

KYBERTURVALLISUUDEN YLLÄPITÄMINEN

Todistus

Kyberturvallisuuden Ylläpitäminen - Tietoverkon valvonta

Käyttäjä **s2200855@edu.bc.fi** on suorittanut **100%** osiosta **Kyberturvallisuuden Ylläpitäminen - Tietoverkon valvonta**.



Kuvaus:

Tämä polku vastaa kyberturvallisuuden ylläpitäminen (30 op) tavoitteeseen "Osaa valvoa tietoverkkoa hyödyntämällä erilaisia analysointityökaluja"

Suoritetut moduulit:



Mitä on tietoturva-
valvonta?



False positiivinen vs false
negatiivinen

✓	IDS/IPS järjestelmät	✓	Mitä ovat tietoturvatapahtumat? Mitä kannattaa kerätä ja milloin kannattaa tehdä hälytys?
✓	SIEM -järjestelmät	✓	Lokilähteen lisääminen ELK Stackiin
✓	Lokien tutkiminen -harjoitus 1	✓	Lokien tutkiminen -harjoitus 2
✓	Lokien tutkiminen -harjoitus 3	✓	Hälytykset tietoturvalavallvonnassa