cymulate

Build, Validate and Optimize Threat Detections at Scale

Detection engineering is a balancing act between broad, noisy detections and specific, missing threats.

The wrong side of that balancing act can lead to default configurations lacking threat coverage, a time-consuming process to investigate control logs, broken SIEM rules and basic correlation rules that take hours to build. Critical gaps in your detection capabilities can have drastic consequences in your environment.

Metrics reveal critical detection gaps

49% of security teams report challenges validating custom detections *(Anvilogic)*

18% of SIEM rules are broken and will never fire due to issues with data sources (CardinalOps)

81% MITRE ATT&CK techniques are not covered by the average SIEM (CardinalOps)

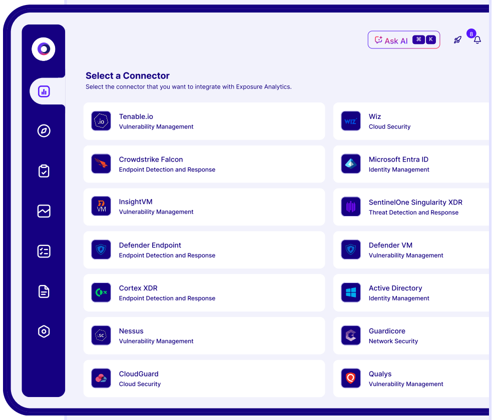
Accelerate detection engineering with Cymulate

Enhance rules, alert logic and threat coverage with automation and AI to build, test and optimize detections at scale.

- **Streamline rule creation:** Validate MITRE ATT&CK and threat coverage to pinpoint weak or missing detection rules.
- **Optimize existing rules:** Map rules to attack actions. Automate testing for actionable insights when detection rules fail to trigger.
- **Visualize MITRE ATT&CK coverage:** Map rules to attack actions. Automate testing for actionable insights when detection rules fail to trigger.

Our platform's security control ecosystem integrates with industry-leading technology to improve your threat resilience, including SIEM, EDR, vulnerability management, cloud security, networking, web gateway, Active Directory, SOAR, ticketing and more.

Our platform's security control ecosystem integrates with industry-leading technology to improve your threat resilience.



Select a Connector

Select the connector that you want to integrate with Exposure Analytics.

Tenable.io
Vulnerability Management

Wiz
Cloud Security

Crowdstrike Falcon
Endpoint Detection and Response

Microsoft Entra ID
Identity Management

InsightVM
Vulnerability Management

SentinelOne Singularity XDR
Threat Detection and Response

Defender Endpoint
Endpoint Detection and Response

Defender VM
Vulnerability Management

Cortex XDR
Endpoint Detection and Response

Active Directory
Identity Management

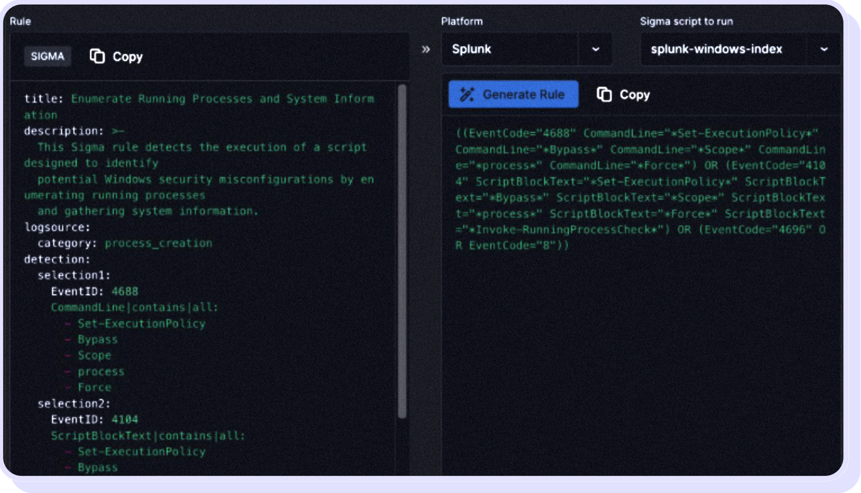
Nessus
Vulnerability Management

Guardicore
Network Security

CloudGuard
Cloud Security

Qualys
Vulnerability Management

Your detection engineering workflows in Cymulate



Rule

SIGMA Copy

```
title: Enumerate Running Processes and System Inform
ation
description: >-
  This Sigma rule detects the execution of a script
designed to identify
  potential Windows security misconfigurations by en
umerating running processes
  and gathering system information.
logsource:
  category: process_creation
detection:
  selection1:
    EventID: 4688
    CommandLine|contains|all:
      - Set-ExecutionPolicy
      - Bypass
      - Scope
      - process
      - Force
  selection2:
    EventID: 4104
    ScriptBlockText|contains|all:
      - Set-ExecutionPolicy
      - Bypass
```

Platform: Splunk

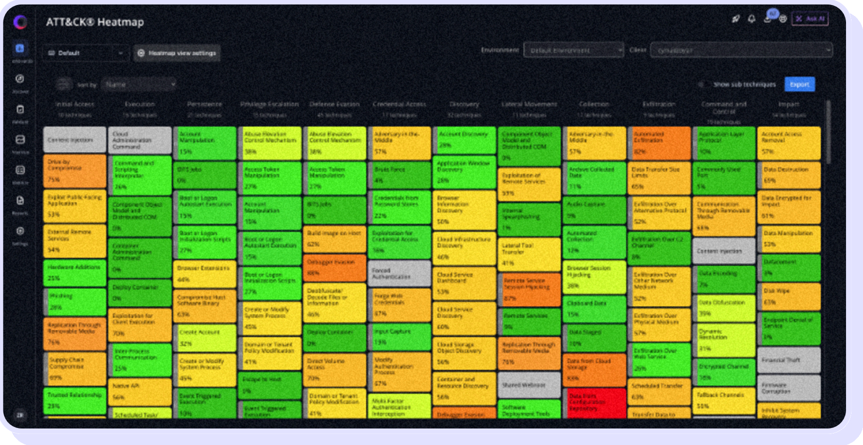
Sigma script to run: splunk-windows-index

Generate Rule Copy

```
((EventCode="4688" CommandLine="*Set-ExecutionPolicy*"
CommandLine="*Bypass*" CommandLine="*Scope*" CommandLin
e="*process*" CommandLine="*Force*") OR (EventCode="410
4" ScriptBlockText="*Set-ExecutionPolicy*" ScriptBlockT
ext="*Bypass*" ScriptBlockText="*Scope*" ScriptBlockTex
t="*process*" ScriptBlockText="*Force*" ScriptBlockText
="*Invoke-RunningProcessCheck*") OR (EventCode="4696" O
R EventCode="8"))
```

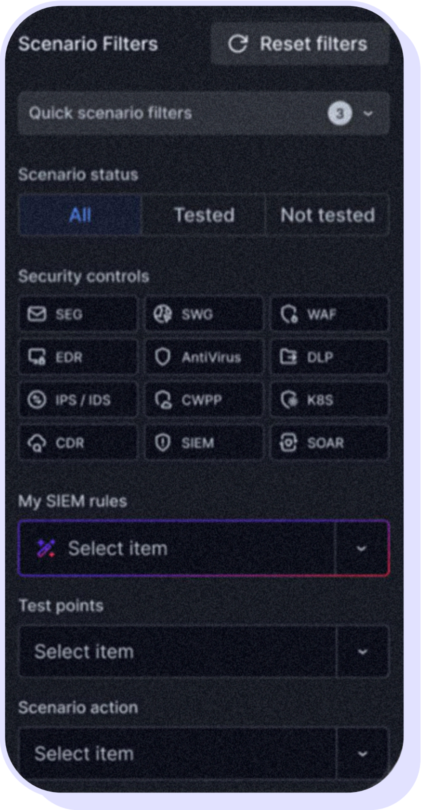
☑ Build and validate new detections for emergent threats:

1. **Consume** threat intel via AI Template Creator to automatically create a custom assessment
2. **Run** assessment
3. **Build** new rules based on missed threat detection with Cymulate-suggested EDR/XDR/SIEM rules, formatted to the specific vendor
4. **Retest** to validate that new rules trigger the correct alerts



☑ Baseline and optimize MITRE ATT&CK threat coverage:

1. **Visual baseline** of detection coverage, mapped against real-world threat behavior
2. **Focus** on missing or underperforming threat behaviors by selecting a MITRE technique or sub-technique to validate
3. **Run** assessment
4. **Build** new rules based on missed threat detection with suggested EDR/XDR/SIEM rules
5. **Retest** to validate and confirm rule performance



Scenario Filters — Reset filters

Quick scenario filters: 3

Scenario status: All | Tested | Not tested

Security controls: SEG, SWG, WAF, EDR, AntiVirus, DLP, IPS / IDS, CWPP, K8S, CDR, SIEM, SOAR

My SIEM rules: Select item

Test points: Select item

Scenario action: Select item

☑ Validate, tune and maintain SIEM detection rules:

1. **Automatically map** existing SIEM rules to Cymulate attack scenarios
2. **Run** assessment
3. **Analyze** details and evidence of logs and alerts
4. For missed detection, Cymulate suggests improvements to the detection log and rule
5. **Retest** to validate and confirm rule performance

Drive Purple Teaming and SOC Engagement

The Cymulate platform allows teams to excel at collaboration and promotes purple teaming among security groups.

We provide one place where teams can test security processes, policies and playbooks while integrating offensive (red team) and defensive (blue team) strategies for a complete, holistic approach to security validation.

What customers say

Customers report cutting incident response exercise set up time by 60% with Cymulate.

★★★★★

"Cymulate's AI SIEM Rule Validation streamlines our detection engineering validation processes with automated rule matching, saving us hundreds of hours at scale."

– Markus Flatscher, Senior Security Manager at Raiffeisen Cyber Defense Center

★★★★★

"Cymulate has strengthened our threat detection by simulating real-world attacks, helping us validate and fine-tune our SIEM, EDR, WAF and email security rules. It identified detection gaps early, allowing us to improve alerting and response workflows before actual threats could exploit them."

– Samyak Jeevane, Senior Cyber Security Analyst at REBIT

Why Choose Cymulate?

Build new detections in minutes, not hours

Create or improve rules with targeted guidance, indicators of behavior, pre-built Sigma and EDR rules.

Optimize threat coverage

Visualize threat detection gaps and create detection logic for full MITRE ATT&CK coverage.

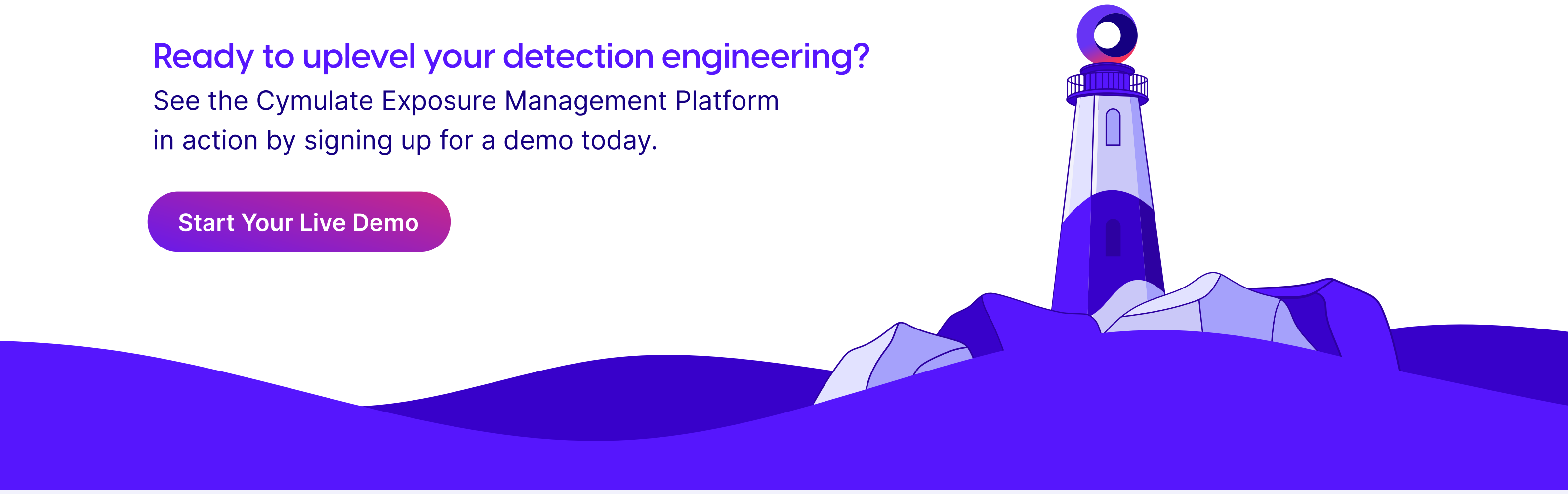
Know the true state of threat resilience

Map SIEM rules to attack actions for automated and continuous validation.

Ready to uplevel your detection engineering?

See the Cymulate Exposure Management Platform in action by signing up for a demo today.

Start Your Live Demo



About Cymulate

Cymulate is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to prove, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. Cymulate integrates with assessment tools and continuously tests defenses against the full kill chain of attack techniques providing cybersecurity teams with the automation and insights to prove and optimize threat resilience; accelerate detection engineering; drive continuous threat exposure management; and measure and baseline security posture. Prove the threat. Improve resilience. For more information, visit www.cymulate.com.