




SIEM Use Cases!

Part 2



 [scspcommunity](#)

 [SCSP Community](#)

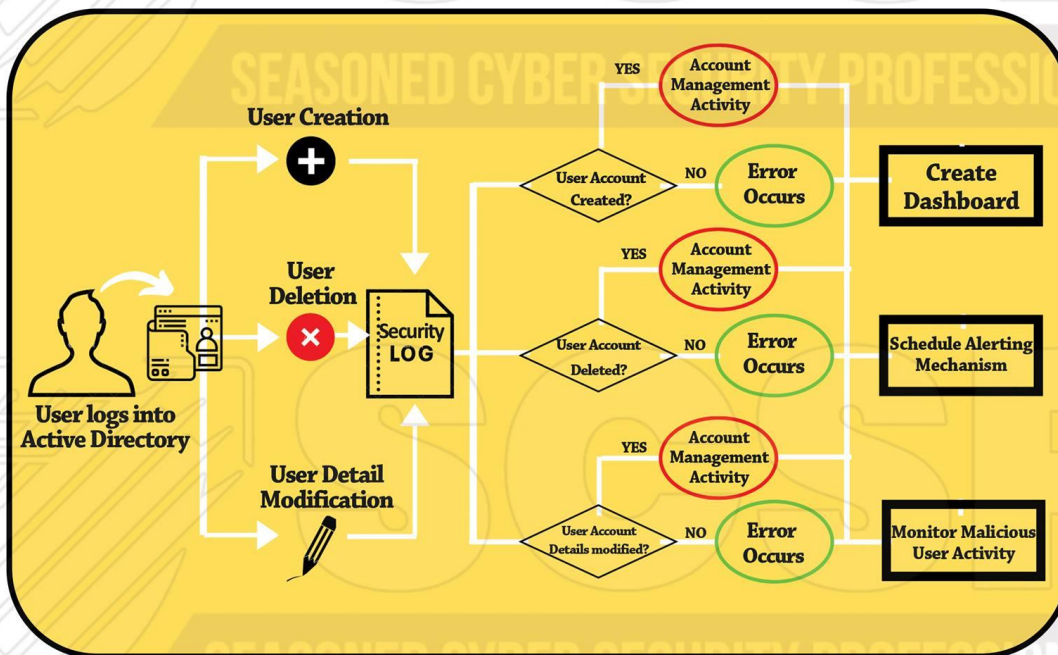
 [scsp-community](#)

 [scsp-community](#)

 [CommunityScsp](#)

Use Case # 01

User Account Management



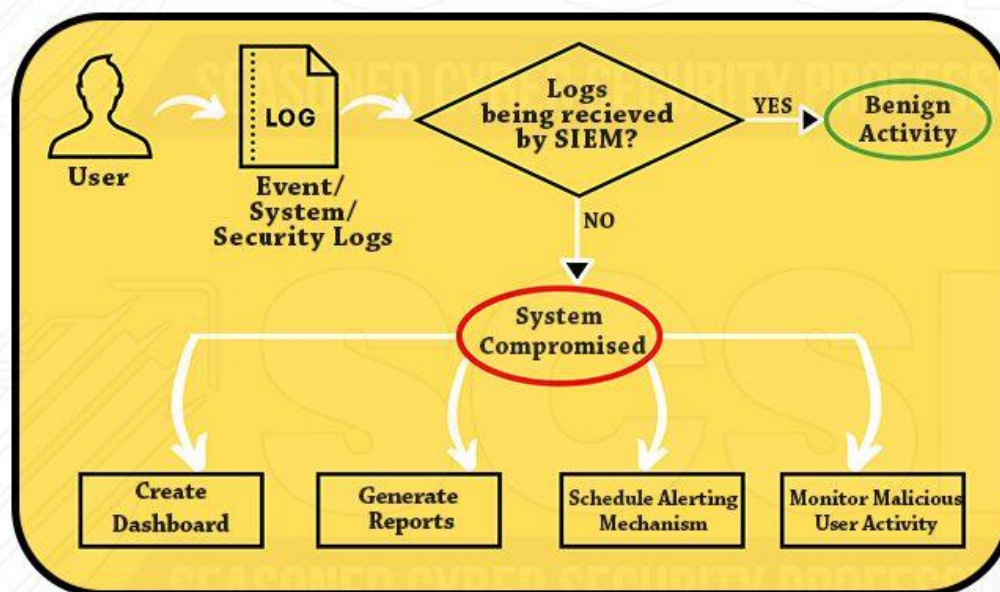
Follow us @ scspcommunity



Use Case # 02

Suspicious Behavior of Log Source

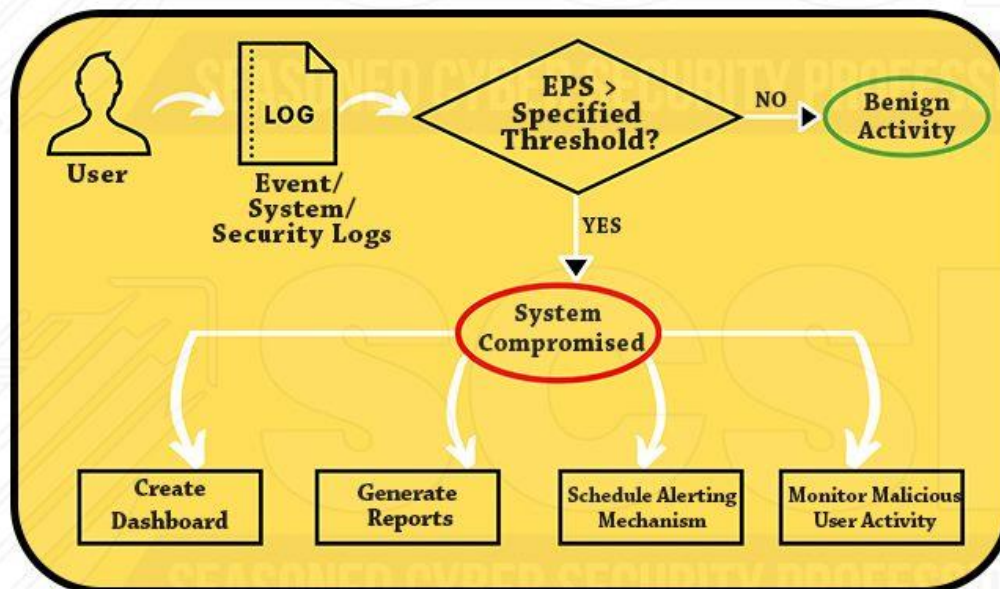
Expected Host/Log Source Not Reporting



Use Case # 03

Suspicious Behavior of Log Source

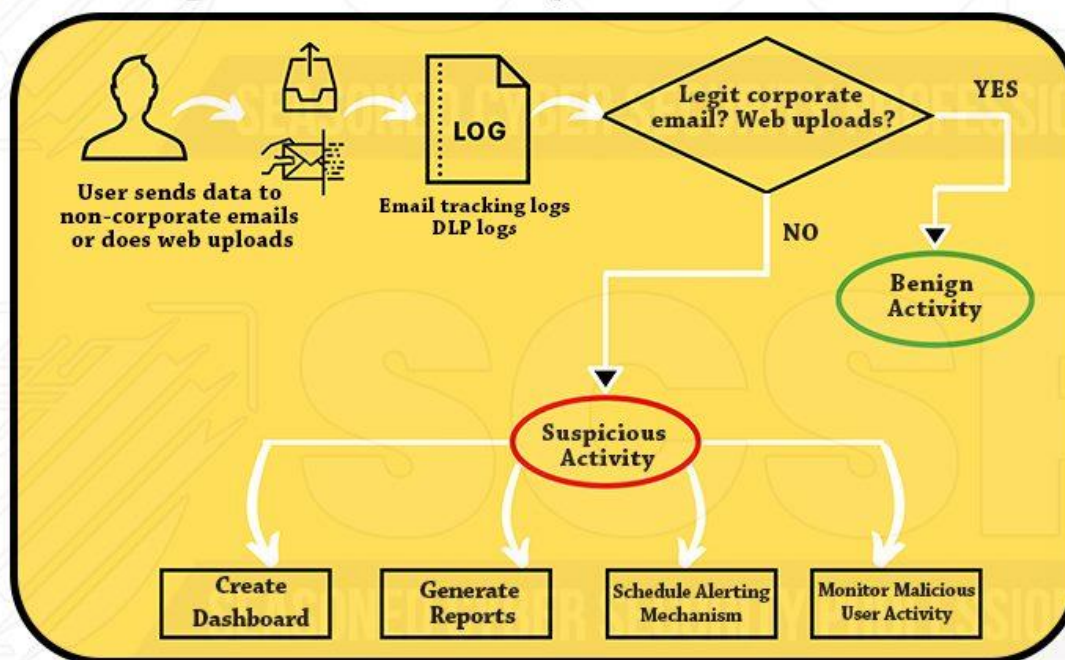
Unexpected Events Per Second (EPS) from Log Sources



Use Case # 04

Data Exfiltration

Sending data to non-corporated emails and web uploads





Use Case # 05

Data Exfiltration

Visiting watch listed or recently registered domains

