cymulate

SOLUTION BRIEF

SIEM Validation

New Attack Techniques Outpace SIEM Detection Rules

Successful security operations depend on a security information and event management (SIEM) deployment that both continuously adapts to new attack techniques and tactics while not overwhelming security teams with alerts and false positives.

While new threats and attacks often outpace the capabilities of detection rules, SIEM deployments must also evolve with diverse and constantly changing IT environments, including on-premises, cloud and hybrid systems. Without continuous security control validation of their SIEM, security teams face gaps in coverage and noisy false positives that prevent them from identifying true threats quickly.

An Absence of Detections Doesn't Mean an Absence of Threats

Security analysts rely on SIEM technologies to correlate events and detect potential threats in real time. However, when malicious actions and high-privilege behaviors are not detected within the SIEM, security teams are unaware of an imposing threat and the SIEM loses considerable value as a threat detection tool.

Security leaders need to constantly validate the effectiveness of their SIEM detections to ensure that potentially malicious activity can be observed and investigated by security analysts to detect the presence of a threat actor, especially those persistent threats operating in stealth mode across the environment.

With breach and attack simulation, Cymulate provides the automated security validation that tests and validates malicious actions and high-privilege activities that are detected and alerted within the SIEM. Cymulate SIEM assessments simulate different types of threat activity, including:

- **Immediate threats**
- **Endpoint threats**
- **Cloud and container threats**
- **Assume breach (high privilege) threats**
- **Other persistent threats**

The results of these assessments highlight the gaps and weaknesses in SIEM detections that could allow a persistent threat actor to operate undetected within your network as they get ready to take action on their objectives and launch a full-scale cyber attack.

Solution Benefits

Continuous validation

Automated continuous testing of SIEM detection capabilities against the latest attack techniques.

Identify missed detections

Find gaps where your SIEM has failed to detect potential threat activity.

Optimize security controls

Tune SIEM detection rules and reduce false positives to optimize SIEM effectiveness.

Reduce exposure risk

Continuously measure and improve your SIEM detections to reduce the risk of a cyber incident.

> **When we create a new detection rule in our SIEM that we can't validate with historical logs, we use Cymulate assessments to generate the appropriate events and see if the rule was successful in its detection. The immediate feedback is useful when fine-tuning our SIEM and practicing detection engineering.**
>
> — Markus Flatscher,
> Senior Security Manager, RBI

Validate SIEM Detection with Breach and Attack Simulation

The Cymulate Exposure Management Platform includes breach and attack simulation to automate production-safe security assessments that determine if your SIEM is accurately detecting various attack scenarios and high privilege behaviors. The assessments validate SIEM deployments for both the visibility of log collection and analysis that produces actionable alerts. All results feed into a MITRE ATT&CK heatmap that visualizes validated threat coverage provided by SIEM, other controls and collectively for the security stack.

Detecting potential threat activity is your last line of defense against advanced persistent threats operating within your environment. By running automated security validation of your SIEM detections on a frequent (weekly) basis, you can reduce your exposure risk to the latest threat tactics and techniques used by advanced threat actors.

Optimize SIEM with Automated Sigma Rules and Remediation Guidance

For each identified coverage gap, Cymulate provides the evidence of detection gaps and the guidance to tune and optimize the SIEM for broad coverage of threat techniques. Detailed findings provide deep insight into the detection results, attack technique used, alerts and events triggered, attack indicators and mitigation guidelines that highlight missing logs as well as recommended Sigma detection rules that can be directly applied to the SIEM.

Safely Automate Detection Engineering

Cymulate provides security analysts with tools, resources and automation to accelerate detection engineering with production-safe simulations and rule creation. In addition to a library of more than 2,000 attack scenarios that simulate common threat activities and malicious behaviors that should be detected by the SIEM, Cymulate allows security teams to design their own attack simulations based on customized executions, files and Sigma rules. Analysts launch these assessments to test and validate the SIEM detection and create new rules for coverage gaps.

Integrate with Leading SIEM Platforms

Cymulate easily integrates with the leading SIEM platforms to run assessments that validate whether the SIEM is accurately detecting relevant threats and properly alerting security analysts. For every assessment, Cymulate provides indicators of compromise (IOCs), indicators of behavior (IOBs) and Sigma rules to help fine tune the SIEM configuration for more accurate detections.

Azure Sentinel · splunk> · Chronicle part of Google Cloud · CROWDSTRIKE · Trellix · McAfee · elastic · exabeam · IBM Radar · LogRhythm · ArcSight · NETWITNESS An RSA Business · RAPID7 insightIDR · SECURONIX · sumo logic

Why choose Cymulate?

Depth of attack simulations

The Cymulate platform provides a comprehensive suite of more than 2,000 attack scenarios that can be used to validate the effectiveness of your SIEM.

Production safe

The full suite of attack scenarios is completely production-safe and will not harm your production environment.

Automated validation

The assessments are fully automated enabling weekly validation of your SIEM effectiveness to detect the latest threat activity.


Azure Sentinel
splunk >
Chronicle
part of Google Cloud
CROWDSTRIKE
Trellix
McAfee
elastic
exabeam
IBM Radar
LogRhythm
MICRO FOCUS
ArcSight
NETWITNESS
An RSA Business
RAPID7
insightIDR
SECURONIX
sumo logic