**Introducere**

**De ce ar trebui să iau acest modul?**

Bun venit la Switch Security Configuration!

O parte importantă a responsabilității tale ca profesionist în rețea este să păstrezi rețeaua în siguranță. De cele mai multe ori ne gândim doar la atacurile de securitate care vin din afara rețelei, dar amenințările pot veni și din interiorul rețelei. Aceste amenințări pot varia oriunde, de la un angajat care adaugă inocent un comutator Ethernet la rețeaua corporativă, astfel încât să poată avea mai multe porturi, până la atacuri rău intenționate cauzate de un angajat nemulțumit. Este datoria dumneavoastră să mențineți rețeaua în siguranță și să vă asigurați că operațiunile de afaceri continuă fără compromisuri.

Cum menținem rețeaua sigură și stabilă? Cum îl protejăm de atacurile rău intenționate din interiorul rețelei? Cum ne asigurăm că angajații nu adaugă comutatoare, servere și alte dispozitive în rețea care ar putea compromite operațiunile rețelei?

Acest modul este introducerea dumneavoastră în menținerea rețelei în siguranță din interior!

**Ce voi învăța în acest modul?**

**Titlul modulului** : Configurarea securității comutatorului

**Obiectivul modulului** : Configurați securitatea comutatorului pentru a atenua atacurile LAN.

|  |  |
| --- | --- |
| Legenda tabelului | |
| **titlul topicului** | **Obiectivul subiectului** |
| Implementați securitatea portului | Implementați securitatea porturilor pentru a atenua atacurile tabelelor de adrese MAC. |
| Reduceți atacurile VLAN | Explicați cum să configurați DTP și VLAN nativ pentru a atenua atacurile VLAN. |
| Reduceți atacurile DHCP | Explicați cum să configurați DHCP Snooping pentru a atenua atacurile DHCP. |
| Reduceți atacurile ARP | Explicați cum să configurați inspecția ARP pentru a atenua atacurile ARP. |
| Reduceți atacurile STP | Explicați cum să configurați PortFast și BPDU Guard pentru a atenua atacurile STP. |