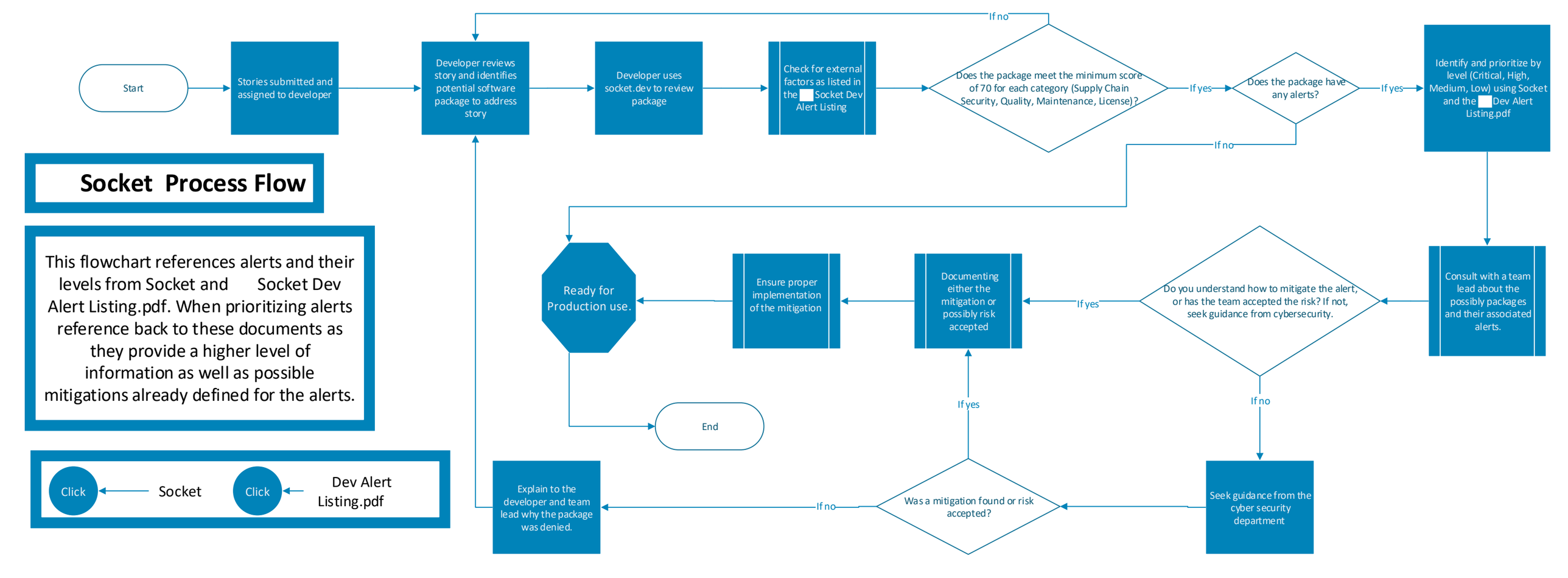
Socket Process Flow
This flowchart references alerts and their levels from Socket and Socket Dev Alert Listing.pdf. When prioritizing alerts reference back to these documents as they provide a higher level of information as well as possible mitigations already defined for the alerts.
Click
Socket
Click
Dev Alert Listing.pdf
Start
Stories submitted and assigned to developer
Developer reviews story and identifies potential software package to address story
Developer uses socket.dev to review package
Check for external factors as listed in the Socket Dev Alert Listing
Does the package meet the minimum score of 70 for each category (Supply Chain Security, Quality, Maintenance, License)?
If no
If yes
Does the package have any alerts?
If yes
If no
Identify and prioritize by level (Critical, High, Medium, Low) using Socket and the Dev Alert Listing.pdf
Consult with a team lead about the possibly packages and their associated alerts.
Do you understand how to mitigate the alert, or has the team accepted the risk? If not, seek guidance from cybersecurity.
If yes
If no
Documenting either the mitigation or possibly risk accepted
Ensure proper implementation of the mitigation
Ready for Production use.
End
Seek guidance from the cyber security department
Was a mitigation found or risk accepted?
If yes
If no
Explain to the developer and team lead why the package was denied.