Comment l'intégration de l'IA dans les systèmes de détection d'intrusion peut-elle améliorer la détection des menaces en temps réel et la réponse aux incidents de sécurité ?

Tarek MAHFOUDH

Sommaire

Introduction

La sécurité proactive sert à anticiper et prévenir les attaques avant qu'elles n'aient le temps de se produire, on l'oppose à la sécurité réactive, qui quant à elle, se concentre sur la réponse aux incidents après qu'ils ne surviennent.

Avec l'évolution rapide des cybermenaces, cette approche préventive devient élémentaire.

L'intelligence artificielle joue un rôle crucial dans cette transformation et continuera d'être un élément essentiel pour les années à venir. En analysant des volumes de données massifs en temps réel, les systèmes de sécurité basés sur l'IA peuvent détecter les anomalies, pour intervenir avant qu'une brèche de sécurité ne se réalise. Cela fait donc des IA des éléments essentiels de la résilience des organisations face aux cyberattaques.

Le thème de ce rapport porte sur la sécurité proactive dans le domaine de la cybersécurité, et plus spécifiquement sur l'intégration de l'intelligence artificielle dans les systèmes de détection d'intrusion (IDS), de prévention d'intrusion (IPS), de réponse et détection sur les endpoints (EDR, endpoints étant les terminaux finaux comme les mobiles, les ordinateurs, etc.), de détection et réponse étendues (XDR = EDR + arsenal réseau), ainsi que dans les systèmes de gestion des informations et des événements de sécurité (SIEM).

La problématique centrale de cette étude est la suivante : Comment l'intégration de l'IA dans les systèmes de sécurité proactive (IDS, IPS, EDR, XDR, SIEM, etc.) peut-elle améliorer la détection des menaces en temps réel et la réponse aux incidents de sécurité ?

Cette question est essentielle dans le contexte actuel où les cybermenaces deviennent de plus en plus complexes et sophistiquées. Les systèmes de sécurité traditionnels, basés sur des règles statiques (firewall classiques) ou des signatures de malwares connus, sont souvent dépassés par l'attaquant moderne. L'IA, avec ses capacités d'apprentissage automatique et de traitement en temps réel, offre des solutions très prometteuses pour surmonter ces défis. En permettant une analyse plus fine et plus rapide des données, l'IA détecte les menaces plus tôt et fournit ainsi des réponses plus efficaces pour minimiser surfaces d'attaques et les a dégâts réalisées.

J'ai personnellement eu la chance, a travers ce projet, de rencontrer Monsieur Arthur Ebel est le Responsable de la Sécurité des Systèmes d'Information (RSSI) à l'Université de Technologie de Troyes. Fort de plus de vingt ans d'expérience dans le domaine des télécommunications et de la sécurité informatique, il a commencé sa carrière en travaillant sur des projets d'infrastructure système et réseau, mettant un accent particulier sur la sécurité. Il a pu mettre en place les procédures de sécurité, la conduite d'audits de sécurité, et la gestion des incidents cyber. Il joue un rôle clé dans le maintien et l'amélioration continue de la sécurité de l'université, notamment à travers l'adoption de nouvelles technologies et pratiques, ce qui fait de lui une source précieuse d'informations et d'insights pour ce rapport sur la sécurité proactive

I. Sécurité Proactive dans la théorie

Arsenal du bon RSSI

Pour mieux comprendre l'esprit de la proactivité en sécurité informatique, voici une liste non exhaustive qu'un RSSI avec une approche proactive pourrait déployer.

Pare-feu

Un pare-feu (ou firewall en anglais) est un dispositif de sécurité réseau qui surveille et contrôle le trafic réseau entrant et sortant en fonction de règles de sécurité prédéfinies. Un pare-feu peut être implémenté sous forme de logiciel ou de matériel, ou une combinaison des deux. Voici ses principales fonctions :

1. **Filtrage de paquets** : Le pare-feu examine les paquets IP et les autorise ou les bloque en fonction de critères définis, tels que l'adresse IP source et destination, le port et le protocole.
2. **NAT** : Le translation d'adresses réseau (NAT) permet au pare-feu de modifier les adresses IP dans les paquets réseau, ce qui contribue à cacher les adresses internes et à améliorer la sécurité.
3. **Filtrage de contenu** : Le pare-feu peut bloquer l'accès à des sites web ou à des contenus spécifiques en fonction de règles définies.

IDS & IPS

L'IDS et l'IPS sont deux technologies utilisées pour détecter et prévenir les intrusions et les attaques sur un réseau informatique. Voici une explication détaillée de chacune :

IDS (Intrusion Detection System)

Un IDS est un système de détection des intrusions qui surveille le réseau ou les systèmes informatiques pour détecter les activités suspectes et/ou malveillantes. Il existe deux principaux types d'IDS :

1. **NIDS (Network Intrusion Detection System)** : Surveille le trafic réseau pour détecter les attaques ou les comportements anormaux.
2. **HIDS (Host-based Intrusion Detection System)** : Surveille les activités d'un seul hôte ou appareil, comme un serveur ou un ordinateur individuel, pour détecter les anomalies ou les comportements suspects.

L'IDS fonctionne principalement en mode de surveillance et d'alerte. Lorsqu'une activité suspecte est détectée, le système génère une alerte pour informer les administrateurs de réseau ou de sécurité. Cependant, l'IDS ne prend pas de mesures pour bloquer ou prévenir l'intrusion.

IPS (Intrusion Prevention System)

Un IPS est un système qui va un cran plus loin. Il détecte les intrusions et activités suspectes, mais prend également des mesures pour les bloquer ou les prévenir en temps réel. Comme l'IDS, l'IPS peut être basé sur le réseau (NIPS) ou sur l'hôte (HIPS).

Les fonctions principales de l'IPS incluent :

1. **Analyse du trafic en temps réel**
2. **Prise de mesures immédiates**

En résumé, l'IDS se concentre sur la détection et l'alerte en cas d'intrusion, tandis que l'IPS ajoute une couche supplémentaire de protection en prenant des mesures proactives pour bloquer les intrusions en temps réel. Ensemble, ces technologies offrent une protection renforcée contre les menaces réseau.

Serveur de journalisation

Un serveur de log est un système centralisé utilisé pour collecter, stocker et analyser les journaux (logs) provenant de divers terminaux, applications ou outils de réseau. Voici une liste de ses fonctionnalités :

Fonctionnalités du serveur de log

1. **Collecte centralisée**
2. **Stockage sécurisé**
3. **Conformité et audits (la Loi dit de garder des traces pendant 2 à 3 ans)**

SIEM

Le SIEM (Security Information and Event Management) est une solution de sécurité informatique pour offrir une vue d'ensemble des activités et des incidents de sécurité au sein d'une organisation. Voici un aperçu des fonctionnalités d'un SIEM :

Fonctionnalités du SIEM

1. **Collecte de données** : Agrège les logs et les événements de sécurité provenant de diverses sources, telles que les pare-feux, les systèmes d'exploitation, les applications, les bases de données, et les appareils réseau et les serveurs de logs.
2. **Normalisation des données** : Convertit les données collectées en un format standardisé pour permettre une analyse cohérente et efficace.
3. **Analyse en temps réel** : Surveille et analyse les événements de sécurité en temps réel pour détecter les comportements anormaux et les incidents potentiels.
4. **Corrélation des événements** : Utilise des règles de corrélation pour relier différents événements et identifier des menaces complexes qui pourraient passer inaperçues si elles étaient analysées de manière isolée.
5. **Alertes et notifications** : Génère des alertes et envoie des notifications aux équipes de sécurité lorsqu'un incident de sécurité est détecté.

6. **Reporting et tableaux de bord** : Fournit des rapports détaillés et des tableaux de bord interactifs pour visualiser les tendances de sécurité, les incidents détectés, et les performances du réseau.
7. **Forensique et audits** : Facilite les enquêtes post-incident et les audits de conformité en conservant des enregistrements détaillés des activités et en permettant une analyse approfondie des incidents.

EPP & EDR & XDR

EPP (Endpoint Protection Platform)

Endpoint Protection Platform (EPP) est une solution de sécurité conçue pour protéger les endpoints ou terminaux en français (ordinateurs de bureau, portables, serveurs, appareils mobiles, etc.) contre les menaces de cybersécurité. Voici ses principales caractéristiques :

1. **Antivirus et antimalware** : Détection et élimination des virus, malwares et autres programmes malveillants.
2. **Pare-feu personnel** : Filtrage du trafic réseau entrant et sortant sur les endpoints.
3. **Contrôle des périphériques** : Gestion de l'accès aux périphériques externes comme les clés USB et les disques durs externes.
4. **Protection contre le phishing** : Blocage des sites web et des e-mails malveillants qui tentent de voler des informations sensibles.
5. **Mise à jour des signatures** : Actualisation régulière des bases de données de signatures pour détecter les nouvelles menaces.

EDR (Endpoint Detection and Response)

Endpoint Detection and Response (EDR) est une solution avancée de sécurité qui se concentre sur la détection, l'investigation et la réponse aux menaces sur les endpoints. Voici ses principales fonctionnalités :

1. **Surveillance en temps réel** : Surveillance continue des endpoints pour détecter les activités suspectes.
2. **Analyse comportementale** : Utilisation d'algorithmes et de machine learning pour identifier les comportements anormaux.
3. **Réponse aux incidents** : Capacités intégrées pour contenir, neutraliser et corriger les menaces détectées.
4. **Forensique et investigation** : Intégration d'outils pour mener des enquêtes approfondies sur les incidents de sécurité et comprendre la chaîne d'attaque.
5. **Threat hunting** : Capacités de chasse aux menaces pour identifier et éradiquer les menaces persistantes.

XDR (Extended Detection and Response)

Extended Detection and Response (XDR) est une solution de sécurité qui étend les capacités de l'EDR en intégrant la détection et la réponse à travers plus d'appareils ; incluant les endpoints, les réseaux, les serveurs et les applications. Voici ses principales caractéristiques :

1. **Intégration multi-sources** : Agrège et corrèle les données de sécurité de diverses sources, telles que les endpoints, les réseaux, les serveurs et les applications.
2. **Visibilité sur toute l'infrastructure** : Offre une vue centralisée et holistique des menaces et des incidents à travers l'ensemble de l'infrastructure informatique.
3. **Réponse automatique** : Automatisation des réponses aux incidents pour réduire le temps de réaction et limiter l'impact des attaques.
4. **Corrélation avancée des menaces** : Utilisation de l'intelligence artificielle et du machine learning pour corréler les événements et identifier les attaques.
5. **Efficacité opérationnelle** : Simplifie la gestion de la sécurité en réduisant les silos et en offrant une plateforme intégrée pour la détection et la réponse aux menaces.

En résumé, tout cet arsenal permet de garantir les DICP sur un réseau.

1. **Disponibilité** : Cet arsenal protège contre les attaques et les interruptions, de manière à ce que les systèmes restent opérationnels.
2. **Intégrité** : Ils détectent et préviennent les modifications non autorisées, maintenant la fiabilité et l'intégrité des données.
3. **Confidentialité** : Ils bloquent les accès non autorisés et protègent les données sensibles (pensez aux RGPD).
4. **Preuve** : Il fournit également des journaux d'activités détaillés offrant ainsi des capacités d'investigation pour documenter et prouver les actions effectuées sur les systèmes par les utilisateurs ou les attaquants, maintenant ainsi le principe de non-répudiation.

Une cybersécurité basée sur l'IA

La sécurité proactive se distingue fondamentalement de la sécurité réactive.

Alors que la sécurité réactive se concentre sur la détection et la réponse aux menaces pendant ou après leur occurrence, la sécurité proactive vise à prévenir ces menaces avant qu'elles ne se manifestent. Cette approche préventive implique une analyse continue et systématique des systèmes pour identifier et corriger les vulnérabilités potentielles.

La sécurité réactive répond aux incidents de manière immédiate, cherchant à limiter les dégâts une fois que l'attaque est en cours. Cette méthode, bien que nécessaire, peut souvent être coûteuse et moins efficace à long terme, car elle traite les symptômes plutôt que l'origine des incidents de sécurité.

L'intelligence artificielle joue un rôle crucial et même élémentaire dans l'évolution de la sécurité proactive. Les algorithmes de machine learning et de deep learning permettent de traiter et d'analyser de vastes volumes de données en temps réel. Les antivirus, firewalls, IDS et IPS traditionnels reposent souvent sur des signatures et des règles prédéfinies pour identifier les menaces. Ces systèmes, bien que efficaces contre des attaques connues, sont souvent dépassés par les menaces nouvelles et sophistiquées. Les EPP, EDR, XDR et SIEM ou tout autre outils basés sur l'heuristique, apportent une couche supplémentaire en

surveillant les activités sur les endpoints et en corrélant les données de différentes sources pour fournir une vue d'ensemble des menaces potentielles.

Grâce à l'IA, les systèmes de sécurité peuvent apprendre et s'adapter continuellement aux nouvelles menaces, améliorant ainsi leurs capacités à anticiper et prévenir les attaques. Les technologies d'IA permettent de réduire les faux positifs et les faux négatifs, de manière à offrir une détection plus précise des incidents de sécurité. Des outils tels que les EDR, les SIEM, et les XDR utilisent l'IA pour renforcer les défenses proactives des organisations.

Les outils alimentés par l'IA améliorent ces systèmes en leur permettant de détecter des schémas de comportement anormaux et de réagir de manière complètement autonome aux incidents, la prise de décision est donc aux mains de ces outils. Par exemple, un EDR basé sur l'IA peut non seulement identifier une intrusion mais aussi isoler automatiquement l'endpoint compromis pour empêcher la propagation de l'attaque. De même, un SIEM utilisant l'IA peut analyser les journaux de sécurité en temps réel pour détecter des anomalies et déclencher des alertes ou des réponses automatiques. Ces capacités renforcent significativement la posture de sécurité proactive des organisations.

II. Implémentation pratique de la sécurité proactive

1. Étude de cas : L'université de Technologie de Troyes

Description des pratiques actuelles de sécurité à l'UTT

À l'Université de Technologie de Troyes, la sécurité des systèmes d'information est une priorité essentielle supervisée par M. Arthur Ebel.

La politique de sécurité de l'UTT inclut une combinaison de mesures proactives et réactives visant à protéger les infrastructures informatiques de l'université.

Les pratiques actuelles de sécurité à l'UTT comprennent l'utilisation de pare-feux, de solutions anti-malware, et de systèmes de surveillance en temps réel pour détecter et répondre aux menaces potentielles. L'université a aussi mis en place des campagnes de sensibilisation à la sécurité pour les étudiants et le personnel, afin de réduire les risques liés aux erreurs humaines et aux attaques de phishing comme les fraudes au Président qui sont assez courantes dans notre cas. Des tests de pénétration réguliers sont également effectués pour identifier et corriger les vulnérabilités au sein du SI de l'université.

L'UTT utilise également des solutions avancées telles que les IDS et IPS. Le SIEM est quant à lui en train d'être mis en place par M. Gaëtan Henry, le stagiaire de M. Arthur Ebel. Ces outils permettent une surveillance continue et une analyse approfondie des journaux de sécurité pour identifier les comportements légèrement anormaux qui peuvent se révéler être des intrusions. Pour ce qui est de l'analyse des logs, l'UTT fait de l'infogérance avec une entreprise française qui lui fait office de SOC.

Types d'attaques courantes rencontrées à l'UTT

Lors de l'interview avec Monsieur Ebel, il nous a été rapporté que plusieurs types d'attaques courantes rencontrées à l'UTT ont été identifiées. Parmi elles, les attaques de récupération d'identifiants de connexion sont fréquentes. Les attaquants cherchent à obtenir les identifiants des utilisateurs pour accéder aux systèmes d'information de l'université avec des privilèges limités, qu'ils essaient ensuite d'augmenter. Ces attaques sont souvent détectées grâce aux systèmes mis en place par les équipes de sécurité.

[CONFIDENTIEL]

Les attaques de phishing, y compris les fraudes au président, sont également courantes à l'UTT. Ces attaques tentent de tromper les utilisateurs en leur faisant croire qu'ils reçoivent des mails de responsables de l'université, pour les inciter à divulguer des informations sensibles ou à effectuer des actions pouvant mener à des incidents de sécurité. Pour lutter contre ces menaces, l'UTT a intensifié ses efforts de sensibilisation à la sécurité pour aider les utilisateurs à reconnaître et à signaler les tentatives de phishing.

En résumé, l'UTT utilise une approche équilibrée intégrant des mesures proactives et réactives pour assurer la sécurité de ses systèmes d'information.

Les pratiques actuelles et les leçons tirées des attaques passées continuent de façonner et d'améliorer la stratégie de sécurité de l'université.

2. Stratégies de mise en œuvre de l'IA dans les outils de cyberdéfense

Intégration de l'IA dans les infrastructures existantes

L'intégration de l'IA dans les IDS et autres outils de sécurité représente un défi technique significatif. À l'UTT, plusieurs mesures techniques ont été mises en œuvre pour incorporer l'IA dans les infrastructures de sécurité existantes. Selon Arthur Ebel, RSSI de l'UTT, des outils tels que les EDR et un SIEM sont en cours d'installation pour améliorer la surveillance et la détection des menaces.

Les systèmes EDR utilisent l'IA pour surveiller les endpoints en temps réel, détecter des comportements anormaux et répondre rapidement aux incidents de sécurité. Par exemple, lorsqu'une menace est détectée, l'EDR peut isoler automatiquement l'endpoint compromis pour empêcher la propagation de l'attaque. Le SIEM, quant à lui, centralise et analyse les journaux de sécurité provenant de diverses sources, permettant une corrélation des événements et une identification plus précise des anomalies grâce à des algorithmes d'IA.

Mais ces outils, bien qu'utiles et efficaces présentent énormément de défis, notamment dans leur phase d'installation et d'implémentation.

Défis liés au déploiement de l'IA

Le déploiement de l'IA dans les systèmes de sécurité pose plusieurs défis. Monsieur Arthur Ebel souligne que l'un des principaux obstacles est le besoin de compétences techniques spécialisées pour gérer et maintenir ces systèmes. L'IA nécessite des connaissances approfondies en apprentissage automatique, en traitement de données et en cybersécurité, ce qui peut représenter une barrière pour de nombreuses organisations comme l'UTT, un organisme public, et qui doit donc justifier son besoin de budget ; chose qui est difficile en cybersécurité. De plus, la veille et la formation continue des équipes de sécurité est essentielle pour s'assurer qu'elles sont à jour avec les dernières avancées technologiques et les nouvelles techniques d'attaque.

Les contraintes budgétaires sont également un défi majeur. L'implémentation et la maintenance de solutions de sécurité basées sur l'IA peuvent être coûteuses, tant en termes d'achat de logiciels et de matériel que de formation du personnel. Comme mentionné précédemment, l'université doit souvent faire des choix budgétaires pour allouer ou non suffisamment de ressources à la sécurité tout en jonglant avec ses autres priorités

institutionnelles. Il est donc, encore une fois, crucial de pouvoir justifier ces dépenses par des améliorations tangibles de la sécurité.

Enfin ces outils ne sont pas des outils facilement et rapidement configurables. Chaque réseau est unique. Chaque organisation est unique. Et les IA qui peuvent être implémentées doivent apprendre à s'adapter. La plupart de ces outils prennent deux à dix mois d'apprentissage après leur intégration avant d'être opérationnels. L'IA doit surveiller le réseau, mais doit aussi surveiller ce que fait le SOC pour répondre aux incidents, quand il y a incident et si il y a incident. L'IA doit apprendre à discerner entre les comportements normaux et anormaux, chose qui est difficile avec un environnement aussi unique et dynamique que l'UTT.

En résumé, bien que l'intégration de l'IA dans les outils de sécurité offre des avantages significatifs, elle nécessite des investissements importants en compétences techniques et en ressources financières. Les expériences de l'UTT illustrent à la fois les opportunités et les défis de cette transition vers des systèmes de sécurité plus intelligents et surtout plus proactifs.

III. Défis et perspectives de la sécurité proactive avec l'IA

1. Défis techniques et organisationnels

L'intégration de l'intelligence artificielle dans les systèmes de sécurité proactive présente plusieurs défis techniques et organisationnels.

Problèmes de transparence et d'explicabilité : Les algorithmes d'IA, en particulier ceux basés sur l'apprentissage profond, peuvent fonctionner comme des "boîtes noires", rendant difficile la compréhension de leurs processus décisionnels. Cela pose un problème de transparence, crucial pour que les équipes de sécurité puissent faire confiance aux recommandations de l'IA et les expliquer à d'autres parties prenantes. Pour résoudre ce problème, il est essentiel de développer des modèles d'IA explicables qui permettent de comprendre comment les décisions sont prises et de vérifier leur conformité avec les politiques de sécurité de l'organisation. Pensez à l'AI ACT proposé en 2021 et signé le 13 Mars 2024 au Parlement Européen.

Gestion des données et protection de la vie privée : Les systèmes de sécurité basés sur l'IA nécessitent l'accès à de grandes quantités de données pour s'entraîner et fonctionner efficacement. Cela soulève des préoccupations concernant la confidentialité et la protection des données, en particulier dans le contexte des réglementations comme le RGPD en France et en Europe. Les organisations doivent s'assurer que les données utilisées pour entraîner les modèles d'IA sont anonymisées et protégées contre les accès non autorisés. Il est donc nécessaire pour les organisations de posséder (ou d'avoir accès) à une solution ou un modèle sur lequel ils ont souveraineté.

Compétences techniques et formation : Comme mentionné par Monsieur Ebel, le déploiement de solutions de sécurité basées sur l'IA nécessite des compétences techniques spécialisées en apprentissage automatique, en traitement des données, et en cybersécurité. Les organisations doivent investir dans l'éducation et la formation continue de leur personnel de sécurité pour s'assurer qu'elles sont à jour avec les dernières avancées technologiques et les menaces émergentes.

Contraintes budgétaires : L'implémentation de solutions d'IA peut être coûteuse, tant en termes de logiciels et de matériel que de formation et de recrutement de personnel qualifié. Les organisations doivent souvent faire des choix budgétaires pour équilibrer les investissements en sécurité avec d'autres priorités. C'est un choix (le bon) et une décision stratégique que les dirigeants de l'organisation doivent prendre pour assurer la bonne résilience de leur SI.

2. Perspectives d'évolution et de recherche

Innovations récentes et futures : L'IA continue d'évoluer rapidement, offrant de nouvelles possibilités pour la sécurité proactive. Les avancées en matière d'apprentissage automatique et d'apprentissage profond permettent de développer des systèmes de sécurité plus

sophistiqués capables de détecter des menaces inédites, sophistiquées et plus complexes. Des technologies comme le machine learning fédéré et les modèles de sécurité explicables (eXplainable AI ou XAI) sont en cours de recherche et développement pour améliorer la transparence et l'explicabilité des systèmes d'IA.

Impact de l'IA sur la stratégie de cybersécurité à long terme : L'adoption de l'IA dans la cybersécurité proactive transforme fondamentalement la manière dont les organisations perçoivent et gèrent les menaces. En automatisant cette détection et cette réponse aux incidents, l'IA permet aux équipes de sécurité de se concentrer sur des tâches à plus forte valeur ajoutée. Cette automatisation contribue également à réduire le temps de réponse aux incidents, de manière à minimiser les dégâts potentiels. À long terme, l'IA deviendra un élément central des stratégies de cybersécurité, offrant une bonne résilience face à un paysage de menaces en constante évolution.

En conclusion, bien que l'intégration de l'IA dans les systèmes de sécurité proactive présente des défis significatifs, elle offre également des opportunités prometteuses pour améliorer la détection et la réponse aux menaces. Les organisations doivent apprendre à naviguer ces défis, en investissant dans des technologies qui pourront être explicables, pour ne pas briser la chaîne de responsabilité.

Les recherches et les futures avancées façonneront la manière dont on utilise l'IA pour sécuriser les infrastructures critiques.

Conclusion

1. Résumé des points clés

L'intégration de l'intelligence artificielle (IA) dans les systèmes de sécurité proactive présente de nombreux avantages. J'ai constaté que l'IA permet une détection plus rapide et plus précise des menaces. Les systèmes basés sur l'IA peuvent analyser d'énormes volumes de données en temps réel, détectant des anomalies subtiles et réduisant les faux positifs mais aussi les faux négatifs. Cela améliore l'efficacité des mesures de sécurité et permet une meilleure anticipation des attaques potentielles.

Cependant, cette intégration n'est pas sans problèmes. Il y a des obstacles techniques, comme le besoin de compétences spécialisées en apprentissage automatique et en cybersécurité, ainsi que (et surtout) des contraintes budgétaires. De plus, il est essentiel de garantir la transparence et l'explicabilité des modèles pour maintenir la confiance des utilisateurs. La gestion des données et la protection de la vie privée restent des préoccupations majeures, notamment en conformité avec les réglementations comme le RGPD, l'ISO 2700x, etc.

L'importance de la sécurité proactive est claire : anticiper et prévenir les attaques pour non seulement minimiser les dommages mais aussi renforcer la résilience des organisations face aux cybermenaces. Les pratiques de sécurité proactive, soutenues par l'IA, permettent une réponse plus efficace et plus rapide aux incidents de sécurité, assurant une protection continue des systèmes d'information.

2. Réflexions finales

Pour maximiser les avantafes de l'IA en cybersécurité, une collaboration étroite entre les experts en sécurité et les développeurs d'IA est cruciale. Cette coopération favorisera l'avenir de la recherche en solutions de sécurité plus robustes et adaptées aux besoins des organisations. Il est également nécessaire de noter l'importance d'adopter une approche équilibrée et éthique dans l'utilisation de l'IA pour la cybersécurité, en s'assurant que les systèmes sont transparents et respectueux de la vie privée de toutes et tous.

En conclusion, bien que l'intégration de l'IA dans les systèmes de sécurité proactive présente des défis, elle offre des opportunités significatives pour améliorer la détection et la réponse aux menaces. Les organisations doivent investir dans des technologies explicables (XAI), protéger les données et former continuellement leurs équipes pour naviguer avec succès dans ce paysage en constante évolution. Les avancées futures continueront de transformer l'utilisation de l'IA pour sécuriser les infrastructures critiques.

Annexe:

Transcript conversation avec Mr. Ebel

Tarek MAHFOUDH : Bonjour Monsieur Arthur Rebel, c'est un plaisir de vous recevoir aujourd'hui. Alors rapidement, est-ce que vous pouvez vous présenter et nous décrire votre rôle dans le domaine de la cybersécurité ?

Arthur EBEL : Donc Arthur Ebel, moi je suis ingénieur. Il se trouve que je suis ingénieur en télécommunications, promotion 1999. Je travaille a la direction numérique depuis 2001 et je suis responsable de la sécurité des systèmes d'information depuis début 2024. Avant cela, j'étais suppléant et je m'occupais principalement de projets d'infrastructures système et réseau, mais avec un fort accent sur la sécurité, notamment les firewalls, les VPN, les scanners, enfin tout ce qui concerne la sécurité. Maintenant, je suis plus impliqué dans la partie stratégique, les procédures, les audits, et des choses comme ça. Donc, moins de technique et plus de gouvernance.

Tarek MAHFOUDH : Ok, merci beaucoup. Et du coup, qu'est-ce qui vous a inspiré a travailler dans ce domaine spécifique ? Est-ce que c'était une appétence pour tout ce qui était informatique quand vous étiez jeune ou est-ce que c'est vraiment par hasard que vous avez choisi cette branche ensuite ?

Arthur EBEL : Non, ce n'était pas par hasard. J'étais attiré par l'informatique assez jeune. Ça fait un peu cliché, mais j'ai eu mon premier ordinateur quand j'avais dix ans. C'était le début, il n'y avait pas d'Internet, rien de tout ça. Et puis ma scolarité s'est orientée vers des études plus scientifiques. J'ai fait une prépa après le bac en maths physique.

Tarek MAHFOUDH : MPSI ?

Arthur EBEL : Oui, c'est ça. Mais a l'époque, ça ne s'appelait pas comme ça. J'ai fait une année seulement parce que ça ne me correspondait pas vraiment, c'était un peu trop intense. Donc après, j'ai fait un DUT en génie électrique et informatique industrielle. Ensuite, j'ai postulé a plusieurs endroits et l'UTT (Université de Technologie de Troyes) venait d'ouvrir. J'ai été accepté dans leur programme informatique, qui s'appelait GCD a l'époque, avec une spécialisation en télécommunications et réseaux d'entreprise. J'ai obtenu mon diplôme en 1999. Après cela, j'ai travaillé dans le privé pendant deux ou trois ans, notamment dans une startup qui a malheureusement fait faillite. Un poste était disponible a l'UTT, j'ai postulé et depuis, je suis ici.

Tarek MAHFOUDH : Très bien, et vous êtes épanoui dans votre travail ?

Arthur EBEL : Ça va. Épanoui est un grand mot. En vingt ans, on fait un peu le tour de tout ce qui se passe sur la partie infrastructure réseau. Même si les technologies évoluent constamment, a un moment donné, on a envie de voir autre chose. C'est pour ça que j'ai proposé ma candidature au poste de directeur l'année dernière, pour sortir du maintien en condition opérationnelle et de la sécurité technique, et aller vers plus de gouvernance. Le contexte actuel, avec les attaques cyber qui font la une des médias chaque semaine, se prêtait bien a ce changement. Donc, je me suis proposé et ils ont accepté.

Tarek MAHFOUDH : De ce que j'ai entendu, vous êtes quelqu'un de très compétent et on ne cesse de chanter vos louanges. C'est pourquoi je suis la pour vous interviewer. Alors, pour comprendre les menaces cyber aujourd'hui, est-ce que vous voulez qu'on parle de manière générale ou plus spécifiquement de votre expérience ? Je pense qu'il serait utile de couvrir les deux aspects. Quels sont les types de cyberattaques les plus courantes selon vous ?
Arthur EBEL : Moi, je vais parler de ce qu'on vit a l'UTT. Nous faisons face principalement a ce qu'on appelle des attaques de récupération d'identifiants de connexion. Les attaquants essayent d'obtenir ces identifiants pour se connecter au système d'information avec quelques privilèges, et ensuite augmenter leurs privilèges. Il y a régulièrement des scans de vulnérabilités, des personnes extérieures qui cherchent les failles et les portes ouvertes sur nos systèmes. En ce moment, nous subissons pas mal de fraudes au président, où des emails prétendent venir du président ou de quelqu'un d'autre. Ces emails ne sont pas très bien faits, mais quelqu'un qui n'est pas averti peut se faire piéger.

Tarek MAHFOUDH : Comme Monsieur Lionel Amodeo, hier ?

Arthur EBEL : Oui, c'est ça.

Tarek MAHFOUDH: C'était marrant car une amie venait de sortir de son examen et m'a demandé si j'avais reçu ce mail étrange. Il ne ressemblait pas du tout a un mail du professeur.

[CONFIDENTIEL]

Arthur EBEL : C'est tout un programme que j'essaie de mettre en place depuis fin 2023 pour améliorer ces points. Il y a maintenant une obligation légale d'homologation de sécurité pour tous les services que nous proposons. Toutes les applications mises en ligne doivent passer par cette homologation. Nous posons des questions aux développeurs et obtenons un cyber score pour évaluer la sécurité de l'application. Si nous avions fait cela, nous aurions pu éviter le problème avec cette application.

Ensuite, il y a des mesures techniques comme l'installation d'EDR (Endpoint Detection and Response) et de SIEM (Security Information and Event Management) pour la détection des événements de sécurité. Malgré toutes les mesures techniques, une attaque ciblée peut

toujours réussir. C'est pourquoi il faut également organiser des exercices de gestion de crise pour sensibiliser la direction et préparer des plans de reprise d'activité et de continuité.

Tarek MAHFOUDH : D'accord. Vous avez défini les PRA et PCA ?

Arthur EBEL : C'est en cours. Cette année, nous travaillons sur l'analyse des risques et la politique de sécurité de l'information, avec l'aide d'une société spécialisée. Nous espérons avoir le temps et le budget pour finaliser les plans de reprise et de continuité d'activité cette année, sinon ce sera pour l'année prochaine.

Tarek MAHFOUDH : Quelle société vous accompagne ?

Arthur EBEL : C'est une société appelée [CONFIDENTIEL].

Tarek MAHFOUDH : Ça marche. Euh justement, vous avez parlé de... euh, est-ce que je peux vous poser une dernière question avant de plonger dans tout ce qui concerne le DSI, RSSI, etc. ? Ça va être une question un peu marrante parce que vous allez vous dire "OK, il est taré" ou bien "il ne m'écoute pas". Quelle décision assez importante en rapport avec votre emploi avez-vous dû prendre dernièrement ?

Arthur EBEL : Non, ce n'est pas une décision, enfin ce n'est pas... c'est une bonne question. Je parle de...

Tarek MAHFOUDH : De décision parce que c'est un petit peu le sujet de ce que tu veux.

Arthur EBEL : Le rôle du RSSI dans l'organigramme, on va dire au niveau fonctionnel, je suis directement rattaché au directeur de l'établissement, Christophe Collet. C'est lui qui est l'autorité qualifiée pour la sécurité des systèmes d'information. On est dans une école publique. Tout ça, c'est vachement codifié. En fait, c'est lui qui a la responsabilité de la sécurité informatique ici, donc je suis directement sous lui. Donc c'est lui qui va prendre les décisions importantes. D'accord, c'est moi qui vais le conseiller. Euh, c'est moi aussi qui vais demander au DSI de mettre en place des choses. Euh, la chose qui a été la plus... euh, pas difficile mais... euh, c'est de mettre un système en ligne, un serveur. Donc dernièrement, à un moment donné, quand tu constates une attaque, ce qu'il faut éviter, c'est la latéralisation de l'attaque. Oui, donc ça s'étale. Donc pour ça, tu isoles la machine. Mais la machine, c'est un serveur avec des services dessus. Quand tu isoles, tu pénalise les utilisateurs. Si c'est de la messagerie, t'as plus de messagerie, etc. Donc à un moment donné, tu dis maintenant il faut isoler, donc je dis je vous conseille, il faut vraiment isoler cette machine.

Tarek MAHFOUDH : Pour un certain délai ?

Arthur EBEL : Ouais, la tu ne sais pas parce que tu ne sais pas ce qui arrive. T'as pas le temps d'analyser, tu sais qu'il y a un truc qui ne va pas. Donc moi, j'ai vu sur la machine

qu'elle était en train de se faire chiffrer, ça s'est passé en plein jour. Je l'ai vu en direct, en fait. Donc la on s'est dit la ça ne va pas et donc voila, tu coupes, mais après il faut analyser parce que tu ne sais pas d'où c'est venu et tu ne sais pas quels sont les dégats. Tu ne sais pas s'ils sont déja allés sur les côtés, etc. Donc tu ne sais pas pour combien de temps tu coupes. C'est ça qui est compliqué. C'est ça qu'on va te poser comme question et donc la pire des décisions, enfin ce n'est pas pire, c'est ce qu'il faut faire. La, on a isolé une machine, mais tu peux être amené a isoler tout ton système d'information. Tu peux t'isoler d'Internet aussi. Et la, au niveau communication, au niveau image, c'est compliqué en fait.

Tarek MAHFOUDH : D'accord. Ben merci beaucoup. Euh, très bien, je pense qu'on a assez d'informations pour finir cette partie, comprendre les menaces d'aujourd'hui. Maintenant, on va plonger dans le cœur du sujet. Je sais que vous m'avez dit que vous n'aviez pas de système d'IA qui était utilisé dans le cadre de la cybersécurité, mais je pense qu'on va faire sans. Ce n'est pas grave.

Arthur EBEL : On va y venir hein, on va y venir.

Tarek MAHFOUDH : Oui je sais, j'ai des questions par rapport a ça aussi. Ok, c'est des questions un petit peu bateau pour le début. Euh, déja ces deux dernières années, qu'est- ce que ça vous évoque cette montée en puissance de l'IA ? C'est vrai que quand on y pense, il y a deux ans et après quand on dit montée en puissance, l'exemple parfait c'est GPT, c'est l'IA générative, mais c'est une des nombreuses utilisations de ces systèmes. Et donc si on voit d'où GPT est parti jusqu'a où il en est maintenant, on ne peut qu'imaginer pour les autres systèmes quelle évolution ils ont eu. Et donc justement, qu'est-ce que ça vous évoque ? Est-ce que ça vous effraie ? Est-ce que ça vous excite ? Est-ce que vous êtes un petit peu dans cet engouement ?

Arthur EBEL : Non ? Moi, je suis plutôt dans la partie excitation technologique du truc. Je suis vraiment la-dedans. J'ai suivi la semaine dernière la sortie de GPT-4 qui a fait grand bruit. Évidemment, je l'ai essayé dès que c'était possible. Euh, alors on fait attention a ça, nous, pour s'en servir. Maintenant, on travaille beaucoup avec des terminaux pour accéder a nos serveurs et nous, on est quasiment que sous Linux, donc c'est quasiment que de la ligne de commande. Donc, les terminaux proposent maintenant de s'appuyer sur des API avec les IA. Au lieu de faire, je sais pas si tu connais, des recherches sur une fonction, sur un truc pour savoir comment ça marche. Tu poses la question a l'IA dans ton terminal et elle te répond, elle te donne la syntaxe.

Tarek MAHFOUDH : Comment ça ? Une IA dans un terminal ?

Arthur EBEL : Bah, c'est connecté en API sur un GPT ou quelque chose comme ça.

Tarek MAHFOUDH : Donc c'est une ligne de commande du style "GPT espace" et puis tu poses ta question entre guillemets ?

Arthur EBEL : Il y a une espèce d'assistance comme ça qui existe maintenant, qui est vachement déployée. On fait attention parce qu'on sait très bien, moi en tant que responsable de sécurité, je sais que tu envoies tes données a l'extérieur sur ces choses- la. Donc j'ai mis en garde mes collègues, il faut vraiment éviter de faire ce genre de choses-la, mais ça existe quoi. Donc je trouve qu'a titre personnel, c'est génial. La, on va voir avec GPT-4, au niveau assistant personnel, ça va être top. Le côté multimodal, il est génial aussi. Le fait de pouvoir interpréter des images, de l'audio, etc. Au niveau de nos métiers. Le problème, c'est qu'il faut qu'on ait nos IA en interne en fait, ou qu'on ait un truc au niveau souverain français, mais qu'on ne fasse pas comme avec Google, je dirais, pour aller filer nos données a l'extérieur. On ne peut pas taper des lignes de commande dans un truc qui envoie a l'extérieur et qui nous aide. En fait, on ne peut pas faire ça. Donc ça va être super si on arrive a avoir un modèle français pour l'État dans ce qui nous concerne et savoir que c'est sécurisé. La aussi, la où c'est dangereux, c'est évidemment que les attaques vont être plus sophistiquées. Mais c'est déja le cas en fait maintenant et depuis longtemps qu'il existe des scripts, des scripts pour les enfants en fait. Tu lances une attaque en cliquant sur un bouton sans rien comprendre, tu récupères un script, tu lances et ça va repérer un truc. Donc maintenant, je veux dire, les attaques, c'est assez facile a lancer, ça va être encore plus facile a lancer.

Tarek MAHFOUDH : D'accord.

Arthur EBEL : Donc c'est ça qui me fait peur.

Tarek MAHFOUDH : Ok.

Arthur EBEL : Pardon, mais ça va nous aider a sécuriser aussi.

Tarek MAHFOUDH : Vous avez bien compris la transition. Ouais, c'est ça. Bah déja, attends, avant d'aller vers le côté défense, est-ce que vous pensez que, quels outils d'IA, j'appuie sur le côté IA, est-ce que les attaquants utilisent a votre avis, a votre sens ? Parce que moi déja, je me dis, bon allez, même les IA génératives en soi, parce que vous m'avez dit que la première des cybermenaces c'était les... c'était le... et donc ils pourraient être la. Bref, ils...

Arthur EBEL : vont pouvoir générer des mails qui sont vachement plus pertinents et percutants que les mails un peu nuls d'avant, qui sont mal écrits et pas bien formulés. Donc ça, ça va être méchant. Ils vont... enfin, je veux dire, tu interroges n'importe quel modèle, comment on appelle ça, modèle de langage, genre GPT-like, mais il y en a d'autres hein ! Tu lui demandes ce qu'est l'Université de Technologie de Troyes et il va te répondre ce que c'est, donc toute la partie ingénierie sociale va être plus facile.

Tarek MAHFOUDH : Exactement. Et j'aime aller plus loin parce qu'il y a un truc un peu fou avec ça, c'est que je suis quasiment sûr que si on allait sur Google et qu'on tapait le nom de

votre collègue pour lequel quelqu'un s'est fait passer dernièrement, il saurait exactement qui c'est. Et donc ça, c'est quelque chose que je trouve un peu fou. Euh, c'est que GPT connaît des gens et se permet de donner des infos assez précises. Enfin, voila, c'est...

Arthur EBEL : Comme... bon, on a déja ça sur un moteur de recherche standard aussi hein. Si tu fais une recherche sur des enseignants de l'UTT, bah ils ont déja fait des publications, ils sont déja référencés donc GPT se base aussi sur ces connaissances-la.

Tarek MAHFOUDH : Mais la, ce que je veux dire, c'est qu'on n'a pas vraiment besoin de faire le travail de copier-coller. On peut dire, "fais-moi un mail parce que j'ai besoin de ça et ça", et avec une IA assez rapide, je pense qu'on peut se faire passer pour n'importe qui avec une présence en ligne. Euh, ok, ça c'est une question qui m'intéresse. Quels outils est-ce que vous utilisez personnellement dans votre travail ? Qui n'ont rien a voir avec l'IA.

Arthur EBEL : Ah, donc pas avec l'IA.

Tarek MAHFOUDH : Ben vous m'avez dit qu'il n'y en avait pas.

Arthur EBEL : Si t'es la la semaine prochaine en R23, je te montrerai.

Tarek MAHFOUDH : Je suis en R23 la semaine prochaine et je serai présent a votre cours.

Arthur EBEL : Donc je te montrerai les outils qu'on utilise. Ce qui peut être intéressant comme outil, euh, alors maintenant je fais de moins en moins de technique, mais euh, les principales consoles que j'utilise, c'est la partie sécurité, plutôt sur l'IPS, les logs qui font une détection d'attaque. On est entre quinze et trente attaques arrêtées par semaine en ce moment par l'IPS, d'accord, qui arrête donc principalement l'IPS. La partie SIEM qu'on est en train de monter avec mon collègue Gaétan, euh, qui va nous permettre de faire de la détection et de l'alerte. Parce que la, on a ce qu'on appelle un SIEM et puis le SOC, mais c'est plutôt d'un point de vue réglementaire qu'on a ça, et ils ne sont pas exploités. On les exploite a posteriori parce qu'il y a tellement d'événements par seconde que... il y a tous les équipements, tous les serveurs qui arrivent la-dedans, donc ça défile a une vitesse incroyable en fait. Donc il faut qu'il y ait quelque chose qui analyse, qui passe les logs et qui cherche, qui détecte. Ce sera le SIEM qui va faire ça. En fait, j'en avais monté un il y a cinq ans. Euh, ça marchait bien. Mais voila, on a eu une augmentation de la capacité des logs, il n'a pas tenu au niveau de la charge. Et puis on a un peu laissé tomber le truc et déja a l'époque, c'était Elastic, qui est assez connu et qui proposait un modèle d'IA qui était payant, donc qu'on n'avait pas pris. Mais ils avaient déja a l'époque un petit modèle qui appelait ça l'IA. C'est très marketing en ce moment, donc il faut faire attention quand même a ce qu'on dit. Euh, ils proposaient en fait de l'apprentissage avec les logs et de pouvoir faire de la détection.

Tarek MAHFOUDH : C'est un petit peu ça a quoi on s'attend dans un...

Arthur EBEL : Film, non. Voila, c'est faire la corrélation d'événements et se dire "waouh, ça c'est pas top en fait". Et souvent c'est collé, c'est superposé a ce qu'on appelle la matrice MITRE ATT&CK. Je ne sais pas si tu vois ce que c'est. Ah oui, on a une matrice en fait qui part de la phase de reconnaissance jusqu'a l'exploitation. On essaie de détecter déja les phases de reconnaissance, puis après il y a toutes les phases successives d'une attaque jusqu'a ce que tu prennes les identifiants, tu fasses l'escalade de privilèges et puis tu fasses de la latéralisation. Donc ça, c'est bien décrit. Donc le SIEM est normalement capable de détecter ces attaques-la puis de te prévenir en fait.

Tarek MAHFOUDH : Ok. Justement, on a parlé de DSI, d'IPS... Enfin, a mon sens, une des choses auxquelles j'ai pensé immédiatement quand on m'a dit "ok, mettre de l'IA dans les outils de cybersécurité", c'était les techniques heuristiques. Bah déja, si vous voulez que je l'explique, je l'explique moi-même si vous savez ce que c'est ou pas.

Arthur EBEL : Non, je sais que ça existe, mais ça existait déja au niveau des antivirus, hein ? C'est une méthode d'apprentissage.

Tarek MAHFOUDH : Oui c'est ça. Grosso modo, c'est non pas analyser ce qui est fait, mais analyser le comportement et l'intention du programme ou l'intention de l'utilisateur ou ce qui est fait sur le réseau. Et donc quand on parle de SIEM, ce serait pas vraiment essayer de voir exactement ce qui est fait mais de comprendre un peu le comportement et l'intention qu'il y a derrière cet événement-la. Donc vous avez dit qu'il y en avait dans les antivirus, ce qui est le cas. Et justement, la suite de ma question, c'est est-ce que ce sont des techniques qui sont déja mises en place dans les antivirus aujourd'hui ?

Arthur EBEL : Les analyses heuristiques ? Ouais, par contre, enfin la ça fait six mois qu'on est un peu sur le sujet hein et on est même un peu en retard par rapport à des boîtes du privé. Mais voilà, ça demande des investissements importants dans ces outils-la. Il y a vraiment le monde du SIEM, le monde de l'EDR, XDR, tout ça commence à émerger en fait, à se mélanger donc il y a des fois on ne comprend pas bien. Il y a des SIEM qui font EDR, XDR, il y en a qui ne le font pas. EDR, XDR, mais c'est quoi par rapport a un antivirus ? Puis maintenant on ne parle plus d'antivirus, on parle d'EPP. Donc les trucs basés sur des signatures, on n'en veut plus quoi. Il faut qu'on mette en place ça. Donc le point de départ, c'est vraiment la défense, que ce soit un serveur ou un poste de travail. Donc c'est pour ça qu'on cherche à mettre en place un EDR et l'EDR, il fait l'analyse comportementale. Donc quand on met en place un EDR, il y a une phase d'apprentissage, généralement qui dure deux mois où l'EDR va être en mode passif. Il ne va pas faire de réponse à l'incident. Il va faire de la détection et à nous gestionnaires d'analyser ce qui se passe et de dire "ça, c'est un comportement normal" ou "ça ne l'est pas". Donc en fonction des différentes applications, ceux qui travaillent au service manufacturier n'ont pas les mêmes applications que des chercheurs qui font des trucs avec des logiciels peu connus. Donc en fonction des différents profils, on va roder l'outil. Enfin c'est lui qui va faire de l'apprentissage parce que c'est de l'IA. J'imagine qu'il y a une base d'IA dedans mais c'est plutôt de l'apprentissage pour dire "ça

c'est normal, ça c'est pas normal". Et au bout de deux mois, une fois qu'on a fini cette période-la, on fait de la réponse à incident automatique. Donc si on voit une dérive du comportement sur la machine, il va pouvoir bloquer un processus et voir même isoler la machine du réseau.

Tarek MAHFOUDH : Non, c'était une super réponse, merci. J'ai juste une question qui vient de me traverser l'esprit : où s'arrête le SIEM et où commence l'IA pour vous ? Parce que pour moi, je me disais la ce que vous décrivez c'est du SIEM mais je pense qu'on a peur de mettre le mot dessus, mais concrètement c'est la même technologie, donc où sont les limites de l'un et de l'autre ?

Arthur EBEL : J'irai pas sur ce chemin-là parce que je ne connais pas en fait ce domaine. J'ai jamais étudié. Ok, je vois un petit peu ce que sont les méthodes d' apprentissage. Euh, quand on me dit "réseau de neurones", je comprends un petit peu ce qu'il y a derrière. J'ai peut-être lu deux trois trucs mais je ne connais absolument pas ça d'accord. Donc je ne peux pas aller la-dedans et je sais juste qu'on met trop l'étiquette IA sur tout. Il faut faire attention et c'est très, très, très vendeur. À chaque fois que tu contactes un éditeur de logiciel en ce moment, il dit "ouais, on a un module IA". Il faut faire super gaffe à ça, c'est pour vendre, c'est tout. Donc comprendre ce qu'il y a derrière, c'est pas évident. Il faut être prudent.

Tarek MAHFOUDH : Ouais non mais en fait ma question elle est... tu vois il...

Arthur EBEL : Il y a différentes IA, ouais. Les LLM, les Large Language Models, c'est de l'IA. Euh, mais il y a d'autres trucs enfin, ça, c'est ce qui est le plus courant en ce moment. Mais il y a d'autres choses quoi.

Tarek MAHFOUDH : Oui, mais je suis d'accord avec vous. Mon discours n'était pas vraiment axé sur le terme IA en lui-même. Dès que, par exemple, vous me dites "allez, un EDR qui apprend et qui fait du machine learning", je n'ai pas envie d'un truc compliqué. Je n'ai pas envie d'avoir un truc très complexe qui va bouffer du processeur et auquel je vais devoir allouer tout un serveur. J'ai juste envie d'une solution simple qui fait ce qu'elle doit faire et qui ne pose pas de problèmes.

Arthur EBEL : Notre besoin, maintenant, avec les éléments de sécurité, c'est qu'il y a énormément d'événements, tu ne peux pas faire la corrélation tout seul, tu ne peux pas faire la détection tout seul. Donc t'as besoin d'avoir un outil fiable qui fait l'analyse pour toi. IA ou pas IA, je ne sais pas comment on l'appelle, mais voila, il faut qu'il fasse l'analyse et qu'il nous sorte des alertes.

Tarek MAHFOUDH : Ok, vous avez dit un truc assez intéressant qui m'a vraiment un peu titillé. À un moment, vous avez dit tout ce qui est IDS, IPS, EDR, XDR, SIEM... Tout ça rentre un peu plus dedans pour avoir un outil ultime. Vous n'avez pas donné la partie outil ultime,

mais j'imagine que c'est un peu ça a quoi vous pensiez. Est-ce que vous pouvez m'en parler plus ? Pourquoi pensez-vous que ces outils distincts sont en train de se regrouper ?

Arthur EBEL : Ils mélangent toutes les technologies pour essayer de prendre le meilleur de chacun. Euh, t'as des solutions qui font a la fois EPP, donc les antivirus de nouvelle génération. Pour bien comprendre la différence entre un antivirus et un EDR : l'antivirus va simplement regarder ce que tu télécharges sur ton poste et l'analyser avant qu'il soit dessus et l'arrêter. L'EDR ne fait pas ça en fait. L'EDR va analyser un comportement. "Tiens, c'est bizarre, ce processus-la commence a faire du chiffrement" ou des choses comme ça. Donc c'est pas la même chose. Euh, mais voila, t'as des outils maintenant qui font EPP, EDR, XDR. Le XDR, c'est l'EDR élargi, pas uniquement aux terminaux comme les postes Windows ou Linux, mais aussi tu vas pouvoir balancer dans un XDR les journaux d'événements de sécurité de tes équipements réseau. Donc on va encore un cran plus loin avec XDR, c'est qu'on prend tous les logs de l'infrastructure, pas uniquement des applicatifs. Et paf, on balance ça aussi dans ce puits énorme. Donc le truc ultime, c'est ce qu'on essaie d'avoir la, c'est d'avoir tous ces logs la. On les balance quelque part. Euh, nous, on n'a pas la capacité, on n'a pas un SOC ici, on n'a pas une équipe assez grosse pour avoir des analystes cyber qui vont analyser tout ça. Donc on va essayer de sous-traiter ça, a un prestataire. Euh, donc on devrait pouvoir envoyer ces choses-la dans un contexte contractuel avec toute la partie légale, respect de la vie privée, etc. Et eux, ils ont des outils automatiques, ils ont des SOAR (Security Orchestration, Automation, and Response) pour orchestrer les réponses a incident ou des choses comme ça. Ils vont analyser et c'est eux qui vont nous dire un peu comment ça se passe, mal ou pas mal. On va sous-traiter ça.

Tarek MAHFOUDH : D'accord, c'est très clair, merci. Euh, partie trois, et la vraiment ça va aller très vite. Euh, d'ailleurs quand je vous pose des questions par exemple "pouvez- vous partager des exemples où l'IA serait décisive pour détecter une intrusion", vous avez absolument le droit de dire "non je ne pense pas que l'IA est ultimement décisive pour détecter une intrusion". Donc euh vraiment, si vous voulez nuancer, nuancez, donc voila.

Arthur EBEL : Attends, juste pour dire encore une fois, hein, je ne connais pas ces technos. Ouais, c'est super compliqué de me prononcer. J'ai pas envie de dire des bêtises, tu vois. Donc euh, il faut me prendre comme un néophyte sur ces niveaux de l'IA. Je connais plus la partie sécurité mais cette brique-la... mais vas-y.

Tarek MAHFOUDH : Très bien, d'accord. Euh, comment l'IA améliorerait-elle les systèmes de détection d'intrusion ? Et la maintenant que vous m'avez dit "ok, les experts et les SIEM c'est un peu l'avenir", d'ailleurs question pour vous, est-ce que le SIEM regroupe les logs et analyse un peu tout de la même manière, pour centraliser les logs et centraliser l'analyse des logs ? C'est pareil non ?

Arthur EBEL : L'XDR, ouais. C'est pour ça que je te dis des fois ça regroupe vraiment le SIEM. À l'origine, c'était vraiment je sais plus dire, un système d'information, de gestion des

événements de sécurité. Quelque chose comme ça. En fait, c'était un endroit où c'était un syslog un peu amélioré, plus graphique où tu avais tes événements de sécurité qui étaient la. Et puis on commençait a pouvoir compter, il y avait un peu une partie graphique pour compter les événements, les regrouper, faire des recherches, etc. Euh, les logs étaient remis en forme, donc c'était beaucoup plus exploitable. Et puis au fur et a mesure, on a rajouté la détection, etc. Donc effectivement quand on parle, je dirais, un des plus connus, c'est Elastic. Euh, maintenant Elastic est considéré comme un EDR et un XDR. Ils ont sorti des agents qu'on installe sur les postes et ça fait EDR et XDR aussi, d'accord ? Tout le monde se lance sur ce marché-la.

Tarek MAHFOUDH : Ok, ok, merci.

Arthur EBEL : Donc alors, dis-moi ce que pourrait... L'IA, vas-y pose tes questions.

Tarek MAHFOUDH : Je préfère vos questions a vous. Bon alors, j'ai des questions un peu bateau, vous savez, quelle est l'efficacité de l'IA par rapport aux méthodes traditionnelles, par exemple ? Vous pouvez dire "je ne sais pas".

Arthur EBEL : Alors je pense que je l'ai déja dit. Moi je crois que ça pourra aider pour traiter des volumes importants de données, mais également pour traiter des attaques qui ne sont pas connues, des comportements nouveaux.

Tarek MAHFOUDH : D'accord, ok. Personnellement, j'aurais tendance a croire le contraire. L'IA fonctionne de manière... enfin après si on disait "allez, tu vas apprendre de l'intention", oui, mais si on va dire "ok, on va te balancer des attaques et tu vas les apprendre derrière", c'est un peu limitant par rapport aux attaques zero-day. Vous me direz quoi ?

Arthur EBEL : Je te dis, tu fixes, tu bloques, tu dis ça c'est un comportement normal. Tarek, il se connecte a Moodle généralement le weekend, le dimanche, entre dix-sept heures et vingt-et-une heures depuis une IP française. Tiens, on voit que tu as une connexion depuis une IP russe. Je prends un exemple comme ça quoi. Et puis c'est pas le dimanche, c'est le samedi, alors que d'habitude le samedi il sort avec ses copains. C'est un comportement qui n'est pas normal. Donc ces choses-la, chaque utilisateur a un comportement particulier, on ne peut pas le savoir. Donc il faut que le système l'apprenne. Qui dit "ça c'est normal, ça c'est pas normal", etc. Et après qu'il puisse détecter ça. On ne sait pas faire ça a la main ou etc. Alors s'il y a besoin d'IA pour faire ça je ne sais pas, mais c'est pour ça que ça pourrait aider. C'est vraiment au niveau comportemental.

Tarek MAHFOUDH : Et justement, dans votre vision de la chose, vous diriez "ok, on doit maintenir notre souveraineté sur cet outil-la et donc il doit être contenu dans l'infrastructure UTT" ou du moins française, ou du moins ça doit être français.

Arthur EBEL : Moi j'ai deux problèmes en ce moment. Quand on parle de souveraineté au niveau d'EDR, il y a un acteur français qui est vachement bien, qui s'appelle HarfangLab. On a vu la démo, c'est cool hein ? Ils sont français, c'est bien et au niveau des SOCs, il y a Orange Cyberdefense qui est très connu, ils sont français donc c'est cool. Mais il y a d'autres solutions d'EDR qui ne sont pas françaises mais qui sont mieux. Et comment on fait ? On reste en France, on prend du moins bien. Les produits français ne sont pas, de ce qu'on a vu, au niveau top du top. Mais voila donc c'est une question qu'on se pose. Et après c'est vraiment au niveau des contrats, au niveau des contrats que tu fais avec ton fournisseur, qu'il faut être attentif en fait. Mais euh, il y a une chose que je pourrais répondre si les gens... bon je détourne un peu la question mais admettons qu'on installe un outil d'EDR comme ça qui n'est pas français d'accord mais qui fait partie de nos alliés. Euh on va dire c'est pas bien, il faut garder la souveraineté sauf que vous utilisez Windows non ? C'est pas toi mais voila, la majorité, ben c'est pas français donc le principal problème c'est votre système d'exploitation. Déja réglons déja ça. Donc on essaie de privilégier les solutions françaises. On essaie de privilégier les solutions qui sont, euh j'ai oublié le terme, certifiées par l'ANSSI. D'accord ? C'est souvent les solutions françaises. Ouais parce que les solutions commerciales américaines, ça ils aiment pas trop ouvrir leur code pour que l'on regarde dedans.

Tarek MAHFOUDH : D'accord.

Arthur EBEL : C'est dans les critères de choix mais la c'est bon.

Tarek MAHFOUDH : J'ai d'autres questions un petit peu. Attendez, on peut parler encore de l'IA dans les systèmes d'intrusion ou on peut passer a la gouvernance. Qu'est-ce que vous préférez ?

Arthur EBEL : La gouvernance. Parce que je te dis, c'est pas... voila, l'IA, ce sera dans la partie EDR. Il y en aura aussi dans la partie SIEM. Et voila ce que je peux dire.

Tarek MAHFOUDH : La-dessus, très bien. Ok, passons alors, moi aussi je préfère ça. Alors du coup, puisqu'on a parlé de l'ANSSI, de souveraineté nationale... On a parlé des États- Unis, de la Russie. Qui dit RGPD, dit aussi protection des données bancaires, personnelles, médicales, etc. Donc ma question est : est-ce que sur le front légal, on encourt des risques vis-a-vis de l'utilisation de l'IA avec les soucis de vie privée, soit avec la divulgation, soit avec l'entraînement continu ? Parce que les données sont très respectées en France et en Europe, non ?

Arthur EBEL : Vraiment, c'est très réglementé avec le RGPD, c'est très contraignant. Donc nous ici on a un DPO, Data Protection Officer, qui est le pendant du RSSI mais pour la partie RGPD. Donc on est attentif a tout ça. T'as oublié une directive qui va sortir qui s'appelle NIS 2, une directive européenne au niveau de la sécurité. Ça va être aussi contraignant, c'est un peu comme le RGPD pour la sécurité. Donc c'est une directive européenne, NIS version 2, qui va être transposée dans le droit français bientôt. Donc on va avoir des obligations légales

en termes de sécurité comme on a des obligations légales au niveau RGPD. C'est-a-dire qu'au niveau RGPD, on est obligé de déclarer les données personnelles que l'on conserve sur vous, étudiants par exemple. Dans notre cas, combien de temps, etc. Donc tout ça c'est déclaré. Euh, au niveau de l'IA, je pense que c'est a peu près pareil que les autres services des GAFAM. Parce qu'on peut maintenant inclure GPT au même titre que Google. Ils récupèrent de la data pour entraîner leurs modèles et puis qu'est-ce qu'ils en font ? On ne sait pas. Tu utilises GPT gratuitement, c'est pas normal. T'imagines les infrastructures qu'il y a derrière pour faire tourner ça. Donc tes données, bah c'est tes données privées en plus. Je ne sais pas ce que tu écris a GPT mais ça peut être utilisé. Donc la il n'y a pas de réglementation et en plus c'est aux États-Unis. Donc ça serait quand même mieux qu'on ait des modèles français. Alors je crois qu'ils en ont sorti un, j'ai oublié le nom, Claude, je crois, qui va être plus orienté pour de l'aide. Je ne sais pas si ça va être plus un chatbot ou autre chose, mais ça serait bien alors ce qu'on arrivera a être au niveau de...

Tarek MAHFOUDH : Mais est-ce que vous y croyez vraiment a la souveraineté française dans ce domaine-la ? C'est Mistral d'ailleurs.

Arthur EBEL : Mistral. Donc il y a un truc que je...

Tarek MAHFOUDH : Parce qu'en soi, avec toutes ces réglementations, avec toutes les règles qui sont mises en place, elles freinent un peu l'innovation. Elles freinent un peu l'avancée puisque, d'un côté... Après, si vous voulez, on va en parler. Qu'est-ce qu'ils font concrètement ? Ils nettoient leurs données avant de...

Arthur EBEL : Comme très intéressé, je vais te conseiller un livre que j'ai lu dernièrement qui va bien t'ouvrir l'esprit sur ça, qui met en parallèle l'innovation et la peur de la fuite des données. C'est quelqu'un qui s'appelle Alain Damasio qui écrit de la science-fiction généralement et la qui a fait un essai...

Tarek MAHFOUDH : Avec un Z, Damasio ?

Arthur EBEL : Oui, M. Corp qui s'appelle... J'ai oublié le nom, ça doit être "La vallée du silicium" ou quelque chose comme ça. Je vais te trouver le titre. Donc Alain Damasio, il a été dans la Silicon Valley pendant un mois, ou deux, je ne sais plus. C'est quelqu'un qui est très... qui écrit beaucoup sur la liberté, l'autonomie des gens, un peu anarchiste, on va dire. Mais voila, il fait le constat qu'on a ramené les restaurants chez nous avec la livraison, les rencontres chez nous avec les applications de rencontre, le cinéma chez nous avec Netflix. Donc il y a un repli, voila. En attendant, ils ont toutes nos données. Ils ont maintenant les données médicales avec tous les objets connectés, etc. C'est quand même super dangereux de balancer ton rythme cardiaque, ton poids, ton machin, etc. en ligne a quelqu'un, tu ne sais pas ce qu'il en fait. Il analyse les voitures autonomes aussi. Voila, t'es aux États-Unis, t'as des taxis autonomes qui parcourent la ville tout le temps. C'est comme en Chine, c'est super déployé tout ça. Donc il dit attention, il parle de lien, il parle de la réalité augmentée. Lis ce

bouquin-la, il est vachement bien, très bien. Donc il y a quand même des dangers a tout ça, de perdre un peu notre autonomie et d'être un peu trop assisté par tout ça aussi quoi. On va perdre un peu de créativité.

Tarek MAHFOUDH : Ouais, mais justement ma question derrière c'était... Euh, vous ne pensez pas que toutes ces réglementations et toutes ces lois, qui d'un point de vue éthique sont totalement légitimes, sont un frein pour la créativité et le développement et l'innovation française ?

Arthur EBEL : C'est le parti pris de la France de protéger un peu plus, beaucoup plus qu'aux États-Unis. Et on voit que les États-Unis, l'innovation est plus présente, c'est vrai, et il y a moins de protection. Donc euh, tu veux créer ta start-up aux États-Unis ?

Tarek MAHFOUDH : Non, non, ça ne m'intéresse pas. Après, ce que je voulais dire, c'est que ce n'est pas seulement aller prendre des données. Il y a des scandales sur, je ne sais pas si vous savez, par rapport a l'exploitation et le fait de payer des Indiens une misère pour traiter les tonnes et les tonnes de données qu'ils reçoivent. Derrière, il faut les nettoyer, il faut être sûr que ce n'est pas de la daube. Donc il y a des gens derrière en Éthiopie et en Inde qui traitent toutes ces données, qui regardent, qui lisent avant de dire ok, c'est validé et on peut le balancer a GPT-4. Donc quelque part, on sacrifie un peu l'éthique pour l'innovation. Et après, c'est un choix comme vous avez dit, les États- Unis permettent, la France ne le permet pas.

Arthur EBEL : Oui, sur les réseaux sociaux, les modérateurs regardent un peu les contenus avant de publier les vidéos de n'importe qui. Et ça c'est fait a la main aussi, hein. Mais euh, oui, donc c'est un frein pour l'innovation mais je pense, je préfère être sur le modèle français. Voila, que sur le modèle américain. Je suis bien content qu'il y ait ces garde-fous ici. Euh, jusqu'a quand ? Je sais pas. Est-ce qu'on est capable de faire ça en France ? Bien, ouais je crois. Parce que tu vois, en termes d'hébergeur, on n'a pas d'équivalent d'Amazon ou de Google hein, c'est sûr, ou de Microsoft. On n'a pas d'équivalent. Bizarrement OVH, il se démerde pas mal. Donc il y a un moment donné ils ont sorti aussi la partie pour avoir vraiment une protection sécurité française, etc. Bah on n'a pas tout mais ça suffit largement pour faire plein de choses. Donc il faut vraiment réfléchir avant de se faire héberger chez Amazon ou je ne sais pas où. Je comprends, il y a des grosses boîtes où c'est important, mais dans la plupart des cas t'as des hébergeurs français, j'en ai cité un, mais il y en a d'autres. Et puis en Europe, qui répondent très très bien. Donc nous, ce qu'on fait ici, c'est qu'on héberge chez OVH. Voila, pas tout, mais nous on héberge chez nous la plupart des choses, notre politique c'est du on-premise. Et c'est compliqué parce que maintenant tous les éditeurs te demandent de mettre les choses en SaaS a l'extérieur. Donc nous on essaie de refuser et de mettre tout dans notre...

Tarek MAHFOUDH : Tous les auditeurs ?

Arthur EBEL : Éditeurs de logiciels.

Tarek MAHFOUDH : Ah, d'accord.

Arthur EBEL : Ah, vous voulez pas mettre ça en SaaS ? Non non non, on va mettre ça ici chez nous. Donc voila, on essaie de garder tout chez nous comme ça t'as la maîtrise de tes données.

Tarek MAHFOUDH : D'accord, ok c'est très intéressant. Et justement, je voulais juste mentionner l'incroyable étude de Mistral. Ben justement, Mistral est une entreprise française et elle fait concurrence a GPT même si elle est plus dans le respect des données, RGPD, etc. Donc je ne sais pas comment ils font mais bien joué a eux.

Arthur EBEL : Une force aux États-Unis, c'est qu'ils arrivent a obtenir des investissements colossaux, donc travailler a perte, sans gagner d'argent au début, hein, parce qu'il y a des investissements. On est moins capable de faire ça en France, je pense.

Tarek MAHFOUDH : Euh justement, pensez-vous que l'introduction de l'IA pour l'aide a la décision, qu'elle soit stratégique, opérationnelle ou technique, peut induire une perte de compétence des utilisateurs de ces outils ? Et si oui, dans notre domaine, comment est-ce qu'on peut l'éviter ?

Arthur EBEL : La, c'est compliqué de répondre. Il y a les deux. Les gens vont perdre leurs compétences, c'est sûr. Je le vois avec moi ou avec mes enfants, ou la génération de mes parents. Avant, tu n'avais pas Internet, puis tu as eu Internet. Après, mes enfants ont les réseaux sociaux, tu commences a avoir de l'IA. Évidemment, on apprend moins. Enfin, je ne sais pas comment expliquer ça. On a moins besoin de se servir de notre mémoire peut- être, puisqu'on a beaucoup d'assistants qui nous aident. Je prends des références personnelles. Mon grand-père, par exemple, avait une connaissance en physique avec toutes les formules, a quatre-vingt ans, il les répétait. Nous, maintenant, notre génération ne serait plus capable de le faire, parce qu'on sait qu'on a une bibliothèque universelle en ligne disponible tout le temps. Donc de cette manière, on est moins bons quand même. Mais on a besoin de résoudre des problèmes, je pense, plus complexes qu'avant. Donc on a besoin des outils qui nous aident, qui nous accompagnent, un peu comme une extension, en fait, un peu comme un boost. Enfin, je ne sais pas comment expliquer ça, mais c'est ça, on a besoin de ça. Parce que les défis a relever, pas qu'en informatique mais dans tous les domaines, sont tellement compliqués maintenant qu'on a besoin d'une assistance. Évidemment, si c'est mal utilisé... Mais tu vois, je pense par exemple a l'enseignement, on est dans une école. Il faut continuer d'enseigner les fondamentaux, c'est obligé. Il faut que les gens comprennent comment ça fonctionne. Il ne faut pas uniquement savoir utiliser, mais il faut savoir comment ça fonctionne. Moi, j'hallucine que les générations, pas forcément celle de maintenant, mais les jeunes avec les smartphones, ne savent pas ce qu'est Internet. Ils savent ce qu'est une appli, c'est tout. Mais ils ne vont pas savoir ce qu'est une URL. Ils ne vont pas connaître comment

ça marche les échanges client-serveur. L'arrivée du smartphone, ça a été un truc, je pense, qui n'a pas aidé. Enfin, qui a fait perdre beaucoup de compréhension de l'informatique. C'est tellement facile a utiliser. T'as tellement tout a portée de main que les gens ont l'habitude, ils ne savent même pas qu'il y a du réseau, des serveurs derrière.

Tarek MAHFOUDH : C'est fou ! C'est fou de se dire qu'aujourd'hui on a une abstraction dingue pour ne pas connaître l'architecture qu'il y a derrière.

Arthur EBEL : Ça, je pense que c'est vraiment l'iPhone qui a introduit ça. Ils ont été très forts la-dessus.

Tarek MAHFOUDH : Très bien, c'est une super réponse. Je pense justement que ça va être encore pire avec les technologies. Mais je suis un peu plus mitigé que vous et je dirais même que tout va dépendre de comment on les utilise. Mon téléphone, par exemple. Certes, c'est quelque chose qui peut être horrible dans les mains d'un enfant qui n'a absolument aucune idée, mais pour moi, je sais un peu ce que je fais, j'ai zéro jeu dessus. Je l'utilise uniquement pour travailler, ouvrir mes mails, etc. Prendre des photos, partager des trucs et rester en contact avec ma famille. Donc pour moi, tout ce que le téléphone me ressort, c'est bon. Allez, a part quelques vidéos sur Instagram, il y a que du positif.

Arthur EBEL : Mais si on parle des IA génératives, hein, moi je m'en sers pour faire de la reformulation de texte par exemple, ou des choses comme ça. Tu sais que maintenant t'es capable de déposer un PDF dessus et de lui demander un résumé. Ouais, tu perds ta compétence de lecture et de synthèse. Tu veux un résumé ? Non, tu lis et puis tu fais le résumé toi-même. On va perdre ça si on ne le fait plus. Moi je m'en sers pour, pas pour rédiger des textes entiers, mais pour reformuler, pour trouver des synonymes, pour voir si... voila, c'est pas mal. Mais tu peux générer un texte en entier, tu t'en fous, ça marche.

Tarek MAHFOUDH : C'est vrai.

Arthur EBEL : Les gens vont le faire par simplicité. Ouais, je crois que les gens vont opter pour la simplicité.

Tarek MAHFOUDH : Ah ouais, d'accord, je vois, je vois absolument ce que vous voulez dire. Mais j'aurais tendance a dire que si tu gagnes du temps avec ça, fais-le, mais assure-toi de savoir le faire sans l'outil.

Arthur EBEL : T'arrives a te repérer, a conduire sans GPS ?

Tarek MAHFOUDH : Euh, je ne suis jamais allé a Paris en voiture.

Arthur EBEL : N'importe où. Oui.

Tarek MAHFOUDH : Oui, je peux rouler sans GPS, mais tu le fais ou pas ?

Arthur EBEL : La plupart des gens ne le font plus, ils dépendent du GPS. Tu vois, les gens maintenant sont incapables de prendre une carte et d'essayer de se repérer. On a perdu cette notion d'orientation a cause de ça. Mais bon, c'est un outil génial.

Tarek MAHFOUDH : Je vois ce que vous voulez dire et vous avez raison. Maintenant je dirais que pour cet exemple de Google Maps, il faut apprendre a se repérer sans ça, il faut apprendre a le faire. Après, on n'est pas obligé de le faire a chaque fois, mais il faut le faire. Par exemple, faire des synthèses, faire des résumés. La raison pour laquelle je peux me permettre d'utiliser des outils pour faire tout ça, c'est parce que j'ai passé toute ma scolarité a le faire. On m'a dit "Ok, lis ce livre, fais-moi un résumé, lis cet essai, fais-moi un résumé", et je m'en suis bien sorti. Je suis un élève brillant, incroyable.

Arthur EBEL : Je regarderai tes résultats après.

Tarek MAHFOUDH : Non, ne regardez pas du tout mes résultats à l'UTT. Mais bon bref, vous avez le droit de regarder mes résultats justement en parlant de RGPD.

Arthur EBEL : Je ne suis pas dans l'administration.

Tarek MAHFOUDH : Bah merci beaucoup, c'était vraiment super sympa de discuter avec vous.

Arthur EBEL : C'était pour quelle UE ?

Tarek MAHFOUDH : Ça ? C'est pour l'UE "Prise de décision à l'ère de l'IA". C'était avec Madame Loubna, maître de conférences.

Arthur EBEL : D'accord, donc ça va nous aider mais ça aidera aussi les "méchants" entre guillemets. Ça va équilibrer un peu. Il faut qu'on sache utiliser les outils parce qu'eux, ils vont savoir les utiliser aussi.

Tarek MAHFOUDH : D'accord, merci beaucoup pour ça. Voila, au revoir Monsieur.