**White Glove Service – Executive Protection**

## Intelligence Gathering

The various types of intelligence gathering steps followed by attackers such as Open Source Intelligence (OSINT), Cyber Space Intelligence (CYBINT), and Human Intelligence (HUMINT), and how these are interconnected. This chapter discusses how attackers use Internet and openly available information about individuals and organizations from different sources such as Online Social Networks (OSNs), websites, magazines, etc., to gather intelligence about the targets before performing any kind of reconnaissance. The information collected about the targets determines the direction of targeted attacks

**Open Source Intelligence (OSINT); Cyber Intelligence (CYBINT); Human Intelligence (HUMINT); Online Social Networks (OSNs).**

A substantial amount of information is needed to target an individual or organization. More information creates more potential attack paths for launching an attack, which increase the probability of success.

Gathering Process from an attack modeling perspective, we present intelligence gathering as the transformation of raw data into useful information.

Our **WhiteGlove Service Covers a methodology of intelligence** gathering model covering expanding Tiers of “aggression”.