IBM Security Systems

Nicolas Atger

Responsable Marché Sécurité

@NicolasAtger

Security Intelligence.
Think Integrated.

IBM

Votre équipe France 2013

IBM Security Systems

Laurent Léger
SWG Brand Leader
Security

Marc Giacometti
Sales Manager
Tivoli & Security

Didier Eugene
Sales Manager
Tivoli & Security

Denis Collin
Sales Manager
Tivoli & Security

Aurore Ominetti
Security Sales

Pascal Tarin
Security Sales

Lionel Guillemot
Security Sales

Catherine Chappot
Security Sales
Enterprise

Cecile Chamelot
Inside Sales
Enterprise & MM

Pierre Herbelot
Sales Specialist
QRadar

Charles Tostain
Client Technical
Professional Manager

Arnaud Delande
Client Technical
Professional

Frédéric Michel
Client Technical
Professional

Serge Richard
Security Solution
Architect

Kamel Moulaoui
Client Technical
Professional

Stephan Ly
Zsecure Client Technical
Professional

Alexandre Videt
Channel Security Sales

Nicolas Atger
Field Market Manager
Security

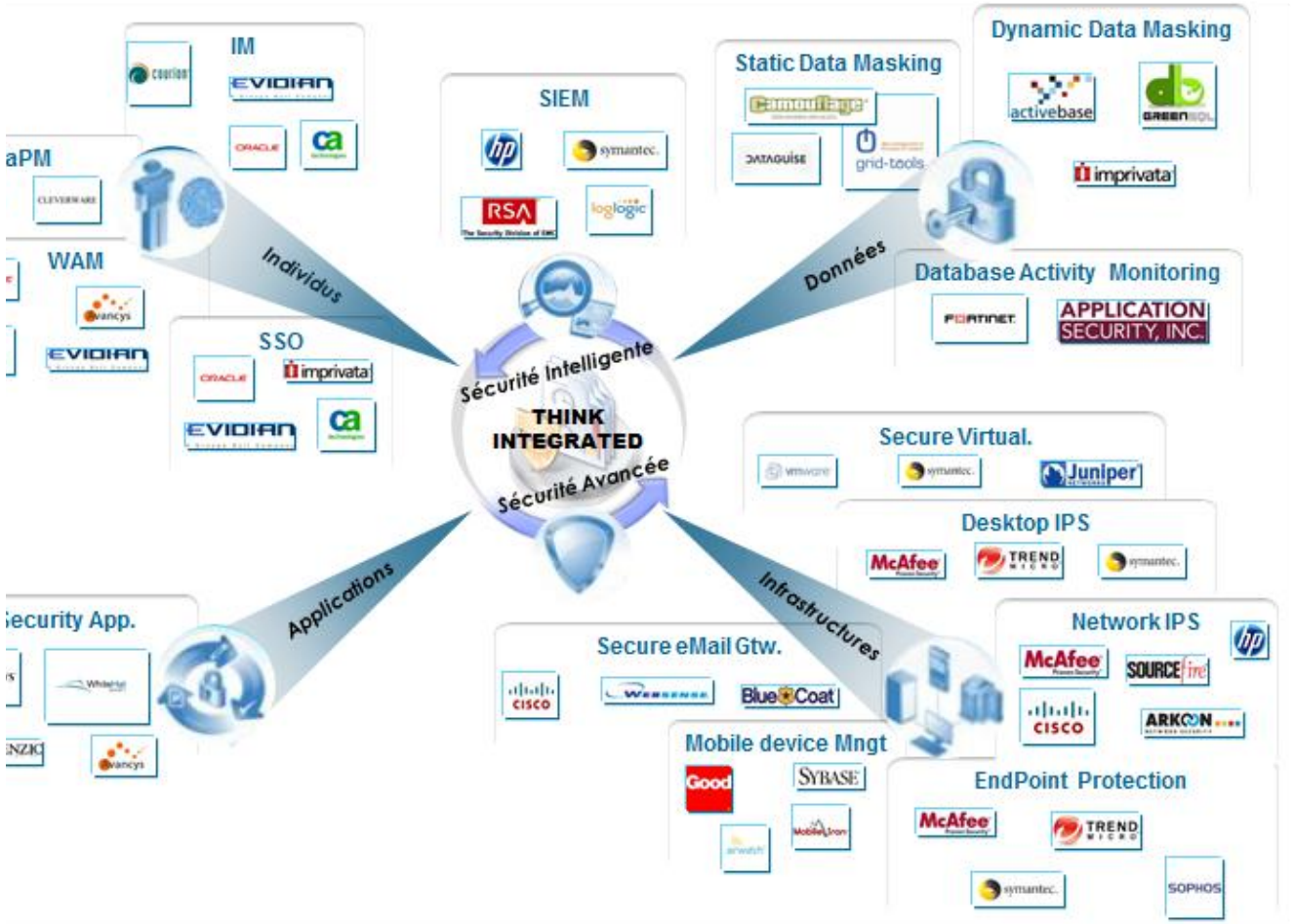
Martine Sobara
Demand Program
Marketing

Sophie Tacchi
Security Tiger Team

La position de la concurrence

IDC Worldwide IT Security

	Revenue
Symantec	3,659
Cisco	1,746
McAfee (an Intel company)	1,727
IBM	1,284
Check Point	1,228
Trend Micro	1,212
EMC	748
Microsoft	705
Juniper Networks	661
HP	644
Kaspersky Lab	613
Sophos (includes Astaro)	451
CA Technologies	447
Oracle	410
SafeNet	407
Fortinet	392
Websense	362
NetIQ (an Attachmate company)	332
Barracuda	212
AVG Technologies	207
SonicWALL (purchased by Dell)	202
F-Secure Corp.	194
ESET	193
Fujitsu	176
Hitachi	167
Palo Alto Networks	166
Sourcefire	159
Panda Security	156

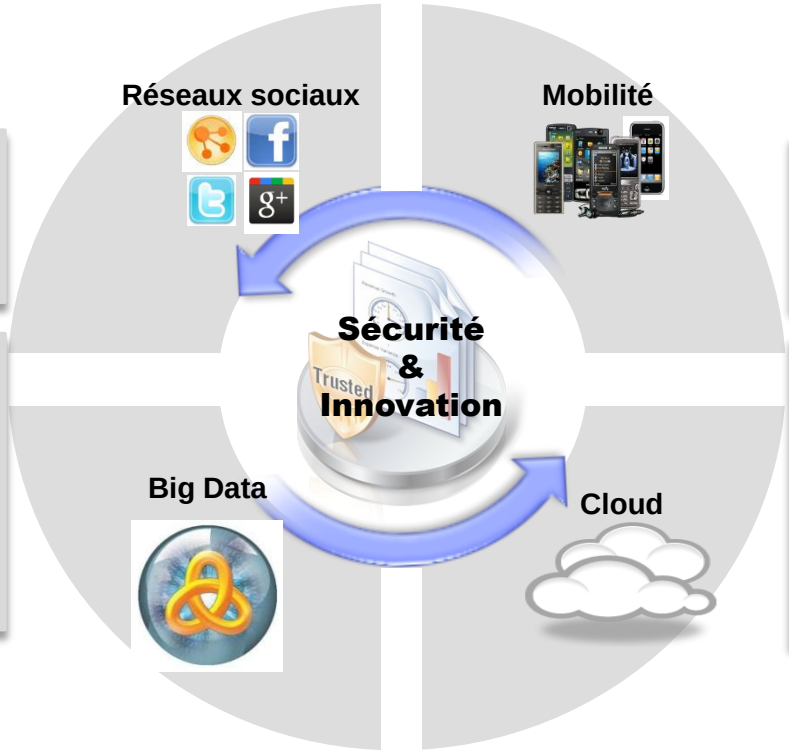


Evolution des menaces :
Les nouveaux challenges de l'innovation ont un impact sur la sécurité

Menaces externes

Augmentation des attaques externes à partir de sources non traditionnelles

- Cyber-attaques
- Crime organisé
- Espionnage d'entreprise
- Attaques par un pays
- Social engineering



Menaces internes

Comportements négligents et à risques

- Erreurs d'administration
- Comportements négligents
- Failles internes
- Employés mécontents
- Pas de distinction sur les données privées et sensibles

Conformité

Besoin croissant pour adresser de nombreuses contraintes

- Réglementations nationales
- Standards de l'industrie
- Contraintes locales

Quatre évolutions qui modifient l'écosystème

Innovation Technologique

Menaces Extrêmes

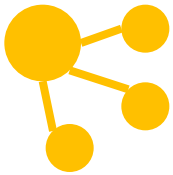
Nouvelle Approche

Nouveaux Outils

L'innovation technologique apporte le changement

1 trillion d'objets connectés

1 billion de "Travailleurs Mobiles"



Social business

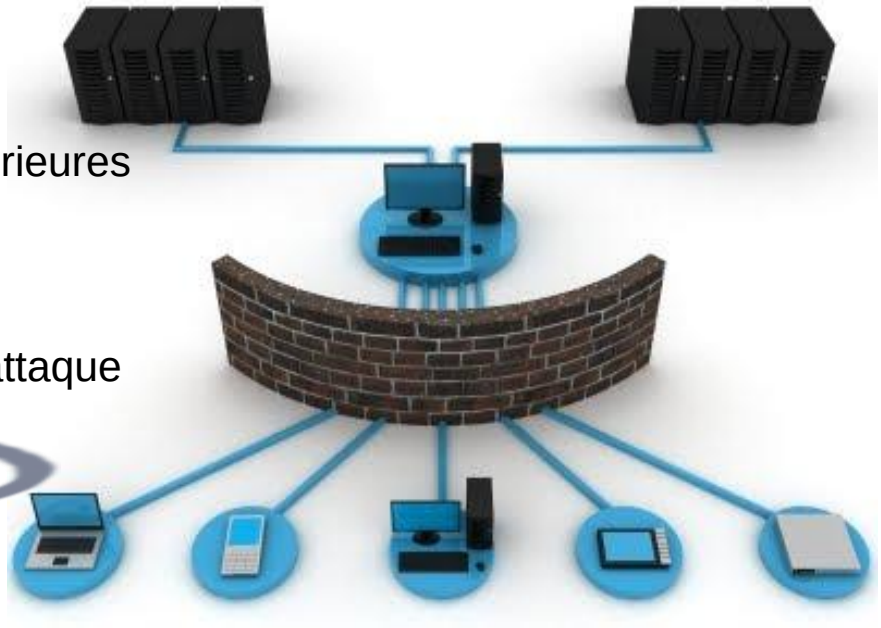
Bring your own IT

Cloud et virtualisation

Jouer la défense…

L’approche traditionnelle de la sécurité repose sur une mentalité défensive

- Suppose un périmètre organisationnel explicite
- Optimisée pour la lutte contre les menaces extérieures
- Une normalisation pour atténuer les risques
- Une prise de conscience des méthodologies d'attaque
- Nécessite une surveillance/un contrôle des flux



Origines de la sécurité Intelligente

Couches de défense essentielles pour une bonne hygiène de sécurité et contre les menaces traditionnelles …***mais les attaquants s’adaptent***

Des attaquants bien organisés et des utilisateurs malveillants sont les clefs pour contourner les défenses de sécurité

Infiltrer un partenaire de confiance et charger un malware sur l'infrastructure cible

Création d'un logiciel malveillant adapté pour infecter une cible particulière et de ce fait ne pouvant pas être détecter les solutions de sécurité du marché

Utilisation des réseau sociaux et de l'ingénierie sociale pour effectuer la reconnaissance des cibles pour hameçonnage dans le but de compromettre les comptes et les serveurs

Exploitation des vulnérabilités zero-day pour permettre un accès aux données, applications, systèmes et terminaux

Communiquer sur les ports autorisés tel que le port 80 pour exfiltrer les données de l'entreprise

Nouvelles motivations et sophistication

- Crime organisé
- Espionnage and Activisme
- Nations et Etats

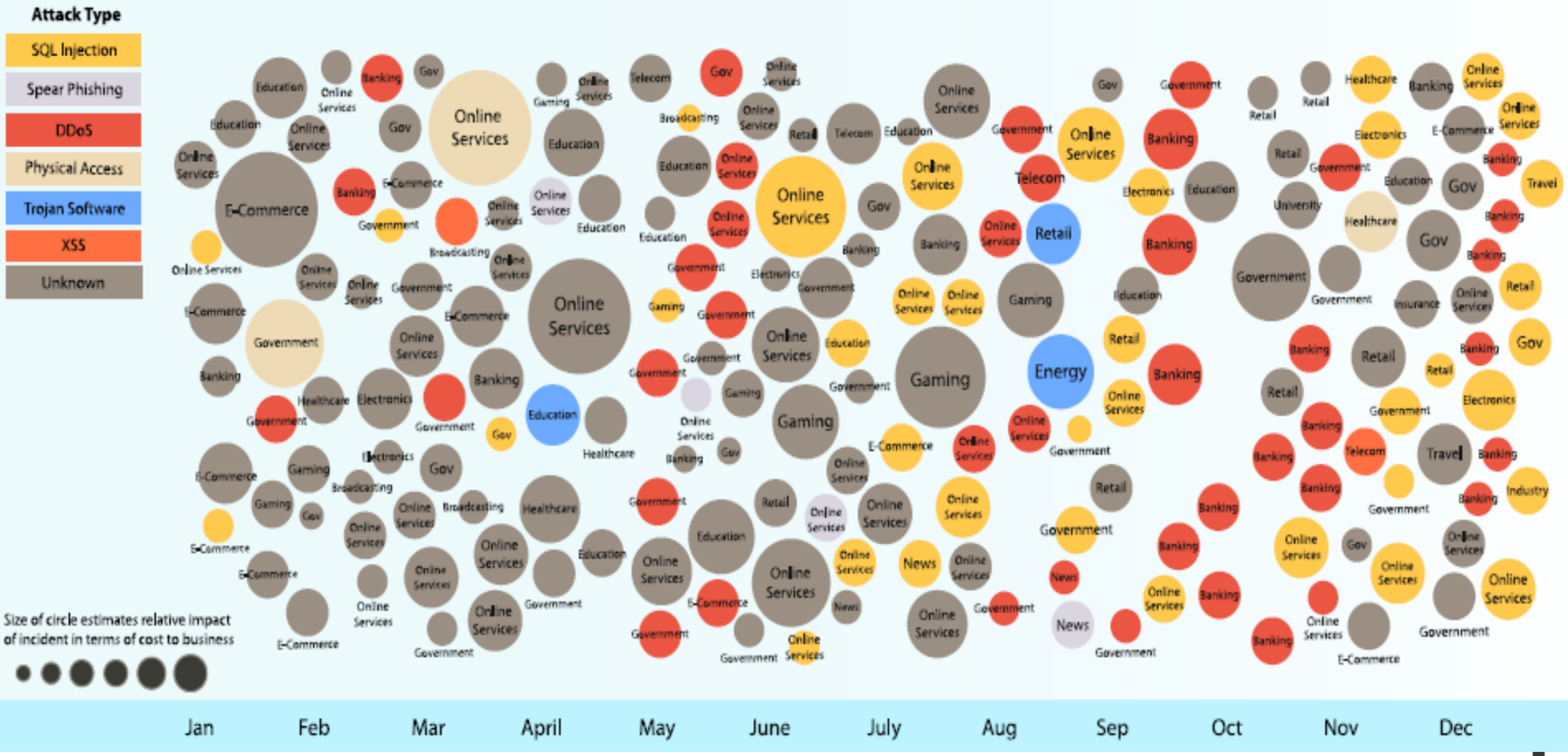
Designer Malware

Backdoors

Spear Phishing

Persistence

Personne n'est à l'abri, il n'y a aucun signe de ralentissement.



Source: IBM X-Force® Research 2012 Trend and Risk Report

Comment adresser cette problématique ?

IBM Security Systems,
la réponse à vos problématiques de sécurité

IBM Security Systems

- Un modèle de sécurité unique basé sur COBIT et les standards ISO
- $1.8B d'investissement dans l'innovation technologique
- Plus de 6000 consultants et ingénieurs en sécurité
- Plus grande bibliothèque de vulnérabilités recensées
- Laboratoire de recherche X-Force® mondialement reconnu
- Reconnaissance en tant que leader sur le marché de la sécurité par les analystes

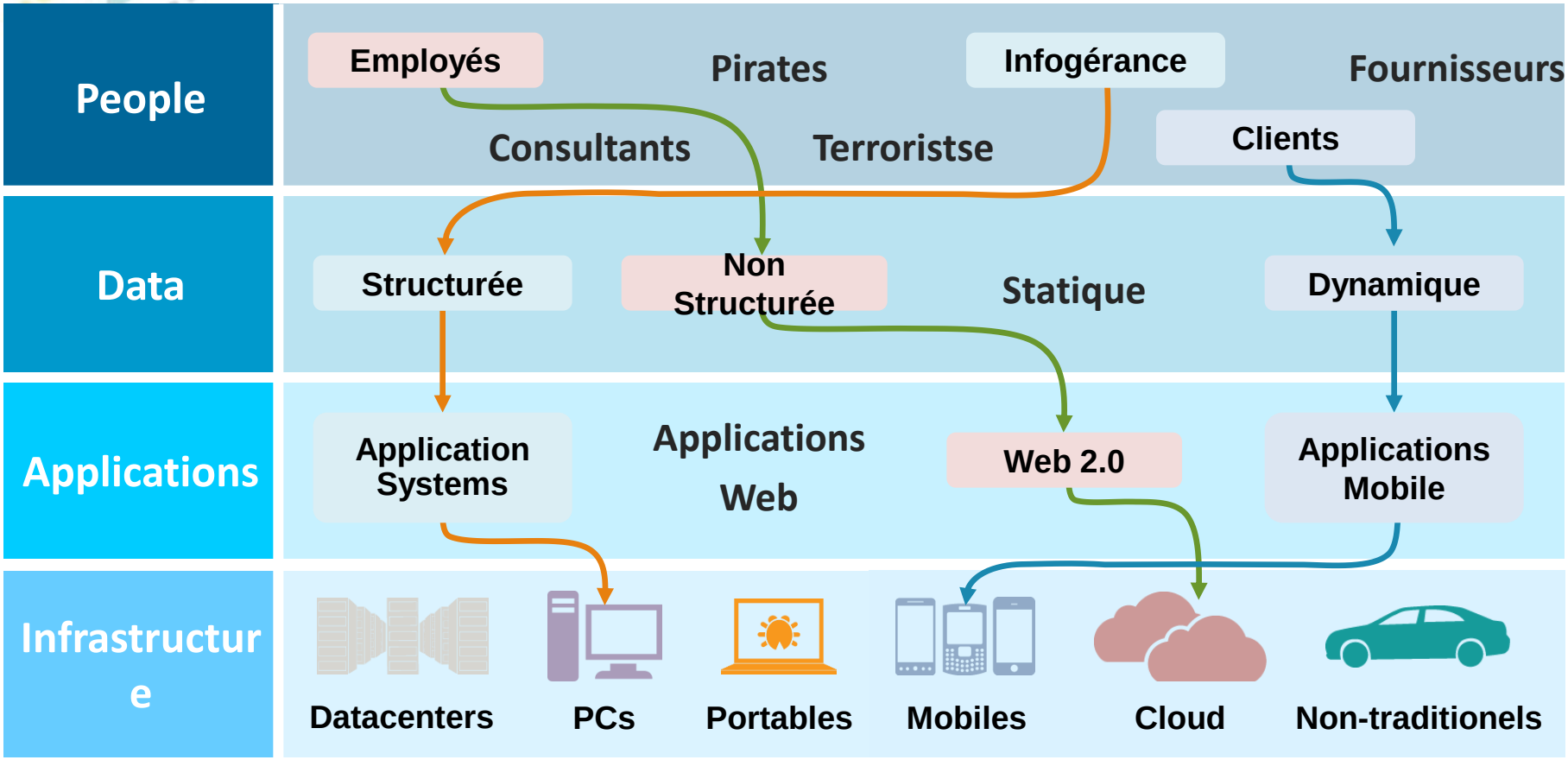
New : Trusteer an IBM Company

Vos équipes de sécurité voient du bruit

L'accent a été mis sur la sécurité des infrastructures...

Infrastructure	Datacenters	PCs	Portables	Mobiles	Cloud	Non-traditionels

L'accent a été mis sur la sécurité des infrastructures...



Mais la problématique de sécurité est complexe, Un casse-tête à quatre dimensions

People

Aujourd'hui : **Administration**

- Gestion des identités
- Contrôle des coûts

Demain : **Perspicacité**

- Identifier et gérer les utilisateurs à risque élevé
- Connaitre qui a accès aux données et aux systèmes sensibles
- Gestion des comportements
- Prioriser les identités privilégiées

Surveiller tout !!!

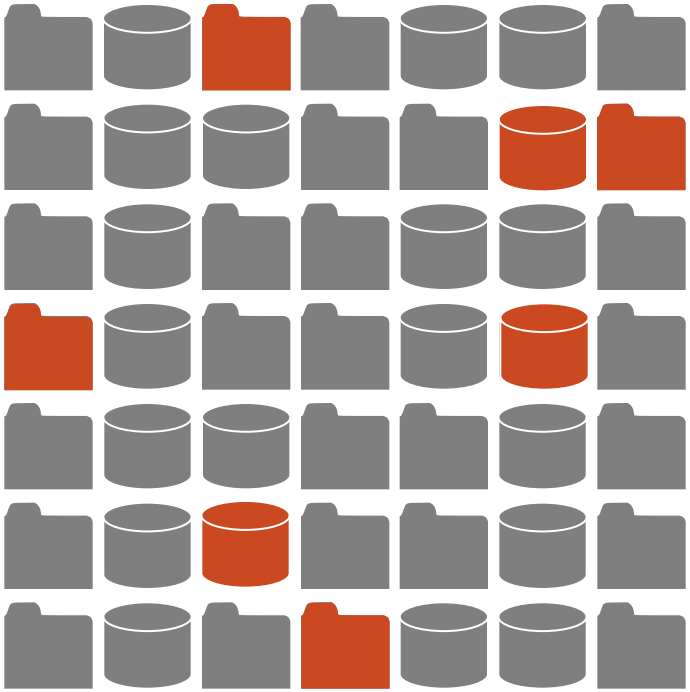
Data

Aujourd'hui : Contrôle basique

- Des contrôles d'accès simples et le chiffrement

Demain : Focus précis

- Découvrir et protéger les données sensibles
- Comprendre qui a accès aux données, à quel moment de la journée, d'où, et avec quel rôle
- Gestion des comportements



Surveiller tout !!!

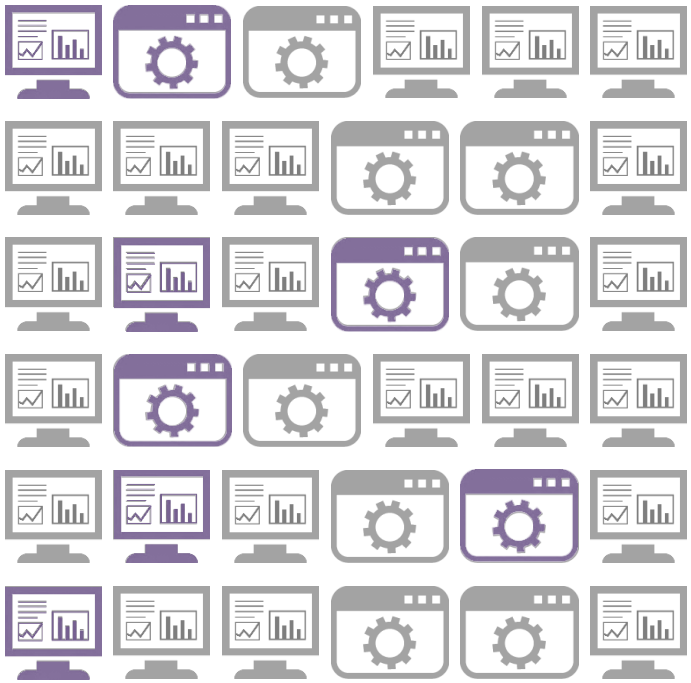
Applications

Aujourd'hui : **Adaptée**

- Vérification périodique des applications Web

Demain : **Intégrée**

- Durcissement des applications qui ont accès à des données sensibles
- Vérification du code source et des applications en temps réel
- Comportement des applications et alerte



Surveiller tout !!!

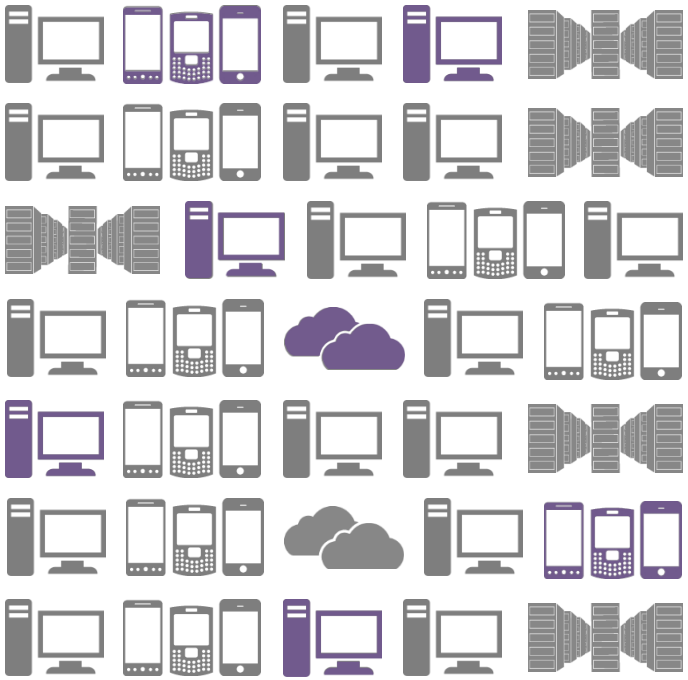
Infrastructure

Aujourd'hui : Périmétrique

- Pare-feu, correctif manuel et antivirus
- Focus sécurité périmétrique

Demain : Réfléchie

- Comportement système et réseau
- Analyser les menaces inconnues en utilisant une technologie heuristique avancée
- Étendre la couverture dans les environnements Cloud et Mobiles



Surveiller tout !!!


People
Data
Applications
Infrastructure
Advanced Security
and Threat Research

Recherche avancée

Domain	IP Address	File Checksum
dogpile.com	**117.0.178.252**	c69d172078b439545dfff28f3d3aacc1
kewww.com.cn	83.14.12.218	**51e65e6c798b03452ef7ae3d03343d8f**
ynnsuue.com	94.23.71.55	**6bb6b9ce713a00d3773cfcecef515e02**

Surveiller tout !!!

Aujourd'hui : Réaction

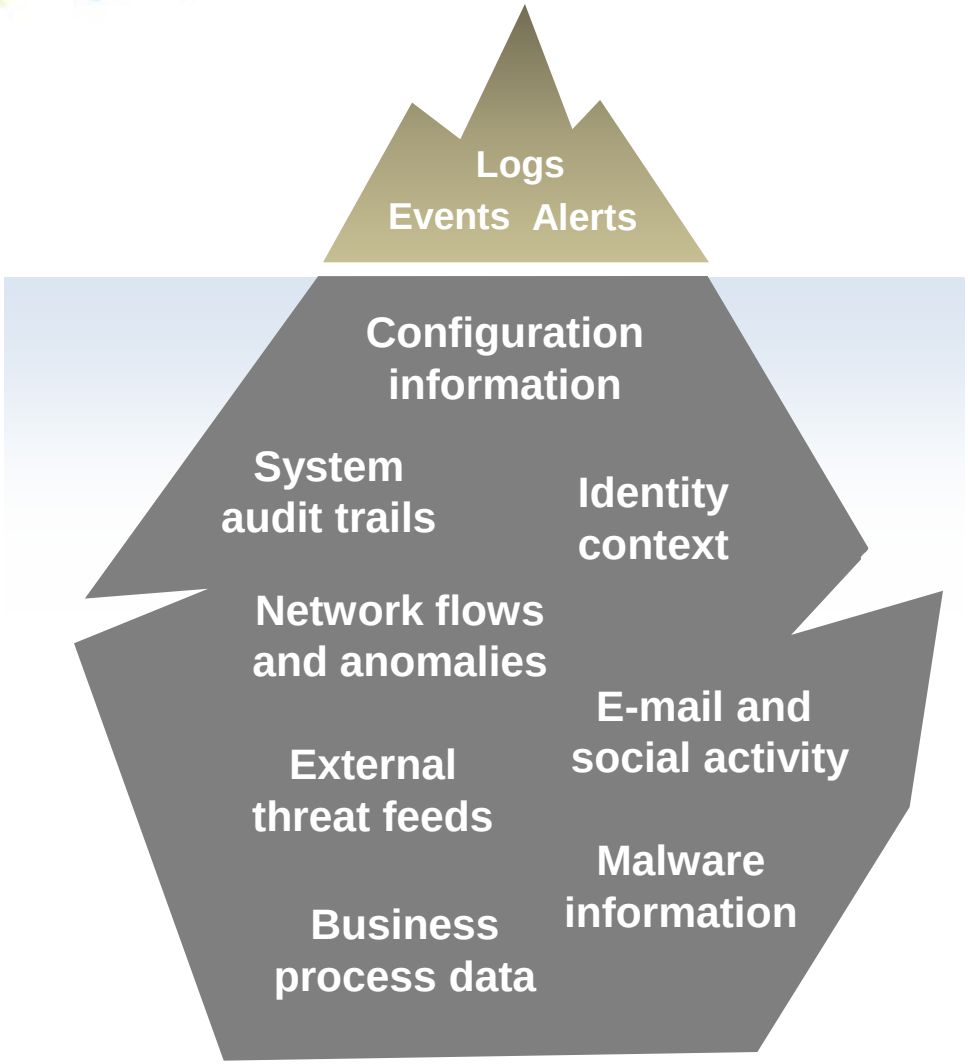
- Consulter les blogs et les informations sur les dernières menaces
- Travailler sur les signatures connues

Demain : Connaissance

- Utiliser en temps réel les renseignements sur les dernières menaces
- Corréler les alertes sur les comportements et sur la réputation
- Bloquer pro-activement les domaines, les adresses IP et les logiciels malveillants


Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research

Security Intelligence



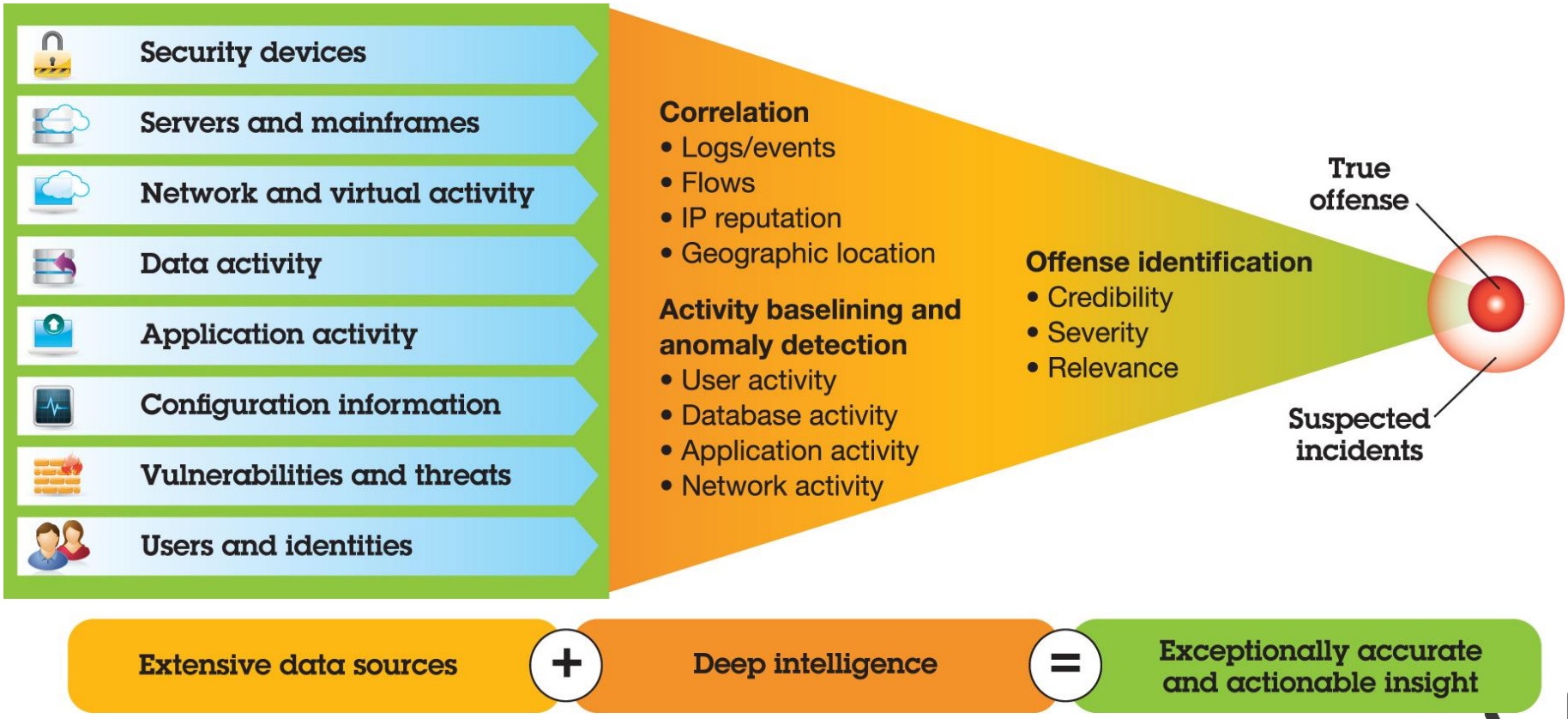
Aujourd'hui : Consolidation

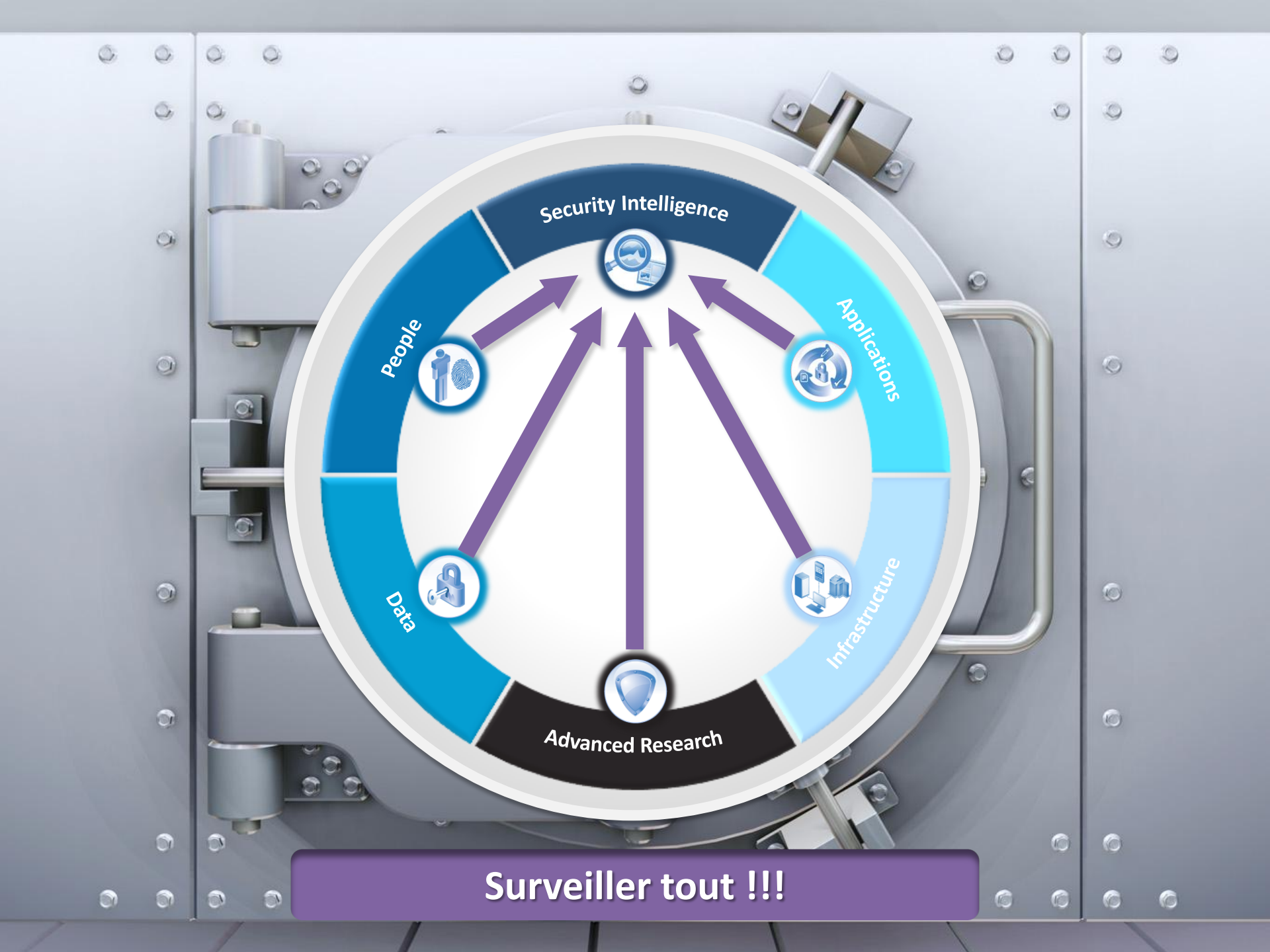
- Consolidation des journaux
- Détection basée sur les signatures

Demain : Intelligence

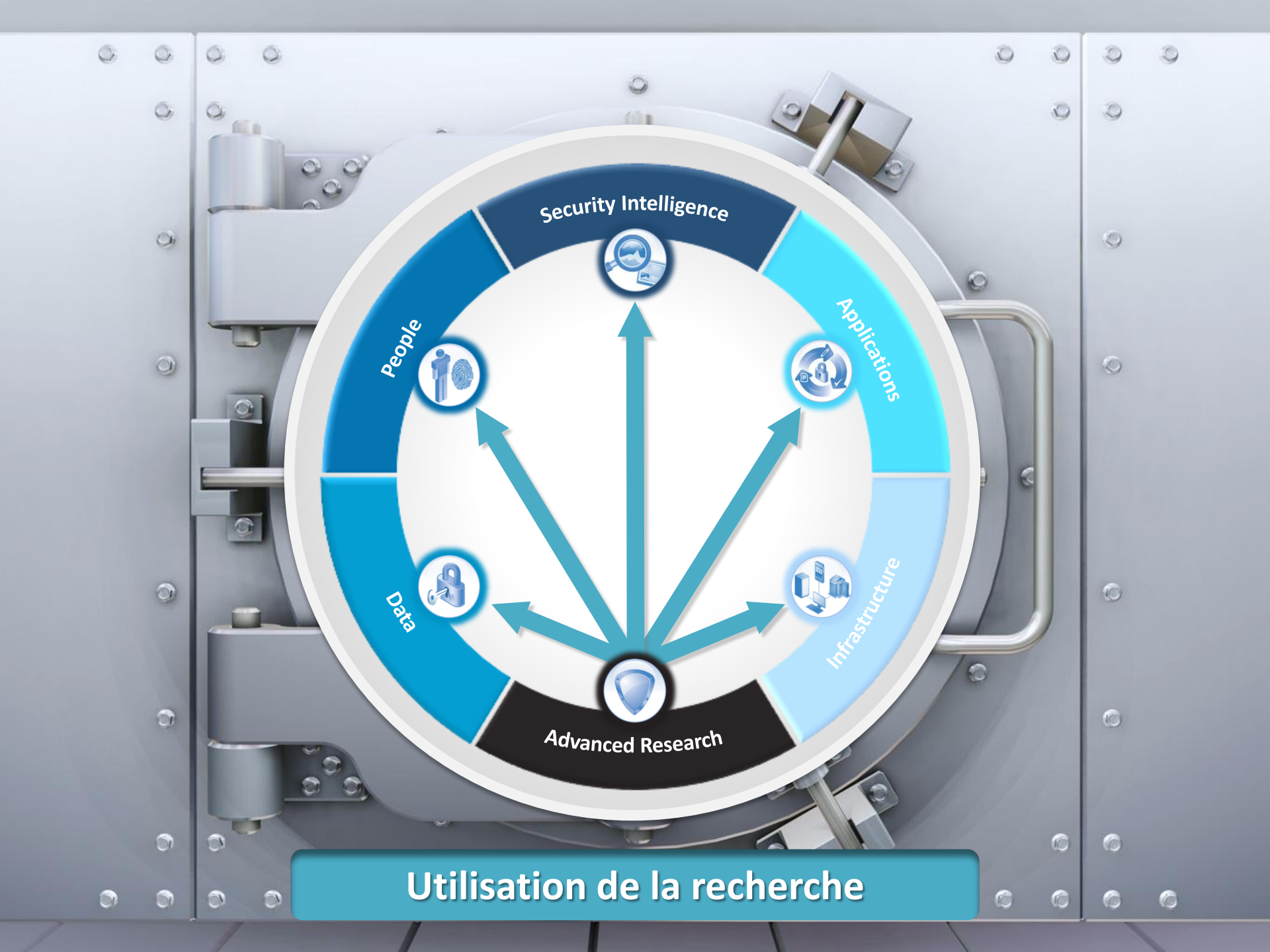
- Gestion en temps réel
- Détection d'anomalie en prenant en compte le contexte
- Analyse et corrélation automatique

Security Intelligence: *Détection des signaux faibles sur les événements et les informations de sécurité*

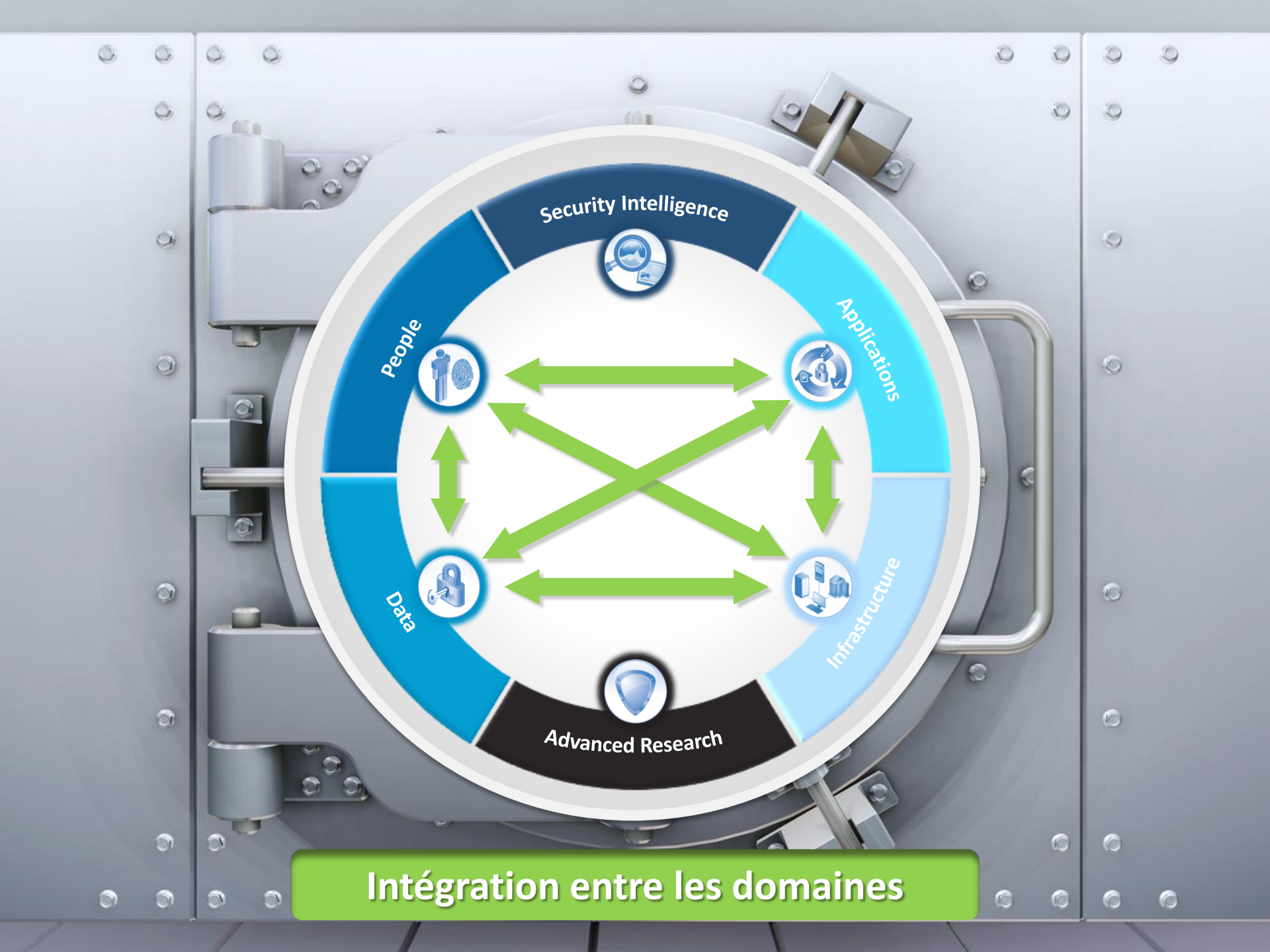




Surveiller tout !!!



Utilisation de la recherche



Intégration entre les domaines

Demain vos équipes de sécurité pourront voir…

Avec clarté…

Avec perspicacité…

Et cela n’importe où…

Nos prochains rendez-vous

ibm.com/pulse

#ibmpulse

Pulse 2014
BP Sponsorship

- DIAMOND
- PLATINUM
- GOLD
- SILVER
- EXHIBITORS

IBM Business Partner Awards
2013
Tivoli Software

Security Intelligence. Think Integrated.

@IBMSecurityFR

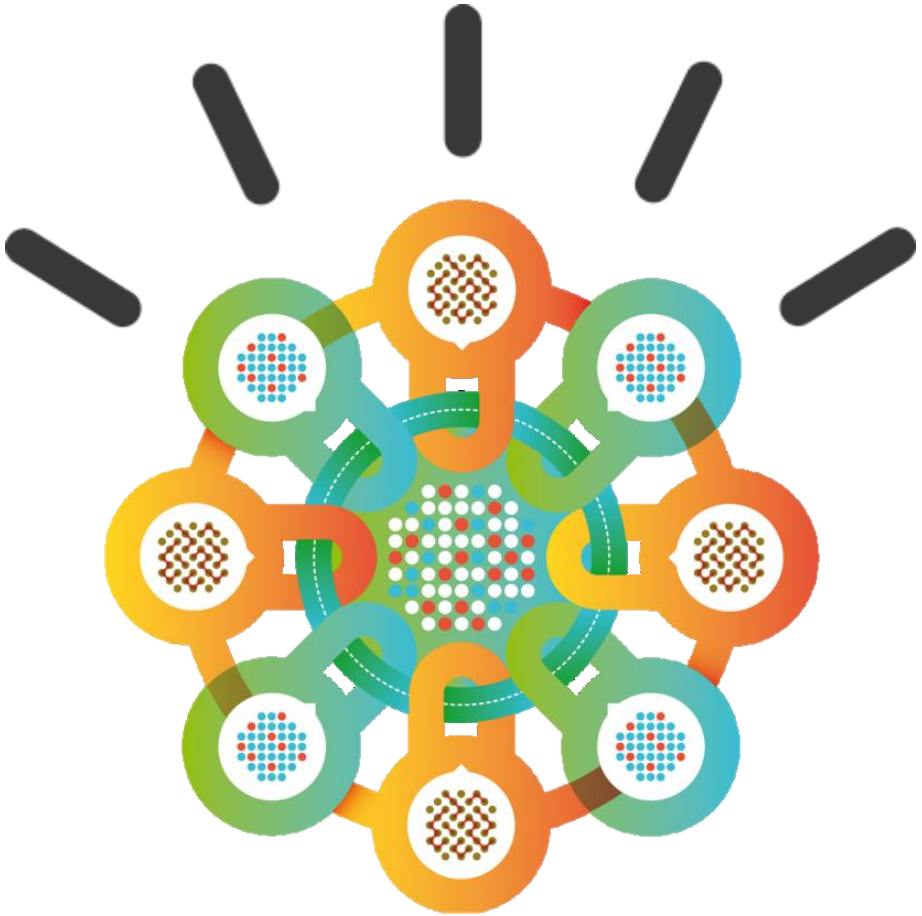
www.ibm.com/security/fr

www.lasecuriteintelligente.fr

www.lemondeinformatique.fr

select Parner Zone / Sécurité

www.ibm.com/partnerworld/security

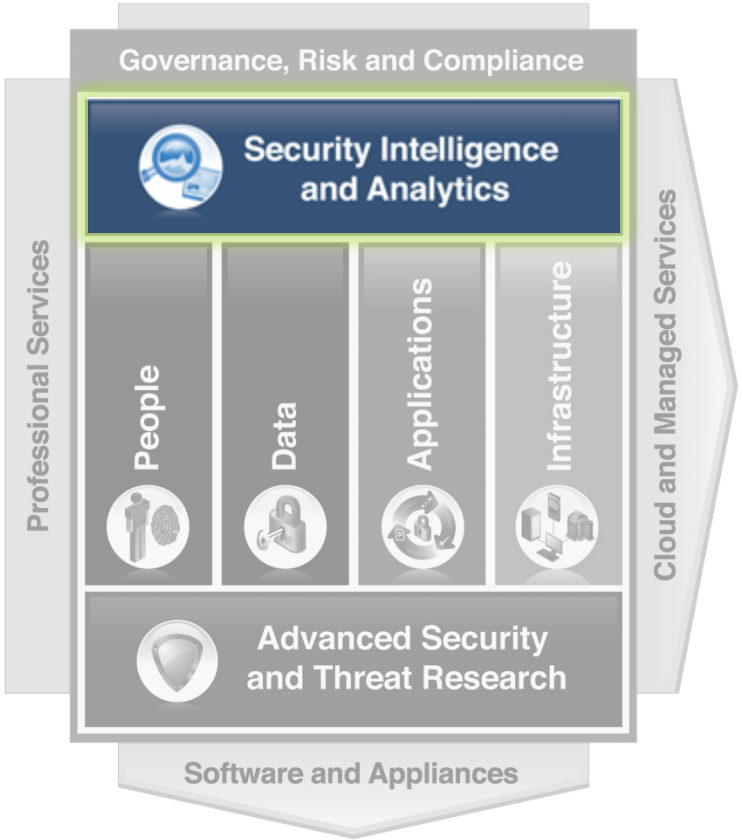


Security Intelligence

Security Intelligence

Domaine

Gouvernance et pilotage de la sécurité



Solutions

QRadar SIEM

- Gestion des signaux faibles
- Analyse des flux réseaux et des activités utilisateurs
- Gestion des menaces et des fraudes

QRadar Risk Manager

- Modélisation et simulation prédictive des menaces
- Surveillance de l'évolution des configuration et audit
- Analyse des menaces et des impacts

QRadar Log Manager

- Gestion des journaux clef en main
- Evolutif vers la solution SIEM

IBM Identity and Access Management: *Gouvernance*

Thèmes

Standardisation IAM et gestion de la conformité

Approche verticale pour fournir des renseignements d'identité et d'accès à l'entreprise. Approche

Sécurité Cloud, Mobilité, Réseau social

Améliorer le contrôle d'accès dans les nouvelles technologies, ainsi que dans le mode SaaS

Gouvernance IAM et menaces internes

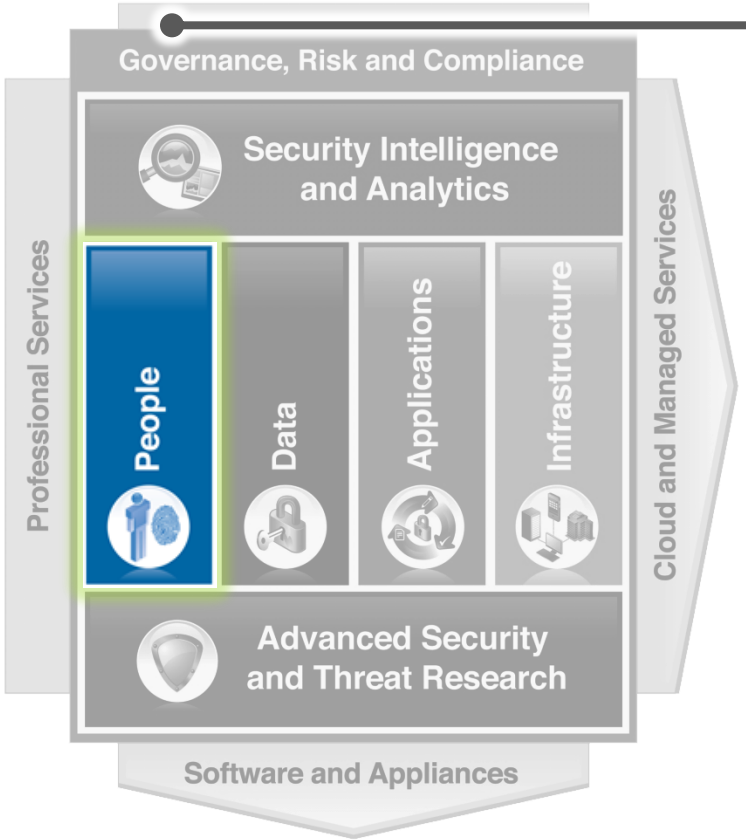
Gestion des comptes à privilège et gestion des accès basés sur la notion de rôle

People

People

Domaine

Gérer et étendre le contexte d'identité à l'ensemble de l'entreprise avec une approche gouvernance de l'identité



Solutions

IBM Security Identity Manager

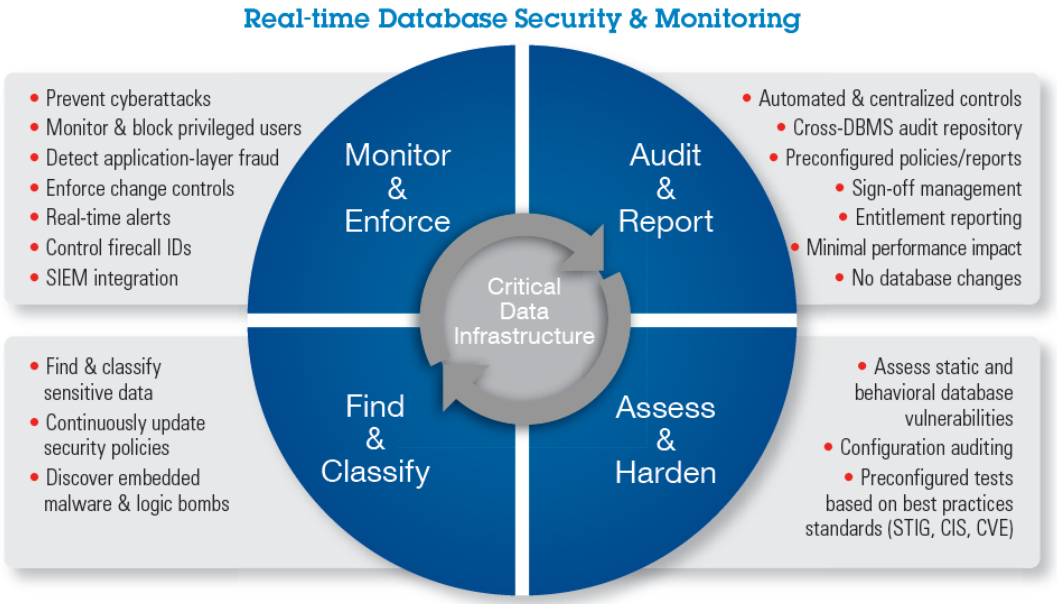
- Automatisation de la création, de la modification et de la résiliation des comptes d'utilisateurs à travers un cycle de vie complet de l'identité
- Contrôle d'identité, y compris la gestion des rôles et de l'audit

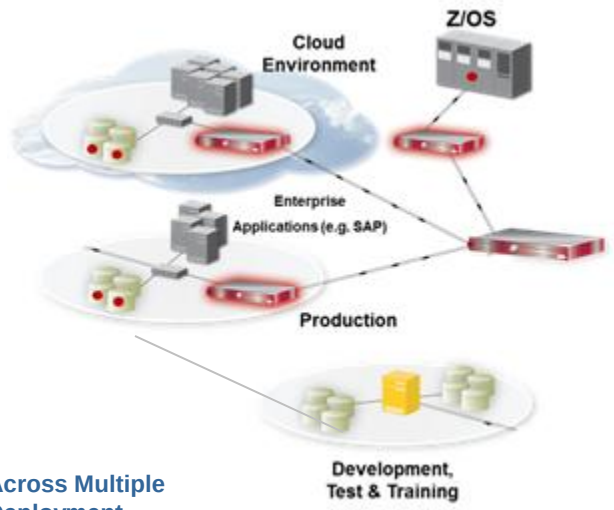
IBM Security Access Manager Family

- Automatise l'ouverture de session et d'authentification pour les applications Web d'entreprise et des Web services
- Gestion des droits d'accès fin aux applications

IBM Security zSecure suite

Data Security: *Gouvernance*





Across Multiple Deployment Models

Thèmes

Réduction du Total Cost of Ownership

Prise en charge des bases de données et des données non structurées. Automatisation, manipulation et analyse de grand volume de données

Gestion avancée de la conformité

Amélioration des services Vulnerability Assessment (VA) et Database Protection Subscription Service (DPS) avec une fréquence mise à jour améliorée, la prise en compte

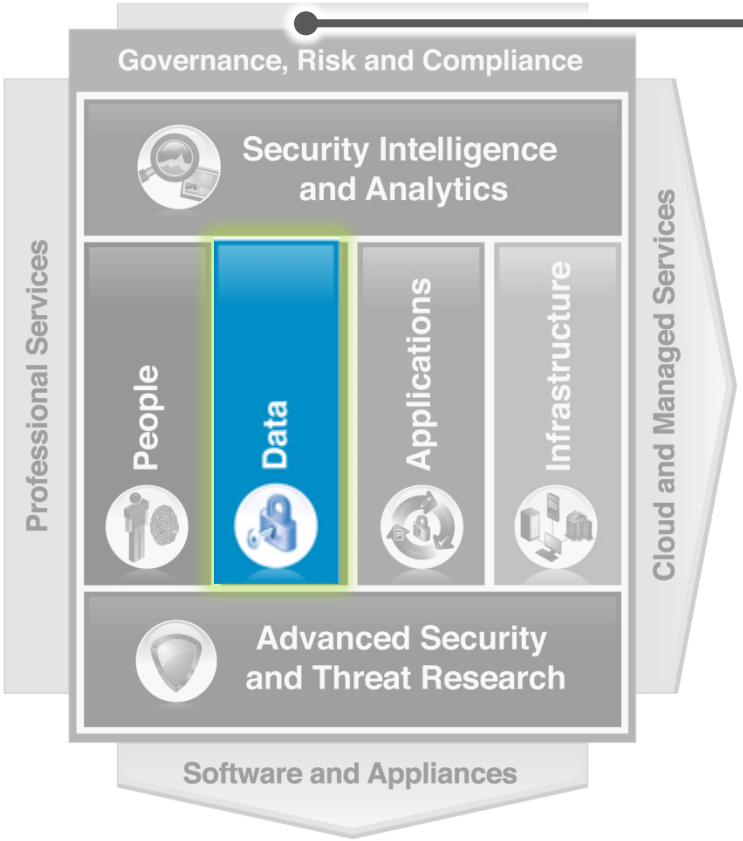
Protection dynamique des données

Capacité de masquer le contenu des bases (au niveau de la ligne, au niveau du rôle) et pour les applications (au niveau du modèle, au niveau de la forme) dans le but de protéger

Data

Domaine

Des solutions de sécurité pour protéger les données sensibles de l'entreprise

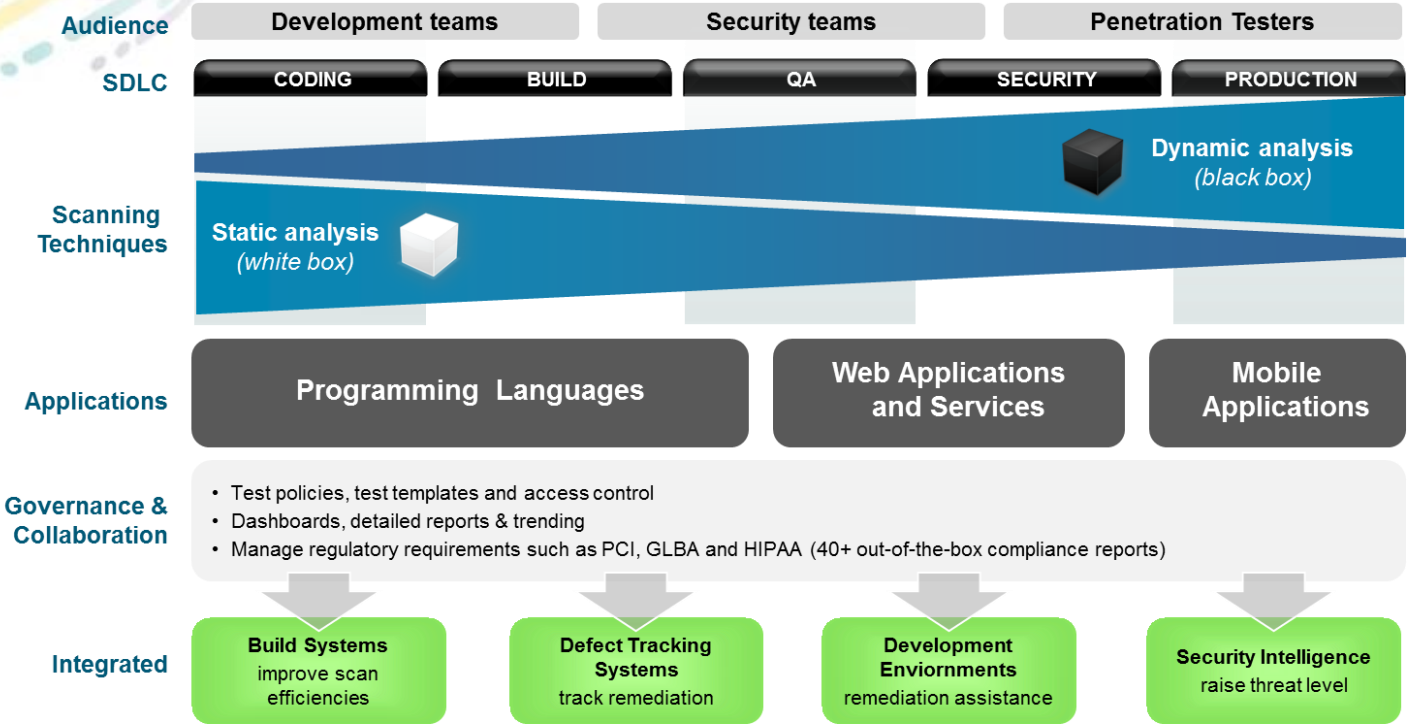


Portfolio Overview

IBM InfoSphere Guardium Product Family

- Database Activity Monitoring : gestion et blocage des accès non autorisés
- Privileged User Monitoring : Détecter et bloquer les accès frauduleux ou inappropriés des administrateurs, développeurs ou info géreurs
- Prevent Database Leaks : Détecter ou protéger les tentatives de fuite des données
- Database Vulnerability Assessment : Analyser les bases de données pour détecter les vulnérabilités
- Audit and document compliance : Simplifier les processus de certification SOX, PCI-DSS, avec des rapport préconfigurés

Application Security : *Gouvernance*



Thèmes

Couverture pour les applications mobiles et les nouvelles menaces

Continuer à identifier et à réduire les risques en élargissant les capacités d'analyse sur les nouvelles

Interfaces simplifiées

De nouvelles fonctionnalités pour améliorer le temps passé sur l'analyse avec de nouveaux modéles statistiques et des facilités d'utilisation

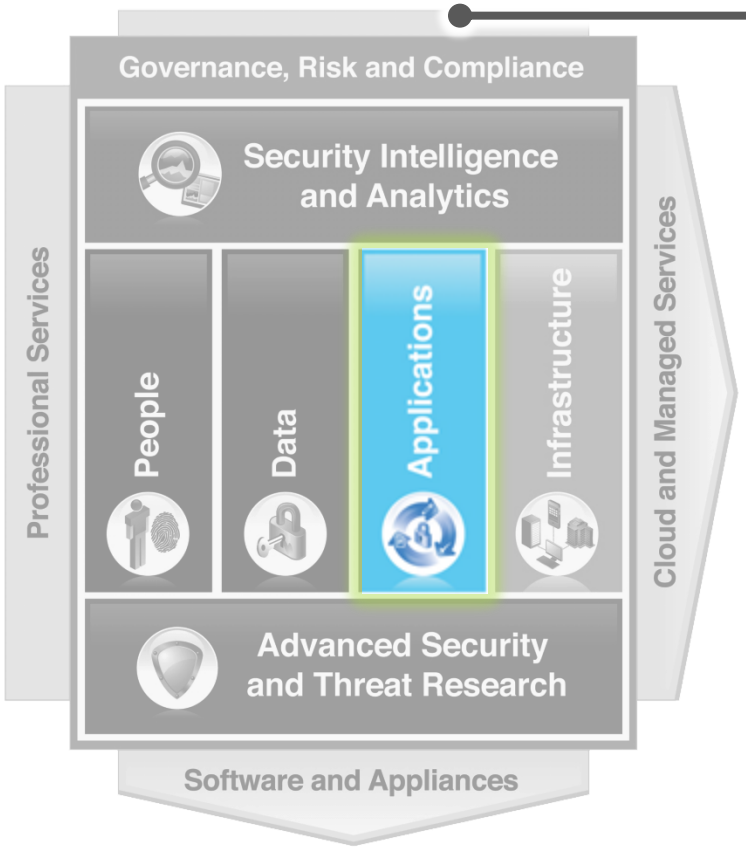
Intégration gouvernance de la sécurité

Ajuster automatiquement les niveaux des menaces en se basant sur la connaissance des vulnérabilités des applications. Intégration et analyse des

Applications

Domaine

Permettre de développer des applications sécursées à moindre coût



Solutions

AppScan Enterprise Edition

•Approche globale par une gouvernance de la sécurité des applications dans son ensemble (collaboration au niveau de l'entreprise)

•Solution multi-utilisateur fournissant des analyses et des rapports centralisés

AppScan Standard Edition

•Solution "poste de travail", permettant une analyse automatisée des applications Web. A destination des auditeurs et lors des tests de pénétration.

AppScan Source Edition

• Solution permettant l'analyse du code

Threat Protection : *Gouvernance*

Security Intelligence Platform

- Log Manager
- SIEM
- Network Activity Monitor
- Risk Manager
- Future

Threat Intelligence and Research

- Vulnerability Data
- Malicious Websites
- Malware Information
- IP Reputation

Advanced Threat Protection Platform

- Intrusion Prevention
- Content and Data Security
- Web Application Protection
- Network Anomaly Detection
- Future

IBM Network Security

Plateforme gestion des APTs (Advanced Persistent Threats)

Permet de prévenir des attaques avancés et des événements anormaux sur le réseau. Corrélation des journaux de sécurité avec des événements en temps sur le

Support du laboratoire de recherche IBM X-Force

Augmenter la couverture de nos solutions par l'intégration des informations issues de la base de connaissance du laboratoire IBM

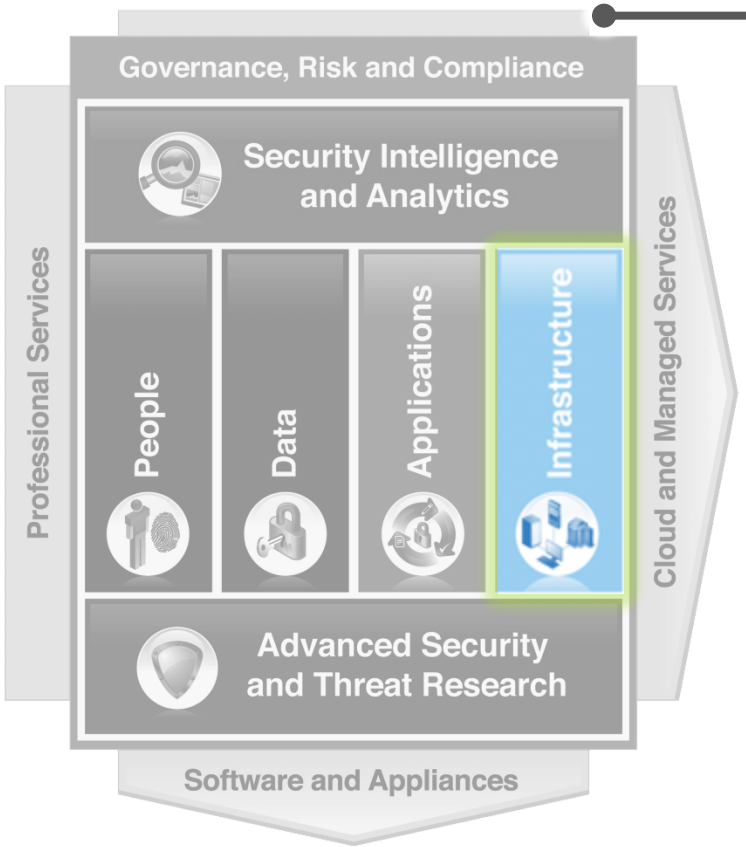
Intégration gouvernance de la sécurité

Détection des signaux faibles de sécurité par une intégration forte entre les différentes composants de la solution

Infrastructure (réseau)

Domaine

Protection contre les attaques sophistiquées par la mise en place d'une plateforme contre les nouvelles menaces



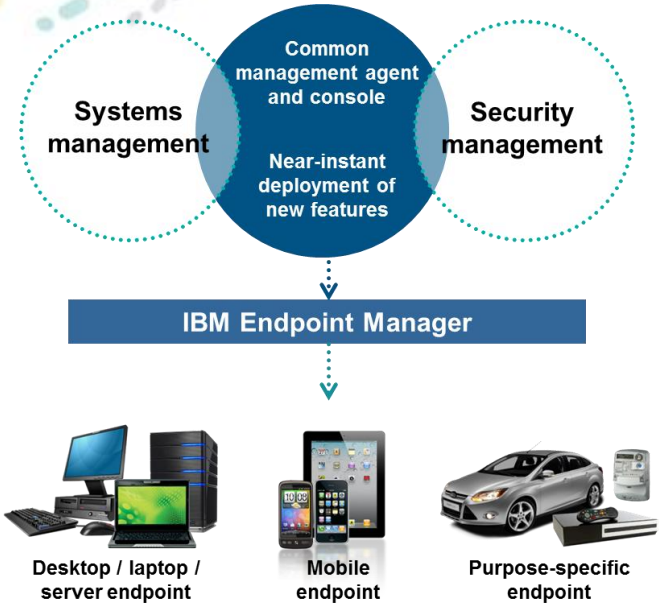
Solution

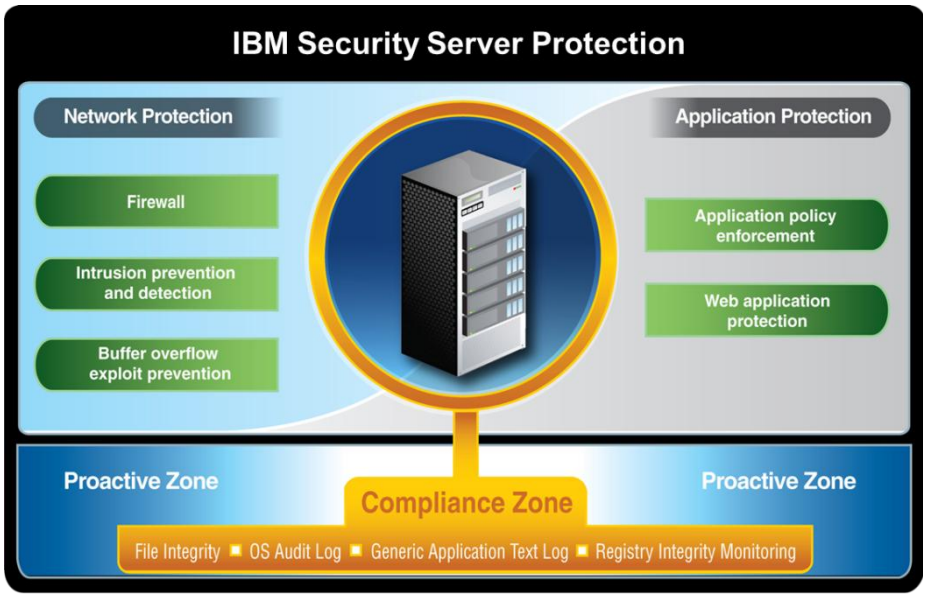
IBM Security Network Intrusion Prevention (IPS)

- Délivre une protection et une prévention contre les nouveaux types d'attaque
- Protection pro-active avec la mise en place de la technologie IBM Virtual Patch®
- Délivre une protection contre les menaces classiques sur les applications WEB (SQL Injection, Cross-site Scripting)
- Intégration de l'approche Data Loss Prevention (DLP)
- Délivre des informations sur les anomlies sur le réseau pour une analyse prédictive des menaces
- Délivre une protection avancée en s'appuyant sur le service IBM X-Force Research

Infrastructure Protection – Endpoint and Server :

Gouvernance





Thèmes

Sécurité pour terminaux mobiles

Solution de sécurité pour la gestion des terminaux mobiles : Apple iOS, Google Android, Symbian, et Microsoft Windows Phone – au travers d'une seule infrastructure

Couverture sécurité

Couverture de la sécurité à l'ensemble du système d'information (application, infrastructure, système d'exploitation)

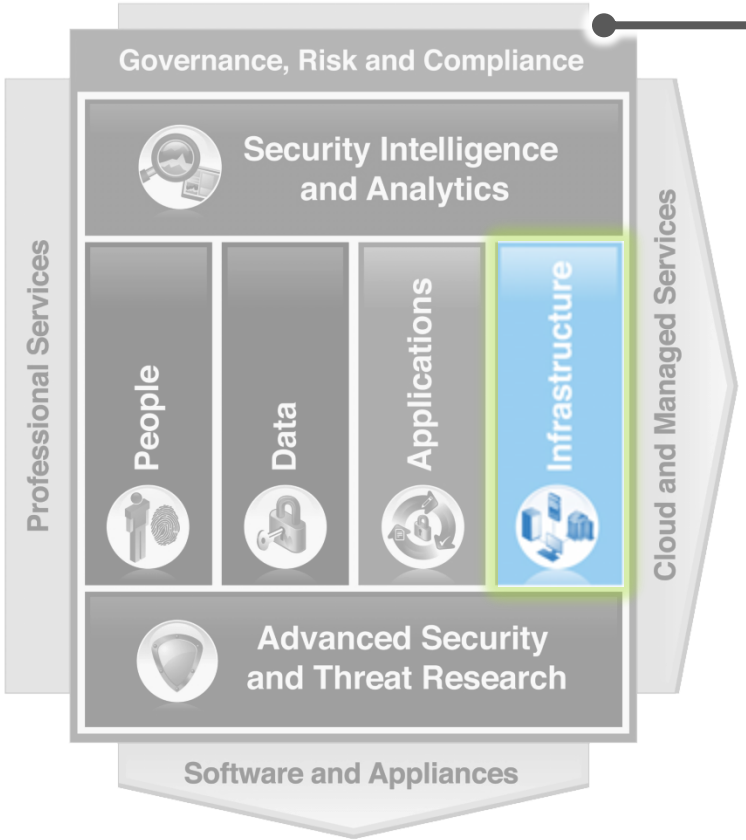
Intégration gouvernance de la sécurité

Meilleure utilisation des outils d'analyse, fournir des informations précieuses pour répondre à la conformité et objectifs de sécurité informatique, ainsi que

Infrastructure (terminaux et serveurs)

Domaine

Délivrer un service de sécurité pour l'ensemble des terminaux et serveur du système d'information



Solutions

IBM Endpoint Manager for Security and Compliance

•Gestion de la sécurité sur l'ensemble des terminaux (poste de travail et mobile) au travers d'une seule console

IBM Endpoint Manager for Core Protection

•Protection en temps réel contre les différentes menaces

IBM Endpoint Manager for Mobile Devices

• Gestion de la sécurité et de la configuration des terminaux mobiles : iOS, Android, Symbian, and Microsoft devices

IBM Security Server Protection

•Protection en temps réel contre les différentes menaces sur un grand nombre de système

Atelier : Analyse de la maturité sécurité
Enterprise IT Security Maturity Workshop (ESMW)

- ✓ L'atelier IBM ESMW permet d'analyser le niveau de maturité sécurité IT :
  - ➢ Atelier d'un jour pour adresser la sécurité globalement, approcl haut niveau
  - ➢ Résultats et recommandations confidentiels
- ✓ Bénéfices :
  - ➢ Donner les axes de travail pour améliorer l'approche sécurité
  - ➢ Outil permettant de définir le schéma directeur sécurité
  - ➢ Outil permettant de gérer le budget prévisionnel sécurité IT
- ✓ Cet atelier est gratuit(*), mais il nécessite la présence d'un sponsor CxO et d'une participation des différents acteur sécurité de l'entreprise :
  - ✓ Participation active du RSSI (sponsor)
  - ✓ Participation des différents acteurs de la sécurité

(*) Cet atelier n'a pas pour objectif de remplacer les missions d'analyse de

IBM a développé 10 approches essentielles pour la gouvernance de la sécurité

Les approches

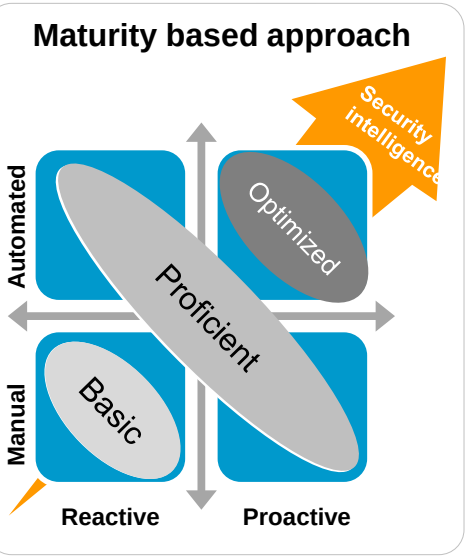
1. Développer et mettre en place une approche de gestion des risques

2. Gérer les incidents de sécurité dans un prinicipe de gouvernance

3. Protéger les environnements innovants (cloud, mobiles, réseaux sociaux)

4. Approche de la sécurité dès les phases de définitions

5. Automatiser les services de sécurité



6. Contrôler les accès au réseau et assurer la continuité des services

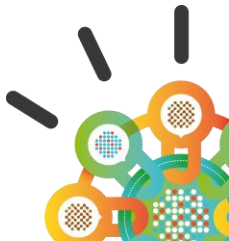
7. Gérer la complexité des environnements cloud et virtualisés

8. Gérer les contraintes réglementaires et de conformités

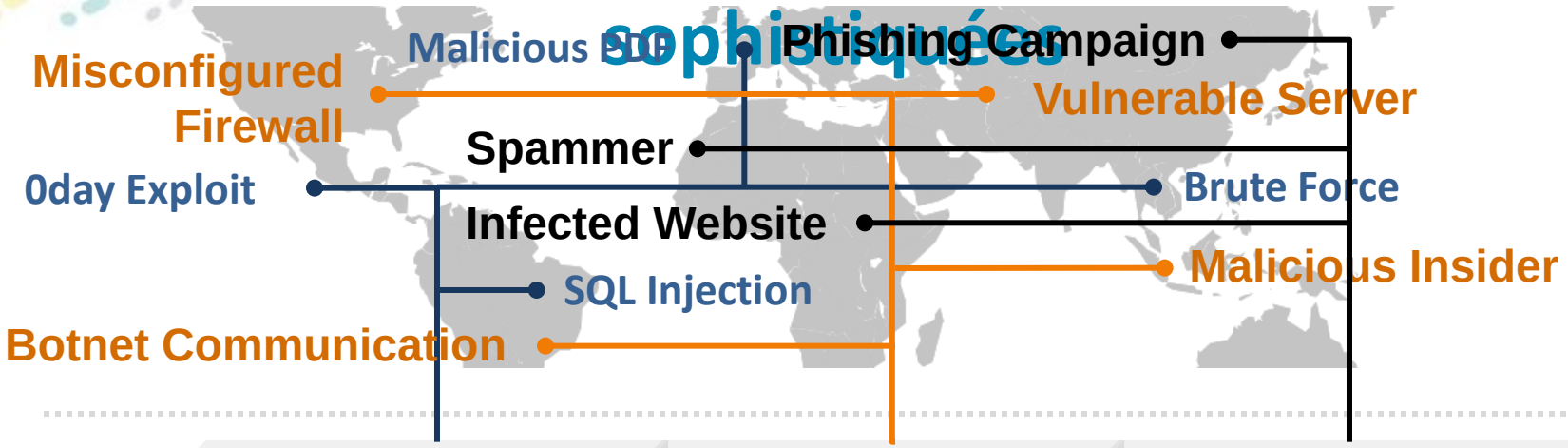
9. Protéger les données sensibles et confidentielles

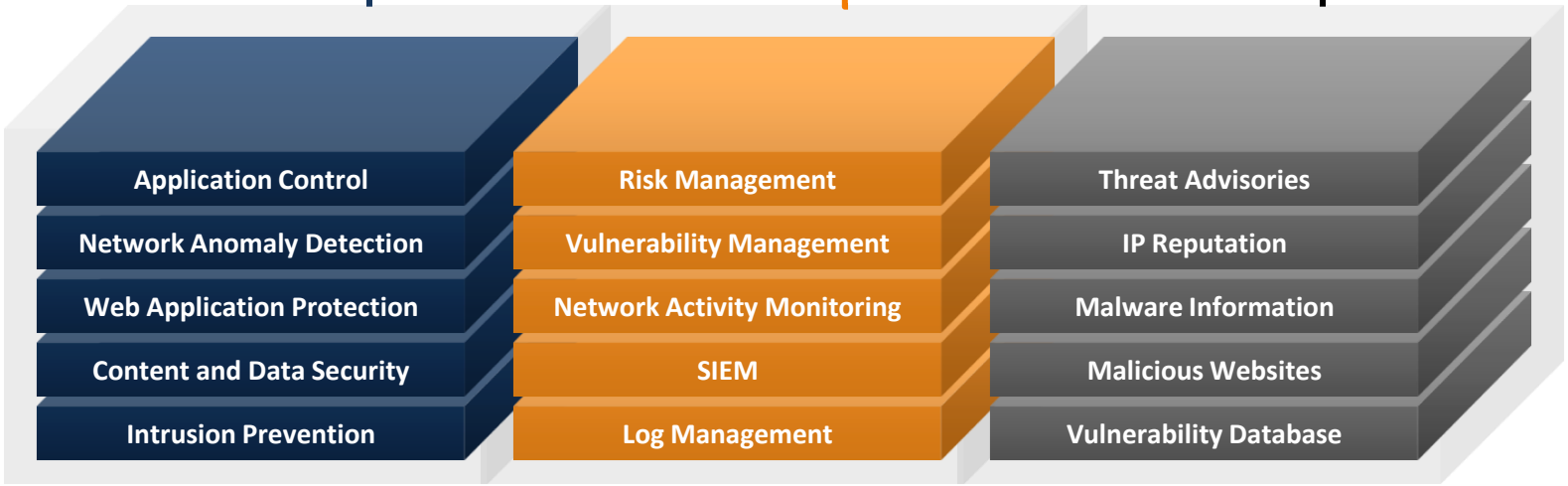
10. Gouvernance de la sécurité

Appliquer les principes…



La meilleure protection contre les attaques sophistiquées





Sur le réseau | Dans l'entreprise | Dans l'Internet

La meilleure protection contre les attaques sophistiquées

IBM Advanced Threat Protection Platform

ibm.com/security/fr

Annexes

Glossaire sur la sécurité informatique (Produits IBM)

- IM (Identity Management) : Solution de gestion centralisée du cycle de vie de l'individu dans le système d'information de l'entreprise. Cela consiste à la définition des autorisations et des droits d'accès aux applications, aux services et aux systèmes informatique.

- AM (Access Management) : Solution qui consiste à autoriser l'accès aux applications, aux services et aux systèmes informatique de l'entreprise en s'appuyant sur les autorisations et droits d'accès effectifs de l'individu. Ce type de solution nécessite la mise en place d'un mécanisme d'identification (identifiant) et d'authentification (password, certificat, token, ...) de l'individu

- FIM (Federated Identity Management) : Solution qui consiste à partager les informations d'identité concernant les individus d'une entreprise, avec une organisation partenaire qui vise à permettre l'accès à distance contrôlé et sécurisé aux ressources de ce partenaire. La fédération concrétise, pour un groupement d'organisations, l'interconnexion de leurs services d'authentification et l'utilisation d'un ensemble commun d'attributs des individus.

- SIEM (Security Information & Event Management) : Solution qui consiste à fournir une vue globale en temps réel des activités liées à la sécurité et à la conformité dans l'ensemble de l'environnement informatique.

- IPS (Intrusion Prevention System) : Solution qui consiste à assurer le contrôle du trafic réseau et générant des alertes sur des tentatives d'intrusion ou de l'existence d'un trafic suspect.

- GRC (Governance, Risk & Compliance) : Terme générique regroupant la gouvernance, la gestion des risques et la compliance qui sont de plus en plus intégrés et alignés entre eux afin d'éviter la confusion et les doublons.

Glossaire sur la sécurité informatique (Extrait)

- Authentification / identification : L'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité

- Confidentialité : propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

- Intégrité : garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime

- Disponibilité : Propriété d'un système informatique capable d'assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite.

- Contrôle d'accès : Processus par lequel les données d'authentification fournies par une personne, ou toute autre entité, pour avoir accès à un centre ou à un système informatiques, sont comparées avec des valeurs de référence définies touchant cette entité, permettant ainsi l'autorisation ou le refus de l'accès demandé, qu'il soit physique ou logique.

- Journalisation : Enregistrement dans un journal des opérations informatiques effectuées dans un système

- Vulnérabilité (Vulnerability) : Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser.