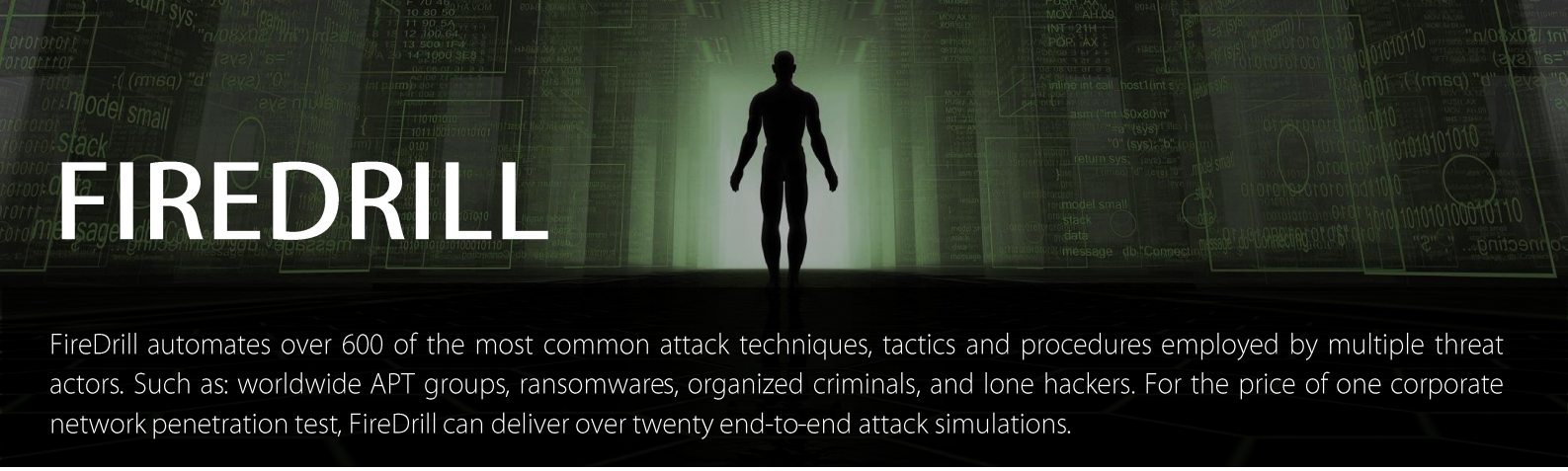

FIREDRILL

FireDrill automates over 600 of the most common attack techniques, tactics and procedures employed by multiple threat actors. Such as: worldwide APT groups, ransomwares, organized criminals, and lone hackers. For the price of one corporate network penetration test, FireDrill can deliver over twenty end-to-end attack simulations.

OVERVIEW

FireDrill automates security testing for the top 600 most commonly used techniques, tactics and procedures employed by cyber attackers to compromise organisations.

For a fraction of the cost of a penetration test, FireDrill gives you continuous, automated, easy-to-use, security testing. FireDrill alerts you in real time when one of your security protections is failing.

Top organisations around the world use FireDrill as their go-to product to compare security solutions offered by vendors and test the effectiveness of their security controls 24/7.

FEATURES

- Threat Modelling: FireDrill allows you to run realistic attack scenarios to assess the effectiveness of your security defences against the threat actors and attack techniques that matter most to your organization.
- Scale & Speed: FireDrill can run thousands of attack scenarios in a matter of minutes. New endpoint agents can be deployed within seconds, thus allowing our clients to test their entire network without the considerable challenges of hiring more security testers.
- APT Simulation: FireDrill enables you to replay advanced persistent threat network traffic, techniques and tactics against your network for defence purposes.
- Reports: FireDrill generates meaningful reports allowing our clients to benchmark their security defences against industry standards and best-practices. FireDrill provides historical vulnerability data allowing our clients to demonstrate improvements in their defences over time.

BENEFITS:

Price & Coverage:

FireDrill simulates the entire range of cyber threat actors for fraction of the cost compared to traditional penetration testing. Organised criminal organisations, ransomeware, espionage, nation-state actors, APT groups are examples of threat actors covered.

Force Multiplier:

A single, competent, penetration tester can only conduct between 20 and 30 attack scenarios per day. In contrast, FireDrill allows to run over 600 attack scenarios in a matter of minutes.

Data-Driven Security:

FireDrill generates security reports confirming whether or not you are stopping the techniques employed by the adversaries you are facing. ROI for security investments can then be backed by real adversary data.

Mossé Security, 454 Collins Street. Melbourne, 3000, Victoria, Australia
www.mosse-security.com contact@mosse-security.com