

Lettre des "Lundi de la cybersécurité" n° 93

Cyber attaque sur un Centre Hospitalier

Etude de cas et stratégie de mitigation

The poster is for an event titled "Cyber attaque sur un Centre Hospitalier" (Cyber attack on a Hospital Center) with the subtitle "Etude de cas et stratégie de mitigation" (Case study and mitigation strategy). The event is part of the "Lundi de la Cybersécurité" (Monday of Cybersecurity) series, organized by ARCSI (Association des Responsables des Centres de la Sécurité de l'Information) and Université Paris Cité. The event is scheduled for Monday, June 15, from 18h00 to 20h00. The main speaker is Thomas VADOT, RSSI of CHI de Haute Comté. Other speakers include Judith NICOGLOSSIAN (Anthropologue), Vincent TRELY (Président de l'APSSIS), and Gérard Peliks. Organizers include Pr Ahmed Mehaoua and Bêatrice Laurent. Logos for Université Paris Cité, ARCSI, and CENTRE BORELL are also present.

Une soutenance de thèse professionnelle d'un MBA qui allait un mois plus tard subir, hélas, une application pratique

Thomas a vécu, en octobre 2025, une expérience très particulière, mais qui hélas peut arriver à d'autres employés d'un centre hospitalier. Je connais bien Thomas qui a été un de mes élèves du MBA Cybersécurité de De Vinci Executive Education, à Nanterre, promo 2024-2025. Il a écrit sa thèse professionnelle, qui terminait son MBA sur le sujet : « Impact des cyberattaques sur la continuité des soins dans les hôpitaux publics français : Études de cas et stratégies de mitigation » qu'il a soutenue en septembre 2025. 170 pages de théorie sur les cyberattaques et leur remédiation.

Comme directeur pédagogique de sa thèse professionnelle, je lui avais mis une très bonne note. Mais sa théorie allait dès le mois suivant, hélas, trouver une application très pratique. Tôt dans la nuit, le dimanche 19 octobre, le Centre Hospitalier de Pontarlier, pour lequel il est responsable de la cybersécurité, subissait une violente cyberattaque, attribuée à une mafia russe. Fichiers chiffrés, plus de SI, plus de téléphonie, demande de rançon, Retour au papier crayon !

Des experts, cyber-pompiers de l'ANSSI sont venus au secours de son hôpital. Je vous laisse imaginer ce que Thomas a vécu !

Enfin, le plan de continuité et le plan de reprise d'activité lui ont rendu son sourire.

Je donne la plume à Thomas VADOT



Le 15 juin, je proposerai un retour d'expérience immersif autour d'une cyberattaque ayant touché un établissement de santé. L'intervention sera construite comme une narration "heure par heure" de la gestion de crise : découverte de l'incident, sidération initiale, organisation de la réponse, fonctionnement en mode dégradé, continuité des soins, communication, reconstruction et enseignements tirés de l'événement.



L'objectif sera d'aller au-delà de l'approche purement technique pour montrer ce que représente concrètement une cyberattaque dans le quotidien d'un hôpital : la pression sur les équipes, les arbitrages permanents, les difficultés de coordination, mais aussi les capacités d'adaptation et de résilience des professionnels de santé et des équipes techniques.

Cette intervention sera enrichie par le regard de **Judith Nicogossian**, docteure en anthropologie, spécialisée dans les environnements de santé et les situations complexes. Elle maîtrise la gestion de crise dans une dimension humaine et psychologique, et de la gestion du stress qui l'accompagne. Elle est venue nous accompagner directement sur le terrain, au plus près des métiers et des équipes, afin d'observer et de comprendre concrètement les mécanismes humains et organisationnels mobilisés durant la gestion de crise.

La complémentarité de nos approches opérationnelle et organisationnelle pour ma part, anthropologique, et centrée sur les dynamiques humaines pour elle, permettra d'offrir une lecture à la fois concrète, immersive et approfondie de ce type d'événement.

Qui est Thomas VADOT ?



Thomas VADOT évolue depuis plus de 25 ans dans le monde de la santé, où il a occupé différentes fonctions liées aux systèmes d'information et à la conduite de projets, notamment comme chef de projet puis RSI adjoint.

Depuis maintenant 2 ans, il exerce les fonctions de RSSI sur trois établissements : le CHI de Haute-Comté, l'hôpital Paul Nappes de Morteau et l'hôpital Saint-Louis d'Ornans.

Ces expériences lui ont permis d'accompagner les établissements de santé sur des problématiques très concrètes de transformation numérique, de sécurité des systèmes d'information, de gestion des risques et de continuité d'activité dans des environnements particulièrement contraints et sensibles.

En parallèle de ces responsabilités opérationnelles, il a repris un parcours académique en intégrant le MBA co-dirigé par Gérard Peliks au sein de De Vinci Executive Education. Il y a soutenu une thèse professionnelle consacrée aux enjeux de cybersécurité dans les établissements de santé, avec une approche centrée sur la résilience organisationnelle, les facteurs humains et la gestion de crise en contexte hospitalier.

Qui est Judith NICOGOSSIAN ?

Les travaux de Judith Nicogossian portent notamment sur les interactions humaines, les mécanismes de décision et la relation entre les individus, les organisations et les technologies.

Son accompagnement a permis à l'équipe de réaction à la cyberattaque d'apporter une lecture complémentaire particulièrement intéressante sur le fonctionnement des cellules de crise, les dynamiques collectives, les prises de décision en situation dégradée et les capacités d'adaptation des organisations hospitalières confrontées à une cyberattaque.



Demande d'inscription au lundi 15 juin, par visio-conférence à partir de 18 h 00.



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique (surtout celui-là, assistez et vous verrez pourquoi 😊). Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien pour entrer dans la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à **Béatrice Laurent** co-organisatrice de nos évènements :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@noos.fr).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 15 juin dès 18 h 00 ou mieux, un peu avant**. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00** pour des conversations informelles entre intervenants et participants. Ce sont toujours d'agréables échanges qui se font avant 18 h 00.

Quelques minutes avec une association : l'APSSIS

Association Pour la Sécurité des Systèmes d'Information de Santé



Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé des intervenants et la session questions / réponses, qui commence autour de 19 h 30, nous donnons pour une quinzaine de minutes la parole à une organisation qui opère dans l'écosystème du numérique et dans la sécurité de l'information.



Dans cette séquence des **quelques minutes avec une association**, sera présentée l'APSSIS - Association Pour la Sécurité des Systèmes d'Information de Santé - et sera animée par **Vincent TRELY**,

Vincent Trély est le **président fondateur de l'APSSIS**, une association dédiée à la **sécurité des systèmes d'information de santé**, qu'il a créée en **2010**. Il est également **conférencier, animateur et enseignant** dans le domaine de la cybersécurité appliquée à la santé.

L'APSSIS organise chaque année, au Mans, le **Congrès National de la SSI Santé**. Le **14^e Congrès aura lieu du 23 au 25 juin** : <https://apssis.com/>.

L'APSSIS organise aussi les **Rencontres SSI Santé**. Les 5^e Rencontres SSI Santé, en novembre 2025, à Paris, ont été conclues par une conférence de Judith NICOGOSSIAN sur le thème : « L'humain au cœur de la crise », et Thomas VADOT, aussi présent, nous avait raconté, en début d'après-midi, sa mésaventure, vécue au Centre Hospitalier de Pontarlier.

Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?



Prompt posé à Gemini :

Qu'est-ce que mon centre hospitalier risque en cas de cyberattaque ?

Réponse de Gemini :

Une cyberattaque contre un centre hospitalier n'est pas seulement un problème informatique ; c'est une crise de sécurité civile. En France, comme ailleurs, les risques se déclinent sur plusieurs plans critiques.

Voici les principaux impacts auxquels votre établissement pourrait être confronté :

1. Risque Vital et Continuité des Soins

C'est le risque le plus grave. Une attaque par **rançongiciel (ransomware)** paralyse l'accès aux Dossiers Patients Informatisés (DPI).

- **Retard de prise en charge** : Difficulté d'accès aux antécédents, allergies ou traitements en cours.
- **Paralysie technique** : Impossibilité d'accéder aux résultats d'imagerie (IRM, scanners) ou d'analyses biologiques.
- **Déprogrammation massive** : Les interventions chirurgicales non urgentes sont annulées, et les urgences sont détournées vers d'autres établissements, saturant le réseau régional.

2. Risque Juridique et Réglementaire

Le milieu hospitalier manipule des données dites "sensibles". En cas de fuite de données, la responsabilité de l'établissement est engagée :

- **RGPD** : Sanctions lourdes de la CNIL si des failles de sécurité majeures sont constatées ou si la notification n'est pas faite dans les 72 heures.
- **Actions de groupe** : Risque de plaintes de la part de patients ou de personnels dont les données privées (numéro de sécurité sociale, pathologies) auraient été divulguées sur le Dark Web.

- **Loi Santé** : Non-respect des obligations de sécurité pour les Établissements de Santé d'Importance Vitale (ESIV).

3. Risque Financier

Le coût d'une cyberattaque dépasse de loin la simple question de la rançon (qu'il ne faut d'ailleurs jamais payer).

- **Coûts de remédiation** : Intervention d'experts en cybersécurité, reconstruction complète du système d'information.
- **Perte d'activité** : Baisse drastique des recettes liée à la réduction de l'activité médicale pendant la crise (parfois plusieurs mois pour un retour à la normale).
- **Surcoût RH** : Paiement d'heures supplémentaires pour le personnel soignant et administratif qui doit repasser au "tout papier".

4. Risque de Réputation et de Confiance

Un hôpital repose sur le contrat de confiance avec ses usagers.

- **Fuite de données médicales** : La divulgation de diagnostics ou de données d'identité peut nuire durablement à l'image de l'institution.
- **Démotivation du personnel** : Travailler en mode dégradé (papier/crayon) pendant des semaines est une source d'épuisement professionnel majeur.

À savoir : En France, l'**ANSSI** (Agence nationale de la sécurité des systèmes d'information) et les **ARS** accompagnent les hôpitaux via des programmes comme *CaRE* pour renforcer la résilience face à ces menaces croissantes.

Nous écouterons ce que **Thomas Vadot** et **Judith Nicogossian** en pensent.

Inscrivez-vous (mail à beatricelaurent.cde@gmail.com) ou cliquez ici :

JE M'INSCRIS

Gérard

