La détection et la réponse aux incidents de sécurité de l'information dans un contexte gouvernemental, 11 avril 2017, Université Laval

Denis Shaink, conseiller en sécurité de l'information

ISACA®

Fiabilisez, optimisez et rentabilisez les systèmes d'information

Section de Québec

Agenda

- Présentation du Ministère
- Structure de gouverne
- Lignes de défense
- Mécanismes de détection
- Processus d’escalade
- Exemples d’alertes (console et antivirus)
- Arrimage avec les bonnes pratiques
- Conclusion
- Questions

Présentation du ministère de l'Économie, de la Science et de l'Innovation (MESI)

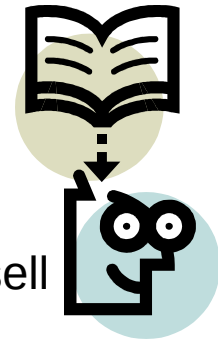
Le Ministère a pour **mission de soutenir** la croissance des entreprises, l'entrepreneuriat, la science, l'innovation ainsi que l'exportation et l'investissement. Il coordonne l'élaboration et la mise en œuvre de la **stratégie numérique**.

Il conseille également le gouvernement en vue de favoriser le **développement économique de toutes les régions du Québec**, et ce, dans une perspective :

- de création d'emplois;
- de prospérité économique;
- de développement durable.

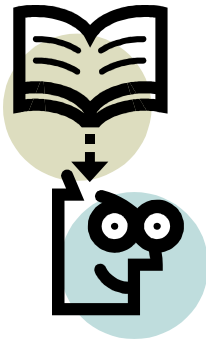
Le Ministère compte au 31 mars 2016, près de **700 employés** (répartis dans une vingtaine de bureaux) et un budget de 590 M$. (Source : Rapport annuel de gestion 2015-2016)

Structure de gouverne (1)



- ROSI (Responsable organisationnel de la sécurité de l'information) – David Beardsell
  - Il joue le rôle de porte-parole du DPI auprès de son organisation et doit s'assurer de la contribution de son organisation au processus de gestion des risques et **des incidents de sécurité de l'information à portée gouvernementale.**
- COSI (Conseiller organisationnel de la sécurité de l'information) – Denis Shaink
  - Il apporte son soutien au ROSI au niveau tactique, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels de sécurité de l'information dont **la gestion des incidents.**
- COGI (Coordonnateur organisationnel de gestion des incidents) – Denis Shaink
  - Outre sa participation active au réseau d'alerte gouvernemental, le COGI a notamment comme responsabilité de contribuer à la mise en place du **processus de gestion des incidents** de sécurité de l'information de son organisation.

Structure de gouverne (2)



- CSI (Centre des services informatiques)
  - Le centre des services informatiques (MESI) est **l'équipe de première ligne** pour la réponse aux incidents. Elle analyse et diagnostique l'incident de sécurité.
- CERT/AQ (Équipe de réponse aux incidents de sécurité de l'information du gouvernement)
  - Cette équipe contribue à la **mise en œuvre du processus de gestion des incidents à portée gouvernementale**. De plus, ce groupe constitue une **plateforme de partage d'information** entre les coordonnateurs organisationnels de gestion des incidents désignés en vertu de la Directive sur la sécurité de l'information gouvernementale.

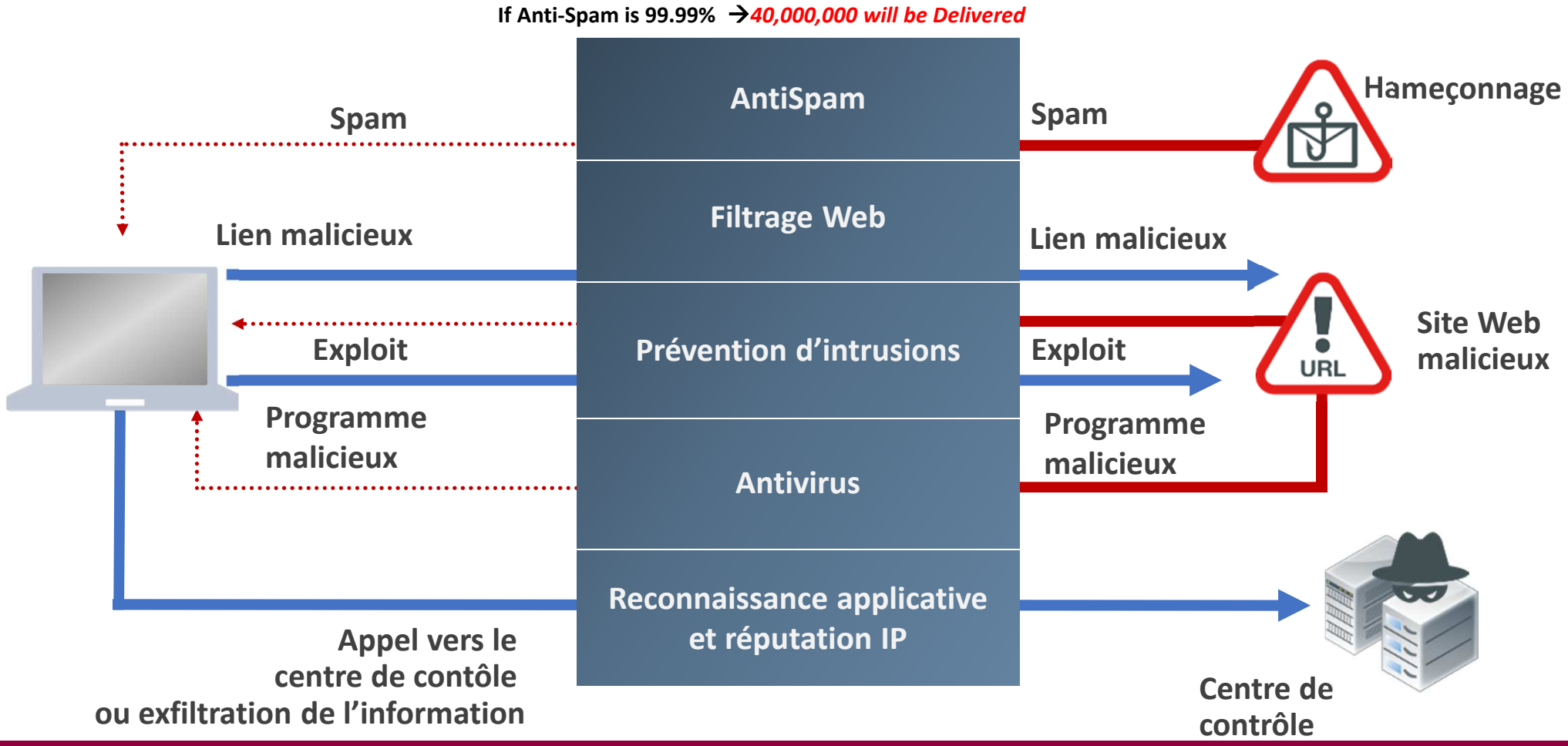
Lignes de défense internes

- Pare-feu avec antivirus (Firewall) pour les accès Internet
- Anti-spam avec antivirus pour la gestion du courriel
- Protection de certains types de fichiers (contre les programmes malveillants)
- Antivirus sur les postes de travail
- Capsules de sensibilisation

Mécanismes de détection

- Surveillance
- Firme de télésurveillance
- Consoles de surveillance
- Alertes
- Aspect humain

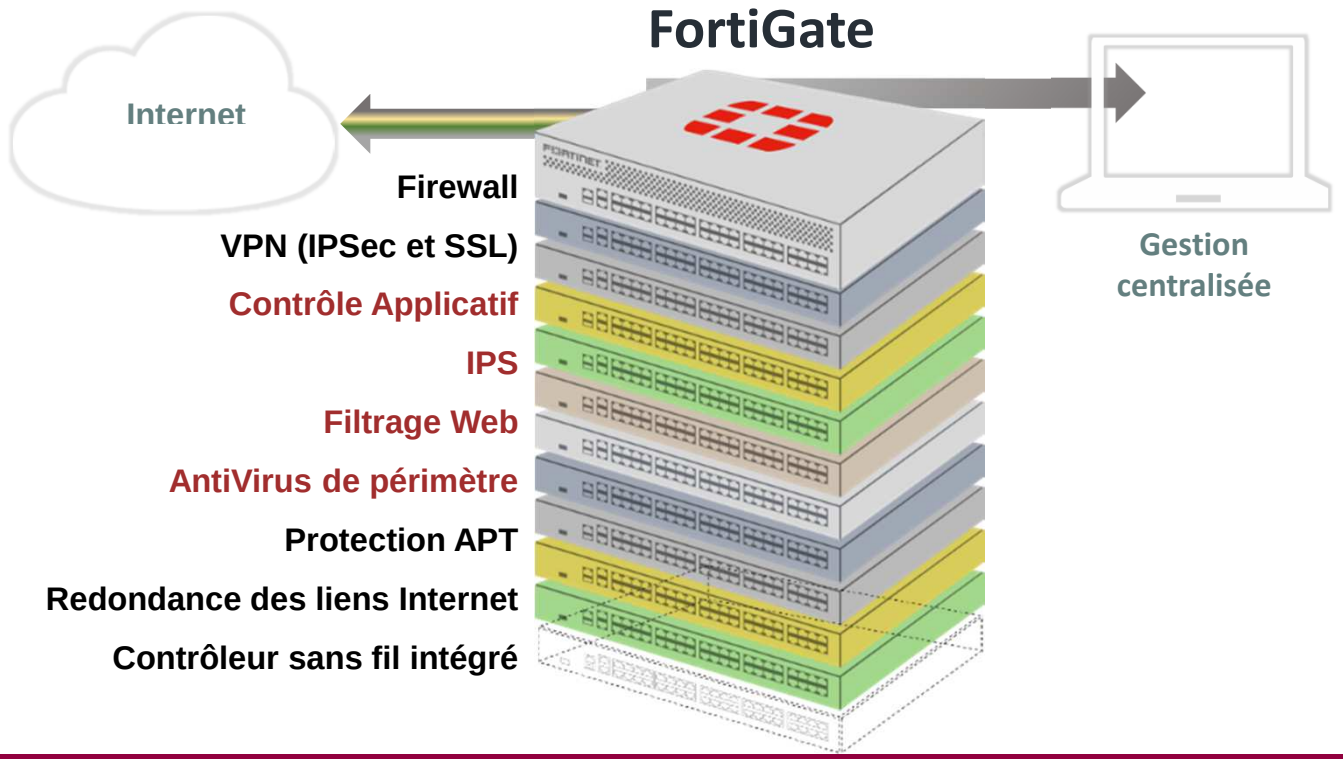
Vecteurs d'attaque et mécanismes de défense



L'Avantage Fortinet – Plateforme **Consolidée**

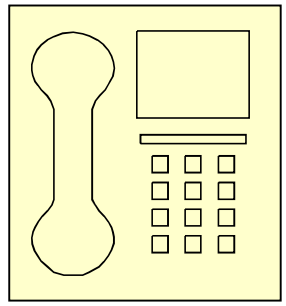
FortiOS permet la convergence Réseaux & Sécurité et la consolidation de la sécurité

Une seule licence pour l'accès à toutes les fonctionnalités sans limite d'usager



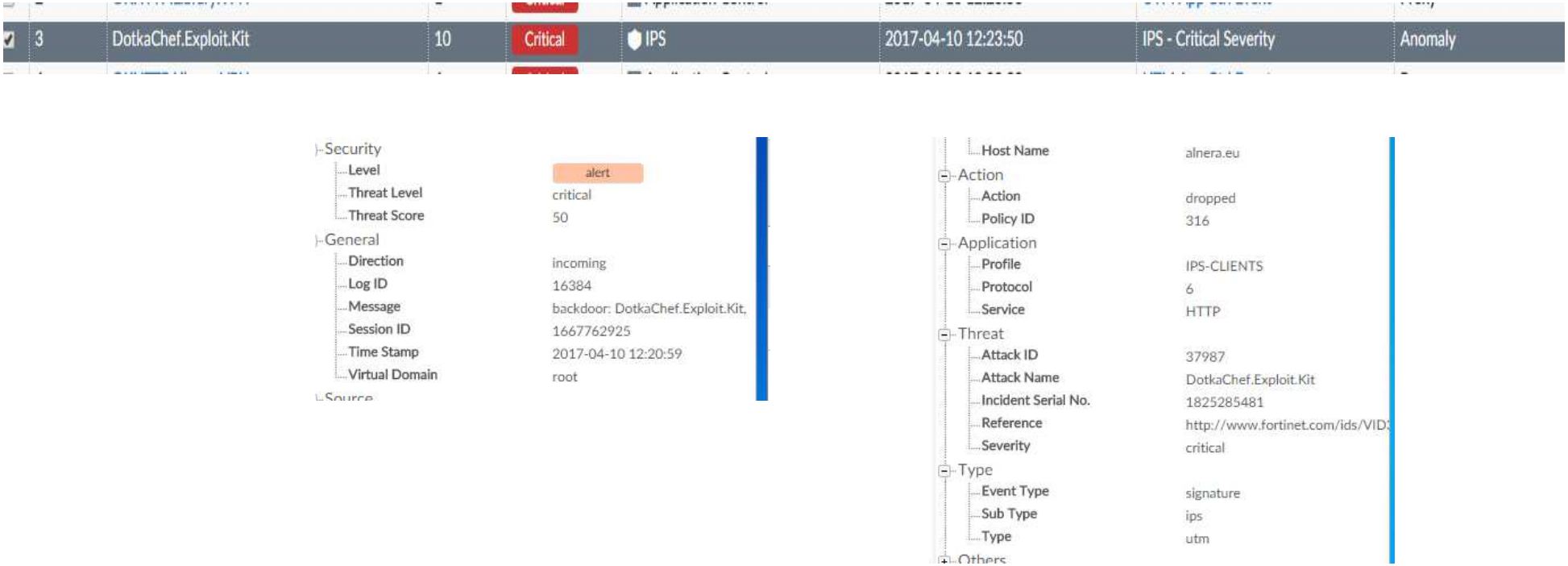
- Gestion simplifiée et centralisée
- Stratégie de sécurité unifiée
- Meilleure corrélation et visibilité des événements de sécurité
- Améliorer globablement votre architecture de sécurité

Processus d’escalade



À des fins internes seulement

Exemple d’alerte de la console Fortinet (1)



☑	3	DotkaChef.Exploit.Kit	10	Critical	IPS	2017-04-10 12:23:50	IPS - Critical Severity	Anomaly

Exemple d’alerte antivirus (2)

06/04/2017 13:58:00 to 06/04/2017 13:59:00

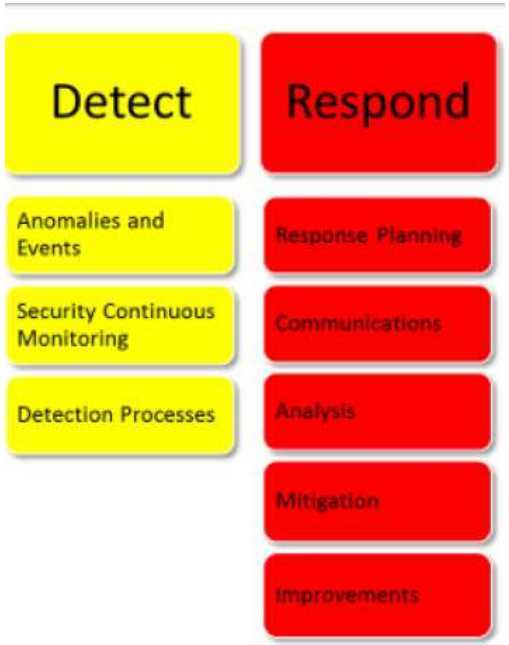
Computer User IP Address	Risk Risk Type	Risk Count	Date Time	Domain Server Group	Action Source	File / Entry	Hash Type / File Hash

Arrimage avec les bonnes pratiques

- ISO 27002 (Domaine 13)
  - Gestion des incidents liés à la sécurité de l'information dont l'objectif est de garantir que le mode de notification des événements et failles liés à la sécurité de l'information permette la mise en œuvre d'une action corrective, dans les meilleurs délais.
    - Signalements et failles
    - Gestion des améliorations et incidents (politique cohérente et efficace)

Arrimage avec les bonnes pratiques

- NIST (extrait du cyber security framework)



Arrimage avec les bonnes pratiques

- ISACA

Livre Blanc
de ISACA
Mars 2012

ISACA
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

Gestion et réponse aux incidents

CONCLUSION

- Processus de gestion des incidents doit être adapté à votre contexte organisationnel
- Souple et flexible
- Niveau d'escalade approprié
- Informer les parties prenantes en fonction de la gravité de l'incident (engagement)

Questions

MERCI