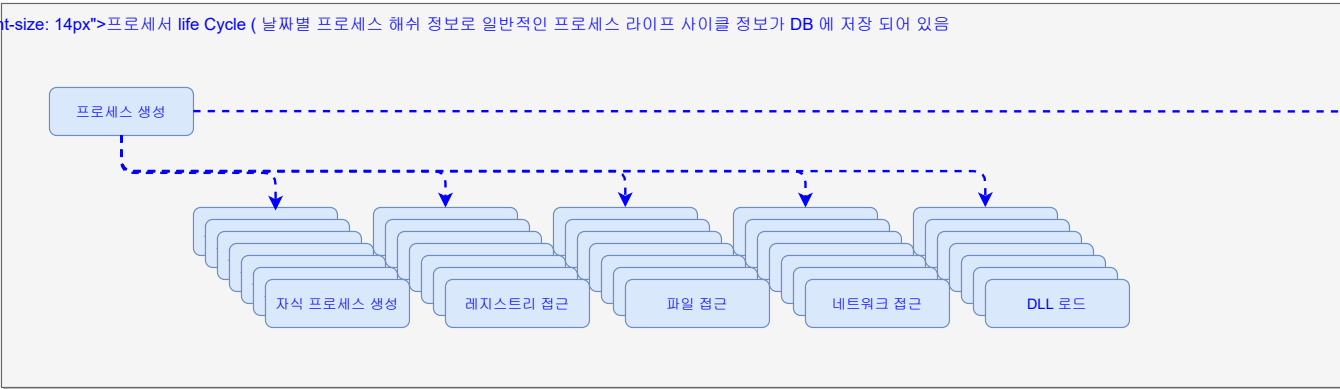
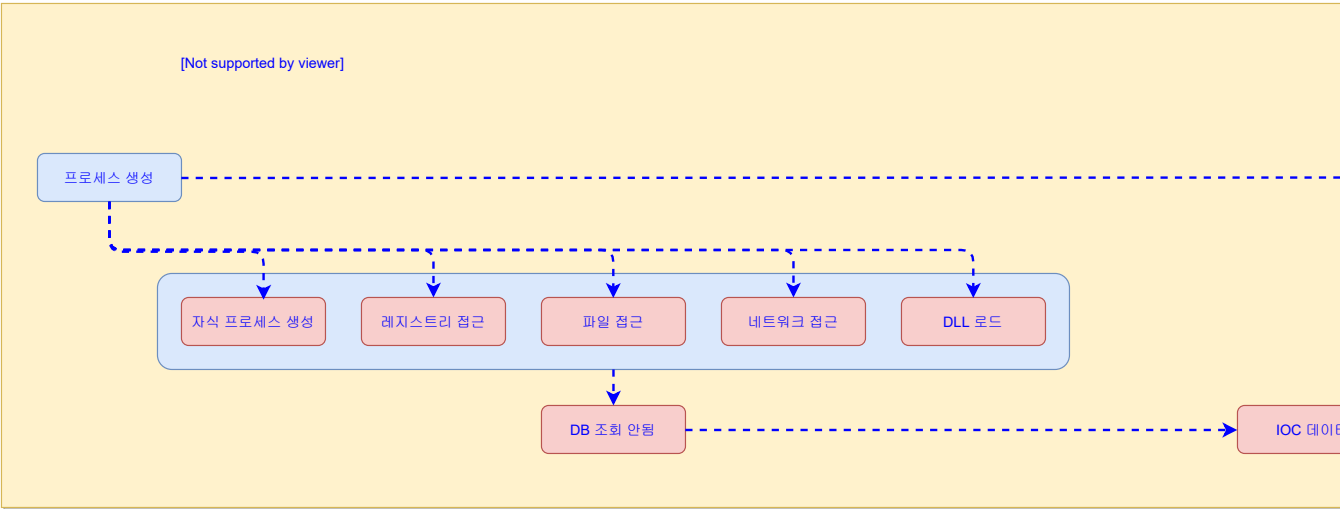


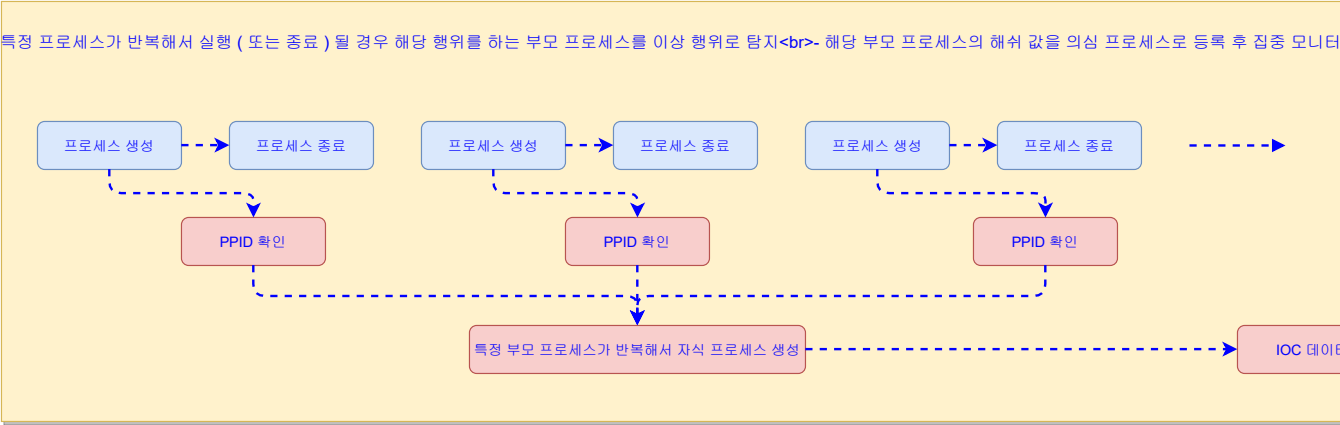
<br style="font-size: 14px">프로세서 life Cycle ( 날짜별 프로세스 해쉬 정보로 일반적인 프로세스 라이프 사이클 정보가 DB 에 저장 되어 있음



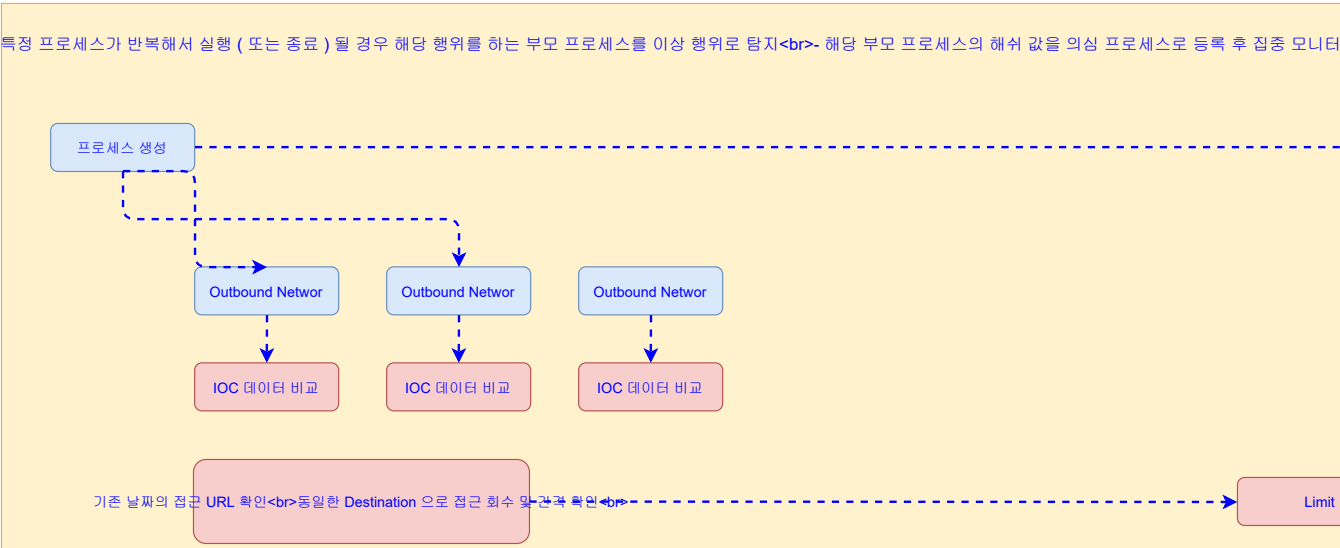
[Not supported by viewer]



행위로 탐지<br>특정 프로세스가 반복해서 실행 ( 또는 종료 ) 될 경우 해당 행위를 하는 부모 프로세스를 이상 행위로 탐지<br>해당 부모 프로세스의 해쉬 값을 의심 프로세스로 등록 후 집중 모니터



행위로 탐지<br>특정 프로세스가 반복해서 실행 ( 또는 종료 ) 될 경우 해당 행위를 하는 부모 프로세스를 이상 행위로 탐지<br>해당 부모 프로세스의 해쉬 값을 의심 프로세스로 등록 후 집중 모니터



기피에서 들어올 경우 Source IP에 해당하는 다른 피시 로그 확인<br>- 해당 IP에 해당하는 Host 로그를 통해 어떤 호스트의 어떤 프로세스가 반복 접근하는지<br>확인 후 처리 조치 가능<br><br><br><br><br><br>

