VARONIS

CYBER RESILIENCY ASSESSMENT

A complimentary risk assessment designed to stress test your security stack using the latest adversary tactics and tradecraft.

CHALLENGE

Many organizations don't have a clear picture of their cyber resiliency – their ability to detect, investigate, prevent, and recover from a data breach. Often, organizations are unaware of the gaps until an adversary or insider commits a data leak, theft, or even a ransomware attack. Waiting for a threat actor to reveal weaknesses is too risky for an organization entrusted with safeguarding sensitive data.

SOLUTION

The Varonis Cyber Resiliency Assessment (CRA) is a bespoke and comprehensive adversary simulation that identifies gaps in detection and prevention policies in an organization's defensive stack.

This service is designed to discover security gaps and attack paths to help you confidently answer:

+ Can I detect a breach?
+ Can I investigate and recover quickly?
+ Can I protect my data?

After the simulation, Varonis will provide a report with in-depth findings and recommendations to help improve your organization's security posture. Varonis analysts will share best practices, tips, and tricks that your team can use to enhance future posture analysis.

HOW IT WORKS

1. Varonis analysts and customers host a kickoff call to discuss engagement specifics, expected outcomes, and requirements for the simulated attack.
2. During a ~2 hour attack session, Varonis will **deploy a real Command and Control (C2) framework** into your environment, mimicking threat actors, adversary tactics, and attack scenarios in actual investigations.
3. During the simulation, Varonis will generate host and network activity using custom tools designed to **evade defenses in order to evaluate prevention and detection responses** from an assume-breach perspective.

VARONIS

TEST DEFENSE IN DEPTH.

Attackers are stubborn and will try every trick in the book. Varonis includes multiple attack types during simulations including host recon, credential attacks, ransomware, and more to test your organization's defense in depth strategy.

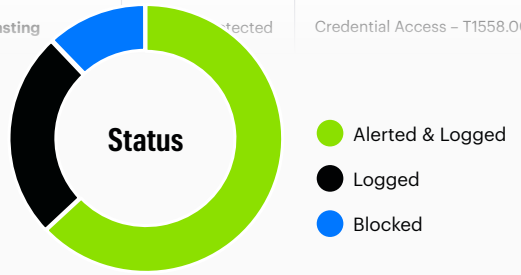
Simulate real attacks.

Varonis customizes the attacks used in the simulation based on the customers environment and industry specific cyber threats seen in real adversary attacks.

SIMULATED ATTACK SCENARIOS INCLUDED:

- Host Enumeration
- User Enumeration
- Share Discovery
- Password Spray
- Kerberoasting
- C2 via DNS
- Exfl via DNS
- Ransomware
- C2 via HTTPS

Test case	Status	MITRE tactic and technique
AD Password Spray	Detected	Credential Access – T1110.003
AD User Enumeration	Detected	Discovery – T1087.002
Kerberoasting	tected	Credential Access – T1558.003



Identify gaps.

Block future intrusion attempts by closing vulnerabilities and gaps in coverage today. With each simulation, Varonis will use custom tools designed to evade defenses and evaluate threat detection and response capabilities.

START YOUR FREE CYBER RESILIENCY ASSESSMENT TODAY.

Speak with your account representative to learn more.