



2MN LTD

- ❑ A propos de 2MN
- ❑ Gestion projets : expert en management et en gestion de projets, avec expérience prouvée dans des multinationales
- ❑ Technique: ingénieurs informaticiens, anciens consultants de grands opérateurs et constructeurs
- ❑ Certifications: CISCO, RSA, CHECKPOINT, MICROSOFT, CISSP





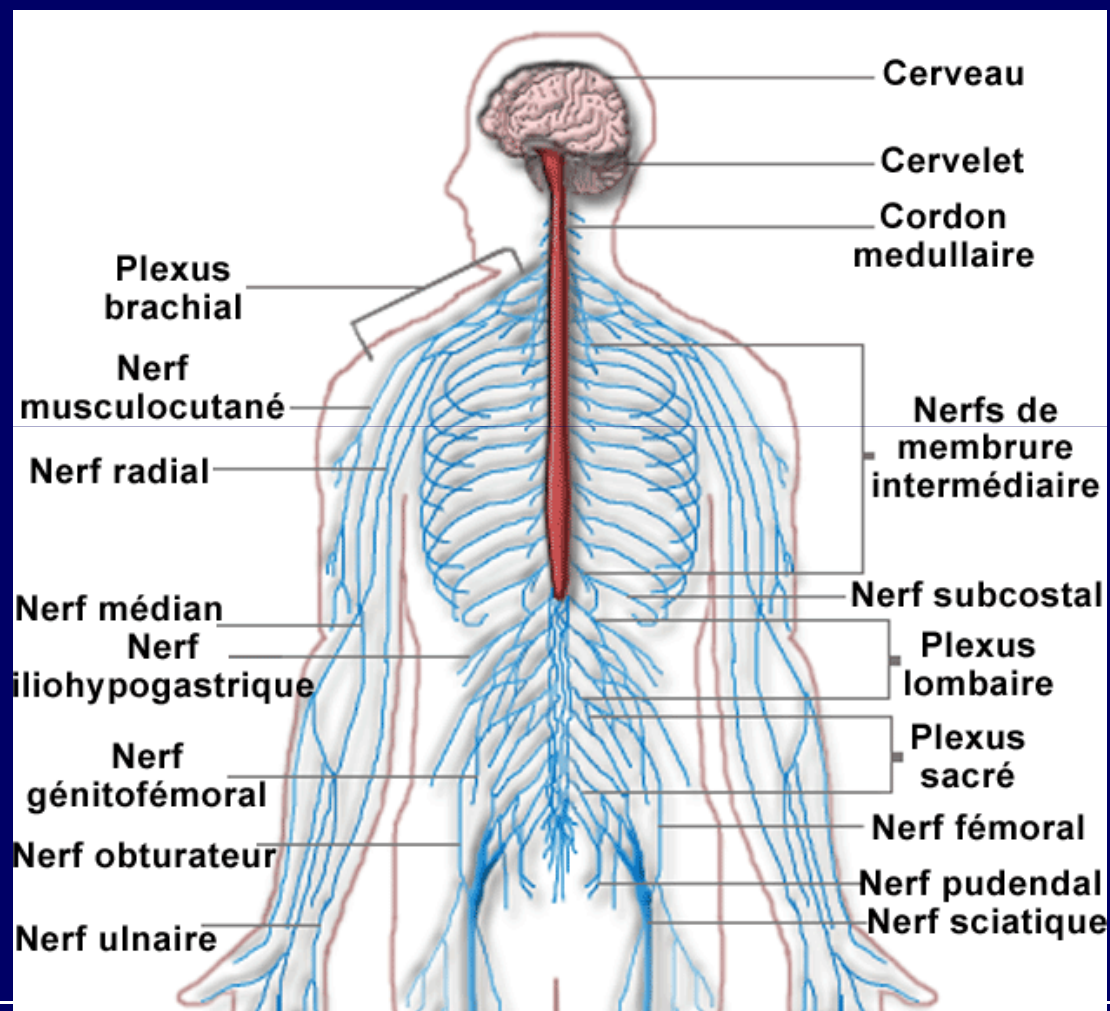
RSA ENVISION

SOMMAIRE

- ❑ LE CONCEPT SIEM
- ❑ FONCTIONALITES
- ❑ LES SOURCES ET TYPE DE CAPTURE
- ❑ QUELS SONT LES BENEFICES?
- ❑ ENVISION EN ACTION
 - Correlation
 - Watchlist
- ❑ ARCHITECTURE
- ❑ QUESTIONS/REponses



LE CONCEPT SIEM



LE CONCEPT SIEM



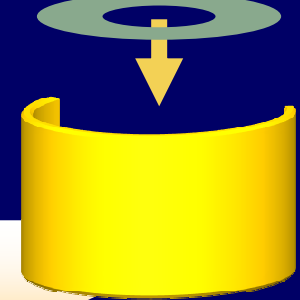
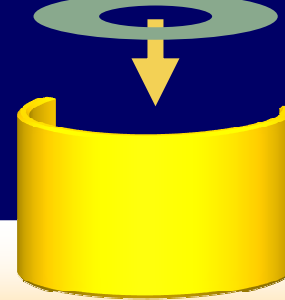
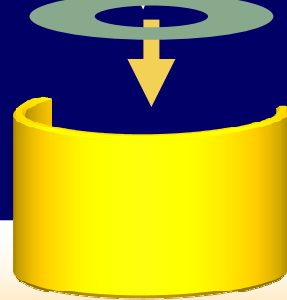
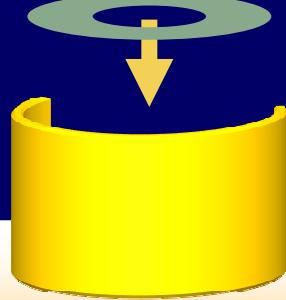
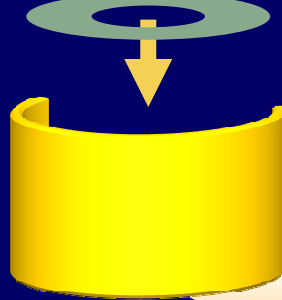


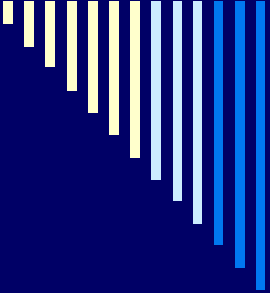
FONCTIONALITES

- COLLECTE DES JOURNAUX D'ÉVÉNEMENTS EN TEMPS REELS
- OUTILS GRAPHIQUE D'ANALYSE
- VUE PANORAMIQUE ET FORENSIQUE
- LE WATCHLIST
- LA SAUVEGARDE HISTORIQUE
- LE VAM (Vulnerability Asset Mgmt)
- GESTION D'INCIDENTS ET DISTI DES TACHES
- MODEL SIMPLE OU DISTRIBUE



DIVERS INCIDENTS



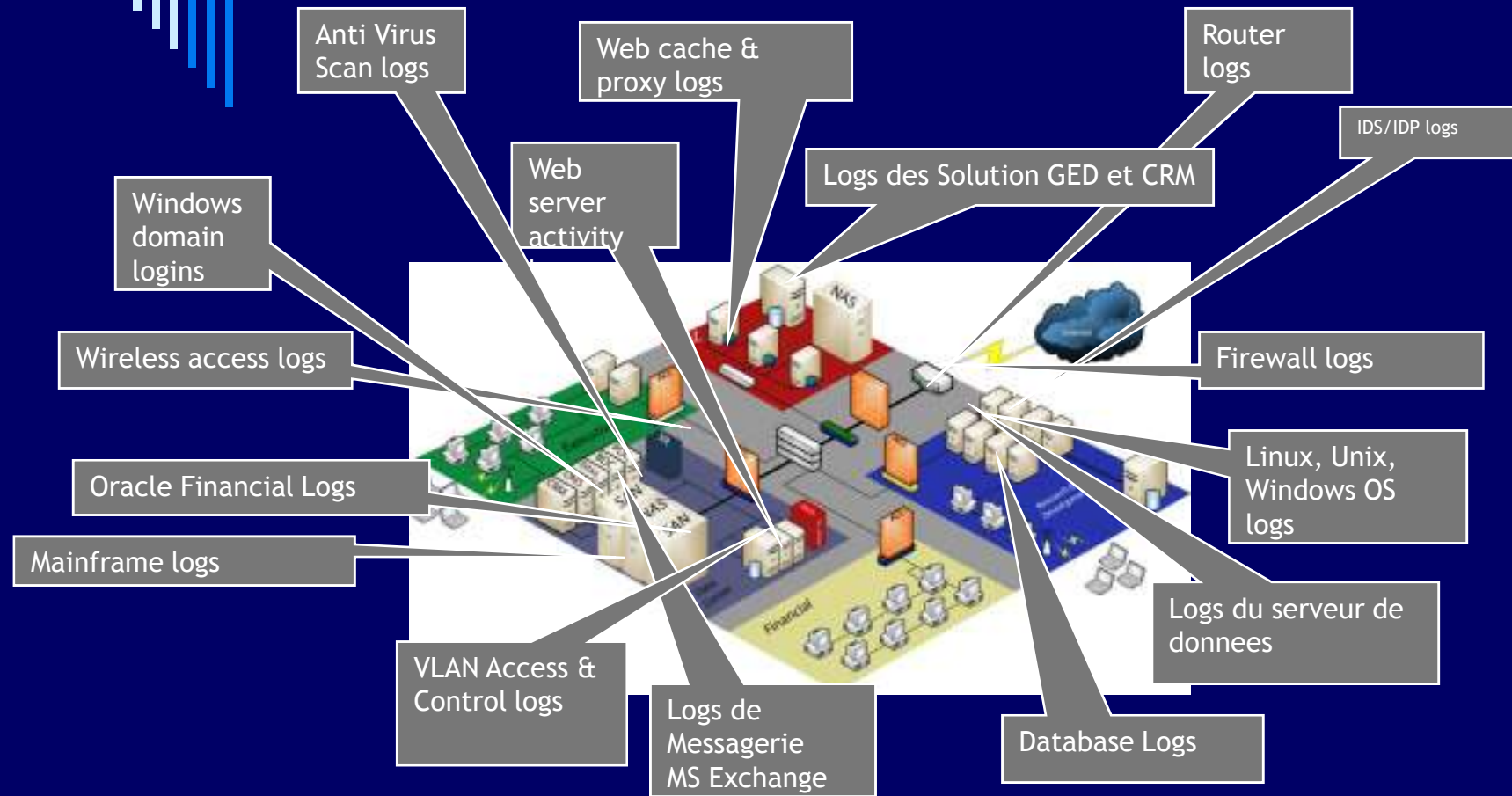


SOURCES ET TYPE DE CAPTURE

- INFRASTRUCTURE RESEAUX
- SERVEURS D'APPLICATIONS
- BASE DE DONNEES
- SERVEURS WEB
- CONTROLLEUR D'ACCES
- SURVEILLANCE VIDEO CAMERA
- SYSTEM D'EXPLOITATION
- GESTION DE STORAGE
- REPORTING IMPRIMANTE RESEAUX...ETC...



LES DIFF SOURCES

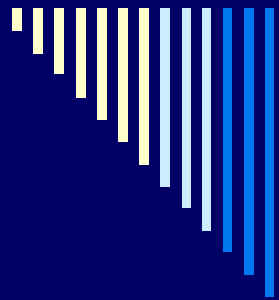




QUELS SONT LES BENEFICES ?

- VUE CENTRALISEE DES EVENEMENTS
- COORDINATION DES ACTES ET REACTION
- INFORMATION ET RAPPORT SUR LE PATRIMOINE INFORMATIQUE ET RESEAU
- LESSON HISTORIQUE
- CONFORMITE REGULARISATION





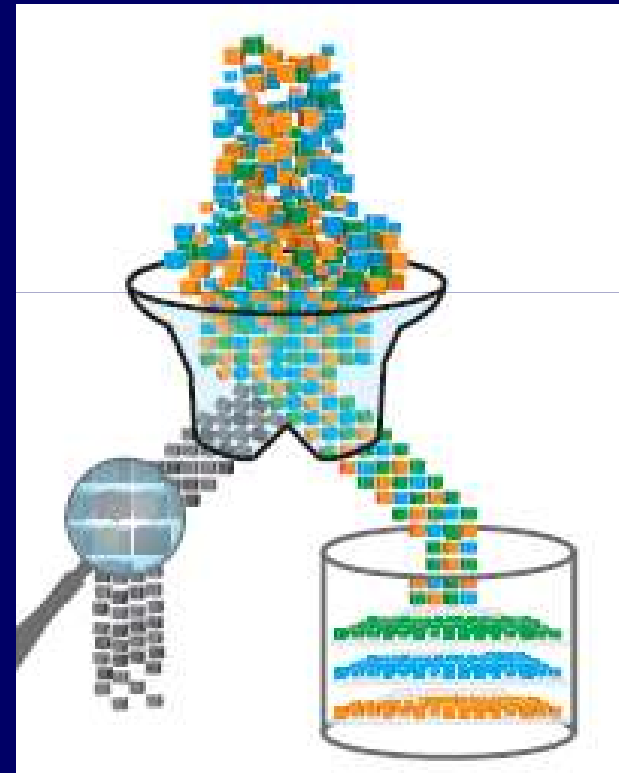
ENVISION EN ACTION

- LA CORRELATION DES JOURNAUX D' EVENEMENTS
- LE WATCHLIST



ARCHITECTURE

- ❖ LES COMPOSANTES
 - IPDB
 - ANALYSE
 - REPORT
- ❖ DEPLOYMENT
 - MODE UNIQUE
 - MODE DISTRIBUEE





QUESTIONS / REPOSES

?

