# SOC L1 töövoog – samm-sammuline juhend

See dokument annab samm-sammulise juhendi SOC (Security Operations Center) Level 1 analüütikule. Lisatud on ka CSV-mall alertide jälgimiseks ja Excelis analüüsimiseks.

1. Vastuvõtt – vaata uued alertid (kas uus või korduv).
2. Rikastamine – kontekst: vara kriitilisus, kasutaja roll, IP geograafia, tihedus.
3. Prioriseerimine – Severity × Asset_Criticality × korduvus.
4. Esmane analüüs – kas tegevus oli blokeeritud või reaalselt kahjulik?
5. Otsus & tegevus – tõkestamine, eskaleerimine või false positive.
6. Dokumenteerimine – Action_Taken, Notes, Evidence_Link, Status.
7. Järeltegevus – korduvuse kontroll, sulgemine, õppetundide jagamine.

| Username | User_Privileged | Geo | Event_Count | Severity | Status | Owner | SLA_min | Due_At | Age_h | Repeat_7d |
|---|---|---|---|---|---|---|---|---|---|---|
| svc_backup | Yes | EE | 50 | High | New | nan | 30 | nan | nan | nan |
| jane | No | EE | 1 | High | New | nan | 60 | nan | nan | nan |
| system | Yes | EE | 3 | Critical | Triage | analyst1 | 30 | nan | nan | nan |
| nan | No | DE | 200 | Low | New | nan | 240 | nan | nan | nan |
| mark | No | US | 6 | Medium | New | nan | 180 | nan | nan | nan |