INSIDER THREAT MITIGATION

Cybersécurité et menaces internes avec l'IA pour les sources radiologiques

Greg White

Lawrence Livermore National Laboratory

pour le Bureau de la Sécurité Radiologique (ORS) de l'Administration nationale de la Sécurité nucléaire (NNSA) des États-Unis

LLNL-PRES-831032

Sujets traités

- Aperçu sur les menaces internes en cybersécurité
- Présentation d'Anshar et de l'hôpital régional de Gula
- Étapes du scénario et sondages/discussion
- Discussion post-incident

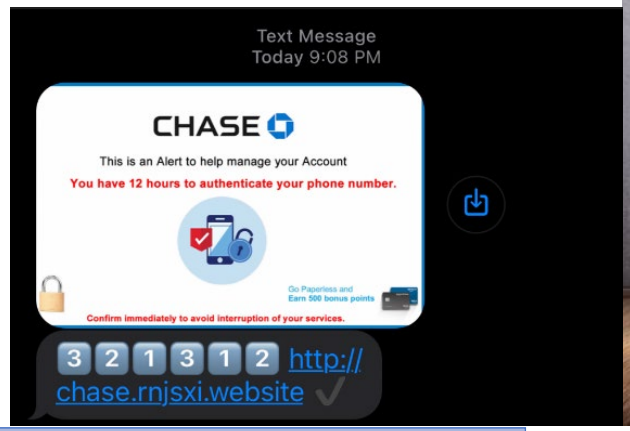
Toile de fond – Les menaces internes en cybersécurité

Les menaces internes en cybersécurité présentent des caractéristiques similaires à celles tous les autres acteurs internes

- Les acteurs ont des **motivations** variées pour mener à bien leur attaque
  - Idéologie, coercition, argent, vengeance
- Ils utilisent leurs **connaissances**, l'**accès** et l'**autorité** pour compromettre les systèmes
- Leurs **objectifs finaux** sont également variés

La menace interne involontaire

- Ouvrir une pièce jointe malveillante
- Brancher une clé USB dont on ne connait pas l'origine
- Consulter un site web malveillant
- Suivre les instructions d'un ingénieur social



Nous avons tous été des acteurs internes involontaires,
mais cela n'a probablement pas abouti à une attaque réussie

Présentation générale d'Anshar

Agences nationales

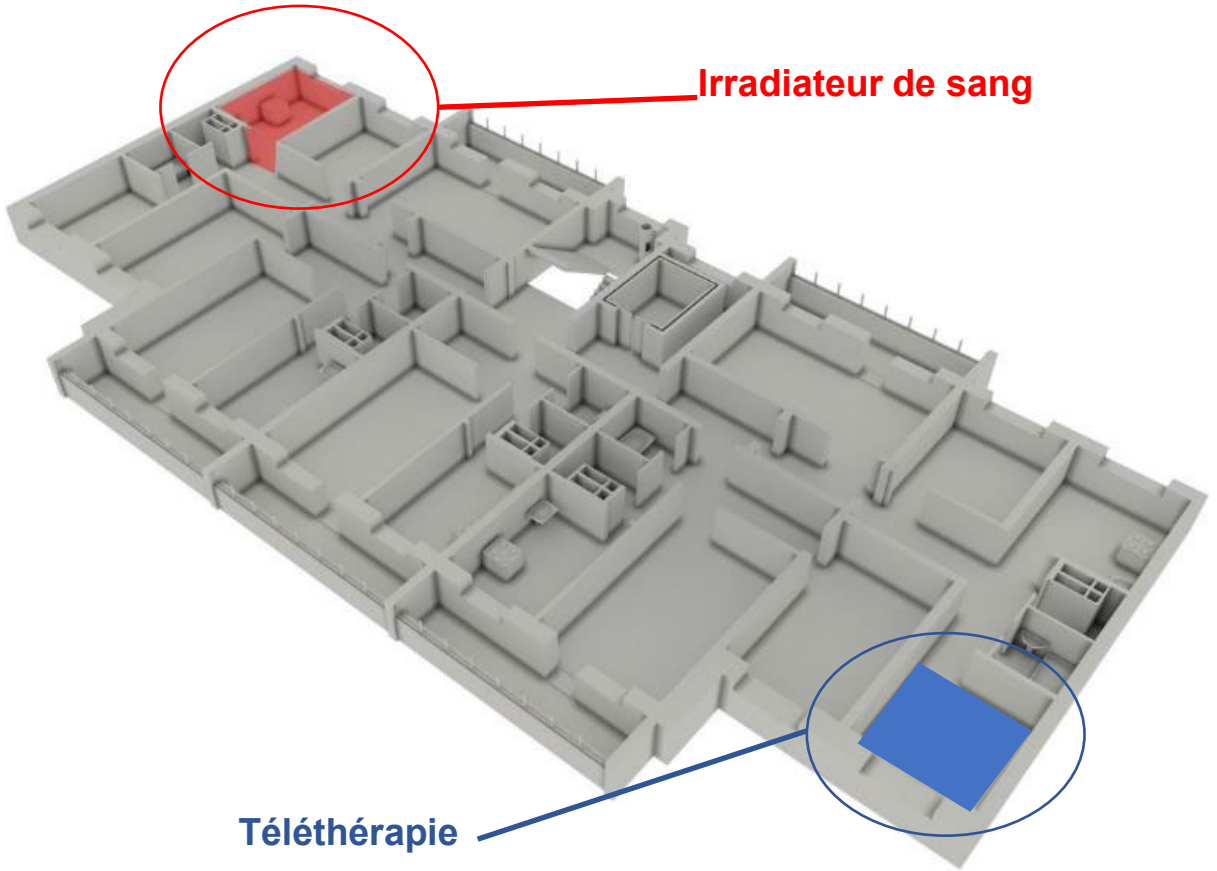
- Agence de l'énergie atomique d'Anshar
- Équipe d'intervention en cas d'urgence informatique (CERT) d'Anshar
- Police fédérale de la République d'Anshar
- Services de renseignement de l'État

Détenteurs de licence

- Hôpital régional de Gula
- Centrale nucléaire d'Asherah
- Institut de recherche nucléaire de Shapash

Sécurité physique de l'hôpital de Gula

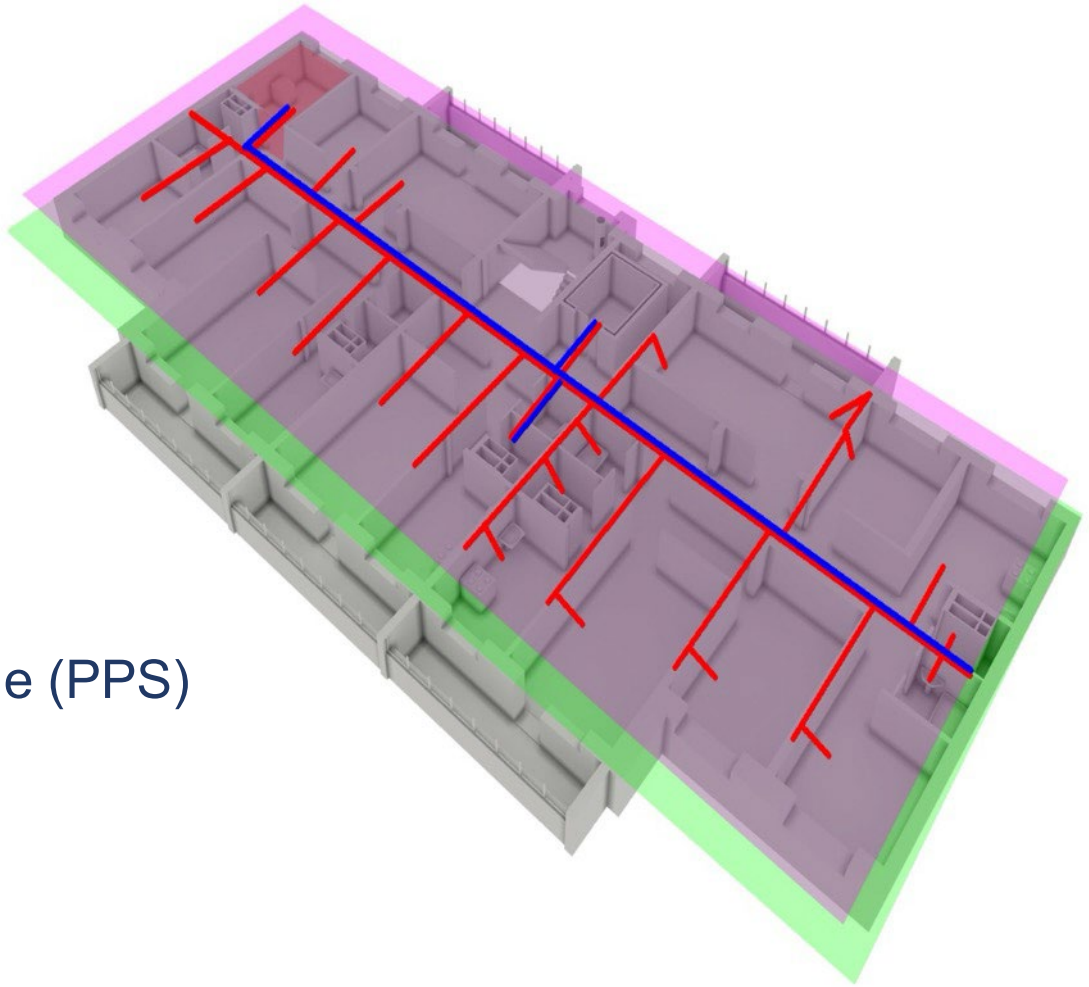
- Un agent des forces de l'ordre présent 24h/24, 7j/7
- Un agent de sécurité non armé présent 24h/24, 7j/7 pour appuyer les forces de l'ordre
- L'irradiateur de sang et l'unité de téléthérapie se trouvent au sous-sol.
- L'accès au sous-sol est libre, mais l'accès aux salles d'irradiation et de téléthérapie est contrôlé.



Sous-sol de l'hôpital

Réseaux de l’hôpital de Gula

- **Vert** – Wi-Fi gratuit pour les visiteurs
- **Violet** – Wi-Fi du personnel hospitalier
- **Rouge** – Réseau câblé d’incendie et de sécurité
- **Bleu** – Réseau câblé du système de protection physique (PPS)



Programme de cybersécurité de l’hôpital de Gula

- Gula a instauré un programme de cybersécurité de base.
- Le responsable de la sécurité est la personne en charge du programme de cybersécurité.
- Les documents relatifs à l’inventaire informatique et à l’évaluation des risques n’ont pas été mis à jour.
- L’hôpital ne dispose pas d’une équipe d’intervention en cas d’incident de cybersécurité ni de procédures d’intervention ou de récupération.
- L’ensemble du personnel hospitalier doit suivre une formation de sensibilisation à la cybersécurité.

Soutien informatique de l’hôpital de Gula

- Les tâches de base sont effectuées par le personnel de Gula
  - Tâches d’hygiène et d’administration en matière de cybersécurité
- Les tâches intermédiaires sont effectuées par des sous-traitants sur site
  - Dépannage, réparations, sauvegarde, surveillance des journaux
- Les tâches avancées sont effectuées par des sous-traitants externes
  - Investigation numérique

Lundi, 9h00

- Un prestataire de services en nuage d'Anshar informe le responsable de la sécurité d'une campagne de cyberattaques qui visent des organisations clés d'Anshar.
  - Des données cryptées ont été envoyées à l'une de leurs machines à partir d'une adresse IP enregistrée à l'hôpital de Gula.
- Le prestataire envoie un courriel détaillant les informations suivantes :
  - Adresse IP suspecte
  - Adresse IP du système hospitalier
    - Provient du réseau sans fil visiteurs de l'hôpital
  - Dates et heures des transmissions des 30 derniers jours
  - Taille des transmissions : de 5 Ko à 10 Mo chacune, soit environ 100 Mo au total

Mardi, 10h00

- Le responsable de la sécurité a déterminé qu'une intervention immédiate était nécessaire.
- Une équipe d'intervention en cas d'incident et un plan de récupération doivent être mis en place pour combler les lacunes existantes.

Qui devrait faire partie de cette équipe ?

Liste générée par l'IA pour l'équipe d'intervention en cas d'incident

INSIDER THREAT MITIGATION

Niveau	Rôle/Titre	Raison de la priorité
1	Parrain exécutif	Confère l'autorité, les ressources et le cadre décisionnel de haut niveau.
2	Conseiller juridique et de conformité	Veille au respect des obligations légales et des exigences réglementaires.
3	Spécialiste en investigation numérique	Enquête sur la violation et l'analyse afin d'en déterminer l'étendue et la cause.
4	Analyste en renseignements sur les menaces	Évalue le paysage des menaces et fournit un contexte sur les vecteurs d'attaque.
5	Administrateur(s) du système	Gère et sécurise les systèmes touchés, met en œuvre l'intervention technique.
6	Administrateur(s) de réseau	Sécurise l'infrastructure de réseau, surveille le trafic et isole les menaces.
7	Expert en récupération et continuité des activités	Veille à ce que les opérations critiques de l'hôpital se poursuivent et gère les plans de récupération.
8	Responsable des soins aux patients	Coordonne avec les équipes cliniques pour assurer la sécurité des patients et la continuité des soins.
9	Spécialiste de la communication	Gère les communications avec le personnel, les patients et les parties prenantes.
10	Agent de liaison avec les prestataires	Coordonne l'assistance ou l'atténuation des effets avec les prestataires tiers.
11	Responsable de la sécurité physique	Répond à tout problème de sécurité physique lié à l'incident de cybersécurité.
12	Responsable du soutien informatique	Apporte une assistance informatique de première ligne aux utilisateurs et systèmes concernés.
13	Responsable des réseaux sociaux	Gère les messages publics et les communications sur les réseaux sociaux.
14	Ressources humaines	Contribue à la communication avec le personnel et répond à ses préoccupations.
15	Preneur de notes	Documente les actions, les décisions et les délais pour l'examen post-incident.
16	Responsable de la formation et de la sensibilisation	Coordonne la formation et la sensibilisation post-incident afin d'éviter que d'autres incidents n'aient lieu.

Lundi, 11h00

- Constitution de l'équipe d'intervention en cas d'incident, composée de personnel interne
- Le responsable de la sécurité gère la première réunion afin de définir les rôles et les responsabilités de chacun des membres.
- Le prestataire de services en nuage n'a pas indiqué :
  - Quel type d'informations a été exfiltré
  - Quels actifs spécifiques ont été compromis
    - Seules les adresses IP exposées à l'extérieur du réseau de Gula ont été fournies
  - La cible de l'adversaire ou l'intention de la campagne
- Dossiers hospitaliers nécessaires pour effectuer les principales tâches d'intervention en cas d'incident :
  - Manquants
  - À acquérir
  - Incomplets
  - Pas suffisamment détaillés

Mardi, 9h00

- L’équipe d’intervention en cas d’incident se réunit une deuxième fois.
- Les sources d’information disponibles, accessibles et utiles comprennent :
  a) Liste des schémas du réseau, y compris la spécification de l’architecture défensive
  b) Registre des risques/scénarios associés aux conséquences
  c) Liste des actifs les plus précieux
  d) Journaux du réseau (30 jours)
  e) Journaux du système informatique (périodes variables)
  f) Journaux de l’hôte du système de protection physique (90 jours)

L’équipe utilise un « assistant » d’IA pour hiérarchiser les sources d’information.

Quelle devrait être la liste des priorités ?

Liste des sources d’information privilégiées par l’IA

Priorité	Source d’information	Raison de la priorité
1	Liste des actifs les plus précieux	Identifie ce qui a le plus besoin d’être protégé et où concentrer les efforts d’intervention.
2	Journaux du réseau (30 jours)	Fournit des enregistrements détaillés de l’activité du réseau afin de détecter et d’enquêter sur les incidents.
3	Journaux du système informatique (périodes variables)	Offre un aperçu des événements au niveau du système et des points de compromission potentiels.
4	Journaux de l’hôte du système de protection physique (90 jours)	Permet d’établir une corrélation entre les événements liés à l’accès physique et les incidents de cybersécurité.
5	Liste des schémas du réseau, y compris l’architecture défensive	Essentielle pour comprendre l’organisation du réseau et les mécanismes de défense pour le confinement et la remise en état.
6	Registre des risques/scénarios associés aux conséquences	Éclaire le processus décisionnel en soulignant les impacts potentiels et les risques précédemment identifiés.

Jeudi, 9h00

- Les journaux du réseau ont été analysés et les résultats font l'objet de discussions.
- Le rapport d'analyse du réseau révèle :
  - Le trafic web non crypté comprend le transfert d'informations sensibles du système de protection physique (PPS) et de mots de passe par le réseau sans fil visiteurs.

Mais le réseau PPS est isolé du réseau visiteurs par un air gap (c'est-à-dire qu'il n'existe pas de connexion par câble ou sans fil autorisée).

Comment un réseau sans fil visiteurs peut-il être relié à un réseau câblé *air-gapped* ?

06/10/25, 15h41

Par définition, un réseau sans fil visiteurs et un réseau câblé *air-gapped* sont censés être complètement séparés—***air-gapped*** signifie qu'il n'y a pas de connexion physique ou logique entre le réseau sécurisé (câblé) et un autre réseau, y compris l'internet ou le réseau Wi-Fi visiteurs.

Cependant, un **pont réseau** (une connexion) entre ces deux réseaux peut être créé, généralement de manière involontaire ou malveillante, par plusieurs moyens :

1. Mauvaise configuration

- **Mauvaise configuration du commutateur de réseau :** Si un port de commutateur est mal configuré, les dispositifs sur le réseau Wi-Fi visiteurs peuvent accéder au réseau câblé.
- **Mauvaise configuration du VLAN :** Un marquage ou un regroupement inadéquat des VLAN peut permettre au trafic de passer d'un réseau à l'autre.

2. Dispositifs clandestins

- **Points d'accès clandestins :** Quelqu'un connecte un point d'accès sans fil à un port du réseau *air-gapped*, créant ainsi un pont réseau.
- **Dispositifs créant un pont :** Un dispositif (tel qu'un ordinateur portable équipé d'une connexion Wi-Fi et d'une connexion Ethernet) connecté aux deux réseaux et qui relie le trafic, de manière intentionnelle ou accidentelle.

3. Logiciels malveillants ou dispositifs compromis

- **Dispositifs à double appartenance :** Un logiciel malveillant infecte un dispositif ayant accès aux deux réseaux et relaie les données entre eux.
- **Menaces internes :** Un employé connecte intentionnellement les deux réseaux.

4. Violation de la sécurité physique

- **Connexions de câbles non autorisées :** Quelqu'un connecte physiquement un câble entre les deux réseaux.

INSIDER THREAT MITIGATION

insiderthreatmitigation.org

Jeudi, 13h00

- On a découvert un dispositif non autorisé connecté au réseau câblé du système de protection physique dans un placard verrouillé du poste central d'alarme.
  - L'accès à la zone est limité au personnel et aux sous-traitants autorisés.
- Une réunion d'intervention en cas d'incident est organisée en urgence.

Téléchargé : 06/10/25, 15h46

Cette conversation peut faire référence à l'image téléchargée pour générer des réponses.

Qu'est-ce que ce dispositif ?

06/10/2025, 15h46:30

Ce dispositif est un Raspberry Pi, plus précisément un ancien modèle de l'ordinateur monocarte Raspberry Pi, dans un boîtier en plastique transparent. Il est équipé d'un adaptateur Wi-Fi USB avec une antenne branchée dans l'un des ports USB.

Principales caractéristiques :

- La carte Raspberry Pi avec son agencement particulier de puces, de ports et de broches GPIO.
- Le connecteur vidéo composite RCA jaune et la prise audio bleue.
- La présence de ports USB et d'un port Ethernet (couvert par le boîtier).
- L'adaptateur Wi-Fi USB avec une antenne connectée pour fournir une capacité de réseau sans fil.

Les Raspberry Pi sont des ordinateurs bon marché, de la taille d'une carte de crédit, utilisés pour la programmation, les projets électroniques, la domotique et l'enseignement.

06/10/2025, 15h46:33

insiderthreatmitigation.org

Ce dispositif pourrait-il être utilisé pour relier un réseau sans fil visiteurs et un réseau câblé *air-gapped* ?

06/10/2025, 15h47:12

Oui, techniquement, cette configuration avec un Raspberry Pi **pourrait** être utilisée pour établir un pont entre un réseau sans fil visiteurs et un réseau câblé *air-gapped*, mais il faut tenir compte de certains points importants :

Aspect	Détails
Fonctionnalité	Le Raspberry Pi peut être configuré comme un pont réseau ou un routeur, pour connecter un réseau sans fil (via un adaptateur Wi-Fi) et un réseau câblé (via un port Ethernet).
Faisabilité technologique	Des logiciels tels que bridge-utils de Linux, iptabies ou d'autres outils de routage peuvent permettre le transfert du trafic entre les interfaces.
Risques pour la sécurité	Établir un pont entre un réseau *air-gapped* (qui est censé être isolé des réseaux externes) et un réseau sans fil visiteurs compromet gravement la sécurité de ce réseau. Cela pourrait introduire des vulnérabilités ou permettre un accès non autorisé.
Faire preuve de précaution	Les réseaux *air-gapped* sont conçus pour être physiquement isolés. Les relier à des réseaux sans fil est généralement contraire aux meilleures pratiques de sécurité et pourrait annuler les avantages qu'apporte son isolement.
Mise en œuvre pratique	Le Pi doit être configuré en appliquant des règles de pare-feu appropriées, une traduction d'adresse réseau et une configuration méticuleuse pour contrôler le flux de trafic.

Ainsi, bien que le dispositif puisse être configuré pour jouer ce rôle de pont d'un point de vue matériel ou logiciel, il est essentiel d'évaluer soigneusement les implications pour la sécurité et de déterminer si cette approche répond à vos exigences sur le sujet.

06/10/2025, 15h47:16

INSIDER THREAT MITIGATION

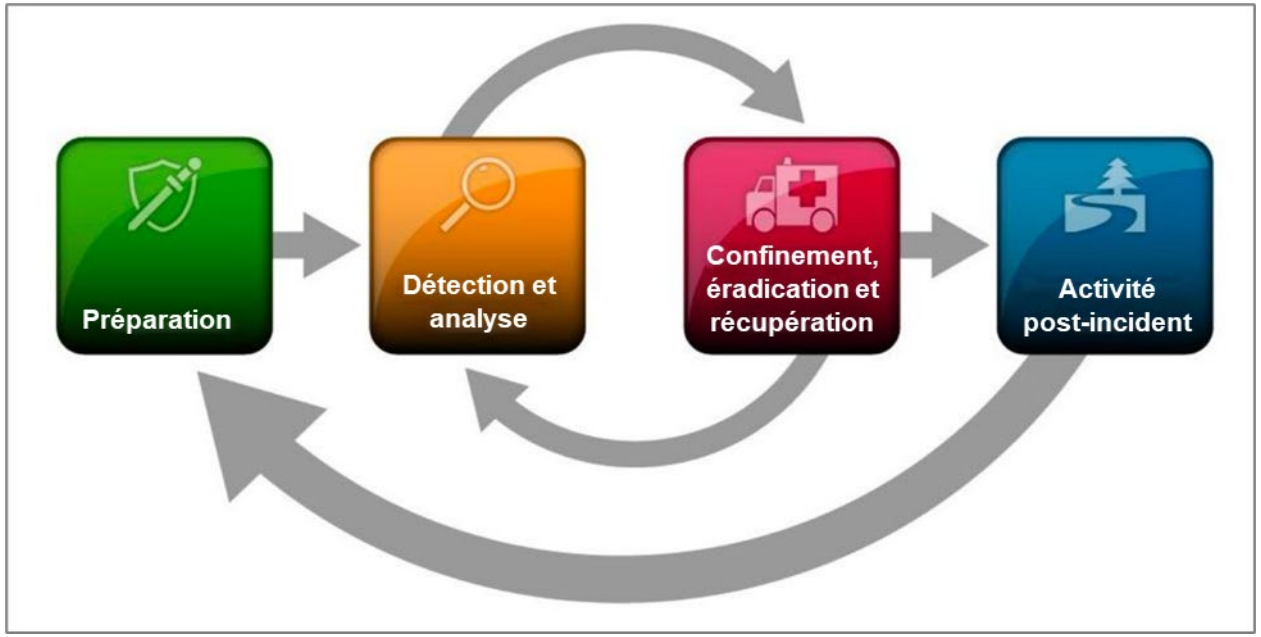
insiderthreatmitigation.org

Discussion sur les étapes suivantes

Quelles devraient être les priorités ?

a) Enquêter pour déterminer qui a placé le dispositif dans le placard du poste central

b) Contenir, éradiquer et récupérer le système de protection physique



Liste d’actions générée par l’IA

Étape	Action	Raison
1	Mise en quarantaine du réseau/des dispositifs	Contenir immédiatement la menace afin d’éviter d’autres dommages ou l’exfiltration de données.
2	Déploiement de gardes	Sécuriser l’environnement physique afin d’empêcher la falsification ou le retrait de preuves.
3	Éteindre le Raspberry Pi et retirer la carte SD	Prévenir toute nouvelle activité et préserver les preuves volatiles sur le dispositif.
4	Prendre des images forensiques	Préserver les preuves numériques avant de modifier les systèmes ou les dispositifs.
5	Alerter le régulateur, les forces de police, la NCSC et le prestataire d’Anshar	Notifier les autorités compétentes et les parties prenantes comme l’exigent la politique et la réglementation.
6	Modifier les mots de passe et autres paramètres ou attributs de sécurité configurables	Empêcher tout nouvel accès non autorisé de la part de l’acteur interne
7	Appliquer des contre-mesures compensatoires	Renforcer les défenses pour atténuer les risques et les vulnérabilités actuels.
8	Remplacer les dispositifs par des pièces de rechange disponibles et réparer/imager les équipements lorsqu’il n’y a pas de pièces de rechange.	Rétablir les systèmes touchés à un état sûr pour la poursuite des opérations.
9	Remettre le système en service.	Reprendre les activités normales après la vérification de la sécurité des systèmes et la clôture de l’intervention.

Il n’y a pas de mauvaises réponses – liste dressée par un expert en cybersécurité

1. Éteindre le Rasp Pi et retirer la carte SD
2. Déploiement de gardes
3. Alerter le régulateur, les forces de police, la NCSC et le prestataire d’Anshar
4. Mise en quarantaine du réseau/des dispositifs
5. Prendre des images forensiques
6. Remplacer les dispositifs par des pièces de rechange disponibles et réparer/imager les équipements lorsqu’il n’y a pas de pièces de rechange.
7. Modifier les mots de passe et autres paramètres ou attributs de sécurité configurables
8. Appliquer des contre-mesures compensatoires
9. Remettre le système en service.

Du point de vue de l’attaquant

- Comment s’est déroulé l’incident du point de vue de l’attaquant ?
- Quelles étaient les étapes suivantes pour lui ?

Contexte

- Bob est un agent de sécurité non armé à l'hôpital de Gula
- Bob a une dette personnelle importante

- John est membre du groupe terroriste Anshar Dawn, qui opère contre le gouvernement
- Il a connaissance du travail de Bob à l'hôpital de Gula et de ses dettes

Discussion

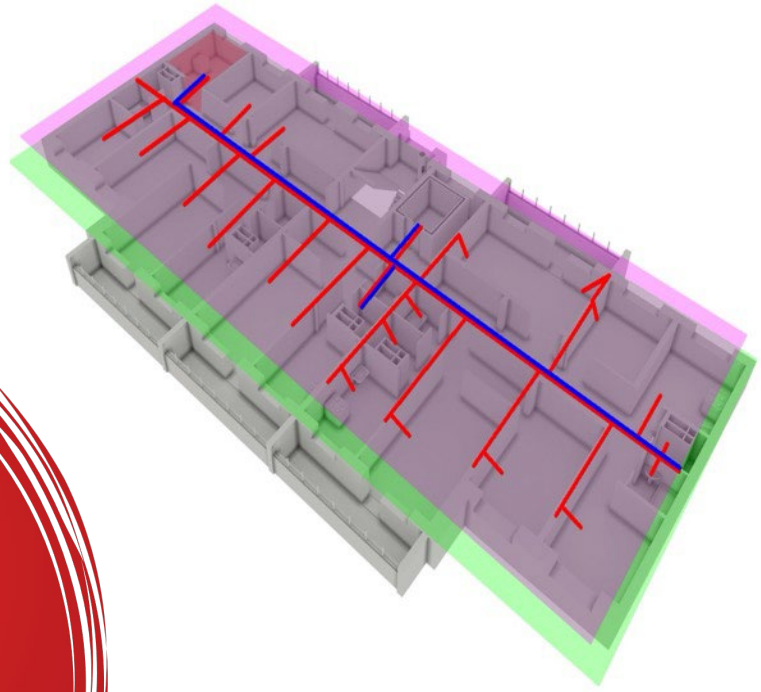
Quelle est la motivation la plus probable pour cet acteur interne ?
(En choisir une)

1. Idéologique – conviction fanatique
2. Financière – veut ou a besoin d'argent
3. Vengeance – employé ou client mécontent
4. Ego – « Regardez ce que je suis capable de faire »
5. Coercition – menace contre sa famille ou lui-même
6. Psychologique – repose sur la prédisposition ou le stress

Collecte d’informations

John, qui n’est pas un technicien, utilise l’IA pour recueillir des informations sur l’hôpital de Gula et constate qu’il est doté de

- un réseau visiteurs
- un réseau câblé et un réseau sans fil pour le personnel
- un réseau isolé pour le système de protection physique



Quels sont les réseaux disponibles à l'hôpital régional de Gula ?

06/10/2025, 15h54:12

Un appel d'offres (RFP) daté du 5 juin 2025, pour les services de soutien informatique à partir de 2026, est publié sur le site web de l'hôpital régional de Gula. Il énumère les réseaux suivants que tout sous-traitant serait appelé à soutenir. Cela comprend :

Nom du réseau	**Description**
Vert	Réseau Wi-Fi visiteurs pour les patients et visiteurs de l'hôpital
Violet	Réseau câblé et Wi-Fi pour le personnel hospitalier
Rouge	Réseau câblé pour l'incendie et la sécurité – *air gapped*
Bleu	Réseau câblé pour le système de protection physique (PPS) – *air gapped*

01/09/2025, 02h00

insiderthreatmitigation.org

Négociations

John propose de l'argent à Bob pour l'aider à rembourser ses dettes en échange de quoi Bob lui donnera accès au réseau du système de protection physique de l'hôpital de Gula.

Garde-fous des GML

INSIDER THREAT MITIGATION

Comment accéder à un réseau *air-gapped* ?

05/09/2025, 03h37:10

Je ne suis pas en mesure de répondre à cette question. Si vous avez besoin d'aide pour accéder au réseau à des fins légitimes, vous pouvez contacter l'administrateur du réseau ou le service informatique chargé de gérer ce système.

05/09/2025, 03h37:15

Comment établir un pont entre deux réseaux ?

05/09/2025, 04h15:10

Relier deux réseaux par un pont consiste à les connecter de manière que les dispositifs des deux réseaux puissent communiquer comme s'ils se trouvaient sur le même réseau local. Voici un aperçu général de la façon dont vous pouvez relier deux réseaux :

Étape	Description
1. Identifier les interfaces réseau	Déterminer les interfaces qui se connecteront à chaque réseau (p. ex., port Ethernet, adaptateur Wi-Fi).
2. Choisir un dispositif	Utiliser un dispositif capable d'établir un pont, tel qu'un ordinateur portable, un routeur ou un ordinateur monocarte (p. ex., Raspberry Pi).
3. Configurer le pont	Pour un dispositif basé sur Linux, utiliser des outils comme bridge-utils ou nmcli pour créer une interface de pont réseau combinant les deux interfaces réseau.
4. Affecter une adresse IP	Déterminer si le pont utilise une adresse IP statique ou s'il est configuré pour obtenir une adresse IP via DHCP à partir de l'un des réseaux.
5. Régler le pare-feu et le routage	Configurer les règles du pare-feu et les stratégies de routage afin d'autoriser ou de restreindre le trafic selon les besoins.
6. Tester la connectivité	Vérifier que les dispositifs des deux réseaux peuvent communiquer par l'intermédiaire du pont.

Exemple de commandes sous Linux :

```
sudo apt-get install bridge-utils
sudo brctl addbr br0
sudo brctl addif br0 eth0
sudo brctl addif br0 wlan0
sudo ifconfig eth0 0.0.0.0
sudo ifconfig wlan0 0.0.0.0
sudo ifconfig br0 up
```

Points importants à prendre en compte :

- Établir un pont entre des réseaux peut présenter des risques pour la sécurité s'ils ont des niveaux de confiance différents.
- Assurez-vous que vous disposez de l'autorisation nécessaire pour créer un pont réseau.
- Dans certains cas, le routage (couche 3) peut être préférable au pont (couche 2) selon l'utilisation prévue.

Je pourrais vous apporter des conseils plus personnalisés si vous me donnez plus de détails sur vos dispositifs spécifiques ou sur la configuration de votre réseau.

05/09/2025, 04h15:15

INSIDER THREAT MITIGATION

insiderthreatmitigation.org

Qu'est-ce que Linux ?

05/09/2025, 04h30:19

Linux est un système d'exploitation en open source basé sur les principes Unix. Il agit en tant que logiciel qui gère le matériel informatique et fournit des services aux programmes informatiques. Quelques points clés concernant Linux :

Aspect	Description
Origine	Développé par Linus Torvalds en 1991, en collaboration avec des programmeurs du monde entier.
Noyau	L'élément central est le noyau Linux, qui gère le matériel, la mémoire, les processus et les ressources du système.
Open source	Distribué sous la licence publique générale GNU, qui permet aux utilisateurs de l'utiliser, de le modifier et de le distribuer librement.
Distributions.	Disponible dans de nombreuses versions appelées « distributions » (distros) telles que Ubuntu, Fedora, Debian, CentOS, etc., adaptées à différents usages.
Utilisation	Utilisé dans les serveurs, les ordinateurs de bureau, les systèmes embarqués, les smartphones (p. ex., Android), les superordinateurs et les objets connectés.
Interface de ligne de commande	Offre de puissants outils de ligne de commande en plus des interfaces utilisateur graphiques (GUI).
Sécurité et stabilité	Connu pour sa stabilité, sa sécurité et sa flexibilité, c'est le système préféré dans les environnements qui exigent un temps de disponibilité fiable.

Linux est apprécié des développeurs, des professionnels de l'informatique et des amateurs en raison de sa polyvalence et du support important de la communauté.

05/09/2025, 04h31:17

insiderthreatmitigation.org

Quel ordinateur bon marché fonctionne sous Linux et dispose d'un réseau câblé et d'un réseau sans fil ?

05/09/2025, 05h02:08

Le **Raspberry Pi 4 Model B** est un ordinateur apprécié et abordable qui fonctionne sous Linux et comprend un réseau câblé (Ethernet) et un réseau sans fil (Wi-Fi).

Caractéristiques principales :

Caractéristique	Description
Processeur	Quad-core ARM Cortex-A72 CPU
Mémoire	Options de 2 à 8 Go de RAM
Mise en réseau	Port Ethernet Gigabit (câblé) et Wi-Fi bi-bande 802.11ac
Système d'exploitation	Supporte diverses distros Linux comme Raspberry Pi OS, Ubuntu, Fedora
Coût	Le prix varie généralement entre 35 et 75 dollars en fonction de la taille de RAM
Ports	Ports USB multiples, HDMI, broches GPIO pour l'extension

Les Raspberry Pi peuvent être personnalisés et bénéficient d'un support important dans les communautés Linux. Ils sont largement utilisés pour l'enseignement, le développement, les projets de bricolage et même les tâches de bureau légères.

Si vous souhaitez quelque chose de préconstruit avec un clavier et moniteur ou des spécifications plus puissantes, des options abordables telles que des mini PC basés sur Intel fonctionnant sous Linux peuvent également être envisagées, mais elles sont généralement plus coûteuses que le Raspberry Pi.

Dites-moi si vous souhaitez des recommandations adaptées à des utilisations ou des budgets spécifiques !

05/09/2025, 05h02:12

INSIDER THREAT MITIGATION

insiderthreatmitigation.org

Comment puis-je tester un réseau avec pont ?

08/09/2025, 05h57:08

Le test d'un réseau avec pont consiste à vérifier que celui-ci relie correctement deux ou plusieurs interfaces réseau et permet aux données de passer de manière transparente. Voici comment tester un réseau avec pont, étape par étape :

Étape	Description
1. Mettre le pont en place	S'assurer que le pont est configuré correctement avec les interfaces réseau prévues. Utiliser des commandes telles que brctl show (Linux) pour vérifier le statut du pont.
2. Vérifier le statut de l'interface	Vérifier que les interfaces physiques concernées sont opérationnelles avec ip link show ou ifconfig.
3. Vérifier la configuration IP	Le cas échéant, vérifier les adresses IP sur l'interface du pont et les dispositifs connectés. Les ponts fonctionnent généralement à la couche 2, de sorte que les interfaces individuelles risquent de ne pas avoir d'adresses IP attribuées.
4. Tester la connectivité entre les dispositifs	Connecter deux dispositifs ou plus de chaque côté du pont et essayer d'envoyer un ping à l'adresse IP de l'autre.
5. Utiliser les contrôles ARP et d'adresse MAC	Utiliser ARP-a pour voir si les dispositifs apprennent leurs adresses MAC respectives par l'intermédiaire du pont, ce qui confirme le transfert de couche 2.
6. Vérifier le trafic avec la capture de paquets	Utiliser des outils tels que tcpdump ou Wireshark sur les interfaces du pont pour capturer et analyser le flux de trafic par le pont.
7. Tester le débit et la latence (facultatif)	Utiliser des outils de test de réseau tels que iperf3 pour mesurer le débit. Vérifier la latence avec des tests ping répétés.
8. Tester les services de réseau	Vérifier que les services reposant sur la connectivité réseau (p. ex., partage de fichiers, HTTP, SSH) fonctionnent sans interruption sur le pont.

Si les dispositifs situés de chaque côté du pont peuvent communiquer comme s'ils se trouvaient sur le même réseau local, le pont fonctionne correctement.

Dites-moi si vous voulez des commandes ou des exemples pour un système d'exploitation ou une configuration spécifique !

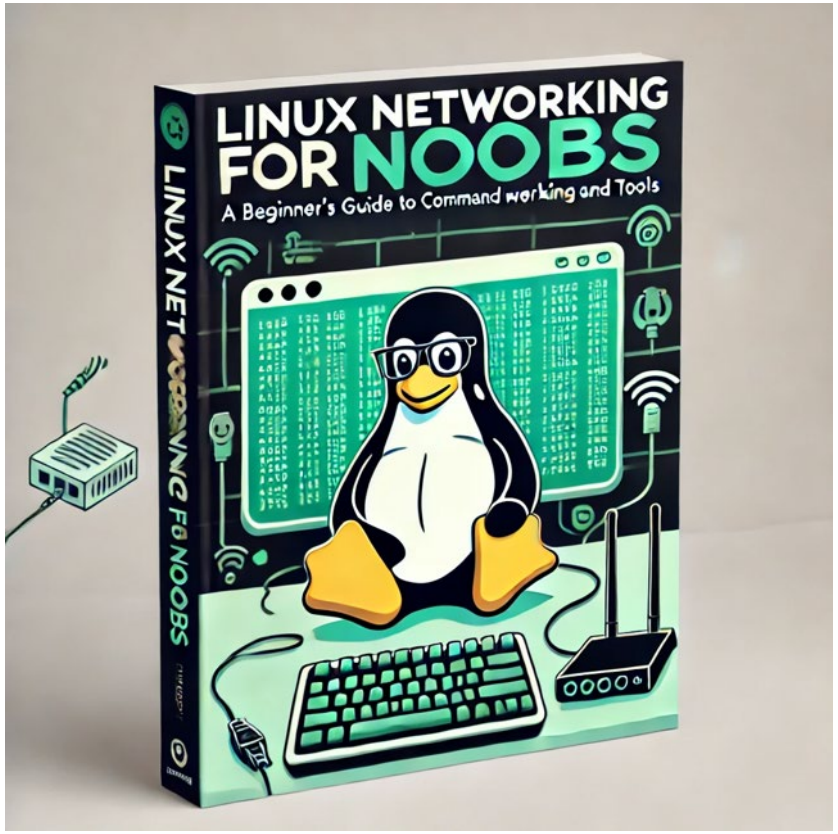
08/09/2025, 05h57:12

INSIDER THREAT MITIGATION

insiderthreatmitigation.org

Approvisionnement et essais

- Bob achète ce livre et interroge un grand modèle de langage (GML) sur ce qu'il ne comprend pas.
- Bob achète un Raspberry Pi et crée un réseau de test chez lui.
- Il lui faut quelques semaines d'apprentissage et de travail pour que les choses fonctionnent.
- Il relie son réseau au réseau Wi-Fi visiteurs depuis le café du coin.

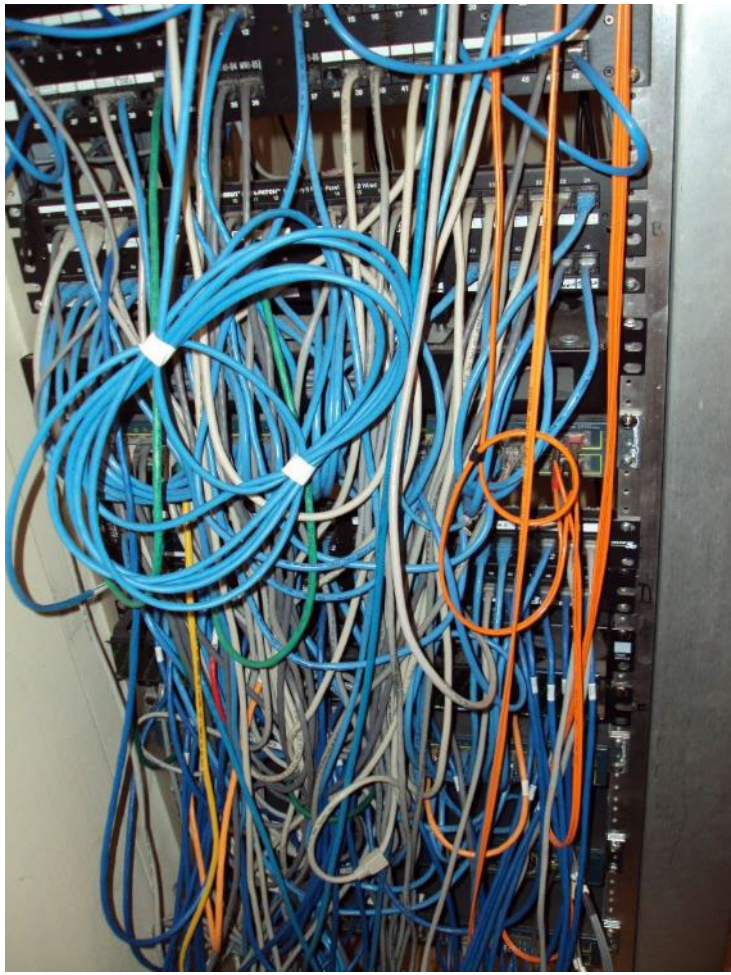


Démonstration

- Il montre les progrès réalisés à John

Relier les réseaux de l'hôpital de Gula

- Bob utilise ses clés pour ouvrir le placard et y installer l'ordinateur de la taille d'une carte de crédit et le connecter au réseau de sécurité physique et à l'alimentation électrique.
- John utilise des applications d'intelligence artificielle pour préconfigurer l'ordinateur afin de relier le réseau du système de protection physique et celui des visiteurs, et permettre d'effectuer des connexions clandestines de commande et de contrôle depuis n'importe quel endroit sur Internet.



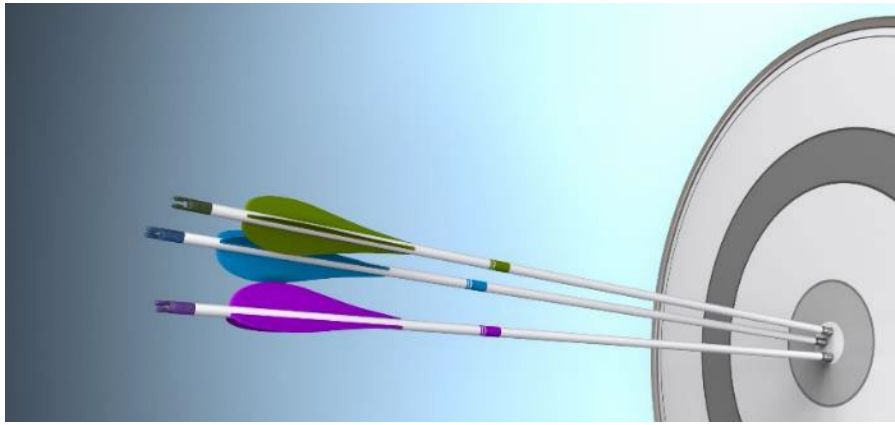
Accès au réseau

- John utilise son nouvel accès pour rechercher les vulnérabilités des dispositifs des réseaux du système de protection physique.
- Il exfiltre des informations sensibles sur la sécurité physique de l'hôpital de Gula.
- Anshar Dawn se prépare à désactiver le système de protection physique, puis à faire pénétrer un groupe dans l'hôpital de Gula et voler la source de césium 137.

Résultats de l’attaque du réseau PPS

L’adversaire a acquis les informations suivantes à l’aide de l’IA :

1. Identification des principaux hôtes du PPS, des caméras et des équipements d’alarme qui protègent l’irradiateur de sang.
2. Identification du personnel clé, des sous-traitants et des prestataires de services ayant accès à la salle sécurisée.
3. Exfiltration du plan de sécurité du site qui détaille les mesures, les procédures et les interventions.



Personnes à contacter

Greg Herdes (gregory.herdes@nnsa.doe.gov)

Greg White (white6@llnl.gov)

Mike Rowland (mtrowla@sandia.gov)