Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE
ET DES
ANCIENS COMBATTANTS

Séminaire ARCSI – 13 juin 2014

dpsd

Plan

- La DPSD
- Protection des systèmes d'information classifiés
- Panorama des cyberattaques en Midi-Pyrénées

LA DPSD

Direction de la protection et la sécurité de la défense

Missions

Service de renseignement de la défense

Assure la sécurité :

- du personnel
- des informations
- du matériel
- des installations



Direction de la protection et la sécurité de la défense

Missions au profit de la sphère industrielle défense

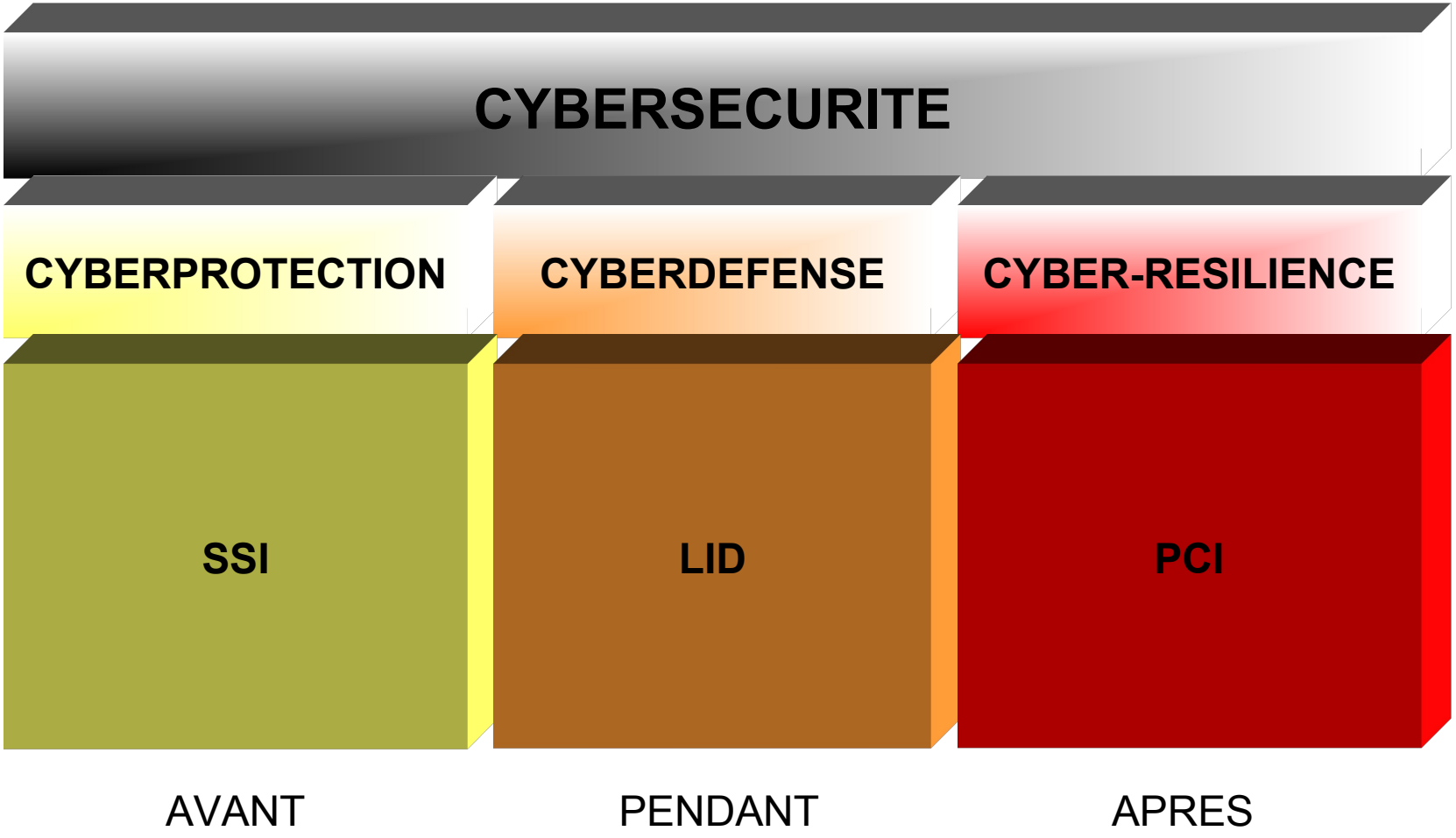
Sécurité économique

- Sécurité industrielle
- Contre ingérence économique

Acteur cybersécurité

- **SSI**
- **Cyberdéfense**

Direction de la protection et la sécurité de la défense



Direction de la protection et la sécurité de la défense

La sensibilité des informations

SENSIBLES

- PSTN
- Diffusion restreinte
- Données personnelles
- Confidentiel personnel
- Confidentiel médical
- Propriété intellectuelle
- Secret des affaires
- Et le reste…

CLASSIFIEES

- Très secret défense
- Secret défense
- Confidentiel défense

Code pénal
IGI 1300 du 30 novembre 2011

SYSTEMES D'INFORMATION CLASSIFIES

Systèmes d'information classifiés

Principes de protection des SI classifiés

- **Principes relatifs à l'organisation**
- **Principes relatifs aux moyens techniques**
- **Principes de défense en profondeur**

Systèmes d'information classifiés

Principes relatifs à l'organisation

- **Homologation du système**

- Prise en compte de la sécurité
- Politique de sécurité
- Organisation de la chaîne des responsabilités
- Contrôle de la sécurité du SI
- Gestion des incidents de sécurité

Systèmes d'information classifiés

Principes relatifs aux moyens techniques

- Protection physique du système
- Protection technique du système
- Agrément des dispositifs de sécurité
- Gestion et contrôle d'accès au système

Systèmes d'information classifiés

Principes de protection des lieux

- Dispositifs de protection
- Dispositifs de détection et d'alarme
- Moyens d'intervention
- Dispositifs de dissuasion

$$\text{Intrusion} > \left(\sum \begin{matrix} \text{Détection} \\ \text{Freinage} \\ \text{Intervention} \end{matrix} \right)$$

Systèmes d'information classifiés

Principes de défense en profondeur

- Prévenir
- Bloquer
- Contenir
- Détecter
- Réparer

PANORAMA DES CYBERATTAQUES

EN REGION MIDI-PYRENEES

Cybermenaces mondiales

- Espionnage (Affaire Snowden, 2013)
- Déstabilisation (Crimée, 2014)
- Sabotage (Ver Stuxnet, 2010)

En Midi-Pyrénées ?

- Espionnage
  - Attaques via Internet (APT, troyens, etc.)
  - Vols d'ordinateurs portables
  - Vols de documents sensibles
  - Ingénierie sociale

- Déstabilisation / Sabotage
  - Modification de sites web
  - Cybercriminalité (phising, FOIV, ransomware, etc.)

Conclusion

- Adopter une démarche globale
- Adapter la SSI aux enjeux
- Gérer les risques
- Élaborer une PSSI
- Utiliser les produits et prestataires labellisés
- Viser une amélioration continue

Merci pour votre attention

Questions ?

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE
ET DES
ANCIENS COMBATTANTS

DIRECTION DE LA PROTECTION ET DE LA SECURITE DE LA DEFENSE

« Renseigner pour Protéger »

dpsd