



Pitch Deck

Pierre-Adrien Ducasse
Marc Molina
Experts IA et cybersécurité

mai 2018

L'équipe.



Marc Molina
CTO
GRENOBLE INP

Ministère des Armées :

- **Lead Data Scientist** sur la prédition des cyber-attaques.
- **Lead Architect** des systèmes de traitements massifs distribués pour la cyber-sécurité.



Pierre-Adrien Ducasse
CEO
Imperial College/ENSEEIHT

Ministère des Armées :

- **Lead Data Scientist** sur la détection des entités malveillantes.
- **Project manager** sur la rénovation des systèmes de traitements massifs distribués pour la cyber-sécurité.



“The goal is to turn data into information, and information into insight.”

— Carly Fiorina, Former CEO of HP

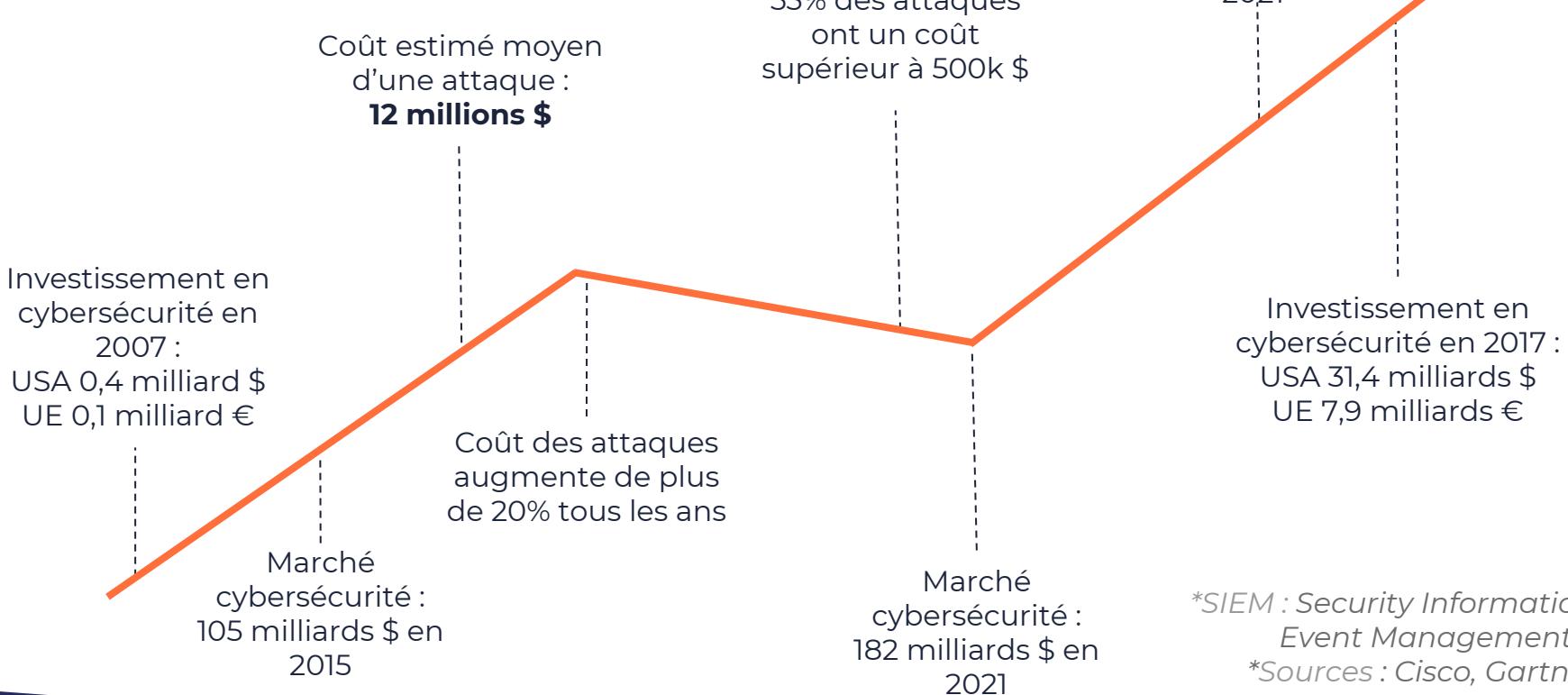
“War is ninety percent information.”

— Napoléon Bonaparte

“It is time for cybersecurity to use data!”

— Datak

Le marché.



*SIEM : Security Information and Event Management

*Sources : Cisco, Gartner, Accenture.

Le marché.

780 attaques graves dévoilées en 2015



Le temps moyen de détection d'une compromission grave est de **239 jours** en 2015

90% des attaques suivent le **même mode opératoire**

Cisco recommande la mise en place de mécanismes de **détection basés sur le ML** en 2018



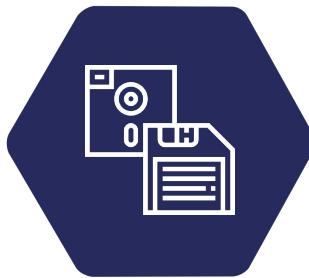
92% des entreprises voient de la **valeur** dans l'utilisation du ML en cybersécurité

34% des entreprises croient **totalemen**t en l'IA pour améliorer la sécurité

Sources : Cisco, Gartner, Accenture.

Le problème.

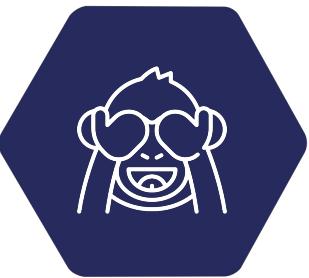
UN PROBLÈME À TROIS NIVEAUX



Les technologies utilisées
sont dépassées.



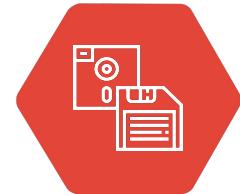
L'expérience utilisateur
est difficile.



La qualité des détections
reste très perfectible.

Le problème.

LA TECHNOLOGIE



Les SIEM dits “classiques” :

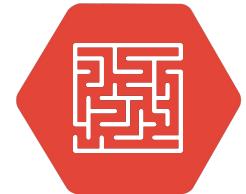


Les SIEM dits “nouvelle génération” :

- peu nombreux ;
- très difficiles à déployer ;
- pas spécialement dédiés à la cybersécurité ;
- souvent plus coûteux que les solutions dites *classiques*.

Le problème.

L'EXPÉRIENCE UTILISATEUR



Les SIEM du marché :



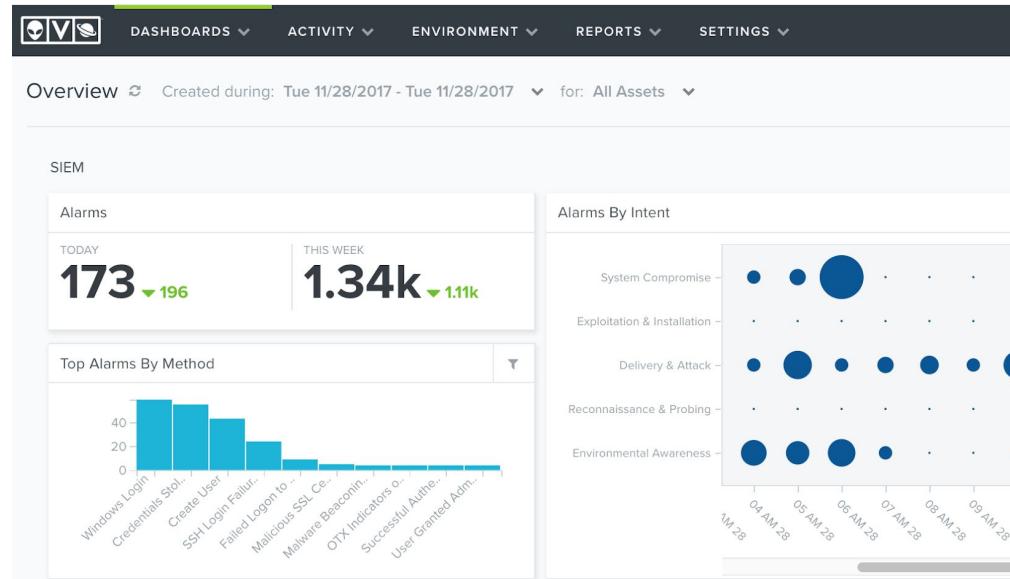
Ressources humaines



Usine à gaz



Syndrome de la fausse alarme



Le problème.

LES DÉTECTIONS



Les SIEM dits “classiques” :

- levées de milliers d’alertes qui correspondent rarement à un réel besoin d’intervention ;
- manque d’intelligence pour des remontées d’alertes pertinentes ;
- détection des attaques connues/cadrées dans un bruit de faux positifs.

Les SIEM dits “nouvelle génération” :

- capacités réelles opaques ;
- beaucoup de *buzzwords* mais whitepapers souvent pauvres scientifiquement ;
- mise en avant des détections mais manque d’intelligence artificielle pour permettre la prédiction.

The screenshot shows the Splunk Enterprise Security interface under the "Incident Review" tab. At the top, there's a navigation bar with tabs: Security Posture, Incident Review (which is active), Investigations, Glass Tables, Security Intelligence, and Security Domains. Below the navigation is a large red box titled "Incident Review" containing a summary of incident counts by urgency level:

Urgency	Count
Critical	0
High	193
Medium	365
Low	0
Info	0

Below the summary are several search and filter fields: Status (All), Correlation Search Name, Owner (All), Search, Security Domain (All), Time | Associations? (Last 24 hours), and a Tag field.

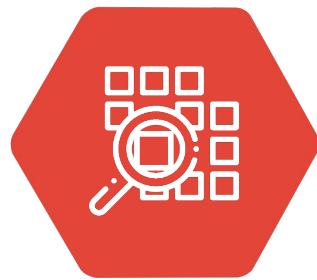
The screenshot shows the IBM QRadar Security Intelligence interface under the "Quick Insights" tab. At the top, there's a navigation bar with tabs: Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, and Admin. Below the navigation is a "Quick Insights" section with two main metrics:

- Monitored Users: 3.6k
- Current High Risk Users: 3.5k

Below these metrics is a chart titled "System Score (Last Day)" with a value of 7.71M. There are also sections for "Risk Categ" and "Risk Categ".

Notre vision.

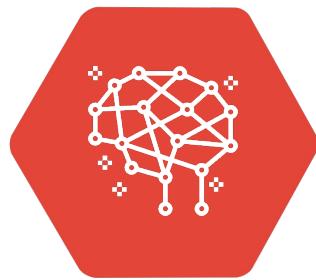
UNE SOLUTION COMPLÈTE



Datak utilise des technologies
à l'état de l'art.



Datak a été pensé pour les
analystes et les experts.



Datak exploite l'intelligence
artificielle pour protéger les
systèmes d'information.

Notre vision.

LA TECHNOLOGIE



CONTENU
CONFIDENTIEL

Notre vision.

LA TECHNOLOGIE



CONTENU
CONFIDENTIEL

Notre vision.

LA TECHNOLOGIE



CONTENU
CONFIDENTIEL

Notre vision.

L'EXPÉRIENCE UTILISATEUR

Datak est une solution :



Simple

intégration & scalabilité



Claire

tarification & exploitation



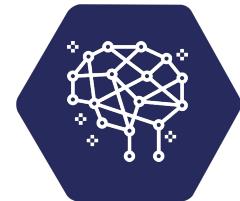
Avancée

technologies & algorithmes



Notre vision.

DÉTECTION ET PROTECTION



Les points forts de Datak sont :



Les données



**La connaissance
en IA**



**Le savoir-faire en
sécurité**

Les domaines de supervision maîtrisés sont :

- Vulnerability Center ;
- IOC real time detection ;
- DNS monitoring ;
- NIDS alert monitoring ;
- URL malicious prediction ;
- HIDS alert monitoring;
- Authentication anomaly detection ;

- Windows event monitoring ;
- Web app monitoring ;
- Netflow monitoring ;
- Antivirus alert correlation ;
- *Attack prediction* ;
- *User entity behaviour analytics*.

L'opportunité.

Le lancement de ce type de service novateur est aujourd'hui facilité par plusieurs facteurs :

MATURITÉ TECHNOLOGIQUE

- l'écosystème des technologies Big Data est aujourd'hui mature et performant.

L'ENVOI DE LA DATA SCIENCE

- les données sont les nouvelles matières premières des entreprises ;
- la data science a fait ses preuves dans de nombreux domaines ;
- les décideurs savent qu'il faut prendre le virage de la data dans tous les secteurs y compris la cybersécurité.

L'EXPLOSION DE LA CYBERMENACE

- aujourd'hui même les systèmes les plus critiques sont informatisés ;
- un manque de connaissances et de moyens rendent ces systèmes vulnérables ;
- l'impunité vis à vis des hackeurs renforce la menace.



Le produit.

“Une courte démonstration vaut mieux qu'un long argumentaire.”

— Marc Roussel

Business model.



Une tarification simple claire et précise par abonnement aux features.



Deux offres distinctes *cloud* et *on premise* pour satisfaire tous les clients.

Business model.

EXEMPLE DE TARIFICATION MENSUELLE

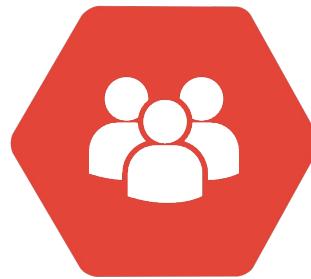
CONTENU
CONFIDENTIEL

Business model.

DES BÉNÉFICES AU RENDEZ-VOUS



Une marge brute aux alentours de 50% selon les abonnements souscrits.



Un chiffre d'affaire par ingénieur R&D de 500k€ d'ici 3 ans.

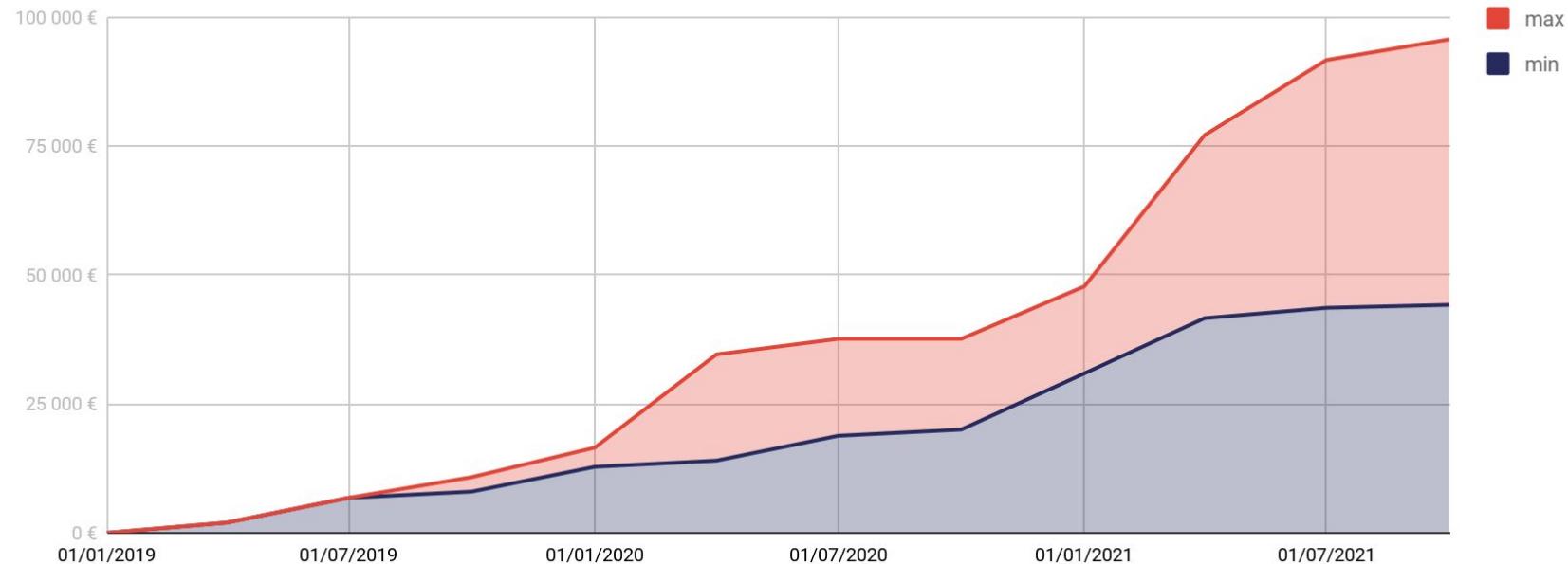


Une projection de MRR comprise entre 45k€ et 100k€ d'ici 3 ans.

Business model.

MONTHLY RECURRING REVENUE

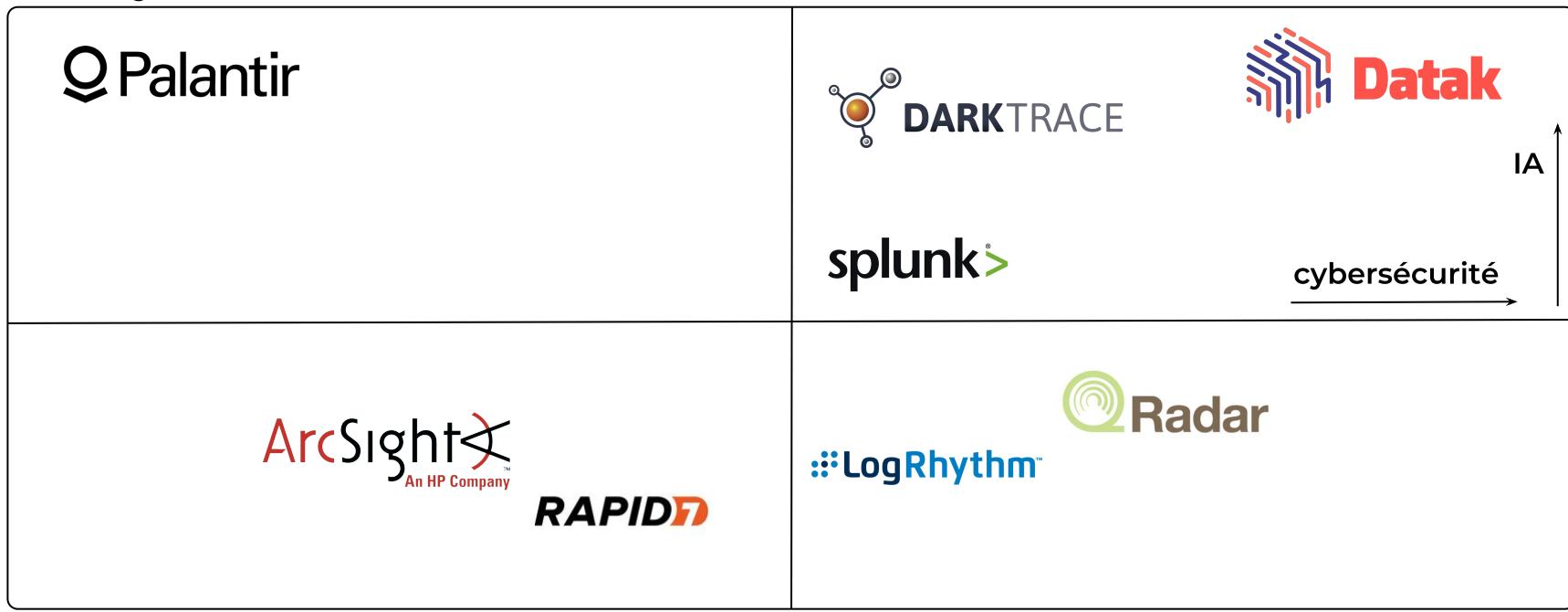
Projected MRR



Matrice concurrentielle.

challengers

leaders



niche players

visionaries

Roadmap.

CONTENU
CONFIDENTIEL



“The world is changing.
Big will not beat small
anymore. It will be the
fast beating the slow.”

— Rupert Murdoch



Points de contact.



Pierre-Adrien Ducasse (CEO) : pierre-adrien.ducasse@getdatak.com

Marc Molina (CTO) : marc.molina@getdatak.com



Pierre-Adrien Ducasse (CEO) : [+33 6 88 09 93 77](tel:+33688099377)

Marc Molina (CTO) : [+33 6 63 85 66 15](tel:+33663856615)