MOBIUS
BINARY
Clearly secure

THREAT SIMULATION

THREAT SIMULATION

Without a clear understanding of what makes your company vulnerable to cyber-attacks, defending against threats will be an impossible task.

Drive improvements in your security posture and gain real-time insight into your cyber threat landscape by pinpointing weaknesses in your security controls with the Mobius Binary Threat Simulation service offering.

LEVERAGING PENETRATION TESTING EXPERTISE TO SIMULATE ATTACKS

The Mobius Binary team has developed a practical, hands-on Threat Simulation service using the **MITRE ATT&CK®** matrix to simulate real-world attack scenarios effectively.

WHAT IS THE MITRE ATT&CK MATRIX?

According to MITRE, the **ATT&CK®** matrix is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations used to develop specific threat models and methodologies in the private sector, government, and the cyber security product and service community.

THE MOBIUS BINARY APPROACH TO THREAT SIMULATION

The Mobius Binary approach to Threat Simulation leverages the **MITRE ATT&CK®** matrix and utilises other open source tools/scripts to identify a substantial number of steps that have been automated for execution against targets in an organisation's network. The approach can be implemented in one of two scenarios; a collaborative or adversarial scenario with each having their own benefits.

ADVERSARIAL APPROACH

This scenario is more real-world as the blue team / IT department is unaware of the simulated attacks. This scenario is delivered by:

a) Preparing three to five dedicated attack machines for the simulation. The blue team / IT are not informed which machines will be used for the simulated attacks and therefore are solely reliant on existing monitoring and alerting controls to identify the simulated attacks.
b) The attacks are randomised across the attack machines, and "dummy" behaviour or diversionary "noise" is initiated in an attempt to distract the blue team / IT department.

If the simulation attacks are detected, the simulation should result in the blue team / IT jumping into action to eliminate the threat. If the simulation attacks are not detected, this would be evidence of gaps in the existing monitoring processes. Therefore, this simulation is an actual test of the monitoring and detection tools and the preparedness of the blue team / IT.

COLLABORATIVE APPROACH

Working in collaboration with an organisation's blue team / IT department, the simulated attacks are launched from a dedicated attact machine on the internal network.

The collaborative approach allows the blue team / IT department to be aware of the attacks so that they can attempt to:

a) Actively block the attacks with manual intervention; or
b) Rely entirely on their security solutions to defend against the attacks.

While this is considered less real-world, this scenario enables the blue team / IT department to test and monitor existing security solutions, controls and configurations to see whether these are performing as intended and whether they will be effective should an actual attack occur. It can also assist the team in identifying other gaps or corrective actions required in order to minimise the impact should an actual attack occur.

Performing Threat Simulation testing by using Mobius Binary's Adversarial or Collaborative approaches could mean the difference between a successful or failed response to a future threat. Regular Threat Simulation testing will drive improvements in security posture, validate existing controls and solutions, and create peace of mind.

CONTACT MOBIUS BINARY FOR A CUSTOM THREAT SIMULATION TEST TO ENSURE THAT YOU ARE "CLEARLY SECURE".

MOBIUS BINARY
Clearly secure

CONTACT US NOW

London: +44 84 5544 4656 | Email: info@mobiusbinary.com | Website: mobiusbinary.com