Guidelines after detecting IoCs

Why shouldn't we start Incident Response immediately?

1. IoCs contains false positives – Not all feeds are to be used for alerting or blocking based on MISP (https://www.misp-project.org/feeds/)
2. IoCs are ephemeral indicators – As attackers may use IP addresses allocated to cloud infrastructure, these IoCs can be easily changed and thus can be relocated to other services hosted on web, which are not real Indicators of Attackers
3. Verification of non-standard behaviour – Verification of IoCs to be Indicator of Attacker by checking for non-standard behaviour (eg. URL connection IoC detected from notepad.exe)

How to check for non-standard behaviour? (3 Levels)

1. SIEM Logs / EDR Logs – Getting better context by understanding the origin of IoC
2. Velociraptor – Using velociraptor to get a better understanding of processes being taken within a flagged machine. Velociraptor is an open-source tool that is easy to setup and use (https://rhq.reconinfosec.com/tactics/initial_access/), hence "Shifting Left" with the implementation of incident response tools helps organisations to detect faster and provides real-time insight which are otherwise not readily accessible.
3. Proactive threat hunting – Proactive checking for behaviours that are outside of the standard behaviours expected within the organisation (eg. Detecting of C2 via discord, when discord is not used within the organisation)