Algorithmes prédictifs et Big Data

Algorithmes prédictifs et Big Data

Savoir ce que sera demain, ce mythe philosophique personnalisé par Cassandre dans l'antiquité Grecque est-il aujourd'hui en passe de devenir une réalité scientifique ?

Nombreuses sont les applications qui aujourd'hui s'appuient sur des algorithmes prédictifs, que ce soient dans les domaines du marketing, de la finance ou encore de la santé. Cet engouement multidisciplinaire est le résultat d'un phénomène, qui naquit il y a plus de 10 ans mais qui a aujourd'hui trouvé un terreau favorable de croissance : le Big Data.

Socle de cette émergence, la donnée constitue un or noir disponible, aisée d'exploitation de prime abord mais aussi potentiellement facteur décisionnel dans certaines disciplines. Au cours des dernières années est apparu le terme de «données massives» pour englober la mine de renseignements collectée à partir de nos activités quotidiennes, des articles publiés, de nos interactions sociales et des objets de plus en plus connectés, c'est à dire eux même générateurs de données.
La donnée offre la possibilité d'envisager des évolutions à court, moyen et long termes comme des comportements à venir parfois même en temps réel. Elle permet de faire le grand écart entre la globalisation et l'individualisation. En effet, il est, à la fois, possible de suivre et d'anticiper les grandes épidémies à l'échelle mondiale tout en analysant le comportement individuel de monsieur X par rapport à ses déplacements ou ses achats.
La lutte contre la criminalité n'échappe pas à l'intérêt que présente la donnée dans la capacité à prévoir les évolutions et pourquoi pas le comportement criminel. En effet, les données massives constituent la source de l'analyse prédictive en ce qu'elles alimentent des applications à vocation opérationnelle.
Derrière la notion simplificatrice et vulgarisée d'algorithme prédictif se dissimule un processus analytique complexe et polyvalent. Loin d'être le fruit d'une génération spontanée, l'analyse prédictive repose sur des préceptes mathématiques et statistiques à des fins d'extraction de connaissances et de formes criminelles particulières. Il n'existe pas de logiciels ou d'algorithmes miracles pour lutter contre la délinquance. Il s'agit de développer des méthodes, de les tester, de les évaluer préalablement à une quelconque utilisation. Les méthodes reposent sur des techniques d'apprentissage capable d'exploiter les données dans leurs multiples dimensions. Loin de toute notion de préemption, l'analyse prédictive a une vocation de prévention, c'est à dire non pas d'agir préalablement à toute commission d'infraction mais plutôt d'interrompre l'évolution d'un processus en cours. A l'opposé des clichés véhiculés par la fiction (Minority Report, Person of Interest), l'analyse prédictive constitue une aide à la décision pour un chef opérationnel qui la complète par une approche prospective. En effet, l'anticipation criminelle nécessite de prendre en compte l'héritage des événements du passé, c'est la prédiction. Mais elle intègre aussi, en élaborant les scenarii les plus probables, des événements ponctuels impactant le futur, c'est le domaine de la prospective. Dès lors, en matière de lutte contre la criminalité, le pilotage ne peut s'effectuer par la donnée comme cela peut être le cas dans d'autres disciplines. En effet, l'analyse prédictive apporte des éléments objectifs de compréhension mais quoiqu'il arrive et en dépit de la masse de données disponible, incomplets. Elle est, par exemple, utilisée dans la prise en compte des perspectives d'évolution d'infractions de masse telles que les cambriolages. Elle peut aussi être utilisée dans la détection préalable de fraudes sociales ou bancaires ou encore dans la compréhension à des fins d'anticipation des variables pesant sur certaines formes d'infractions. En effet, la politique d'ouverture et de partage des données publiques permet de tirer profit de variables liées à un contexte social ou économique ou encore à l'évolution météorologique, voire à la création de nouvelles infrastructures.
En dépit de l'intérêt manifeste que présentent les méthodes prédictives, il convient de se garder de tout risque d'atteintes aux libertés individuelles. Ce point est un préalable obligatoire à un quelconque déploiement en matière de sécurité publique où la donnée à caractère personnel est exclue du champ d'analyse. Outre cette question essentielle, le risque de l'analyse prédictive est aussi une mauvaise interprétation de ce qu'est réellement l'apport de la prédiction. Gardons nous du joug infligé par Apollon à Cassandre.

Réagissez à cet article

Source : *L'algorithme prédictif [par Patrick PERROT, Chef de la Division Analyse et Investigations Criminelles, Service Central de Renseignement Criminel de la Gendarmerie Nationale] | Observatoire FIC*

Comment l’industrie peut aussi anticiper les cyberattaques ?

Comment l’industrie peut aussi anticiper les cyberattaques ?

Les cyberattaques se multiplient ces derniers mois et ont augmenté de 51 % (*) cette année en France, en particulier à l'encontre des technologies de l'information (messageries hackées, serveurs victimes d'attaques #DDoS entre autres). Pourtant, un tout autre domaine suscite de nouvelles préoccupations : l'industrie.
Les systèmes industriels, ou Industrial Control System (ICS), désignant l'ensemble des moyens informatisés et automatisés assurant le contrôle et le pilotage de procédés industriels, subissent les mêmes menaces que dans le milieu IT.
Cependant, une attaque à l'encontre de l'ICS peut avoir des répercussions encore plus graves, non seulement sur l'industrie en elle-même, avec son corollaire de pertes financières, mais aussi, et surtout, sur l'homme et l'environnement.

Des réseaux vulnérables, car en flux tendus
Tandis que l'IT se soucie davantage de la confidentialité des données, les industriels se préoccupent essentiellement de la disponibilité et de la rentabilité de leur production. Il faut ainsi comprendre que pour des questions de coût, il est inconcevable pour un industriel de stopper sa production, nonobstant une menace imminente.

La dernière crise ukrainienne a illustré cette problématique. Malgré des bombardements massifs, le système de production n'a pas été arrêté. Les réseaux industriels sont d'autant plus vulnérables qu'il n'est pas possible d'effectuer de maintenance sur le système, puisqu'il est en cours de production.

Mais qui sont ces « pirates » qui tirent profit de ces vulnérabilités ?
Il s'agit de groupes bien organisés, de terroristes, qui s'attaquent directement à la vulnérabilité de l'État et des grandes entreprises. On parle d'une véritable cyberarmée qui s'attaque aux réseaux industriels de plusieurs manières : déni de services, prise de contrôle à distance des systèmes, vol de données, mise en faillite par détournement de fonds, pour n'en citer que quelques-uns. En 2003, la centrale nucléaire de Davis-Besse aux USA avait été la cible d'attaques DDoS.
Pour autant, la plupart des incidents de sécurité sont accidentels, liés par exemple à l'activation fortuite de malware se trouvant dans un mail, sur une clé USB ou encore des softwares mal sécurisés.
À l'échelle de l'industrie, les attaques peuvent entraîner des retards de production, un impact économique – consécutif au vol de secrets de fabrication – une perte d'image et de contrats. In fine, l'industriel se retrouve face à une véritable perte de compétitivité.
Les réseaux industriels étant en contact direct avec la vie humaine, celle-ci est également en danger. Ces attaques peuvent en effet entraîner des accidents physiques ; l'arrêt de la production d'énergie pouvant entraîner des coupures d'électricité dans les hôpitaux qui peuvent être critiques. À plus grande ampleur, la santé humaine et l'environnement sont également menacés dans le cas d'une attaque des systèmes nucléaires.
L'exemple le plus connu est celui de Stuxnet, un ver informatique découvert en 2010 et conçu pour attaquer une cible industrielle déterminée pour l'espionner. Le ver a affecté 45 000 systèmes informatiques, y compris des ordinateurs de la centrale nucléaire de Bouchehr ainsi que 15 000 ordinateurs et centrales situés en Allemagne, en France, en Inde et en Indonésie (**).

Les industriels ne sont pas suffisamment préparés à ces types d'attaques, car les moyens mis en œuvre sont limités et la sécurité est considérée comme annexe, dans la mesure où elle n'est pas fondamentale pour assurer les services. À cela s'ajoute qu'elle représente un coût additionnel pour la production, qui se répercute sur les consommateurs qui devront payer plus cher leurs eau, électricité et autres services.
Dès lors, quelles sont les mesures pour se prémunir de ces attaques ? Quels outils peuvent être mis en place ?
La loi est un instrument essentiel pour assurer la protection des ICS et aider à recréer de la confiance. La France a mis en place, en 2006, un décret qui définit 12 secteurs d'importance vitale comprenant notamment la gestion de l'eau, la santé, l'énergie, l'alimentation et les transports, des fondamentaux pour le fonctionnement d'un État.

« Le projet de loi de programmation militaire, prévu pour 2014-2019, précise qu'il est de la responsabilité de l'État d'assurer une sécurité suffisante des systèmes critiques des OIV (opérateurs d'importance vitale). À travers quatre mesures principales, il vise à établir un socle minimum de sécurité pour les organisations.
Il donne notamment au pouvoir exécutif la possibilité d'imposer aux OIV des obligations en matière de sécurisation de leur réseau, de qualification de leurs systèmes de détection, d'information sur les attaques qu'ils peuvent subir et de soumission à des contrôles.
Avec ce texte, qui sera examiné sous peu au Sénat, l'État fixera donc des règles en collaboration étroite avec l'ANSSI. Règles que les OIV seront tenus d'appliquer, à leur frais. Les sociétés mauvaises élèves seront susceptibles de se voir infligées une sanction pouvant aller jusqu'à 750 000 euros d'amende » (***).

Au-delà de cette législation, il est essentiel, pour retarder l'attaque, de mettre un point d'honneur à la sensibilisation de l'utilisateur dans la chaîne de production, mais aussi, et surtout, de la direction des industries, en l'incitant à appliquer de bonnes pratiques au quotidien et en investissant dans les hommes et les outils (firewall, anti-vers ou encore systèmes de détection d'intrus).
Cependant, même le plus puissant des firewalls n'est pas suffisant si l'on n'identifie et ne traite pas les menaces dans le détail, sur un service en particulier. Cela sous-entend qu'il y ait un opérateur qui assure la maintenance des systèmes d'informations, sans quoi les intrusions dans les réseaux industriels ne pourront être empêchées.

(*) Source : étude réalisée par le cabinet PwC
(**) Source : Wikipédia
(***) Source : Nextimpact.com

Réagissez à cet article

Source : *Les Echos.fr – Actualité à la Une – Les Echos*

Antivirus software could make your company more vulnerable

	Antivirus software could make your company more vulnerable !

Security researchers are worried that critical vulnerabilities in antivirus products are too easy to find and exploit

Imagine getting a call from your company's IT department telling you your workstation has been compromised and you should stop what you're doing immediately.
You're stumped: You went through the company's security training and you're sure you didn't open any suspicious email attachments or click on any bad links; you know that your company has a solid patching policy and the software on your computer is up to date; you're also not the type of employee who visits non-work-related websites while on the job. So, how did this happen?

A few days later, an unexpected answer comes down from the security firm that your company hired to investigate the incident: Hackers got in by exploiting a flaw in the corporate antivirus program installed on your computer, the same program that's supposed to protect it from attacks. And all it took was for attackers to send you an email message that you didn't even open.
This scenario might sound far-fetched, but it's not. According to vulnerability researchers who have analyzed antivirus programs in the past, such attacks are quite likely, and may already have occurred. Some of them have tried to sound the alarm about the ease of finding and exploiting critical flaws in endpoint antivirus products for years.
Since June, researchers have found and reported several dozen serious flaws in antivirus products from vendors such as Kaspersky Lab, ESET, Avast, AVG Technologies, Intel Security (formerly McAfee) and Malwarebytes. Many of those vulnerabilities would have allowed attackers to remotely execute malicious code on computers, to abuse the functionality of the antivirus products themselves, to gain higher privileges on compromised systems and even to defeat the anti-exploitation defenses of third-party applications.
Exploiting some of those vulnerabilities required no user interaction and could have allowed the creation of computer worms – self-propagating malware programs. In many cases, attackers would have only needed to send specially crafted email messages to potential victims, to inject malicious code into legitimate websites visited by them, or to plug in USB drives with malformed files into their computers.

Attacks on the horizon

Evidence suggests that attacks against antivirus products, especially in corporate environments, are both possible and likely. Some researchers believe that such attacks have already occurred, even though antivirus vendors might not be aware of them because of the very small number of victims.
The intelligence agencies of various governments have long had an interest in antivirus flaws. News website The Intercept reported in June that the U.K. Government Communications Headquarters (GCHQ) filed requests in 2008 to renew a warrant that would have allowed the agency to reverse engineer antivirus products from Kaspersky Lab to find weaknesses. The U.S. National Security Agency also studied antivirus products to bypass their detection, according to secret files leaked by former NSA contractor Edward Snowden, the website said.

Réagissez à cet article

Source : *Antivirus software could make your company more vulnerable | Computerworld*

Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab

Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab

---

Avec Enigma, système de cryptage de données basé sur le blockchain, des informations confidentielles peuvent être stockées et partagées en ligne, sans intervention d'un tiers de confiance pour contrôler leur utilisation.

Enigma. Derrière ce nom mystérieux se cache l'une des dernières créations du MIT Media Lab, l'un des laboratoires de recherche du Massachusetts Institute of Technology. Ce système de cryptage de données est basé sur le blockchain, la technologie qui sous-tend le bitcoin (monnaie virtuelle mise en circulation en 2009). Elle fonctionne grâce au partage d'un registre d'informations par l'ensemble d'une communauté d'internautes.

Enigma, dont la version bêta sera lancée prochainement, permettra à des utilisateurs anonymes (particuliers, entreprises, associations…) de stocker dans le cloud et de partager des informations sensibles avec des tiers, de manière sécurisée. Pas besoin d'un intermédiaire de confiance, qui aurait accès à ces data pour contrôler leur utilisation et les crypter. Ces opérations sont effectuées par un réseau d'ordinateurs membres, grâce au système du blockchain. Les informations peuvent être traitées par des algorithmes, sans que le jeu de données brut ne soit jamais révélé dans sa totalité à l'une des parties.

DES RETOMBÉES DANS LE DOMAINE DU MACHINE LEARNING

Le registre blockchain, partagé par les ordinateurs membres du réseau, contrôle l'identité des utilisateurs d'Enigma (via un code, car ils sont anonymes) et leur donne accès ou non à tout ou partie des données. Il enregistre l'ensemble des opérations réalisées sur Enigma : enregistrement de nouvelles informations, consultation, opérations réalisées sur ces data…

Les données stockées par Enigma pourront être analysées par des applications et des logiciels extérieurs, tout en maintenant ces informations sous le contrôle de leur propriétaire. Le programme pourrait avoir des retombées intéressantes dans le domaine de la data science et du machine learning.

UN NOM DE BAPTÊME HISTORIQUE

Enigma pourrait également contribuer au développement d'un Internet des objets respectueux de la vie privée de ses utilisateurs, souligne le site spécialisé Bitcoin Magazine dans un article présentant le projet. Les propriétaires des données pourront, s'ils le souhaitent, les monétiser. Ils pourraient par exemple vendre à des laboratoires pharmaceutiques qui réalisent des recherches un accès partiel et contrôlé à leurs données de santé.

Guy Zyskind, étudiant au MIT, et Oz Nathan, entrepreneur qui a travaillé par le passé avec la défense israélienne, sont à l'origine de ce programme. Ils n'ont pas choisi son nom par hasard. Le système de cryptographie électro-mécanique utilisé par les Allemand pendant la deuxième guerre mondiale était baptisé Enigma. Un groupe de chercheurs, dont faisait notamment partie Alain Turing, a réussi à trouver la clef de ce code complexe.

Réagissez à cet article

Source : *Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab*

Plusieurs escrocs sur Leboncoin écopent de peines de prison

Plusieurs escrocs sur Leboncoin écopent de peines de prison

Les autorités utilisent Leboncoin pour surveiller les escrocs qui revendent du matériel volé. Plusieurs forces de police indiquent avoir réussi à arrêter des auteurs présumés, certains ont même été condamnés à des peines de prison.

Comme bon nombre de plates-formes de vente en ligne, Leboncoin.fr peut servir pour des escrocs de moyen d'écouler une marchandise indûment obtenue voire d'appâter des victimes. En région parisienne, un groupe de personnes vient d'être condamné à des peines de prison pour avoir revendu des voitures sur le site.
Ces véhicules d'occasion étaient achetés avec de faux chèques de banque pour les revendre, 30 à 40 % moins cher que l'argus, contre des espèces. Des annonces étaient régulièrement publiées sur Leboncoin puis rapidement retirées, une fois la vente conclue. Au total, 71 automobiles ont été répertoriées par les forces de police.
Selon Le Parisien, les escrocs ont pu être repérés notamment grâce aux annonces publiées sur le site.
Le cerveau du réseau, un homme de 28 ans, écope d'une peine de 5 années de prison dont 1 an avec sursis avec mise à l'épreuve. Il devra en outre rembourser les victimes. Les autres membres ont été condamnés par le tribunal correctionnel de Pontoise à 4 et 2 ans de prison (associées à des peines de sursis).

Le site internet leboncoin.fr
Un voleur arrêté après avoir mis des annonces sur Leboncoin
En Bretagne, les autorités indiquent avoir interpellé un homme soupçonné d'avoir dérobé du matériel de jardinage auprès d'une enseigne locale. L'individu a volé des objets pour un préjudice total estimé à 2 500 euros puis a tenté de revendre une partie du butin sur Leboncoin, sans se soucier que le vendeur ou la gendarmerie surveillerait la plate-forme.
Dans les jours suivants le délit, le responsable du magasin qui avait subi le vol a trouvé une annonce pertinente. « Nous avons ensuite travaillé à partir de cette annonce, puis nous sommes remontés jusqu'à l'auteur présumé des cambriolages », explique le maréchal des logis-chef Goby auprès du quotidien Ouest-France.
Le domicile de la personne a été perquisitionné et nombre d'objets dérobés s'y trouvaient. L'affaire a été transmise au parquet de Brest, où sera jugé l'auteur présumé.

Réagissez à cet article

Source : *Plusieurs escrocs sur Leboncoin écopent de peines de prison*

FIC 2016 – Demandez le programme…

FIC 2016 – Demandez le programme…

Les données sont le carburant de la transformation numérique de nos sociétés. Elles irriguent désormais l'ensemble des réseaux et systèmes d'information et, à travers eux, des activités humaines. Les chiffres donnent le vertige : 144 milliards de mails sont échangés dans le monde chaque jour, 30 gigaoctets sont publiés chaque seconde, 800 000 nouveaux sites web apparaissent quotidiennement, la quantité d'informations disponibles double tous les deux ans…. avec seulement 42 % de la population mondiale connectée.

Le thème du FIC 2016 :
Malgré cette croissance exponentielle, les données restent un capital fragile. Il faut en effet susciter les conditions de leur création, puis les entretenir, les enrichir, les transformer, les valoriser et les protéger pour en faire une source de progrès pour l'Homme. Les défis sont donc multiples. Au plan stratégique, tout d'abord : le primat accordé par l'Union européenne aux données personnelles serait-il donc incompatible avec le « business » de la donnée ? Au plan juridique, également : comment concilier l'imbrication croissante des données et l'application de la notion de propriété ? Au plan sécuritaire, enfin : comment créer le climat de confiance propice au développement de nouveaux usages pour le citoyen, l'entreprise, la collectivité territoriale, l'Etat ?

Programme FIC 2016 Lundi 25 janvier 2016

lundi 10:00 – 11:00|Séance plénière VA-T-ON VERS UNE CRISE DE CONFIANCE DES UTILISATEURS ?
lundi 11:00 – 11:30|Séance plénière ALLOCUTION DE GÜNTHER OETTINGER, COMMISSAIRE EUROPÉEN CHARGÉ DE L'ÉCONOMIE ET DE LA SOCIÉTÉ NUMÉRIQUES
DT01|lundi 12:00 – 12:30|Démonstration technique INFOBLOX – CIBLE D'ATTAQUES ET VECTEUR D'EXFILTRATION DE DONNÉES : VOTRE DNS EST VULNÉRABLE !
C01|lundi 12:15 – 13:00|Conférence ANSSI – BSI : CYBERSÉCURITÉ : LA COOPÉRATION FRANCO-ALLEMANDE
C02|lundi 12:15 – 13:00|Conférence SOPRA-STERIA – PROTÉGER LES SUPPLY CHAIN DES SECTEURS ÉCONOMIQUES SENSIBLES AVEC L'INNOVATION BOX@PME
C03|lundi 12:15 – 13:00|Conférence THALES – PROTECTION DES DONNÉES ET TRANSFORMATION NUMÉRIQUE
C05|lundi 12:15 – 13:00|Conférence QUALYS – TÉMOIGNAGE CLIENT DÉFENSE
FT01|lundi 12:15 – 12:30|FIC Talk RSA – INTELLIGENCE DRIVEN SECURITY » : L'UTILISATEUR EST LE NOUVEAU PÉRIMÈTRE
DT02|lundi 12:30 – 13:00|Démonstration technique NES – LE SOC 'INTELLIGENT' : OU COMMENT APPRÉHENDER LA DÉMARCHE D'UN HACKER
FT02|lundi 12:30 – 12:45|FIC Talk CONTEXTUAL SECURITY INTELLIGENCE
MC01|lundi 12:30 – 12:45|Master class DE FRUTAS À ALIENSPY, ANALYSE D'UNE FAMILLE DE RAT JAVA
DT03|lundi 13:00 – 13:30|Démonstration technique IMS NETWORKS – ANTI DDOS AS A SERVICE
TV03|lundi 13:00 – 13:05|Plateau TV LES RÉSEAUX ÉLECTRIQUES INTELLIGENTS.
DT04|lundi 13:30 – 14:00|Démonstration technique CONIX – VERS UN DÉVELOPPEMENT D'OUTILS INNOVANTS EN MODE AGILE EN RÉPONSE À LA CYBER-MENACE
A05|lundi 14:00 – 15:30|Agora ETHIQUE ET CYBERESPACE
A09|lundi 14:00 – 15:30|Atelier PROCÈS SIMULÉ SUR UNE FUITE DE DONNÉES CONFIDENTIELLES
DT05|lundi 14:00 – 14:30|Démonstration technique BACKBOX- AUTOMATING NETWORK AND SECURITY DEVICE OPERATIONS
A01|lundi 14:30 – 15:30|Atelier LA NOUVELLE CYBERCRIMINALITÉ LIÉE AUX DONNÉES
A02|lundi 14:30 – 15:30|Atelier INTERNET DES OBJETS : LA NOUVELLE FRAGILITÉ ?
A03|lundi 14:30 – 15:30|Atelier INCIDENT DE SÉCURITÉ : COMMENT PRENDRE EN COMPTE TOUTES LES CONTRAINTES ?
A04|lundi 14:30 – 15:30|Atelier COMPRENDRE ET ORGANISER SES DONNÉES
A06|lundi 14:30 – 15:30|Atelier CYBERSÉCURITÉ ET OIV : QUELLES OBLIGATIONS ?
A07|lundi 14:30 – 15:30|Atelier EXTERNALISATION DU SOC : QUELS AVANTAGES POUR QUELS RISQUES ?
A08|lundi 14:30 – 15:30|Atelier THE CYBER GAME
A10|lundi 14:30 – 15:30|Atelier LES NOUVEAUX MÉTIERS LIÉS AUX DONNÉES
A11|lundi 14:30 – 16:00|Atelier CLUSTERS ET CYBERSÉCURITÉ : COMMENT SOUTENIR LE DÉVELOPPEMENT DE LA FILIÈRE ?
MC03|lundi 14:30 – 15:15|Master class LES TECHNIQUES SPÉCIALES D'ENQUÊTE
DT06|lundi 15:00 – 15:30|Démonstration technique SECLAB – TIXEO : VISIOCONFÉRENCE SÉCURISÉE ENTRE SYSTÈMES NON CONNECTÉS
DT07|lundi 15:30 – 16:00|Démonstration technique BITDEFENDER – COMMENT GARANTIR LA CONTINUITÉ DES SERVICES DE SÉCURITÉ
MC04|lundi 15:30 – 16:15|Master class UTILISATION OPÉRATIONNELLE DES TECHNIQUES D'EXTRACTION DE CONNAISSANCE (DATAMINING, BIG DATA) DANS LE RENSEIGNEMENT ET LA CONCEPTION D'ATTAQUES
TV06|lundi 15:30 – 15:40|Plateau TV LES NOUVELLES CONNAISSANCES EN NEUROSCIENCES, SCIENCES ET THÉRAPIES COGNITIVES PEUVENT ELLES AIDER À MIEUX COMPRENDRE ET GÉRER LA CYBER SÉCURITÉ ?
C07|lundi 16:00 – 16:45|Conférence INEO – RETOUR D'EXPÉRIENCE D'UN LEADER DE LA GRANDE DISTRIBUTION EN MATIÈRE DE GESTION GLOBALE DU CYBER-RISQUE
C08|lundi 16:00 – 16:45|Conférence PÔLE D'EXCELLENCE CYBER – EXPÉRIMENTER AVEC SON CLIENT : EXEMPLES EN SANTÉ, CHIMIE ET DÉVELOPPEMENT LOGICIEL
C09|lundi 16:00 – 16:45|Conférence HARMONIE TECHNOLOGIE – EXTERNALISATION DES DONNÉES, PANORAMA DE MENACES ET ORIENTATIONS 2016
C10|lundi 16:00 – 16:45|Conférence PWC
DT08|lundi 16:00 – 16:30|Démonstration technique TIXEO – DÉMONSTRATION DE LA SOLUTION DE VISIOCONFÉRENCE HAUTEMENT SÉCURISÉ TIXEO
FT04|lundi 16:00 – 16:15|FIC Talk SOLUTION ANTI D-DOS, OÙ VONT MES DONNÉES ?
FT05|lundi 16:15 – 16:30|FIC Talk CLOUD – COMMENT MÉRITER LA CONFIANCE À L'HEURE DE LA REMISE EN CAUSE SAFE HARBOR ?
MC05|lundi 16:15 – 17:00|Master class IMPUTABILITÉ DES CONNEXIONS INTERNET EN ENTREPRISE : PROBLÉMATIQUES TECHNIQUES ET RÉGLEMENTAIRES. RETOUR D'EXPÉRIENCE SUR LE PROJET LIBRE ALCASAR
DT09|lundi 16:30 – 17:00|Démonstration technique HEXATRUST – BERTIN IT – SENTRYO – CYBERSÉCURITÉ INDUSTRIELLE : 6 MESURES D'HYGIENE A PRENDRE EN 2016
FT06|lundi 16:30 – 16:45|FIC Talk 2020 NEW TECHNOLOGIES, NEW HOPES, NEW CHALLENGES
DT10|lundi 17:00 – 17:30|Démonstration technique HEXATRUST – WALLIX / ITRUST – FUITE DE VOS DONNÉES SENSIBLES, COMMENT VOUS PRÉMUNIR ET IDENTIFIER LES COMPORTEMENTS À RISQUES DES UTILISATEURS ?
TV08|lundi 17:00 – 17:05|Plateau TV
P02|lundi 17:15 – 18:15|Séance plénière DONNÉES : UNE CHANCE POUR L'EUROPE

Programme FIC 2016 Mardi 26 janvier 2016

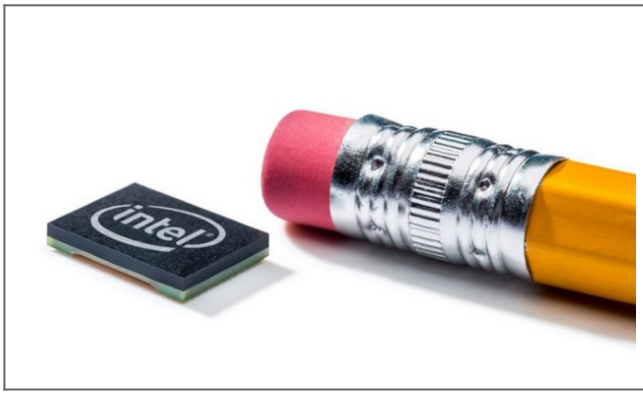
mardi 09:00 – 09:30|Séance plénière ALLOCUTION DE MONSIEUR BERNARD CAZENEUVE, MINISTRE DE L'INTÉRIEUR, RÉPUBLIQUE FRANÇAISE
P03 mardi 09:30 – 10:30|Séance plénière QUELLE SOUVERAINETÉ SUR LES DONNÉES ?
B01 mardi 11:00 – 12:00|Atelier DATA 2030
B02 mardi 11:00 – 12:00|Atelier RÈGLEMENT E-IDAS : UNE RÉELLE OPPORTUNITÉ POUR L'INDUSTRIE EUROPÉENNE DE LA CONFIANCE NUMÉRIQUE
B03 mardi 11:00 – 12:00|Atelier L'USINE DU FUTUR : QUELS RISQUES ?
B04 mardi 11:00 – 12:00|Atelier LA GESTION DES CRISES CYBER
B05 mardi 11:00 – 12:00|Atelier COMMENT ASSURER SES DONNÉES ?
B06 mardi 11:00 – 12:00|Agora CYBERSÉCURITÉ ET FRANCOPHONIE
B07 mardi 11:00 – 12:00|Atelier LES APT EN MILIEU MILITAIRE
B08 mardi 11:00 – 12:00|Atelier DATA LOSS PREVENTION : ENFIN QUELQUES SOLUTIONS MATURES ?
B09 mardi 11:00 – 12:00|Atelier SMART GRID : QUELLES VULNÉRABILITÉS ?
B10 mardi 11:00 – 12:00|Atelier SANTÉ : LA CYBERSÉCURITÉ VITALE
DT11 mardi 11:00 – 11:30|Démonstration technique PALO ALTO NETWORKS – DE LA RÉSILIENCE À LA PRÉVENTION DE LA CYBERCRIMINALITÉ
MC06 mardi 11:00 – 11:45|Master class POURQUOI SÉCURISER L'IMPLÉMENTATION DES ALGORITHMES CRYPTOGRAPHIQUES ?
MC07 mardi 11:00 – 11:45|Master class DONNÉES PERSONNELLES ET OBJETS CONNECTÉS : ATTAQUES, DÉFENSE ET CONTRE-MESURES
DT12 mardi 11:30 – 12:00|Démonstration technique HEXATRUST – ILEX . INWEBO / OPENTRUST – GESTION DES IDENTITÉS ET DES ACCÈS : LA RÉPONSE CONCRÈTE ET ILLUSTRÉE D'HEXATRUST
DT13 mardi 12:00 – 12:30|Démonstration technique HEXATRUST – DENYALL / NETHEOS – SÉCURISATION DES TRANSACTIONS : UN ENJEU VITAL À L'HEURE DU DIGITAL
MC08 mardi 12:00 – 12:45|Master class LA FAILLE LOGJAM
DT14 mardi 12:30 – 13:00|Démonstration technique HEXATRUST – IDECSI / VADERETRO – APPLICATION CENTRALE ET AU CŒUR DU RISQUE : QUELLES SOLUTIONS POUR PROTÉGER LA MESSAGERIE ?
DT15 mardi 13:00 – 13:30|Démonstration technique HEXATRUST – THEGREENBOW / PRIM'X – CHIFFRER LES DONNÉES – TOUJOURS PAS UN REFLEXE NATUREL ?
TV11 mardi 13:00 – 13:10|Plateau TV
C11 mardi 13:30 – 14:15|Conférence ORANGE CYBERDEFENSE – CAC 40 : RETOUR SUR LES PROBLÉMATIQUES DE SÉCURITÉ EN ENTREPRISE
C12 mardi 13:30 – 14:15|Conférence KASPERSKY – ANALYSE DE L'ATTAQUE AVANCÉE DUQU 2.0
C13 mardi 13:30 – 14:15|Conférence TÉMOIGNAGE DU MINISTERE DE L'ÉDUCATION NATIONALE – SÉCURISATION DES CENTRES DE DONNÉES
C14 mardi 13:30 – 14:15|Conférence MINISTÈRE DE LA DÉFENSE – ECHANGE DE POINT DE VUE SUR LA FORMATION ET ENTRAÎNEMENT
C15 mardi 13:30 – 14:15|Conférence TREND MICRO – TÉMOIGNAGE DU GROUPE KEOLIS – UNIFORMISER SES SOLUTIONS DE SÉCURITÉ POUR MIEUX LUTTER CONTRE LES NOUVELLES MENACES
DT16 mardi 13:30 – 14:00|Démonstration technique HEXATRUST – ERCOM / PRADEO – PROTECTION DES FLUX MOBILES ET WEB : LA CLÉ DE VOUTE DU DÉVELOPPEMENT DE L'ÉCONOMIE DIGITAL
FT07 mardi 13:30 – 13:45|FIC Talk QUALYS – ADOPTEZ UNE STRATÉGIE CONTRE LES MENACES
MC09 mardi 13:30 – 14:15|Master class IOT, SERRURES CONNECTÉES ET SÉCURITÉ DU CONTRÔLE D'ACCÈS ÉLECTRONIQUE
MC10 mardi 13:30 – 14:15|Master class LA TECHNOLOGIE FROGANS SÉCURISE LA PUBLICATION DE DONNÉES SUR L'INTERNET
FT09 mardi 14:15 – 14:30|FIC Talk ET SI LA SÉCURITÉ ÉTAIT EN RÉALITÉ LE PRINCIPAL ENJEUX DE L'INTERNET DES OBJETS ?
DT17 mardi 14:30 – 15:00|Démonstration technique SPLUNK – IDENTIFICATION ET ANALYSE DES COMPORTEMENTS DÉVIANTS PAR LE MACHINE LEARNING
TV12 mardi 14:30 – 14:40|Plateau TV E-DISCOVERY OR FORENSIC : HOW TO DEAL WITH LEGAL PRIVILEGE AND PERSONAL INFORMATION
B11 mardi 14:45 – 15:45|Atelier INVESTIGATIONS DANS LE CYBERESPACE : LES TECHNIQUES D'ENQUÊTE AU REGARD DE LA PROTECTION DE LA VIE PRIVÉE ?
B12 mardi 14:45 – 15:45|Atelier PEUT-ON PARLER DE THÉÂTRE D'OPÉRATIONS CYBER ?
B13 mardi 14:45 – 15:45|Atelier LE MARCHÉ EUROPÉEN DU NUMÉRIQUE : CHIMÈRE OU RÉELLE OPPORTUNITÉ ?
B14 mardi 14:45 – 15:45|Atelier BIG DATA : L'OUTIL SÉCURITAIRE ULTIME
B15 mardi 14:45 – 15:45|Atelier ANALYSE FORENSIQUE : LES NOUVEAUX DÉFIS
B16 mardi 14:45 – 15:45|Atelier CYBER THREAT INTELLIGENCE : ENTRE MYTHES ET RÉALITÉ
B17 mardi 14:45 – 15:45|Atelier COMMENT RÉUSSIR LE DÉPLOIEMENT D'UN SECURITY OPERATION CENTER ?
B18 mardi 14:45 – 15:45|Atelier QUEL RÔLE POUR LES COLLECTIVITÉS TERRITORIALES DANS LES SMART CITY ?
B19 mardi 14:45 – 15:45|Atelier RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES : QUELLES CONSÉQUENCES ?
B20 mardi 14:45 – 15:45|Atelier DE LA NÉCESSITÉ DE SÉCURITÉ DANS LES TRANSPORTS INTELLIGENTS : CHALLENGES ET SOLUTIONS
MC11 mardi 14:45 – 15:30|Master class AN APPROACH TO SHARED DATA TRACEABILITY
MC12 mardi 14:45 – 15:30|Master class DE L'HAMEÇONNAGE CIBLÉ À LA COMPROMISSION TOTALE DU DOMAINE : DÉMONSTRATION ET LIMITATION DES RISQUES
DT18 mardi 15:00 – 15:30|Démonstration technique DARKTRACE – L'ENTERPRISE IMMUNE SYSTEM : » COMMENT UTILISER L'AUTO-APPRENTISSAGE POUR LA DÉTECTION DES MENACES À L'INTÉRIEUR DU RÉSEAU ?
TV13 mardi 15:00 – 15:05|Plateau TV PRÉSENTATION DES PROJETS EUROPÉENS «ORIGIN » ET «EKSITENZ »
DT19 mardi 15:30 – 16:00|Démonstration technique SECLAB – PROTECTION TOTALE HARDWARE CONTRE LES ATTAQUES USB
TV14 mardi 15:30 – 16:00|Plateau TV NEUROSCIENCES ET ERGONOMIE PEUVENT-ELLES CONTRIBUER À RÉDUIRE LE RISQUE HUMAIN EN CYBER SÉCURITÉ ?
C16 mardi 16:15 – 17:00|Conférence PRÉSENTATION DU PROGRAMME EUROPÉEN DE RECHERCHE ET D'INNOVATION EN SÉCURITÉ : HORIZON 2020 SOCIÉTÉS SÛRES.
C17 mardi 16:15 – 17:00|Conférence MICROSOFT – PROTÉGEZ VOS ACTIFS PAR LE BIAIS DE LA CLASSIFICATION DE L'INFORMATION
C18 mardi 16:15 – 17:00|Conférence OTAN – RENFORCER LA CYBERDÉFENSE DE L'OTAN : DU SOMMET DE GALLES À CELUI DE VARSOVIE
FT10 mardi 16:15 – 16:35|Conférence PANORAMA DE LA CYBERCRIMINALITÉ
DT21 mardi 16:30 – 17:00|Démonstration technique DELL – DATA SECURITY SOLUTIONS : UNE PROTECTION DE NOUVELLE GÉNÉRATION CONTRE LES MENACES
TV16 mardi 16:30 – 16:40|Plateau TV TRAITEMENT JUDICIAIRE DE LA CYBERCRIMINALITÉ

Lien vers le site officiel
Programme FIC 2016 jour 1
https://www.forum-fic.com/site/FR/Programme/Jour_1
Programme FIC 2016 jour 2
https://www.forum-fic.com/site/FR/Programme/Jour_2
FIC 2016 Inscrivez-vous / Enregistrez-vous

Réagissez à cet article

Source : *FIC 2016*

Intel veut encore et toujours que vous enfiliez un ordinateur

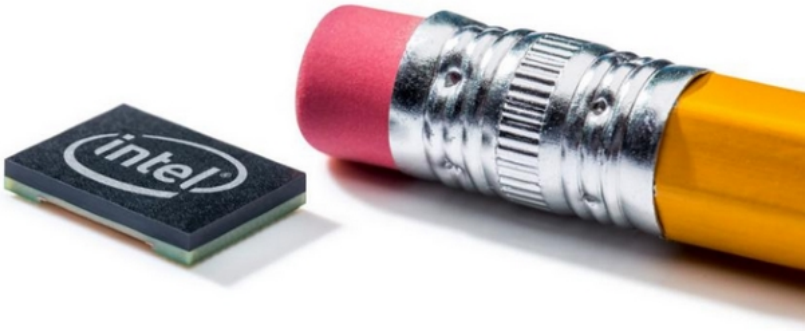


Intel veut encore et toujours que vous enfiliez un ordinateur

---

Si les objets connectés connaissent des fortunes variables, Intel creuse le sillon des wearables et met à disposition des constructeur son module Curie, un ordinateur miniature équipé de capteurs de mouvements.

Intel annonce être prêt à livrer Curie, un petit ordinateur qui pourrait aider les wearables dans leur quête de minceur. Le PDG d'Intel Brian Krzanich a annoncé lors de la keynote de la société au CES que Curie serait disponible au premier trimestre de cette année, et couterait moins de 10 dollars l'unité.



L'ordinateur Curie d'Intel, destiné au marché des wearables. (Source : Intel)

Présenté l'an passé à Las Vegas, Curie est un micro ordinateur portable qui tient littéralement dans un bouton de veste. Le PDG d'Intel en avait fait la démonstration lors de la keynote de l'édition précédente. Le tout petit ordinateur Curie est un enjeu capital pour Intel et le secteur des wearables. Protocole de communication Bluetooth, accéléromètre, gyroscope ; Intel assure que Curie possède également une batterie de longue durée de la taille « d'une pièce de monnaie ». De quoi assurer un fonctionnement constant.
Le module Curie est équipé également d'un processeur 32-bit Intel Quark, de 384ko de mémoire flash, de 80ko de SRAM et de capteurs DSP.

Diminuer la taille des équipements

De quoi aussi diminuer sensiblement la taille des équipements électroniques qui équipent montres et bijoux connectés, mais aussi proposer des fonctionnalités de suivi de la santé des utilisateurs sur des vêtements sans les déformer pour autant. Surtout, le coût additionnel de ces produits connectés serait modique.
A titre d'exemple, le PDG d'Intel a présenté sur scène deux cyclistes BMX dont la selle et le guidon de leur vélo sont équipés d'un module Curie rapporte Technology Review. Leurs cascades réalisées en direct étaient ainsi analysées en temps réel et retransmises sur un écran géant. Et si Intel se concentre si fort sur le marché des wearables, c'est qu'il s'agit pour lui d'un enjeu majeur pour enfin trouver grâce aux yeux du marché de la mobilité.

Un marché en croissance et déjà embouteillé

A noter qu'Intel est loin d'être le seul a se positionner sur le segment des composants pour wearables.Samsung vient par exemple de présenter un processeur. Côté marché, la baisse des prix provoque un certain engouement des consommateurs. L'Idate prévoit que 123 millions de wearables seront vendus en 2018.
En France, Cityzen Sciences aurait levé 100 millions d'euros en 2015 pour développer des capteurs à destination des vêtements.

Réagissez à cet article

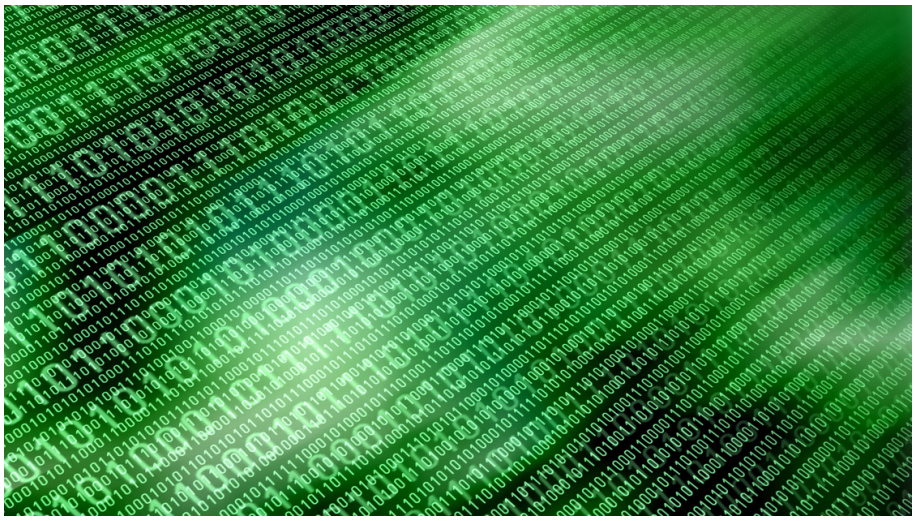
Source : *Intel veut encore et toujours que vous enfiliez un ordinateur*

Le département des Alpes Maritimes salué par la CNIL pour sa politique départementale de sécurité des données personnelles

	Le département des Alpes Maritimes salué par la CNIL pour sa politique départementale de sécurité des données personnelles

---

Le Département des Alpes-Maritimes ,1er organisme français à obtenir le Label Gouvernance Informatique et Libertés de la CNIL.



Le Département a depuis longtemps intégré le numérique comme nouvelle dimension de la vie de l'usager. Il s'est ainsi engagé formellement dans le respect du droit des personnes au travers de la mise en oeuvre d'un cadre de confiance autour de l'économie numérique en établissant une politique de gestion des données à caractère personnel. Un engagement récompensé au niveau national pour la première fois en France.
Le 22 octobre 2015, la CNIL a délivré au Département des Alpes-Maritimes le premier Label Gouvernance Informatique et Libertés tous secteurs confondus. L'obtention de ce label vient récompenser le travail des services départementaux, ainsi que l'attachement éthique du Département à la protection des données relatives aux usagers ou à celles de ses agents.
Cette distinction et les bonnes pratiques qui en découlent, illustrent ainsi, à juste titre, le comportement responsable et loyal que la collectivité a engagé en matière de réalisation et d'exploitation des données à caractère personnel.
Le Lab 06 a ouvert ses portes le 25 septembre 2015 au cœur du Centre administratif départemental. Il incarne la volonté du Département des Alpes-Maritimes de s'engager davantage dans la voie de la transformation numérique avec la création de #E-zy06 dont l'ambition est d'offrir un service public encore plus accessible quelle qu'en soit la modalité : physique, téléphonique ou numérique.
L'objectif est de faire des Alpes-Maritimes un département pionnier dans le numérique, capable d'apporter le plus grand service aux usagers.

Réagissez à cet article

Source : *La politique départementale de sécurité des données personnelles saluée par la CNIL – Département des Alpes-Maritimes*

Critical Infrastructure Sectors of Nations facing cybercrime

Critical Infrastructure Sectors of Nations facing cybercrime

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.
PPD-21 identifies 16 critical infrastructure sectors:

Chemical Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Commercial Facilities Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector.

Communications Sector
The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government.

Critical Manufacturing Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Dams Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Defense Industrial Base Sector
The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

Emergency Services Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. A system of prevention, preparedness, response, and recovery elements, the Emergency Services Sector represents the nation's first line of defense in the prevention and mitigation of risk from terrorist attacks, manmade incidents, and natural disasters.

Energy Sector
The U.S. energy infrastructure fuels the economy of the 21st century.

Financial Services Sector
The Department of Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Food and Agriculture Sector
The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Specific Agencies for the Food and Agriculture Sector.

Government Facilities Sector
The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Healthcare and Public Health Sector
The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Information Technology Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Nuclear Reactors, Materials, and Waste Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

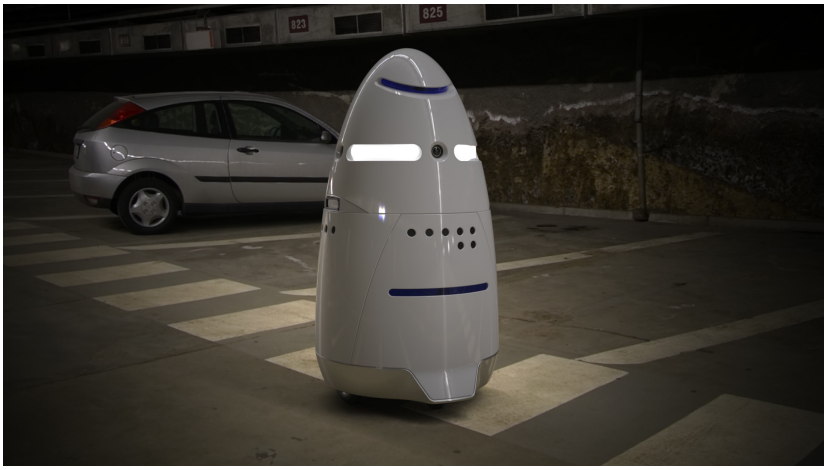
Transportation Systems Sector
The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Water and Wastewater Systems Sector
The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

Réagissez à cet article

Source : *Critical Infrastructure Sectors | Homeland Security*

Des robots sentinelle contre le crime dans la Silicon Valley



Des robots sentinelle contre le crime dans la Silicon Valley

Une start-up de Palo Alto, Knightscope, déploie dans les rues de la Silicon Valley des robots pour lutter contre le crime.

Non, ce n'est pas le pitch d'un nouveau film d'anticipation ou de science-fiction, mais bien une réalité d'aujourd'hui. Ces robots, les Knightscope K5 Security Robot, sont déjà dans les rues et patrouilles pour dissuader ou récolter des données.

Bardés de capteurs

Ces robots ne sont pas armés, ce qui pourrait arriver aux États-Unis vu les lois en vigueur dans certains états. Par contre, ils sont équipés de multiples capteurs qui leur permettent de voir à 360°, d'entendre, de sentir et de ressentir. Le système de guidage et de pilotage est le même que celui des Google Car.

Ils mesurent un peu plus d'un mètre cinquante, pèsent près de 137 kg, sont de forme ovoïde et de couleur blanche. Ils téléchargent en temps réel ce qu'ils voient et entendent et sont conçus pour réagir à des bruits significatifs comme le bris de glace ou des coups de feu. Si cela se produit, le K5 enregistre alors beaucoup d'informations sur son environnement comme la géolocalisation, photos, vidéos, plaques d'immatriculation des véhicules à proximité et même les visages des personnes proches dans l'éventualité d'une reconnaissance faciale.

Les K5 peuvent donner l'alerte aux autorités compétentes en cas de « détection » crime via une plateforme Internet accessibles aux forces de l'ordre.

Le K5 est déjà en fonction dans des centres commerciaux ou des campus universitaires comme assistant de sécurité et, selon Stacy Stephens cofondatrice de Knightscope, ils ont un très bon accueil et reçoivent même des câlins.

Le business model de Knightscope pour les K5 est MaaS, Machine-as-a-Service, et coûte 4 500 dollars par mois, pour un service 24h/24 et 7jr/7 soit 6,25 dollars de l'heure.

Toutes ressemblances avec Dalek de Docteur Who est fortuite…

Réagissez à cet article

Source : *Des robots contre le crime dans la Silicon Valley – Ere Numérique*