BEYOND THE KNOWN THREATS

JOHNATHAN PARTOUCHE, CEO
JP@ORISECURE.COM

Team

Jonathan Partouche

Founder & CEO

Experience

Israeli Aerospace Industries, Scientific Research

Andy Butterworth

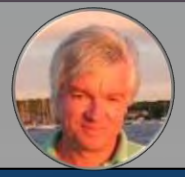
Head of Operation

Experience

UK Military / CTO / CISO

Jean Pierre Decamps

Head of Partnerships



Experience

Director IBM Innovation Center 15Y+

Stefan Norberg

Head of Business Dev

Experience

International Business Development Expert

Stephen Anning

Head of Research Ops

Experience

UK Military Intelligence / IBM Security

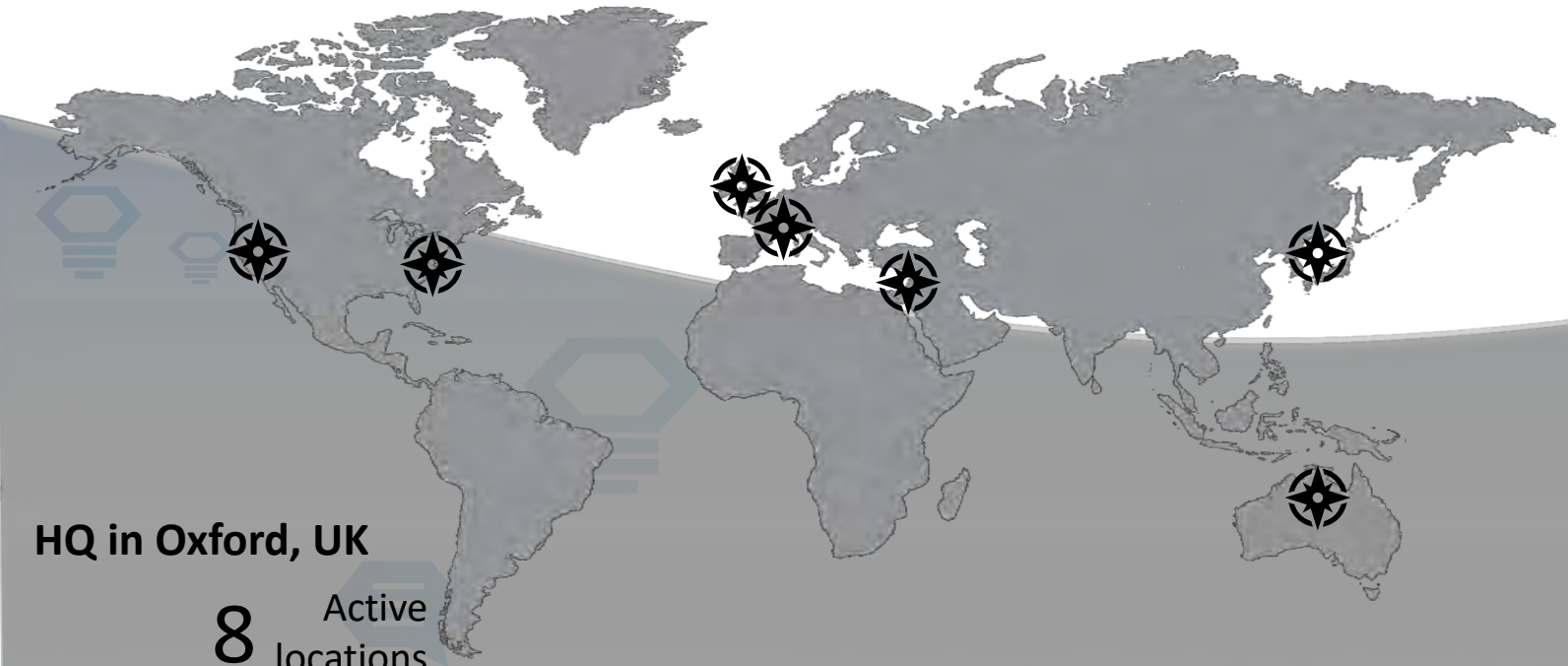
Mehdi Bouzoubaa

Head of Sales EMEA

Experience

Thales Security & Communication

Global footprint to support businesses



HQ in Oxford, UK

8 Active locations

Created |2014

ISRAEL AEROSPACE INDUSTRIES

accenture
High performance. Delivered.

SYSTRA

Gartner

European Institute of Innovation & Technology

ISO 9001 QUALITY + TL 9000 ICT + ISO 14001 ENVIRONMENTAL + ISO 27001 SECURITY Coming Soon!

UNICOM Engineering, Inc.
A Division of UNICOM Global

Customers

Home Office

Northamptonshire Police

SIEMENS
Ingenuity for life

BARCLAYS

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTERE DE L'INTERIEUR, DE L'OUTRE-MER ET DES COLLECTIVITES TERRITORIALES

ENGIE
by people for people

GRTgaz

BANK OF ENGLAND

BT

Deutsche Telekom

Bank of America

Telefónica

citi

Deutsche Bank

U.S. DEPARTMENT OF HOMELAND SECURITY

DCNS

UBS

SYSTRA

ferrovial

Our Disruption & innovation

INTELLIGENCE

Skilled manpower created automatically

INCREASINGLY VULNERABLE

Better security through integrated solution

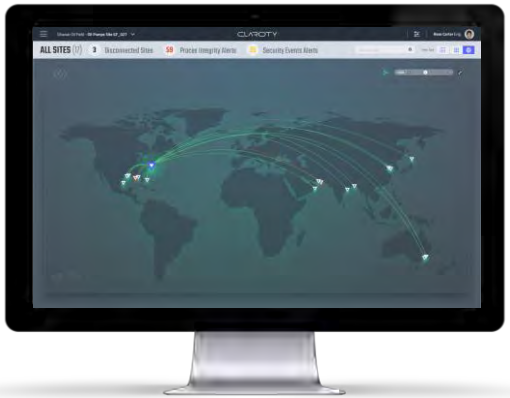
LACK OF THREAT PREDICTIVE ANALYSIS

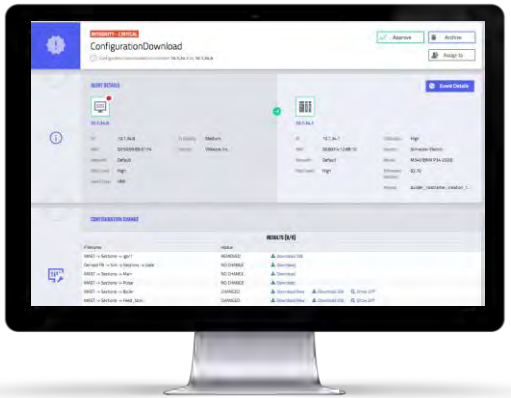
Automatic integration across organization

INSUFFICIENT VISIBILITY

Simplicity as a service

Modular, Flexible Plug-&-Play





Our Disruption & innovation

INTELLIGENCE

Require relevant threat intelligence avoiding false alarms and noisy alerts

Focus on Human Factor by empowering employees with technology

INCREASINGLY VULNERABLE

Assets are increasingly complex and connected.

Create a prosperous & secure environment

LACK OF THREAT PREDICTIVE ANALYSIS

IT Security, plant operations & teams

Use all source analysis to hunt for attackers and predict threats

INSUFFICIENT VISIBILITY

Enterprise IT security solutions not designed to see or protect OT/IT assets.

Enabling Business Resilience through skill transfers and automation

Next steps

Early adopters

Seeking solution focused on prevention including other methodologies than detection based

CISOs with key issues to be solved

Seeking a hyper-effective, cross-assets solution saving time & resources through automation

Willing to uncover problems and test the solutions

Seeking to understand financial impact & existing defensive measures against specific attack vectors and attackers' profiles

Ready to deploy

Seeking one cost with an organic platform growing with complexity of needs

PAY-AS-YOU-GROW Functionalities

ORISECURE FOUNDATION

IT INFRASTRUCTURE PROTECTION

SecureAPI | ProtectKeyboard | SecureMedia | ProtectMobile | SecureEmail | ProtectID

Undercover operation information gathering

ORISECURE AUDIT

VULNERABILITY & ANOMALY DETECTION	META ANALYSIS OF CYBER POSTURE	PATTERN DETECTION & PREDICTIVE ANALYSIS	GOVERNANCE & ENTERPRISE VISIBILITY
ICT/ICS insights, Network visibility	Maturity of Security Controls, Risk Assesments	Financial impacts, Geo/industrial threat Trends	Assess controls compliance, assets auto-discovery remotely

Dynamic and agile case working

ORISECURE INTELLIGENCE

AUTOMATIC COLLECTION	THREAT PREDICTIVE	IDENTIFY ATTACKERS	IDENTIFY ATTACK METHODS
All sources analysis (OSINT, Deep, Dark, OT)	Behavior Profiling, Mass Data Collection, Forecasting & Prediction	Covert monitoring and surveillance online	Eavesdropping on hackers activities

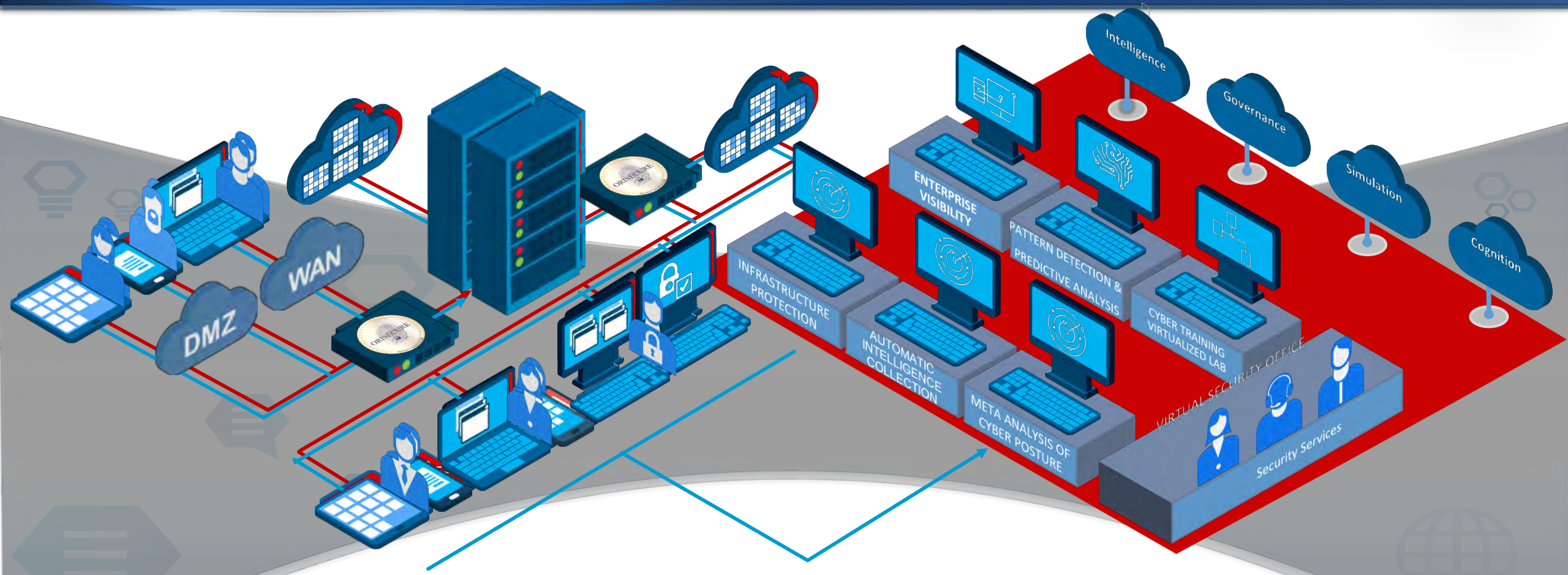
Quick Intelligence gathering

ORISECURE CYBER-DEFENSE

VIRTUAL CYBER LAB	SIMULATION SCENARIOS	VIRTUAL LEARNING MANAGEMENT SYSTEM	REPORTING
Virtualized, private-cloud, Scalable, certified data-center hardware specifications	Comprehensive Cyber Warfare Curriculum	Cyber Learning Management System (CLMS)	Enables organizations to start training cyber teams within weeks.

Cross departmental collaboration

Technical architecture



Focus on Human Factor by empowering employees with technology

Create a prosperous & secure environment

Use all source analysis to hunt for attackers and predict threats

Enabling Business Resilience through skill transfers and automation

BEYOND THE KNOWN THREATS

JOHNATHAN PARTOUCHE, CEO
JP@ORISECURE.COM

Projet

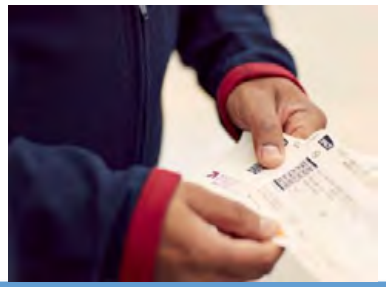
SNCF
FRAUDES ET ATTENTATS

SNCF
Risque de fraudes
Plan Anti-Fraudes & Chiffres clés

- Fraudes
  - Plan et mesures anti-fraudes
  - Top 20 des gares
  - Caractéristiques billets et contrôles

- Risque d'attentats
  - Collecte Web (Actus, stades, gares, critères de recherche).





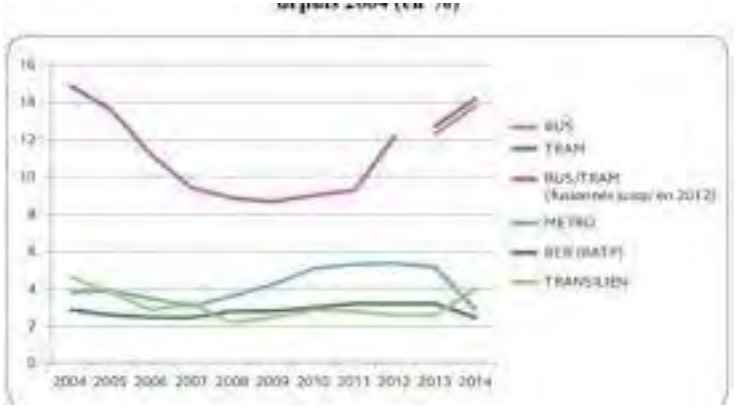
SNCF
Risque de fraudes
Plan Anti-Fraudes & Chiffres clés

Un plan renforcé

•la réduction de la durée de validité des billets sans réservation obligatoire à 7 jours depuis sept. 2014
•le développement de valideurs sans-contact avant l'accès aux trains d'ici à 2017
•l'évolution du montant des régularisations à bord et des amendes en mars 2015
•l'amélioration du taux de recouvrement des procès-verbaux à partir de 2015

Chiffres clés

•10 000 chefs de bord SNCF
•2 800 agents de la sûreté générale SNCF
•22 000 multirécidivistes au délit de fraude d'habitude en 2014
•2,5 millions de PV établis en 2014



SNCF
Introduction
Top 20 : Liste des plus grandes gares

Ville	Gare	Nombre de voies à quai	Voyageurs SNCF (millions/an)
Paris	Gare du Nord	31	201,8 (2014)
Paris	Gare Saint-Lazare	27	102,8 (2014)
Paris	Gare de Lyon	28	95,9 (2014)
Paris	Gare d'Austerlitz	25	22,9 (2014)
Paris	Gare Montparnasse	28	51,2 (2014)
Paris	Gare de Paris Est	29	30,5 (2014)
Montigny-le-Bretonneux	Gare de Saint-Quentin-en-Yvelines - Montigny-le-Bretonneux	6	25,5 (2010)1
Lille	Gare de Lille - Flandres	17	21,0 (2012)2
Paris	Gare de Magenta	4	16,6 (2005)3
Strasbourg	Gare de Strasbourg	13	16,1 (2011)4
Ermont	Gare d'Ermont - Eaubonne	8	15,85 (2008)
Lyon	Gare de la Part Dieu	6	28,6 (2014)
Marseille	Gare Saint-Charles	15	11,5 (2013)6
Nantes	Gare de Nantes	16	11,0 (2012) 7
Bordeaux	Gare de Bordeaux-Saint-Jean	15	11,0 (2012)8
Rennes	Gare de Rennes	10	9,608 (2013)9
Nancy	Gare de Nancy-Ville	11	9,0 (2014)10
Toulouse	Gare de Toulouse-Matabiau	13	8,619 (2010) 11
Nice	Gare de Nice-Ville	9	8,5 (2010)12
Grenoble	Gare de Grenoble	7	7,0 (2008) 13

SNCF
Risque de fraudes
Plan Anti-Fraudes + Actions

La SNCF passe à l'attaque contre la fraude

http://www.ladepeche.fr/article/2016/01/11/2253515-la-sncf-passe-a-l-attaque-contre-la-fraude.html
Publié le 11/01/2016 à 11:43, Mis à jour le 11/01/2016 à 11:51

•300 millions d'euros de manque à gagner pour la SNCF.

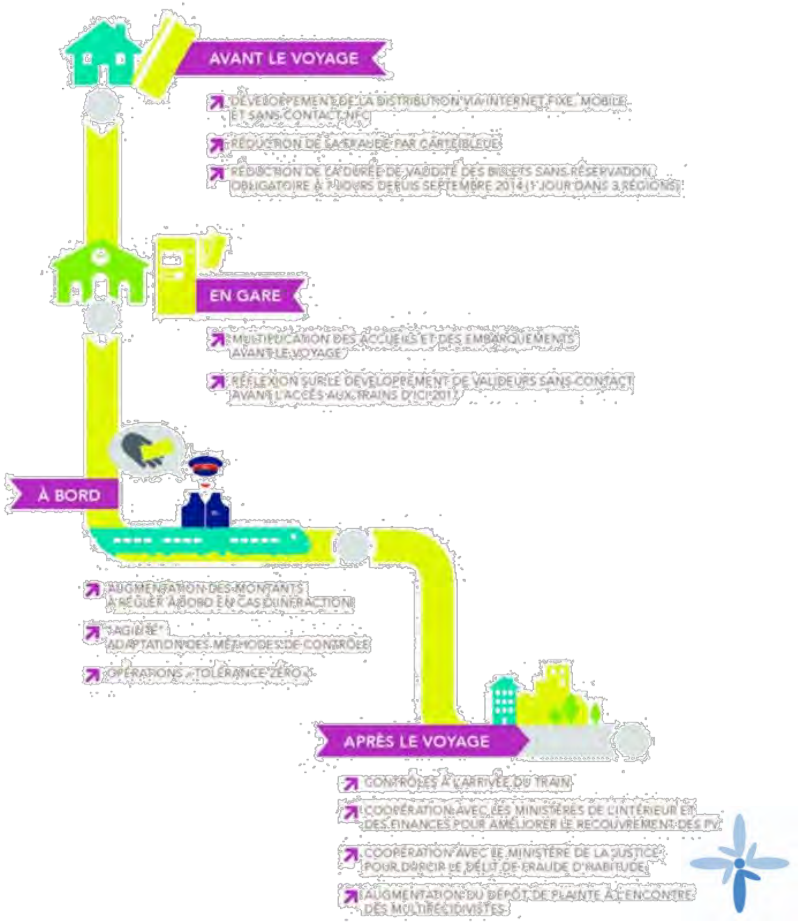
•Dispositif "Test" mis en place à partir du 11 janvier dans 2 gares : Paris-Montparnasse et Marseille-Saint-Charles.

•Objectif : munir les principales gares TGV d'ici 2017.

Président de la SNCF: Guillaume Pepy
•Gardes de la SNCF, en civil et armés sur certains trains
•Possibilité de demander à un voyageur d'ouvrir son sac dans une gare, alors qu'aujourd'hui ça n'est pas possible.

Un plan d'action pour faire reculer la fraude

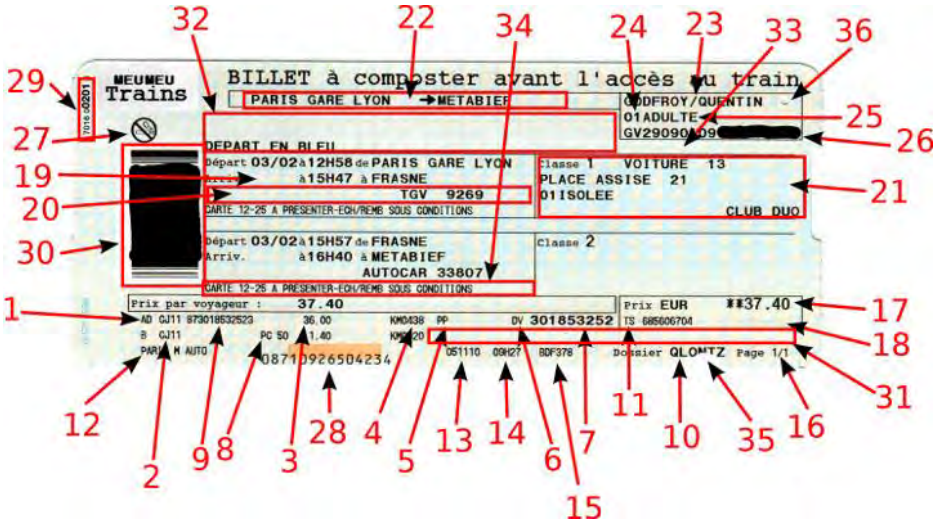
http://www.sncf.com/fr/presse/fil-info/plan-anti-fraude-transports-71235



SNCF
Risque de fraudes
Les billets SNCF – Une mine d'informations

« Comment sont contrôlés les billets des passagers ? »

Voir légende en commentaire ou suivre le lien suivant :
http://tarification.blogspot.fr/2011_11_01_archive.html



Quels sont les éléments contrôler ?

Quels sont les formats des données contrôlées (ex: IQR) ?

Quel appareil est utilisé (Constructeur/Fiches Techniques) ?
N'est-il pas possible de les reproduire afin de les rendre valides aux yeux des contrôleurs ?

SNCF
Risque de fraudes
Les billets SNCF – Une mine d'informations

CONTRÔLE INFORMATISÉ DES BILLETS : PEUT MIEUX FAIRE !

Informatique Technologie | Mots clés: code à barres franco-allemand Psion SNCF

Déplacement hier en Alsace, pour visiter l'usine AsteelFlash de Duttlenheim, qui fabrique des récepteurs TNT par satellite pour le compte d'Aston. Je voyage dans un TGV franco-allemand, à destination de Karlsruhe. Désormais, l'équipe de bord est mixte. J'approuve l'initiative. Mais il y a encore quelques progrès à réaliser. Le premier contrôleur à se présenter est allemand. « Il va falloir attendre mon collègue, m'indique-t-il. Mon appareil ne peut pas lire votre billet électronique, nous n'avons pas le même système ».

J'en profite, alors que le contrôleur français pointe le lecteur de code à barres pour engager la conversation et jeter un œil sur le terminal utilisé, un Workabout Pro de Psion Teklogix. « Ce n'est pas terrible, reconnaît mon interlocuteur. Le système est bogué, et plante souvent. C'est parce qu'il y a trop de choses dedans. J'ai par exemple accès à des plans de villes de pays par lequel notre TGV ne passe pas… ». Je suis par certain que l'explication technique soit pertinente. Si les plans sont stockés dans de la mémoire statique, il n'y a pas raison qu'un « trop plein » génère des disfonctionnements. J'imagine surtout que les développeurs de

Applications codes à barres
- Lecture laser ID en standard, longue portée ou réglage automatique de la portée
- Imageur linéaire 1D
- Imageur 2D
- Poignée en option
- Note: ces modules sont configurés en usine ou à la demande par l'utilisateur

workabout Pro³

Processeur et Mémoire
- PXA270 624 MHz
- 1 Go Flash ROM, 256 Mo RAM

Système d'exploitation
- Windows® CE 5
- Windows Mobile® 6.1 Classic, Professional

Logiciels
- Internet Explorer® 6.0
- Psion Voice Dialer et Contacts Manager incluant Windows CE 5
- PTX Connect VoIP
- Emulation Terminal : IBM 5250, IBM 3270, HP2392, ANSI et TESS
- Gestion de parc de terminaux

Mobile Control Centre (MCC)

Environnement de programmation
- HTML, XML
- SDK pour produits Psion
- HDK (Hardware Development Kit)
- .NET et C++ avec Microsoft Visual Studio® 2005
- Java supportant JDK 1.2.2 ou plus
- APIs Windows sockets (CE.net)

Certifications
- Sécurité : CSA/UL60950-1, IEC 60950-1, EN60950-1
- EMC: FCC Part 15 Class B
  EN 55022
  EN 55024
  EN301 489
- Laser: IEC 60825-1, Class 2 FDA 21 CFR 1040.10, 1040.11 Class II
- Bluetooth: 1.2

http://www.teknix.fr/doc/WORKABOUT_PRO_3_Spec_Sheet_A4_FR.pdf

SNCF
Risque d'attentats
Preuves recueillies - EURO 2016

Le réseau terroriste franco-belge voulait frapper avant l'Euro 2016

http://www.bfmtv.com/societe/un-enregistrement-audio-revele-des-projets-d-attentats-du-reseau-terroriste-franco-belge-966124.html
http://www.bfmtv.com/mediaplayer/video/nouveau-projet-dattentat-un-document-audio-dvoile-les-plans-des-terroristes-22-792786.html
Mis à jour le 11/04/2016 à 20h07

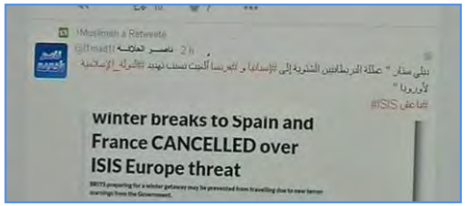
Nicolas Hénin, consultant jihadisme BFMTV.
Par E. M. avec Cécile Ollivier et Annabelle Vilmont

16 minutes et 8 secondes d'enregistrement audio retrouvé dans l'ordinateur portable de l'un des frères ***El Bakraoui***.

BFMTV a pu écouter l'intégralité de ce document.

Concerne les membres du réseau franco-belge à l'origine des attentats de novembre dernier à Paris et de mars à Bruxelles.

- Les communications utilisées un cloud
- La voix de l'homme est probablement celle de Najim Laachraoui
- Deuxième kamikaze de l'aéroport de Zaventem en Belgique s'adresse à des complices à Racca, soupçonné d'être l'artificier de la cellule.
- Leur donneur d'ordre en Syrie.
- Les messages vocaux enregistrés étaient déposés sur un cloud.



Najim Laachraoui

- Demande des conseils pour fabriquer des explosifs, s'interroge sur les dosages, les proportions.
- En 10 jours, dit-il, il a réussi à fabriquer 100 kg de TATP.
- Plans des terroristes : la France (« Il faut éviter de taper la Belgique, comme ça, ça reste une base de repli »).
- Faire annuler l'Euro 2016 en France qui aura lieu en juin.
- Ils voulaient frapper avant la compétition, programmée le 10 juin 2016.
- Tester une méthode en Syrie : déposer des explosifs sous des rails sans qu'on sache s'il parle de métro ou de train.
- Il demande même à son interlocuteur d'aller tester cette méthode sur une ligne ferroviaire désaffectée en Syrie, en périphérie de Racca.

SNCF
Risque d'attentats
Liste des matchs d'ouverture critiques

VENDREDI, 10 JUIN 2016

Groupe A	Stade de France, Saint-Denis		FRANCE	21:00	ROUMANIE

SAMEDI, 11 JUIN 2016

Groupe A	Stade Bollaert-Delelis, Lens Agglo		ALBANIE	15:00	SUISSE
Groupe B	Stade de Bordeaux, Bordeaux		PAYS DE GALLES	18:00	SLOVAQUIE
Groupe B	Stade Vélodrome, Marseille		ANGLETERRE	21:00	RUSSIE

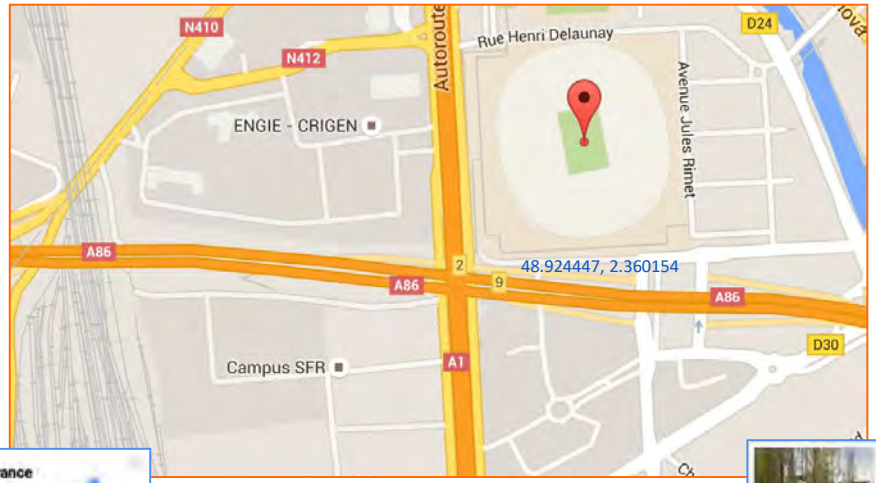
DIMANCHE, 12 JUIN 2016

Groupe C	Stade Pierre Mauroy, Lille Métropole		ALLEMAGNE	21:00	UKRAINE

SNCF
Risque d'attentats
Stade de France – Paris St Denis

Chef de la sécurité :
Société de Sécurité :
Système de Sécurité :
Société d'entretien :
Société de maintenance :

STADEFRANCE



Le Rendez-Vous
10 JUIN - 10 JUILLET

UEFA EURO2016 FRANCE

Architectes
Michel Macary
Aymeric Zublena
Michel Regembal
Claude Costantini

« Quels sont les accès pour les spectateurs ? »
« Les portes, escaliers, tribunes les plus fréquentés? »

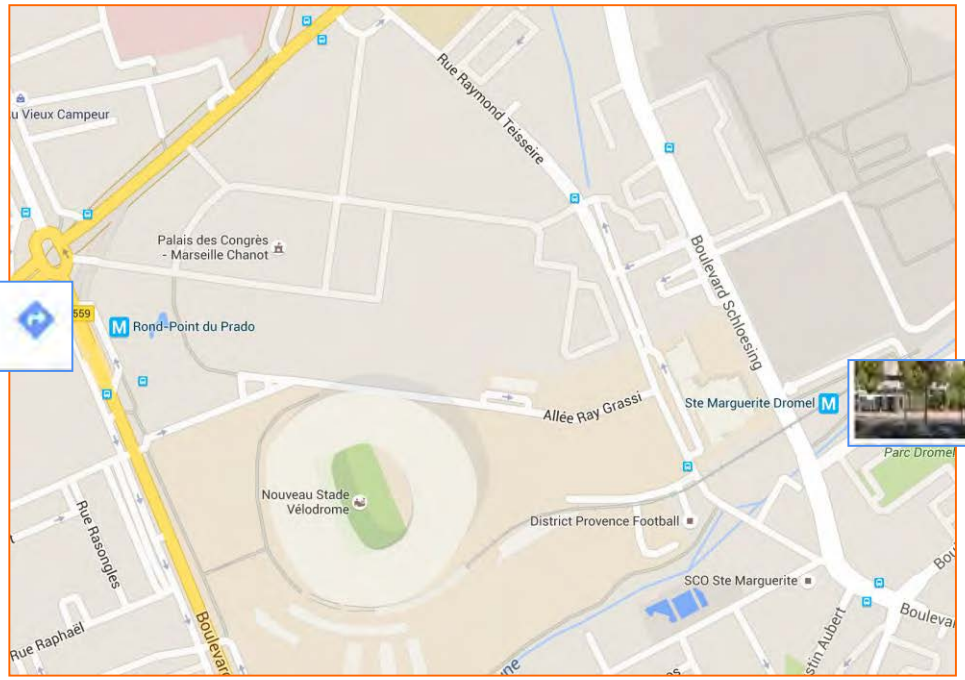
SNCF
Risque d'attentats
Stade Vélodrome - Marseille

Chef de la sécurité :
Société de Sécurité :
Système de Sécurité :
Société d'entretien :
Société de maintenance :

LE NOUVEAU STADE VÉLODROME

Le Rendez-Vous
10 JUIN - 10 JUILLET

UEFA EURO2016 FRANCE

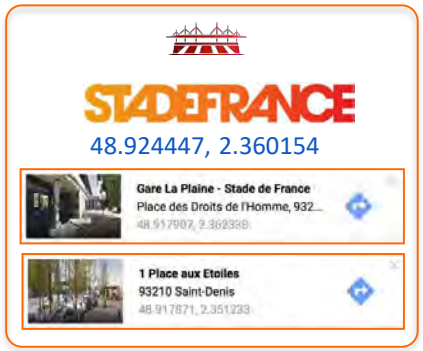


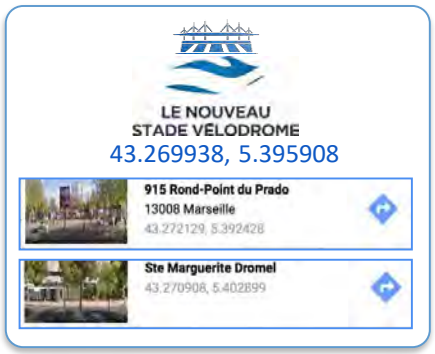
« Quels sont les accès pour les spectateurs ? »
« Les portes, escaliers, tribunes les plus fréquentés? »

SNCF
Risque d'attentats
Mots clés : Critères de recherche

- El Bakraoui
  - Racca, Syrie
  - Explosifs (TATP),
    - dosages, proportions, sous des rails.
  - Muslimah, Muslimah32, Harun

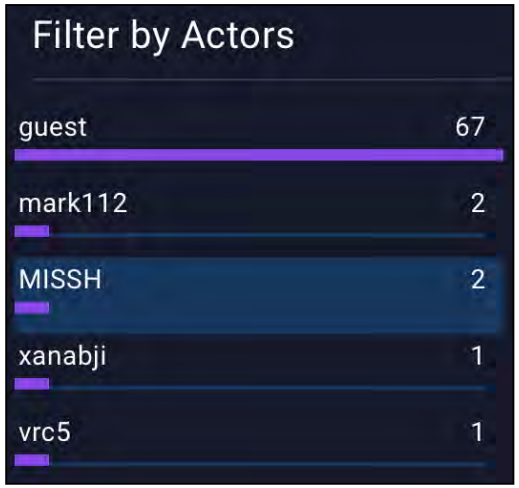
- Euro 2016
  - Date avant le 10 juin 2016.
  - Ville : Paris, Marseille, Lille
  - Nations : FR, DE, RU, UK

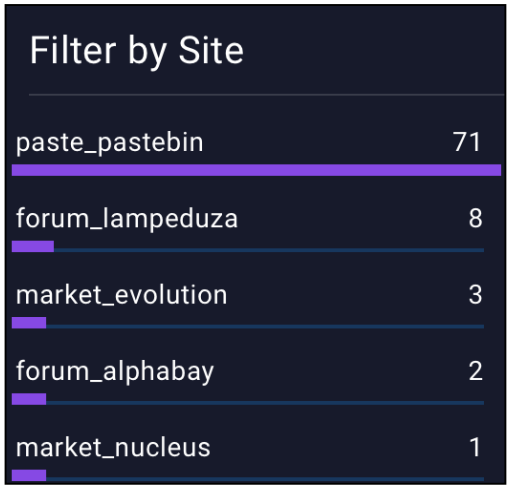




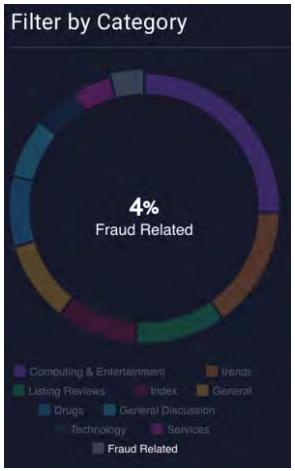
Ville	Gare sncf	Nombre de voies à quai	Voyageurs SNCF (millions/an)
Paris	Gare du Nord	31	201,8 (2014)
Paris	Gare Saint-Lazare	27	102,8 (2014)
Paris	Gare de Lyon	28	95,9 (2014)
Paris	Gare de Paris Est	29	30,5 (2014)
Lille	Gare de Lille - Flandres	17	21,0 (2012)2
Marseille	Gare Saint-Charles	15	11,5 (2013)6

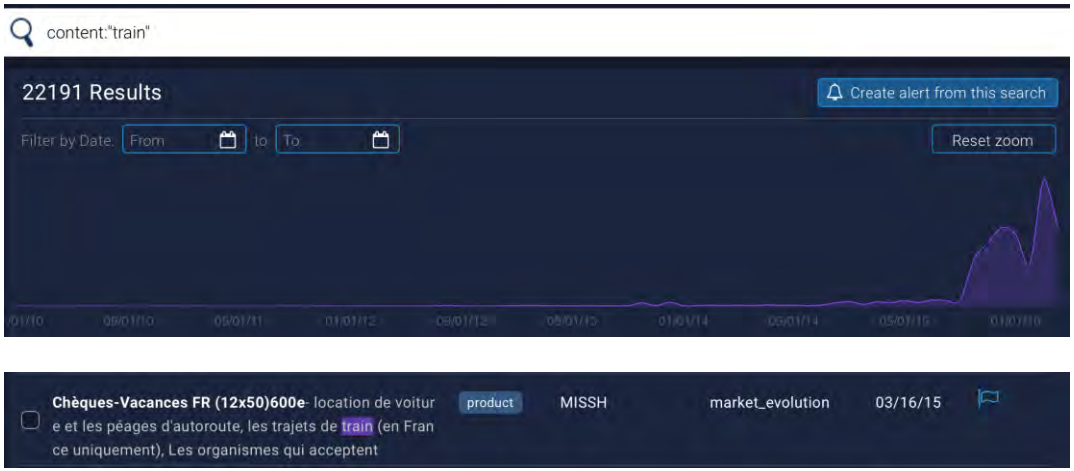
SNCF
Collecte d'informations
Critères de recherche : SNCF

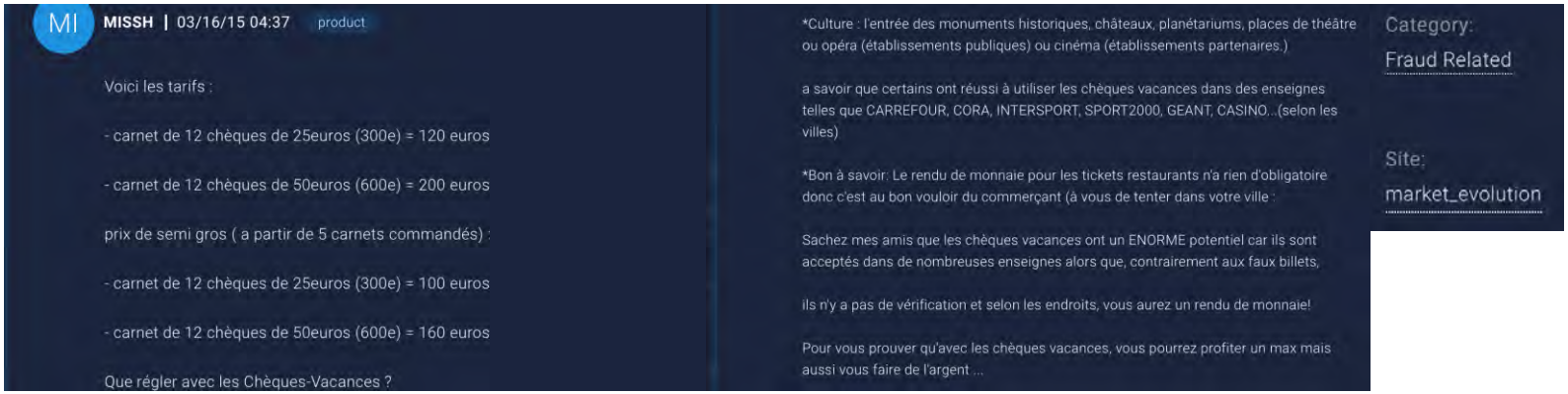




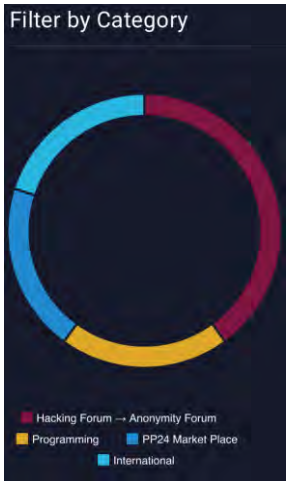
SNCF
Collecte Fraudes
Les billets SNCF contre Chèques Vacances

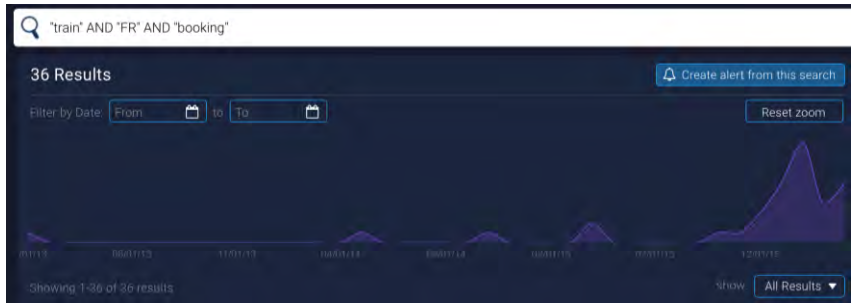


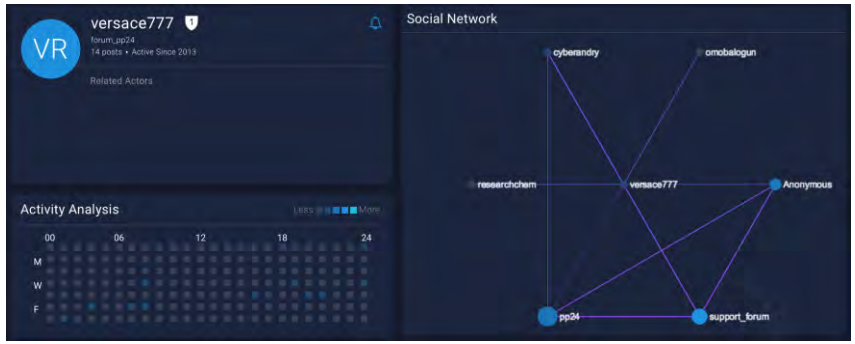


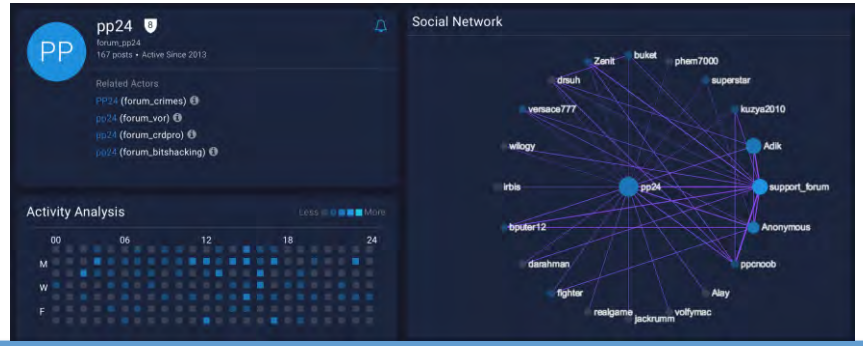


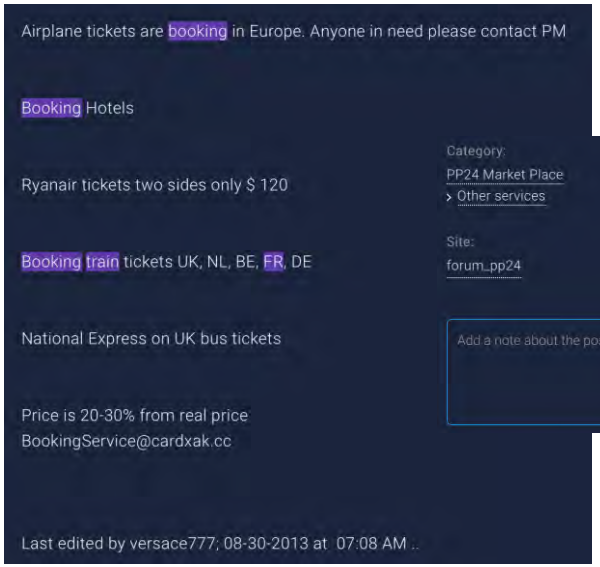
SNCF
Collecte d'informations
Critères de recherche : Train, FR, booking



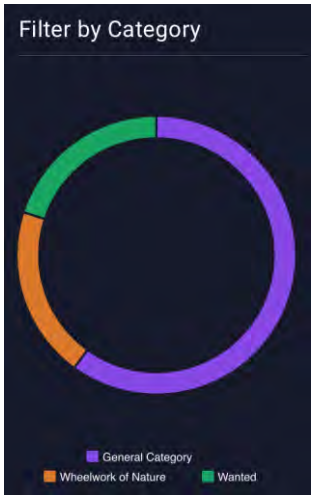


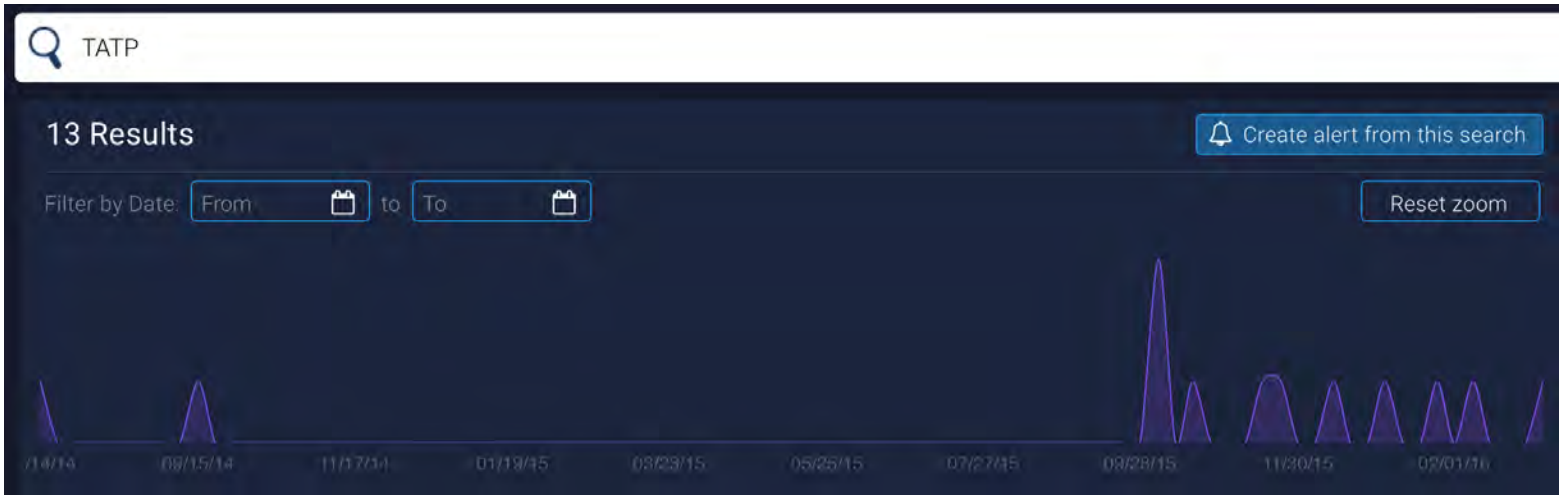




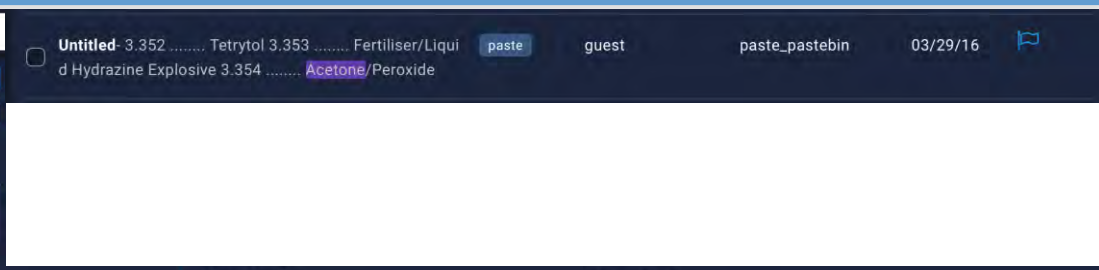


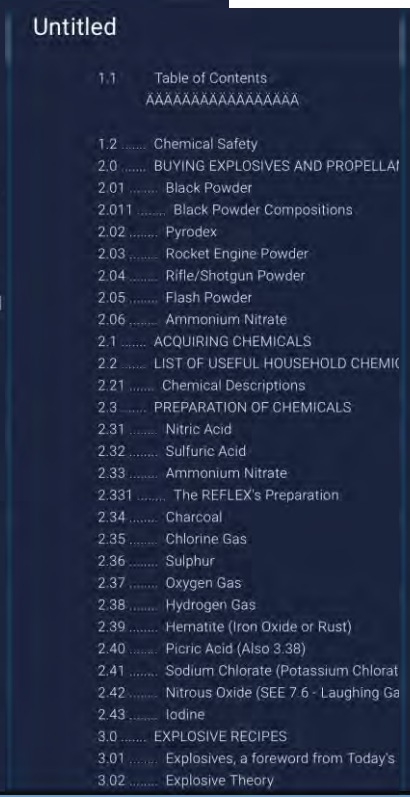
SNCF
Collecte Attentats
Critères de recherche : TATP

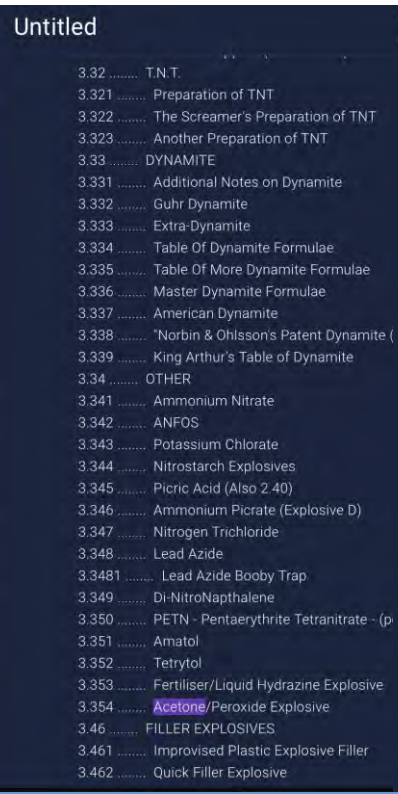


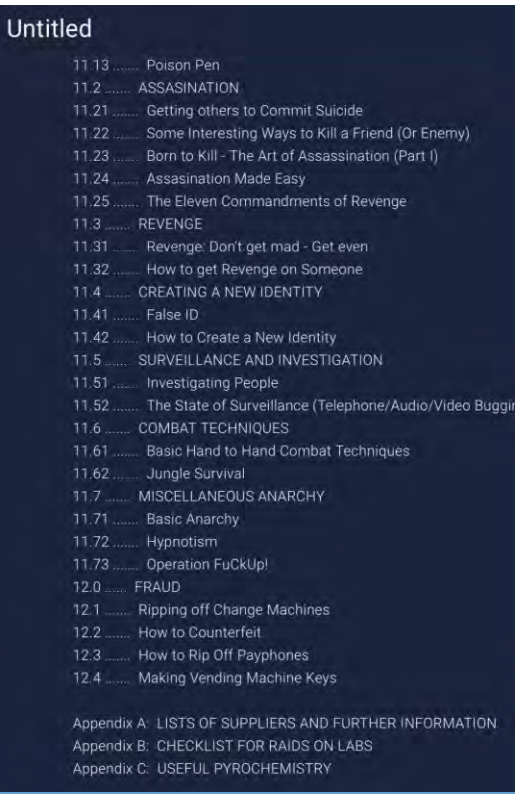


SNCF
Collecte Attentats
Critères de recherche : Acetone & Train









Q&A

Thank you!

BEYOND THE KNOWN THREATS

JOHNATHAN PARTOUCHE, CEO
JP@ORISECURE.COM
+447533610616

ORISECURE Industrial Security Transportation Use Case

1 Introduction

1.1 About this Document

ICS Ranger is an agentless and passive security solution designed to keep Industrial Control Systems (ICSs) operational. It provides real time visibility over assets and networks, and uses both signature-based and behavior-based profiling to identify operational and security threats, including network failures, malicious attacks, and operator errors.

The following use case focus on **ICS Ranger's** Operational Technology benefits to organizations providing immediate ROI benefits. The example given is for a Land Transport Authority that is responsible for monitoring various functions of the transportation system they are monitoring. Including train scheduling, security systems, smart door systems, ticketing systems, and other common systems within a land transport authority. The example shows how **ICS Ranger** can be leveraged within this environment to not only enhance the security of the Land Transport Authority's networks, but increase their operational efficiency, and visibility into their networks as well.

Further examples of how **ICS Ranger** can be implemented into specific Land Transport Authority environments can be created by ORISECURE Industrial for specific end users' environments. ORISECURE Industrial has a large amount of experience implementing **ICS Ranger** across different industry verticals, with vastly different network and system architectures, this use case is simply one of these examples.

2 Transport Authority Monitoring

2.1 Monitoring

2.1.1 Lack of Monitoring

A transport authority currently uses a large control system environment to perform various functions within their system, including safety door controls, ingress and egress controls on ticketing systems, track control systems, and large scale train monitoring systems. These systems are all utilizing the same network infrastructure, but have different control system interfaces, and serve widely different purposes. Because of the large nature of this system, they currently have no visibility into what the actual traffic that occurs within their control environment. Without this visibility, any of these different systems could become compromised without being noticed or understood by the transport authority until an event has already occurred.

2.1.2 Monitoring with ICS Ranger

ICS Ranger has the ability to monitor all of these different systems, regardless of the different vendors utilized and the different functions these systems perform. This makes ICS Ranger particularly valuable in a transport authority system, where different systems with widely different requirements are utilized within the same control environment. ICS Ranger utilizes its understanding of proprietary protocols and baselining technology to learn the network it is monitoring, and to understand what normal valid traffic looks like within this network. After it has learned the network, and all of the communication patterns within systems and between systems, it can alert on any deviation from this baseline data. This means that any change that occurs in the network will be captured and alerted on within ICS Ranger.

Additionally, ICS Ranger gives the ability to understand where cross communication occurs between different systems within the land transport authorities' networks. Typically, an attacker would use less critical systems, such as a ticketing system, as a jumping off point to reach more critical systems, such as a track control system. Utilizing ICS Rangers baselining technology, and the model it builds of the network, any communication between networks or assets is immediately identified, and it allows the land transport authority to protect these vulnerable communication pathways.

Finally, for any large network that the land transport authority does not have well defined configuration management and asset management processes for, ICS Ranger will automatically detect all endpoint devices within the network, and gather configuration data on these endpoints. This includes information such as IP address, MAC address, vendor, model number, serial number, firmware version, and other critical configuration parameters.

2.2 Summary

ICS Ranger is uniquely designed to monitor large and complex ICS networks such as the ones that exist within a land transport authority. It also provides the visibility required to detect the complex attacks that can occur within these environments due to the high level of system interconnectivity. Additionally, the asset management and configuration management functions of the ICS Ranger solution give benefits beyond the security gains, and allows the land transport authority to more efficiently and effectively operate their control networks.