

# Bezpečnostní technologie

- [Základní studijní materiál](#)
- [Závěrečné práce k tématu](#)
- [Obsah kurzu](#)

# Základní studijní materiál

## **DP: Informační a kybernetická bezpečnost ve zdravotnictví**

## **Protokoly aplikační vrstvy: Zabezpečení počítačových sítí**

## **Technická specifikace předmětu veřejné zakázky: FIREWALL**

# Závěrečné práce k tématu

**DP: Analýza síťových dat v kontextu kybernetické bezpečnosti**

**DP: Metodika nastavení pravidel firewallu**

**BP: Bezpečnost mobilních zařízení v malé společnosti**

# Obsah kurzu

- 1. Správa systému, automatizace a orchestrace.**
- 2. Akcelerace.**
- 3. Správa vzdálených přístupů.**
- 4. Ochrana před sofistikovanými útoky.**
- 5. Bezpečnost OS, databází, mobilních sítí a serverů.**
- 6. Pokročilé technické a softwarové prostředky bezpečnosti informačních systémů.**
- 7. Mapování PC a sítě, zneužití samotné sítě.**
8. Aktivní a pasivní preventivní opatření, řízení přístupu.
9. Současná práce více administrátorů, delegovaná administrace, Správa licencí.
10. Analýza a údržba logů, tvorba reportů, clustering, clusterXL, VRRP.
11. Ochrana před sofistikovanými útoky a přehled pokročilých příkazů.
12. Infrastruktura Check Point Firewall, získávání informací prostřednictvím CPView a CPInfo.
13. Řešení pro vzdálený přístup, check Point Mobile Access, check Point Capsule.
14. Ochrana proti zero-day a APT útokům, check Point SandBlast. check Point Mobile Threat Prevention.