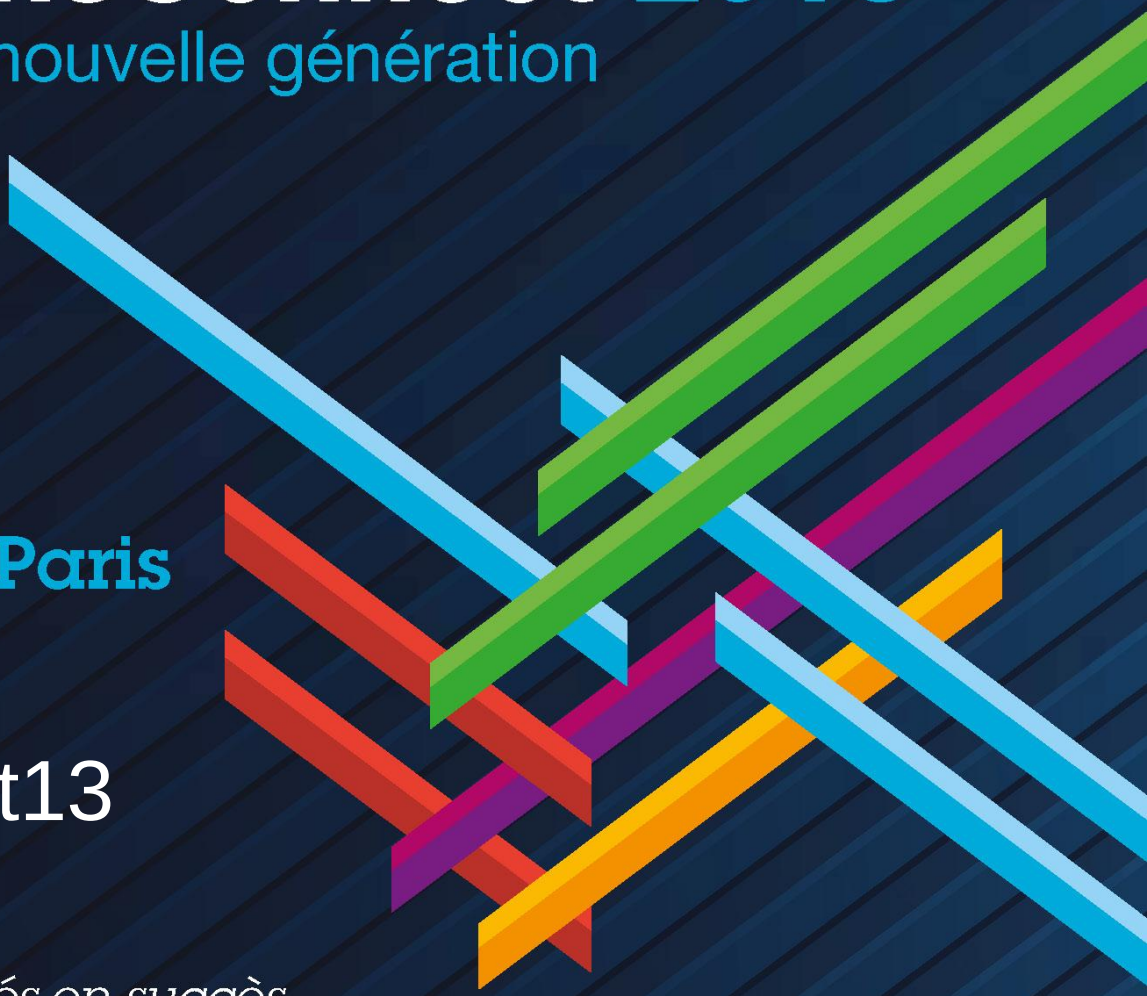
IBM SolutionsConnect 2013

L'IBM TechSoftware nouvelle génération



28, 29 et 30 août

IBM Client Center Paris

#solconnect13

Transformez vos opportunités en succès

IBM

Sec04 - BigData
Quel apport pour la cyber-sécurité ?

Serge RICHARD - CISSP®
Security Solution Architect – IBM Security Systems

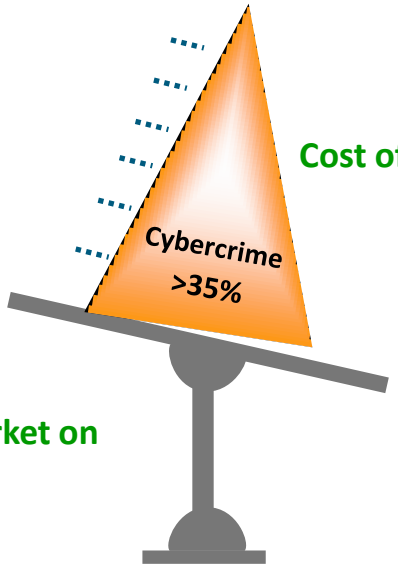
Agenda

- Un besoin réel
- Des cas d'utilisation
- Les offres logicielles IBM

Agenda

- Un besoin réel
- Des cas d'utilisation
- Les offres logicielles IBM

Bienvenue dans le monde de la Cyber Criminalité…



Cost of Global Cyber Crime

$388B

Global Black Market on Drugs

$288B

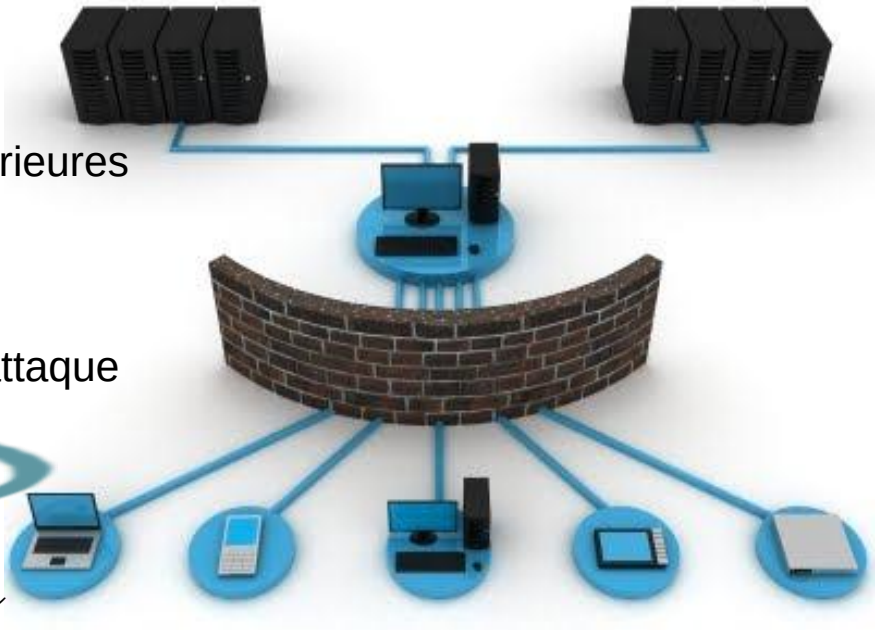
http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

"You know you can do this just as easily online."

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

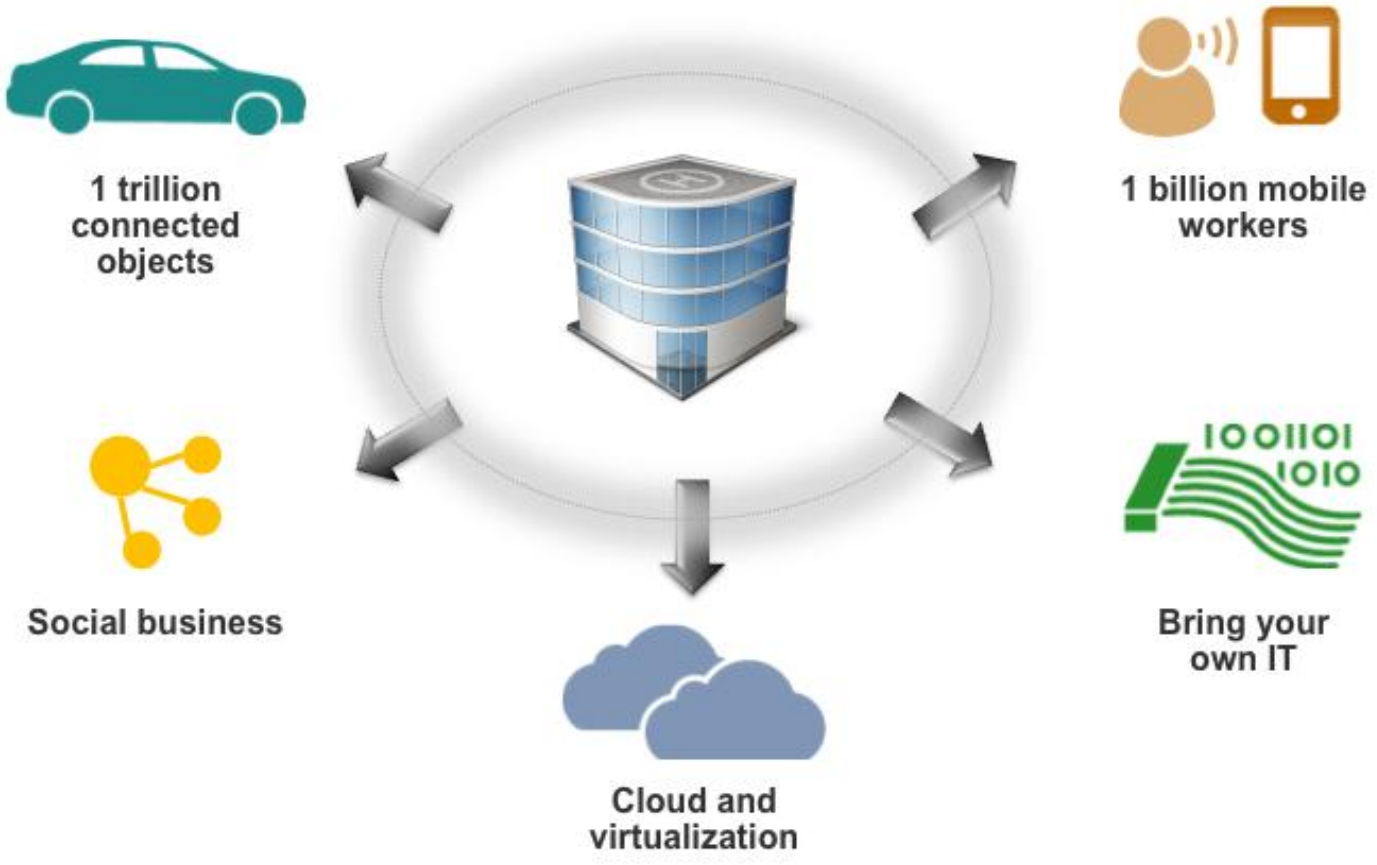


Origines de la sécurité Intelligente

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

L'écosystème change…Si ce n'est déjà fait !!!

Les entreprises sont en perpétuelles mutations



Les limites du périmètre "Cyber" deviennent floues…Comment appréhender cela ?

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

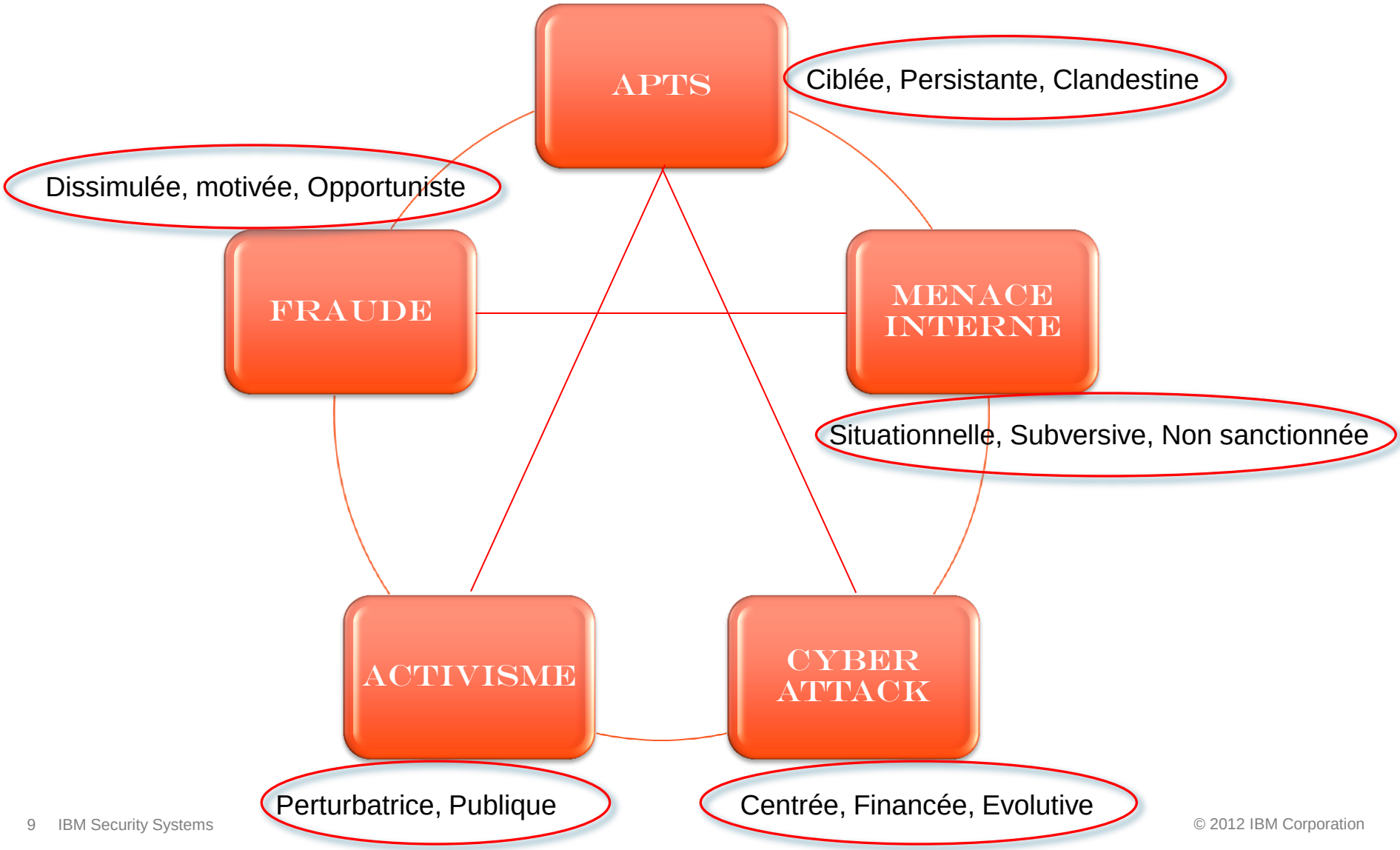
Designer Malware

Backdoors

Spear Phishing

Persistence

Paysage des menaces émergentes



Avoir une approche proactive de la sécurité

Auditer, Corriger & Bloquer

Penser comme un défenseur, Mentalité défense en profondeur

- ✓ Protéger tous les actifs
- ✓ Mettre l'accent sur le périmètre
- ✓ Mettre à jour les systèmes
- ✓ Utiliser une détection basée sur les signatures
- ✓ Analyser les terminaux
- ✓ S'informer sur les blogs
- ✓ Collecter les journaux
- ✓ Mener des audits
- ✓ Arrêtez systèmes

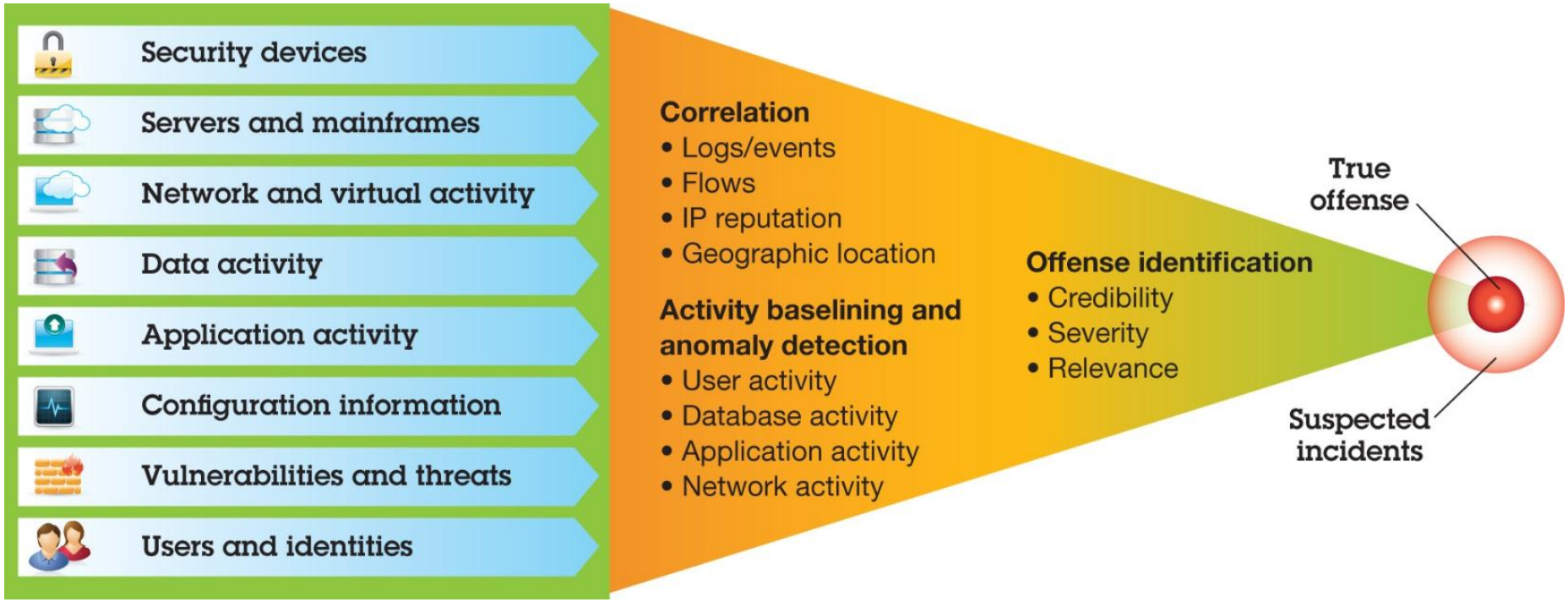
Détecter, Analyser & Remédier

Penser comme un attaquant, Mentalité de contre espionnage

- ❑ Protéger les actifs sensibles
- ❑ Mettre l'accent sur les données
- ❑ Durcir les cibles
- ❑ Utiliser la détection basée sur les anomalies
- ❑ Suivre les comportements des systèmes
- ❑ S'appuyer sur des experts
- ❑ Collecter toutes les informations
- ❑ Automatiser les corrélations et les analyses
- ❑ Rassembler et préserver les preuves

Générale **Ciblée**

Besoins accrus pour la sécurité intelligente…



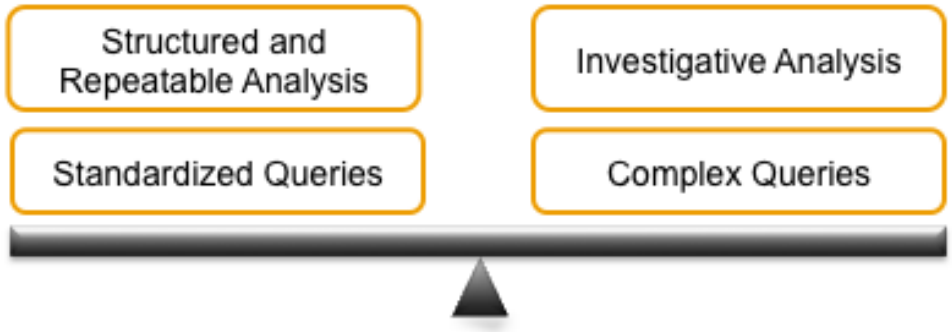
Visibilité sur les systèmes de sécurité de l'entreprise afin d'améliorer les temps de réponse et d'intégrer l'adaptabilité / flexibilité nécessaire pour la détection précoce des menaces ou des comportements à risque (signaux faibles)

Augmentation des informations de sécurité avec l'analyse BigData

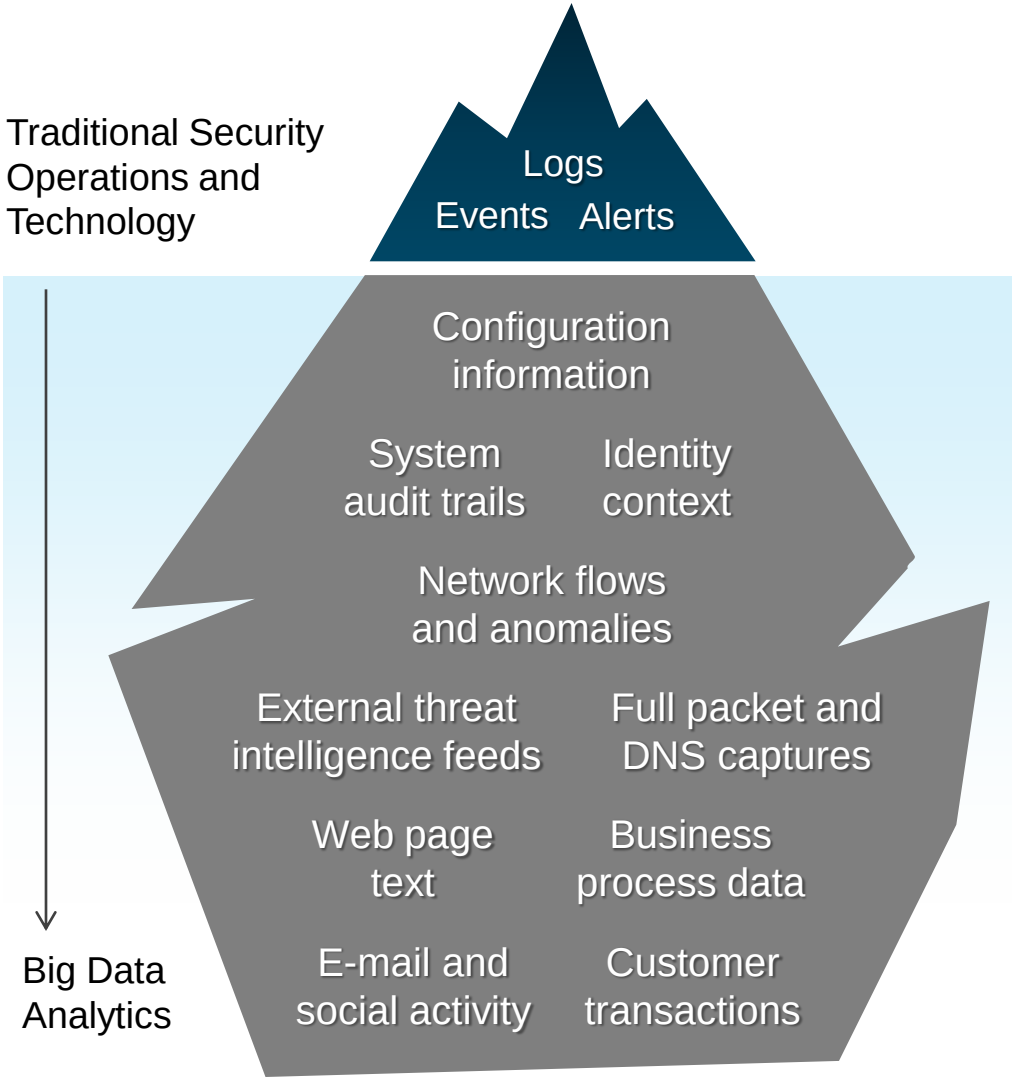
Les déclencheurs qui motivent l'utilisation de l'analyse BigData

Additional Analytical Requirements:

Real-Time	Asymmetric/Forensics
Proactive	Predictive
Formalized	Inquisitive
Speed	Depth



Les clients ont un besoin croissant d'identifier et de se protéger contre les menaces à partir d'un ensemble de données plus importantes



Nouvelles considérations

Collecte, stockage et traitement
- Collecte et intégration
- Taille et vitesse
- L'enrichissement et la corrélation

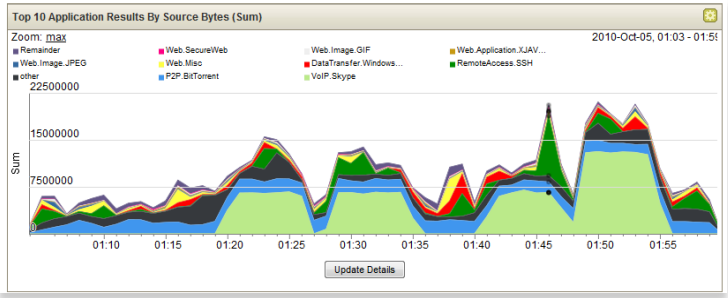
Analyse et worflow
- visualisation
- analyse non structurées
- Apprentissage et prédiction
- Personnalisation
- Partage et export

Agenda

- Un besoin réel
- Des cas d'utilisation
- Les offres logicielles IBM

Sécurité Intelligente à partir du traitement en temps réel des données BigData

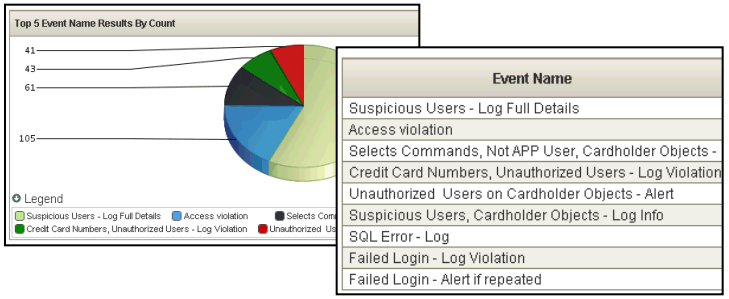
Behavior monitoring and flow analytics



Network Traffic Doesn‘t Lie

Attackers can stop logging and erase their tracks, but can’t cut off the network (flow data)

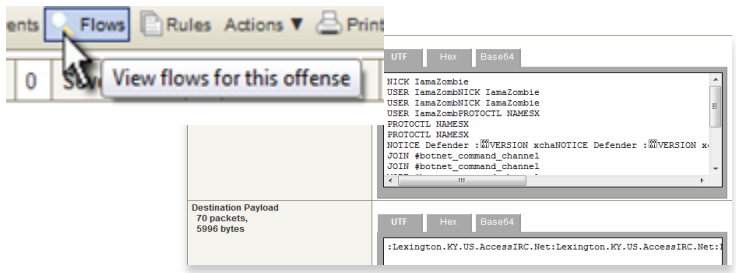
Activity and data access monitoring



Improved Breach Detection

360-degree visibility helps distinguish true breaches from benign activity, in real-time

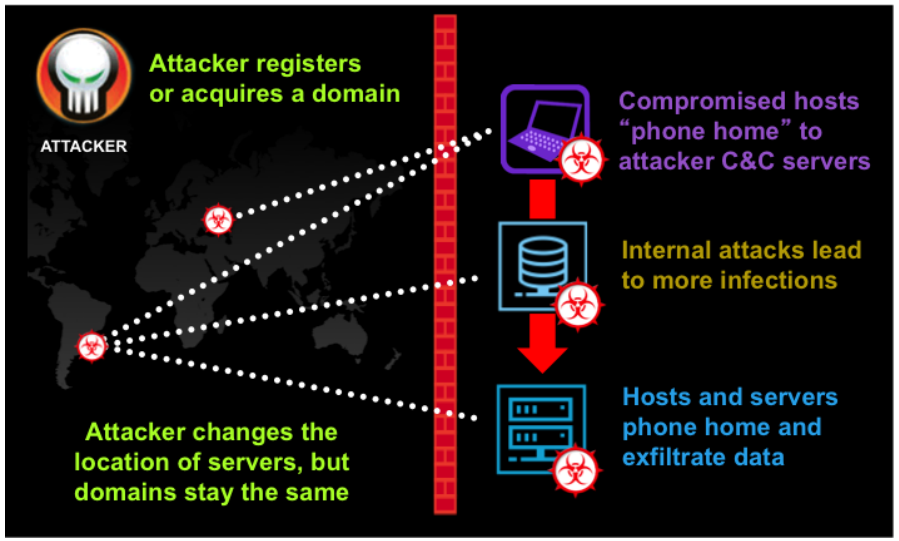
Stealthy malware detection



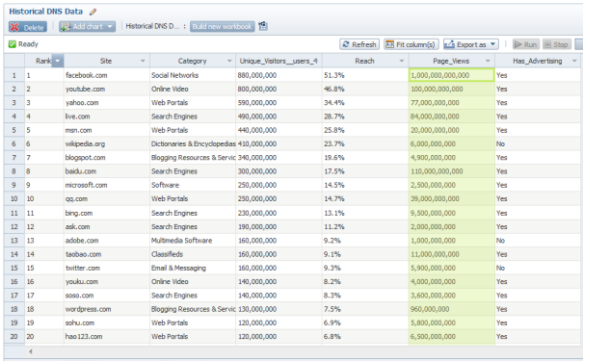
Irrefutable Botnet Communication

Layer 7 flow data shows botnet command and control instructions

Sécurité Intelligente avec analyse des traitements BigData :
Hunting for External Command & Control (C&C) Domains of an Attacker

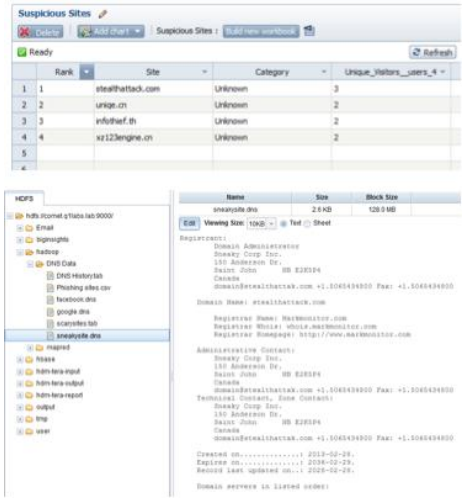


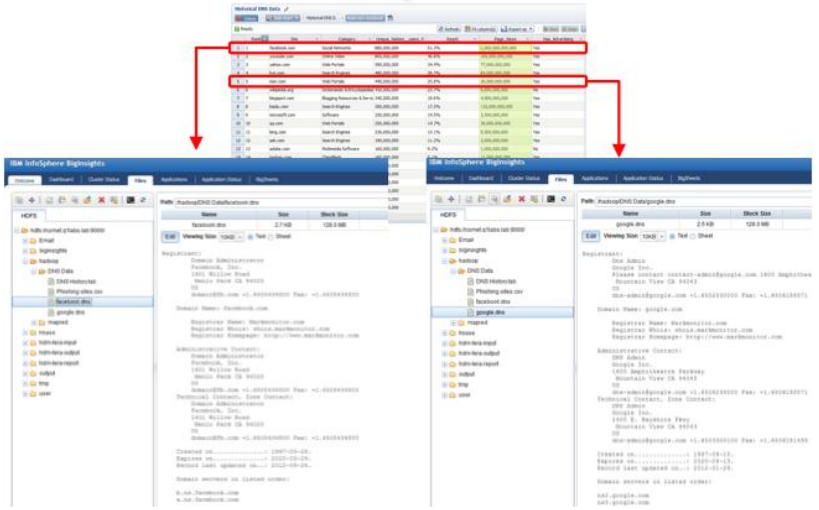
Historical analysis of DNS activity within organization



Advanced analytics identify suspicious domains

- Why only a few hits across the entire organization to these domains?
- Correlating to public DNS registry information increases suspicions

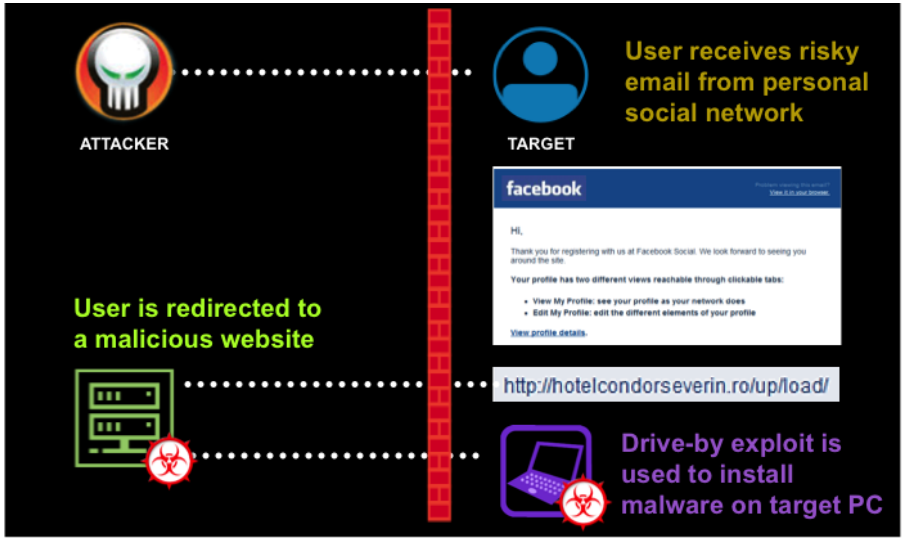




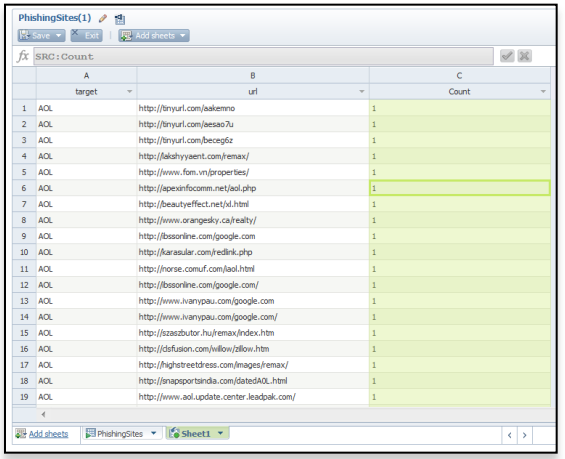
Automate correlation against external DNS registries

Sécurité Intelligente avec analyse des traitements BigData :

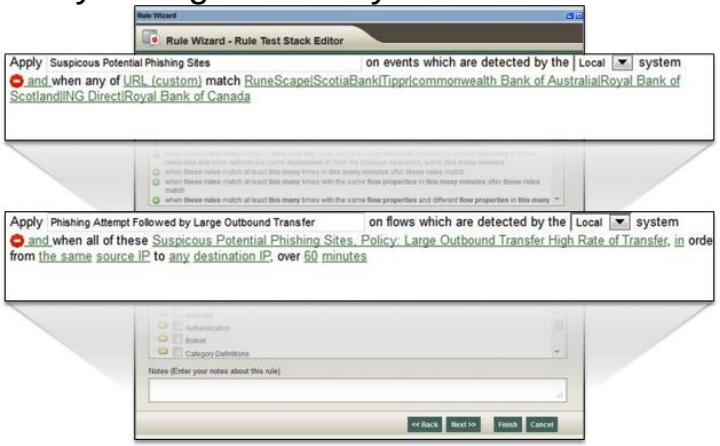
Pursue Active Spear-Phishing Campaigns Targeting the Organization

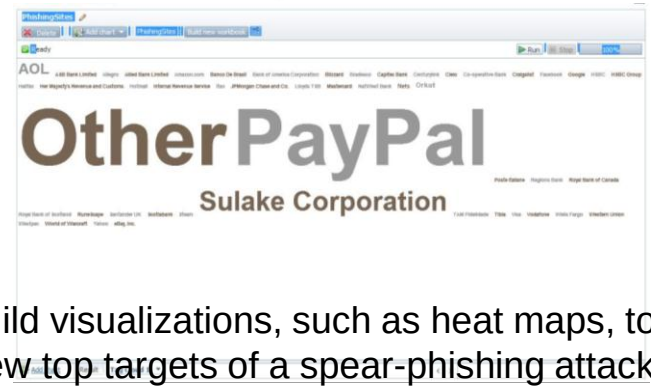


Employ Big Data Analytics on email to identify patterns to identify targets and redirects



Load Spear-Phishing targets and redirect URLs into real-time security intelligence analysis to thwart the attack



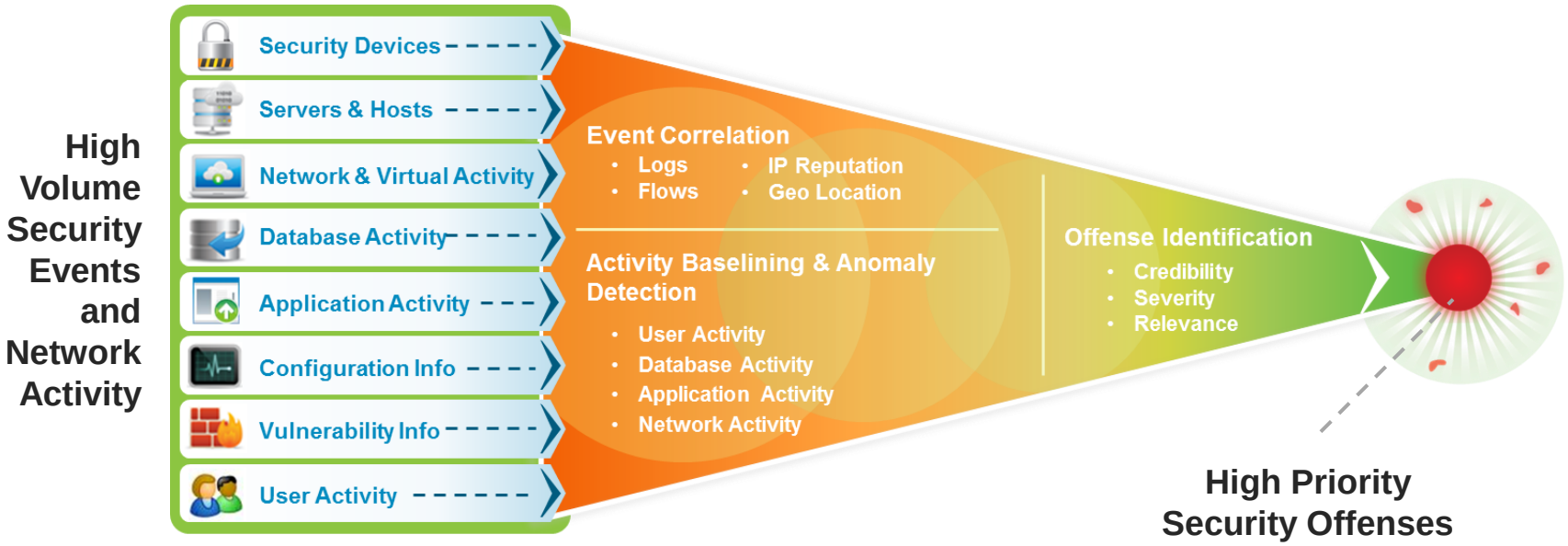


Build visualizations, such as heat maps, to view top targets of a spear-phishing attacks

Agenda

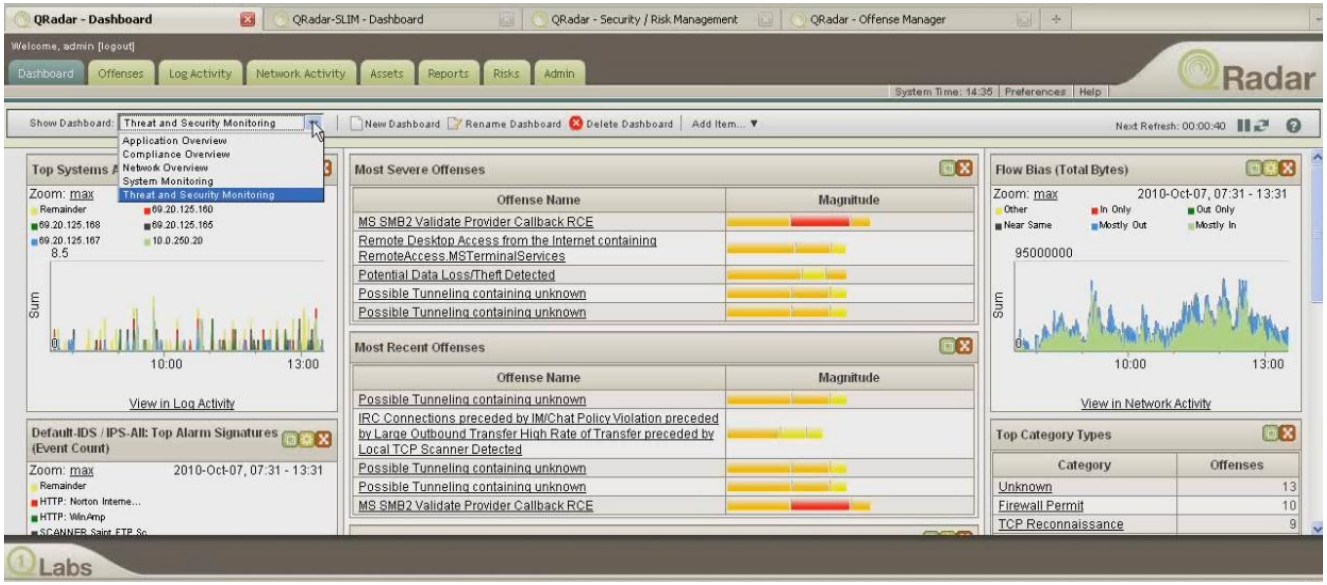
- Un besoin réel
- Des cas d'utilisation
- Les offres logicielles IBM

QRadar utilise les possibilités BigData pour identifier des événements critiques de sécurité



IBM QRadar Big Data Capabilities	Customer Results
▪ New SIEM appliances with massive scale	✓ Quickly find critical insights among 1000s of devices and years of data
▪ Payload indexing for rapid ad hoc query leveraging a purpose-built data store	✓ Search 7M+ events in <0.2 sec
▪ Google-like Instant Search of large data sets (both logs and flows)	✓ Instant, free-text searching for easier and faster forensics
▪ Intelligent data policy management	✓ Granular management of log and flow data
▪ Advanced Threat Visualization and Impact Analysis	✓ Attack path visualization and device / interface mapping

IBM QRadar: Plus qu'un SIEM, c'est une solution de sécurité intelligente



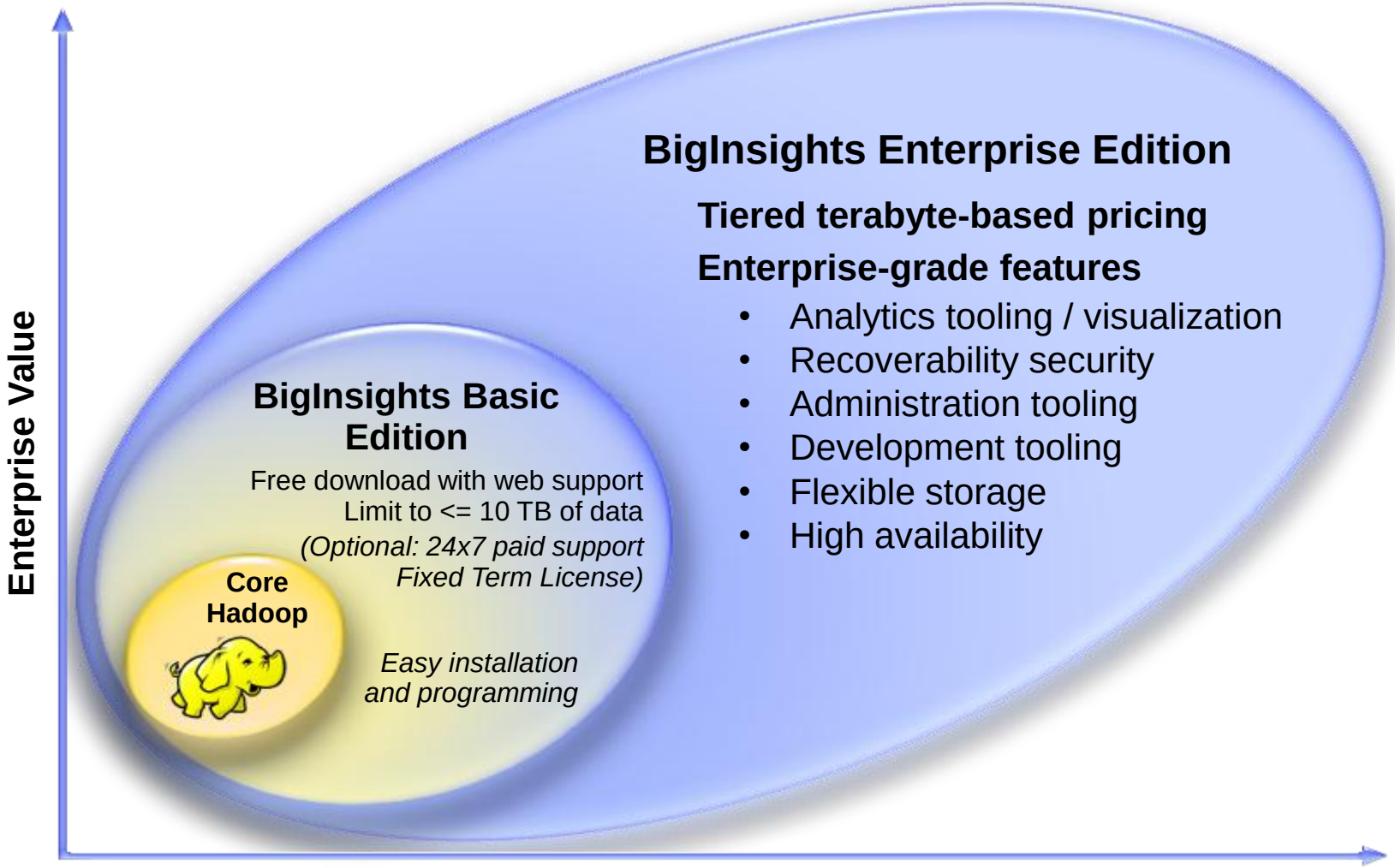
QRadar:

- Filters out the noise, improves incident & offense identification
- Enables proactive detection of targeted & zero-day attacks
- Is scalable to add more data sources and extensible to incorporate logic to detect new attack patterns

Log Management | **SIEM** | **Configuration & Vulnerability Management** | **Network Activity & Anomaly Detection** | **Network and Application Visibility**

- Purpose-Built Security Intelligence Solution
  - Pre-built support for 100s of scenarios
  - Capability to ingest security data from 1000s of IT devices and numerous data feeds including XForce
- Single Console with Unified Data Architecture
  - Powerful correlation engine to add security context to data
  - Rich Asset Database with profiles of assets, applications, vulnerabilities and other security related content

IBM InfoSphere BigInsights – Une solution flexible pour le traitement de gros volumes de données



Une nouvelle approche d'exploration et d'analyse intégrée

Structured, analytical, repeatable

Creative, exploratory, intuitive

Security Intelligence Platform

Real-time Processing

- Real-time data correlation
- Anomaly detection
- Event and flow normalization
- Security context & enrichment
- Distributed architecture

Security Operations

- Pre-defined rules and reports
- Offense scoring & prioritization
- Activity and event graphing
- Compliance reporting
- Workflow management

Integrated IBM Solution

Big Data Platform

Big Data Processing

- Long-term, multi-PB storage
- Unstructured and structured
- Distributed Hadoop infrastructure
- Preservation of raw data
- Enterprise Integration

Analytics and Forensics

- Advanced visuals and interaction
- Predictive & decision modeling
- Ad hoc queries
- Interactive visualizations
- Collaborative sharing tools
- Pluggable, intuitive UI

Intégration de QRadar avec la solution IBM's Hadoop

Security Intelligence Platform

IBM Security QRadar

- Data collection and enrichment
- Event correlation
- Real-time analytics
- Offense prioritization

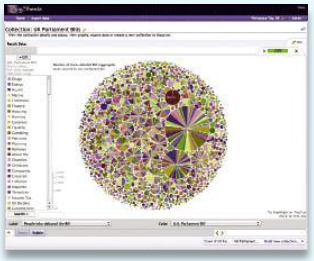
QRadar

Real-time streaming

Insights

Advanced Threat Detection

Big Data Platform



IBM InfoSphere BigInsights

- Hadoop-based
- Enterprise-grade
- Any data / volume
- Data mining
- Ad hoc analytics

Custom Analytics

Traditional data sources

Non-traditional

Solution de Sécurité Intelligente avec BigData

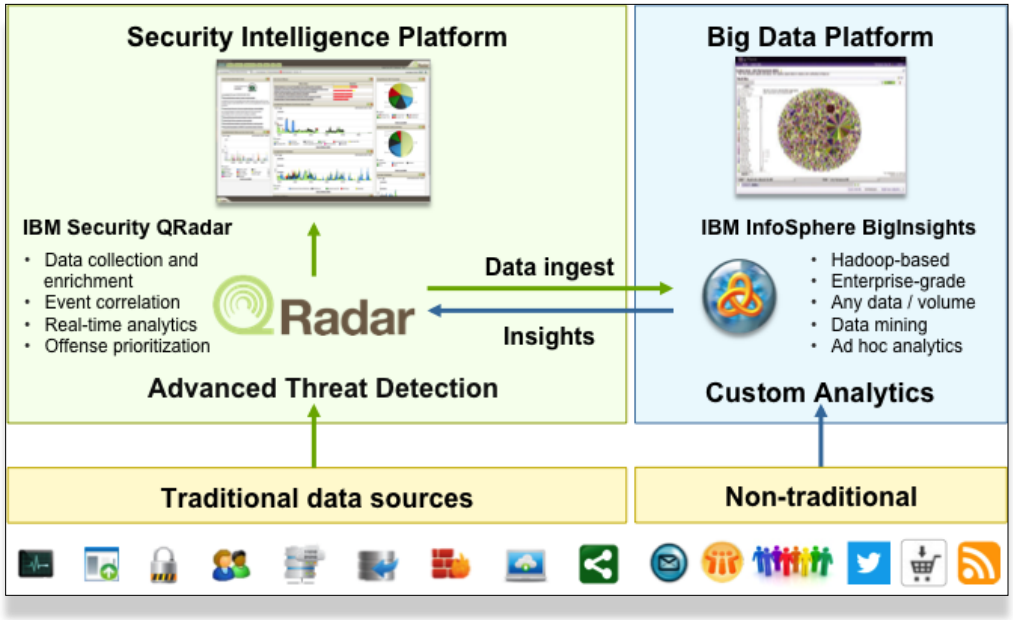
Analyse en temps réel (QRadar) couplée avec un analyse de l'information asymétrique (BigData)

Establishing Baseline
- Who are the attractive targets within my enterprise?
- Which applications and what data do we need to defend due to their sensitivity?
- What is the normal behavior profile for users, assets, and applications?

APTs
- Which assets within my organization are already compromised or are vulnerable?
- Which external domains may be the source of attacks?
- Are there any low profile network traffic elements that might signal an ongoing or imminent attack?

Counter Cyber Attacks
- Which geographical region may be the origin of an attack?
- Which hacking tools may be used and who is gaining access to them?
- Are their symptoms of an attack underway or being planned manifesting themselves as support issues?

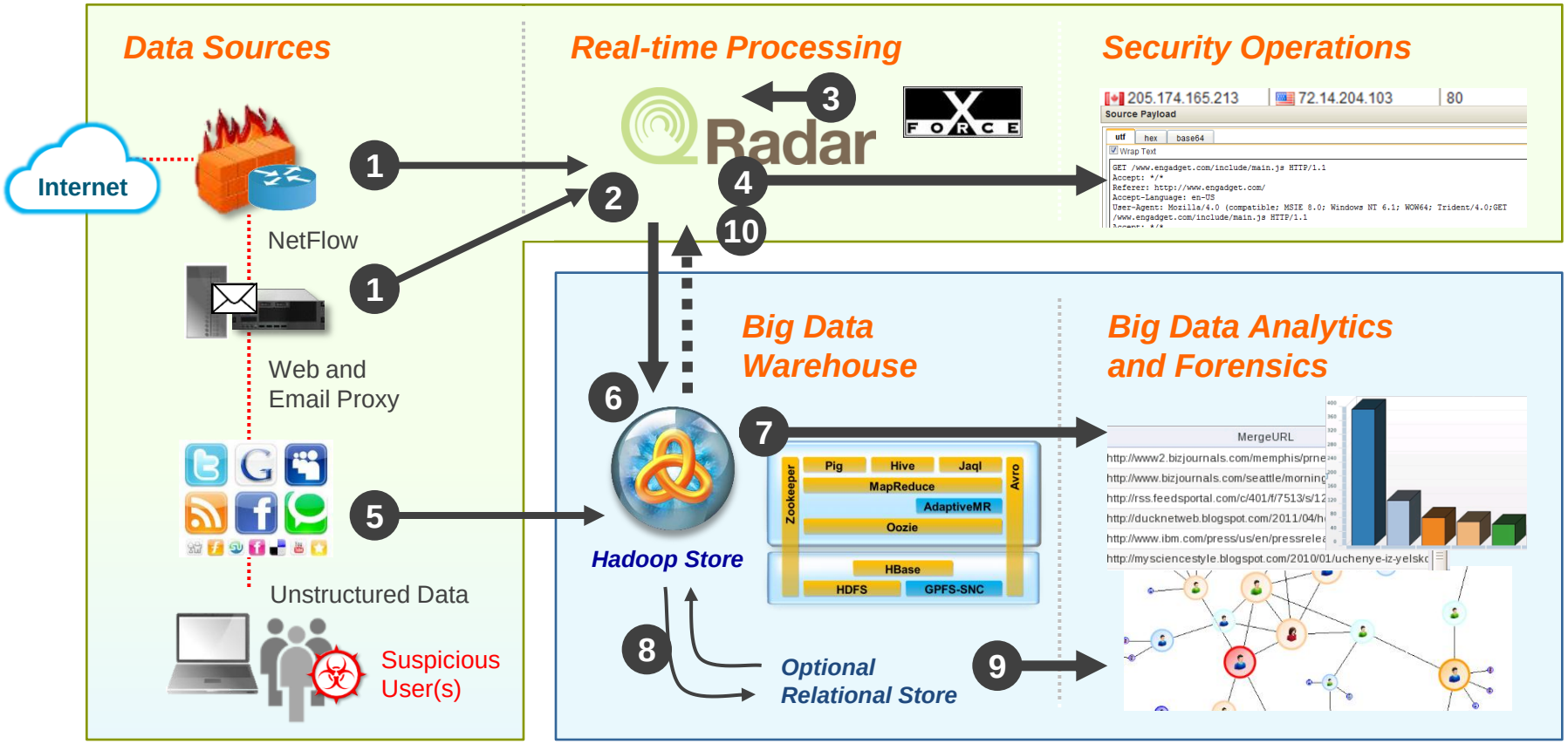
Qualify Insider Threats
- What data is being leaked or lost and by whom?
- Who internally has the motivation and skills to compromise the cyber operations of the company?
- Who is exhibiting abnormal usage behavior?



Mitigate Fraud
- How can the organization identify a fraudulent activity?
- Which users have compromised identities that may lead to fraudulent activity?
- Can well known fraud attempts have patterns can either be detected or even anticipated?

Predict Hacktivism
- Which controversial issues may trigger a negative sentiment about the organization triggering an increased risk of attack?
- How to identify and monitor intentions of entities antagonistic to the organization's business practices?
- How does publicity of the company in the media impact risk?

Exemple client – Profilage d'un utilisateur en se basant sur de multiples sources d'information



1. NetFlow and logs sent to QRadar
2. Event and flow processing
3. Correlation against external feeds
4. Real-time user alerts to SOC
5. Unstructured data to BigInsights
6. Enriched events and flows sent to BigInsights
7. Spreadsheet UI for business analysts (BigSheets)
8. Post-processed data storage
9. i2 link-based visuals and analytics
10. Update of QRadar real-time rule sets

“Big Value from Big Data” – Cas d’utilisation

	 **Découverte des menaces ciblées**	 **Détection de la fraude**	 **Analyse menaces internes**
Customer Problem	Organizations need help in identifying advanced threats and zero-day attacks	Fraudulent claims, account takeovers, and invalid transactions cause substantial losses – and many organizations are unaware the fraud is being committed	As repositories of private information expand, the cost of data loss by insiders action grows, whether intentional or through human error
Technical Challenges	▪ Collection of high volume network and DNS events ▪ Rapidly changing identifiers ▪ Analytics to find subtle indicators ▪ Integration of external intelligence	▪ Collection of user, application and network activity ▪ Unstructured data analysis ▪ Long-term baselining capabilities ▪ Integration with fraud workflow	▪ Collection of inter- and intra-company communications ▪ Sentiment and linguistic analysis ▪ Ability to identify anomalies and outliers ▪ Integration with IAM solutions
IBM Approach	▪ QRadar event and flow collection ▪ Correlation against external threats ▪ Collection of all DNS transactions using BigInsights ▪ Custom analytics to identify suspicious domain names ▪ Analysis of historical data to detect infections / past intrusions ▪ Import BigInsights findings into QRadar	▪ QRadar to collect and normalize application and transaction data ▪ Anomaly detection in real time ▪ Real-time export to BigInsights ▪ Baseline historical user and account activity ▪ Send insights to QRadar for real-time fraud correlation ▪ Extend information flow to IBM i2 for link analysis, visualization and dissemination to fraud analysts	▪ Use QRadar to correlate real-time system and user activity ▪ Analyze ordinary and privileged users accessing sensitive data ▪ Collect full text email and social activity with BigInsights ▪ Leverage advanced analytics to understand unstructured content ▪ Share findings with existing IAM systems—such as IBM Security Privileged Identity Manager

Personnalistion de l'approche IBM Sécurité Intelligente avec la solution BigData

Triggers for Specific Capabilities to Augment Core Security Intelligence with Big Data Solution:

Ingesting and Pre-processing Domain or Industry Specific Very High Velocity Data Streams for correlation with cyber security data

Example Data Sources:
Telecom: Customer Data Records
Energy & Utilities: Grid Sensor Data
Surveillance: Video/Audio content

Performing Advanced Statistical, Predictive and/or Identity Analytics on all data captured to yield security insights

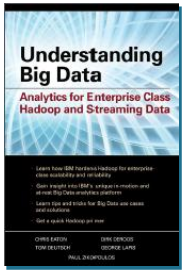
Example Analysis:
- Visualize linkages of users to privileged identities
- Which user group has the highest propensity for insider fraud?

Executing Frequently Repeated Queries and other Analytical workloads best suited for massive parallel processing on Warehoused Security-enriched data

Example Queries:
- Quarterly reporting on historical warehoused security data

Des informations vers nos offres

- Visit the website
- Watch the video
- Read the white paper
- Read the thought pieces
  - What is Your Organization's Security IQ?
  - What You Need to Know About Security Intelligence with Big Data
- Develop a richer understanding of big data
  - Understanding Big Data eBook
  - Harness the Power of Big Data eBook
- Download some collateral
  - Security Intelligence white paper
  - QRadar SIEM data sheet
  - InfoSphere BigInsights data sheet



IBM SolutionsConnect 2013

L'IBM TechSoftware nouvelle génération