COLLOQUE CYBERSECURITE

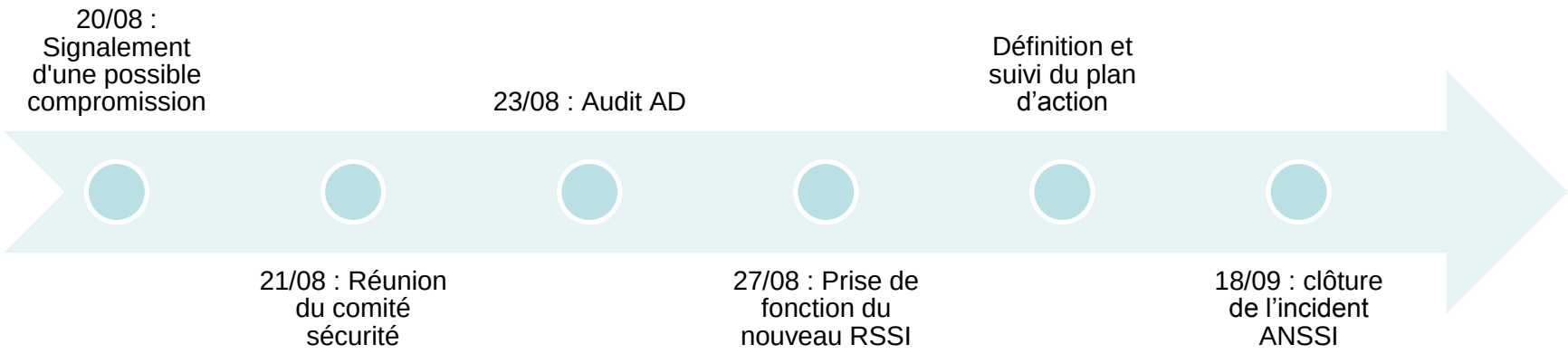
19 Octobre 2018

CHRU NANCY

- 12 000 agents
- 1 600 lits
- 700 000 patients accueillis par an
- Acteur majeur de la recherche biomédicale et de l'innovation (ex : hôpital virtuel)
- 11 établissements de formation forment 5000 professionnels par an
- Classement Le Point 2018 : 10ème au niveau national

CHRONOLOGIE

Accès database [CHRU DE NANCY HOPITAL] j'ai accès a la database entière du chru de nancy, ont pourrais on en parler un peu plus si vous le souhaitez ? :)



INVESTIGATION ET REMEDIATION

- Dépôt de plainte par l'officier de sécurité
- Analyse de l'activité des 3 mois précédents (volumétrie, source, destination, contenu)
- Surveillance renforcée des accès internes et externes (analyse de logs)
- Audit Active Directory
- Revue de comptes applicatifs et techniques
- Filtrage des principales infrastructures C2
- Identification et correction de vulnérabilités
- Mail de sensibilisation utilisateurs
- Durcissement de la politique de mots de passe

ENSEIGNEMENTS

- Aucune anomalie détectée
- Mobilisation des ressources (/!\ DoS humain)
- Actions correctives (court terme) et actions préventives (long terme)
- Meilleure prise en compte des sources de menaces internes
- Opportunité de mettre des PROCESSUS en place
- Constats :
  - Manque de visibilité sur la surface d'attaque
  - Nécessité de mettre en œuvre un processus de veille (OSINT, Dark web)