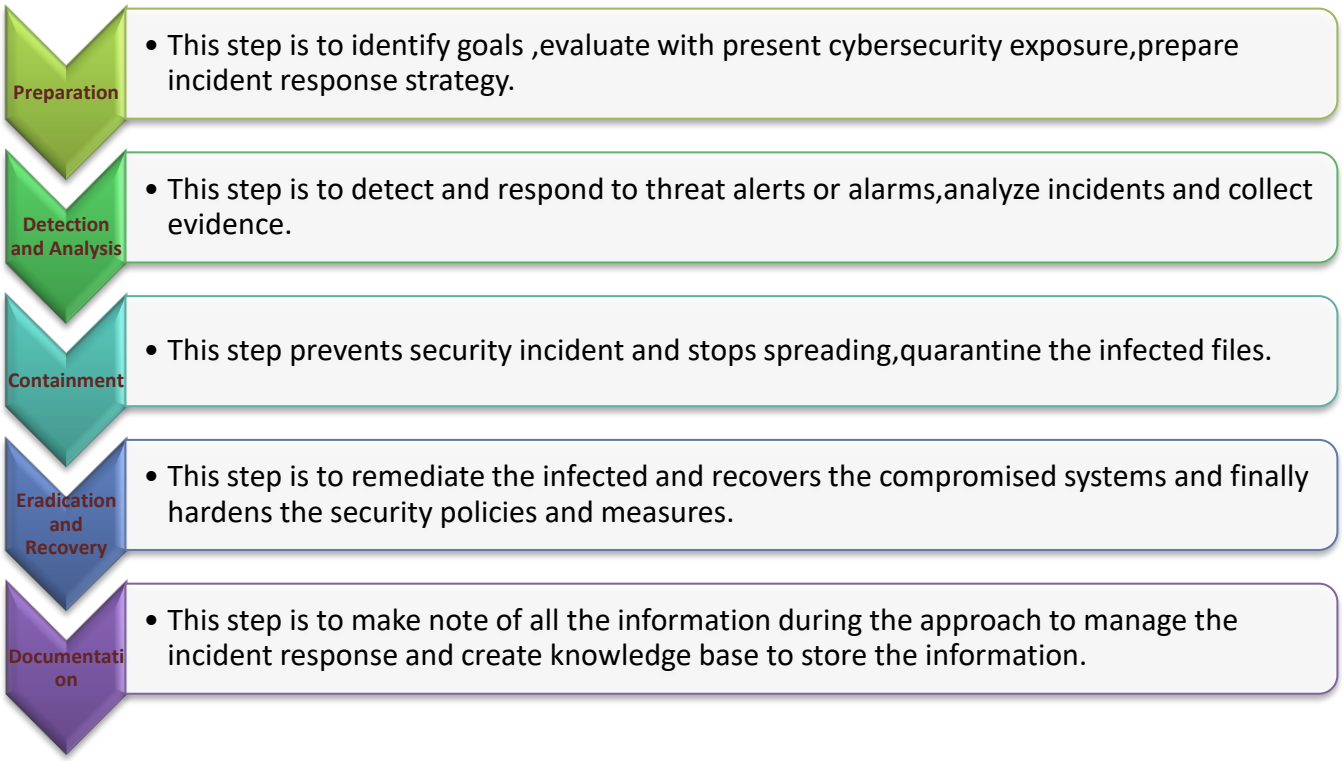

- **Security Orchestration and Automation(SOA):**

  Security Orchestration and Automation(SOA),the name itself mentions that there are two main capabilities to required i.e, **Orchestration and Automation**

  Orchestration…which means the gathering of information from various sources i.e, connecting security tools and integrating disparate security systems i.e, we will dig through some logs to find out the origin of the file and check whether infected or not.

  Automation…here the name itself says that without any human assistance.This is implemented by constructing playbooks(manual trigger is used) which is understandable to every analyst in the team which helps analysts by automating common, repetitive and menial tasks driven by machine learning for faster response to all alerts and finally allowing security analysts to proactively focus on higher skilled tasks such as threat hunting and intelligence gathering.

Conclusion…

SOAR is the only platform to offer full incident response lifecycle management with machine learning and threat hunting.Acting as a force multiplier, it enables security teams to do more with less, empowering security analysts, while ensuring organizations stay one step ahead of any potential threat. Implementing a SOAR solution is an effective and reliable answer that many organizations have chosen to remedy some of the largest obstacles in cybersecurity including, alert fatigue, lack of qualified personnel, and increased efficiency .