

WHO ARE THE THREAT ACTORS?

THREAT ACTORS, ALSO KNOWN AS BAD ACTORS, CAN BE BROKEN DOWN INTO THE FOLLOWING CATEGORIES...



ORGANISED CRIME

consists of groups out to make money



HACKTIVISTS

threat actors with ideological agendas that primarily attack government, leak information or seek to disrupt websites, also attacking companies, organised crime and individuals



INSIDERS

rogue employees or people making mistakes who potentially have access to key applications, systems and data



NATION STATES

other countries that want to know what your company or your country is up to and may want to interfere



COMPETITORS

other firms that may want to know what products you're developing or target your customer base



BLACK HATS

threat actors that attempt to break into systems just because they can or for personal gain



SCRIPT KIDDIES

new hackers who are out to make a name for themselves and are indiscriminate and unpredictable

BUT NOT ALL ATTACKS ARE MALICIOUS...



WHITE HATS

will attempt to break into systems, but will not, purposefully, cause any irreparable damage, instead notifying the target of a successful breach and telling them the vulnerabilities, probably for a price or reward, perhaps even working for regulators!

THREAT-LED PENETRATION TESTING

- » Threat-Led Penetration Testing (TLPT), also known as Ethical Red Teaming, is a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors.
- » The purpose of TLPT is to assess and provide insights on entities' resilience capabilities against a real world simulated cyber incident. Examples of national/international TLPT programs include CBEST (Bank of England), TIBER-EU (ECB) and iCAST (HKMA).