A proactive strategic threat framework for better security architecture

Gokul Srinivasan[1]
[1]*Control Risks*

Nation states are increasingly using cyber as an instrument of power, and attacks on critical infrastructure can go beyond a catastrophic disruption to day-to-day business, and expose a calamitous risk to property and lives.

Organisations are now facing threats from actors that are more commoditised, sophisticated and structured than ever before, and the use of traditional threat intelligence is increasingly becoming ineffective to predict future cyber-attacks from nation state actors, hacktivists and criminals.

Reactive threat intelligence methods to combat cyber-attacks can sometimes be too little, too late. These tactical and technical methods typically monitor attacks that have or are being executed, and use indicators of compromise such as IP addresses, domain names and hashes etc., all which can be easily manipulated.

Rather organisations need to be proactive and forward looking. Implementing a strategic threat intelligence framework can help determine what events could trigger an attack, who are the likely threat actors and how will they carry out the attack.

Through a case study example, Gokul will demonstrate how to implement a step-by-step strategic threat intelligence framework that can feed into your organisations threat hunting campaigns and help improve your strategic decision making.