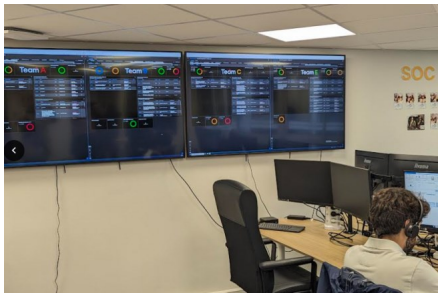
Nomios accélère dans le SOC

Dominique Filippone, publié le 03 Octobre 2024

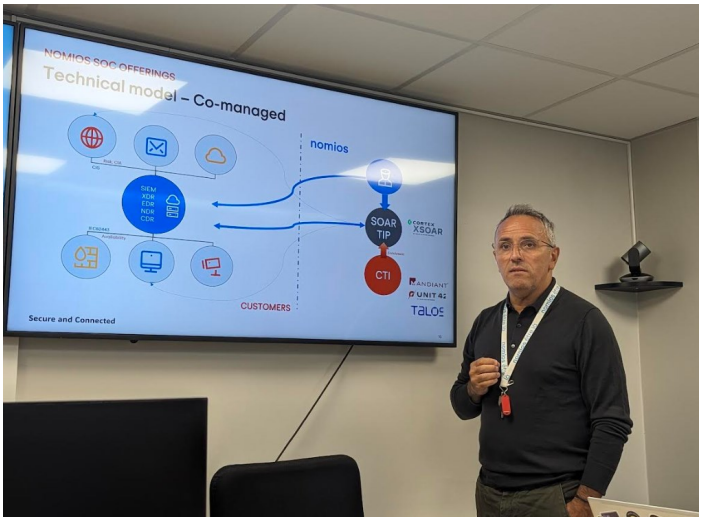
La société de services et d'intégration Nomios créée en 2004 a lancé son activité de centre de sécurité opérationnel il y a 3 ans. Elle commence à trouver sa vitesse de croisière avec une quarantaine de clients de tous horizons.



Le siège du SOC de Nomios est localisé à Boulogne-Billancourt mais ses infrastructures sont hébergées dans deux datacenters Equinix. (crédit : D.F.)

Les sociétés de services qui ont créé ou fait grossir leur activité cybersécurité se sont multipliées ces dernières années, principalement par le biais de rachats (Hub One avec Sysdream, Groupe CS avec Novidy's...). Celles qui ont lancé leur propre SOC sont moins courantes, Cheops Technology s'est par exemple positionné sur ce créneau via le rachat de la société suisse DFI Service. De son côté, l'intégrateur francilien Nomios créé il y a une vingtaine d'années, a récemment monté d'un cran son activité liée à la cybersécurité industrielle en montant une équipe dédiée pilotée par Emmanuel Le Bohec, précédemment directeur France de Claroty (spécialisé dans la sécurité de l'OT). Mais bien avant, il y a 3 ans, la PME (qui a réalisé en 2023 435 M€ de chiffre d'affaires), avait décidé de sortir de terre un centre de sécurité opérationnelle (SOC) qui a aujourd'hui bien grandi.

Cette activité constitue désormais un pilier du groupe même si le pari était loin d'être gagné d'avance. "Se lancer sur ce marché présentait un véritable risque", nous a expliqué Luis Delabarre, directeur de l'activité SOC de Nomios à l'occasion d'un point presse. "De nombreux clients se plaignaient de leur SOC externalisé et nous avons décidé de nous lancer quand nous avons trouvé que les outils de sécurité sur lesquels s'appuyer étaient arrivés suffisamment à maturité et que nous étions en mesure de répondre à la fois à des engagements de résultats que de moyens".



Pour Luis Delabarre, directeur de l'activité SOC de Nomios, la caractéristique de co-gestion entre la SSII et le client final constitue un avantage clé pour ce dernier. (crédit : D.F.)

La carte de la proximité clients

Aujourd'hui, le SOC de Nomios est utilisé par une quarantaine de clients, avec des équipes réparties dans 6 pays. Pas question cependant qu'une équipe localisée en Pologne réponde à une entreprise ayant été prévenu d'un incident de sécurité en France. "Chaque pays à sa culture et nous avons voulu être proche de nos clients sur ce point", explique Luis Delabarre. En termes d'organisation, la société a choisi de ne pas se doter d'un pôle d'analystes de niveau 1 mais réaliser le triage des remontées d'alertes avec de l'automatisation et concentrer ses ressources humaines sur les niveaux à plus fort valeur ajoutée, à savoir les niveaux 2 et 3. "Chaque client a une équipe dédiée composée d'un référent de relation client, de deux analystes référents techniques de niveau 2 et 3", indique le dirigeant. "Chaque analyste connait son client par son nom et son prénom et connait les enjeux de l'entreprise". Le siège du SOC de Nomios est localisé

à Boulogne-Billancourt (92) mais ses datacenters (ISO 27001) sont hébergés et redondés chez Equinix.

Outre le SOC (orchestration, automatisation et réponse aux incidents de sécurité aka SOAR, audit de sécurité, contrôles de sécurité, gestion des vulnérabilités...), Nomios couple également son service avec du CSIRT (pen test, investigation, réponse à incidents...), et du CERT (analyse proactive et découverte avancée des menaces, threat intelligence, partage de connaissances sur les vulnérabilités...). L'une des caractéristiques du SOC que Nomios n'hésite pas à présenter comme un véritable différenciant par rapport à d'autres est l'aspect de co-management avec ses clients. "Les clients gèrent comme ils veulent leur environnement de sécurité (SIEM, XDR, EDR, NDR et CDR) et nous nous occupons de tout le traitement des alertes et s'ils décident d'arrêter leur contrat nous leur restituons toutes les analyses et remontées de logs", indique Luis Delabarre. "Contrairement à d'autres, la réversibilité est totale."

Le réseau, nerf de la cyber-surveillance

La société met en avant son expertise sur quelques solutions sans chercher l'exhaustivité de la couverture incluant par exemple Stormshield, Tehtris, Wallix, Sekoia, Seclab, Fortinet, Pal Alto Networks et IBM QRadar vendu à ce dernier...) avec en spectre d'analyse et de vigilance principalement orienté sur le réseau. Pour le groupe, les risques ne sont en effet pas tant sur les postes et les serveurs car les cyberattaquants peuvent facilement cacher leurs traces alors qu'ils laissent une empreinte beaucoup plus visible sur le réseau, ne serait-ce que pour communiquer avec un serveur de contrôle de commande distant. "La tendance n'est pas à l'empilement des solutions de sécurité mais à une console unifiée", insiste Luis Delabarre.


Article rédigé par
Dominique Filippone
Chef des actualités LMI