Contenir les Cybermenaces critiques grâce à l'intelligence de sécurité

Youssef Hbilate

LogRhythm
The Security Intelligence Company

LogRhythm™

The Security Intelligence Company

Youssef Hbilate
Consultant en sécurité informatique

La prévention seule est vaine

“ La prévention est vaine en 2020 ”

“ La sécurité de l’informatique ne peut plus empêcher les attaques ciblées ”

“ En 2020, 60% des budgets sécurité de l’informatique seront alloués à la detection et aux réponses rapides contre 10% en 2013. ”

Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence

Published: 30 May 2013

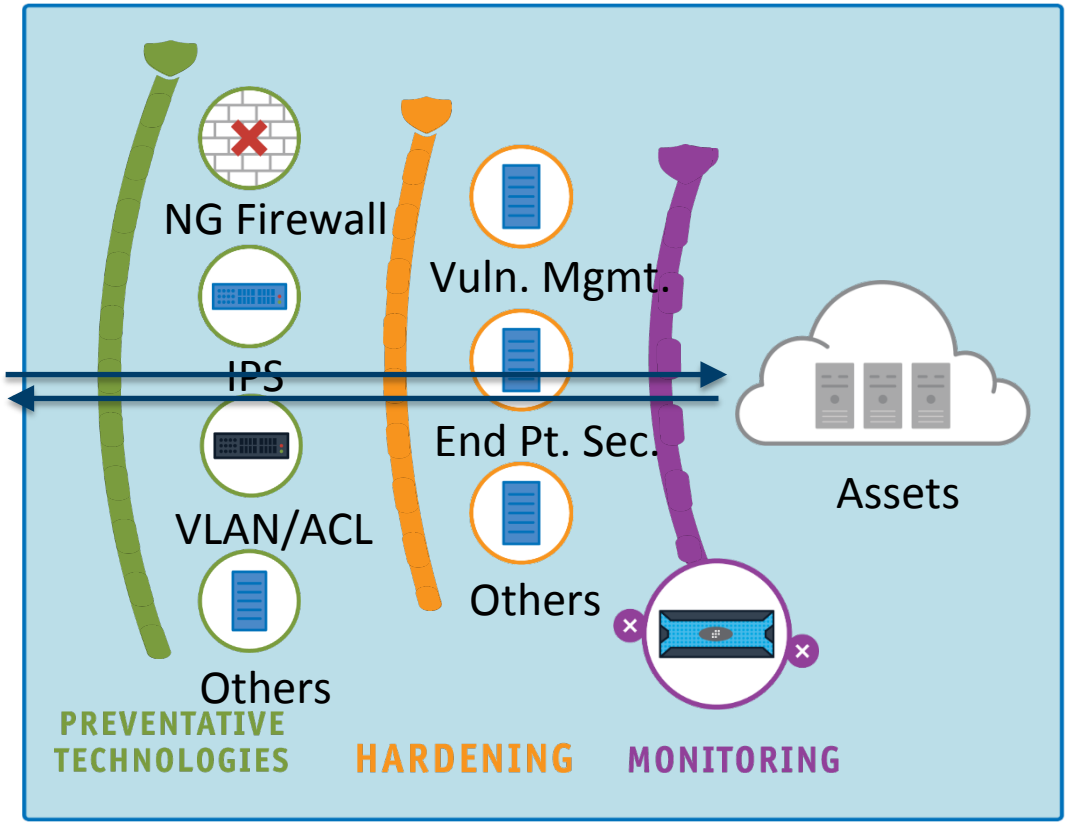
Analyst(s): Neil MacDonald

Advanced targeted attacks make prevention-centric strategies obsolete. Securing enterprises in 2020 will require a shift to information- and people-centric security strategies, combined with pervasive internal monitoring and sharing of security intelligence.

Gartner

Lacunes des protections traditionnelles

- **Identifiants faibles ou volés**
  76% des attaques
- **Ingénierie sociale/Phishing**
  52% des attaques
- **Botnets/APT**
  59% des attaques
- **Menaces internes**
  35% des attaques



 Sources: Ponemon et Verizon

Cyber attaques majeurs des 12 derniers mois

Devriez-vous être inquiet ?

As seen on: BBC News, Reuters, The Sun, The Telegraph, The Times

Ashley Madison is the world's leading married dating service for ***discreet*** encounters

Qui est LogRhythm

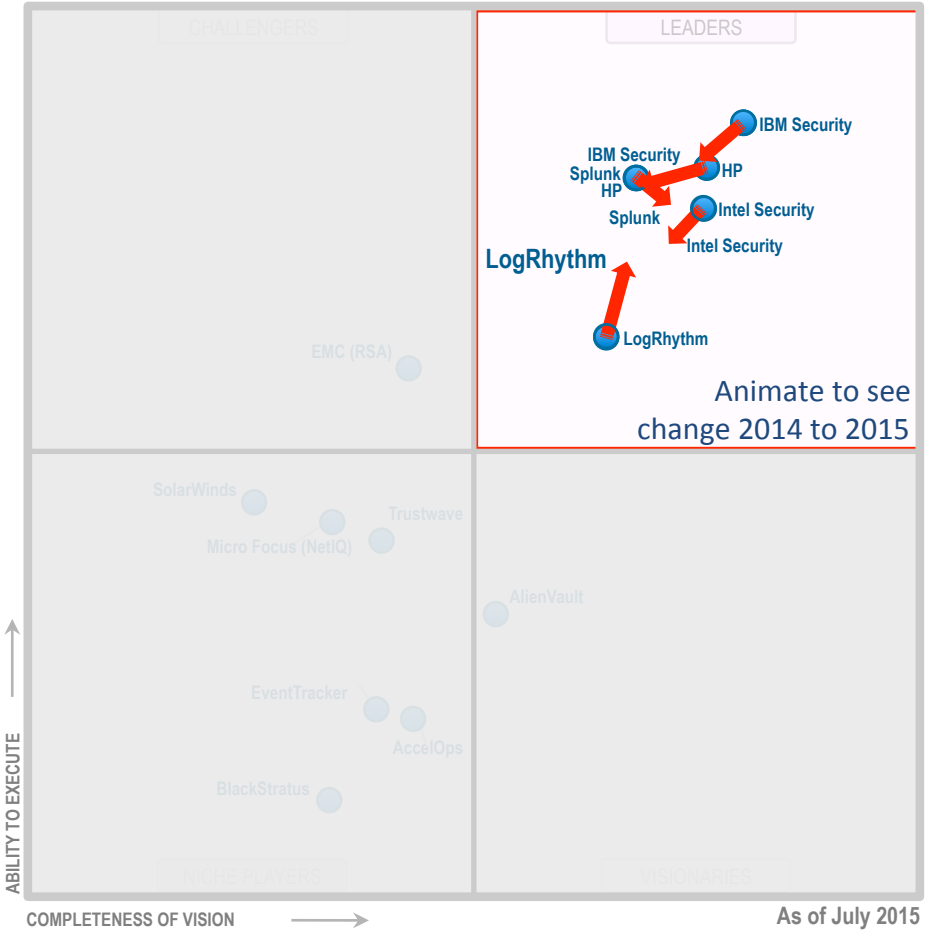
- Fondée en Mars 2003
- Siège social dans le Colorado
- Croissance annuelle > 50%
- Le plus grand éditeur indépendant de SIEM
- Solution Best of Breed, Leader
- Plus de 2500 clients
- Focalisation sur la satisfaction client : > 95% de clients restent nos clients

Gartner – Magic Quadrant for SIEM- 2015

LogRhythm

- LogRhythm combines **SIEM capabilities** with **endpoint monitoring, network forensics and incident management capabilities** to support security operations use cases.
- Gartner receives consistent user feedback stating that **LogRhythm's solution is straightforward** to deploy and maintain, and provides **effective out-of-the-box use cases and reporting templates**.
- The average of LogRhythm reference customers **satisfaction scores** for **scalability and performance**, effectiveness of predefined rules, usefulness of predefined reports, ease of use and effectiveness of predefined queries, product quality and stability, and support experience is **higher than the average scores for all reference customers in those areas**

Gartner – Magic Quadrant for SIEM : Change from 2014 to 2015



La différence avec LogRhythm

- Focus
- Innovation
- Gestion globale des indicateurs des cyber menaces
- Gestion des incidents de sécurité du début à la fin
- Platforme évolutive
- Valeur ajoutée rapide pour nos clients

Pourquoi LogRhythm?

LogRhythm

- Security Intelligence:
  - Log Management + SIEM + Threat Analytics + Threat Intelligence
  - Endpoint forensic + Network forensic
- Rapidité de déploiement et d'évolution:
  - 700+ normalisation de sources de log préconfigurées
  - 700+ règles de corrélation préconfigurées (par modules) faciles à modifier
  - Modules de conformité PCI-DSS, ISO27001, Quick Start… préconfigurés
- Interface puissante et facile d'utilisation
- SOC Nouvelle Génération (produits & team qui gèrent les incidents)

Objectifs

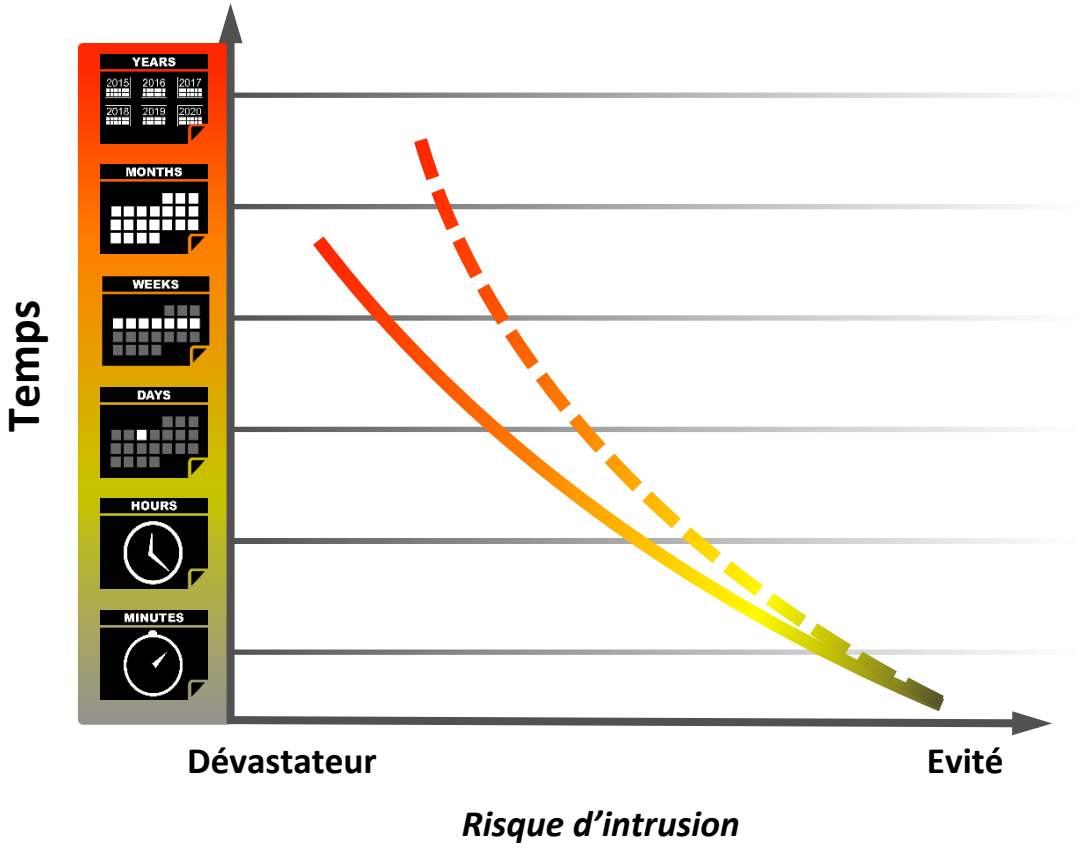
- **MTTD** = **M**ean **T**ime **T**o **D**etect

  Temps Moyen De Détection

- **MTTR** = **M**ean **T**ime **T**o **R**espond

  Temps Moyen De Réponse

Une détection et réponse plus rapide réduit les risques

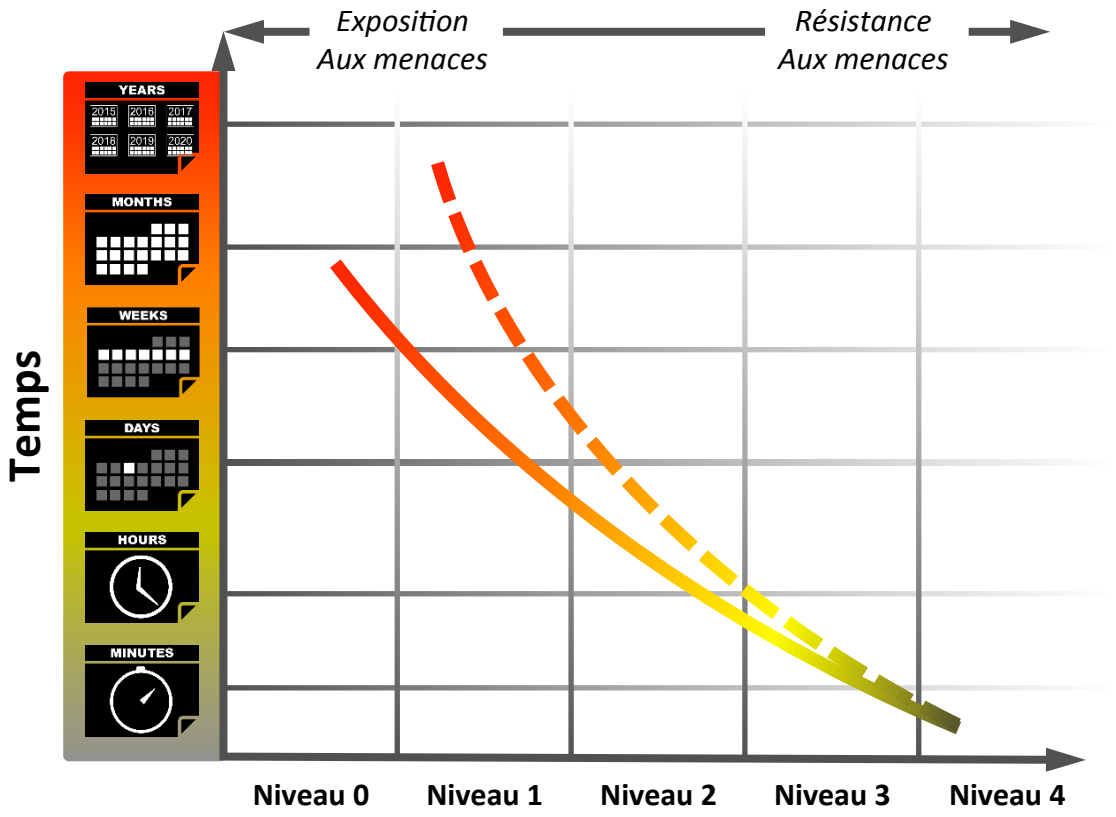


MEAN-TIME-TO-DETECT (MTTD)*

MEAN-TIME-TO-RESPOND (MTTR)

* 31 jours en moyenne (rapport Ponemon 2014)

Model de maturité du “Security Intelligence”



Niveaux de sécurité

Niveau 0: Aveugle

Niveau 1: Conforme à Minima

Niveau 2: Solidement conforme

Niveau 3: Vigilant

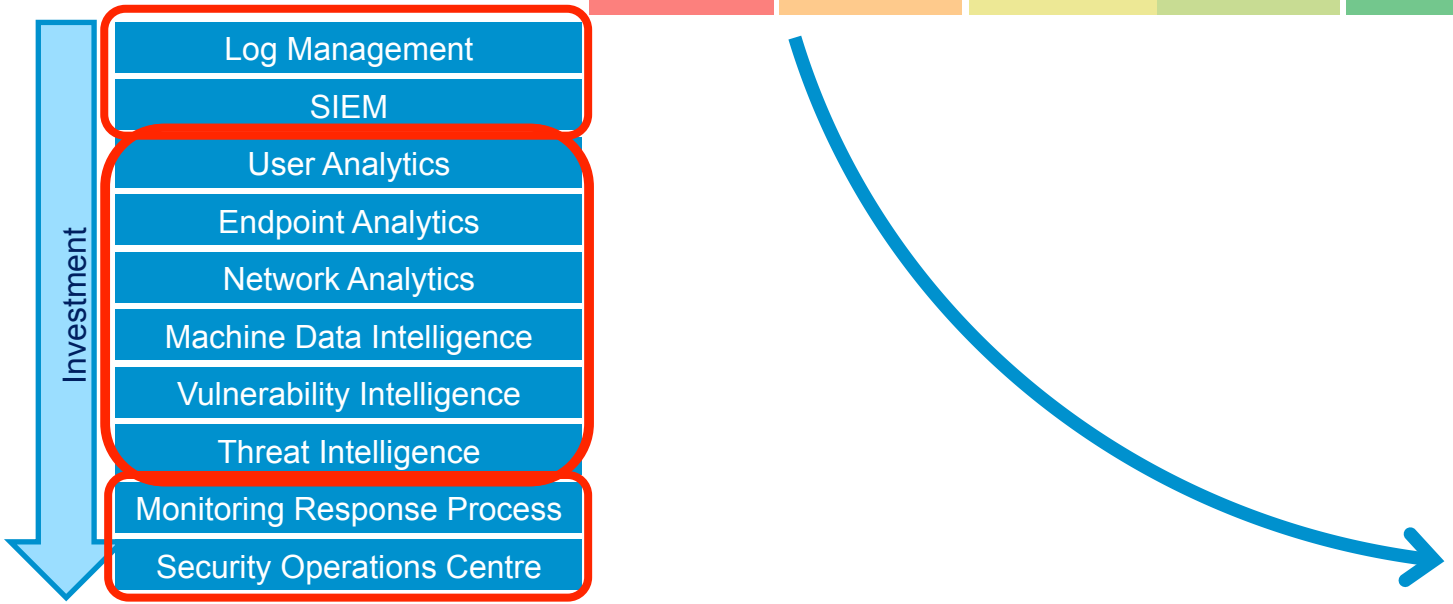
Niveau 4: Resistant

MEAN-TIME-TO-DETECT (MTTD)*

MEAN-TIME-TO-RESPOND (MTTR)

Model de maturité du “Security Intelligence”

Maturity Level	0	1	2	3	4
Security Posture	Aveugle	Conforme à Minima	Solidement conforme	Vigilant	Resistant



User Analytics

LogRhythm

Reconnaissance	Initial Compromise	Command & Control	Lateral Movement	• Exfiltration • Corruption • Disruption
External network scan	Phishing email	Malware	Internal network scan	Connection to control center
Port and vulnerability scan	External vulnerability exploit (can create errors)	Haking tools and new processes	Internal vulnerability exploit (can create errors)	Data encryption, destruction or corruption
Wifi tapping	Infected web site	Creation of temporary accounts	Access to confidential data	Web site content modification
Stolen email addresses	Malware	Escalation of priviledges	Internal brute force	DDOS Attack
Data from breach of other companies	Stolen credentials	Connection to control center	Pass the hash	Industrial devices attack
Phone jacking	External brute force	Configuration Change	Generation of spam /phishing emails	Evidences, log, account destruction

OS / Devices
Access Control logs
User Patterns Analytics
User Behavioral Analytics

User

Endpoint analytics

LogRhythm

Reconnaissance	Initial Compromise	Command & Control	Lateral Movement	• Exfiltration • Corruption • Disruption
External network scan	Phishing email	Malware	Internal network scan	Connection to control center
Port and vulnerability scan	External vulnerability exploit (can create errors)	Haking tools and new processes	Internal vulnerability exploit (can create errors)	Data encryption, destruction or corruption
Wifi tapping	Infected web site	Creation of temporary accounts	Access to confidential data	Web site content modification
Stolen email addresses	Malware	Escalation of priviledges	Internal brute force	DDOS Attack
Data from breach of other companies	Stolen credentials	Connection to control center	Pass the hash	Industrial devices attack
Phone jacking	External brute force	Configuration Change	Generation of spam /phishing emails	Evidences, log, account destruction

OS / Devices Audit logs
Endpoint Forensic data
Patterns Analytics
Behavioral Analytics

Endpoint

Network Analytics

LogRhythm

Reconnaissance	Initial Compromise	Command & Control	Lateral Movement	• Exfiltration • Corruption • Disruption
External network scan	Phishing email	Malware	Internal network scan	Connection to control center
Port and vulnerability scan	External vulnerability exploit (can create errors)	Haking tools and new processes	Internal vulnerability exploit (can create errors)	Data encryption, destruction or corruption
Wifi tapping	Infected web site	Creation of temporary accounts	Access to confidential data	Web site content modification
Stolen email addresses	Malware	Escalation of priviledges	Internal brute force	DDOS Attack
Data from breach of other companies	Stolen credentials	Connection to control center	Pass the hash	Industrial devices attack
Phone jacking	External brute force	Configuration Change	Generation of spam /phishing emails	Evidences, log, account destruction

Firewall logs
Internal traffic
Deep packet inspection
Patterns Analytics
Behavioral Analytics

Network

Threat and malware intelligence

LogRhythm

Reconnaissance	Initial Compromise	Command & Control	Lateral Movement	• Exfiltration • Corruption • Disruption
External network scan	Phishing email	Malware	Internal network scan	Connection to control center
Port and vulnerability scan	External vulnerability exploit (can create errors)	Haking tools and new processes	Internal vulnerability exploit (can create errors)	Data encryption, destruction or corruption
Wifi tapping	Infected web site	Creation of temporary accounts	Access to confidential data	Web site content modification
Stolen email addresses	Malware	Escalation of priviledges	Internal brute force	DDOS Attack
Data from breach of other companies	Stolen credentials	Connection to control center	Pass the hash	Industrial devices attack
Phone jacking	External brute force	Configuration Change	Generation of spam /phishing emails	Evidences, log, account destruction

Threat lists
Anti-malware data
Anti-spam data
Next Gen Firewalls

Threat intel

Vulnerability intelligence

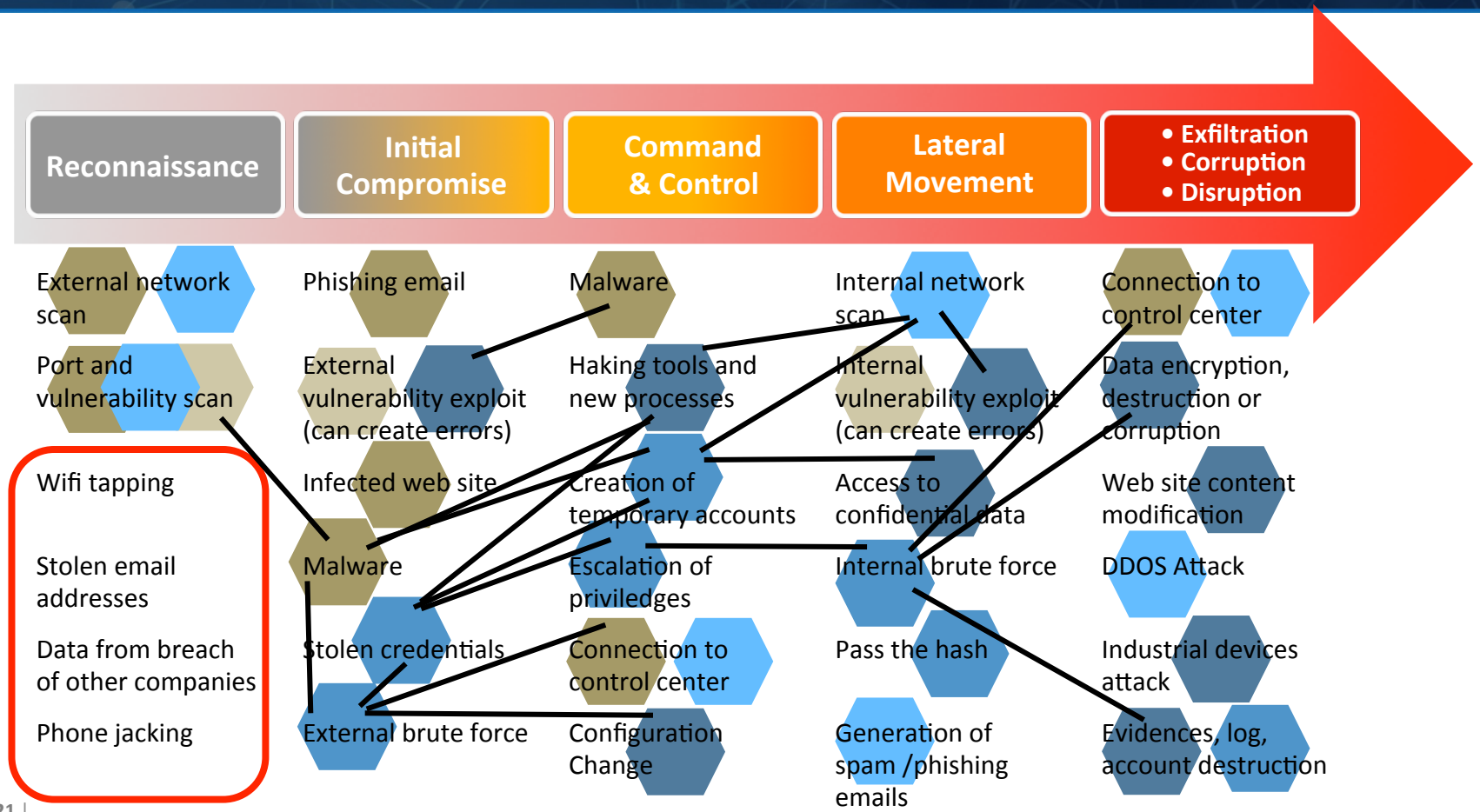
LogRhythm

Reconnaissance	Initial Compromise	Command & Control	Lateral Movement	• Exfiltration • Corruption • Disruption
External network scan	Phishing email	Malware	Internal network scan	Connection to control center
Port and vulnerability scan	External vulnerability exploit (can create errors)	Haking tools and new processes	Internal vulnerability exploit (can create errors)	Data encryption, destruction or corruption
Wifi tapping	Infected web site	Creation of temporary accounts	Access to confidential data	Web site content modification
Stolen email addresses	Malware	Escalation of priviledges	Internal brute force	DDOS Attack
Data from breach of other companies	Stolen credentials	Connection to control center	Pass the hash	Industrial devices attack
Phone jacking	External brute force	Configuration Change	Generation of spam /phishing emails	Evidences, log, account destruction

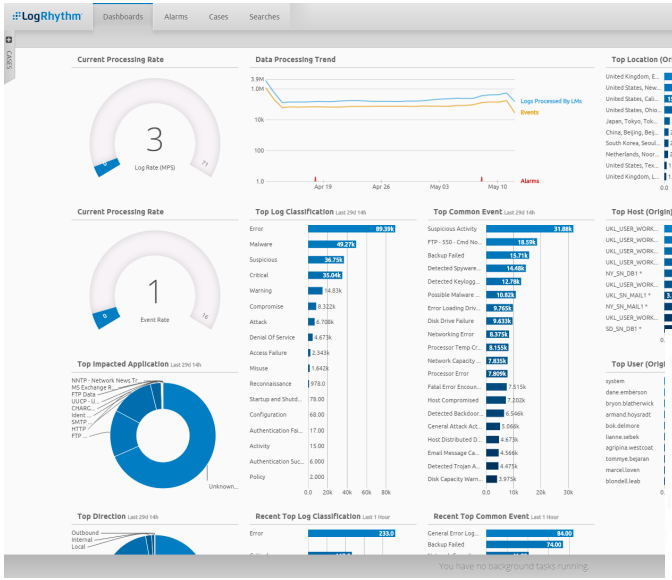
Vulnerability scanners
Patch assessment

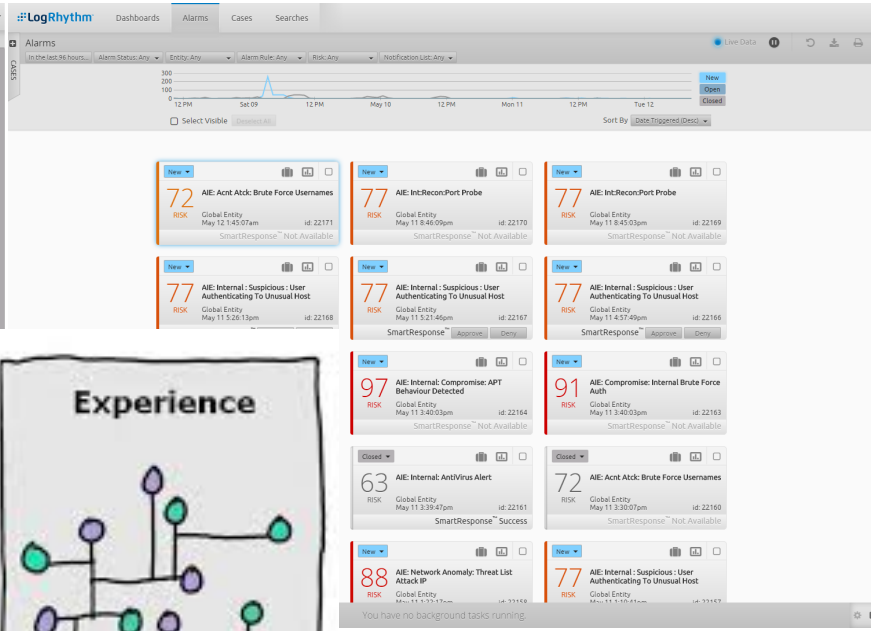
Vulnerability

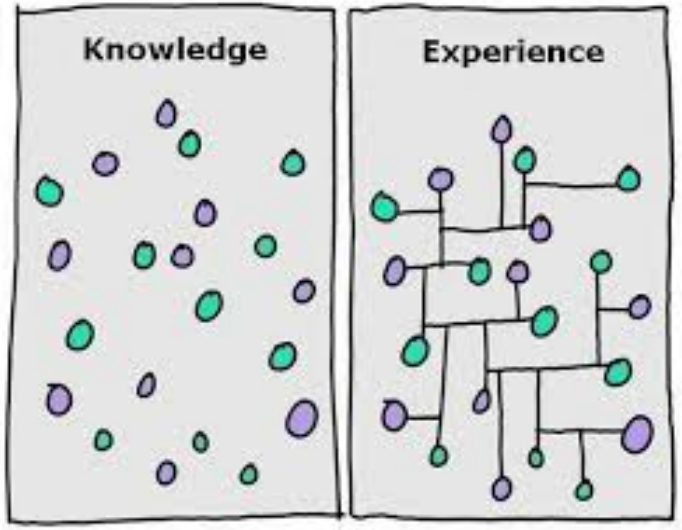
Holistic Machine data intelligence



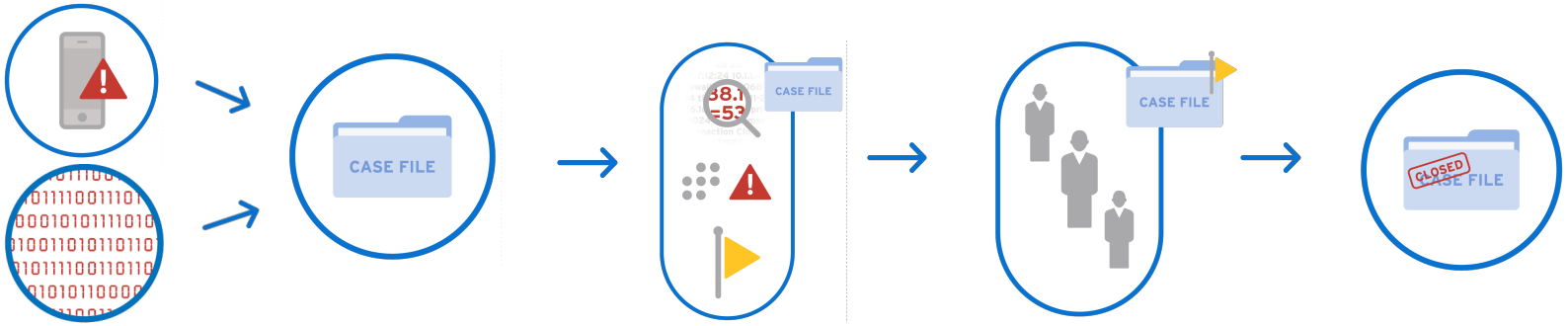
Event vs Incident







Gestion d’incident, Personnes et Processus



Détection d’un incident potentiel et évaluation

Création du dossier et option de l’ escalader en incident

Réponse si incident:

- Enquête
- Contrôle:
  - Désactivation du compte
  - Contrôle d’accés au réseau
  - Récupération des données forensiques
- Analyse
- Historique

Collaboration

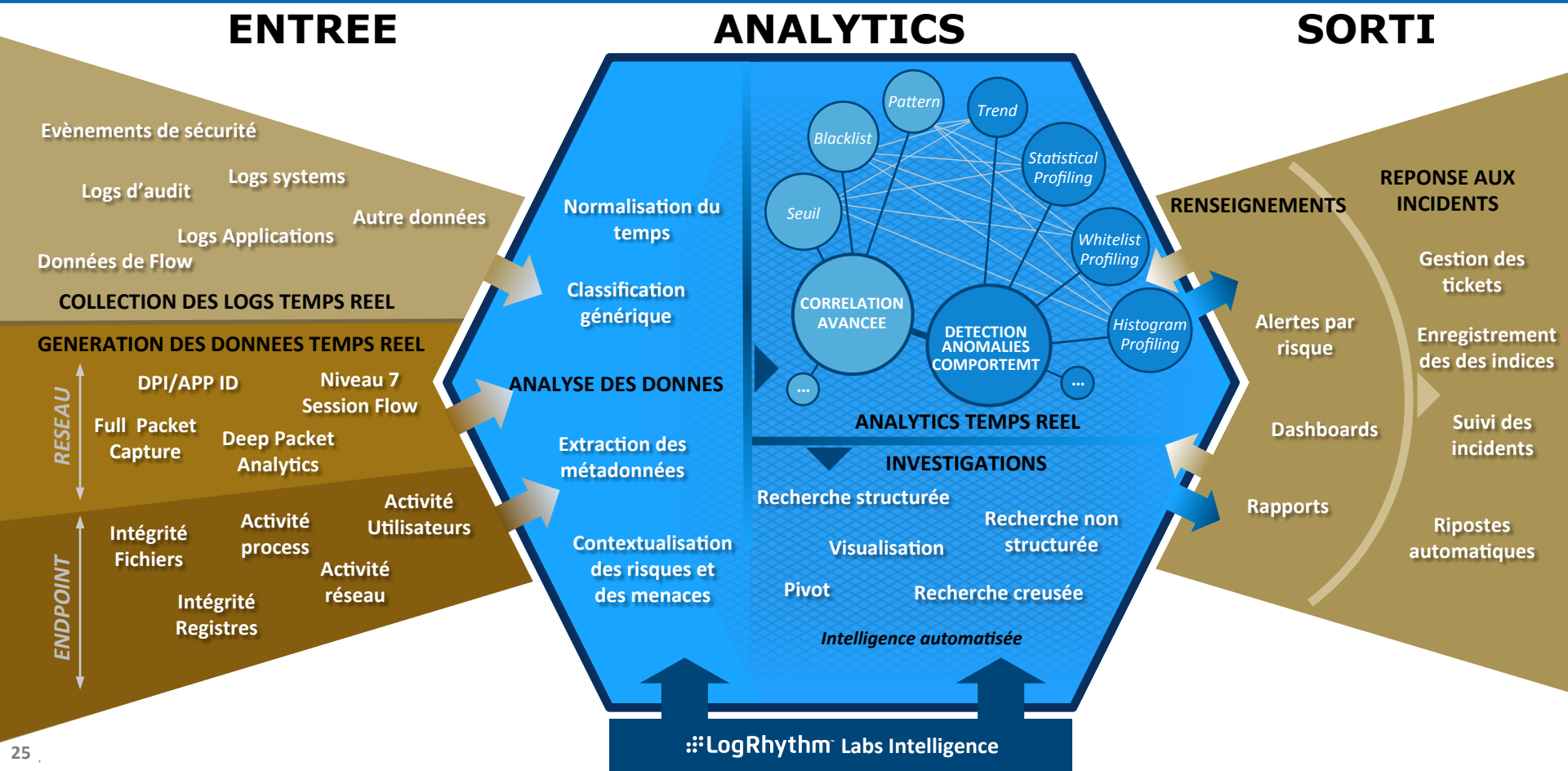
Cloture du dossier

Nouveautés

LogRhythm

- Gestion d'incident intégrée (nouveau module)
- Appliances de 4ème Génération: Plus de disque + Plus rapide
- Version 7
  - Elasticsearch (auparavant SQL server):
    - **Plus rapide**
    - **Plus puissant**
    - **Recherches non structurées** (Comme Splunk) **et structurées**
  - Meilleurs support des gros déploiements (+200K MPS)
  - Console Web améliorée
  - Réponses automatiques (SmartResponse) améliorées

Plateforme de “Security Intelligence” LogRhythm



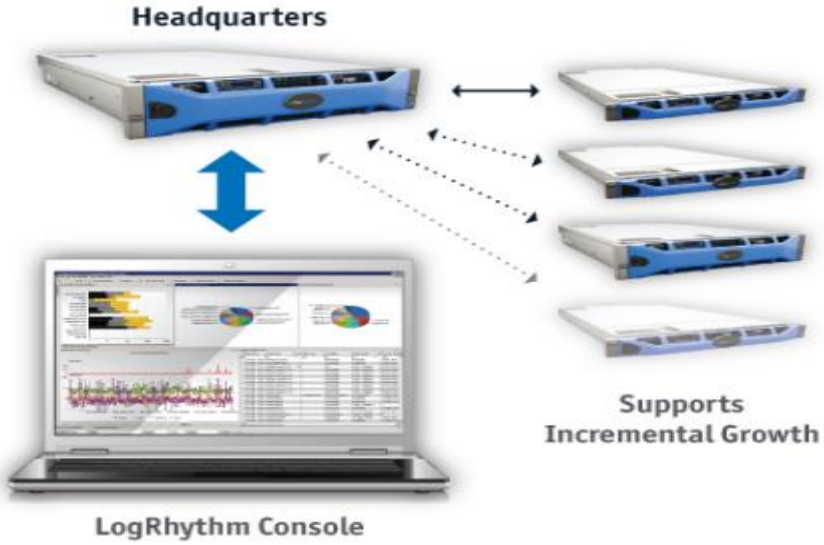
Options de Déploiement

All-in-one (Appliance XM)

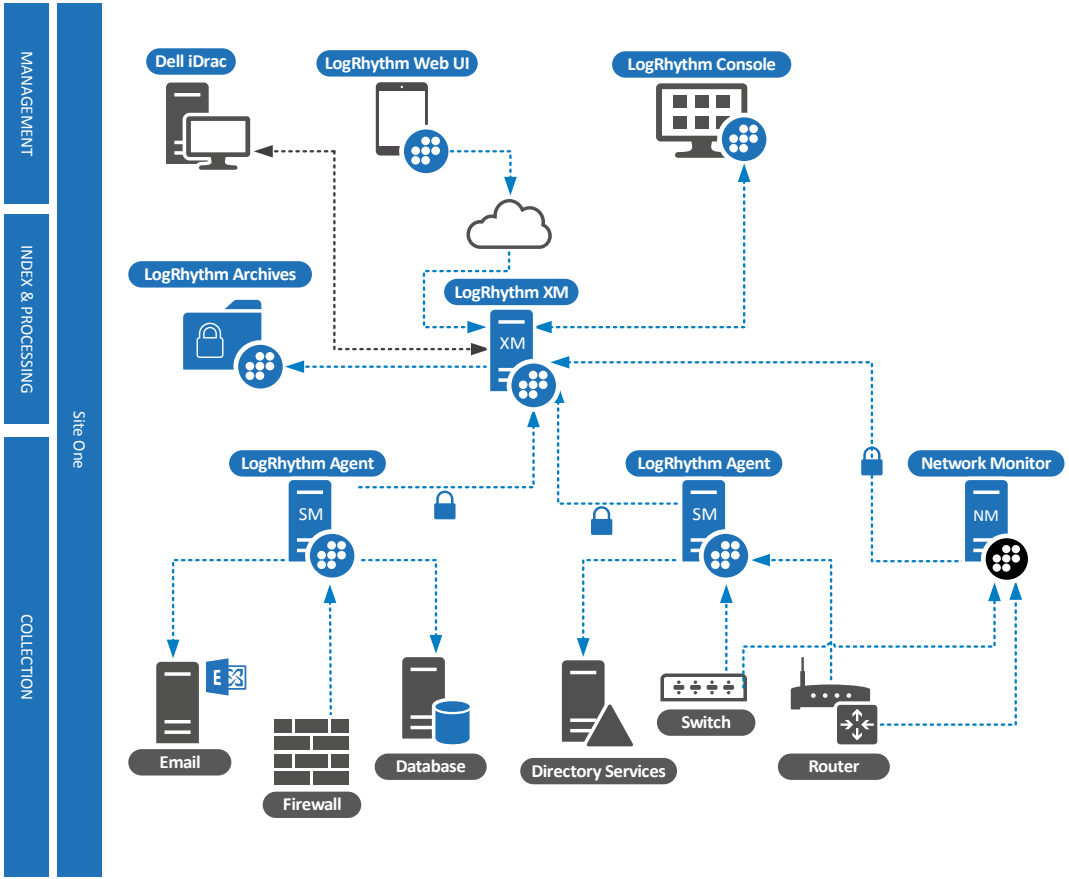
- Une Appliance Unique
- Deploiement simple
- Toutes les fonctions disponibles
- Solution évolutive

Appliances Dédiées, Software ou VM

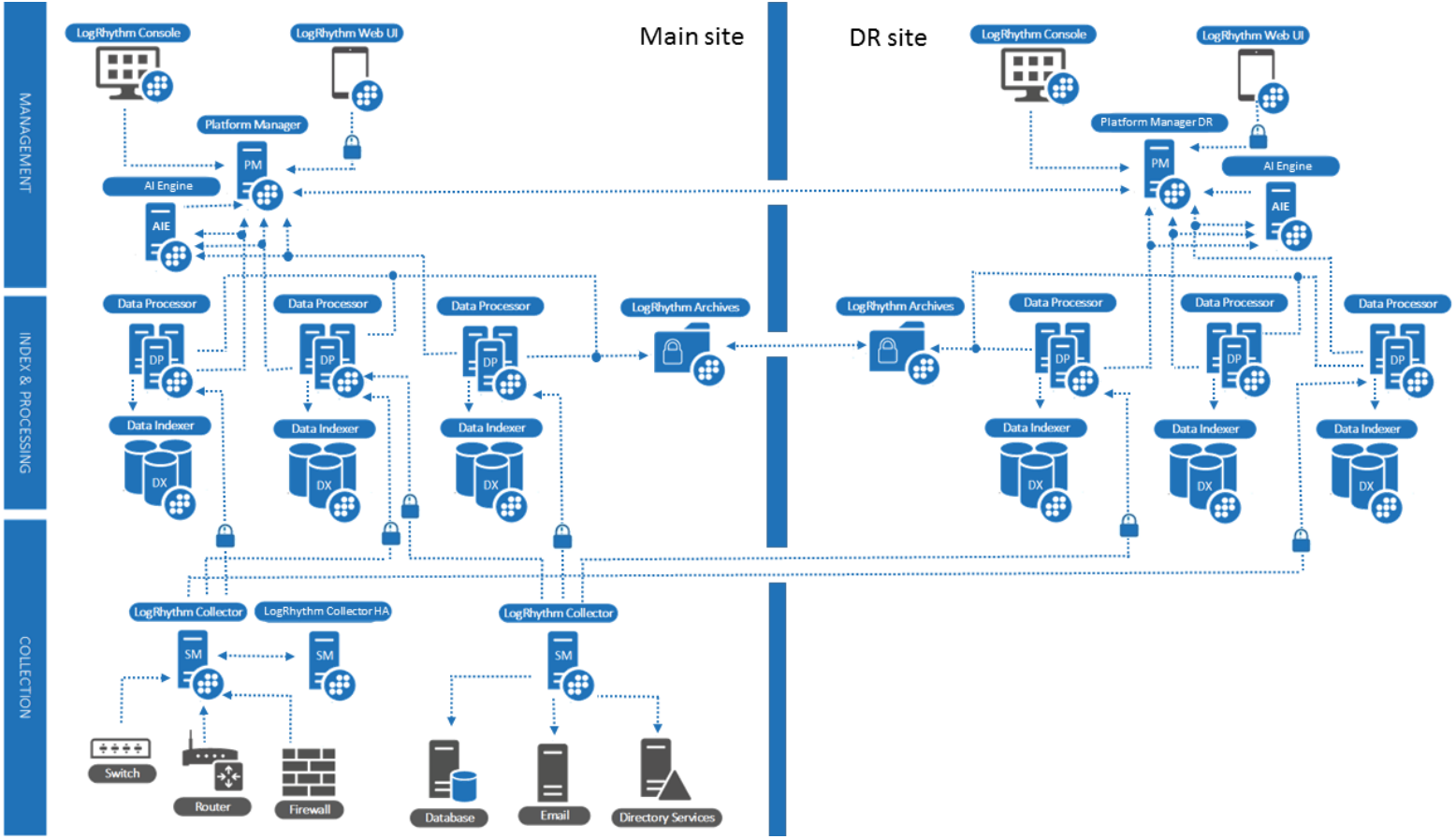
- Management Centralisé
- Support pour Environnements distribués
- Solution hautement évolutive



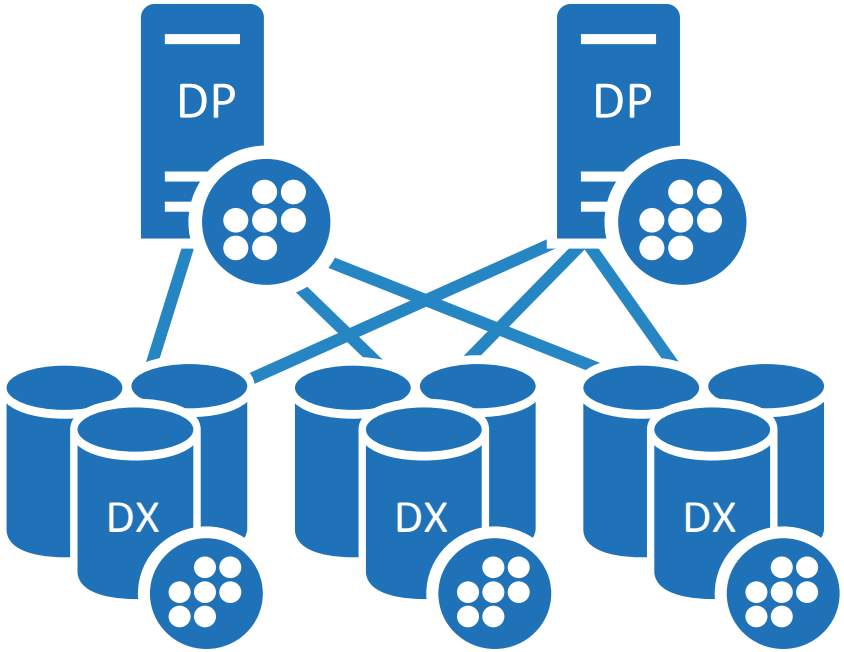
Architecture all in one



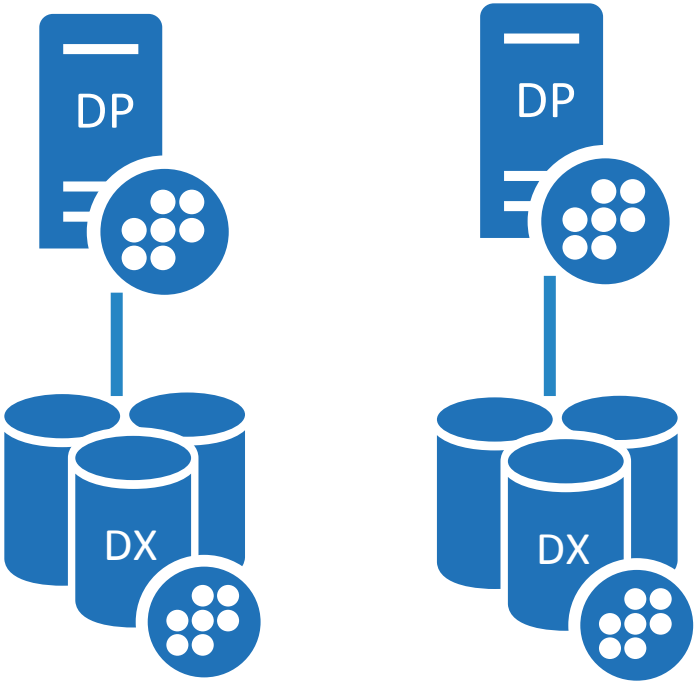
Distributed Architecture with HA and DR



Data indexer architecture options



Clustered Architecture



Pinned Architecture

Scalable architecture

LogRhythm

Hardware Solution	Max Indexing	License Processing	AIE Processing	Total Log Storage (TB)	Log TTL (Days)	Event TTL (Days)
XM4300 (6 Cores, 1.6 TB Storage)	750	250	1 000	1.3	22	90
XM6400 (12 Cores 6.8 TB Storage)	3 000	1 000	5 000	7	36	90
XM6400 (12 Cores 6.8 TB Storage) 1 x SA3450 (6TB storage extension)	3 000	2 500	5 000	12	26	90
PM5400 (6 Cores 2.4TB Storage) or XM6450 1 x DP5300 (6 Cores 0.5 TB Storage) 1 x DX5300 (6 Cores 4.6 TB Storage) 1 x SA3350 (4TB storage extension)	5 000	5 000	10 000	12	21	90
PM5400 (6 Cores 2.4TB Storage) 2 x DP5300 (6 Cores 0.5 TB Storage) 2 x DX5300 (6 Cores 4.6 TB Storage) 2 x SA3350 (4TB storage extension)	10 000	10 000	10 000	25	21	90
PM7400 (16 Cores 7.3 TB Storage 15K RPM) 7 x DP7400 (16 Cores 1.4 TB Storage) 7 x DX7400 (12 Cores 12.5 TB Storage) 15 x SA7470 (6TB storage extension) 1 x AIE7400 (32 Cores 1 TB Storage)	105 000	70 000	75 000	171	30	90

Hardware options

	Appliance Lines	PERFORMANCE RATES	Max Archiving Rates	Max Processing Rates	APPLIANCE SPECIFICATIONS	Chassis	CPU Physical / Physical + Virtual (HT)	Memory (Expandable)	Internal Storage (Usable/Raw)	Expandable To (Usable/Raw)
ALL-IN-ONE (XM) (Includes PM, DP, DX, AIE)	4301		10,000 MPS	1,000 MPS		1U	6 Core / 12 Core	64 GB	1.36 TB/2.17 TB	25.25 TB/28.23 TB
	6400		25,000 MPS	5,000 MPS		2U	12 Core / 24 Core	128 GB	6.79 TB/8.14 TB	30.68 TB/34.20 TB
DEDICATED PLATFORM MANAGER (PM) (Includes AIE license)	5400		N/A	N/A		1U	6 Core / 12 Core	128 GB	2.44 TB/4.89 TB	15.48 TB/30.95 TB
	7400		N/A	N/A		2U	16 Core / 32 Core	128 (256) GB	7.33 TB/13.57 TB	26.89 TB/52.66 TB
DEDICATED DATA PROCESSOR (DP)	5300		10,000 MPS	5,000 MPS		1U	6 Core / 12 Core	64 GB	556 GB/1.08 TB	24.43 TB/27.14 TB
	7400		50,000 MPS	15,000 MPS		1U	16 Core / 32 Core	128 (256) GB	1.08 TB/2.17 TB	24.97 TB/28.23 TB
DEDICATED DATA INDEXER (DX)	5300		N/A	N/A		1U	6 Core / 12 Core	64 GB	4.62 TB/7.06 TB	52.40 TB/59.19 TB
	7400		N/A	N/A		2U	12 Core / 24 Core	128 (256) GB	12.2 TB/13.57 TB	83.87 TB/91.76 TB
DEDICATED AI ENGINE (AIE)	5400		N/A	30,000 MPS		1U	16 Core / 32 Core	128 (256) GB	1.08 TB/2.17 TB	N/A
	7400		N/A	75,000 MPS		1U	32 Core / 64 Core	256 (512) GB	1.08 TB/2.17 TB	N/A
DATA COLLECTOR (DC)	3300		N/A	N/A		1U	4 Core	16 GB	278 GB/556 GB	N/A
NETWORK MONITOR (NM)	3300		N/A	1 Gbps		1U	10 Core / 20 Core	64 GB	1.9 TB/3.8 TB	25.9 TB/28.9 TB
	5400		N/A	2.5 Gbps		2U	24 Core / 48 Core	128 GB	12.5 TB/13.9 TB	60 TB/66 TB
WEB APPLIANCE	3300		N/A	N/A		1U	8 Core / 16 Core	32 GB	556 GB/1.08 TB	N/A

Expertise Embarquée: Security Modules

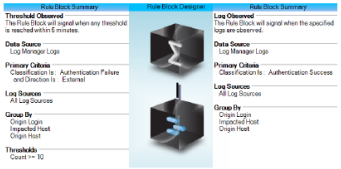
- Sécurité de base
- Surveillance des menaces du réseau
- Surveillance des menaces des utilisateurs
- Surveillance des menaces des serveurs et des postes
- Services de renseignement des menaces open source, ou du « Threat Intelligence Ecosystem »
- Top 20 des Contrôles Critiques du SANS Institute
- Monitoring des utilisateurs privilégiés
- Reconnaissance des premiers indicateurs des APTs
- Analyse des “Honeypots”
- Protection contre les fraudes

User Threat Analytics Premium Suite AI Engine Rules

This section lists describes the AI Engine rules included in the suite, including any additional configuration notes.

Compromise: Brute Force Auth

Gaining access to an internal account is often the first step in a malicious actor's efforts to pilfer an organization. Because software frequently uses default logins and many users have inadequate passwords, this is an extraordinarily effective method (change your default passwords!!). This rule detects a successful brute force authentication from an external source -- it first tracks multiple failed authentication attempts from the same account, origin host, and impacted host. Then connects that with a following successful authentication.



Log Sources

Minimum

» Active Directory or LDAP

Recommended

» Host Logs

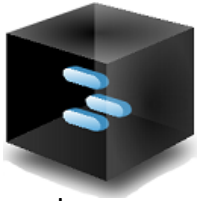
Knowledge Base Content

ID	Name
1	Compromise: Brute Force Auth

Actions

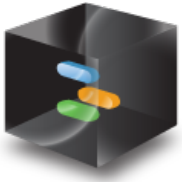
This rule fires when the same user account was seen failing authentication multiple times followed by an authentication success. In this case, it is vital to quickly contain the compromised account by disconnecting infected hosts, disabling the compromised account, and blocking the attacker's access -- organizations should have an incident response plan for a compromise. Also, after stopping the active attack, forensics will need to be conducted to insure that an implant isn't hidden in the network, information wasn't stolen, or other accounts were compromised.

Scénarios de correlation par Blocs

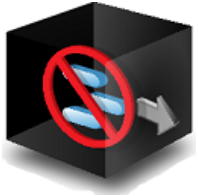


Log
Observé

Seuil
Observé



Valeur Unique
Observée



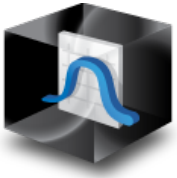
Log Pas
Observé

Seuil Pas
Observé

Valeur Unique
Pas Observée

Liste
Blanche

Tendance



Statistique

Console Web pour les analystes

LogRhythm | Dashboards | Alarms | Cases | Searches | Search...

Current Case: Case Nicolas 1

Open

P3

Case Nicolas 1
AGE ~ 22H 22M
OWNER Stricher, Nicolas

Evidence | History

ALARMS

Stricher, Nicolas added an alarm Jan 7 2:40pm

New

97 RISK

AIE: Internal: Compromise: APT Behaviour Detected >
Global Entity
Jan 7 12:06pm
id: 13760

SmartResponse™ Not Available

Stricher, Nicolas added an alarm Jan 7 2:40pm

New

72 RISK

AIE: Ext:Acnt Comp:Concurrent Auth From Multiple Locations >
Global Entity
Jan 7 12:25pm
id: 13763

SmartResponse™ Approve Deny

LOGS (view in analyzer)

Stricher, Nicolas added a set of logs Jan 6 4:29pm

Search of nicolas.stricher logs (393 logs)

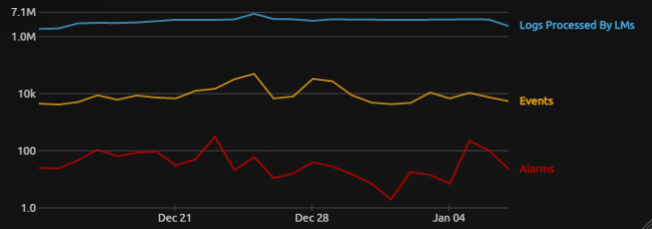
NOTES

Stricher, Nicolas added a note Jan 6 4:28pm

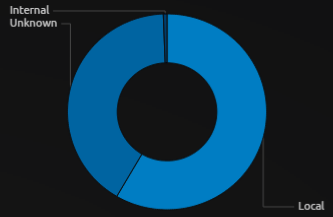
Add Note | Add Logs | New Case

Live Data

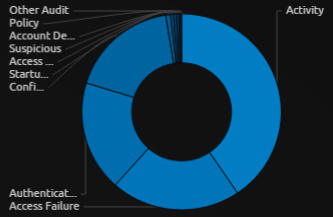
Logs, Events, Alarms by Day Past 30 Days



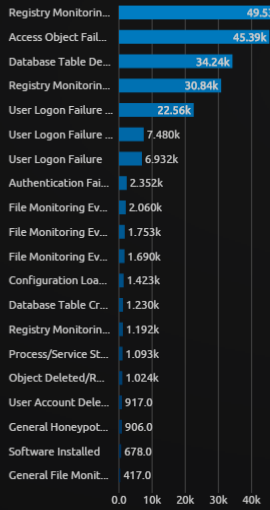
Direction Last 15d 3h



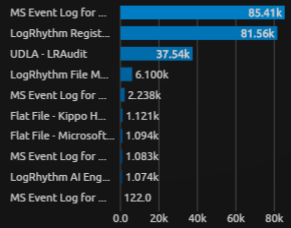
Top Log Classifications Last 15d 3h



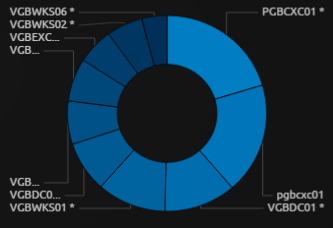
Top Common Events Last 15d 3h



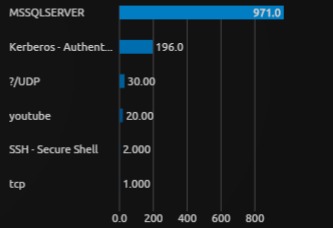
Top Log Source Types Last 15d 3h



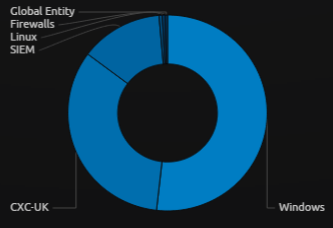
Top Impacted Hosts Last 15d 3h



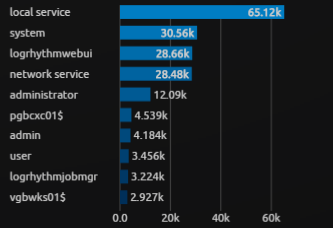
Top Impacted Applications Last 15d 3h



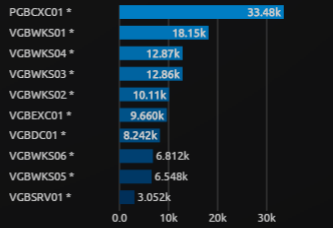
Top Impacted Entities Last 15d 3h



Top Origin Users Last 15d 3h



Top Origin Hosts Last 15d 3h



Top Origin Countries Last 15d 3h

LOGS | TASKS

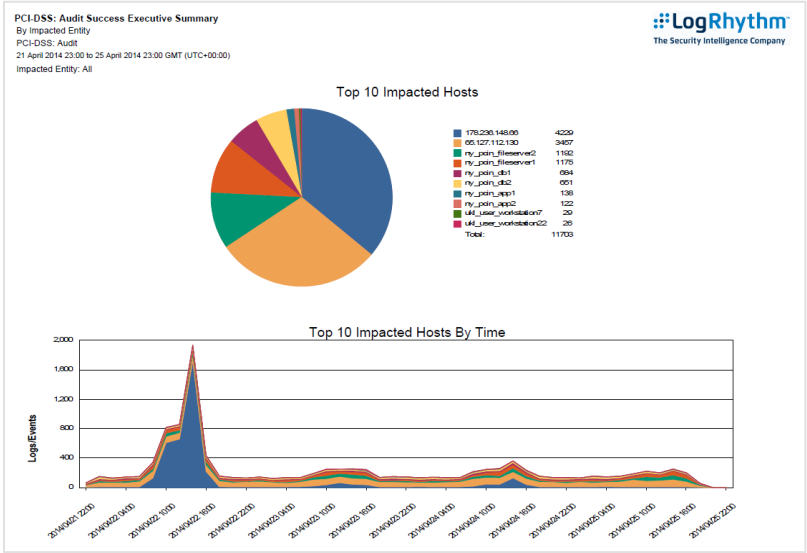
Les défis

- PME:
  - Prix d'entrée plus élevé que les solutions de gestion de log
  - **Solution: Proposer la version logicielle et en vendant la valeur de LR**
- Grand comptes:
  - Petit éditeur par rapport aux principaux concurrents
  - Peu de références grand compte en France (Gemalto, AXA, Verifone)
  - **Solution: Parler du Gartner 2015 et du SANS Institute**
- Intégrateurs:
  - Relations existantes avec RSA, McAfee, HP, Splunk
  -

Automatisation et Assurance de la Conformité

- ISO 27001
- PCI –DSS
- SANS TOP 20 Critical Controls
- GPG 13

ISO/IEC 27001:2005



- NIST 800-53
- SOX
- HIPAA
- NERC
- NEI
- FISMA
- DoDI
- GCSX

Plus de 2500 Clients sur 6 continents

LogRhythm

RETAIL

HEALTHCARE

FINANCIAL

OTHER

EDUCATION

GOVERNMENT

ENERGY

Affaires majeures gagnées en Europe en 2015

- UK – Industrie aéronautique: 5.8M Dollars
- UK – Ministère infogéré: 1.3M Dollars
- Allemagne – Editeur: 270K Euros
- France - Organisation Internationale: 150K Euros
- Turquie – Institut financier: 105K Dollars
- Tunisie – Banque: 86K Euros

Leadership Validation

LogRhythm

Industry Analysts

Gartner
A 2012-2015 LEADER
SIEM Magic Quadrant

FROST & SULLIVAN
2013 Global SIEM/LM
Market Penetration Leadership Award

BEST-IN-CLASS 2014-15 DCIG BUYER'S GUIDE SIEM APPLIANCE

VENDOR LANDSCAPE AWARD CHAMPION INFO-TECH research group

SIEM 2014-15 DCIG BUYER'S GUIDE APPLIANCE

Company Awards

TOP 100 WORKPLACES 2014 THE DENVER POST

TOP 100 WORKPLACES 2015 THE DENVER POST

UNITED STATES PATENT AND TRADEMARK OFFICE DEPARTMENT OF COMMERCE

APEX COLORADO TECHNOLOGY ASSOCIATION
Company of the Year

Certifications & Validations

CoN U.S.ARMY

FIPS VALIDATED LEVEL 1 140-2

EAL2 Common Criteria CERTIFIED

ONC Certified HIT

Industry Awards

SANS BEST OF 2014 WINNER IN SIEM

INFORMATION SECURITY READERS' CHOICE AWARDS WINNER 2014

SC MAGAZINE AWARDS 2015 WINNER Honored in the U.S.

SC MAGAZINE ★★★★★

SC MAGAZINE RECOMMENDED

BEST PRODUCT FORENSICS SOLUTION 2014 CDM

MOST INNOVATIVE SECURITY INFORMATION EVENT MANAGEMENT (SIEM) SOLUTION 2014 CDM

LogRhythm™

The Security Intelligence Company

LogRhythm®
The Security Intelligence Company