Zoznam špecifických use casov

detegovaný a neodstránený malware na zariadení

používanie administrátorských účtov

nadmerný počet neúspešných prihlásení

detekcia malware v odchádzajúcej pošte

prístup na stránky s nízkou reputáciou

používanie účtu používateľa počas jeho neprítomnosti

pridanie alebo odobranie používateľa z privilegovaných AD skupín

integrácia udalostí zo SWIFT

detekcia vPC athentication failure

detekcia TU athentication failure

priamy prístup do db IS IBFO mimo aplikácie IS IBFO

zvýšený prenos údajov z aplikačného servera IS IBFO

zmena používateľských oprávnení IS IBFO

detekcia prihlásení do IS IBFO

Nginx alarm

detekcia používania Teamviewer

detekcia obchádzania proxy servera

detekcia zneužívania komunikačných kanálov malware na SWIFT serveroch

detekcia prihlásení na Oracle privilegované účty mimo pracovnú dobu

detekcia neúspešných prihlásení na rôzne Oracle účty z rovnakej IP

detekcia prihlásení na MSSQL privilegované účty mimo pracovnú dobu

detekcia neúspešných prihlásení na rôzne MSSQL účty alebo inštancie z rovnakej IP

detekcia neúspešných prihlásení na rôzne DAFNE účty z rovnakej IP

detekcia prihlásení na DAFNE privilegované účty mimo pracovnú dobu