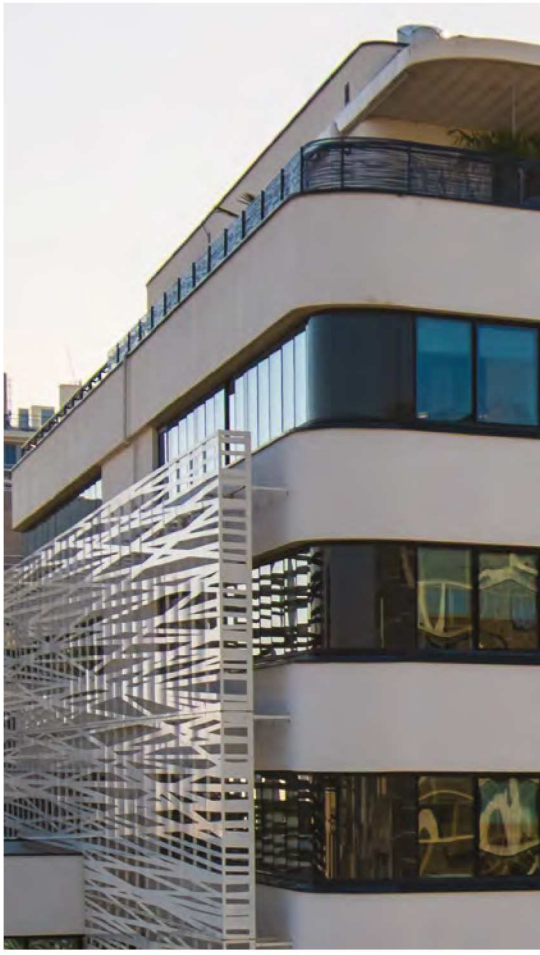
Citya Immobilier
s'aide d'une IA générative pour la sécurité de son SI

Le groupe immobilier s'est doté d'un NDR avec une IA générative associée pour protéger son infrastructure informatique. Les équipes opérationnelles et les analystes sont secondés par Gaia, cet assistant de nouvelle génération proposé par Gatewatcher.



Avec Laforêt, Guy Hoquet et Century 21, Citya Immobilier est l'un des grands réseaux d'agences immobilières du groupe Arche. Le SI de cette enseigne est remarquable puisque, en 2025, il reste 100% on-premise. C'est une filiale spécialisée baptisée Q1C1 qui en assure la gestion. *«Nous couvrons pratiquement tout le périmètre informatique du groupe, à l'exception de celui des franchisés qui disposent d'un SI full SaaS»*, explique Dominique Reuillon, directeur de Q1C1 et DSI du groupe Arche.

«Ce déploiement en mode on-premise s'appuie sur deux data centers en PCA.» Messagerie, ERP, CRM, toutes les applications mises en œuvre par les collaborateurs de Citya sont hébergées dans ces data centers. Toutes marques du groupe confondues, cela représente de l'ordre de 400To de données en production et de 8 à 9Po sauvegardées. Car, outre Citya Immobilier, Q1C1 interagit avec d'autres filiales du groupe, dont Saint Pierre Assurances, Belvia Garanties, API Financement dans le courtage de prêts, Citya Développement, Snexi, Cousin Hub, etc.

Pour assurer la sécurité de ce système d'information, le groupe mise sur des solutions à l'état de l'art, donc ce qui se fait de mieux en cybersécurité. Q1C1 a par exemple déployé des firewalls Palo Alto, ainsi que la solution XDR de l'éditeur américain pour son SOC. Il centralise aussi les données générées de la plateforme d'authentification Okta. Cette solution de type SASE est hébergées dans le cloud. L'exploitation du SOC est assurée par le toulousain Exaprobe qui prend également en charge l'analyse des incidents de sécurité remontés dans les logs. *«Ils traitent pour nous toutes les alertes qui arrivent sur notre XDR, y compris celles générées par Okta.»*

Il y a cinq ans environ, ce dispositif a été complété avec une solution de sécurisation du réseau de type NDR (Network Detection and Response). Plutôt que d'opter pour celle de Palo Alto, le DSI a choisi de diversifier ses outils de détection et a fait le choix de celui de l'éditeur français Gatewatcher. *«Nous souhaitions avoir la meilleure solution de NDR du marché, interopérable avec notre écosystème afin d'être en capacité de détecter en temps réel et de répondre à tous types d'attaques.»*

La mise en œuvre de ce NDR souverain a permis à l'ensemble du groupe Arche d'avoir accès à l'IA générative Gaia développée par Gatewatcher. Celle-ci traite l'aide à la configuration des éléments de sécurité, la définition de la politique de sécurité et l'interaction avec les solutions tierces. Enfin, Gaia est nourrie des fils de données de toutes les sources de type CTI (Cyber Threat Intelligence), ce qui lui donne la connaissance de tous les modes d'attaques référencés par les experts.

Dominique Reuillon explique le rôle dévolu à cette IA dans le cadre du groupe Arche : *«Les volumétries de données à traiter sont énormes et elle nous permet d'automatiser le traitement des logs. Elle apporte une solution à la fragmentation des données qui sont rapatriées de tous nos systèmes de sécurité* [NLDR : Firewall, EDR, Authentification SASE et NDR] *vers le XDR, et cela fait gagner beaucoup de temps à nos équipes.»* L'IA Gaia met en rapport tous les éléments techniques liés à un incident qu'elle parvient à trouver dans les logs et permet de détecter des corrélations d'événements de sécurité. Cette recherche dans des Go de données est particulièrement rébarbative et l'IA allège considérablement la charge des équipes infrastructures et des analystes du SOC. *«Elle retrouve l'ensemble des informations pertinentes depuis le data lake, ce qui nous permet de gagner du temps dans la résolution des incidents. Dans son quotidien, l'ingénieur cyber doit trier beaucoup de faux positifs avant de tomber sur un réel incident de sécurité. Avec Gaia, il est beaucoup plus rapide d'écarter ces faux positifs et cela accélère grandement l'ensemble des opérations.»*

Sur l'interface d'administration de la solution Gatewatcher, G Center, l'ingénieur cyber a aussi la possibilité de corriger une alerte remontée par le NDR et d'affecter un scoring minoré à un incident s'il considère que celui-ci correspond au comportement normal d'une application. Ce cas de figure est assez fréquent sur les applicatifs relativement anciens. *«Comme nous avons la*

Pour assurer la sécurité de son SI, le groupe mise sur des solutions à l'état de l'art

Q1C1 est la filiale de Citya Immobilier dédiée à la gestion de son système d'information. Celle-ci compte 27 personnes. Elle s'appuie sur les services managés d'Exaprobe, filiale d'Econocom, pour son SOC. Avec le NDR de Gatewatcher, elle peut désormais utiliser le potentiel de l'IA générative associée Gaia pour qualifier puis traiter plus rapidement les incidents de sécurité.

connaissance de nos applications, cette démarche nous permet de créer et de qualifier facilement les nouvelles règles de filtrage de nos firewalls.» L'IA générative créée par Gatewatcher est par ailleurs capable de générer la règle à déployer sur le firewall Palo Alto pour écarter les autres incidents du même type.

La gestion des incidents facilitée par l'IA

L'interface G center et l'assistant Gaia jouent aussi un rôle de centralisation des informations mises à disposition des analystes du SOC et des opérationnels, quelle que soit leur provenance. Classiquement, le prestataire de SOC assure un traitement automatisé des logs provenant des infrastructures de son client. Il met en œuvre des technologies de type SOAR, une approche à base de règles que l'IA générative vient aujourd'hui compléter : «*Cet enrichissement facilite grandement leur traitement*», note Dominique Reuillon. Toutes les alertes remontées dans le XDR chaque jour sont catégorisées. De l'ordre de 60 d'entre elles sont considérées comme critiques chaque semaine et sont remontées aux ingénieurs de Q1C1 pour investigation. «*Gaia nous aide dans la levée de doute sur ces incidents. L'IA Gatewatcher est connectée avec les grandes bases de données de threat intelligence. Elle dispose donc d'une bonne connaissance sur les malwares. Cela nous permet d'être beaucoup plus efficients dans le traitement des incidents et dans cette levée du doute*», ajoute le responsable. En outre, Gaia peut déclencher des actions basées sur le contexte, mais pour Dominique Reuillon, l'objectif n'est pas de supprimer l'humain dans la boucle de décision. «*Il faut toujours conserver un libre arbitre quant aux décisions qui doivent être prises en présence d'un incident, dans la pertinence d'activer ou non une nouvelle règle de filtrage sur nos firewalls.*» L'IA ne va donc pas remplacer le rôle des experts en cybersécurité, mais dans un contexte de pénurie de main-d'œuvre et d'augmentation du nombre d'incidents de sécurité à traiter, elle constitue une aide plus qu'appréciable pour les équipes en place.

ALAIN CLAPAUD

Dominique Reuillon,
directeur de Q1C1
et DSI du groupe Arche

« Dans le labyrinthe fragmenté des SOC modernes, l'IA n'est pas seulement une boussole, mais le fil d'Ariane qui unifie les outils disparates, contextualise l'information et transforme la surcharge en une défense intelligente et proactive. »

31 000
assets sous surveillance

572
incidents de sécurité détectés par mois

60
incidents critiques par semaine

L'ENTREPRISE

Activité
Immobilier

Effectif
23 000 collaborateurs

CA
1 Md€