cymulate

SOLUTION BRIEF

Network Security Validation

Robust Network Security Essential to Safeguard Against Cyber Threats and Data Breaches

Network security faces increasingly complex challenges that extend far beyond managing a firewall's open ports. Organizations must guard against a wide range of attacks from command and control (C2) servers to distributed denial of service assaults and malicious bot activity from a host of sophisticated threat actors.

Your network security controls provide the critical infrastructure needed for both the **north–south** traffic to and from the Internet, as well as the **east–west** internal traffic that connects your users to systems, applications and data.

Threat actors use techniques like spoofing, sniffing, hijacking, poisoning, stripping and injection to exploit network traffic and gain unauthorized access to systems, steal credentials, exfiltrate data and disrupt services. Using techniques like man-in-the-middle attacks, threat actors can secretly intercept and alter communications between two legitimate devices or hijack a legitimate session to potentially gain access to confidential information or authenticated sessions without a user's knowledge. By intercepting network traffic, attackers can steal sensitive information or inject malicious data or commands into the communication stream.

Simulate Malicious Network Traffic

Security leaders need to constantly validate the effectiveness of their network security controls to ensure that potentially malicious traffic can be detected for the presence of a threat actor operating within the network and bypassing perimeter controls.

Cymulate delivers automated security validation to simulate north–south traffic and east–west internal traffic across your network. Network security validation assessments enable you to test the effectiveness of security controls and policies associated with your:

- Web gateways and firewalls
- Intrusion prevention / detection systems
- Virtual private networks
- Network segmentation
- Lateral movement and data loss prevention

Through the evaluation of network traffic simulations, your organization can proactively strengthen your network security posture and enhance your ability to mitigate potential risks.

Solution Benefits

Continuous validation

Automated continuous testing of network security controls against the latest threat tactics.

Identify gaps and weaknesses

Find gaps and weaknesses in your network defenses that could expose your users to a sophisticated attack.

Optimize security controls

Configure and tune your network security controls and policies with mitigation guidance and rules to better defend your perimeter.

Reduce exposure risk

Continuously measure and improve network security controls to reduce the risk of a cyber attack.

> This tool is great for doing simulations and great for knowing your tools capabilities on detecting attacks related to malware, phishing, command and control, etc."
>
> – SOC Analyst, Banking Industry

Automated Security Validation for Your Network Security Controls

The Cymulate Exposure Management Platform uses breach and attack simulations for automated validation and assessment of your network security controls. These production-safe security assessments of your network defenses use a wide range of advanced scenarios for network traffic simulations using PCAP files, network penetration testing and specific network traffic exploits against known security vulnerabilities.

Network traffic simulations (PCAP files)
Cymulate executes attack simulations for both malicious and non-malicious network traffic using packet capture (PCAP) files. This capability enables your organization to replay network traffic scenarios within a controlled environment, providing valuable insights into potential vulnerabilities and the effectiveness of network intrusion prevention and detection controls.

The pre-built scenarios include ransomware, malware, web shells, hack tools and backdoors. The scenarios also incorporate the use of different protocols such as SMB, TCP and HTTP, allowing you to assess the security posture of your network against multiple types of threats.

Network segmentation and penetration testing
Cymulate also tests internal network configurations and segmentation policies of firewalls and routers to identify the potential for lateral movement using various techniques and protocols to elevate privileges, evade detection, spread within a network, gain control over additional systems and reach critical assets and crown jewels like domain controllers.

Resilience to threats
Cymulate tests and validates network controls like web gateways, firewalls and web application firewalls by simulating network threats and exploits for command and control, malicious URLs, file downloads, exploits of vulnerabilities, OWASP web application security risks and other malicious traffic.

Network reports and dashboards
The Cymulate platform provides detailed reports, findings and dashboards that highlight your strengths and weaknesses in the prevention and detection of different tactics and techniques across the MITRE ATT&CK® framework. Monitor the resilience of your network security solutions and manage drift to stay protected.

To conduct network security assessments, Cymulate requires the installation of two agents within a connected network environment: one acting as the client (or attacker) and the other as the server (or victim). The process of simulating network traffic from PCAP files entails the simultaneous assessment of both agents. The client agent initiates the network traffic simulation, while the server agent acts as the recipient of the packet in the simulated scenario.

Why choose Cymulate?

Depth of attack simulations

The assessments contain over 30 network traffic simulation templates with hundreds of test executions to fully validate the effectiveness of your network security controls.

Production safe

The full suite of test executions is completely production-safe with no execution of malicious code or commands in your production environment.

Automated validation

The assessments are fully automated enabling continuous weekly validation and performance optimization of your network security effectiveness.

About Cymulate

Cymulate is the leader in exposure management and security validation. More than 500 customers worldwide rely on the Cymulate platform for continuous discovery, validation, prioritization, and guided remediation of security gaps before attackers can exploit them. For more information, visit www.cymulate.com.

Get a Demo