SAYERS BREACH & ATTACK SIMULATION

Safely Validate Cyber Controls

Sayers, leveraging an industry-proven breach and attack simulation tool, will test your security infrastructure through a pre-defined hacker playbook based on the MITRE ATT&CK framework.

Our breach & attack assessment will run through a hacker playbook, validate security controls accross the kill chain, and immediately output actionable results for you and your security team.

Explore the realm of continuous security control validation and remediation, and leverage tools that help prioritize investments based on real business risks.

Challenges	Remediation
Protecting Sensitive Data	Ensure threat inspection policies work against high-profile attacks. Visualize the impact of attacks via a cyber kill chain view.
Security Exposure	Ensure your organization hasn't inadvertently left any exposing vulnerabilities.
Business Rationalization	Build a business case to enable additional features when security gaps are discovered.
Security Controls: Validation & Optimization	Challenge and optimize security policies for the best defenses.
Compliance	Validate segmentation for PCI, GDPR, HIPAA, and other regulatory requirements.
Encrypted Traffic	Show where encrypted traffic can be used to bypass security, and tunnel data out to command and control.

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

- Persistence
- Privilege Escalation
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

sayers
built around you

CONDUCT A BREACK & ATTACK SIMULATION
INFO.SAYERS.COM/LETS-TALK