound vectors using the following categories:

Outbound Vectors

Ransomware - Test against a daily updated list of IP addresses and URLs that are associated with ransomware activity.

Phishing - Daily list of IP addresses and URLs that are associated with Phishing

Command & Control (C&C) - Test against a daily updated list of IP addresses and URLs that are associated with botnet C&C activity.

Policy - Test against a sample list of websites that are commonly deemed inappropriate for the workplace and blocked by category. such as Porn, Gambling, etc.

Inbound Vectors

Files - Crafted payloads that mimic the behavior of common malware types such as worms, trojans, and spyware (downloaded over HTTPS).

Exploits - Working PoCs for known CVEs that exploit buffer overflows and other vulnerabilities in various applications (downloaded over HTTPS).

Test Execution – Once the test is launched, the Cymulate agent runs through all the attack vectors. Malicious files and exploits are downloaded in a controlled and safe manner, without execution. All downloaded files are deleted from the disk by the end of the assessment. Testing can be performed on-demand or scheduled.

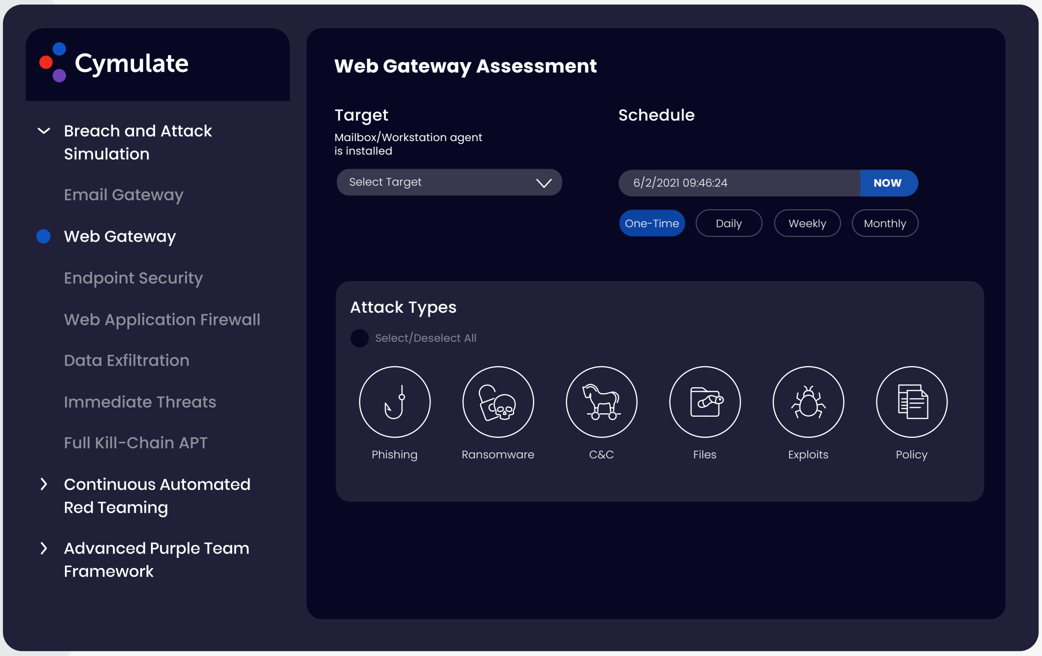
Test Results and Remediation – A comprehensive report is generated after each web gateway assessment, comparing the result to previous assessments and identifying the security gaps that need to be addressed.

Key Features

- Test using one dedicated machine which does not affect users or servers in the organization's network.
- All stages of the test are done automatically, including website access, file downloads, and clean-up on completion
- The tests are updated daily with malicious URLs for continuous validation of the web security controls.

Actionable Insights

The simulation results are presented in an easy-to-understand comprehensive report. Mitigation recommendations are offered for each security gap discovered depending on the type of simulated attack, enabling IT and security teams to take the appropriate countermeasures.



Web Gateway Assessment

Target
Mailbox/Workstation agent is installed
Select Target

Schedule
6/2/2021 09:46:24
One-Time

Attack Types
○ Select/Deselect All

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