3 commandes :

ping #IP ou #@dns
ping -a #IP → pour avoir le nom d'une adresse IP
ping -t #IP ou #@dns → pour un ping constant, peut servir en cas de matériel défectueux, maintenance, supervision
ipconfig → pour adresse ip, masque etc
ipconfig /all → connaître toutes les ip du réseau

Toujours travailler sur l'IP.

Éléments de sécu dans une entreprise :
-Firewall
-Antivirus
-Antispam
-Système de sauvegarde (backup)

Firewall → filtre les fluxs(def) entrant et sortant
liste d'instructions :
→ Règles
→ Numéro de règles
→ IP source
→ IP destination
→ Allow / Deny
→ numéro de port
Constructeur de pare feu: Cisco, Stormshield

Antivirus → Analyse, comportement, IPS / IDS

IPS : base international d'IP malveillante si on veut communiquer avec IPS nous bloque
IDS : si IP avec qui on communique pas connu, si IDS remarque un comportement suspect il nous bloque

Antispam → idem que antivirus → Entrant et Sortant

Système de sauvergarde → Vecas, Akronis, Windows Backup

Exemple pour empêché mes employés de consulter certains sites :
On peut agir sur le firewall, sur l'antivirus

Ransonware → cryptage de données + rançon en cryptomonnaie
Phishing → Emails
Mind on the middle → Usurpation
Trojan → Emails / fichiers
Ddos → Surcharge réseaux

Attaque la plus dangereuse = Ransonware
// la plus rapide = Ddos

En moyenne pour Ransonware, entre le début et la fin de l'attaque il se passe 1an et 3mois
Exfiltration de données peut prendre un bon moment (24 décembre, jours fériés)
Cryptage des données à lieu à la fin

Entre début et exfiltration : Constatation(voir si c intéressant) , si oui Analyse, si toujours intéressant Injection du virus 8otcet par 8octet toutes les sec, min, heures, jours

Seule chose qu'on peut faire c'est activer IPS, géolocalisation, faire un audit de sécurité(regarder ce qui rentre et sort du réseau pour voir si nous sommes exposé ou pas)

Si on paie la rançon on est pas sur qu'on nous rende nos données ou si on nous les rend pas avec les mêmes virus à l'intérieur
Vitesse de cryptage = 2gigas / min

Il faut sensibiliser les collaborateurs au danger
Sensibilisation → Informations
→ Faire un faux Phishing anonyme et voir le nb de clics, de réponses, de dl de la pièces jointes et nb d'emails non ouverts
→ Faire une démo (exemples : mdp → complexité, prouver aux users que tout est ok, listing des clients impactés – pertes financières – responsabilité du collaborateur)