Lettre mensuelle – Janvier 2020 – Disponible sur omc.ceis.eu

Table des matières

ANALYSES (1/2)

IOT : LA QUESTION DU MAINTIEN EN CONDITION DE SÉCURITÉ

Parmi les problématiques de sécurité qui minent l'Internet des Objets (IoT) figure la difficulté, voire parfois l'impossibilité, d'assurer leur maintien en condition de sécurité (MCS) : il n'est pas toujours possible pour l'utilisateur de corriger les failles de sécurité découvertes à l'aide d'une mise à jour logicielle.

Les caractéristiques de ces dispositifs qui les rendent attractifs sont également celles qui rendent difficile leur sécurisation : faible coût, faible taille, accessibilité à distance. Conséquence de cela, un nombre important de ces objets sont produits en masse par des entreprises qui se focalisent sur la réduction des coûts, sans perspective de maintenance logicielle. Les objets qui avaient vocation à avoir un très long cycle de vie, comme des interrupteurs ou des serrures, sont remplacés aujourd'hui par des objets connectés qui deviennent obsolètes en quelques années.

Si cet état de fait est moins problématique pour des objets très basiques qui ont vocation à être jetables et donc disparaître avant de se révéler porteurs de vulnérabilités exploitables, ceci est plus difficilement acceptable pour les dispositifs plus complexes et au cycle de vie plus long. Il existe pourtant des exemples d'objets connectés qui bénéficient d'un réel suivi. On peut citer l'exemple des smartphones, pour lesquels l'industrie a beaucoup progressé dans ce domaine. On se situe ici dans le haut du panier en termes de valeur et de capacités pour un objet connecté, et il reste beaucoup à faire pour les objets intermédiaires au cycle de vie indéfini, qui peut aussi bien être déterminé par des critères d'obsolescence (subjectif) que de panne.

Pour demain, l'arrivée de la 5G laisse entrevoir une accélération du déploiement d'objets connectés directement à Internet, sans dispositif intermédiaire de sécurité. À l'aube de cette nouvelle vague, quel est l'état de l'art de la maintenance en condition de sécurité des objets connectés ? Quelles difficultés sont à surmonter et quelles sont les perspectives pour l'avenir ?

1. Les difficultés de maintenance logicielle des objets connectés

Du côté du fabriquant, les plus petits dispositifs sont contraints par les très faibles ressources en mémoire ou en capacités dont ils disposent. Certains possèdent un type de microprocesseur qui ne contient qu'un jeu limité d'instructions, rendant certaines opérations impossibles. Ces limites empêcheront généralement le déploiement de solutions de détection de menace sur le dispositif lui-même (*endpoint*) et l'utilisation de chiffrement, renforçant encore davantage le risque et les possibilités de mise à jour.

D'autres dispositifs plus puissants voient leur capacité de mise à jour limitée par le régime juridique qui les encadre. Certains objets sont effectivement soumis à des certifications, qui ne valent que pour un produit défini, statique d'un point de vue matériel et logiciel : il ne sera pas possible de faire évoluer ce dernier sans que le produit final ait également été certifié. Ceci va concerner par exemple les dispositifs médicaux.

Du côté opérateur/utilisateur final, il existe plusieurs difficultés de maintien de contrôle :

- La multiplication des dispositifs dans l'environnement rend difficile le maintien d'un inventaire et d'une cartographie des objets déployés ;
- La difficulté à disposer d'une solution de suivi unificatrice : l'Internet des objets rassemble de nombreuses technologies de communication différentes (Cellulaire, WiFi, bluetooth, Zigbee, Sigfox, LoRaWAN, NFC, etc.) ;
- Le risque de perte de fonctionnalité, notamment du côté de l'interopérabilité, voire l'échec du processus de mise à jour menant à une panne définitive.

2. Quel mode de maintenance ?

Trois types de maintenance logicielle peuvent être distinguées :

- **Un système de mise à jour manuel**. L'opérateur final doit réaliser une veille sur l'existence de nouvelles versions du micrologiciel de l'objet, et décider ou non de procéder au téléchargement et à l'installation de la nouvelle version. Étant donnée la multiplication de ces objets, cette option n'apparait pas satisfaisante.
- **Un système de mise à jour semi-automatique**. Le dispositif final vérifie automatiquement l'existence d'une mise-à-jour et le notifie à l'utilisateur, qui doit faire le choix de procéder ou non à celle-ci. Ceci prévient le risque d'interruption des opérations en cours (ou futures dans le cadre d'une perte de fonctionnalité due à la mise à jour), mais fait porter le risque d'un report prolongé d'une mise à jour qui aurait pu permettre d'éviter un incident de sécurité. Les constructeurs de smartphone choisissent généralement cette méthode.
- **Un système de mise à jour automatique**. Dans ce cadre, l'utilisateur final est retiré de la boucle de décision, en définissant un processus où le choix par défaut est l'installation du patch. C'est par exemple le choix de Microsoft par exemple pour ses systèmes d'exploitation. Il reste néanmoins possible pour l'utilisateur final de modifier cette configuration, mais ce système est pertinent pour la majorité des cas d'usage, notamment pour le grand public.

Face à l'effervescence du déploiement de ces objets, l'utilisateur/opérateur final a besoin de bénéficier d'un mode de maintenance semi-automatique ou automatique. En effet, si le processus de mise-à-jour n'est pas automatique ou semi-automatique, comment informer et permettre aux utilisateurs finaux, notamment le grand public, de réaliser ces mises-à-jour ? Dans son livre « *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* », Bruce Schneier compare les cas Tesla et Chrysler. Tesla assure le MCS de ses voitures connectées de façon automatique, alors que Chrysler a dû rappeler 1,4 millions de véhicules afin de corriger une faille de sécurité, car la seule alternative était d'envoyer aux propriétaires une clé USB à brancher sur le *dashboard* de leur véhicule.

Il faut cependant préciser que l'existence d'un système de mise à jour fait également porter un risque aux produits concernés. En effet, cela implique qu'il existe un vecteur pour remplacer le software de l'objet qui peut être exploité par un attaquant. Un système de mise à jour efficace protège de cette menace via l'utilisation de certificats, de telle sorte que l'objet n'accepte que les mises à jour signées par le constructeur. La sécurité du fournisseur devient critique car :

- La compromission des clés privées du fabriquant permet à un attaquant de créer des updates malicieux ;

- Dans le cas d'un déploiement piloté directement par le fabricant, sa compromission peut provoquer la compromission du parc de tous ses clients.

3. Perspectives

Il existe des solutions sur lesquelles les fabricants et les intégrateurs peuvent se reposer pour assurer la maintenance logicielle de leurs produits, telles que Mender ou Asvin[1].

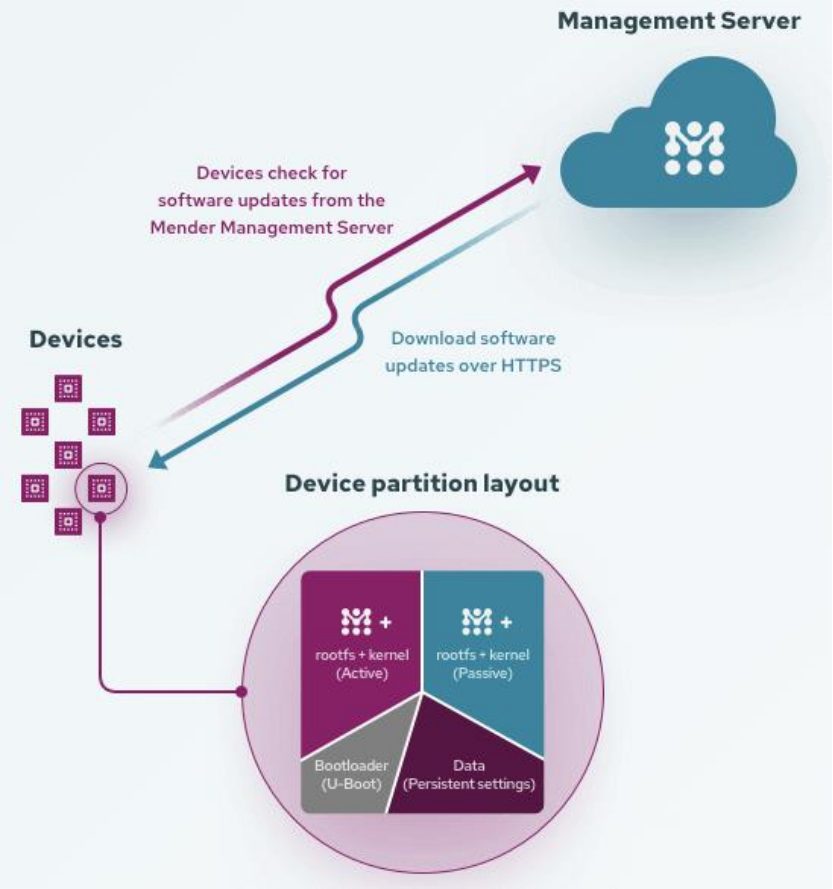


Figure 1 : Architecture de maintenance logicielle Mender[2]

De son côté, l'IETF (Internet Engineering Task Force) commence à appréhender le problème avec le groupe de travail SUIT[3] (Software Update for Internet of Things). Ce dernier vise à répondre au besoin d'un mécanisme de mise à jour des micrologiciels de tout objet connecté, notamment ceux dont les ressources sont restreintes.

[1] https://mender.io/ ; https://www.asvin.io/
[2] https://mender.io/overview/how-it-works
[3] https://datatracker.ietf.org/wg/suit/about/

Le processus de mise à jour du micrologiciel doit répondre aux prérequis suivants :

- Être opérable sur des dispositifs aux ressources très limitées ;
- Le protocole de mise à jour doit être agnostique quant au moyen de transport des images de *Firmware* et des *Metadata* associés vers l'objet ciblé (USB, UART, WiFi, etc.) ;
- Permettre une haute fiabilité. Ceci en prévoyant soit deux instances du micrologiciel de façon à ce que l'un puisse prendre le relai en cas d'échec d'installation de l'autre (correspondant à l'architecture de Mender plus haut), soit un bootloader capable de reprendre une mise à jour interrompue ;
- Être à l'état de l'art en matière de fonctionnalités de sécurité, à savoir notamment :
    - L'image du micrologiciel doit être authentifiée et son intégrité protégée, de sorte à rendre impossible le mise à jour du dispositif avec une image modifiée ou provenant d'une source inconnue ;
    - L'image du micrologiciel doit être protégée de façon à ce qu'aucun adversaire ne puisse obtenir les fichiers binaires du micrologiciel ;
    - Une protection contre les attaques de type *Rollback* (installation par un attaquant d'une version plus ancienne du micrologiciel afin d'exploiter une vulnérabilité ancienne).
- Permettre plusieurs modes de mises à jour : initialisation par le client, par le serveur, ou hybride.

Du côté juridique, le RGPD a introduit plusieurs principes qui concernent directement les objets connectés dont le *Privacy by Design* et le *Security by Default*. Aux États-Unis, le Congrès a introduit en 2019 un nouveau texte visant à imposer aux administrations un certain nombre d'exigences pour tout objet connecté qu'elles achètent, notamment le maintien en condition de sécurité[4]. Au Royaume-Uni, le gouvernement a publié en octobre 2018 le *Code of Practice for Consumer IoT Security*[5], qui propose aux fabricants d'indiquer explicitement la période minimale de maintenance logicielle, et a annoncé en 2019 son intention de légiférer sur cette base.

Et en attendant ? Plusieurs axes peuvent être recommandés aux opérateurs finaux :

- La segmentation. Pour reprendre l'expression de Mike Loyd, CTO de RedSeal, il faut considérer les objets connectés comme des « bébés-bulle » : possédant un système immunitaire défaillant, il est nécessaire de les isoler dans un environnement stérile afin de les protéger des menaces[6].
- Le monitoring constant de la surface d'exposition, notamment à Internet. On notera à ce sujet que la compagnie d'assurance cyber Coalition vient tout juste d'annoncer le rachat de BinaryEdge, un scanner de vulnérabilité de dispositifs connectés à Internet. Ce rapprochement vise à intégrer ce service à l'offre d'assurance afin de mieux évaluer le risque de l'assuré pour mieux définir le montant de sa prime, et a fortiori de le responsabiliser davantage.

[4] https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=88A88A37-AD5E-4C01-932D-A23684AAD7AE
[5] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security
[6] https://www.darkreading.com/edge/theedge/what-do-you-do-when-you-cant-patch-your-iot-endpoints/b/d-id/1336196

ANALYSES (2/2)

ÉTAT DES LIEUX DES NOUVELLES SOLUTIONS DE « DÉCEPTION »

La tromperie est une tactique utilisée depuis des siècles par les armées et le renseignement pour se défendre contre l'ennemi. Par des techniques dites de « déception », c'est-à-dire la mise en œuvre de leurres aussi réaliste que possible, le défenseur peut par exemple être en mesure de détecter une attaque et y répondre plus habilement ou encore de connaitre les capacités et les intentions d'un attaquant. Ces techniques présentent un grand intérêt pour la cybersécurité et le développement des moyens de cyberdéfense du fait notamment que les cyberattaques sont encore difficiles à détecter rapidement. Les premières solutions de « déception » font leur apparition dans les années 2000 avec le développement des « honeypots »[7] (en français « pots de miel »). Cependant, ces solutions se révélent rapidement inefficaces d'un point de vue opérationnel et leur utilisation se limita à la recherche en cybersécurité. En effet, les difficultés à reproduire les activités quotidiennes d'un système d'information (SI) ont rendu facilement détectables les « honeypots » qui manquaient alors de réalisme[8].

Aujourd'hui, de nouvelles solutions de « déception » nettement plus évoluées et plus dynamiques émergent sur le marché et relancent l'intérêt de l'utilisation de la tromperie comme moyen de cyberdéfense et repose la question de l'efficacité de ce type de solution. Si ces nouvelles solutions sont prometteuses au niveau opérationnel et pourraient bien redonner l'avantage à la défense contre les cyberattaques, leur niveau de maturité nécessite encore que leur efficacité opérationnelle soit démontrée avant d'être déployées dans les systèmes d'information du défenseur.

Des solutions prometteuses pour redonner l'avantage au défenseur

En matière de cybersécurité, les techniques de « déception » ont évolué depuis l'émergence des « honeypots » classiques et apportent désormais de véritables nouveautés qui pourraient bouleverser les moyens de cyberdéfense actuels[9]. Elles offrent notamment la capacité pour le défenseur de prendre l'avantage sur l'attaquant, ce qu'aucune solution actuelle sur le marché n'est en mesure de proposer[10]. Des

[7] *« Un honeypot une méthode de défense active qui consiste à attirer, sur des ressources identifiées et prévues à cet effet (serveur, programme ou service) des attaquants, déclarés ou potentiels, de manière à les identifier pour neutraliser, par la ruse en collectant des informations sur leurs méthodes et comportements, les futures attaques sur le réseau de l'entité considérée. Un honeypot pourra prendra la forme d'une ou plusieurs machines virtuelles plus ou moins isolées du reste du réseau de l'entreprise* » (Honeypots et sinkholes, outils de défense active, OMC, Lettre n°64, Juillet 2017)

[8] https://cybersecurite-hq.fr/2017/06/nouvelle-approche-de-cyber-defense-les-leurres-pour-detecter-les-attaques-furtives/

[9] https://www.sciencedirect.com/science/article/abs/pii/S1361372319300089

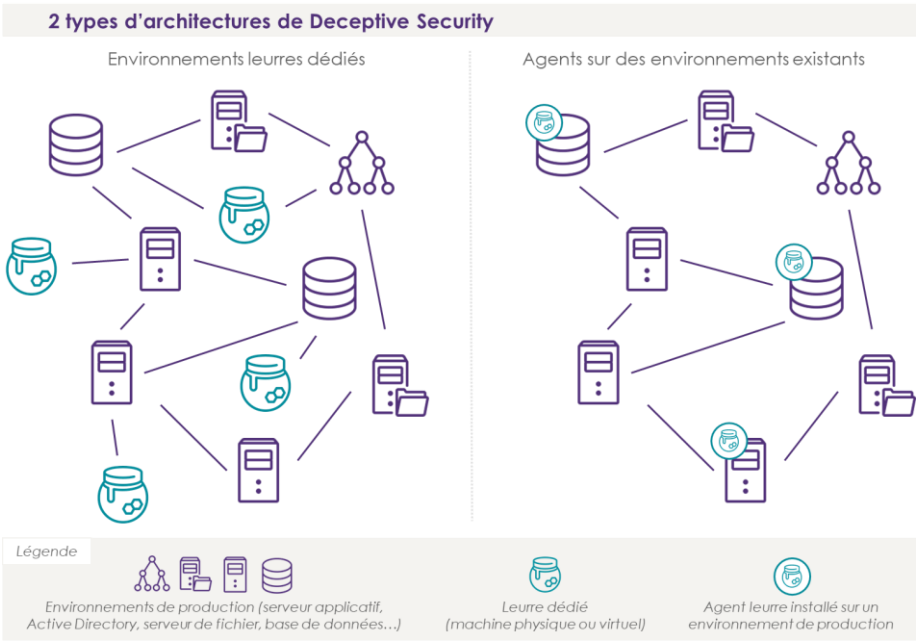
[10] https://www.forbes.com/sites/danwoods/2018/06/22/how-deception-technology-gives-you-the-upper-hand-in-cybersecurity/#42ce070c689e

solutions concrètes et opérationnelles sont aujourd'hui déployées par des sociétés plus ou moins spécialisées, notamment aux États-Unis, en Asie mais aussi en Europe.

Les nouvelles solutions de « déception » utilisent des outils pour leurrer un cyberattaquant, qui peuvent être déployés sur un maximum de ressources du véritable système d'information du défenseur. Ils disposent d'une meilleure capacité de leurrage que les « honeypots » classiques[11]. Ces outils peuvent parfois, en diffusant de fausses informations notamment, volontairement inciter le cyberattaquant à réaliser certaines actions au profit du défenseur. De manière générale, les nouvelles solutions de « déception » mettent en œuvre deux types de leurres :

- Des « agents » installés sur des ressources informatiques du défenseur comme un serveur de production par exemple ;
- Des « leurres dédiés » qui sont des machines physiques ou virtuelles placées sur des segments réseaux et qui reproduisent un produit, un service ou une application utilisée par le défenseur.

Schéma des deux types de leurres



(*Source : https://www.riskinsight-wavestone.com/2017/11/deceptive-security-comment-arroser-larroseur/*)

Plus spécifiquement, il est possible également d'identifier différentes catégories d'outils de « déception » comme par exemple[12] :

[11] https://www.riskinsight-wavestone.com/2017/11/deceptive-security-comment-arroser-larroseur/

[12] https://securitytoday.com/Articles/2019/08/12/How-Deception-Technology-Can-Help-You-Detect-Threats-Early.aspx?Page=2

- Les « honeypots » comme leurres dédiés ;
- Les « honey users » ou « honey credentials » qui sont des utilisateurs ou identifiants leurres ayant des accès privilégiés pour inciter les cyberattaquants à les utiliser/usurper et qui permettent de détecter une connexion malveillante ;
- Le « géo-tracking » qui consiste à placer dans les fichiers qui sont volés un outil de collecte et de transmission des données IP et de localisation à l'équipe de sécurité ;
- Les « sinkhole servers » (ou « DNS sinkhole ») qui ont pour fonction de rediriger un cyberattaquant ou un malware vers un domaine maitrisé par l'équipe de sécurité.

Les nouveaux outils innovent aujourd'hui par leur capacité à répondre à trois conditions qui pouvaient faire défaut dans les « honeypots » classiques[13] :

- Authenticité et réalisme ;
- Couverture de toutes les surfaces d'attaque du SI ;
- Évolution suivant l'activité du SI et des cyberattaques.

In fine, les nouvelles solutions de « déception » présentent des avantages certains, que les solutions actuelles de prévention, de détection ou de réponse à incident ne sont pas pleinement en mesure d'apporter à la cyberdéfense, dont notamment :

- La réduction drastique de faux positifs dans la détection d'une cyberattaque par la seule utilisation de leurres[14] ;
- La capacité de détecter les « déplacements latéraux » des cyberattaquants dans le SI, ce qui convient particulièrement à la détection des menaces de type APT et notamment pour lutter contre le cyberespionnage par exemple[15] ;
- La facilité de déployer rapidement des solutions de « déception » et de les utiliser[16], notamment en permettant aux équipes de sécurité d'ajouter dans de brefs délais de nouveaux leurres pour mettre toujours plus en difficulté l'attaquant[17] ;

[13] https://www.forbes.com/sites/danwoods/2018/06/22/how-deception-technology-gives-you-the-upper-hand-in-cybersecurity/#5981fc19689e

[14] http://s3.eurecom.fr/docs/mtd17_han_deception.pdf

[15] https://cybersecurite-hq.fr/2017/06/nouvelle-approche-de-cyber-defense-les-leurres-pour-detecter-les-attaques-furtives/

[16] https://www.helpnetsecurity.com/2018/12/06/introduction-deception-technology/ ; https://www.riskinsight-wavestone.com/2017/11/deceptive-security-comment-arroser-larroseur/

[17] https://www.forbes.com/sites/danwoods/2018/06/22/how-deception-technology-gives-you-the-upper-hand-in-cybersecurity/#65b3a680689e

- La capacité de détecter des menaces inconnues sur l'ensemble du SI, même sur des ressources difficiles à protéger comme les objets connectés par exemple, et de manière rapidement opérationnelle sans avoir besoin d'avoir une connaissance préalable des menaces ni de passer par une phase d'apprentissage (la connexion à un leurre entraine directement la détection d'une menace avérée)[18]. Notons cependant qu'une connaissance de la surface d'attaque du SI reste nécessaire pour déployer correctement les leurres.

Panorama des nouvelles solutions de « déception » présentes sur le marché

Une vingtaine d'entreprises spécialisées commercialisent aujourd'hui des solutions nouvelles et concrètes de « déception »[19]. Les solutions les plus abouties, comme par exemple TrapX[20] ou Attivo Networks[21], sont majoritairement implantées aux États-Unis mais certaines sont développées et commercialisées en Europe comme CounterCraft[22] ou encore CyberTrap[23]. En France, ce type de solution ne connait pas le même succès qu'en Amérique du Nord mais suscite un grand intérêt, notamment de la part du ministère des Armées avec le Challenge DGA/COMCYBER « Deceptive Security »[24].

Selon une comparaison des différentes solutions de « déception » proposées par ces entreprises spécialisées (voir tableau comparatif), il semblerait que les nouveaux outils de « déception » les plus courants sur le marché soient principalement :

- Les leurres reproduisant intégralement une ressource informatique comme un serveur de production par exemple (« Full OS Traps ») ;
- Les leurres reproduisant le système d'exploitation Windows (« Fake OS platforms »). Peu de solutions proposent des leurres Mac ou Linux ;
- Les leurres sur les services centralisés d'identification et d'authentification à un réseau (« Active directory »).

Si les nouvelles solutions de « déception » prétendent pouvoir s'adapter à de nombreuses ressources parfois difficiles à protéger, notons qu'il semble que peu proposent aujourd'hui des outils adaptés aux objets connectés ou aux systèmes SCADA par exemple.

[18] https://www.riskinsight-wavestone.com/2017/11/deceptive-security-comment-arroser-larroseur/
[19] https://blog.aimultiple.com/deception-tech-companies/
[20] https://trapx.com/
[21] https://attivonetworks.com/
[22] https://www.countercraft.eu/
[23] https://cybertrap.com/
[24] https://systematic-paris-region.org/fr/actualite/challenge-dga-et-commandement-de-la-cyberdefense-deceptive-security/

Comparaison des nouvelles solutions de « déception » et de leurs applications

Solutions Applications	Acalvio Shadowplex (USA)	Attivo Networks (USA)	CounterCraft (Espagne, RU)	CyberTrap (Autriche)	Cymmetria (USA)	Fidelis (USA)	GuardiCore (USA, Israël	Smokescreen (Amérique du Nord, Asie-Pacifique)	Illusive (Israël, USA)	Ridgeback Interactive Deception (USA)	The Achilles Javelin (USA)	Thinkst Canary (Asie-Pacifique)	TrapX (USA)
Deception Tokens (fake OS platforms)	Windows	Window Linux Mac	Windows	Windows	Windows	Windows		Windows	Windows	N/A	Windows	Windows Linux Mac iOS	Windows Linux
Web App integration				✓				✓					
C&C detection		✓				✓							✓
Detecting attacks in stages	Active reconnaissance Lateral movement Exfiltration	Active reconnaissance Lateral movement Exfiltration	Active reconnaissance Lateral movement	Active reconnaissance Lateral movement Exfiltration	Active reconnaissance Lateral movement Exfiltration	Active reconnaissance Lateral movement Exfiltration		Active reconnaissance Lateral movement Exfiltration	Active reconnaissance Lateral movement	Active reconnaissance Lateral movement	Active reconnaissance Lateral movement	Active reconnaissance Lateral movement Exfiltration	Active reconnaissance Lateral movement Exfiltration
Detection of MITM		✓	✓		✓								✓
Emulated traps	✓	✓				✓		✓		✓			✓
Industry-specific lures		✓							✓				✓
NAC integration	✓	✓							✓				✓
Full OS traps	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓
SIEM integration	✓	✓				✓	✓	✓	✓			✓	✓
Endpoint integration	✓	✓				✓		✓	✓			✓	✓
EDR	✓	✓											✓
Orchestration	✓	✓	✓									✓	✓
Active Directory	✓	✓	✓			✓		✓	✓		✓	✓	✓
Built-in correlation	✓	✓	✓		✓	✓	✓		✓			✓	✓
Built-in ticketing		✓											✓
Sandbox integration	✓	✓											✓
Database	✓	✓		✓	✓			✓				✓	✓
Shared ressource	✓	✓						✓				✓	✓
POS		✓											✓

ATM													✓
SCADA	✓	✓				✓		✓				✓	✓
IoT	✓	✓			✓								✓
Clouds	AWS Azure OpenStack	AWS Azure OpenStack SaaS available GCP	AWS Azure OpenStack	SaaS available	Yes	N/A	AWS Azure OpenStack SaaS available	N/A	N/A	N/A	Yes	AWS GCP	AWS Azure OpenStack
Using client images	✓	✓							✓				✓
Open API for integration	✓	✓										✓	✓
Botnet detection		✓	✓			✓							✓
Automatic code analysis													✓
Custom trap builder		✓										✓	✓
REST API	✓	✓	✓									✓	✓

(*Source : https://roi4cio.com/en/categories/category/deception-techniques-and-honeypots/*)

Enfin, le marché des solutions de « déception » reste limité[25]. Actuellement, seuls les acteurs de la finance, de la santé, de l'énergie ou encore les agences gouvernementales et militaires semblent faire appel à ce type de solution pour protéger leur SI[26]. Cet engouement limité s'explique notamment par le fait que ces solutions ne sont pas encore suffisamment matures et présentent encore un certain nombre de difficultés pour être généralisées.

[25] https://www.esecurityplanet.com/network-security/deception-technology.html

[26] https://dagorettinews.com/cyber-deception-market-grows-with-changing-consumer-preferences-new-opportunities-2018-2026/

Des solutions pas encore suffisamment matures pour une utilisation généralisée

Le déploiement des nouvelles solutions de « déception » rencontre un certain nombre de difficultés qui viennent freiner la généralisation de ce type de solution[27] :

- D'un point de vue technique : de nombreux tests de « Red teaming » réalisés sur ces nouvelles solutions ont révélé qu'il était souvent possible de détecter les leurres proposés sur le marché pour ce qu'ils sont, ce qui oblige les entreprises spécialisées à régulièrement revoir leurs solutions. Il est alors recommandé de réaliser des tests de « Red teaming » aussi réalistes pour l'organisation que possible durant le déploiement des leurres[28]. Soulignons en outre que pour être efficaces, les outils doivent être personnalisés en fonction de l'activité de l'organisation, ce qui rend difficile leur développement et leur déploiement ;

- D'un point de vue juridique : les solutions de « déception » constituent des mesures actives de cyberdéfense qui peuvent dans certains cas se heurter à la législation sur les infractions liées aux systèmes d'information ou à la protection des données. En effet, des fichiers leurres peuvent collecter des données de géolocalisation ou des adresses IP de personnes ou encore pourraient permettre aux équipes de sécurité de remonter à des serveurs tiers utilisés pour dérober les fichiers concernés et de s'y introduire. Par ailleurs, ces solutions peuvent également constituer des provocations à l'infraction. Pour certains chercheurs en cybersécurité, ces solutions devraient être exclusivement réservées aux forces de l'ordre[29] ;

- D'un point de vue organisationnel : le déploiement de leurres très réalistes peut entrainer un risque de confusion pour les personnels de l'organisation. Sensibiliser ces derniers à ce type de solution peut s'avérer nécessaire mais en limiterait davantage l'efficacité face à une menace interne. Il convient alors pour les responsables du SI de bien organiser l'utilisation des ressources pour qu'un utilisateur légitime ne déclenche pas un leurre, ainsi que d'être vigilants pour pouvoir intervenir en cas de confusion. De même, il convient de ne pas déployer de fausses informations qui pourraient, en cas de vol et de divulgation par des pirates, nuire à la réputation de tiers ou de son organisation[30]. Ces préconisations impliquent un certain niveau de maturité organisationnelle dans la gestion d'un SI.

Conclusion

Les nouvelles solutions de « déception » présentent aujourd'hui un réel intérêt pour renforcer la cyberdéfense, proposant des leurres plus opérationnels que les « honeypots » classiques[31]. En revanche, elles ne sont pas suffisamment matures et efficaces pour remplacer les autres solutions de cyberdéfense. Les solutions de

---

[27] https://www.f5.com/labs/articles/cisotociso/will-deception-as-a-defense-become-mainstream-25665 ; https://cybersecurite-hq.fr/2017/06/nouvelle-approche-de-cyber-defense-les-leurres-pour-detecter-les-attaques-furtives/

[28] https://www.bankinfosecurity.com/deception-technology-worth-investment-a-12881 ; https://pure.royalholloway.ac.uk/portal/files/33861604/dimva19_paper83_final.pdf

[29] https://www.readkong.com/page/demystifying-deception-technology-a-survey-1637590

[30] https://www.bankinfosecurity.com/deception-technology-worth-investment-a-12881

[31] http://all.net/journal/deception/RedTeamingExperiments.pdf

« déception » doivent venir compléter les autres mesures de cyberdéfense adoptées par l'organisation[32]. Dans tous les cas, elles doivent s'intégrer à un processus de monitoring et de gestion pour être réellement avantageuses pour la défense de l'organisation.

Le principal frein à la généralisation des solutions de « déception » est la difficulté technique à assurer l'adaptation continue des leurres pour les rendre réalistes au regard du SI de l'organisation. Ceci nécessite une grande implication des équipes informatiques et de sécurité. Cependant, avec les développements de l'intelligence artificielle, notamment de l'apprentissage machine, l'émergence de leurres autonomes pourraient faciliter le déploiement de ce type de solution à l'avenir[33]. Par ailleurs, notons qu'une autre évolution envisagée des solutions de « déception » consisterait à faire passer de véritables ressources informatiques sensibles pour des leurres aux yeux des cyberattaquants, afin que ces derniers ne les ciblent pas[34].

FOCUS INNOVATION

Citalid, GPS d'aide à l'investissement cyber

Présentation

Citalid est une startup française fondée fin 2017 par Maxime Cartan (Président) et Alexandre Dieulangard (Directeur général). Précédemment à la sous-direction Opérations (SDO) de l'ANSSI, les deux spécialistes en Cyber Threat Intelligence (CTI) ont édité une solution logicielle permettant aux entreprises utilisatrices de mesurer leur exposition financière aux risques cyber, ainsi que d'optimiser leur stratégie d'investissement en cybersécurité.

L'innovation

Unique acteur européen à recouper automatiquement des données de CTI, géopolitiques et financières, Citalid oriente de manière pragmatique les entreprises dans leurs décisions d'investissements cyber. La solution permet à ses utilisateurs d'identifier les cybermenaces susceptibles de les cibler (fréquence et ampleur), de hiérarchiser les mesures techniques à déployer en priorité, et de modéliser les impacts financiers potentiels.

À la manière d'un tableau de bord GPS, Citalid indique en premier lieu la « localisation » de leurs utilisateurs quant au risque cyber, en prenant en compte le niveau de défense, le contexte business et les menaces propres à l'entreprise. Après avoir suggéré une « destination » à atteindre pour atteindre le niveau de sécurité ciblé par l'entreprise, si de nouvelles menaces – c'est-à-dire de nouveaux obstacles – apparaissent, ou si son

[32] https://www.crn.com/news/security/300077992/the-art-of-deception-new-class-of-security-startups-use-decoys-to-disrupt-a-hackers-movement.htm ; https://www.forbes.com/sites/danwoods/2018/06/22/how-deception-technology-gives-you-the-upper-hand-in-cybersecurity/#494c7d32689e

[33] https://www.forbes.com/sites/danwoods/2018/06/22/how-deception-technology-gives-you-the-upper-hand-in-cybersecurity/#494c7d32689e

[34] https://www.riskinsight-wavestone.com/2017/11/deceptive-security-comment-arroser-larroseur/

niveau de défense – c'est-à-dire la nouvelle position – évolue. La plateforme est également un outil de simulation permettant de calculer par anticipation l'impact financier de nouveaux investissements de défense ou encore de nouvelles implantations géographiques projetées par l'entreprise.

La technologie

La solution agrège un nombre important de données pour calculer le risque cyber des entreprises. Afin d'estimer les probabilités qu'une entreprise soit victime d'une cyberattaque, tout en mesurant le cas échéant ses répercussions économiques, les algorithmes de Citalid collectent des données issues de diverses sources d'informations (profil entreprise, localisation, maturité technique, contextes économique et géopolitique, etc.). Citalid se démarque également par sa capacité à assembler différentes briques technologiques et méthodologiques éprouvées tel que le CIS20, FAIR, MITRE, STIX 2.0, etc.

L'actualité

Citalid a d'ores et déjà commencé à développer ses activités en Europe et ambitionne de poursuivre sa montée en puissance en 2020. La startup va en outre étendre son offre au marché de la cyber-assurance, notamment, côté assuré, en modélisant l'impact d'un produit d'assurance (rentabilité et adéquation de la couverture assurantielle) et côté assureur, permettre aux acteurs de la cyber assurance de piloter un portefeuille d'assurés en les aidant à mieux estimer les risques cyber de leurs clients.

Après avoir remporté les deux prix (public et jury) de l'innovation des Assises de la sécurité de Monaco en 2018, Citalid a obtenu le prix spécial du jury de la startup du FIC2020.

CALENDRIER

9-10/03/2020
BIG DATA WORLD PARIS

Big Data Paris organise sa neuvième édition les 9 et 10 mars 2020 (Palais des Congrès). Dédié aux données et à l'intelligence artificielle, cet évènement rassemble l'écosystème européen du Big Data et vise à approfondir les connaissances en la matière de ses participants. Au travers de keynotes, ateliers, conférences et présentations techniques, plus d'une centaine d'intervenants s'exprimeront sur les grands enjeux du Big Data (gouvernance et qualité des données, Machine Learning et IA, industrialisation des projets Big Data, etc.).

Retrouvez le programme : ici.

ACTUALITÉ

Lancement du comité d'éthique de la Défense

Annoncé en avril 2019 par la ministre des Armées, à l'occasion d'un discours sur l'intelligence artificielle (IA), le comité d'éthique de la défense s'est réuni pour la première fois le 10 janvier 2020.

Composé de dix-huit membres, nommés par la ministre des Armées (pour un mandat de trois ans renouvelables une fois), le comité repose sur une équipe pluridisciplinaire (armée, droit, histoire, médecine, nouvelles technologies, philosophie, etc.). Sa mission est de conduire des réflexions sur les questions éthiques liées à la défense. Il sera plus précisément chargé d'étudier les enjeux liés à l'évolution du métier de militaire et à l'émergence de nouvelles technologies de défense, dont notamment l'utilisation de l'IA dans les armées.

Sur la base d'une feuille de route dressée par la ministre des Armées, le comité d'éthique commencera ses travaux à la fin du mois de janvier 2020. Les premières thématiques seront le « soldat augmenté » et le développement de nouveaux systèmes d'armes autonomes, impulsés par les innovations en matière d'IA. Le comité pourra par ailleurs s'autosaisir sur les différents sujets qu'il considère comme prioritaires.

Si l'éthique est inhérente aux doctrines d'action et d'emploi du ministère des Armées, aucune instance ne permettait jusqu'à présent d'appréhender ces questions. En se dotant d'un tel comité, la France devient la première grande puissance militaire à disposer d'une structure de réflexion permanente dédiées aux enjeux éthiques posés par les technologies émergentes et leur emploi dans le domaine de la défense.

Retrouvez le discours de la ministre des Armées ici.

Retrouvez la liste des membres du comité d'éthique ici.

La **Direction générale des relations internationales et de la stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

À ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique (OMC)**, qui s'inscrit dans le contrat-cadre n°2018-02. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction générale des relations internationales et de la stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com