Cymulate

Attack Surface Management (ASM) Data Sheet

Cymulate's ASM technology discovers which digital assets are exposed to adversaries to access, exploit, and collect information during the reconnaissance phase of an attack.
It scans the domains, subdomains, IPs, ports, etc., for internet-facing vulnerabilities and for Open-Source Intelligence (OSINT).

Capabilities

01 **Automated scanning and discovery of public-facing and internal systems**
The Cymulate ASM module scans organizations' external and internal surfaces to identify exposed assets.

02 **Definition of exposed assets and platforms**
Discovered assets and platforms are described to facilitate a rapid understanding of the data collected.

03 **Discovery of outdated and/or exposed applications and frameworks**
Simulated attacks to discover exploitable security gaps stemming from expired subscriptions, outdated or legacy software versions.

How it works

01
Find directly- and indirectly-controlled external assets

02
Prioritize discovered vulnerabilities and misconfigurations

03
Remediate prioritized and exploitable security gaps

Clear-Web & Dark Web Compromised User Information/ Credentials

Cloud and infrastructure misconfigurations

Exploitable web applications

Vulnerable 3rd party software and indirect assets (e.g., shadow IT)

Cymulate

Key Features

Fully automated internal & external ASM
Easy to deploy and straightforward to use

Not reliant on survey-based auditing
All findings are backed by hard data

Discovers unaccounted-for resources
Identifies and locates resources that were previously not accounted for or recorded

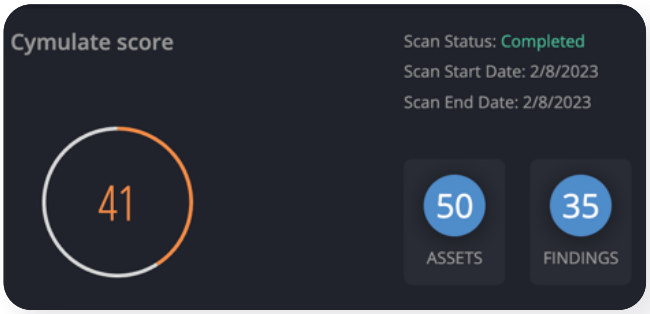
Continuous, automated checkups
Swift evaluations lead to prompt adjustments based on up-to date information

Third-Party Assessments
Evaluate exposures as part of a vendor security assurance program

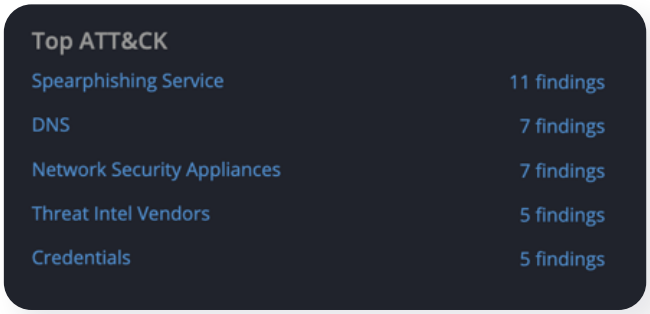
Mitigation and remediation plan
Reduce MTTR with actionable remediation guidance

Attack Surface Management Dashboard

Overall Score -
Security score based on simulated attack success rate correlated with industry standards

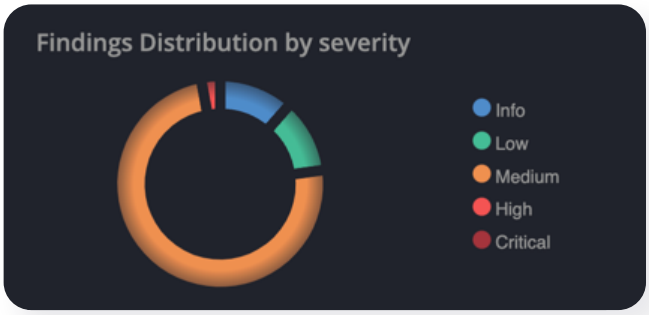


Top Findings -
At a glance, expandable, view of top attacks, top assets and top findings

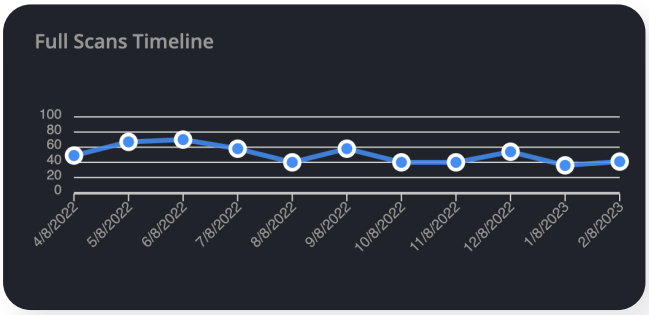


Cymulate

Findings Distribution –
Immediate understanding of findings distributions by category, severity or status, and asset status



Trending -
Easily follow the evolution of the attack surface security with a timeline reflecting the ASM module score at selected time intervals



Customer Quotes

Protection, detection & response measures are effective when there are processes that keep them effective. For this reason, continually testing and analyzing all corporate security measures is a top priority and to carry out these tests effectively & efficiently, Cymulate's continuous validation platform is essential.

Damian Soriano -
Singular Bank- CISO

As the first CISO of SolarEdge I had to build up the team and the security architecture fast. Cymulate has enabled me to benchmark and improve & gain confidence in our results as we continue to build our capabilities Cymulate provides time to value in days, and this value increases as we incorporate it into more aspects of our operations.

Dror Hevlin –
SolarEdge – CISO

As a repeat buyer, I am confident in recommending Cymulate for the visibility it provides to manage our security resources effectively and the efficiencies we gain with continuous security optimization that is simple to use.

Craig Bradley –
YMCA - Senior VP of IT

Awards and Accolades

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

Start Your Free Trial

info@cymulate.com | www.cymulate.com