cymulate BITSIGHT

SOLUTION BRIEF

# Prioritized Threat Validation

## Close the Loop Between Threat Intelligence and Exposure Validation

Security teams have more threat intelligence, exposure data and validation results than ever, but these workflows are often disconnected. Threat intelligence can identify adversaries, campaigns, IoCs and TTPs, but teams still need to know whether their controls can actually prevent or detect that behavior. Validation can reveal control gaps, but without adversary context, teams may struggle to prioritize which scenarios matter most.

The Cymulate + Bitsight integration creates a closed loop between adversary intelligence and continuous exposure validation. Bitsight shows customers which attackers are most active and relevant to their organization. Cymulate uses that insight to prioritize what to test, prove whether defenses are working and help teams fix and retest the gaps that matter most.

Together, Cymulate and Bitsight help security teams move from broad threat awareness to targeted, evidence-based defense improvement.

## Validate Defenses Against Relevant Adversary Behavior

Cymulate operationalizes Bitsight Threat Intelligence through continuous exposure validation. In the Cymulate Platform, Bitsight provides relevant adversaries, campaigns, ransomware groups, APTs, TTPs, IoCs and targeting trends that are then used to focus testing and validation workflows.

Cymulate Vero AI applies the customer's Bitsight threat profile to create custom assessments that reflect the adversaries, techniques and indicators most relevant to the organization.

Security teams can use Cymulate to:

- Analyze MITRE ATT&CK security control coverage for the techniques relevant to their Bitsight threat profile
- Connect flagged techniques to associated adversary groups, scenarios and findings
- Launch existing scenarios or use Cymulate Vero AI to create custom assessments based on the customer's relevant adversary context
- Validate whether controls prevent and detect the techniques and indicators associated with active threats
- Measure prevention and detection coverage against real-world attacker behavior

This helps teams move from identifying relevant threats to validating the defenses designed to stop them.

## Solution Benefits

### Prioritize relevant threats

Focus validation on the adversaries, campaigns, techniques and indicators most relevant to the organization.

### Validate real-world attacker behavior

Test defenses against the TTPs and IoCs used by active threat actors, guided by Bitsight threat intelligence.

### Improve prevention and detection

Identify where controls fail to block or detect relevant threats and apply targeted improvements.

## Close Gaps and Prove Improvement

Validation is only valuable if it leads to stronger defenses. When Cymulate identifies gaps, teams use remediation guidance, automated mitigation and retesting to move from finding a weakness to proving improvement.

Cymulate helps teams:

- Identify where controls fail to prevent or detect relevant techniques and IoCs
- Prioritize remediation based on validated exposure
- Follow remediation guidance to address validated gaps, then deploy relevant IoCs to security controls through Cymulate Auto Mitigate
- Retest after mitigation to confirm protection has improved
- Track whether defenses remain aligned with current attacker behavior over time

This creates a measurable improvement cycle: prioritize the right threats, validate the right controls, close the gaps and prove the defense improved.

## Enrich Threat Intelligence with Validation Evidence

The integration also strengthens the Bitsight experience. Cymulate validation results flow back into Bitsight so customers can see whether relevant adversary techniques, TTPs and CVEs are prevented or detected in their environment.

This gives Bitsight users more actionable context, including:

- Whether a threat actor's techniques are working against the environment
- Whether specific TTPs are prevented, detected, or exposed
- Whether related CVEs are connected to live validation evidence
- Which adversary behaviors represent validated risk versus theoretical concern

By connecting validation evidence back to threat intelligence, the integration helps customers move from assumed risk to evidence-based prioritization.

## Why Choose Cymulate + Bitsight?

### Prioritize with intelligence, prove with validation

Bitsight helps identify which threats matter most. Cymulate proves whether defenses can stop them.

### Focus testing on active attacker behavior

Cymulate users can run scenarios that reflect active adversary behavior instead of testing against the full scenario library.

### Close the loop between intel and action

Bitsight threat context helps focus Cymulate testing, while Cymulate validation results enrich Bitsight views with live evidence.

## About Cymulate

Cymulate is the leader in proactive, AI-powered security that continuously proves, prioritizes and adapts against real attacker behavior – before incidents occur. More than 1,000 enterprise security teams rely on Cymulate for autonomous threat validation and cyber defense engineering. Founded and led by experienced red teamers who know that testing alone does not deliver better security, Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.

Get a Demo