Integration til SIEM

Formål

Du kan via denne vejledning se, hvordan du sender sikkerhedsloggen i XFlow over i dit SIEM-system.

Forudsætning

For at kunne benytte integrationen kræver det, at du har et SIEM-system, og at dette system understøtter at læse og parse logs fra filer.

Det kræver desuden, at du har en SFTP-server til rådighed, hvor logsene kan transporteres til.

Opsætning

For at slå denne funktionalitet til skal du kontakte XFlow, som så kan hjælpe dig med dette.

I den forbindelse skal du oplyse følgende adgangsoplysningerne til din SFTP-server:

- SFTP-adressen
- Brugernavn
- Adgangskode

Logdata

XFlow gemmer følgende informationer for hver gang, der logges i en fil:

- Timestamp - Tidspunkt for hvornår logningen fandt sted
- Log severity - Denne er altid sat til "Information"
- Internt brugerId - XFlow brugerid på brugeren der gennemførte handlingen
- Brugers navn - Navnet på brugeren der gennemførte handlingen
- Brugers CPR - CPR på brugeren der gennemførte handlingen (Valgfri)
- Brugers e-mail - E-mailadresse på brugeren der gennemførte handlingen
- Brugers initialer - Initialer på brugeren der gennemførte handlingen
- Brugers organisationId - XFlow organisationsId på den organisation brugeren der gennemførte handlingen er tilknyttet til
- Brugers IP adresse - IP-adresse på brugeren der gennemførte handlingen
- Handlingsbeskrivelsen er bestående af "Search", "Read", "Delete", "Edit" eller "Create" - Beskrivelse af hvilken type hændelse der blev gennemført af brugeren. Eks. "(IP-adresse) har udført handlingen "Read" på blanket med TaskId XXXX, BlanketID YYYY"

Handlinger der logges

Sikkerhedsloggen indeholder alle de hændelser hvor brugere af XFlow potentielt får adgang til personfølsomt data. En nærmere beskrivelse af disse hændelser finder du her under afsnittet "Logning".

For hver hændelse kobles en handling således at man f.eks. både kan læse, slette, oprette og redigere en blanket, med udgangspunkt i at man har udført hændelsen der omhandler at man får adgang til blanketten.