Silicon

INSIGHTS FOR IT PROFESSIONALS

SPÉCIAL CYBER SÉCURITÉ

Silicon.fr

> BEYOND CORP
COMMENT GOOGLE EST DEVENU LE CHAMPION DU ZERO TRUST

> SAUVEGARDE
POURQUOI LE CLOUD VA S'IMPOSER

> IDENTITÉ NUMÉRIQUE
UN PILIER AU CŒUR DU ZERO TRUST

XDR
La nouvelle donne EDR

Assurance cyber
Focus sur un marché français en tension

N° 12 - Septembre 2022
L 314277 - 7 - F: 25 € - RD

EKOPO AWARDS

LES TROPHÉES DES ACTEURS
ET OPÉRATIONS QUI FONT BOUGER
LES LIGNES DE LA SOCIÉTÉ ET
IMPACTENT POSITIVEMENT NOTRE AVENIR.

APPEL À CANDIDATURES

METTEZ EN LUMIÈRE VOS MEILLEURES STRATÉGIES, CAMPAGNES ET SOLUTIONS INNOVANTES EN CONCOURANT DANS UNE OU PLUSIEURS CATÉGORIES DONT :

NUMÉRIQUE RESPONSABLE

Cette catégorie récompense les projets visant à limiter les impacts négatifs du numérique, à réduire l'empreinte écologique, économique et sociale des technologies de l'information et de la communication.

DATE LIMITE : 15 OCTOBRE
INFOS ET INSCRIPTIONS

L'ENSEMBLE DES CATÉGORIES

ACHATS ÉTHIQUES • ANCRAGE TERRITORIAL • COMMUNICATION RESPONSABLE • ÉCONOMIE CIRCULAIRE • ENGAGEMENT COLLABORATEURS • FINANCE DURABLE • GRANDE CAUSE
INCLUSION ET DIVERSITÉ • MOBILITÉ DOUCE • NUMÉRIQUE RESPONSABLE • PRÉSERVATION DES RESSOURCES NATURELLES • QUALITÉ DE VIE AU TRAVAIL • TRAJECTOIRE CARBONE

UN ÉVÉNEMENT

EKOPO

EN PARTENARIAT AVEC

366 COMMUNITIES · PROLOGIS · BEWORLD HOSPITALITY CONNECT

AVEC LE SOUTIEN DE

bpifrance · IDEDD · leboncoin · union des marques

ZERO TRUST ET DISSUASION

On connaît cette expression d'un ex-Premier ministre québécois. « *Quand je me regarde, je me désole ; quand je me compare, je me console.* » Elle reflète assez bien le sentiment qu'ont pu ressentir les professionnels français de la cyber en écoutant l'intervention de Guillaume Poupard, lors de la dernière édition du FIC de Lille, cet été (voir page 20). L'ex-futur patron de l'ANSSI expliquait combien il lui était difficile de dresser un bilan satisfaisant de son action, quand le degré de menaces et le nombre de cyberattaques n'ont jamais été aussi élevés en France, et partout dans le monde.

Pourtant, beaucoup de travail a été accompli au cours de ces dernières années. Au niveau politique, la prise de conscience dans les plus hautes instances s'est accompagnée d'une législation pour protéger les OIV (opérateurs d'importance vitale) et renforcer les effectifs comme les moyens d'intervention cyber des armées. Du côté des grandes entreprises, le montant des investissements démontre que les menaces sont (enfin) prises au sérieux. Reste à combler l'énorme trou dans la raquette : les TPE-PME qui composent la majorité de notre tissu économique. Et puis, évidemment, il y a les RSSI et leurs équipes qui travaillent sous le coup d'une double injonction de préserver leur système d'information sans freiner sa modernisation, qui passe par une migration vers le cloud. Pour les accompagner, ils peuvent s'appuyer sur une approche zero trust *(voir page 58)* peu restrictive sur les méthodes comme sur les technologies. Dans ce registre où l'identité numérique devient centrale *(voir page 50),* l'EDR s'est imposé dans la protection des terminaux *(voir page 34)*. On assiste aussi à une évolution de la sauvegarde qui glisse dans le cloud *(voir page 28)*. Et si le zero trust n'est pas une assurance tous risques contre les attaques, il reste aujourd'hui la meilleure arme de dissuasion.

SOMMAIRE

Éditialis
98, rue du Château,
92645 Boulogne-Billancourt Cedex
Pour envoyer un e-mail à votre correspondant, suivre le modèle : pleroy@netmedia.group

PRÉSIDENT
Pascal Chevalier

DIRECTEUR GÉNÉRAL ET DIRECTEUR DE LA PUBLICATION
Hervé Lenglart

ÉDITORIAL
RÉDACTEUR EN CHEF
Philippe Leroy (01 53 32 10 08) pleroy@netmedia.group

RÉDACTION
Clément Bohic (cbohic@netmedia.group)
Ariane Beky (abeky@netmedia.group)

ONT PARTICIPÉ À CE NUMÉRO
Alain Clapaud, Olivier Bouzereau

OFFICE MANAGER
Sophie Laguerre (01 46 99 93 92)

RESPONSABLE DU STUDIO
Catherine Saulais

Réalisation - CONCEPTION GRAPHIQUE
Bench Media Factory
Direction : Christophe Gaillard
Maquette : Sylvain Giovagnoli
Secrétariat de rédaction : Philippe Legrain

COUVERTURE Antoine Levesque
CRÉDITS PHOTOS Adobe Stock

PUBLICITÉ
DIRECTEUR COMMERCIAL
Simon Leprat (01 41 31 72 41) sleprat@netmedia.group

DIRECTRICE DE CLIENTÈLE
Cindy Martinez (01 53 32 10 07) cmartinez@netmedia.group

CHEF DE PUBLICITÉ
Mathilde Poirot (01 46 99 22 95) mpoirot@netmedia.group

ABONNEMENT ET MARKETING
RESPONSABLE ECOMMERCE
abonnement@netmedia.group
CHARGES DE TRAFIC et RESPONSABLE DES PARTENARIATS
Irène Lemenager (01 46 99 72 40) ilemenager@netmedia.group
ABONNEMENT ET SERVICE CLIENTS
Léla Guehi (01 46 99 99 77) lguehi@netmedia.group

IMPRESSION
Léonce Deprez, allée de Belgique, 62128 Wancourt

TARIFS
Prix au numéro : France 25 €
Abonnement 1 an. France métropolitaine 120 € (TVA 2,10 %)
L'abonnement comprend le magazine en versions print et digitale accessible sur PC, tablettes et smartphones, la newsletter quotidienne et l'accès au site silicon.fr
4 numéros par an. Trimestriel
Abonnement 1 an. Étudiant, DOM-TOM et étranger : nous contacter

Silicon est édité par Éditialis, SAS au capital de 136 000 €
Actionnaire NetMedia Group
N° ISSN : 2681-1006
Numéro de commission paritaire : 1221T94134
Dépôt légal : novembre 2019
Origine du papier : Hallsta, Suède
Eutrophisation des eaux : 50 g
Gaz à effet de serre : 969 kg

BIGDATA & AI PARIS by Corp

Conférence et Exposition

11e Edition • 26 & 27 septembre 2022

Palais des Congrès • PARIS et en ligne

DevOps

BIG

Reinforcement learning

Ethique

TIME TO ACCELERATE

Robotique

DATA

Data for Good

15 000 PARTICIPANTS

350 INTERVENTIONS

250 ENTREPRISES EXPOSANTES

Cybersecurité

Gouvernance et qualité

Cloud

IA Green

Machine learning

AI

Automatisation

NLP / NLG

Inscription gratuite sur www.bigdataparis.com

Faites évoluer votre WAN en toute sécurité avec le SD-WAN

La sécurité numérique,
partout où vous en avez besoin

Êtes-vous prêt
à passer au SD-WAN ?

Consultez les premiers
résultats de l'étude

FORTINET®

LE SECURE SD-WAN, élément clé de la transformation du réseau

Dans le cadre d'une migration massive des applications et ressources vers les environnements cloud, le SD-WAN a joué un rôle central. Si au début, il offrait principalement un moyen plus souple pour les succursales de se connecter rapidement aux applications basées sur le cloud, il est rapidement devenu clé pour des réseaux hautement dynamiques et largement distribués.

Cette tendance a été validée par une récente étude menée par Fortinet France au cours du premier semestre 2022 auprès de plus de 200 décideurs. Trois besoins majeurs ont été soulignés par les entreprises françaises :

- La connectivité des sites distants (31,8%)
- Une administration centralisée (27,7%)
- Une visibilité sur le fonctionnement et le trafic réseau (17,8%)

Combinés, ils représentent 77,2% des motivations pour migrer vers le SD-WAN.

Christophe Auberger
Evangéliste Cybersécurité de Fortinet France

Dans ce cadre, Fortinet Secure SD-WAN ne se contente pas de connecter et sécuriser les parties disparates du réseau distribué. De nouvelles fonctionnalités avancées lui permettent de fonctionner comme une plate-forme, fournissant tous les services avancés exigés par des réseaux complexes et en évolution rapide.

Un SD-WAN Multi-Cloud

Fortinet Secure SD-WAN s'intègre aux services de sécurité des principaux fournisseurs de cloud pour établir et maintenir une connectivité sécurisée et performante aux applications fonctionnant sur des réseaux hybrides et multi-clouds. Cette stratégie unifiée permet de centraliser la sécurité du réseau, d'uniformiser les politiques de segmentation et de les mettre en œuvre de manière cohérente dans les déploiements sur site, dans les cloud privés et multiples. La hiérarchisation du trafic des applications critiques, associée à une résilience de connexion fiable, garantit une mise en service cohérente du cloud et une expérience utilisateur optimale.

Des politiques d'accès sans confiance - ZTNA

Pour garantir un accès sécurisé et authentifié aux ressources critiques, Fortinet Secure SD-WAN inclut désormais la fonction ZTNA (zero-trust network access) pour appliquer des politiques d'accès sans confiance. Des contrôles explicites par application/par session et une surveillance granulaire permettent de détecter les activités susceptibles d'avoir un impact sur les performances et la sécurité. Le ZTNA de Fortinet garantit que les utilisateurs et les systèmes n'ont accès qu'aux ressources auxquelles ils ont explicitement droit, quel que soit l'endroit où ils sont déployés ou le chemin à travers le réseau nécessaire pour les atteindre.

AIOps

L'ajout de FortiAIOps à Secure SD-WAN permet aux administrateurs réseau d'identifier, de gérer et de corriger les connexions Secure SD-WAN de Fortinet. Il tire des informations du LAN, WAN, et des couches de sécurité pour identifier les problèmes plus rapidement, accélérer le dépannage, optimiser les performances du réseau et la résilience, et maintenir l'efficacité opérationnelle et sa surveillance centralisée.

Alors que les réseaux continuent d'évoluer, les utilisateurs et appareils auront constamment besoin d'un accès rapide, précis, fiable et sécurisé aux applications et ressources critiques. Qu'il soit déployé sur site, dans le cloud, en tant que service basé sur le cloud ou même en tant que partie d'une solution plus large, le SD-WAN sécurisé continuera à connecter en toute sécurité les utilisateurs, les appareils et les réseaux aux applications et ressources critiques, quel que soit l'endroit où ils sont déployés. ■

FORTINET

INVESTISSEMENTS IT : LA CYBER NE FAIBLIT PAS

Dans un contexte géopolitique tendu et de pression inflationniste, les dépenses européennes en cybersécurité progressent à un rythme soutenu, relève IDC. Sur le continent, la croissance des investissements est désormais attendue en hausse de 10,2 % à 47 milliards $ en 2022. Par la suite, les dépenses de logiciels, appliances et services de sécurité IT progresseraient en moyenne de 9,4 % pour franchir les 66 milliards $ à horizon 2026 en Europe. Les services afficheraient la plus forte dynamique (+10,2 % de croissance en moyenne par an) ainsi que la catégorie de dépenses de cybersécurité la plus importante, devant les logiciels et le matériel informatique dédié, selon IDC. Les secteurs de la banque, de la fabrication discrète et des services professionnels investissent le plus, avec respectivement plus de 6, 5 et 4 milliards $ de dépenses attendues cette année.

VERS UN LANGAGE COMMUN POUR L'ANALYSE D'ÉVÉNEMENTS CYBER ?

AWS et Splunk conduisent le projet OCSF (Open Cybersecurity Schema Framework). Ce projet OCSF est destiné à normaliser les logs et les alertes que produisent les solutions de cybersécurité. Parmi tous les participants, on compte également des poids lourds du secteur tels que IBM, Broadcom, Cloudflare, Salesforce, Trend Micro ou encore Zscaler. Certains membres du consortium ont annoncé une feuille de route pour l'intégration de l'OCSF.

DES RSSI AU BORD DE L'ÉPUISEMENT

Face à la multiplication des menaces et des exigences, la tension monte chez les professionnels de la cybersécurité. L'édition 2022 de l'étude « Voice of SecOps », de Deep Instinct, en témoigne : 1000 responsables de la sécurité des systèmes d'information (RSSI) et professionnels de la cybersécurité ont été interrogés. La tendance est plus marquée encore au sein d'équipes chargées de la sécurité cyber d'infrastructures critiques. De surcroît, le stress et l'épuisement professionnel ont amené 45 % des répondants à envisager de quitter la profession, plutôt que de changer d'employeur.

RANSOMWARES : QUE PAIENT LES PME EN FRANCE

Six PME françaises sur dix, qui ont été victimes d'une attaque de ransomware, affirment avoir payé jusqu'à 40 000 euros de rançon, relève GetApp. Mais, parmi celles qui l'ont fait, 33 % déclarent avoir versé entre 10 001 et 20 000 euros. 28 % entre 20 001 et 40 000 euros, 14 % entre 40 001 et 80 000 euros. Seulement 5 % ont déboursé plus de 80 000 euros.

LinkedIn

première victime du phishing

Le réseau social pour professionnels serait visé par plus de 52 % de toutes les attaques de ce type recensées sur le premier trimestre de l'année, selon une étude de Check Point. La cause est à chercher du côté du taux d'ouverture des messages, de l'ordre de 47 %.

Google Cloud

pousse Assured OSS

Google Cloud va distribuer un catalogue de bibliothèques logicielles open source approuvées par ses soins. Son but : limiter la diffusion de vulnérabilités. Actuellement, 550 grandes bibliothèques open source sont scrutées en continu. Elles sont disponibles sur GitHub et peuvent être téléchargées indépendamment. Avec Assured OSS, il est possible d'intégrer des versions auditées et distribuées via Google Cloud.

Interpol

arrête des milliers de « scammers »

À l'issue de l'opération « First Light 2022 » impliquant 76 pays, 2 000 individus, fraudeurs et acteurs du blanchiment d'argent ont été arrêtés. Et 50 millions $ saisis. Les autorités sont intervenues dans des centres d'appels soupçonnés de fraude aux télécommunications ou d'escroqueries et arnaques en ligne (scams).

Accord

ANSSI-CEA

Les deux instances publiques ont signé un accord-cadre d'une durée de trois ans axé sur la sécurité des systèmes numériques et l'analyse logicielle. Au menu : tendre à la détection exhaustive de vulnérabilités logicielles et évaluer puis certifier des produits de sécurité.

Rubrik

engage Chris Krebs

L'ex-directeur de la CISA, équivalent américain de l'ANSSI, sera le président de son nouveau comité consultatif « CISO Advisory Board ». Il devrait réunir des RSSI de différents secteurs. La sélection se fera en fonction des responsabilités actuelles, des expertises et des contributions à l'écosystème.

ESN recherche

cadres désespérément

En France, le volume d'offres d'emploi cadre « cyber » a pratiquement doublé en cinq ans. Une annonce sur deux émane des ESN, relève l'Apec. Les métiers « build & run » (conception, déploiement et maintenance informatique) concentrent 46 % des offres de profils cyber recherchés.

THALES ACQUIERT ONEWELCOME POUR 100 M€

Le groupe de défense et sécurité français Thales poursuit ses emplettes sur le marché des services de cybersécurité avec l'acquisition, pour 100 millions €, du fournisseur de solutions de cybersécurité OneWelcome. Fondé en 2021 et basé à Amersfoort, aux Pays-Bas, il s'est spécialisé dans la gestion des identités et des accès clients (CIAM) en mode cloud. OneWelcome propose ainsi sa plateforme aux industries hautement réglementées qui souhaitent disposer d'un accès sécurisé et pratique pour connecter clients, partenaires et sous-traitants à leurs services en ligne dans un souci de confidentialités des données et de conformité (RGPD). OneWelcome compte Malakoff Humanis, PostNL et la Banque centrale européenne (BCE) parmi ses clients.

MICROSOFT SE RENFORCE CONTRE L'INGÉRENCE CYBER

En rachetant Miburo Solutions (Miburo), Microsoft souhaite *« éclairer la manière dont des acteurs étrangers utilisent des opérations d'influence informationnelle en lien avec d'autres [actions] cyber pour atteindre leurs objectifs. »* Fondée en 2012 à New York, la société s'est spécialisée dans la détection et la réponse aux opérations cyber d'influence et de manipulation informationnelle *« étrangères »*. Elle propose ses services à de grands comptes privés et publics.

ORACLE DATABASE SERVICE GAGNE MICROSOFT AZURE

Service géré, Oracle Database Service pour Microsoft Azure permet aux clients Azure de provisionner, accéder, utiliser et suivre les services de bases de données hébergés par Oracle et d'en visualiser les journaux ainsi que les analyses dans leur tableau de bord Azure. L'objectif est de simplifier l'expérience multicloud de leurs clients conjoints, parmi lesquels AT&T, Marriott International, Veritas ou encore SGS. *« Aucun frais supplémentaire n'est à prévoir pour recourir à Oracle Database Service pour Microsoft Azure, Oracle Interconnect pour Microsoft Azure ainsi que les données entrantes ou sortantes lors de leur déplacement entre OCI et Azure. Les clients ne paieront que les autres services Azure ou Oracle qu'ils utilisent, comme Azure Synapse ou Oracle Autonomous Database »,* indiquent les deux sociétés.

AWS LOUE AUSSI DES MAC M1

Après les Mac x86 fin 2020, AWS intègre des Mac M1 dans son offre compute. Dans les deux cas, il s'agit de Mac mini à louer en tant qu'hôtes dédiés, pour 24 heures minimum (obligation du contrat de licence de macOS). Soit en facturation à la demande, soit dans le cadre des Savings Plans (engagements d'utilisation). Pour se connecter aux instances, deux solutions : SSH et Apple Remote Desktop (y compris via un client VNC prenant en charge le protocole).

ATOS MIGRE SON ÉMULATEUR QUANTIQUE CHEZ OVHCLOUD

Dans le cadre de ce nouveau partenariat, l'émulateur quantique d'Atos, la Quantum Learning Machine (QLM), sera accessible « en tant que service » dans le nuage informatique d'OVHcloud. En émulant un environnement quantique réel, la QLM reproduit différentes approches de calcul quantique. L'ambition des deux groupes : renforcer leurs offres face à la concurrence américaine et chinoise. Ils veulent contribuer au développement d'un écosystème européen investit dans l'informatique quantique.

GOOGLE CLOUD OUVRE SA RÉGION FRANCE

Nommée Europe-West 9, elle s'appuie sur trois datacenters installés en Île-de-France. Pour Google Cloud, il s'agit de la 10e région en Europe. La région est lancée avec trois zones de réplication et l'essentiel de ses services, notamment Compute Engine, App Engine, Google Kubernetes Engine, Bigtable, Cloud Storage, Spanner et BigQuery. Selon Markess by Exaegis, la part de marché de Google Cloud en France était de 8 % en 2021.

FedEx

bascule tout dans le cloud

Le transporteur va abandonner graduellement ses grands systèmes. Ainsi, les 20 % restants de son parc mainframe seront définitivement fermés dans les deux ans alors que progresse la migration vers le cloud de ses opérations.

Bleu

opérationnelle en 2024

Annoncée en mai 2021, la co-entreprise Bleu détenue par Orange et Capgemini sera officiellement créée à la fin de l'année 2022 et opérationnelle en 2024. Son DG pressenti est Jean Coumaros, actuel directeur de la transformation et membre du comité exécutif du groupe Capgemini.

Oracle

ouvre sa deuxième région France

Après l'ouverture de sa première région dans le datacenter d'Interxion à Marseille (13), Oracle réitère, cette fois, à La Courneuve (93), au sein du Paris Digital Park. Précision utile : elle ne dispose pas de l'interconnexion avec les services de Microsoft Azure, dans le cadre de l'accord dévoilé en 2019.

6ÈME ÉDITION

CLOUDWEEK PARIS 2022

by EuroCloud

27, 28, 29 SEPTEMBRE 2022

FORMULE HYBRIDE

CLOUD

AGIR DANS UN MONDE EN CRISE

3 GRANDS THÈMES :

- LE CLOUD AU SERVICE DE L'INNOVATION
- LA CONFIANCE PAR LE CLOUD COMPUTING
- POUR UN CLOUD RESPONSABLE

EN PARTENARIAT AVEC

Adista

APL

infoclip

Hewlett Packard Enterprise

S3NS

THALES

L'UE DONNE DEUX ANS À APPLE POUR PASSER À L'USB-C

Apple a jusqu'à l'automne 2024 pour finaliser sa transition vers l'USB-C. En tout cas s'il veut continuer à vendre des iPhone, des iPad et des Mac portables dans l'Union européenne. Des dispositions législatives dans ce sens entreront effectivement en application à cette échéance, insérées dans la directive relative aux équipements radio. La Commission européenne avait émis sa proposition de révision du texte en 2020. Le Conseil et le Parlement avaient ensuite, tour à tour, arrêté leur position. Il leur restait à les réconcilier. C'est chose faite depuis le 7 juin. Les colégislateurs ont entériné un accord provisoire qui doit être formalisé après l'été. L'entrée en vigueur interviendra vingt jours après la publication au Journal officiel de l'UE.

ÉCOCONCEPTION WEB : LES BONNES PRATIQUES

Circuit breaker, feature flipping, lazy loading sont autant de concepts et de termes qui s'appliquent à l'écoconception web. Quand on sait que le poids des pages web a été multiplié par 155 entre 1995 et 2022, il apparaît plus que nécessaire aujourd'hui de se familiariser avec cette démarche d'écoconception pour respecter les engagements RSE.

« Écoconception web : les 115 bonnes pratiques » (4e édition ; auteur : Frédéric Bordage ; 12,90 €, parus aux éditions Eyrolles).

DU NOUVEAU POUR LE SILL 2.0

Le Socle interministériel de logiciels libres (SILL) s'enrichit d'une soixante de logiciels libres. Leur code source est sous l'une des licences acceptées par la direction interministérielle du numérique (Dinum) ; et ils doivent être déployés par la DSI d'un établissement public... Parmi eux : Raspberry Pi OS (distribution Debian), Homebrew (gestionnaire de paquets logiciels pour macOS et Linux), OnlyOffice (suite bureautique collaborative en ligne)...

FONDATION LINUX : NORMALISER L'ACCÈS AUX DPU

Le projet Open Programmable Infrastructure (OPI) vise à développer et promouvoir un écosystème d'applications tirant parti de projets open source existants, tels que DPDK, SPDK, OVS et P4. L'effort porte sur la standardisation de la pile logicielle (stack) prenant en charge les processeurs programmables de traitement des données (DPU) et des infrastructures (UIP) de nouvelle génération. Un kit de développement (IPDK) est notamment proposé.

Matt Hicks
le nouveau CEO de Red Hat

Arrivé en 2006 en tant que responsable d'équipe de développement logiciel, Matt Hicks a été l'un des membres fondateurs de l'équipe ingénierie de Red Hat OpenShift. Il succède à Paul Cormier qui prend le poste de chairman.

Cloudscape
en open source

Passage en open source finalisé pour Cloudscape, framework de design React sur la base duquel AWS a construit ses services. Cloudscape réunit actuellement une soixantaine de ces composants : carte, formulaire, sélection de dates, indicateur d'état, etc. Ils permettent d'implémenter une trentaine de patterns : densité du contenu, usage des couleurs, accessibilité, typographie...

ABF
promesse d'une blockchain nationale

Orange Business Services et Docapost conduisent l'Alliance Blockchain France, groupement industriel monté sur le modèle d'Alastria (Espagne) et d'IDUnion (Allemagne).

ONE PLATFORM | ONE AGENT | ONE VIEW

Securing your digital journey

Increase Visibility

Reduce Complexity

Reduce Risk

Qualys®

qualys.com/conferences

BLOOM : UN MÉGAMODÈLE D'IA

Issu de BigScience, une démarche scientifique ouverte, BLOOM (BigScience Large Open-science Open-access Multilingual Language Model) est un modèle de langage multilingue qui dispose de 70 couches de neurones, 112 têtes d'attention et 176 milliards de paramètres. Les premiers jalons de BigScience ont été posés au printemps 2021. À la baguette, Hugging Face, une entreprise créée par trois Français à New York, qui est à l'origine d'une plateforme de data science/machine learning. L'objectif : entraîner, sur un modèle de science ouverte et participative, *« le plus grand modèle de langue multilingue et open source »*. Au final, un millier de scientifiques se sont impliqués, représentant 72 pays et des sociétés comme Airbus, Meta AI, Mozilla, Orange Labs ou Ubisoft. La France a apporté un soutien dans le cadre de sa stratégie nationale pour l'IA.

DONNÉES DE SANTÉ : LA FRANCE PREND LE LEADESHIP DANS L'UE

À travers le Health Data Hub, la France va mener le développement d'un pilote du futur data space santé européen (EHDS). Bénéficiant d'une enveloppe de 8 millions €, dont 60 % provenant de la Commission européenne, les travaux devraient durer deux ans.

Objectif : impulser la réutilisation transnationale des données de santé à des fins de recherche et d'innovation, mais aussi l'élaboration de politiques et de réglementation.

DLP : ADIEU WIP, BONJOUR PURVIEW

Microsoft a acté l'abandon progressif de WIP (protection des informations Windows) tout en continuant d'en assurer la prise en charge. D'ici à fin 2022, c'en sera terminé du support sur les appareils non gérés avec Intune. L'éditeur invite à se tourner vers la suite cloud Purview qui comprend une brique DLP à la couverture potentiellement plus large que WIP (macOS, Chrome, SaaS tiers)... à condition d'y associer les bonnes options. Et de basculer sur un modèle de facturation à l'usage.

ASKDATA : UN ATOUT ANALYTICS POUR SAP

Passé par l'accélérateur SAP.io avec sa plateforme d'analyse de données, l'éditeur italien Askdata s'est vendu à l'éditeur allemand. Sa plateforme cloud d'analytics s'accompagne d'un SDK Python pour, entre autres, développer des connecteurs de données et ajouter des visualisations. Elle comprend quelques « workflows IA » qui, pour l'essentiel, ne fonctionnent qu'en italien (classification de phrases, résumé juridique, analyse de sentiment).

MariaDB acquiert CubeWerx

Cette société canadienne fournit une plateforme de publication et de gestion de données géospatiales via des API REST. Ce rachat tout récent permet d'enrichir de manière significative les capacités existantes de MariaDB SkySQL, son système de gestion de base de données en tant que service (DBaaS). Avec CubeWerx, les développeurs ont la possibilité de créer des applications géospatiales qui reposent sur des normes ouvertes et le cloud.

Databand.ai rejoint IBM

La société israélienne vient tout récemment de se positionner sur le volet « observabilité des pipelines » de l'offre de Big Blue. Sa précédente acquisition, Instana, travaille quant à elle sur l'observabilité des apps et des données.

Red Hat rejoint l'écosystème GreenLake

OpenShift, RHEL, Ansible... Red Hat (affiliée à IBM), qui édite des distributions GNU/Linux, va proposer une version sur site avec paiement à l'usage de ses technologies open source via HPE Greenlake.

A Fresh Approach to Reducing Cyber Risk

VMDR 2.0 with TruRisk

qualys.com/TruRisk

Qualys.

VIVA SALES : MICROSOFT VA-T-IL COURT-CIRCUITER SALESFORCE ?

Avec Viva Sales, Microsoft veut automatiser les opérations CRM à partir des logiciels intégrés à Microsoft 365. Disponible au quatrième trimestre 2022, le module est la première application Viva spécifique à un métier : les commerciaux. L'idée est de capturer automatiquement des données provenant de n'importe quel système CRM et de les éditer avec Excel pour les partager lors d'appels/réunions/discussions. Viva Sales fournit par ailleurs un résumé de ces sessions. Officialisée début 2021, l'offre Viva propose une « digital workplace en kit » qui comprend pour le moment cinq modules, autonomes et/ou intégrés à certaines apps Microsoft 365.

PC : UN RECUL SANS PRÉCÉDENT

Selon Gartner, 72 millions de PC ont été vendus dans le monde au deuxième trimestre 2022., soit une baisse de 12,6 % par rapport à l'an dernier. Selon les analystes de la firme américaine, il s'agit de la « baisse la plus forte en neuf ans ». IDC, de son côté, estime que 71,3 millions de PC « *traditionnels* » ont été écoulés sur les segments « *entreprise* » et « *grand public* » d'avril à juin 2022. Soit moins 15,3 % en glissement annuel.

CHROME OS FLEX : QUID DE WINDOWS ET MACOS ?

Destiné à donner une seconde vie aux PC et aux Mac x86, Chrome OS Flex bénéficie des mises à jour de de Chrome OS et de fonctionnalités comme l'Assistant Google, la prise en charge des comptes Family Link et la gestion des options dépendant d'appareils connectés (Smart Lock, Instant Tethering, Nearby Sharing...). Le système d'exploitation ne prend en charge que les processeurs 64 bits et nécessite au moins 4 Go de RAM et 16 Go de disque.

OPEN SOURCE : TENSION AUTOUR DE GITHUB COPILOT

La promotion par GitHub de son IA Copilot provoque des tensions. La Software Freedom Conservancy (SFC) et la Free Software Foundation (FSF) redoutent la réutilisation de code source au mépris des licences libres et disent avoir communiqué ces préoccupations à Microsoft (propriétaire de GitHub) il y a un an. Conséquence : la SFC n'utilisera plus GitHub pour héberger le code de projets membres et exhorte d'autres développeurs à faire de même.

Alinto

adopte SOGo

L'éditeur lyonnais Alinto devient désormais le référent du projet open source SOGo et propose ainsi une édition professionnelle du serveur mail sécurisé et collaboratif. SoGo dispose aujourd'hui d'une interface riche basée sur AJAX et supporte Microsoft Outlook par le biais d'une intégration ActiveSync, et d'autres logiciels, dont Thunderbird,

Thunderbird

absorbe K-9 Mail

Mozilla vient d'obtenir les droits sur la marque K-9 Mail.et sur le code source de ce client de messagerie pour Android, né dans les années 2000.

Teams

Future interface collaborative d'Excel ?

À partir de son framework Fluid, Microsoft esquisse l'intégration d'Excel Online dans Teams. Appliqué à Excel dans Teams, Fluid ainsi permet d'ouvrir des classeurs et d'éditer des tables pendant une réunion. Chacun des participants peut donc exploiter ses filtres et ses visualisations sans perturber l'expérience des autres.

Bitdefender
BUILT FOR RESILIENCE

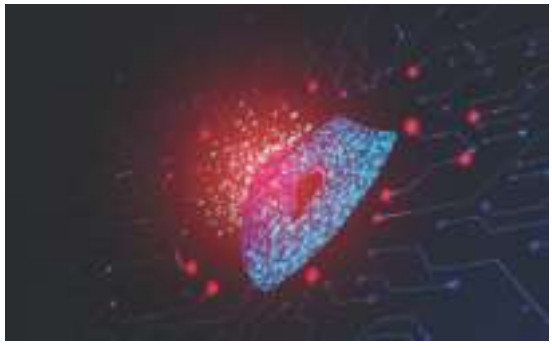
Face au cyber risque, la résilience est la clé.

Parce que les cyber risques ont évolué, votre sécurité doit s'adapter. C'est pourquoi nous avons conçu notre plateforme de cybersécurité et nos services infogérés pour améliorer la résilience de votre entreprise et mieux la protéger.

Une présence dans plus de 170 pays. Des opérations de sécurité 24h/24, 7j/7. Une intelligence artificielle avancée et un apprentissage automatique paramétrable. Des solutions et services de cyber sécurité avancés: MDR - Managed Detection and Response, XDR - eXtended Detection and Response, CWS - Cloud Workload Security

Retrouvez nos solutions et services sur bitdefender.fr/business

LA SÉCURITÉ INFORMATIQUE : facteur d'augmentation des coûts ou de création de valeur ?



Une bonne sécurité informatique ne devrait pas coûter trop cher aux organisations, mais parfois la réalité est toute autre. Quels sont les facteurs de coût qui déterminent l'adéquation des services et produits de sécurité avec les besoins, que permettent-ils d'éviter et quels sont leurs avantages ?

Il est tout à fait possible d'acquérir une cyberprotection adéquate

Pour tout nouvel achat, le rapport prix/performance est souvent un critère décisif – et cela vaut aussi pour les solutions de sécurité. Une analyse coûts/bénéfices aide à distinguer les mesures indispensables de celles qui grèvent inutilement le budget consacré à la sécurité.

En matière de sécurité informatique, inutile de réinventer la roue

Toutefois, il n'y a aucune raison de se passer des technologies les plus courantes. Les antivirus – aujourd'hui appelés protections des endpoints – et les pares-feux sont loin d'être obsolètes. Ils assurent une protection élémentaire contre les menaces déjà connues qui, sans en avoir l'air, sont à l'origine de la majorité des attaques. Mais ce n'est pas parce qu'une attaque est connue et a fait l'objet de plusieurs alertes avant la correction d'une vulnérabilité que le risque n'existe plus.

Les plateformes de sécurité, un choix économique

Il existe plusieurs moyens de faire des économies en concevant votre propre stratégie de sécurité. Vous pouvez par exemple opter pour des plateformes centralisées et indépendantes de détection et réponse sur les endpoints (EDR) ou de détection et réponse étendues (XDR), compatibles avec vos applications existantes.

Les centre des opérations de sécurité, pour créer de la valeur sans faire grimper les coûts

Les plateformes EDR and XDR permettent de repérer les attaques complexes ou, tout du moins, les activités douteuses. Une défense entièrement automatisée est néanmoins encore impossible à ce jour, même en faisant appel à des méthodes aussi sophistiquées. Dans tous les cas, au moins un analyste en sécurité – voire une équipe d'experts – doit intervenir pour évaluer les alertes et prendre les mesures nécessaires.

Les fournisseurs de services de sécurité gérés (MSSP), une solution externe encore plus rentable

Les PME en particulier peuvent réaliser encore plus d'économies en faisant appel à un MSSP, car dans ce cas les coûts fixes couvrent les besoins des différents clients. Par ailleurs les entreprises bénéficient alors des services de sécurité d'un partenaire qui peut transmettre des connaissances à haute valeur ajoutée à différents clients de manière rentable.

Calculez les bénéfices

Le coût de la sécurité informatique doit aussi être envisagé au regard de ses bénéfices. Et les bénéfices peuvent être très importants pour la plupart des entreprises qui font appel à un service expert de détection et de réponse gérées.

À tout bien considérer

Il n'est pas simple d'effectuer une analyse coûts/bénéfices de la sécurité informatique, mais c'est possible. Dans tous les cas, ce travail doit comporter deux aspects très importants : une étude individuelle mais aussi une étude liée au secteur, qui prend en compte non seulement votre propre entreprise mais aussi l'intégralité de la chaîne d'approvisionnement. ■

Bitdefender®
BUILT FOR RESILIENCE

GUILLAUME POUPARD, HUIT ANS SUR LE FRONT DE LA CYBERGUERRE

Guillaume Poupard s'est imposé comme une figure tutélaire de la filière cybersécurité en France. Des OIV au Campus Cyber, passage en revue des temps forts de son mandat à la tête l'ANSSI. *Par Clément Bohic.*

Guillaume Poupard expliquait, dans son intervention au FIC 2022 de Lille : *« Si on devait se mettre des KPI, je ne suis pas sûr que l'on pourrait s'attribuer une très bonne note. Mais si on n'avait pas accompli tout ce travail, ce serait encore pire. »* Une occasion, pour celui qui doit quitter l'ANSSI prochainement, de dresser un bilan de ses huit années comme directeur général (2014-2022). *« La pire des menaces est celle dont on parle le moins : la pression d'un espionnage étatique d'un niveau incroyable »,* a-t-il poursuivi. Et de redouter le jour où cette capacité deviendra offensive, au sens destructeur du terme. *« Ce jour-là, on comptera ceux qui se sont préparés au mieux. »*

Des OIV au Campus Cyber

Selon le futur ex-patron de l'ANSSI, *« on peut être satisfait de ce qu'on a construit avec les OIV ».* Y compris l'écosystème industriel qui va avec. Il en veut pour preuve, d'une part, les centaines de visas de sécurité que l'ANSSI a délivrés, le signe d'une *« dynamique de production de produits et de services de sécurité ».* Et, d'autre part, le Campus Cyber qui matérialise cet écosystème. Autre motif de satisfaction : la *« prise en compte, au niveau politique le plus élevé, de la nécessité de faire pression sur tous les ministères pour assurer leur propre sécurité et celle de leurs administrations ».* Au niveau européen, l'évolution des mentalités se manifeste par la voie réglementaire. En témoignent, notamment, la révision de la directive NIS, le Cybersecurity Act pour rationaliser les schémas de certification et garantir le développement de l'ENISA. *« La NIS 2 va changer les choses par son ampleur »,* déclare Guillaume Poupard, en couvrant des secteurs *« devenus critiques »,* comme la logistique et l'événementiel ; et en permettant de les aborder de manière homogène en Europe. *« À la louche, ce seront dix fois plus d'acteurs qui seront régulés en France. »* La solidarité européenne est une autre paire de manches. Quand un pays a un problème, comment l'aide-t-on ? Comment peut-on déplacer des forces ? Sur ce point, *« nous ne sommes pas prêts. Pour résoudre l'équation, il faut y inclure le secteur privé »,* martèle-t-il. Non sans mentionner des dynamiques de mise en réseau : groupe des CSIRT, groupe de coopération NIS… et le dernier-né CyCLONe, axé sur la gestion de crise.

@Mat Beaudet / Assises de la cybersécurité

> *On peut être satisfait de ce qu'on a construit avec les OIV*

ANSSI : vers une cybersécurité de services

Au niveau territorial, ces derniers mois ont permis d'expérimenter *« quelque chose qu'on n'avait pas prévu ».* En l'occurrence, utiliser de l'argent du Plan de relance pour porter les questions de cybersécurité dans le secteur public. Enveloppe initiale : 136 M€. Enveloppe finale : 176 M€. En première ligne, les parcours de cybersécurité. Le modèle : des fonds (de 90 000 à 140 000 €), un bilan, des audits et la mise en œuvre de places d'action. Ils ont permis de mettre sur les rails environ un millier d'acteurs publics locaux. Autre perspective, plus interne à l'ANSSI : aller vers une cybersécurité de services. Sur le modèle de ce que le Royaume-Uni a appelé, *« de façon peu malhabile »,* cyberdéfense active. L'idée : mettre à disposition des briques permettant de lutter ponctuellement sur des sujets qui, *« mis bout à bout, vont grandement compliquer la vie des attaquants ».* Cela va de l'identification du typosquatting à la sécurisation DNS en passant par un antivirus *« qui n'envoie pas tous les fichiers à Google ».* ■

mgen

GROUPE VYV

EMPLOYEZ-NOUS

À VOUS METTRE AU CŒUR DE LA TRANSFORMATION

EXPERT(E) SÉCURITÉ

Chez MGEN, innovez dans un cadre professionnel favorisant l'esprit collectif et les initiatives individuelles.
Vous avez la possibilité de conjuguer les nouvelles technologies aux exigences de sécurité et d'efficacité pour optimiser nos applications et nos process.
Avec nous, relevez de nouveaux défis en donnant du sens à votre carrière.

REJOIGNONS-NOUS SUR MGEN.FR

Crédit photo : Roman Jehanno. Groupe MGEN – DRH & Affaires générales – **HAVAS PARIS PEOPLE**.

#mutuellement

SOPHIE VIGIER, AMBASSADRICE DU CODE ARTISTIQUE ET INCLUSIF

Depuis quatre ans, cette professionnelle de l'éducation et du code orchestre l'expansion de 42. Avec sa pédagogie « peer to peer » et son modèle de formation sans professeurs, cette école atypique s'implante rapidement à l'international. Portrait. *Par Philippe Leroy.*


© credit

Sophie Viger a une ambition : *« Faire de 42 la meilleure école mondiale de développeuses et développeurs bienveillants armés de valeurs fortes et déployer notre approche pédagogique unique grâce à l'ouverture de campus sur tous les continents. »* Plusieurs classements, dont celui de CodinGame qui a placé 42 à la première place de son classement des meilleures écoles informatiques au monde, lui ont déjà donné raison sur le premier point. *« Notre pédagogie flat, ou apprentissage peer to peer, est un terreau fertile pour donner confiance en soi. Cela développe des compétences non cognitives telles que l'empathie et l'esprit d'équipe par exemple. On forme des gens compétents et talentueux »,* détaille la directrice générale de l'école financée par Xavier Niel, le fondateur de Free.

Au rayon des valeurs, l'inclusion et la féminisation tiennent lieu de priorités absolues. En quatre ans, ce sont plus de 2 000 personnes qui ont participé à des programmes adaptés de sélection, tandis que le pourcentage de femmes sur le campus parisien atteint désormais 30 % des recrues à l'issue de la « piscine », une exigeante épreuve de sélection qui s'étend sur un mois. Comment a-t-elle obtenu ses résultats ? *« Il faut que les femmes se sentent bien accueillies dans cet univers. Nous avons mis en place des règles et des processus afin qu'il n'y ait aucun sexisme »,* ajoute Sophie Viger qui a pris les commandes de 42 en 2018, un quinquennat après sa création.

Une autre représentation du développeur

Son autre cheval de bataille : changer l'image du développeur. *« Il faut arrêter avec cette représentation du geek qui lui est systématiquement associée. On n'est pas obligé d'être passionné d'informatique pour coder. Un développeur, c'est un artiste, au même titre qu'un graphiste. Mais on ne parle pas assez de création et de la diversité des secteurs d'activité dans lesquels on peut exercer ce métier »,* regrette-t-elle. À la tête d'une équipe de soixante personnes, elle pratique un management participatif et récréatif : *« Je dis quand ça va bien et quand ça va mal, mais on doit avoir une certaine exigence. À mon arrivée, l'organisation interne était très peu structurée avec les bons et les mauvais côtés. Les créateurs de 42 étaient des gens transgressifs. »* En bonne place sur sa feuille de route : l'internationalisation de 42. *« D'abord, nous répondons à une demande extrêmement forte de développeurs au niveau mondial. C'est le monde qui vient à nous, et non l'inverse. L'intérêt est très grand pour notre modèle de formation sans professeurs qui s'avère vertueux et peu coûteux »,* se réjouit-elle. Quarante campus ont déjà ouvert leur porte au-delà des frontières de l'Hexagone avec des partenaires aux profils variés. *« Selon les pays, nous travaillons avec des philanthropes, comme au Japon et aux Pays-Bas ; avec des fondations à l'image de l'Espagne et de Allemagne ; et avec des universités, comme c'est le cas en Italie, ou des entreprise sen Belgique »,* précise Sophie Viger. Des ouvertures qui ne freinent pas le développement de 42 en France. Fin 2022, Le Havre deviendra le septième campus à ouvrir ses portes. ■

> *« On n'est pas obligé d'être passionné d'informatique pour coder. Un développeur, c'est un artiste au même titre qu'un graphiste. »*

LE GALAXY BOOK2 PRO DE SAMSUNG testé et adopté par le directeur B2B de Withings

« Léger, puissant et autonome, ce modèle permet d'être alerte, réactif et de prendre de bonnes décisions en déplacement, » apprécie Antoine Pivron (Withings Health Solutions).

L'essor de la télé-médecine mène le fabricant français Withings à concevoir et à vendre une offre de services de santé étendue, via une centaine de nouvelles recrues en 2022 qui viennent renforcer ses 365 salariés.

« Nos collaborateurs de la finance, de l'administration des ventes et de la logistique recherchent beaucoup de performances sous Windows. Ils consultent jusqu'à une quinzaine de fichiers lourds en parallèle. Le portable Galaxy Book2 Pro de Samsung semble extrêmement bien adapté à notre équipe commerciale B2B, car nos cycles de vente sont très longs et, pour nous, la mobilité est un sujet clé, » précise Antoine Pivron, directeur en charge de la stratégie, de la direction commerciale B2B et du suivi des succès clients de Withings Health Solutions en Europe.

Antoine Pivron
Directeur en charge de la stratégie, de la direction commerciale B2B et du suivi des succès clients de Withings Health Solutions en Europe.

Un travail très fluide sur le terrain

Dans ce contexte, les commerciaux B2B participent à de nombreux événements et se déplacent souvent vers les professionnels de santé : *« Ils doivent être rapidement opérationnels, partout. Le Galaxy Book2 Pro se rallume en deux secondes ; il surprend aussi par son poids ultra léger et son autonomie optimisée, »* poursuit-il.

Le travail quotidien des collaborateurs peut gagner en fluidité : *« Toute l'expérience d'utilisation en mouvement doit rester agréable, que le commercial soit dans les transports ou face au médecin qui suivra ses patients à distance. Faire une présentation sur un écran externe ne doit poser aucun souci ; c'est le cas ici. »*

Mieux encore, le Galaxy Book2 Pro rend les applications immédiatement accessibles : *« Nous unifions le plus possible un mode de travail proche des standards du web, avec Salesforce pour le suivi de la relation clients et la suite Google pour partager nos tableaux, présentations et communiquer. Les commerciaux consultent leur boîte mail, planifient et pilotent des visioconférences en quelques clics, de façon autonome. »*

Pour Antoine Pivron, le Galaxy Book2 Pro aurait toute sa place au sein de l'équipe B2B de Withings : *« les matériaux retenus semblent solides. Ils lui confèrent un aspect robuste même si on ne peut pas, en deux semaines, juger de sa fiabilité à long terme. Le portable PC est l'outil principal du commercial. Celui-ci est valorisant, permet d'être plus alerte et plus réactif pour prendre les bonnes décisions. »*

WITHINGS HEALTH SOLUTIONS

inmac wstore

DAS : Galaxy Book2 Pro 15,6" ; tronc : 0.460 W/kg ; membres : 0.460 W/kg

BLACKNOISE

COUP DE CŒUR DU JURY

Son boss :
Arnaud Le Men,
directeur général

➔ **Son business :** développé par Erium, BlackNoise est un générateur d'événements cyber, destiné à évaluer les capacités de détection et de réaction des entreprises. Cette solution de type BAS (Breach & Attack Simulation) est déployée sous forme de boîtiers pour valider l'efficacité des solutions en condition réelle et s'assurer de l'efficience des moyens mobilisés et de la rapidité de réaction.

MINDFLOW

Prix du jury

Ses boss :
Paul-Arthur Jonville, ***président***
Fabrice Delhoste, ***CTO***

➔ **Son business :** elle propose un SOAR (plateforme low code d'automatisation des opérations de sécurité) qui est actuellement en accès anticipé. Mindflow fut l'un des premiers à rejoindre le programme d'incubation de Cyber Booster... comme Malizen, autre fournisseur finaliste du prix FIC. Fondé en 2021 et basé à Paris, Mindflow a le soutien de Thales, dont viennent ses deux fondateurs.

FIC 2022 : 4 LAURÉATS POUR LE PRIX DE LA START-UP

Rendez-vous majeur de la communauté professionnelle de la cybersécurité, le FIC 2022 a décerné ses prix à quatre jeunes entreprises du secteur : le Prix de la start-up FIC, le Prix du jury, le coup de cœur du jury et le Prix Cybersecurity for Industry.

STRONG NETWORK

Prix de la start-up FIC

Son boss :
Laurent Balmelli,
président et directeur produit

Il a créé l'entreprise en 2020
avec Ozrenko Dragic ***(directeur de l'ingénierie)***

➔ **Son business :** Strong Network propose une plateforme de gestion d'IDE cloud fondée sur Kubernetes. En SaaS, cloud privé ou sur site, elle crée une « bulle de sécurité » autour des outils de développement et de data science. La start-up a levé, cette année, un peu plus de 5 M€, auprès du fonds d'investissement finlandais OpenOcean.

NANO CORP

Prix OT - Cybersecurity for Industry

Son boss :
Francis Fanch,
cofondateur et CEO

➔ **Son business :** une plateforme qui permet de superviser la performance des réseaux et de protéger les équipements et les applications critiques via une sonde réseau logicielle – en mode SaaS ou sur site. Additionnée d'un système de visualisation (n.Scope) et d'un enregistreur de flux (n.Rewind), elle analyse les couches 2 à 7 sur du matériel standard, concurrençant en particulier les fonctionnalités de monitoring des firewalls et des IDS/IPS.


FORMATIONS
2013: BACCA
2014: BT
Vous recrutez une personne pas un CV.
Recrutez inclusif avec
Linked out
une idée d' entourage
www.linkedout.fr
EXPERIENCES PROFESSIONELLES

devoteam
Cyber Trust

La confiance de vos clients est précieuse.

Pour maintenir cette confiance,
nos **experts en cybersécurité**
vous **accompagnent** à toutes les étapes
de **vos projets.**

En savoir plus :
france.devoteam.com

Creative tech for Better Change

Zero Trust : un défi qui mérite d'être relevé

L'approche Zero Trust constitue un véritable défi que seulement 10% des organisations sont parvenues à relever. Celle-ci leur permet de faire face aux nouvelles menaces, en donnant aux RSSI la maîtrise des risques résultant de la nouvelle nature du périmètre de leurs systèmes d'information.

Tout en paradoxe avec la confiance totale que son implémentation offrira, la connotation implicite du Zero Trust génère un amalgame alarmant auprès des décisionnaires, déjà soumis à l'accélération exponentielle des besoins business et métier, dans un environnement toujours plus agile.

Dans un contexte en constante évolution, une approche de règles et politiques statiques ne permet pourtant pas de répondre aux challenges d'aujourd'hui. Notre expérience nous a appris qu'une course sans fin aux contrôles de sécurité pénalise les métiers en leur faisant perdre en flexibilité et en autonomie. Nous avons donc adopté une vision "Continuous Adaptative Trust". Celle-ci permet d'assurer une maîtrise des risques, dès le design de l'application et selon des principes fondateurs qui permettent de surveiller le niveau de confiance à accorder en évaluant la posture de sécurité en continu. Cette vision basée sur les risques est dynamique et possède l'avantage de s'adapter à l'évolution des attaques.
La disparition des périmètres classiques, notamment réseaux, et le besoin de recentrer la sécurité sur les utilisateurs ont rendu encore plus prépondérant le rôle de la gestion des identités et des accès (IAM) dans la sécurité : l'IAM est encore plus qu'avant la clé de voûte de la sécurité. Par ailleurs, 84% des entreprises ont subi des brèches basées sur des attaques liées aux identités, suite à l'expansion du Cloud et des environnements collaboratifs en modèle SaaS.

C'est pourquoi nous préconisons que le programme Zero Trust démarre par une stratégie IAM, en imposant une gestion granulaire et continue des besoins utilisateurs et une capacité à authentifier systématiquement une transaction tout au long de son parcours au sein du SI.

Cette pratique s'applique par extension aux règles de sécurisation du réseau, notamment via la communication entre les services, applications et infrastructures, en implémentant le principe du least-privilege au mécanisme de ségrégation par micro-segmentation et l'authentification par attribut pour l'accès et la protection des données.

L'application des principes du DevSecOps apportent agilité et cohérence technique, en insufflant l'approche Security By Design dans les cycles de production et permettent une implémentation de bout en bout du modèle Zero Trust.

Devoteam, leader international du conseil en stratégie digitale, plateformes technologiques et cybersécurité, sera présent aux Assises de la Sécurité à Monaco du 12 au 15 octobre 2022. Dans ce cadre, nous interviendrons lors d'un atelier consacré au Zero Trust le jeudi 13 octobre de 10h00 à 10h45. Cet atelier vous permettra d'en savoir plus sur notre approche pragmatique à ce sujet au travers de cas concrets. Nos experts seront également à votre disposition pour échanger sur le stand n°33 au niveau 1 ainsi que lors de rendez-vous one to one.

devoteam

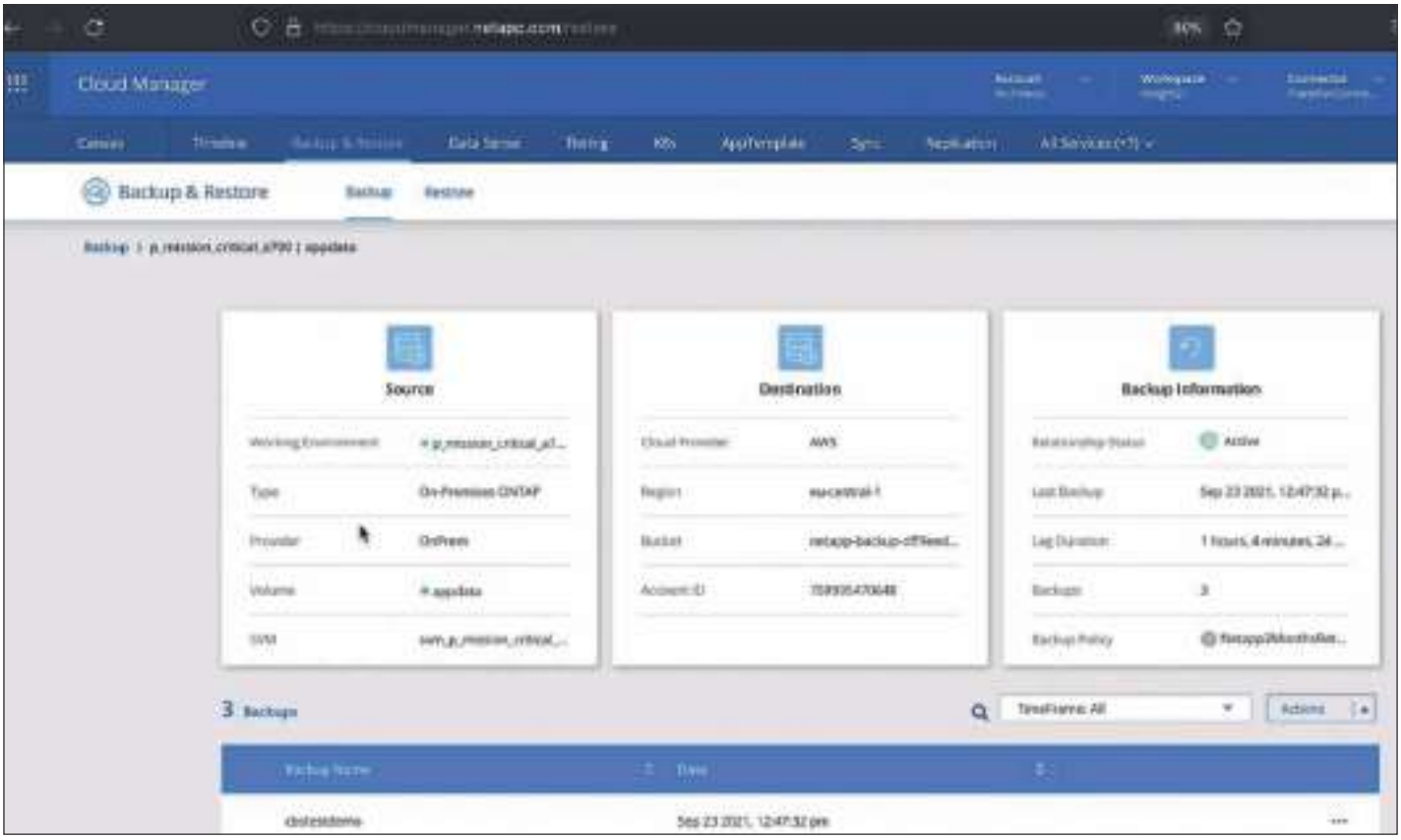
COMMENT LE BACKUP GLISSE DANS LE CLOUD

Si beaucoup de DSI aiment disposer d'une sauvegarde de données on-premise, de nombreux arguments plaident en faveur d'une sauvegarde dans le cloud. Un mouvement aujourd'hui accompagné par tous les acteurs de la sauvegarde, petits et gros.

Par Alain Clapaud.

Avec un taux de croissance annuel de plus de 32 %[1] sur la période 2012-2025, le marché des services BaaS (backup as a service) est en train d'exploser au niveau mondial. Outre la pression mise sur les entreprises par les ransomware et a poussé un grand nombre de chefs d'entreprise à se doter de solutions de backup le plus rapidement possible, beaucoup se sont tournés vers ses services cloud. De nombreux arguments expliquent ce succès : les services cloud offrent une fiabilité souvent bien supérieure à certains systèmes on-premise faiblement maintenus. Les datacenter des fournisseurs cloud sont souvent mieux protégés et sécurisés que ceux de l'entreprise et le cloud public constitue, par définition, un stockage distant des locaux de l'entreprise. Enfin, le mode de facturation du « as a service » sans

(1) Source : Étude « Global Backup-as-a-service Market 2021-2025 », Research&Markets, Mai 2021.



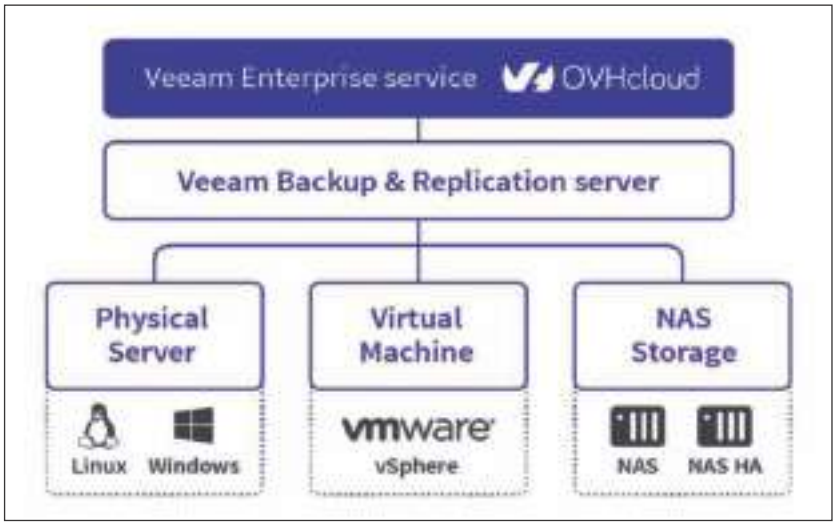
Tous les acteurs du stockage ont étendu leurs offres au backup dans le cloud. Ici, NetApp Cloud Backup, une solution de sauvegarde native fondée sur la technologie ONTAP du constructeur.

investissement initial lourd participe à la démocratisation de la sauvegarde auprès des PME.

UN OFFRE DE BACKUP ENFIN ACCESSIBLE

Si, pour les grands comptes, le cloud public s'est imposé comme le deuxième site idéal dans une stratégie de sauvegarde trois/deux/un (trois copies pour chaque fichier sur deux supports différents et avec une sauvegarde hors-site). Pour ce qui concerne les PME, le service BaaS apparaît souvent comme la seule solution en place, d'où l'importance de ce marché.

De facto, le marché des TPE-PME compte déjà un nombre incalculable d'acteurs : outre les historiques qui y voient un moyen de toucher de nouveaux clients, bon nombre d'ESN se sont lancées dans la bagarre. Ce sont, pour la plupart, des partenaires d'éditeurs de solutions de backup bien connues sur le marché. Ainsi Be-Cloud s'appuie sur Atempo pour proposer une solution de sauvegarde souveraine pour Microsoft 365. Pascal Potier Executive VP Software Engineering & Global Services chez Atempo, l'éditeur de la solution de sauvegarde Tina souligne : *« Nous avons travaillé avec notre partenaire Be-Cloud sur l'automatisation de la solution et le reporting. Lorsqu'ils ont un nouveau client, une nouvelle instance Tina est automatiquement provisionnée sur une machine virtuelle. La refonte de Tina a aussi porté sur la mise à disposition d'une couche API REST qui facilite l'utilisation de notre solution de sauvegarde par les MSP. »* Cette



OVHcloud est l'un des acteurs du cloud français à proposer une offre de sauvegarde de données s'appuyant sur la solution Veeam Backup & Replication.

refonte de Tina a vu ses interfaces utilisateur simplifiées et modernisées de manière à ce que la solution puisse être mise en production en quelques minutes seulement.

Autre solution très présente chez les MSP (managed service provider), la plateforme Veeam qui va aujourd'hui bien au-delà des seules ressources VMware. « *Nous fournissons des solutions de sauvegardes natives pour les ressources cloud fournies par les hyperscalers* », explique Stéphane Berthaud, Senior Director Technical Sales chez Veeam Software. « *Celles-ci exploitent leurs API afin de réaliser des sauvegardes de données. Nous offrons la capacité de piloter l'ensemble des sauvegardes depuis une console unique. Nous pouvons sauvegarder des VM, des instances cloud, des bases de données, des OS. Nous sommes capables de jouer, littéralement, entre ces environnements différents et de prendre une instance VMware, Nutanix AHV ou Microsoft Hyper-V dans un datacenter on-premise, la réinstancier chez AWS, Microsoft Azure ou GCP, ou de chez Google vers AWS. Nous fournissons à nos clients cette fluidité totale entre ces environnements hétérogènes et nous traitons tous ces environnements hétérogènes de façon unifiée.* »

LE BAAS SE FAIT UNE PLACE

Évidemment, tous les constructeurs d'équipements de stockage n'ont pas lâché le marché hardware, mais tous ont dû tenir compte de ce raz-de-marée du cloud dans le domaine du backup. Ainsi, Dell Technologies propose la solution BaaS APEX Backup Services qui s'appuie, en réalité, sur son partenaire Druva, un pure player des solutions de résilience dans le cloud. Lors de la conférence Dell World 2022, Robert Brower, SVP Global Partners and Alliance chez Druva argumentait : « *Un atout important de la plateforme APEX que nous proposons avec Dell est de monter à l'échelle de manière simple, avec des capacités qu'aucun autre fournisseur ne délivre en termes de profondeur et de couverture fonctionnelle. Notre* solution répond tant aux besoins des PME qu'à ceux des grandes entreprises. Avec Dell, nous avons signé plusieurs entreprises du Fortune 50, à la différence de nos concurrents qui ont des offres pour les petits clients, et d'autres pour les grands comptes. » Outre sa simplicité, le responsable estime que la capacité

32 %

la croissance prévue sur la période 2012-2025 pour le marché mondial du BaaS (Back-up as a Service) selon Research&-Markets

Barthélemy Bogaert, consultant SI indépendant

Le cloud contribue au PCA/PRA

« Un espace de stockage disponible et à distance, accessible par le réseau, est une solution basique et simple pour automatiser les sauvegardes nocturnes. À l'époque où il fallait changer quotidiennement les cassettes, ce service proposé par certains hébergeurs apportait un progrès notable. Quelques années plus tard, alors que tout le monde se précipite sur le cloud comme solution miracle aux besoins de stockage, de disponibilité, de performance et d'applications, je cherche à connaître la sécurité associée. Le cloud permet de mutualiser les investissements très lourds requis par la haute disponibilité. Pour se prémunir de la défaillance de son datacenter, le fournisseur de cloud réplique celui-ci sur un autre datacenter. Possiblement dans un autre pays, géré par d'autres équipes. Cette organisation est, en quelque sorte, un secret de fabrication. Seuls les clients assez gros peuvent se permettre des audits de telles structures. Le cloud répond effectivement à une problématique importante, mais globale et aveugle : celle du plan de secours informatique (PSI). Travailler sur le plan de continuité et de reprise d'activité (PCA/PRA) de l'entreprise est l'occasion d'apporter une réponse plus adaptée, plus précise, en repartant des risques inhérents à son activité. Le cloud contribue au PCA/PRA, mais le ne résout pas complètement. »

« Nous avons travaillé avec notre partenaire Be-Cloud sur l'automatisation de la solution et le reporting. Lorsqu'ils ont un nouveau client, une nouvelle instance Tina est automatiquement provisionnée sur une machine virtuelle. La refonte de Tina a aussi porté sur la mise à disposition d'une couche API REST qui facilite l'utilisation de notre solution de sauvegarde par les MSP. »

Pascal Potier Executive VP Software Engineering & Global Services chez Atempo.

de détection des ransomware et de mise en quarantaine des données représente un atout clé sur le marché BaaS.

HPE MISE SUR UN PORTAIL CLOUD UNIQUE

Éternel rival de Dell, HPE mise sur son approche Greenlake pour séduire les entreprises. Sa stratégie consiste à proposer un portail cloud unique pour orchestrer le networking, le compute, l'infrastructure, le stockage et les services de données. Freddy Grahn, Technical Product Manager chez HPE résume les capacités du service HPE Backup et Recovery : « *Il s'agit d'un service de backup qui fournit une solution efficace et sure pour assurer la sauvegarde des machines virtuelles d'un environnement VMware, par exemple. La solution s'appuie sur des règles (policies) qui définissent l'orchestration et l'automatisation des backups. Il est ainsi possible d'avoir une stratégie de backup très agressive si les données l'exigent. Il est possible de faire des snapshots pour une reprise instantanée, faire un stockage on-premise pour accélérer la reprise. Une autre option consiste à utiliser notre cloud Protection Store sur lequel l'entreprise va stocker ses backups et dispose de ressources de stockages infinies.* » Sur le plan de la cybersécurité, les données sont chiffrées et la solution assure une garantie d'immuabilité des données sauvegardées. « *C'est extrêmement précieux pour se protéger des ransomwares et des cyberattaques* », ajoute le responsable HPE. Qu'il s'agisse de services SaaS ultrasimplifiés ou de solutions de classe Entreprise pour lesquelles le cloud n'est qu'un support de stockage parmi d'autres, jamais le monde du backup n'a connu une telle effervescence ! ■

Savbox, un service de sauvegarde en ligne qui s'adresse en priorité aux PME.

REVOLUTION IS ON*

17 - 23 OCTOBRE 2022

PARIS, PORTE DE VERSAILLES

mondial.paris

ORGANISÉ PAR

HOPSCOTCH GROUPE

PFA FILIÈRE AUTOMOBILE & MOBILITÉS

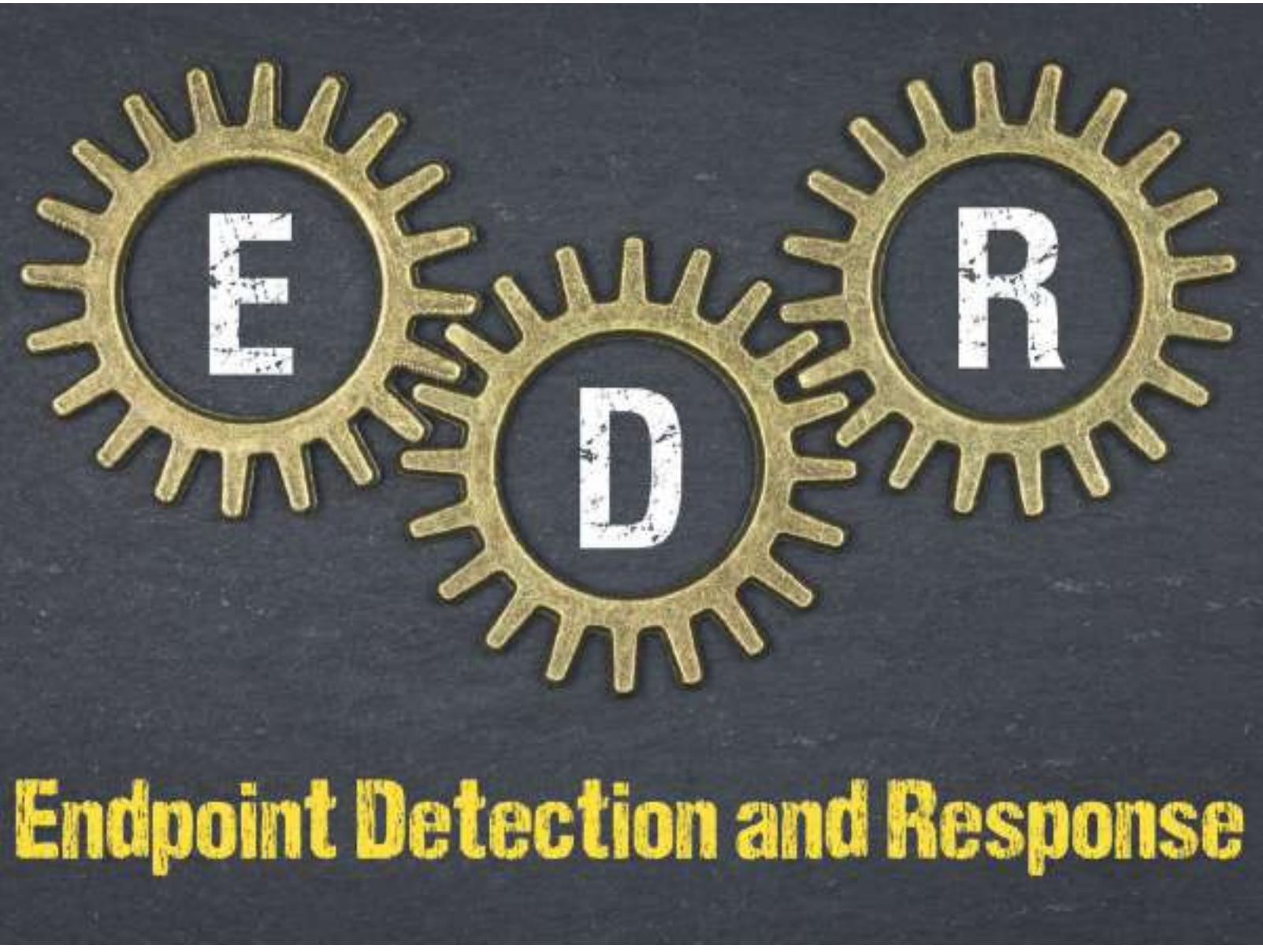
*La révolution est en route

DANS LE CADRE DE LA

PARIS AUTOMOTIVE WEEK

XDR

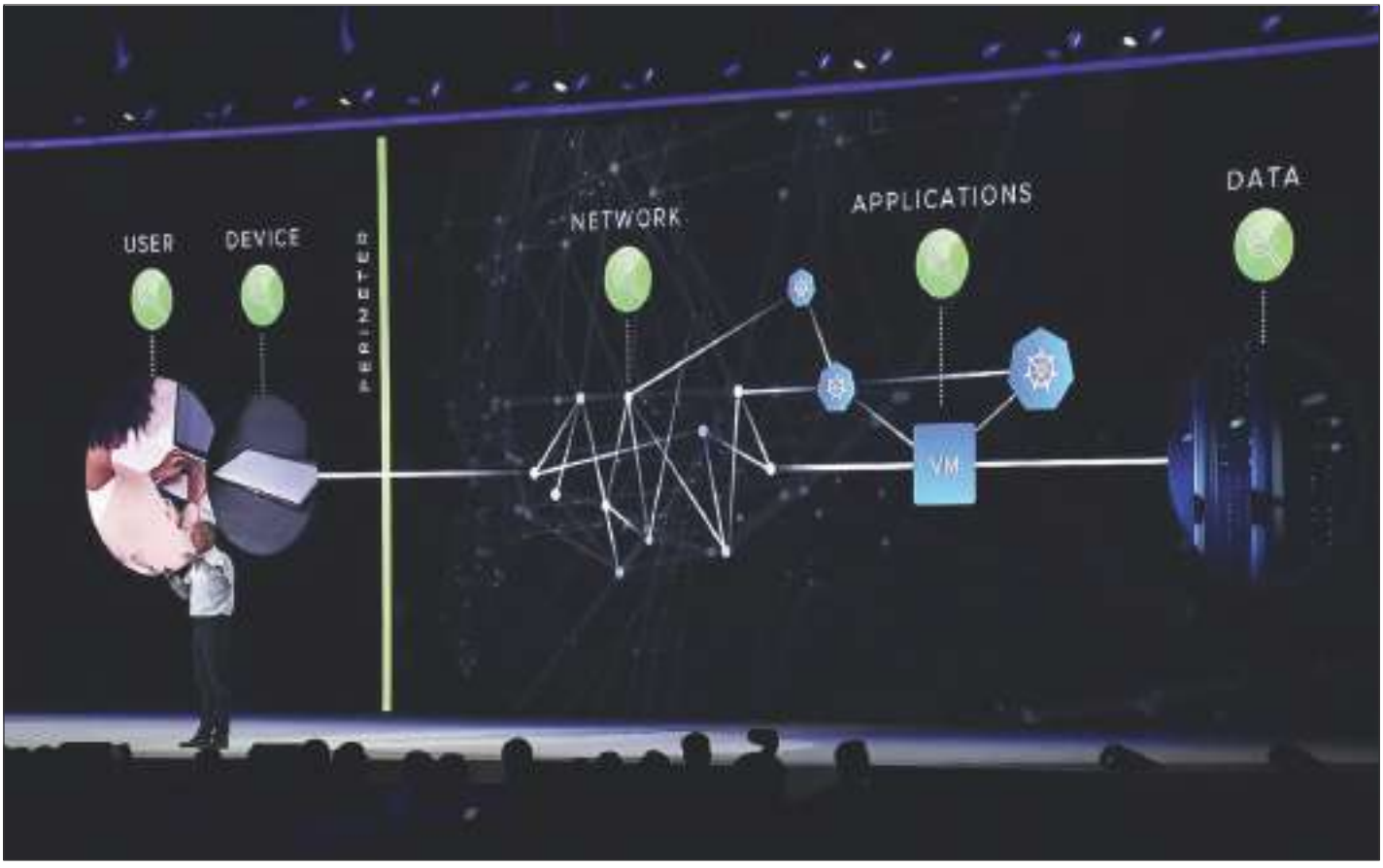
L'EDR DÉPLOIE SES AILES SUR LES SI



En quelques années, l'EDR s'est imposé comme le complément indispensable de l'antivirus traditionnel sur les endpoints. Cette méthode cherche désormais à étendre sa visibilité au-delà des postes clients pour embrasser le reste du système d'information, au point de bousculer l'approche classique des SOC.

Par Alain Clapaud.

En juillet 2022, Allied Market Research publiait une étude estimant à 1,9 milliard de dollars le marché des EDR, ces logiciels de protection des postes clients assurant la détection et un premier niveau de réponse à un incident. Compléments des antivirus, dopés à l'Intelligence artificielle, ces logiciels sont massivement adoptés par les entreprises confrontées à la généralisation du télétravail depuis 2019 et à son corollaire, l'explosion des attaques par ransomware. Cette situation unique a constitué une véritable rampe de lancement pour ces logiciels de protection de nouvelle génération. Les analystes s'attendent à une expansion météorique de +25,3 % par an et la barre des 18 milliards de dollars devrait être dépassée en 2031 ! Dans le dernier Magic Quadrant du Gartner consacré à la protection endpoint, publié en janvier 2022, les



VMware a annoncé son ralliement à la XDR Alliance lors de l'édition 2022 de la RSA Conference.

études placent Microsoft et CrowdStrike en tant que clairs leaders de ce marché, devant TrendMicro, SentinelOne, McAfee et Sophos. En France, on note l'émergence d'une solide offre souveraine avec deux éditeurs, Thetris et Harfang.

Cet essor soudain de l'EDR marque une rupture avec l'évolution des solutions EPP (Endpoint Protection Platform) classiques avec des éditeurs qui ajoutaient à leur solution de nouveaux moteurs de détection à chaque type d'attaque enregistrée. Les éditeurs d'antivirus « classiques » ont pris le pli et se sont positionnés plus ou moins rapidement sur ce marché récent qui progresse encore. Juraj Malcho, Chief Technology Officer chez Eset a résumé cette évolution lors du dernier événement annuel organisé par l'éditeur slovaque : *« Tous nos endpoints disposent de multiples moyens de détection : sécurité réseaux, blocage des "exploits", scan de la mémoire, etc. Chaque fois que nous ajoutons un nouveau moteur de détection, les médias et les analystes nous challengent et nous demandent pourquoi, encore, un tel outils. Ainsi, en 2007, on nous affirmait qu'il n'y avait pas de malwares sur Android. Nous savions qu'il y en aurait un jour... et nous protégeons aujourd'hui le Google Play Store. De même en 2016-2017, on pensait encore qu'il n'y avait pas d'attaque sur UEFI. Aujourd'hui, certains services secrets en ont probablement, mais personne ne le sait et nous en avons découvert. Il faut se préparer à cela. »* Dans cet esprit, l'éditeur s'est placé en early adopter de la technologie de Threat Detection Intel : *« Il s'agit d'une nouvelle couche de sécurité qui peut aider si les autres couches échouent à détecter une attaque. Tout cela participe à un écosystème de sécurité »,* poursuit le CTO.

REPENSER LA SÉCURITÉ

Le renforcement des techniques de détection des EPP se poursuit, mais pour Eset comme pour ses concurrents, l'heure des à l'ouverture et à l'XDR : *« La sécurité est aujourd'hui une question d'écosystème »,* argumente Juraj Malcho. *« Le XDR est un centre de commande auquel se connectent de multiples capteurs, mais aussi des actionneurs. Cette technologie se veut autonome, c'est-à-dire capable de détecter et d'apporter une réponse automatiquement, sans que l'entreprise ait à analyser des données, prendre une décision pour enfin agir, ce qui fait bien évidemment perdre du temps. »*

Lors de la RSA Conference de juin 2022, Tom Gillis, Senior Vice President/General Manager – Networking and Advanced Security Business Group de VMware a bien résumé cette évolution vers l'approche XDR : *« Nous avons assisté à une*

1,9
milliards de dollards
C'est ce que représente actuellement le marché des EDR. La barre des 18 milliards de dollars devrait être dépassée en 2031.

évolution majeure dans la façon dont on conçoit et on déploie les systèmes de sécurité. On place souvent les systèmes de sécurité, notamment de détection, à deux endroits : sur le périmètre du SI et sur les endpoints. On dispose un EDR sur les endpoints et un firewall Next-Generation au périmètre du SI, en dépit du fait que ces systèmes sont aujourd'hui déployés sur une large échelle, on a vu s'accroître la fréquence et l'impact des attaques. Il faut penser la sécurité différemment. Il faut des systèmes qui ne fonctionnent plus uniquement sur les endpoints, plus seulement sur le périmètre, mais qui puissent prendre en compte tout ce qui peut survenir entre les deux. Il faut comprendre comment l'utilisateur interagit avec son application, comment l'application interagit avec l'infrastructure. » Le responsable ajoute que dans le modèle zero trust, l'entreprise doit pouvoir assumer le fait que l'attaquant est déjà présent dans son système d'information, qu'il faut bloquer toutes ses tentatives de mouvement latéral et le déloger dès qu'il est repéré. « *La sécurité latérale est le nouveau champ de bataille* », a ainsi résumé Tom Gillis.

NOUVELLES ALLIANCES

Le Senior VP a profité de sa keynote pour annoncer le ralliement de VMWare à la XDR Alliance, une alliance visant à faciliter l'interconnexion des briques de sécurité au sein d'une approche XDR. Cette alliance compte notamment Google Cloud, NetSkope, SentinelOne et CyberArk en son sein. Blandine Delaporte, Sales Engineer Director – South EMEA chez SentinelOne explique la démarche : « *Plusieurs approches sont possibles vis-à-vis de l'XDR, et chaque éditeur défend sa propre vision. L'idée est d'apporter une détection automatisée sur l'ensemble d'un parc de solutions de sécurité et plus uniquement sur l'EDR. Certains éditeurs ont des portefeuilles produits déjà très complets, avec de la sécurité réseau, de la sécurité email, du CASB, de l'EDR. Ils assemblent toutes ces solutions et affirment faire de l'XDR. Notre approche n'est pas de couvrir tous les besoins : nous restons concentrés sur l'EDR, que ce soit sur les endpoints, les mobiles, les serveurs, le cloud, mais nous voulons développer les capacités de notre solution à communiquer en Open API et s'intégrer à toutes les solutions du marché. Les produits doivent communiquer et s'améliorer mutuellement.* » Au sein de cette alliance, Google joue un rôle de pivot pour plusieurs acteurs via son SIEM Google Chronicle, une plateforme de centralisation des logs que l'Américain a récemment enrichie d'un moteur d'automatisation de type SOAR, avec l'acquisition de Siemplify. Une telle alliance existe aussi pour les offres souveraines

Florian Ledoux, Principal Security Engineer chez Advens

« Il n'y a pas d'outil magique en cybersécurité »

« Il est de plus en plus fréquent que des entreprises qui disposent déjà d'un SOC, de pare-feux et d'antivirus classiques se rendent compte que cela ne leur suffit plus à assurer un haut niveau de sécurité et elles complètent cet arsenal par un EDR. En outre, l'EDR s'avère plus efficient en matière de coût que de collecter des Go de données dans un SIEM auprès de multiples équipements pour, finalement, ne pas avoir une visibilité supérieure à celle d'un EDR/XDR. Néanmoins, il n'y a pas d'outil magique en cybersécurité. L'EDR offre une excellente visibilité sur le fonctionnement du système, les processus qui échangent des données sur le réseau, mais un poste non équipé de l'agent et qui commence à scanner d'autres postes sera invisible ou difficilement détectable. De même, l'EDR ne va détecter une attaque de phishing qu'au moment où l'utilisateur va ouvrir la pièce jointe. C'est la raison pour laquelle les éditeurs se positionnent aujourd'hui sur les XDR. Ceux-ci connectent leurs EDR avec des IPS, des firewalls tels que ceux de Palo Alto Networks et d'autres grands fournisseurs du marché. C'est un moyen d'aller vers l'approche XDR, avec un EDR capable de récupérer des logs comme le ferait un SIEM et ajouter une couche d'intelligence pour contextualiser la menace et affiner les alertes pour abaisser le nombre de faux positifs. »

Le XDR est un centre de commande auquel se connectent de multiples capteurs, mais aussi des actionneurs. Cette technologie se veut autonome, c'est-à-dire capable de détecter et d'apporter une réponse automatiquement, sans que l'entreprise ait à analyser des données, prendre une décision pour enfin agir, ce qui fait bien évidemment perdre du temps. »

Juraj Malcho, Chief Technology Officer chez Eset.

La sécurisation d'un endpoint met en œuvre un nombre impressionnant de moteurs de détection. L'EDR vient en complément et ne permet pas de s'en passer totalement.

articulées autour de l'EDR d'HarfangLab. L'Open XDR Platform compte la détection de malware de Glimps, la solution d'orchestration de Sekoia.io, la sécurité mobile de Pradeo, la sécurité email de Vade et la sonde réseau GateWatcher. Son rival Tehtris a attiré dans l'écosystème TEHTRIS Open XDR une douzaine d'éditeurs dont CybelAngel, eShard, theGreenBow, Proofpoint, Dust Mobile, Cyber-Detect, Olvid et NXLog.

Microsoft leader du Magic Quadrant sur une solution de sécurité, qui l'aurait cru il y a encore quelques années ? C'est pourtant le cas sur les offres EDR avec l'offre Microsoft Defender for Endpoint (MDE).

L'IMPACT DU XDR

Pour Florian Ledoux, Principal Security Engineer chez Advens, si l'EDR a clairement apporté un plus en termes de détection, le « D » d'EDR, des améliorations doivent encore venir du côté du « R » de remediation. *« Les EDR bloquent les menaces sur les postes où elle est identifiée, mais pourront aller beaucoup plus loin en agissant sur les autres briques d'infrastructure. L'EDR peut bloquer les IP malicieuses au niveau des firewalls, par exemple. De nombreux EDR disposent déjà d'un SOAR embarqué ou sont capables d'interagir avec un SOAR externe. L'automatisation sera une tendance forte pour ces prochaines années. »*

L'expert estime que si le recouvrement entre les SIEM et les XDR actuels est encore faible, d'ici à quelques années, les capacités de remédiation automatique des XDR seront plus avancées. Dès lors, ceux-ci auront totalement surpassé les SIEM qui resteront un simple outil de centralisation des logs. Les ESN qui ont développé des SOC assurent des services managés sur le EDR/XDR du marché, mais vont se retrouver en concurrence avec les offres MDR (Managed Detection and Response) des éditeurs eux-mêmes qui bénéficieront d'un effet d'échelle avec lequel peu d'ESN pourront rivaliser. À ces offres ultra-industrialisées, ils pourront miser sur la proximité et un service sur mesure qui peuvent faire toute la différence en cas de coup dur ! ■

UN LABEL RSE
VÉRITABLEMENT ADAPTÉ AUX AGENCES DE COMMUNICATION !

L'AACC a créé avec AFNOR Certification le premier référentiel RSE spécifiquement dédié aux agences-conseils en communication*.

- Vision et gouvernance,
- Réalisation des prestations,
- Ressources humaines et aspects sociaux,
- Impact environnemental.

UN LABEL 100% ADAPTÉ
À LA RÉALITÉ DU MÉTIER DES AGENCES

LES 45 AGENCES AACC LABELLISÉES

4 AOUT, ADFINITAS, ADRÉNALINE, ADVERIS, AGENCE LIMITE, AUSTRALIE GAD, BABEL, BETC, BRAINSONIC, CASTOR & POLLUX, CLAI, COM' DES ENFANTS, DAGRÉ COMMUNICATION, GYRO FRANCE, HAVAS PARIS, HAVAS SPORT & ENTERTAINMENT, HEAVEN, HEREZIE, ICI BARBES, ISOBAR, LEO BURNETT, MARCEL, MCCANN ERICKSON PARIS, OGILVY PARIS, OSWALD ORB, PAMPLEMOUSSE, PRODIGIOUS, PUBLICIS ACTIV FRANCE, PUBLICIS CONSEIL, PUBLICIS CONSULTANTS, PUBLICIS HEALTH, PUBLICIS LMA, PUBLICIS LUXE, RAISON DE SANTÉ, RAZORFISH FRANCE, REACTIVE PRODUCTION, RÉBELLION, SAATCHI, SHORTLINKS, SIDIESE, SOYUZ, SWEETSPOT, THE MARKETING STORE, W & CIE, WOKINE.

*Ce référentiel s'appuie sur le norme internationale **ISO 26000** sur la responsabilité sociétale des entreprises, qui fait référence depuis 2010.

Plus d'informations :

Commission RSE
+33 (0)1 47 42 13 42

afnor CERTIFICATION

AACC RSE

SailPoint

Au coeur de la Sécurité des Identités

Intelligence
inégalée

Automatisation
sans faille

Intégration
complète

LES ASSISES

Venez rencontrer les équipes SailPoint aux Assises et écouter le retour d'expérience d'Hermès le jeudi **13 octobre à 15h.**

SAILPOINT, une approche innovante de la sécurité des identités et des accès

Les solutions SailPoint améliorent la sécurité des accès aux ressources réparties en multicloud, d'où que l'on se connecte, explique Hervé Liotaud, Vice-Président Europe du Sud de SailPoint.

Créée en 2005, SailPoint est un pionnier de la gestion des identités numériques. Comment évolue votre marché ?

Hervé Liotaud: L'accélération des projets d'entreprise est fulgurante. Elle s'explique par trois facteurs principaux. La pandémie du Covid-19 a provoqué une urgence de mise en place du télétravail. Mais, elle a ouvert une boîte de Pandore : les cyberattaquants profitent de réseaux à la maison moins bien protégés que les LAN d'entreprise. Les outils IGA (Identity Governance and Administration) de SailPoint limitent les accès avec une granularité forte : les accès aux bulletins de salaire (pour ne donner qu'un exemple) sont ainsi réservés à quelques employés de la DRH. L'accélération actuelle des projets provient aussi du fait que l'ANSSI recommande, dans sa note sur le déploiement d'une stratégie Zero Trust, de ne plus faire confiance à personne par défaut et d'ouvrir petit à petit les accès aux nouveaux entrants. Enfin, de nombreux projets IGA sont lancés dans le cloud, en mode SaaS (Software as a Service) à présent : le budget consacré est plus acceptable, contrôlable, et contrôlé. Une ETI devait provisionner plusieurs centaines de milliers d'euros durant 18 mois. Aujourd'hui, sa solution est opérationnelle en quelques mois, sans coût caché, avec un TCO plus intéressant. La conjonction de ces facteurs nous aide à mener ce marché auquel nous sommes dédiés, avec plus de 2 000 collaborateurs, dont une cinquantaine en France, très proches de nos clients.

Hervé Liotaud
VP Europe du Sud chez SailPoint

Quelles fonctionnalités innovantes apportez-vous ?

HL: Nos améliorations fonctionnelles sur le cloud sont continues. Tous nos clients bénéficient des dernières mises à jour en même temps, l'équipe de production IT et le RSSI gagnant une maîtrise des accès. Notre module Cloud Access Manager fournit une visibilité et une traçabilité complètes en multicloud. Nous aidons à freiner le shadow IT et à sécuriser les services cloud conçus par l'équipe DevOps. Parallèlement, nos solutions sur site évoluent aussi. Nos clients apprécient de pouvoir suivre tous leurs accès depuis n'importe quel terminal équipé d'un navigateur web. Grâce à nos connecteurs, vers les grandes solutions PAM et SSO du marché notamment, leurs projets peuvent s'étendre à la gestion de comptes à privilèges et à l'authentification unique.

Quel rôle jouent vos partenaires d'intégration ?

HL: Un projet IGA exige de soigner l'implémentation des outils. Il faut comprendre les contraintes et les attentes de chaque client. Nos partenaires d'intégration pointent les compromis à accepter pour gagner en efficacité ; ils harmonisent un ensemble de bonnes pratiques. Nous restons vigilants, en lien direct pour le support technique. Nos équipes et services professionnels vérifient l'implémentation parfaite des outils.
Nous voulons rester l'acteur incontournable d'une bonne gestion des identités afin que nos clients sachent toujours qui accède à quoi dans leur organisation.

*Sylvain **François***
DSI du CHU de Rouen

“Neutraliser un ransomware, c’est courir un marathon et un sprint à la fois”

Juste avant la pandémie de Covid-19, le CHU a été attaqué par le rançongiciel Clop qui a notamment paralysé les connexions aux outils de productivité.

Comme de nombreux établissements hospitaliers, le CHU de Rouen a été victime d'une attaque par ransomware. Sylvain François, son DSI, revient sur les étapes de reconstruction après l'attaque. Et explique comment cet épisode a transformé la stratégie cyber pour protéger les 12 000 utilisateurs soignants, chercheurs et administratifs.

Propos recueillis par Olivier Bouzereau.

Le CHU de Rouen a subi l'assaut d'un ransomware. Pouvez-vous retracer le fil de cet événement ?
Sylvain François : C'était juste avant la pandémie de Covid-19. Le CHU a été attaqué par le rançongiciel Clop qui a notamment paralysé les connexions aux outils de productivité et a entraîné la coupure de nos éléments de communication. Nous étions en novembre 2019. Et, comme souvent, l'aventure a commencé une veille de week-end.

Comment s'organise-t-on dans un tel contexte ?
S. F. : Le ransomware Clop a perturbé notre production informatique. Il a aussi révisé nos priorités numériques durablement, y compris la conception et le déploiement de nouveaux services de santé. Dès les premières investigations consécutives à l'attaque, il a fallu courir un marathon et un sprint à la fois. Les équipes informatiques du CHU ont travaillé jour et nuit pour déterminer l'étendue des dégâts techniques et remettre en place le système d'information au plus vite. (NDLR Clop aurait causé plus de 500 millions d'euros de préjudices dans le monde en bloquant les admissions de centres hospitaliers.)

Avez-vous fait appel à une expertise externe ?
S. F. : L'ANSSI a été contactée dès la détermination de la cyberattaque et a aussitôt délégué une équipe d'experts pour nous épauler. Cela nous a permis de séparer les tâches : l'ANSSI s'occupant vraiment de l'aspect cybersécurité ; de notre côté, nous pouvions nous focaliser sur la remise en place du SI.

Votre fonctionnement en mode dégradé a-t-il été efficace ?
S. F. : Oui. Il avait le mérite d'exister, et d'être testé régulièrement. Le dimanche soir, l'intégralité des applications critiques était à nouveau fonctionnelle. Une semaine plus tard, la quasi-totalité du SI était remise en place. C'est un délai très court par rapport à ce que l'on peut rencontrer dans la moyenne. Néanmoins, pour nos médecins et soignants devant prendre en charge des patients, ce délai peut paraître très long.

Son parcours

Formation
• 2006-2007
EHESP, École des hautes études en santé publique.
• 2000-2003
Telecom Nancy
Diplôme d'ingénieur - ingénieur généraliste Mines Ponts.

Expérience
• Depuis 2019
Directeur du système d'information, CHU de Rouen.
• Oct. 2015 - Févr. 2019
Directeur des systèmes d'information du GHT Yvelines Sud.
• Mai 2011 - Oct. 2015
Directeur des systèmes d'information et des télécommunications du CHU de Reims.
• Avril 2008 - Mai 2011
Directeur des services logistiques et des travaux, directeur des achats du pôle santé Sarthe et Loire.

Avez-vous entamé une restructuration de la DSI ?
S. F. : La DSI se réorganise pour être orientée services, au plus près des utilisateurs, avec des infrastructures fiables, redondées et évolutives, et un parc de logiciels modernisé au bénéfice des salariés et des patients. Notre plan d'action s'articule autour de ces trois axes stratégiques.

Avez-vous adopté, depuis, une combinaison de mesures préventives ?
S. F. : La cyberattaque a conforté nos décideurs dans leur volonté de suivre une stratégie cyber digne de ce nom. Les premiers projets IT ont concerné l'annuaire partagé (Active Directory), la gestion des comptes à privilèges (administrateurs systèmes et sous-traitants), et la protection des postes de travail. L'authentification unique (SSO), la gestion d'identités et de certificats numériques facilitent le quotidien des utilisateurs. Nous essayons de généraliser l'usage de la carte professionnelle d'établissement de santé, du code PIN ou du mot de passe associé. Des équipes dédiées à la gestion des habilitations contribuent à accompagner les parcours d'utilisateurs dans l'hôpital et simplifient l'accès à leur compte et aux applications.

Comment percevez-vous les logiciels de cybersécurité dans le cloud ?
S. F. : J'y vois un véritable atout, en particulier lorsque la mutualisation des ressources procure une force de frappe supérieure. Pour autant, je ne souhaite pas placer tous mes œufs dans un seul panier. Je pense qu'il faut, à la fois, avoir des solutions de sécurité en interne, bien maîtrisées, et des outils puissants et mutualisés dans le cloud.

Comment encadrez-vous les projets R&D et les dispositifs connectés du CHU ?
S. F. : Les projets de recherche du CHU s'appuient sur l'analyse de grands volumes de données médicales fraîches. Dans cet objectif, chaque jour, un entrepôt de données de santé reçoit les informations de l'entrepôt de données de production. On anonymise ces données pour les mettre à disposition des chercheurs, sans impacter les performances des applications utilisées par les soignants. Les dispositifs de santé connectés sont entrés parfois de façon officieuse dans le système d'information. Ils exigent un cadre spécifique pour maîtriser leurs usages et assurer une conformité réglementaire. La gestion des accès s'effectue en lien avec les ressources humaines et nos règles de conception et d'intégration progressent maintenant de concert avec une documentation systématisée. ■

ASSURANCE CYBER

LES MONTAGNES RUSSES DU MARCHÉ FRANÇAIS

Primes, capacités, franchises, indemnisations... Coup de projecteur sur les critères majeurs qui constituent le marché français de l'assurance cyber.

Par Clément Bohic.

« Montagnes russes » sur le marché français de l'assurance cyber ? L'AMRAE emploie l'expression à plusieurs reprises dans la deuxième édition de son étude annuelle. Autant à propos de la fréquence et de l'intensité des sinistres que des résultats techniques des assureurs sur le segment des grandes entreprises. Cette tendance se dégage des données que l'association a collectées en février-mars auprès de sept courtiers spécialistes du risque d'entreprise (AON, Diot-Siaci, Filhet Allard, Marsh, Verlingue, Verspieren, WTW). S'y ajoutent Planète CSCA (syndicat des courtiers d'assurance) et la mutuelle SMABTP. L'échantillon ainsi pris en considération englobe 2028 polices d'assurance cyber et 518 sinistres indemnisés. Le contexte : une année 2020 déficitaire pour les assureurs. Aussi, les conditions de souscription se sont-elles durcies en 2021. Au menu, hausse des taux de prime, réduction des capacités (« voire assèchement » pour certains risques), augmentation des franchises... et, en conséquence, une forme de perte de confiance chez les assurables. Focus sur neuf chiffres qui résument la situation.

2,02 %

Le taux de prime (pourcentage prélevé sur le chiffre d'affaires garanti) sur le segment des grandes entreprises (CA > 1,5 Md€) en 2021. Il est plus élevé qu'en 2020 (1,03 %). Cet indicateur a augmenté pour les ETI (CA entre 50 M€ et 1,5 Md€) : 0,7 %, contre 0,45 % en 2020 et 0,32 % en 2019. Pour les moyennes entreprises (CA entre 10 M€ et 50 M€), il y a eu une forme de correction : 0,33 %, contre 0,71 % en 2020. Dynamique inverse pour les petites entreprises (CA entre 2 M€ et 10 M€), qui ont vu ce taux passer de 0,09 % en 2020 à 0,66 % en 2021.

163,7 MILLIONS €

Le volume global d'indemnisations est plus élevé qu'en 2019 (73,5 M€), mais moins qu'en 2020 (216,6 M€). Pour les grandes entreprises, le montant est de 88,6 M€, contre 201,5 M€ en 2020, dont 62 M€ pour les sinistres XXL (131,3 M€ en 2020), 11,7 M€ pour les XL (vs 49,4 M€), 14,1 M€ pour les M/L (vs 16,5 M€) et 800 k€ pour les XS/S (vs 4,3 M€). Pour les ETI, les indemnisations se montent à 63,1 M€, contre 12,7 M€ en 2020 et 39 M€ en 2019. Pour les entreprises moyennes, c'est 900 k€, contre 2,4 M€ en 2020 et 460 k€ en 2019. Enfin, pour les petites entreprises, le volume est de 11 M€, contre 40 k€ en 2020 et 460 k€ en 2019.

185 MILLIONS €

Le volume de primes qu'ont collecté les assureurs. C'est 44 % de plus qu'en 2020. Une conséquence directe de la hausse des taux de prime. L'enveloppe provient à 82 % des grandes entreprises (+43 % d'une année sur l'autre), à 13 % des ETI (+63 %), à 1 % des moyennes entreprises et à 4 % des petites entreprises.

41,7 MILLIONS €

Le montant global des capacités souscrites est en baisse par rapport à 2020 (53 M€). Un recul généralisé, sauf chez les moyennes entreprises, qui passent à 2,3 M€, contre 2,1 M€ en 2020. Les grandes entreprises sont à 31,3 M€, contre 41 M€ en 2020. Les ETI, 6,6 M€, contre 7,6 M€ en 2020 et 8,1 M€ en 2019. Enfin, pour les petites entreprises, on parle de 1 M€, contre 1,2 M€ en 2020 et en 2019.

-4,4 %

L'évolution du taux de couverture en assurance cyber chez les grandes entreprises. En 2020, elles étaient 251 – soit 84 % des organisations classées comme telles selon la typologie Insee – à avoir souscrit une assurance. En 2021, elles n'étaient plus que 240. Sur le segment des ETI, le taux de couverture a progressé, à 9 % (530 entreprises sur 5763 ; +20,2 % d'une année sur l'autre). Chez les moyennes entreprises, il a reculé : on en est à 0,2 % (322 sur 139 971 ; -11 %). Idem chez les petites entreprises (-21,8 %, à 503 assurés), tandis qu'il a augmenté chez les microentreprises (+32,6 %, à 10 433 assurés).

518/12 028

Le ratio sinistres indemnisés sur nombre d'entreprises assurées. Cela donne un indicateur de fréquence de sinistralité. Il s'élève à environ 4 %. Soit moins qu'en 2020 (17 %) et en 2019 (19 %). Dans la pratique, il n'y a de baisse que sur un segment : les grandes entreprises. À 57 sinistres pour 240 assurés, le ratio s'établit à 24 %. Contre 34 % en 2020 et 35 % en 2019. L'AMRAE évoque toutefois un « effet trompe-l'œil » : c'est surtout le nombre de petits sinistres (XS/S, à moins de 300 k€) qui a diminué, passant de 63 à 33. Et on peut, explique l'association, se demander dans quelle mesure c'est lié aux efforts de prévention… ou plutôt à la hausse des franchises. Chez les ETI, le ratio est à 21 % (110 sinistres pour 530 assurés), contre 17 % en 2020 et 24 % en 2019. Les moyennes entreprises en sont à 8 % (26 sinistres sur 322), contre 4 % en 2020 et 2 % en 2019. Pour les petites entreprises, le ratio a explosé, passant d'environ 1 % en 2019 et en 2020 à 63 % en 2021 (318 sinistres pour 503 assurés).

3,99 MILLIONS €

La franchise moyenne en assurance cyber pour les grandes entreprises. Un niveau sans précédent. C'est 228 000 € pour les ETI, environ 33 000 pour les moyennes entreprises, 7 700 pour les petites entreprises et 1000 pour les microentreprises.

325 %

Le résultat technique (rapport sinistres indemnisés/primes perçues) des assureurs sur le segment des petites entreprises en 2021. Résultat déficitaire, ce qui n'était pas le cas en 2020 (5 %). Sur le segment des grandes entreprises : 58 % (contre 190 % en 2020), se rapprochant du niveau de 2019 (44 %). La conséquence des mesures correctives sus-évoquées. Les ETI *« n'échapperont pas »* à ces mêmes mesures au prochain renouvellement, affirme l'AMRAE. Et pour cause : en 2021, le résultat a été dans le rouge (261 %, contre 85 % en 2020… et 481 % en 2019). Sur le segment des moyennes entreprises, le résultat est en progression constante. Passé de 78 % en 2019 à 45 % en 2020, il a atteint 36 % en 2021. ■

Trophées daf 2022 10 ans

APPEL À CANDIDATURES

REJOIGNEZ LE CONCOURS DE RÉFÉRENCE !
SOUMETTEZ VOTRE CANDIDATURE AVANT LE 30 SEPTEMBRE
DANS L'UNE DES 10 CATÉGORIES

- COMMUNICATION FINANCIÈRE
- COMPTABILITÉ
- DÉVELOPPEMENT INTERNATIONAL
- DIGITALISATION
- FINANCEMENT
- OPÉRATION DE CROISSANCE
- RH
- STRATÉGIE RSE/ESG
- TRANSFORMATION
- TRÉSORERIE

INFOS ET INSCRIPTIONS : WWW.TROPHEES-DAF.FR

radware

Protégez vos applications et les réseaux qui les alimentent

Que pouvez-vous attendre de Radware ?

Sécurité & Innovation

Réservez un rendez-vous 1to1 avec Radware en cliquant ici :

discover.radware.com/les-assises

Protection optimale

Radware fournit des technologies de protection complètes et étendues pour sécuriser vos applications et vos réseaux. Elle couvre tous les vecteurs de menace clés, les vulnérabilités et les cyberattaques contre les applications et les environnements cloud.

Automatisation

Bénéficiez des algorithmes comportementaux et de l'apprentissage automatique pour gérer de manière proactive les changements fréquents apportés aux applications, à leurs environnements sous-jacents, aux nouvelles menaces de sécurité et vulnérabilités.

Sécurité sans faille

Protégez vos applications à chaque instant afin de garantir le même niveau de protection holistique qu'elle que soit l'infrastructure, qu'elle soit sur des clouds publics, privés ou hybrides.

Cohérence

La sécurité est étroitement intégrée aux cycles de développement et n'interfère pas avec le processus opérationnel. Elle s'adapte à la fois aux applications et à leur infrastructure sous-jacente.

MIEUX CONNAÎTRE LES CYBER MALVEILLANTS, POUR MIEUX RÉAGIR face aux cyberattaques

En raison du conflit Ukrainien/Russe, le paysage informatique a été bouleversé avec des attaques plus violentes. Entre partage des connaissances et investissement en recherche, la réponse doit être à la hauteur des menaces.

PQuelles sont les tendances en matière de menaces informatiques en 2022 ?

En tant qu'éditeur de solutions de cybersécurité, Radware s'est spécialisée sur la protection des infrastructures et des applications, au point de devenir leader contre les attaques par déni de services (DDOS). Or, 2022 est une année particulière sur la cybersécurité. Elle a d'abord été marquée par la continuité du télétravail avec un usage massif du cloud public, entraînant des risques importants d'interception de données par les cybercriminels. Le conflit Ukraine/Russie a changé la donne. Le monde des cybercriminels s'est divisé : d'un côté les pro Ukrainiens, de l'autre les pro Russes. Avec à la clé, la mise en place d'une cyberguerre puisque les États appuient et soutiennent des "cyberlégions" (IT Army of Ukraine, Killnet...). Tout en incitant les particuliers à participer aux attaques informatiques via leur propre matériel. En France, mettre à disposition son PC pour participer à une cyberattaque, est considéré comme un acte criminel... Néanmoins en raison du soutien des pays occidentaux à l'Ukraine, une certaine tolérance est admise.

Sameh El Tawil
Regional Director France de Radware.

Quelles sont les réponses apportées par Radware en matière de cyberattaque ?

La violence des attaques de ces derniers mois est montée d'un cran. Nous avons contré une attaque qui a duré 36 heures et dont le volume a atteint 1.5Tbps, ce qui est extrêmement rare. La puissance disponible au service des cybercriminels est donc devenue très importante. Nous devons donc accroître nos investissements sur la recherche pour identifier les menaces, tout en publiant nos connaissances. Il s'agit à la fois d'être plus efficace pour contrer les attaques et propager des informations au service de la communauté des chercheurs. Pour les entreprises, ce partage de connaissance est très important pour qu'elles puissent planifier les ressources nécessaires (humains et financiers) afin d'anticiper les menaces et le cas échéant, pouvoir réagir en cas d'attaques. En connaissant mieux les cybers malveillants, les entreprises se donnent les moyens pour réagir vite et mieux face aux cyberattaques.

Quels sont les atouts dont vous disposez ?

Nous avons fait un "pari" il y a 8 ans. Celui de fusionner notre métier d'éditeur avec le métier d'opérateur de services managés dans le cloud. À l'inverse de l'ensemble des acteurs du marché, nous sommes donc en mesure de créer des outils de cybersécurité que l'on peut exploiter dans des situations urgentes qui réclament réactivité et efficacité. D'autre part, le cycle de développement de nos ressources est ainsi plus pertinent, puisque nous sommes alimentés quotidiennement par des situations réelles de luttes contre des attaques informatiques. Avec à la clé, de nombreux bénéfices pour nos clients.

radware

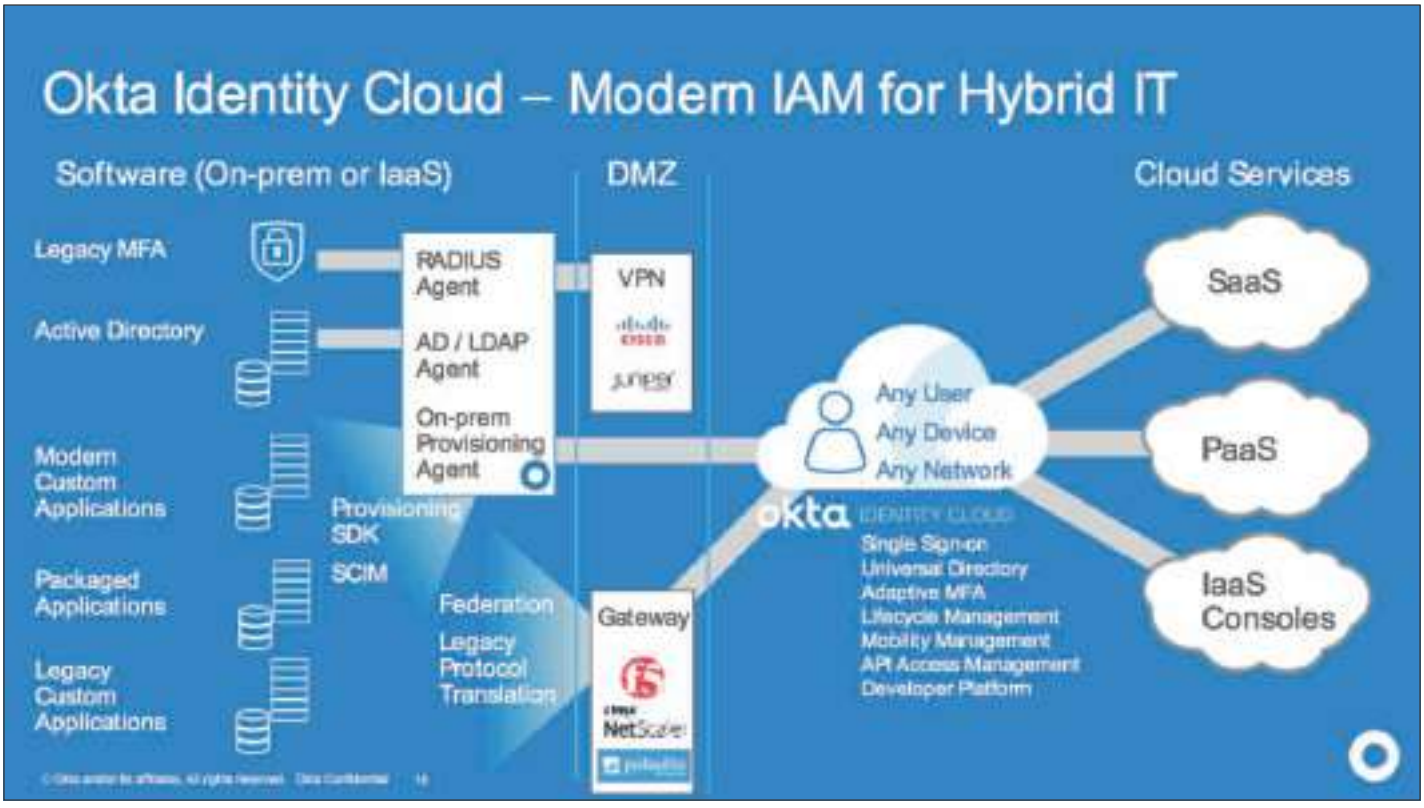
IDENTITÉ NUMÉRIQUE

PIVOT DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION CLOUD

Que ce soit pour gérer les accès des collaborateurs, des prestataires ou même des applications via les API, l'identité numérique joue un rôle déterminant dans la sécurité du système d'information. Elle devient centrale dans l'approche qui s'impose désormais à tous, le zero trust.

Par Alain Clapaud.

Le FIC 2022 a été l'occasion d'un échange sur la sécurité des identités numériques, en particulier celle des citoyens. Le règlement européen eIDAS (Electronic IDentification And Trust Services) vient normaliser l'identité électronique au niveau européen, donc, espère-t-on, accroître son adoption rapide sur le vieux continent. Cette problématique d'identité numérique est tout aussi critique pour les entreprises comme l'expliquait Jameeka Green Aaron, CISO de Auth0, lors de l'événement Okta Identity Forum 2022 : *« Le rôle du CISO a énormément évolué ces dernières années du fait de l'accélération de la transformation digitale induite par la pandémie. Ce que cela signifie pour nous, c'est que nous devons renforcer la protection de nos clients et de nos employés où qu'ils soient. »* L'entreprise doit



L'architecture de gestion des identités a été fortement impactée par la complexité des systèmes d'information modernes, dont l'architecture est majoritairement hybride. L'IDaaS (Identity as a Service) apporte un élément de réponse sur le plan technique.

sécuriser les accès de ses collaborateurs partout où ils se trouvent pour qu'ils bénéficient de ressources on-premise ou cloud. « *Il s'agit de la pierre angulaire de la transformation digitale et de son corollaire, le zero trust* », résume la CISO.

directory, mais aussi la connexion du « decision point » à toutes les sources qui font autorité dans l'entreprise, et coder toutes les règles métiers liés aux autorisations de chacun.

DE L'IAM AU ZERO TRUST IL N'Y A QU'UN PAS

La disponibilité de plateformes IAM (Identity Access Management) sous forme de services SaaS a levé certains freins techniques à la mise en œuvre de ces solutions. L'IDaaS et ces solutions sont amenées à jouer un rôle clé pour aller vers le modèle de sécurité en train de s'imposer, le fameux zero trust. Pour Matthieu Filizzola, Manager IAM chez Magellan Sécurité, la première étape dans la démarche consiste à se doter d'un contrôleur qui validera l'ensemble des accès en temps réel : « *Le contrôleur regroupe le "decision point" qui choisit d'accorder ou pas l'accès à une ressource et l'"enforcement point" qui délivre l'accès et applique la politique d'accès. Il est important de caractériser une matrice d'accès pour définir l'action du "decision point".* » Ce travail peut impliquer une réorganisation de l'active

Matthieu Filizzola, Manager IAM chez Magellan Sécurité

Des solutions moins complexes

« Alors que les projets IAM on-premise étaient très longs, techniques et très coûteux, et empêchaient les entreprises d'atteindre le niveau de sécurité souhaité. L'arrivée de plateforme IAM et même de solutions PAM dans le cloud a permis de réduire ce niveau de complexité. Il ne s'agit certes pas de mesures "clic and deploy", mais elles simplifient grandement les projets. Des normes telles qu'OIDC, SAMLv2 et le protocole SCIM se sont imposées et l'IAM permet de mettre en place des cas d'usage de plus en plus évolués, avec des identités/accès gérés dans le cloud pour accéder à des ressources cloud, mais aussi on-premises. La logique actuelle est de tendre vers le zero trust, et la mise en œuvre de l'IAM doit être pensée selon cette logique : ne jamais accorder la confiance à un utilisateur, à une application par défaut. C'est une approche totalement transverse puisqu'elle doit concerner les métiers, la DRH, les populations plus techniques des administrateurs, dba, etc. »

Les grandes entreprises ont entrepris une marche vers le zero trust, voici déjà quelques années, mais la problématique est tout autre pour les PME.

Selon l'expert, chaque entreprise doit trouver la meilleure façon de tendre vers le zero trust en fonction de sa culture, de ses contraintes réglementaires et de son existant, mais la démarche doit être progressive : *« Je pense qu'il est nécessaire de renforcer graduellement à la fois ce "decision point" en connectant de plus en plus de sources et l'"enforcement point". À cet égard, le PAM jouera un rôle plus important à l'avenir. Autrefois limité aux comptes très techniques, celui-ci est de plus en plus utilisé pour gérer les comptes des prestataires ou, encore, des applications qui ont aujourd'hui une identité. Le PAM est la clé de l'évolution des systèmes IAM de demain. »*

Lors du lancement de la nouvelle version 8.3 d'IdentityIQ, Éric Zimmermann, directeur marketing de l'éditeur SailPoint Technologies soulignait : *« La plupart des grandes entreprises ont des milliers, jusqu'à des millions d'identités, avec, pour chacune d'elles, des besoins d'accès à des ressources on-premise, cloud et applications SaaS qui évoluent en permanence au gré des besoins métiers. Pour une entreprise moderne, connecter de manière sécurisée la bonne personne à la bonne ressource est très complexe et va bien au-delà des capacités humaines. »* La réponse de l'éditeur passe notamment par l'IA et le machine learning, une intégration forte avec le système d'information pour automatiser les processus.

Première étape : se doter d'un contrôleur qui validera l'ensemble des accès en temps réel.

UN ÉCOSYSTÈME ZERO TRUST COMPLET

Si les grandes entreprises ont entrepris cette marche vers le zero trust, voici quelques années, la problématique est tout autre pour les PME qui vont avoir du mal à suivre dans l'empilement de solutions qu'implique une sécurité 100 % dynamique. *« Les grandes entreprises préfèrent ne pas mettre tous les œufs dans le même panier et diversifient leurs solutions de sécurité »,* explique

> *La plupart des grandes entreprises ont des milliers, jusqu'à des millions d'identités, avec chacune d'elles des besoins d'accès à des ressources on-premise, cloud et applications SaaS qui évoluent en permanence au gré des besoins métiers. Pour une entreprise moderne, connecter de manière sécurisée la bonne personne à la bonne ressource complexe et va bien au-delà des capacités humaines. »*
>
> ***Éric Zimmermann, directeur marketing de l'éditeur SailPoint Technologies.***

Christophe Pinjon, consultant expert infrastructure et sécurité chez Upper-Link. *« Pour une PME-PMI, il est bien plus pertinent de réduire le nombre de fournisseurs de solutions de sécurité et de miser sur Microsoft qui a aujourd'hui un portefeuille très riches, au niveau des meilleurs sur le marché. »*

COMMENT OBTENIR UN NIVEAU DE SÉCURITÉ ÉLEVÉ ?

Microsoft est actuellement classée parmi les leaders quant à la sécurité de la messagerie Microsoft 365 pour peu que l'on ait opté pour les licences qui donnent accès à Defender for Office 365. L'activation de ces services permet de bénéficier de fonctions telles que l'antispam, l'antimalware, la protection contre l'usurpation d'identité, etc. *« Attention, ces protections ne sont pas activées par défaut »*, prévient Christophe Pinjon. *« Il est possible d'appliquer des niveaux de configuration standards ou plus stricts. Toute la difficulté est de savoir où placer le curseur pour avoir un niveau de sécurité élevé sans que les contraintes soient rejetées par le personnel. »* Avec l'essor du modèle zero trust, jamais le rôle de l'identité numérique n'est aussi important. Il est temps de renforcer de la gestion du cycle de vie des identités et de durcir l'active directory pour accompagner cette évolution de la sécurité. ■

Christophe Pinjon, consultant expert infrastructure et sécurité chez Upper-Link

Le MFA, c'est un prérequis

« Pour nous, la base même de la sécurité des plateformes cloud, c'est la protection de l'identité. Toutes les entreprises prennent aujourd'hui le chemin du cloud et le plus important est d'être certain que seuls les utilisateurs autorisés peuvent se connecter à des systèmes qui sont accessibles dans le cloud. À cet égard, le MFA est à présent un prérequis. Les cyberassurance le rendent même obligatoire. Le MFA est nécessaire et va protéger la messagerie, mais aussi l'accès à l'ensemble du système d'information. S'il a été décrié, même le MFA avec contrôle d'identité par SMS reste infiniment supérieur à ne pas faire une double authentification du tout ! »

EXPOSITION • CONFÉRENCES • TABLES RONDES • ATELIERS • RENDEZ-VOUS PROJETS

SALONS erp

25 ANS !

11 et 12 octobre 2022

PARIS EXPO
PORTE DE VERSAILLES

Platinum sponsor

axelor

Gold sponsors

coupa UNIT4

Silver sponsor

systhen

@SalonsSolution
#salonssolutions

SalonsSolutions

salons-solutions.com

En parallèle

mobility for business

TERRANOVA SECURITY

SENSIBILISATION À LA CYBERSÉCURITÉ
SIMULATION DE PHISHING

DÉCOUVREZ LES SERIOUS GAME !

Scannez le code QR et obtenez un casque de gaming Razer !

WWW.TERRANOVASECURITY.COM/FR-FR

TERRANOVA SECURITY : Sensibiliser l'humain pour en faire un maillon fort de la cybersécurité

Conscientes des cybermenaces qui pèsent sur leurs activités, les entreprises investissent aujourd'hui massivement dans des solutions technologiques pour se protéger. Elles oublient toutefois un maillon crucial de la sécurité : l'humain.

La cybersécurité, priorité stratégique

Le travail à distance, devenu fréquent depuis la pandémie, a rendu les employés plus vulnérables aux cyber-attaques qui ont augmenté de 31 % entre 2020 et 2021 (Accenture, State of Cybersecurity Resilience 2021). Parallèlement, leur niveau de sophistication grandissant rend les mesures de sécurité des organisations de plus en plus obsolètes (Rapport 2021 du Forum économique mondial).

Un constat appuyé par Theo Zafirakos, RSSI/ Services professionnels chez Terranova Security : « Les organisations ne mettent pas suffisamment l'accent sur l'aspect humain de la cybersécurité. Elles priorisent les solutions technologiques et les processus de sécurité, mais omettent de former les employés sur les risques liés à ces technologies ».

Créer une culture de la cybersécurité

« On ne peut pas compter uniquement sur la technologie, car les cybercriminels savent contourner les contrôles pour atteindre les utilisateurs. Ce sont eux qui doivent pouvoir identifier les menaces » précise Théo.

Le Gone Phishing Tournament le prouve. Ce tournoi mondial d'hameçonnage organisé par Terranova Security démontre qu'un employé sur cinq continue de cliquer sur des liens dans des e-mails de phishing.

C'est dans cette optique que Terranova Security aide les entreprises à établir une culture de cybersécurité. Grâce à des formations et des outils appropriés, chaque employé peut appliquer les bonnes pratiques de sécurité au quotidien.

Un programme d'apprentissage personnalisé et engageant

« Nos programmes de sensibilisation co-construits avec nos clients renforcent les apprentissages grâce à des cours interactifs, multilingues et ludiques et sont combinés à des simulations de phishing pour mettre en pratique les connaissances acquises », remarque Theo Zafirakos.

Les résultats parlent d'eux-mêmes : après 12 mois du programme « champion » de Terranova Security, le taux de clic d'une université a diminué de 10 points de pourcentage auprès du personnel ayant reçu la formation. Le taux de participation du personnel et des étudiants à la formation non obligatoire a également augmenté passant de 5 à 50 %.

Un engagement envers la formation qui s'explique par la gamification. Terranova Security développe des modules de jeux (Serious Game) permettant aux utilisateurs d'accomplir des tâches reliées à la sécurité dans un environnement 3D. Ces jeux favorisent à long terme l'intérêt des utilisateurs pour la cybersécurité ainsi qu'une meilleure rétention des connaissances. ■

Theo Zafirakos
RSSI/Services professionnels chez Terranova Security

ZERO TRUST

3 MÉTHODES ET 5 TECHNOLOGIES POUR LE METTRE EN ŒUVRE

En matière de sécurisation des SI, l'approche zero trust est peu restrictive sur les méthodes comme sur les technologies. De la gestion des identités et des accès à la sécurité applicative, nous faisons le point sur quelques-unes des possibilités.

Par Clément Bohic.

Mobilité, cloud, travail à distance, collaboration interentreprises... Comment maintenir la sécurité d'un SI ? Le zero trust est une réponse potentielle. Pas sous la forme d'une norme ou d'un standard, mais en tant que « philosophie ». Qui laisse le choix des technologies et des méthodes, aussi longtemps qu'on s'aligne sur un objectif : prendre ses distances avec le modèle de défense périmétrique et la confiance « implicite » qu'il induit. À commencer par celle fondée sur la localisation physique des réseaux. En 2020, le NIST (agence gouvernementale américaine) publiait des lignes directrices. Elles font aujourd'hui référence. L'ANSSI, entre autres, les reprend. Notamment concernant les trois principaux axes envisageables pour intégrer les principes du zero trust dans les systèmes d'information.

PREMIER GRAND ANGLE : les identités – et les privilèges associés – en tant que composantes clés. Une approche souvent mise en œuvre sur les réseaux ouverts, avec accès invité ou ceux sur lesquels évoluent des appareils non gérés. Dans ce cadre, l'accès aux ressources est contingent à l'identification de l'utilisateur. D'autres éléments peuvent entrer en ligne de compte, comme l'état de l'appareil employé et le contexte des demandes d'accès (heure, géolocalisation).

DEUXIÈME ANGLE : la microsegmentation, c'est-à-dire le regroupement de ressources en fonction de leur rôle, de leur sensibilité et de leur exposition aux menaces. Puis leur cloisonnement, de sorte que le filtrage des flux devient indépendant des adresses IP des ressources. La microsegmentation peut aussi se faire au niveau des hôtes.

TROISIÈME ANGLE : les périmètres établis par logiciel. Cette implémentation s'établit communément sur la couche applicative par un déploiement de type agent/passerelle. Elle implique généralement les concepts de SDN (réseau défini par logiciel) et d'IBN (administration réseau à renfort d'IA).

À ces trois axes, l'ANSSI ajoute quelques recommandations. Parmi elles, utiliser des moyens d'authentification à l'état de l'art (on considérera le MFA comme un prérequis) et centraliser les journaux de sécurité dans un SIEM (système de gestion des événements et des informations de sécurité). Celui-ci pourra, aux côtés d'autres sources telles que les gestionnaires d'identités, les magasins de certificats et les flux de renseignement sur les menaces, contribuer à alimenter une brique fondamentale des architectures zero trust : les moteurs algorithmiques qui décident ou non d'autoriser les accès.

DU SIEM AU PAM : QUI POUR S'OUTILLER ?

Le SIEM fait partie des marchés que Gartner analyse dans le cadre de son Magic Quadrant. En 2021, le cabinet américain a distingué six fournisseurs comme « leaders ». Nommément, Exabeam, IBM, Securonix, Splunk, Rapid7 et LogRhythm. Exabeam a droit à quelques bons points sur la partie archivage, la modularité, la recherche des logs et l'analyse comportementale. IBM, sur la simplicité de déploiement et de gestion. Securonix, sur la data privacy et la prise en charge des flux de threat intelligence. Splunk, sur les modèles de tarification et l'intégration UEBA (analyse du comportement des utilisateurs et des entités)/SOAR (orchestration, automatisation et réponse). Rapid7, pour son service managé de détection et de réponse. LogRhythm, sur la gestion des cas et l'accompagnement des projets pilotes. Autre composante du zero trust à faire l'objet d'un Quadrant : la protection des terminaux (EPP : Endpoint Protection Platforms). Avec là aussi six fournisseurs « leaders » : Microsoft, Crowdstrike, Trend Micro, SentinelOne, McAfee et Sophos. Microsoft a droit à des bons points sur la couverture fonctionnelle de son produit et l'unification de ses outils (console cloud, API et data lake communs). Crowdstrike,

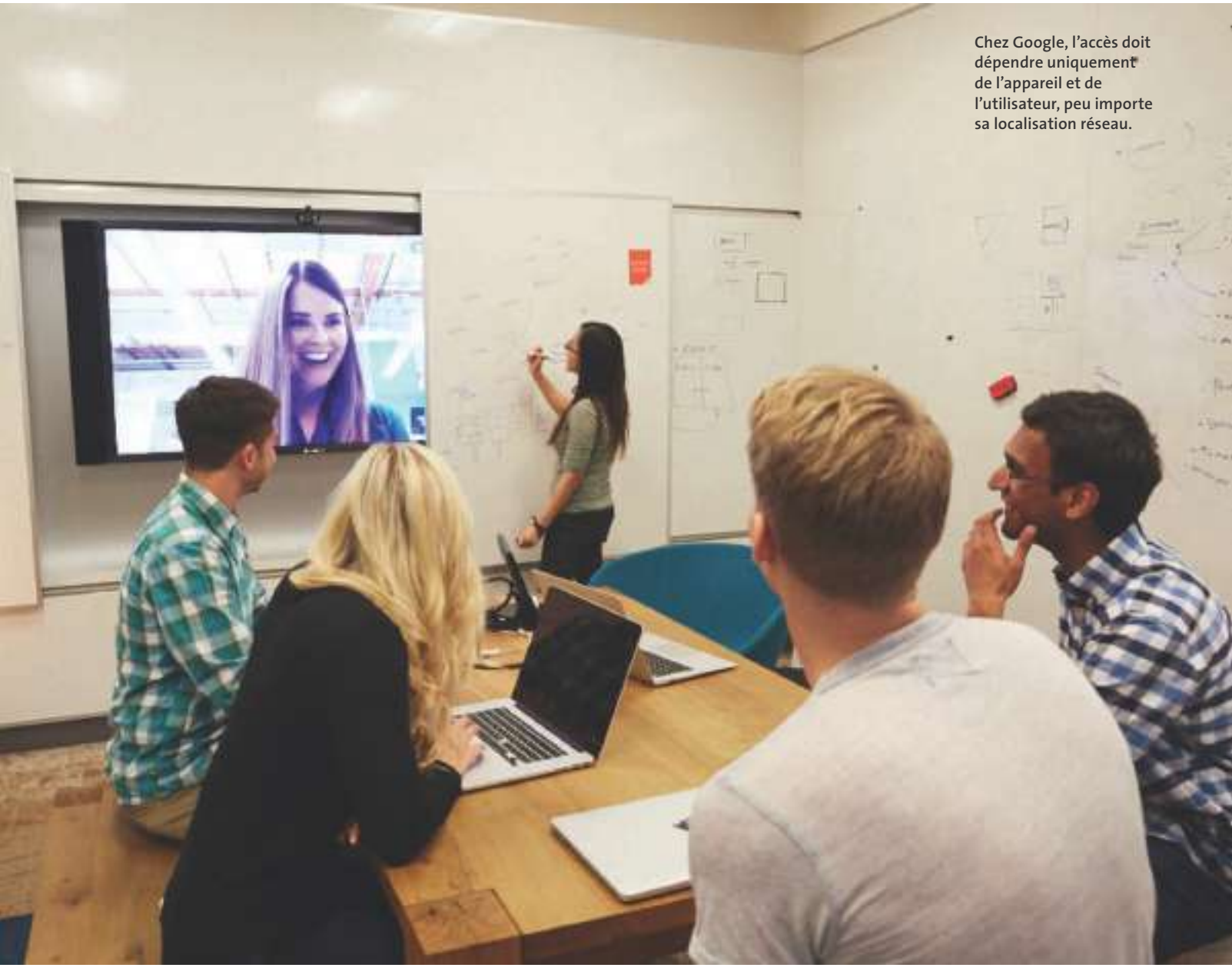
pour la « légèreté » de son agent unique et la simplicité d'usage de sa console de gestion. Trend Micro, sur l'intégration avec les outils de sécurité tiers et la souplesse des options de contrôle des applications. SentinelOne, sur la qualité du support ainsi que la prise en charge des conteneurs et du serverless. McAfee, sur la gestion de la surface d'attaque et la réponse aux incidents. Sophos, pour les capacités d'investigation des menaces et la protection contre les ransomwares. Sur la partie PAM (gestion des accès à privilèges), Gartner a considéré deux composantes comme obligatoires. D'une part, le PASM (gestion des comptes à privilèges et des sessions associées). D'autre part, le PEDM (gestion des actions de ces comptes sur les systèmes cibles, en filtrant les commandes et en orchestrant les élévations de privilèges). La gestion des secrets était un critère facultatif, comme le PTA (automatisation des tâches à privilèges) et la gestion des accès distants.

Là encore, six « leaders » sont ressortis : CyberArk, BeyondTrust, One Identity, Thycotic, Centrify et ARCON. CyberArk était, au moment, de l'examen des offres, le seul des « leaders » à proposer, en natif, du CIEM (gestion des identités et des accès à privilèges en multicloud). BeyondTrust avait pour lui la qualité de son PEDM sur UNIX/Linux, ainsi que ses fonctionnalités de découverte de comptes et de reporting. One Identity, la gestion des OS Windows embarqués et les capacités OCR de son enregistreur de sessions graphiques. Thycotic, sa gestion du cycle de vie des comptes et son add-on étendant le contrôle aux consoles web et aux bases de données. Centrify, l'authentification M2M et les capacités de connexion des annuaires d'entreprise. ARCON, l'expérience client (déploiement, intégration) et le support (uniforme, en 24/7 de base). Les solutions de gestion de la performance applicative (APM) ont aussi droit à un Quadrant. Pour la première fois, avec l'édition 2022, la sécurité a été intégrée comme composante du marché. Gartner a effectivement inclus un critère «*fonctionnalité de sécurité applicative via un agent ou un framework commun*». Dans la pratique, peu de fournisseurs ont droit à un bon point dans le domaine. Chez les « leaders », Dynatrace en fait partie. Chez les autres, Cisco se distingue avec la passerelle entre ses produits Secure Application et AppDynamics. On trouve aussi du zero trust sous l'ombrelle SSE (Secure Service Edge). En l'occurrence, le ZTNA (sécurisation de l'accès distant aux applications privées). Gartner le considère comme une brique fondamentale du marché aux côtés du SWG (sécurisation de l'accès web par proxy) et du CASB (sécurisation de l'accès au SaaS par proxy et API). Il a aussi pris en considération des capacités « additionnelles », dont certaines peuvent trouver placer dans une stratégie zero trust. Comme le FWaaS (firewall as a service), l'UEBA et le CSPM (gestion de la posture de sécurité cloud).

L'approche « tout-en-un » des fournisseurs peut sembler attractive sur le papier, reconnaît l'ANSSI. Surtout au regard du risque de perte de contrôle que présente le recours à de multiples solutions logicielles. Mais elle «*ne dispense pas d'une réflexion autonome sur l'état de l'art de toutes les déclinaisons possibles de la démarche*». ■

BEYONDCORP

COMMENT GOOGLE EST DEVENU UNE « ENTREPRISE MODÈLE » DU ZERO TRUST



Chez Google, l'accès doit dépendre uniquement de l'appareil et de l'utilisateur, peu importe sa localisation réseau.

Sous l'étendard BeyondCorp, Google expose sa démarche zero trust amorcée au début des années 2010. Comment le groupe américain s'y est-il pris ?

Par Clément Bohic.

Google, champion du zero trust ? La société est, en tout cas, souvent présentée comme une référence en la matière. Il faut dire qu'elle communique ouvertement sur ses démarches depuis bientôt une dizaine d'années. Sous une marque ombrelle : BeyondCorp, dévoilée fin 2014 avec la promesse d'une « *nouvelle approche de la sécurité d'entreprise* ». Le postulat : le périmètre informatique de l'entreprise s'agrandit… et ce qui se trouve dedans n'est plus forcément sûr. Dans ce contexte, l'accès doit dépendre uniquement de l'appareil et de l'utilisateur, peu importe sa localisation réseau. Et tout accès doit être authentifié, autorisé et chiffré.

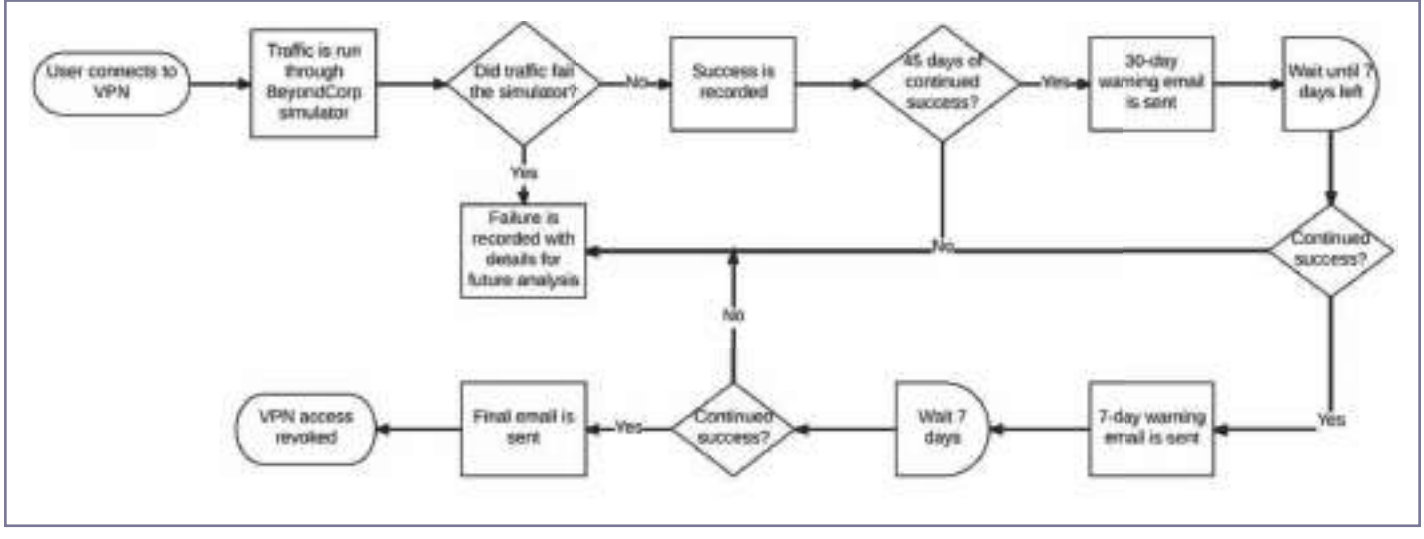
INVENTAIRE, VLAN, PROXY : LES PREMIERS JALONS DE BEYONDCORP

Au moment où Google présentait BeyondCorp, l'essentiel des bases était posé. À commencer par un inventaire permettant de suivre les appareils sur l'ensemble de leur cycle de vie. Le principe : ceux présents dans la base et considérés comme sécurisés peuvent recevoir un certificat spécifique. Celui-ci est stocké dans un TPM (matériel ou logiciel) ou dans un magasin. Renouvelé périodiquement, il est employé pour toute connexion à une ressource. Les utilisateurs – et les groupes – sont eux aussi stockés dans des bases, intégrées avec les processus RH (arrivées, départs, mobilités internes). L'authentification (à deux facteurs) se fait par l'intermédiaire d'un portail SSO externalisé qui génère des jetons éphémères. Côté réseau, l'objectif était de prendre ses distances avec l'intranet « de confiance », au profit d'une segmentation en VLAN dépourvus de privilèges. Le principal pour les terminaux authentifiés. Un second, de type « invité », pour ceux non gérés ou non reconnus. L'assignation, dynamique, s'appuie sur un serveur RADIUS. Elle découle de la décision d'un moteur de contrôle d'accès embarqué dans un proxy placé devant toutes les applications. Avant que Google lance sa démarche zero trust, l'accès à ses apps se faisait soit directement via le réseau privilégié, soit par VPN pour les connexions externes. L'ère BeyondCorp est synonyme de migration en deux étapes. D'abord, substituer le proxy aux accès VPN.

L'ère BeyondCorp est synonyme de migration en deux étapes.

Ensuite, le généraliser pour l'accès depuis tout réseau. Pour l'extinction du VPN, trois grandes règles. Premièrement, restreindre son usage aux utilisateurs capables de prouver qu'ils en ont besoin. Deuxièmement, sur cette population, supprimer les droits d'accès passé une période d'inactivité. Troisièmement, encourager les utilisateurs effectivement actifs à migrer dès lors qu'on est (quasi) certain que tous leurs workflows

titre schéma



sont disponibles au travers du proxy. Pour s'assurer que c'est le cas, on examine le trafic à deux niveaux. D'une part, en analysant un échantillon de données issues des switchs. De l'autre, sur les terminaux, avec une sonde logicielle qui simule le réseau sans privilèges. À partir du moment où on dépasse une proportion de trafic « compatible » (pouvant être acheminé vers le reste du réseau de l'entreprise), on peut envisager d'amorcer le basculement. Le seuil est à 99,99 % sur 30 jours consécutifs. Une fois atteint, on passe la sonde logicielle en mode « actif » : en plus de journaliser, elle bloque le trafic incompatible. Après 30 jours supplémentaires, si le seuil est maintenu, on le consigne dans l'inventaire. Ce qui fournit un signal fort pour assigner l'appareil au réseau sans privilèges lors de sa prochaine authentification RADIUS.

LES DÉFIS DE L'ÉVALUATION CONTINUE

Début 2016, BeyondCorp faisait l'objet d'une deuxième publication. Google y détaillait, entre autres, le processus de mise à l'échelle de son inventaire. Avec notamment des précisions sur les sources de données. Côté interne, il listait Active Directory, Puppet et Simian. En externe, des scans de vulnérabilités, des autorités de certification ou encore des éléments d'infrastructure réseau de type tables ARP. Le tout accompagné d'un ordre de grandeur : en moins de deux ans, sur un périmètre de 15 sources, plus de 80 To de données ingérées. Observées pour certaines (version de l'OS, logiciels installés, date de la dernière analyse de sécurité...). Fournies pour d'autres (propriétaires d'appareils, listes d'autorisations, attributions DNS et DHCP...), autant dans l'optique de commencer à constituer l'inventaire que de s'adapter aux clients non personnalisables à l'image d'une partie des imprimantes. Google revenait également sur les défis liés à la qualité de ces données (gestion des doublons, restauration d'un état précédent de l'inventaire), à leur propagation (disponibilité vs latence)... ainsi qu'à leur corrélation. Par exemple, le fait que différents identifiants peuvent se rattacher à un même appareil (numéro de série dans un système de gestion d'actifs, numéro de disque dans un gestionnaire de chiffrement, adresse MAC dans une base ARP). Et l'amplification potentielle du phénomène à l'échelle du cycle de vie des appareils, étant donné qu'il arrive de remplacer des composants, voire d'en échanger.

> *Avant zero trust, chez Google, l'accès aux apps se faisait soit directement via le réseau privilégié, soit par VPN pour le connexions externes.*

UN PROXY À TOUTE ÉPREUVE ?

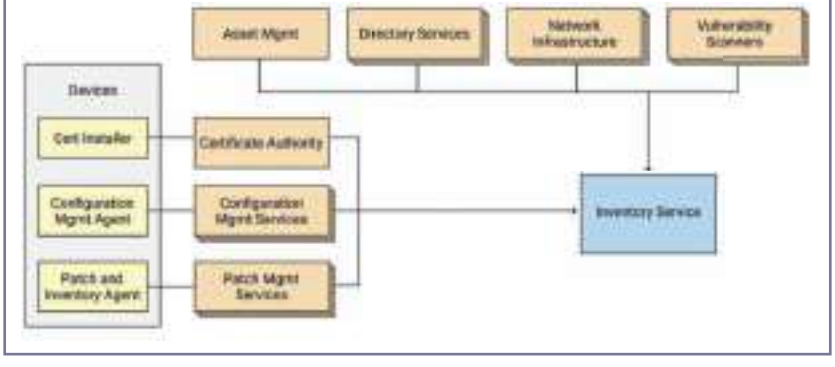
Toujours en 2016, Google consacrait une publication au proxy. On en découvrait le substrat. À avoir la flotte de proxys HTTP(S) inversés formant le front-end des applications web du groupe américain. Un socle sur lequel avaient été greffées des briques d'authentification, d'autorisation et de journalisation automatisée spécifiques à BeyondCorp. Le proxy est capable de gérer les requêtes faites sans identifiants utilisateur, comme celles d'un gestionnaire de logiciels qui tenterait de télécharger des mises à jour. Il est « transparent » pour les back-end, qui peuvent implémenter leurs propres flux d'authentification, potentiellement plus granulaires. Le chiffrement des communications repose sur le framework LOAS (Low Overhead Authentication System). Avec lui, on peut transmettre des métadonnées qui permettront par exemple d'activer des fonctionnalités au vol en fonction du

Un inventaire permettant de suivre les appareils sur l'ensemble de leur cycle de vie.

Début 2017, l'entreprise américaine publiait un nouveau document, axé sur l'équilibre productivité-sécurité.

niveau de confiance des appareils. Le proxy répond à deux types de règles : globales ou spécifiques à un service. Il embarque un mécanisme de provisionnement en libre-service permettant aux propriétaires d'applications de modifier eux-mêmes la configuration. Et surtout plusieurs « parades ». On peut en citer trois. Tout d'abord, la création de tunnels point à point pour gérer les logiciels tiers incapables de présenter des certificats TLS ou qui supposent une connectivité directe. Encuite, le serveur d'autorisation HTTP inclus dans le flux d'ouverture de connexion pour limiter l'effet de latence induit sur Chrome Remote Desktop, principale solution de bureau à distance des employés du groupe. Enfin, les bacs à sable, sous forme d'instances séparées du proxy que le répartiteur de charge ignore, mais que les développeurs peuvent exploiter. À ce stade de la démarche BeyondCorp, les ordinateurs utilisaient, en guise d'identifiants « persistants », des certificats X.509. Leur rotation impliquant de relancer le navigateur pour s'assurer de la fermeture des sockets, Google envisageait de passer à un identifiant tel que ceux exploités sur mobile (sur iOS, ForVendor, codé « en dur » ; sur Android, celui de l'EMM).

Circuit de confiance



DES SYSTÈMES ET DES UTILISATEURS

Début 2017, on franchissait une première étape vers la commercialisation de BeyondCorp : Google ouvrait l'accès à une version expérimentale de son proxy. Au cours de l'été, il en annonçait la disponibilité globale pour ses environnements App Engine, Compute Engine et GKE. En parallèle, il publiait un nouveau document, axé sur l'équilibre productivité-sécurité. Au programme, l'approfondissement de la réflexion sur les fameux certificats. Et sur l'édifice mis en place pour les acheminer vers les appareils (développement d'une autorité de certification, création d'API, déploiement de la couche 802.1x sur les switchs, etc.). Au menu également, d'autres cas particuliers traités avec la solution « tunnel chiffré ». Par exemple, les applications liées à des serveurs de licence non HTTP ou celles invoquant des méthodes à distance. Et côté infrastructure, les serveurs NFS/CIFS ne respectant pas les propriétés minimales requises en matière de chiffrement et d'authentification. Deux solutions substitutives : stockage local + backup cloud ou remplacement par Google Drive. Esquissée dans ce document, l'expérience utilisateur allait véritablement être abordée à l'automne, avec une publication dédiée. Google y explique insister, dès l'intégration des employés, sur leur principal point de contact avec BeyondCorp : l'extension Chrome. Et évoque quelques-unes de ses capacités, dont la détection de portails captifs (hôtels, <aéroports...). La technique : essayer de récupérer une page qui génère une 204. Si on obtient autre chose, on part du principe qu'on se trouve derrière un tel portail. On se rabat alors sur des règles codées en dur et on invite l'utilisateur à basculer un paramètre. Le même, d'ailleurs, que pour accéder à des équipements sur un réseau local. Google revient sur d'autres fonctionnalités d'assistance, dont un portail d'explication des erreurs et la possibilité de basculer sur une extension secondaire de gestion de proxy. À ce moment-là, l'option VPN est toujours disponible. Mais il faut en faire la demande. Et l'accès expire si on ne s'est pas connecté, dans les 75 derniers jours, à un service « non compatible BeyondCorp ».

> *À la Cloud Next'18, Google affichait un premier « gros » cas client :Veolia, avec un déploiement zero trust couvrant 169 000 employés à l'échelle mondiale.*

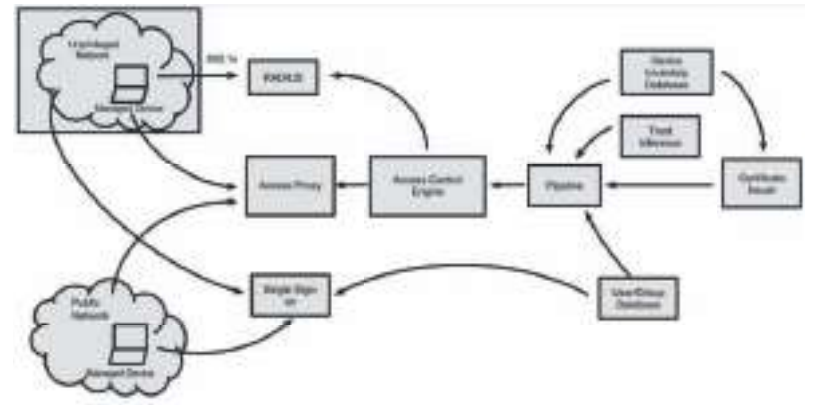
Google a normalisé ses méthodes de contrôle.

BEYONDCORP RALLIE LES EDR

À la Cloud Next'18, Google affichait un premier « gros » cas client, en l'objet de Veolia, avec un déploiement zero trust couvrant 169 000 employés à l'échelle mondiale. L'édition suivante allait mettre en lumière le cas Airbnb. Et être le théâtre du lancement d'une alliance avec un groupement de fournisseurs d'EDR. Initialement, Check Point, Lookout, Palo Alto Networks, Symantec et VMware. Tous s'engageaient à partager des données de posture de sécurité pour alimenter le moteur décisionnel de BeyondCorp. Entre-temps (automne 2018), Google avait apporté des précisions à propos de ses mécanismes d'évaluation continue. Et des outils qui le soutenaient. OS Query de Facebook en faisait partie, pour la télémétrie. Defender Credential Guard (de Microsoft) aussi, au sein d'une liste de conseils pour orchestrer le déploiement des stratégies de sécurité. Limiter l'éventail des configurations hardware en est une. Utiliser des listes blanches plutôt

que des listes noires (plus complexes à maintenir, car potentiellement infinies) en est une autre. Dans la pratique, l'hétérogénéité des plates-formes et des menaces qui les ciblent complique l'application uniforme des stratégies. Aussi Google a-t-il normalisé ses méthodes de contrôle. Et défini, autant que possible, des seuils de conformité plutôt que des valeurs absolues. Tout en adoptant une démarche progressive de déploiement, fonction des populations et des niveaux de criticité.

La méthode RADIUS



VERS LA SÉCURISATION DU CLOUD

Fin 2019 émergeait une nouvelle marque : BeyondProd. Ou BeyondCorp appliqué aux microservices. Dans ce cadre, Google met en œuvre des concepts tels que les points de terminaison de service mutuellement authentifiés, la sécurité des données en transit, la provenance de code de bout en bout et le maillage de services. En 2020, Citrix, Crowdstrike, Jamf et Tanium rejoignaient l'alliance BeyondCorp. L'offre commerciale s'enrichissait quant à elle d'une solution d'accès à distance... qui allait devenir, début 2021, BeyondCorp Enterprise. Sans agent (via Chrome) et exploitant les points de présence du réseau Google. Une version Essentials a été lancée cette année. Elle associe contrôle d'accès contextuel, DLP, filtrage d'URL et protection contre les malwares. ■

Fin 2019 émergeait une nouvelle marque : BeyondProd. Ou BeyondCorp appliqué aux microservices.

Silicon

DAY WORKPLACE

COLLABORER DANS
UN ENVIRONNEMENT
DE TRAVAIL HYBRIDE

RETOUR SUR LES CONFÉRENCES DE LA JOURNÉE DU 14 JUIN 2022

EN PARTENARIAT AVEC :

DARKTRACE GoTo jamf orange Business Services zoom

DARKTRACE : PROTÉGER les applications SaaS des cybermenaces

Les plateformes Cloud et SaaS ont créé des environnements numériques où les entreprises peuvent innover, collaborer et partager plus que jamais. Cela se fait, cependant, souvent au détriment de la visibilité et du contrôle. Quels sont donc les défis de la sécurisation des applications cloud et SaaS ? Comment l'IA Auto-Apprenante détecte-t-elle et neutralise-t-elle les menaces dans les applications cloud ?

En mars 2020, le télétravail s'est imposé du jour au lendemain. Les discussions au bureau sont devenues des emails. Les réunions avec paperboard sont devenues des conférences en visio. Dans ce contexte, les entreprises ont dû faire preuve de flexibilité et ouvrir leurs systèmes qui auparavant étaient utilisés uniquement au sein des locaux de l'entreprise. Selon Alexis Martin, Expert Cybersécurité, Darktrace *« Les entreprises se sont relativement bien adaptées pour ce qui concerne les outils SaaS et l'ouverture de réseau, à une exception près, la cybersécurité ! »*.

Limites de l'approche traditionnelle

Le phishing et l'exfiltration de données sont les 2 menaces que redoutent la plupart des entreprises. Selon Alexis Martin, *« le problème c'est que la façon traditionnelle de faire de la cybersécurité ne permet pas de répondre aux nouvelles méthodes d'attaques toujours plus innovantes. En effet, la sécurité traditionnelle se base principalement sur des outils à règles et signatures tels que les bases de données d'indice de compromission, les bases de données de scénarios d'attaques... ce seraient des outils parfaits si les attaquants ne continuaient pas d'innover en permanence dans la mesure où ils fonctionnent parfaitement pour les menaces connues. »*.

Darktrace DETECT

Darktrace a mis au point une intelligence artificielle basée uniquement sur une approche comportementale. Pas de règles et signatures, ni de bases de données d'attaques passées, l'IA comprend l'entièreté des environnements numériques qui composent le réseau de l'entreprise. Elle va également chercher à comprendre tous les comportements des collaborateurs et créer des modèles qui représentent la façon de travailler de chacun. *« Cette approche dynamique différente d'autres outils permet de s'adapter aux risques que représentent chaque individu. Cette IA Auto-Apprenante cartographie les menaces et anticipe à la fois les attaques basiques mais aussi les attaques aux scénarios plus sophistiqués sur lesquels les outils traditionnels sont aveugles »*, souligne Alexis Martin.

Au cours des 18 derniers mois, 98 % des entreprises ont subi au moins une violation de données dans le cloud (IDC, 2021)

Darktrace RESPOND

La capacité de réponse autonome de la machine aux cyberattaques permet de ne pas seulement être alerté de la menace mais de pouvoir y répondre en temps réel. La Réponse Autonome agit de manière chirurgicale en traitant la menace sans perturber l'activité de l'entreprise. *« Darktrace c'est un moteur d'intelligence artificielle qui regroupe les métadonnées les plus importantes pour bien saisir le fonctionnement de l'entreprise. Contrairement à beaucoup d'autres outils, inutile de se conformer à une solution standardisée, c'est l'IA qui s'adapte aux fonctionnements et aux menaces uniques de chaque entreprise »*, explique Alexis Martin. ■

DARKTRACE

COMMENT LA DIGITAL WORKPLACE remodèle le support informatique ?

Les outils d'assistance à distance de support sont indispensables pour diagnostiquer, dépanner et résoudre les problèmes techniques d'un client. Alors que le monde revient à une certaine normalité, de nombreux centres d'appels/services IT interne, réévaluent leur portefeuille technologique existant afin de répondre à une nouvelle série de défis créés par un travail flexible et de nouvelles habitudes numériques.

Durant la pandémie, beaucoup de changements ont été observés. La pression s'est accrue sur les services informatiques. De grosses faiblesses en termes de sécurité ont été mises au jour avec la recrudescence des attaques. Les outils utilisés se sont révélés peu adaptés pour transitionner vers un monde hybride. Les entreprises se sont donc équipées de nouvelles solutions dans un temps record pour maintenir un niveau de productivité et d'efficacité au sein de leurs équipes.

Tendances constatées concernant l'assistance technique, le support pour les entreprises

Les habitudes numériques ont changé. Tous les utilisateurs sont passés au First Digital. Le contact physique n'est plus indispensable. Les nouvelles attentes se concentrent donc sur la résolution de problème qui doit s'effectuer dans un temps record avec des personnes qualifiées.

On observe également que la perturbation de la chaîne logistique favorise l'utilisation des outils de prise en main à distance. Au pic de la pandémie, il y a eu un goulot d'étranglement qui a complexifié les approvisionnements pour le remplacement des outils. À présent, c'est la réparation qui est privilégiée plutôt que le remplacement.

La 3è tendance observée concerne le phénomène de "la grande démission". À l'heure actuelle, les agents et techniciens de support ont une fonction qui connaît beaucoup d'attrition. Ce sont des postes où il manque du personnel au quotidien. *« Avant la pandémie, le turnover était de 35 à 40 %, il peut à présent monter jusqu'à 80 %. »*, souligne Laura Van de Wiele, Responsable Marketing Europe du Sud, GoTo. L'enjeu pour les entreprises est donc de retenir les talents et d'assurer le maintien de la productivité.

Critères d'évaluation des outils d'assistance à distance

En premier lieu, le critère à évaluer est la flexibilité. Il est indispensable que les outils de prise en main à distance, de supports d'assistance et de monitoring puissent être pris en charge sur n'importe quel type d'appareil (ordinateur, tablette, mobile...).

Ensuite, la sécurité avant tout ! Le travail hybride a augmenté le risque de cyberattaques. C'est donc un élément essentiel à prendre en compte. *« Ça passe par avoir des connexions sécurisées, la confidentialité des informations, le chiffrement des données... tout ce qui permet de s'assurer un niveau supérieur de sécurité »* explique Laura Van de Wiele.

Enfin, la personnalisation des outils aux couleurs de l'entreprise pour rassurer l'utilisateur sur le fait que le site est fiable, la collaboration par le biais de multi-sessions si le cas a besoin d'être escaladé ainsi que toutes les fonctionnalités admin qui permettent de faire du monitoring et mettre en place des audits sont des éléments indispensables à prévoir pour une solution efficace de support à distance. ■

GoTo

EXPÉRIENCE UTILISATEUR ET SÉCURITÉ : les défis des nouveaux environnements de travail

Les préoccupations autour des nouveaux environnements de travail se concentrent sur l'expérience utilisateur, le travail à distance et la capacité à fournir aux collaborateurs des outils sécurisés dans le cloud. Pistes de solutions autour de l'onboarding grâce au BYOD (Bring Your Own Device) et au déploiement zéro-touch.

De plus en plus d'entreprises adoptent les technologies Apple

Alors qu'il y a 15 ans Windows dominait dans les entreprises, aujourd'hui, 91 % des sociétés ont déjà intégré Apple que ce soit avec seulement quelques appareils ou des milliers. Ce chiffre est issu d'une étude menée par Jamf, éditeur de solutions qui aident les entreprises à gérer leur flotte d'appareils Apple depuis 20 ans. Matthieu Castel, Senior Systems Engineer constate que *« la pandémie a accéléré l'usage des terminaux personnels. Ainsi, beaucoup de collaborateurs qui utilisaient leur Mac à titre privé ont demandé la possibilité de l'utiliser également dans le cadre de leur activité professionnelle au sein de l'entreprise »*.

On observe, par ailleurs, qu'Apple est plutôt méconnu dans le secteur de l'entreprise. Or, ce marché, uniquement sur le segment business, pèse 25 milliards de dollars et est en constante évolution. L'étude menée par Jamf révèle même que 62 % des salariés interrogés préfèrent utiliser Apple au travail s'ils en ont la possibilité.

Faciliter l'onboarding des collaborateurs

Les principaux leviers reposent sur l'automatisation de la configuration de tous les types d'appareils Apple, l'automatisation des flux de travail à grande échelle, le suivi de l'état des appareils et la vue 360° de l'environnement. Par exemple, avec Jamf Pro, Matthieu Castel explique qu'il suffit de *« connecter les appareils Apple au compte Apple Business Manager et de les intégrer directement avec le MDM Jamf. Ainsi, lorsque l'appareil sera démarré, tout se configurera automatiquement (applications, profils, restrictions, sécurité) ... Avec cette solution, tous les terminaux Apple sont gérés de manière centralisée »*.

Il est par ailleurs important de laisser le choix aux collaborateurs en termes d'équipement afin qu'ils puissent choisir la technologie avec laquelle ils sont à l'aise pour travailler. Pour certaines entreprises, proposer un Mac est devenu un argument de recrutement. De même que si l'expérience d'onboarding est solide, elle peut améliorer le taux de rétention des collaborateurs.

Des pratiques en constante évolution

L'arrivée des puces M1 a eu un réel impact sur la croissance d'Apple en entreprise. Plus rapides et permettant une meilleure connectivité entre les appareils, elles ont facilité le déploiement zéro-touch.

Autre évolution : la simplification de la gestion des parcs mixtes. En effet, dans les entreprises les parcs ne sont plus composés presque exclusivement que d'ordinateurs. Les mobiles et tablettes sont venus s'ajouter à la composition des parcs informatiques. Enfin, de plus en plus de collaborateurs choisissent Apple pour l'expérience utilisateur et pour la simplicité des appareils. *« Cette tendance ne va faire que se renforcer dans les prochaines années »*, selon Matthieu Castel. ■

jamf

COMMENT S'ASSURER DE L'EFFICACITÉ du Digital Workplace ?

Les organisations doivent repenser l'environnement de travail de leurs collaborateurs autour des nouveaux modes de fonctionnement en alliant efficacité et résilience. Elles doivent aussi répondre aux nouvelles attentes des collaborateurs pour rester attractives. Le Digital Workplace est la pierre angulaire qui rend possible ces changements.

Des nouvelles attentes collaborateurs nombreuses et variées

Parmi ces nouvelles attentes, il y a celle qui consiste à avoir des outils simples, nomades et efficients ainsi que la volonté de combiner travail hybride et efficacité. Vannina Kellershohn, Senior Vice President Business Unit Enriched Interactions & Collaboration chez Orange Business Services, constate que « *la plupart du temps ce qui ne permet pas un usage hybride efficace ce sont des causes très opérationnelles et pragmatiques comme par exemple, un poste de travail qui n'est pas adapté, une salle de réunion qui ne permet pas les interactions hybrides... car le mode hybride, ce ne sont pas uniquement des gens qui travaillent à distance. Ce sont aussi des personnes qui interagissent qu'ils soient au bureau, en télétravail ou sur le terrain* ».

Une culture du travail hybride insuffisante

C'est le plus gros frein à la mise en place du Digital Workplace. En effet, même si l'entreprise dispose des outils, si la culture du travail ne s'adapte pas aux nouveaux fonctionnements l'écueil est de créer un non-sens en reproduisant d'anciens fonctionnements qui ne sont pas efficaces dans le nouvel environnement.

De plus, le travail à distance est devenu pour certains une priorité absolue. Le besoin de flexibilité et équilibre entre vie professionnelle et vie privée, permettant une productivité à la maison accrue sont progressivement devenus la norme pour la catégorie de travailleurs dite de "bureau".

Quels chantiers mettre en œuvre pour un déploiement efficace ?

L'essentiel est d'aborder le déploiement du Digital Workplace avec une vision "Parcours collaborateur" en le pilotant de façon globale et en évitant à tout prix la gestion en silos. Selon Jean-Michel Menant, Directeur Conseil en expérience clients et salariés, Orange Consulting, « *les 6 chantiers prioritaires à lancer sont la renégociation de l'accord de télétravail, la définition des usages hybrides (collaboration et processus), la détermination de l'usage des lieux de travail (réduction du nombre de postes de travail), le renforcement des infrastructures (scalabilité, performance, sécurisation), la modernisation du Digital Workplace (modernisation des outils collaboratifs, move to cloud, téléphonie...) et l'évolution de la culture de travail en mode hybride (nouveaux modes de managements, acculturation aux nouvelles pratiques). Tous ces chantiers sont indispensables et doivent être menés de manière concomitante pour réussir le déploiement du Digital Workplace.* »

Ce sujet du Digital Workplace est au cœur de la transformation de l'organisation de l'entreprise mais intervient également sur sa capacité à attirer des talents, à générer de la productivité ainsi que sur l'excellence de la relation client. Le Digital Workplace est donc un sujet transversal qui concerne aussi bien les DSI que les DRH. « *Plus qu'une simple transformation digitale, c'est une transformation humaine de l'entreprise* » souligne Vannina Kellershohn. ■

orange Business Services

L'INNOVATION dans notre monde VUCA

Dans la réalité de notre monde VUCA (Volatil, Uncertain, Complex, Ambiguous), quels sont les grands enjeux pour les DSI ? Entre gestion des injonctions contradictoires, compréhension des grandes tendances technologiques et gestion des risques... quelles sont les solutions actionnables pour relever les défis actuels ?

Le concept VUCA (Volatil, Uncertain, Complex, Ambiguous) a été créé par l'armée américaine dans les années 80 pour définir la manière dont le monde allait évoluer. La notion est toujours d'actualité pour décrire le monde dans lequel nous vivons. Volatil, les choses changent vite / Complex en raison des crises multiples (économique, sanitaire, climatique) / Uncertain car toutes les crises s'entrecroisent / Ambiguous du fait de la complexité et de l'incertitude.

Saisir les enjeux du monde tel qu'il est

Pour les DSI, le premier enjeu repose sur la compréhension de l'impact de l'évolution technologique sur l'organisation dans les années qui viennent. Par exemple, à l'heure de l'intelligence artificielle et de la réalité augmentée, manquer un virage technologique peut être fatal à une entreprise.

Ensuite, il est indispensable pour les décideurs IT de savoir gérer les injonctions contradictoires, illustrations édifiantes de notre monde VUCA (investissement vs maîtrise des coûts, orientation des demandes utilisateurs vers plus de flexibilité vs cybersécurité...).

Enfin, 3è enjeu majeur, la sécurité ! Cybersécurité, oui mais pas seulement. La difficulté est également de sécuriser les talents en s'assurant d'avoir les compétences informatiques adéquates à la disposition de l'organisation.

Quelle attitude adopter ?

Ne surtout pas se précipiter sur la technologie ! En premier lieu, se poser les bonnes questions et définir le cadre afin d'opter pour une solution technologique adaptée. Par exemple, sur le sujet des communications unifiées, domaine d'intervention de Zoom : comment l'organisation souhaite-t-elle interagir avec ses clients ? Comment l'organisation souhaite-t-elle que les employés interagissent ? *« Il s'agit de se questionner sur comment l'ensemble des technologies à la disposition de l'organisation peuvent faciliter la vie des clients, des employés... C'est à cet endroit que se trouve le cœur du sujet »* selon Etienne Aubourg, CIO Advisor de Zoom.

Innover avec Zoom

« Zoom est une solution simple, fiable et sûre. C'est de là qu'est parti le succès de la plateforme » estime Etienne Aubourg. Toutefois, au-delà de ce qui touche au domaine de la réunion (chat, téléphonie, Zoom Rooms...), la plateforme est également un outil pour les développeurs. Zoom dispose de sa propre place de marché qui héberge plus de 1 000 applications et la plateforme Zoom Developer comprend des API et des SDK qui leur permettent d'intégrer les solutions Zoom à leurs propres applications.

A l'ère de la vidéo, Zoom permet également aux entreprises d'innover en transformant leur business model et d'investir le marché du v-commerce.

« L'innovation est dans l'ADN de Zoom. Ce qui est important ce n'est pas que Zoom innove, c'est le fait que la plateforme elle-même soit innovante pour permettre à ses utilisateurs d'innover dans ce monde toujours plus VUCA » souligne Etienne Aubourg. ■

LA 22

LES ASSISES

12.10.22 →→ 15.10.22

/MONACO///

→ Plus qu'un événement,
une référence, un incontournable

→ lesassisesdelacybersecurite.com

DG CONSULTANTS

COMEXPOSIUM

LastPass •••|

Pilote automatique pour tous vos mots de passe.

#BeCyberSmart

Plus de vigilance. Plus de

#CyberIntelligence.

Notre prochain rendez-vous

LES ASSISES

12 - 15 Oct >> Monaco >> Stand 117

Lastpass.com