Now let's look back to the sentence…"SOAR supports multiple activities for security operations decision making as shown in the figure". Here multiple activities includes

- **Prioritize…**this activity refers to Prioritizing operations activities which implies that SOAR technologies combines collection of security detection tools, third party data sources and IT asset databases not just to identify the threats but also the risk that it posses compared to others.
- **Detect…**this activity refers to Detecting operations activities where SOAR technologies enable organizations to collect security threat data and alerts from different sources and makes a decision about the upcoming threats.
- **Triage…**this activity includes
  1. Threat hunting which means proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions
  2. Validation of threats through investigation and
  3. Through playbooks and predefined workflows which helps the analyst to access quickly and remediate the security incidents and most importantly during these process we automate the repeated threats in containment and analysis which gives time to analysts to work on more complex issues.
- **Respond…**this activity is the last phase which means that the event has confirmed an alert that requires to be remediate as cross verification has already done so remediation must be taken to counteract the threat.

The main goal of the SOAR is to improve the efficiency of digital and physical security operations and to achieve major expected benefits of SOAR were in reducing false positives, prioritizing incidents after risk determination, coordinating actions across security tools, and automating repeatable response actions.