MALWARE ANALYSIS

Mossé Security offers Malware Analysis Services which provide your organisation with expert insights into the effectiveness of your security controls and advise you where you would do best to invest for your organisation to keep safely protected. We identify and analyse malware that may have evaded your security defences and advise you on how to improve your security strategy.

OVERVIEW

Mossé Security offers Malware Analysis Services to provide organisations expert insights on the malware discovered in their networks.

Only organisations who understand how malware can or have entered their environment, can tighten their defences.

Our expert Security Analysts reverse-engineer suspicious files to gain immediate insight into the capabilities, evasion techniques, and overall impact of malicious code that defeat your security controls.

Our Certified Malware Analysis Consultants come equipped with a high level of experience and knowledge that they've acquired from years of training and practice.

Mossé Security has been defending Australian organisations of all sizes since 2010. We have a strong track record of analysing malware and researching threat actors that target the Australian region.

MOSSÉ SECURITY

- **Threat Research:** Mossé Security is the only Australian cyber security company with a dedicated Threat Research team. We have a track record in speedily identifying and responding to threat actors that anti-virus and endpoint detection as well asb response software have failed to catch.

- **Australian Dataset:** Mossé Security has a dataset of over 1 terabyte worth of executables seen in Australia. This dataset allows us to rapidly assess whether a suspicious binary has been seen elsewhere in the country.

- **Regional Focus:** Every year, we respond to a remarkable variety of cyber attacks against customers nationwide. As a result, our expert bteam is a step ahead with cyber-attacks against Australian organisations and the threat actors behind these attacks.

BENEFITS:

Insights:

Assessing the capabilities that malware provided an adversary that entered your networks will answer many questions business leaders have about the impact of an incident

Strategy:

Understanding how come malware defeated your security controls will provide key strategical insights into where security investments may need to be shifted

Improved Defence:

Developing security requirements based on malware incident cases will uplift the defences on your organisation in a tangible manner