L'INNOVATION ET LA R&D PLUS QUE JAMAIS au cœur de la cybersécurité pour Cisco

Technologie, innovation, R&D, information et sensibilisation au risque, collaboration… sont autant de sujets qui mobilisent Cisco dans son appréhension du risque cyber. *Guillaume Sauvage de Saint Marc, Senior Director Engineering au sein de Cisco Emerging Technologies and Incubation,* une entité du groupe dédiée à l'incubation des nouveaux produits, nous en dit plus sur ce que représente la cyber pour Cisco.

Guillaume Sauvage de Saint Marc

Comment un acteur comme Cisco appréhende la question de la cybersécurité ?

Leader des réseaux et d'Internet, Cisco est positionné sur l'ensemble des besoins IT, la transformation et la digitalisation de ses clients. De par notre positionnement, la cybersécurité est un sujet central, car réseau et sécurité sont depuis toujours indissociables.

Nous disposons ainsi d'un très large portefeuille de produits et d'activités en cybersécurité qui nous permet de couvrir toutes les dimensions de ce sujet en nous adressant tant aux entreprises, aux fournisseurs de services télécoms, qu'aux organisations publiques. Nous avons pour habitude de dire que nous couvrons les 3 W : Workforce pour les collaborateurs, Workload pour les applications et Workplace pour les infrastructures et les équipements.

Pour ce faire, chaque année, nous investissons 6,5 milliards de dollars en R&D et dans l'acquisition d'entreprises. En moyenne, Cisco rachète une société toutes les six semaines. En 2021, par exemple, Portshift, spécialisée sur la sécurité des déploiements Kubernetes nous a rejoints, tout comme Kenna Security, axée sur la gestion des risques et vulnérabilités software.

Il y a deux ans, nous avions également racheté la très belle start-up française Sentryo (NDLR Cisco Cybervision) sur le segment de la cybersécurité adaptée aux infrastructures industrielles dont les activités sont souvent critiques.

Par ailleurs, Cisco dispose de la plus grande équipe de threat intelligence non gouvernementale, Talos, dont l'activité consiste à analyser les cybermenaces et les comportements suspects à l'échelle mondiale. Ce travail de veille et de surveillance ne concerne pas uniquement nos produits. Il couvre l'ensemble de la sphère internet et IT. Avec plusieurs centaines de personnes mobilisées, cela représente également un investissement conséquent. Et ces flux d'alerte et d'intelligence sont très importants, car ils permettent non seulement d'enrichir nos produits, de développer de nouvelles fonctionnalités et de gagner en efficacité et en performance, mais surtout de protéger tous nos clients.

Face à une menace et un risque cyber plus fréquents, puissants et sophistiqués, quels sont les principaux enjeux selon vous ?

Le premier est lié à la transformation des entreprises : aujourd'hui, tout le monde doit se digitaliser pour croître, gagner en performance et en compétitivité. Or le risque cyber représente le principal frein à cette dynamique, car plus les entreprises se digitalisent et déploient des technologies et des solutions, plus elles s'exposent à ce risque en élargissant leurs surfaces d'attaques.

Avec la sophistication des technologies et des menaces, les éditeurs ont un rôle clé à jouer en termes de simplification pour s'assurer que leurs solutions soient adoptées de façon optimale et réduire ainsi le risque cyber. Dans une récente étude IPSOS menée pour Cisco, les entreprises plaident pour une simplification des solutions techniques à 74 %, mais également pour un accompagnement afin de mieux les appréhender et les intégrer. Conscients de cet enjeu, nous travaillons sur la simplification et l'accessibilité de nos produits. Nous proposons notamment la plateforme SecureX à nos clients, qui apporte une visibilité sur l'ensemble de l'écosystème sécurité via une interface de supervision unique. Il ne s'agit pas seulement d'apporter les outils, les technologies et les solutions, il est tout aussi important de proposer le conseil et l'accompagnement qui vont avec. Ce travail de sensibilisation et de communication doit mobiliser l'ensemble des parties prenantes, car la sécurité est l'affaire de tous, et face au risque cyber, l'union fait la force ! Nous

collaborons ainsi avec l'ANSSI, sommes un membre actif de Cybermalveillance.gouv.fr sur des actions de sensibilisation sur le risque cyber et de valorisation du label ExpertCyber. Les équipes Cisco sont également présentes au Campus Cyber pour en faire un lieu de coopération, de formation et de co-innovation. Enfin, le dernier enjeu est celui de la pénurie de compétences en matière de cybersécurité. Parmi les freins relatés par les entreprises pour mettre en œuvre une démarche structurée en matière de cybersécurité, on note le manque d'accompagnement (49 %), mais aussi de formation (49 %), de compétences internes (48 %) et de difficultés à recruter (46 %). 75 % d'entre elles révèlent qu'elles n'ont pas encore formé leurs collaborateurs sur le sujet de la cyber ! Fort de ce dernier constat, Cisco a récemment annoncé son ambition de former 100 000 personnes aux enjeux de la cybersécurité et de l'industrie du futur, en s'appuyant sur son programme NetAcad, qui a déjà accompagné plus de 250 000 personnes depuis vingt ans en France.

Quelles sont les mutations les plus structurantes qui redessinent les contours du risque cyber ?

Depuis quelques années, nous assistons à une mutation des surfaces d'attaques de sécurité. La notion de sécurité périmétrique est bien évidemment toujours d'actualité, mais elle ne suffit plus. Aujourd'hui, nous parlons de plus en plus de Zero Trust et d'approche SASE, car il ne s'agit plus seulement de sécuriser les infrastructures et les systèmes au sein de l'entreprise, mais également les données et les applications qui sont désormais largement déployées au-delà de ses frontières, au travers du cloud, qui est par principe une infrastructure tierce et partagée. À cela s'ajoute la question de l'authentification avec des solutions dites MFA (Multi Factor Authentification) – notamment par vérification via le smartphone de l'utilisateur, comme notre solution DUO. Nous nous dirigeons vers le renforcement de cette tendance et même vers l'obsolescence des mots de passe. Non seulement l'authentification multi-facteur va nous faciliter la vie, mais relever le niveau de sécurité de manière significative.

“Cisco dispose de la plus grande équipe de threat intelligence non gouvernementale, Talos, dont l'activité consiste à analyser les cybermenaces et les comportements suspects à l'échelle mondiale.”

La cybersécurité est également une question d'innovation et de R&D. Qu'en est-il ?

Dans le monde cyber, le temps est déterminant : tous les acteurs, cyberattaquants d'un côté, entreprises, institutions et gouvernements de l'autre, sont dans une logique de course à l'armement permanente. L'innovation et la R&D sont clés pour pouvoir répondre aux nouvelles menaces en faisant évoluer les solutions existantes ou en développer de nouvelles. Ces dernières, même si elles se complexifient doivent rester simples à adopter et déployer. L'expérience utilisateur doit primer pour garantir aux utilisateurs de s'en servir correctement et à bon escient. Il faut donc trouver le juste équilibre entre technologie et simplicité d'usage pour que la sécurité soit simple, efficace et n'entrave pas leur quotidien.

Cette démarche d'innovation continue doit s'inscrire aussi dans une logique de collaboration et d'entraide. Le partage d'informations sur des vulnérabilités émergentes ou de bonnes pratiques est essentielle pour contrer les attaques et les cyberattaquants.

Et dans cette continuité, quels sont les sujets qui vous intéressent ?

L'intelligence artificielle a vocation à jouer un rôle stratégique dans la cybersécurité. Utilisée par les attaquants, elle rend leurs attaques plus dangereuses et démultiplie leur impact grâce à l'automatisation. Inversement, nous capitalisons aussi sur sa puissance pour nous défendre et contrer les attaques. Elle est notamment utilisée, dans le cadre d'analyses statistiques, pour détecter des signaux faibles qui peuvent annoncer une nouvelle attaque ou vulnérabilité. Elle permet aussi de faire des détections d'attaques sur du trafic complètement encrypté quand les attaquants se pensent souvent à l'abri des systèmes de surveillance cyber. Nous commercialisons déjà des solutions de ce type. Sans avoir accès à l'information, mais uniquement en observant le comportement des flux, il va être ainsi possible de détecter une attaque.

De plus, nous nous intéressons aux perspectives que l'informatique quantique peut offrir en matière de cybersécurité, même si ces technologies sont encore essentiellement au stade de la recherche appliquée. L'informatique quantique va permettre encore plus de protection avec des chiffrements quantiques forts, voire inviolables. Toutefois, ces mêmes ordinateurs pourront, une fois opérationnels, casser un certain nombre de protections et de chiffrements utilisés aujourd'hui. Mais nous travaillons d'ores et déjà main dans la main avec nos clients sur ces risques, notamment pour faire face à des attaques et des menaces qui pourraient survenir dans le futur sur des données interceptées et enregistrées actuellement.

L'état de l'art est aujourd'hui suffisamment avancé pour mener des réflexions à ce niveau : plus que jamais, Cisco est mobilisé sur la cybersécurité pour protéger ses clients.