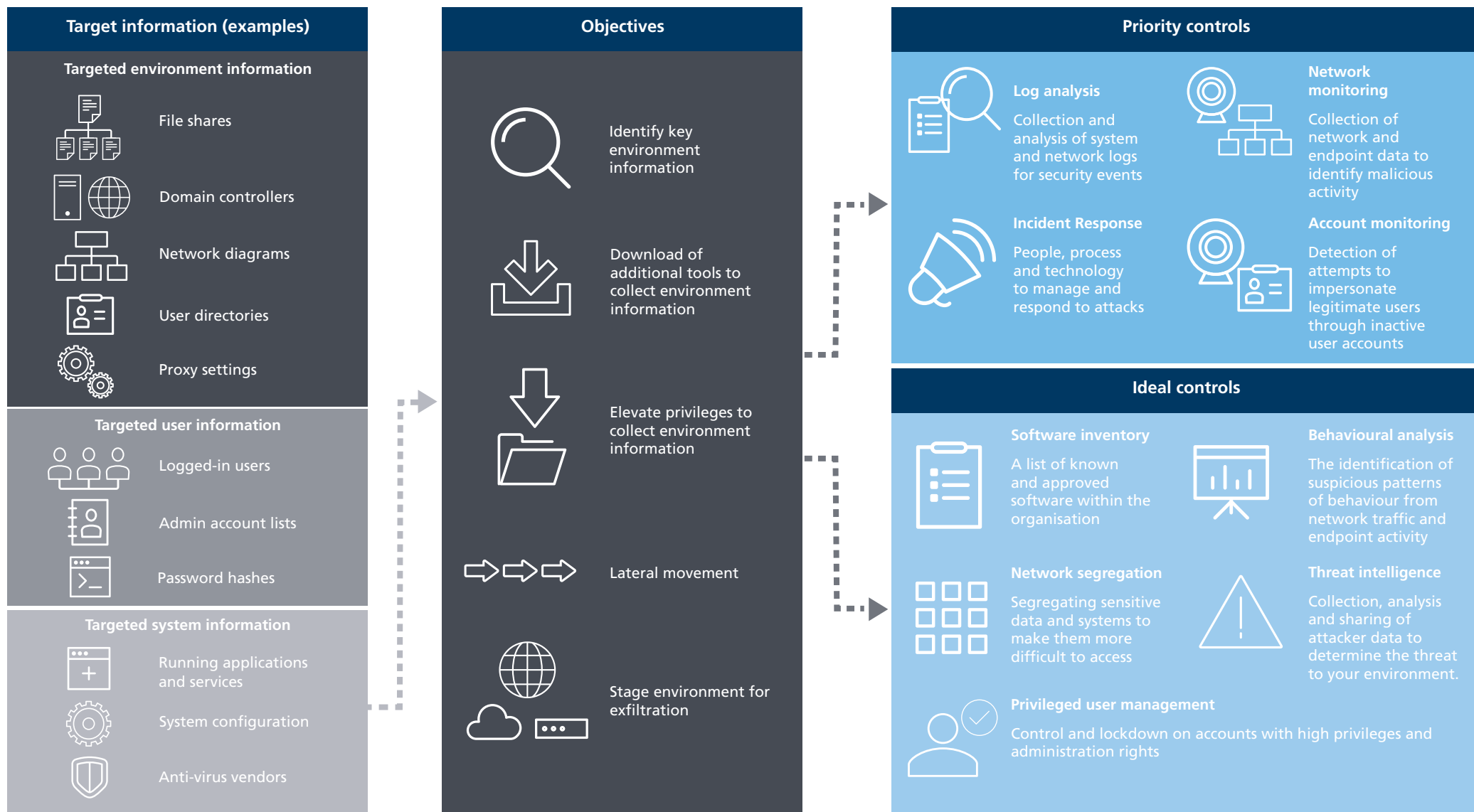


Internal Network Reconnaissance

Internal Network Reconnaissance is where an attacker enumerates information about a target environment before completing their later objectives in the attack such as elevating their privileges or stealing sensitive information.

Do not underestimate the value of technical information describing your environment and the business information describing your organisation to your attacker.



Top 5 questions to ask your CISO:



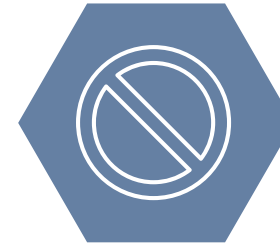
1. Have we identified information that an attacker would target, in order to improve their understanding of our infrastructure(s) and data we possess, to progress an attack post initial-compromise?



2. Do we have effective measures in place to protect this information from an attacker who has already breached our perimeter and is inside our network?



3. What measures do we have in place to impede the progress of an attacker and make them more visible to enable detection of their activities?



4. Do we have plans and capabilities to react and stop an attacker who has already breached our perimeter and is searching around inside our network – can we stop them before they complete objectives (e.g. disrupt operations or steal information)?



5. What are we doing to enhance our existing measures to detect, impede and stop an attacker inside our IT infrastructure?