IT for BUSINESS

COUNTRY:France
PAGE(S) :32-33
SURFACE :165 %
FREQUENCY :Monthly

CIRCULATION :20600
AVE :35,48 K€
AUTHOR :Alain Clapaud Alai…

► 1 September 2025 - N°2308

Page Source

Le GHT de Vaucluse teste un NDR avec succès

Établissement support du Groupement Hospitalier de Territoire (GHT) de Vaucluse, le centre hospitalier d'Avignon a fait le choix de la solution de Network Detection and Response du français Gatewatcher afin de compléter son EDR. Une initiative qu'il espère diffuser dans les autres établissements du groupement.

De par leur informatique extrêmement hétérogène et parfois insuffisamment sécurisée, les hôpitaux font souvent la une des médias, victimes des campagnes de phishing ou des malwares lancés par les groupes d'attaquants. La sécurité des endpoints (postes clients et serveurs) est donc primordiale, ainsi que celle des réseaux.

Le centre hospitalier d'Avignon joue le rôle d'établissement support du Groupement Hospitalier de Territoire (GHT) de Vaucluse. Il a une mission de support et de conseil à mener auprès des dix autres établissements du GHT, mais chacun d'entre eux reste autonome sur son parc applicatif endpoints et ses serveurs. *«Nous sommes engagés dans une stratégie de convergence de ces SI, notamment en termes d'applications, et c'est ce que nous avons réalisé avec un dossier patient informatisé unique sur l'ensemble des établissements*, explique Franck Baibourdian, RSSI du GHT de Vaucluse. *Nous poursuivons nos travaux, notamment dans le cadre du programme CARE, avec une consolidation de nos annuaires Active Directory.»*

Le GHT compte environ 8000 endpoints sécurisés via un EDR. Ses établissements sont interconnectés grâce à un réseau MPLS privé, un réseau qui pourrait être mis à profit par un attaquant pour infecter d'autres établissements s'il parvenait à trouver la faille. D'où l'idée de placer l'ensemble des réseaux sous surveillance.

Un NDR pour compléter les EDR en place

Recruté début 2023, le RSSI peut s'appuyer sur un réseau de correspondants RSI dans chaque établissement. Ces derniers sont les seuls à avoir la maîtrise de leur SI. *«Je m'attache à les aider dans leur plan d'action, avec notamment des audits de sécurité actualisés deux fois par an sur chacun des sites»*, explique Franck Baibourdian, qui pousse aussi en faveur de solutions de sécurité communes pour l'ensemble des établissements, en réalisant des PoC et surtout en essayant de trouver des budgets et des subventions pour acquérir ces solutions. C'est dans ce cadre que le RSSI s'est intéressé aux solutions de NDR (Network Detection and Response). *«Lorsque je suis arrivé, on parlait beaucoup des solutions EDR en tant que dernière barrière pour le système d'information avant l'utilisateur, mais ce n'est plus suffisant : il y a de plus en plus de solutions de contournement de ces solutions d'EDR.»* Le RSSI considère qu'il est désormais indispensable de compléter ces solutions focalisées sur les endpoints par un dispositif capable d'analyser toutes les communications.

Après avoir consulté plusieurs fournisseurs, son choix se porte sur l'offre de l'éditeur français Gatewatcher. *«La souveraineté est une exigence de plus en plus requise, mais au-delà de ce point, j'ai apprécié l'ergonomie de la solution et la qualité des détections. J'estime qu'il est intéressant de disposer d'une interface avec une vision macro pour le RSSI et une vision plus approfondie pour les équipes opérationnelles afin qu'elles mènent des recherches forensiques sur certains incidents.»*

En outre, le NDR Gatewatcher est capable de gérer la bête noire du RSSI dans les établissements de santé, les environnements biomédicaux. *«La solution nous a permis de découvrir dans les flux réseaux tous les protocoles de santé non sécurisés, comme DICOM (Digital Imaging and Communications in Medicine), ou HL7 (Health Level 7). Gatewatcher nous a aidés à identifier tous ces protocoles dans lesquels les informations sensibles passent encore en clair.»* Car si le RSSI ne peut intervenir sur les applications ou les équipements qui communiquent avec ces protocoles, il doit restreindre ces accès et confiner au maximum ces communications non chiffrées pour éviter tout risque d'écoutes et de fuites de données confidentielles.

De même, le NDR joue un rôle précieux dans la découverte des ressources connectées au réseau : *«Comme on ne peut malheureusement pas maîtriser tous nos environnements, notamment dans les secteurs biomédicaux, Gatewatcher détecte leurs échanges et cela nous permet de bien identifier ces équipements pas toujours à jour de leurs patchs de sécurité et de trouver des solutions avant de corriger ou contourner ces*

Le NDR joue un rôle précieux dans la découverte des ressources connectées au réseau

IT for BUSINESS

COUNTRY:France
PAGE(S) :32-33
SURFACE :165 %
FREQUENCY :Monthly

CIRCULATION :20600
AVE :35,48 K€
AUTHOR :Alain Clapaud Alai…

► 1 September 2025 - N°2308

Le Centre Hospitalier d'Avignon intervient comme établissement support du GHT de Vaucluse. À ce titre, il mène les PoC des solutions cyber déployées ensuite dans les dix autres établissements, qui restent néanmoins indépendants dans la gestion de leur informatique et leurs choix.

vulnérabilités en isolant les équipements en question dans des bulles de sécurité.» De même, la détection fait ressortir certains usages de type shadow IT, avec des équipements qui n'avaient pas été inventoriés car ils sortent du périmètre de la DSI. C'est le cas d'équipements biomédicaux, mais aussi des ascenseurs ou de certains équipements mis en œuvre par les services généraux... Gatewatcher a ainsi remonté une alerte quand un salarié a branché une clé USB infectée sur son poste. L'EDR avait bien détecté la clé, mais pas bloqué le poste en question. C'est le NDR qui a déclenché une deuxième alarme à partir d'une communication suspecte détectée sur ce poste.

Une seule sonde Gatewatcher a suffi pour tracer l'activité de l'ensemble des réseaux du centre hospitalier, y compris des VLAN complètement isolés d'internet. Dans un premier temps, tous les réseaux ont été mis sous surveillance, mais devant l'avalanche de faux positifs générés, Franck Baibourdian est revenu à une approche plus progressive. Seuls quelques VLAN ont été configurés sur la sonde afin de faire un gros travail de tri et élargir la surveillance. Outre ce fonctionnement en local, le NDR a pu être connecté au SOC du groupement confié à un MSSP (Managed Security Service Provider) extérieur. *«Notre prestataire avait déjà en charge notre EDR et l'ajout du NDR lui permet d'avoir une contextualisation plus large des incidents de sécurité.»*

La solution a été présentée aux RSI du groupement. S'ils ont été convaincus de son intérêt, il faut encore trouver les budgets nécessaires pour étendre la couverture du NDR à ces établissements. Les équipes sont souvent très réduites. Certaines espèrent que l'établissement support assurera la maintenance de l'outil pour eux, mais là encore, le manque de moyens humains complique une approche centralisée : *«Il faut bien positionner le curseur. Notre mission est de leur apporter du support, leur simplifier au maximum les usages du numérique, mais il restera toujours une part de mises en œuvre sur chaque site, là où réside la connaissance du SI local»*, conclut le RSSI.

ALAIN CLAPAUD

Franck Baibourdian,
RSSI du GHT de Vaucluse

«Un établissement de santé gère des environnements complexes et très hétérogènes en niveau de sécurité. Le NDR nous permet aussi de nous focaliser sur tous les protocoles qui ne sont pas encore sécurisés en interne.»

8 000
endpoints sur l'ensemble du GHT

4 500
endpoints sur Avignon, dont 2 500 postes de travail

15
incidents de cybersécurité remontés par la solution traités à temps

L'ENTREPRISE

Activité
Groupement hospitalier (11 sites au total)

Effectif
8 500 collaborateurs (3 500 lits d'hospitalisation)

CA
NC