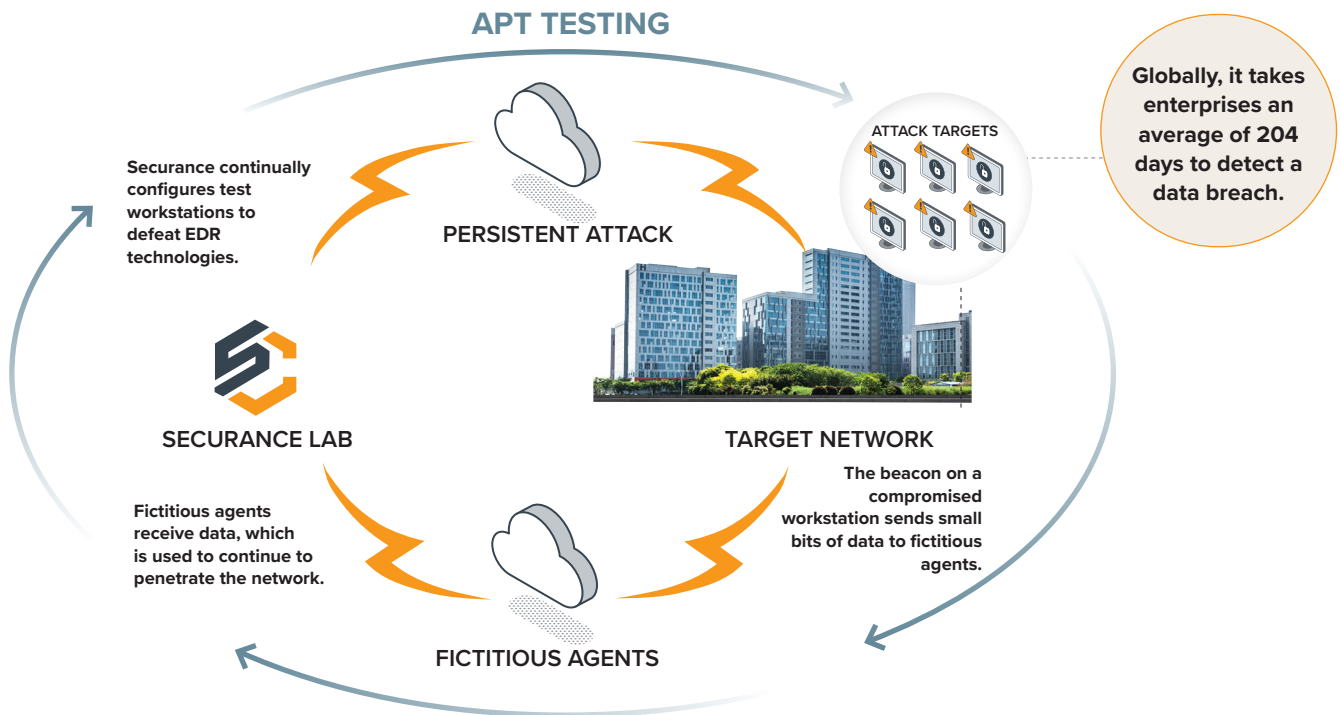# THINK LIKE A HACKER.
Advanced Persistent Threat Simulation Testing

In today's cyber climate, traditional, point-in-time vulnerability and penetration tests are out. Beating hackers at their own game is in. Here's how Securance helps.

Over a 120 to 180-day period, Securance uses real-world tactics, such as exfiltration, privilege escation, evasion, and persistence, to simulate a long-term attack on an organization's IT environment. This rigorous assessment will guage the organization's ability to avoid, detect, and respond to advanced persistent threats (APTs) aimed at stealing intellectual property and user data and disrupting information systems, functionality.

Securance uses innovative tools to perform quiet, persistent network attacks that highlight IT security risks and weaknesses— while evading traditional security defenses.

APT TESTING

ATTACK TARGETS

PERSISTENT ATTACK

Securance continually configures test workstations to defeat EDR technologies.

Globally, it takes enterprises an average of 204 days to detect a data breach.

SECURANCE LAB

TARGET NETWORK

The beacon on a compromised workstation sends small bits of data to fictitious agents.

Fictitious agents receive data, which is used to continue to penetrate the network.

FICTITIOUS AGENTS