



GoldPharma

Projet d'étude du niveau de sécurité
et de sécurisation d'un système
d'information

Tony Ly Soan Massinissa Brahimi Léonard Namolaru Nabil Baltata Céline Ye

PLAN

01 Introduction

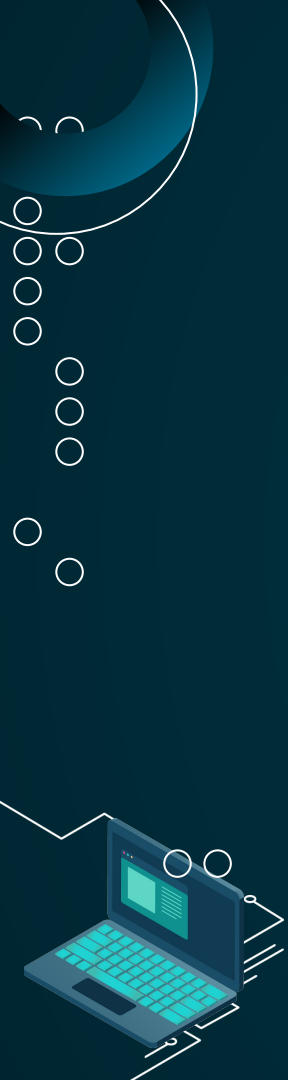
02 Synthèse des résultats

03 Synthèse de l'analyse
des risques

04 Plans d'action

05 Proposition d'une
nouvelle architecture

06 Conclusion





01

Introduction



An isometric illustration on the left side of the slide. It features a laptop with a teal screen displaying a document. A large teal shield with a checkmark is positioned in front of the laptop. Above the shield are two teal padlocks of different sizes. The background is dark teal with white geometric patterns: a grid of small circles and a larger circle with a crosshair.

PARTIES PRENANTES

A teal speech bubble icon with three horizontal lines inside, representing text or communication.

GoldPharma

La société GoldPharma a fait appel à nos services pour réaliser un audit de sécurité de son système d'information, dans le but de vérifier son immunité aux cyberattaques.

A teal shield icon with a checkmark inside, symbolizing security or approval.

AuPenBar

La société AuPenBar a mis à disposition une équipe de 5 auditeurs pour cette mission. L'audit a débuté en janvier 2025 et s'est terminé en mai 2025.

L'ÉQUIPE D'AUDIT

Massinissa Brahim

Compromission de Frontend,
Compromission de NAS, Compromission
de Gate1 & Gate2, Spider



Nabil Battata

Compromission du site web,
Compromission de Frontend,
Compromission de l'AD, Docker
Escape (Rialto)

Léonard Namolaru

Intergold, Shaggy, Rialto, Énumération AD,
Pivoting, Rédacteur principal (rapport
pédagogique), Organisation, Transfert de
compétences



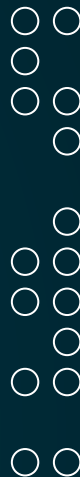
Céline Ye

Analyse de risque, Accès à Gate2,
Analyse en largeur (WSTG, BDD
Frontend), Mise en page des rapports



Tony Ly Soan

Coordinateur, Challenges des affiches, Reverse engineering
(Shaggy), Analyse en largeur (Audit de code du site web,
WSTG, BDD Frontend), Rédacteur principal

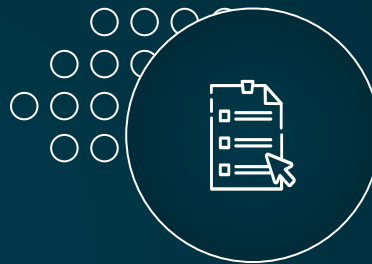


CONTEXTE ET MÉTHODOLOGIE D'AUDIT



Boîte noire

La seule information qui nous a été fournie avant le début de l'audit était l'adresse du site Web de GoldPharma



OWASP WSTG

Le site Web de GoldPharma a été analysé à l'aide de OWASP Web Security Testing Guide



02

Synthèse des résultats



LE CVSS 3.1 (COMMON VULNERABILITY SCORING SYSTEM)

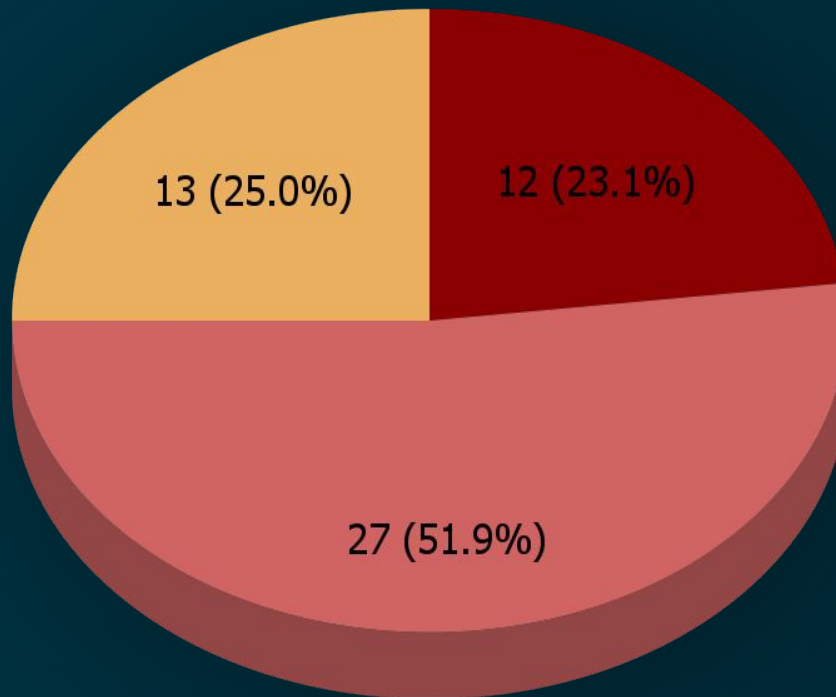
9.0 - 10.0 - Critique

7.0 - 8.9 - Haute

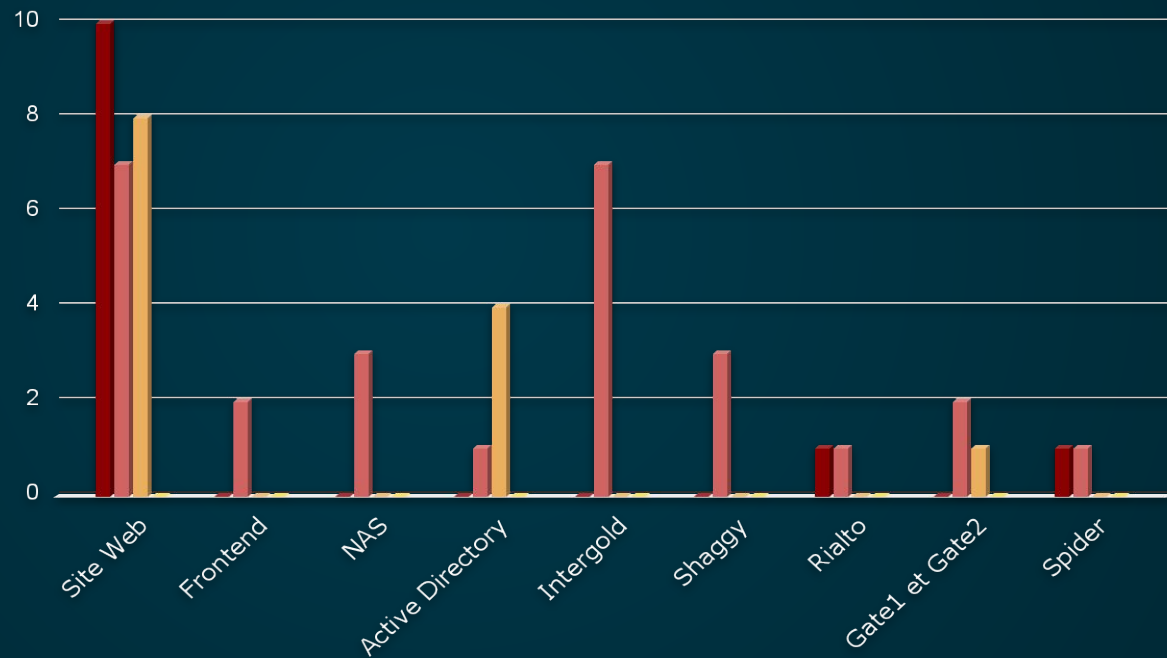
4.0 - 6.9 - Moyenne

0.1 - 3.9 - Faible

SYNTHÈSE DES VULNÉRABILITÉS GLOBALE

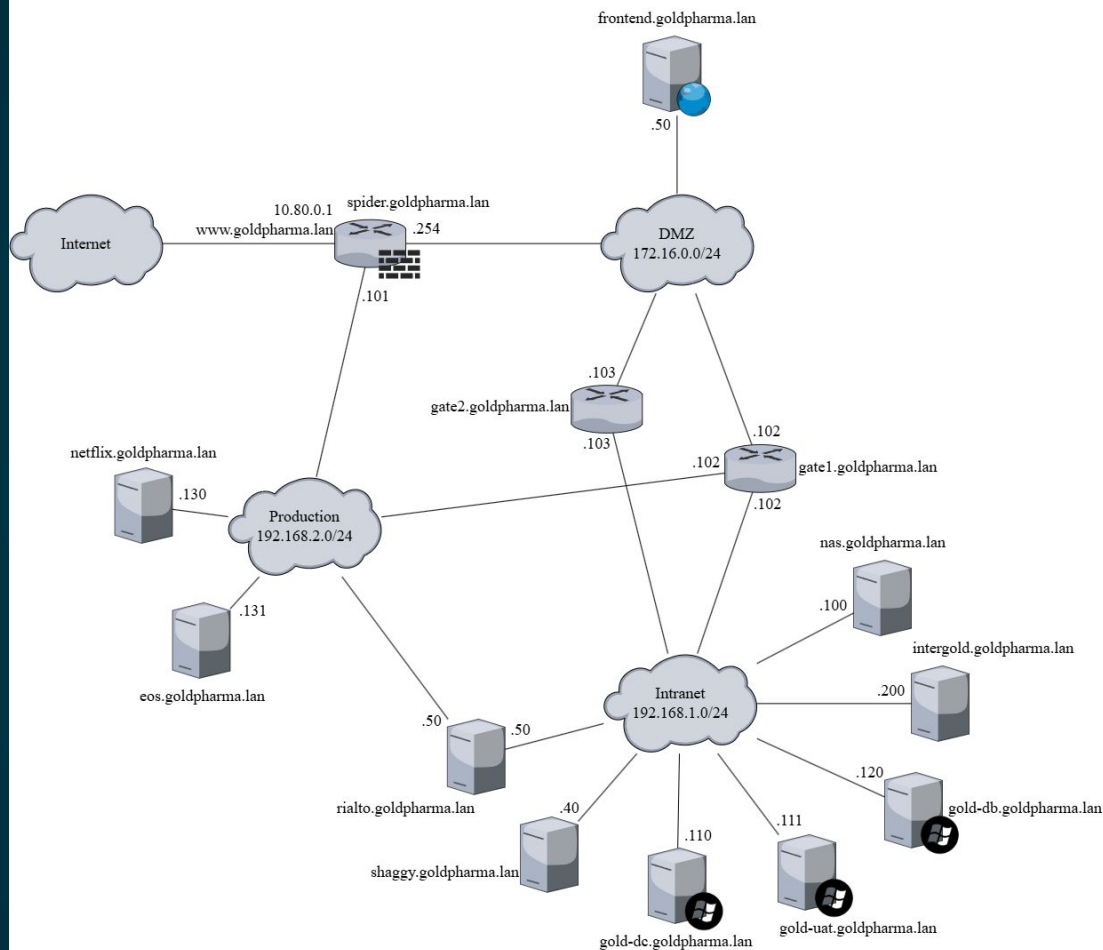


SYNTHÈSE DES VULNÉRABILITÉS PAR ACTIF



CHEMIN D'INTRUSION EXPLOITÉ

Présentation de vulnérabilités remarquables



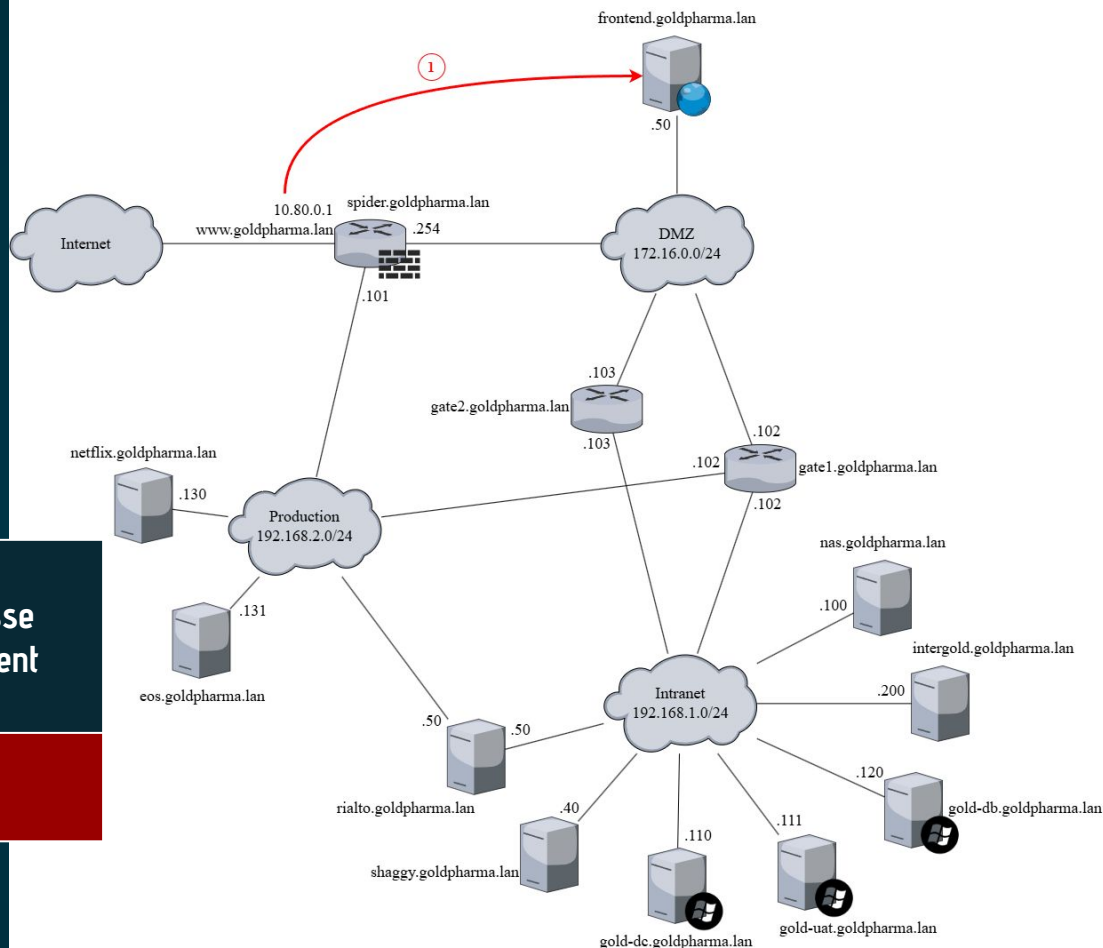
CHEMIN D'INTRUSION EXPLOITÉ

Présentation de vulnérabilités remarquables

[Web-10] Capacité à changer le mot de passe
sans avoir besoin du mot de passe précédent

Criticité

Critique



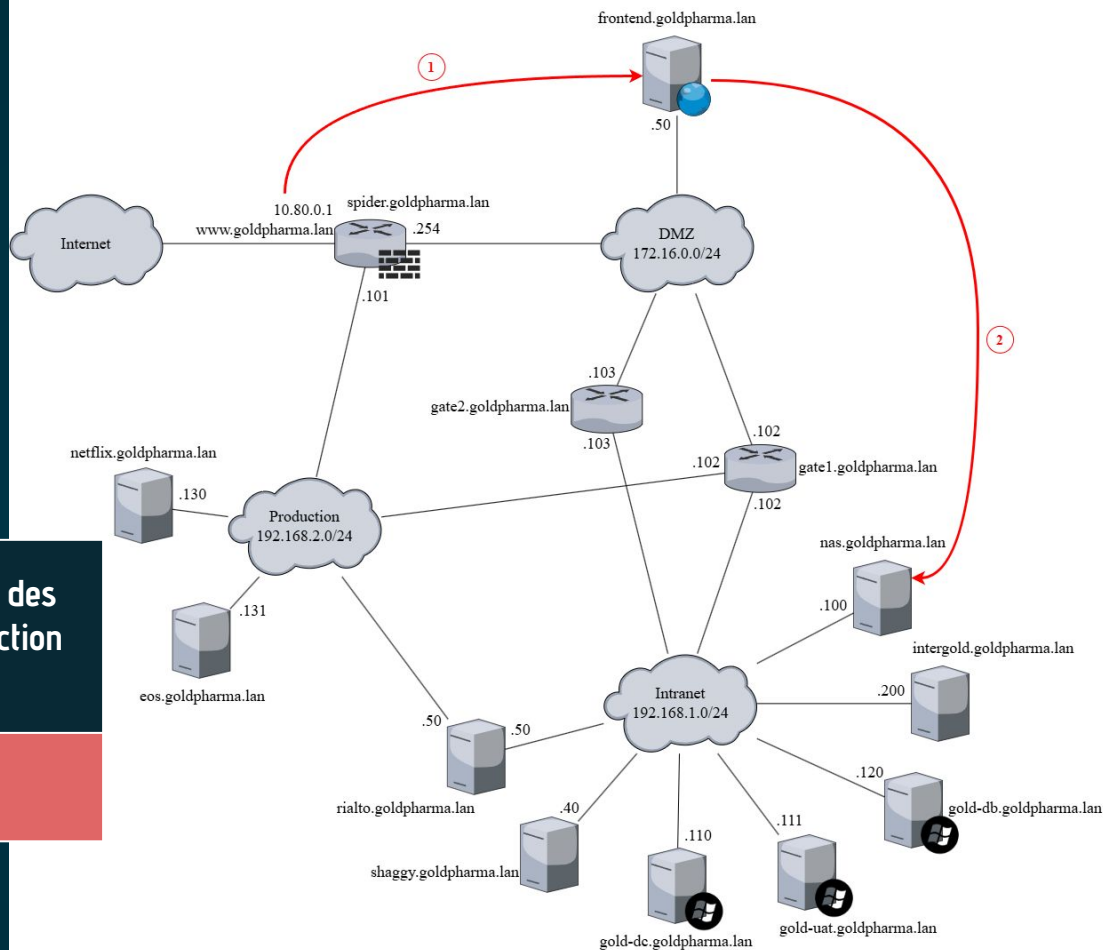
CHEMIN D'INTRUSION EXPLOITÉ

Présentation de vulnérabilités remarquables

[NAS-1] Utilisation de la commande tar avec des caractères génériques (wildcard) sans protection adéquate

Criticité

Haute



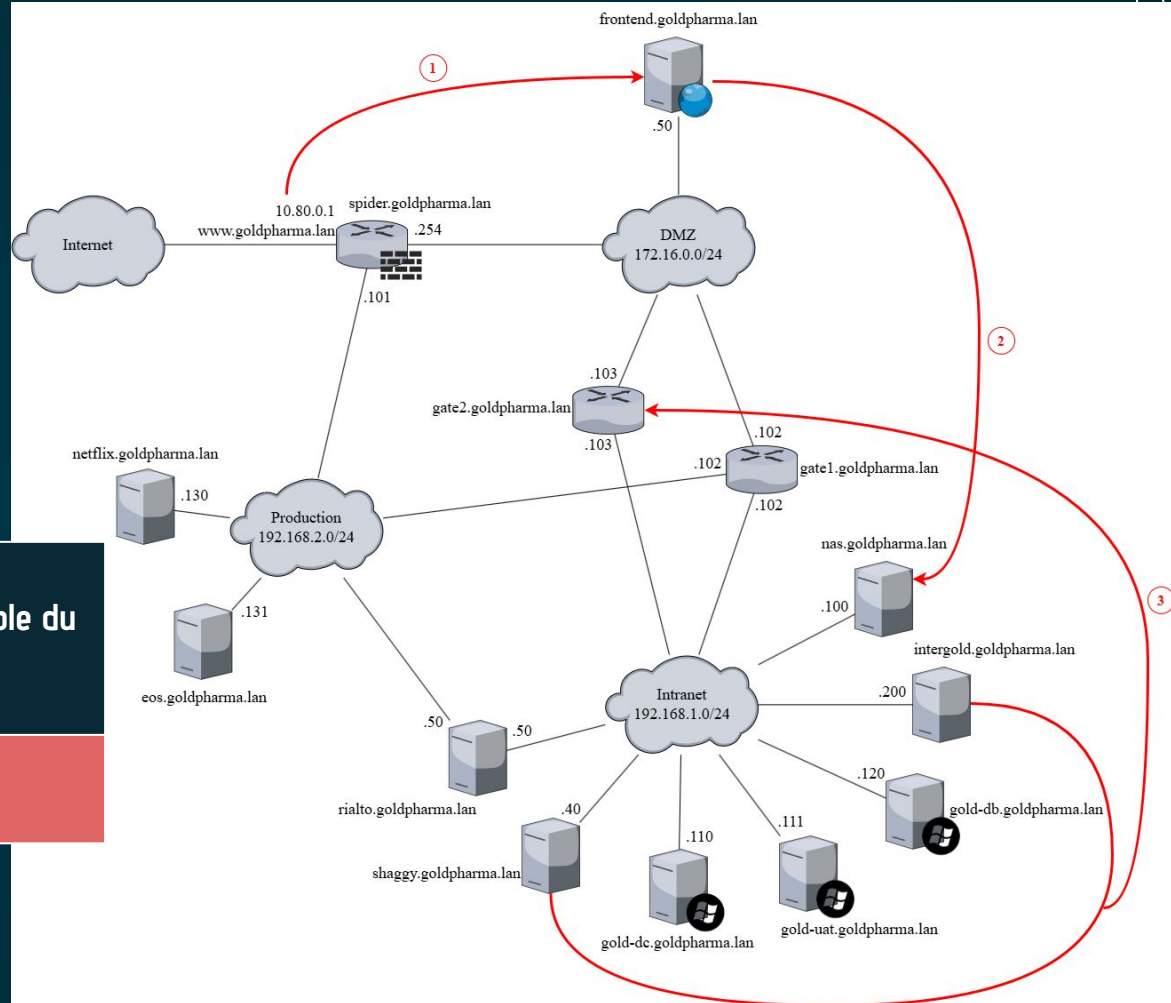
CHEMIN D'INTRUSION EXPLOITÉ

Présentation de vulnérabilités remarquables

[Intergold-1] Utilisation d'une version vulnérable du
plugin Asgaros Forum

Criticité

Haute



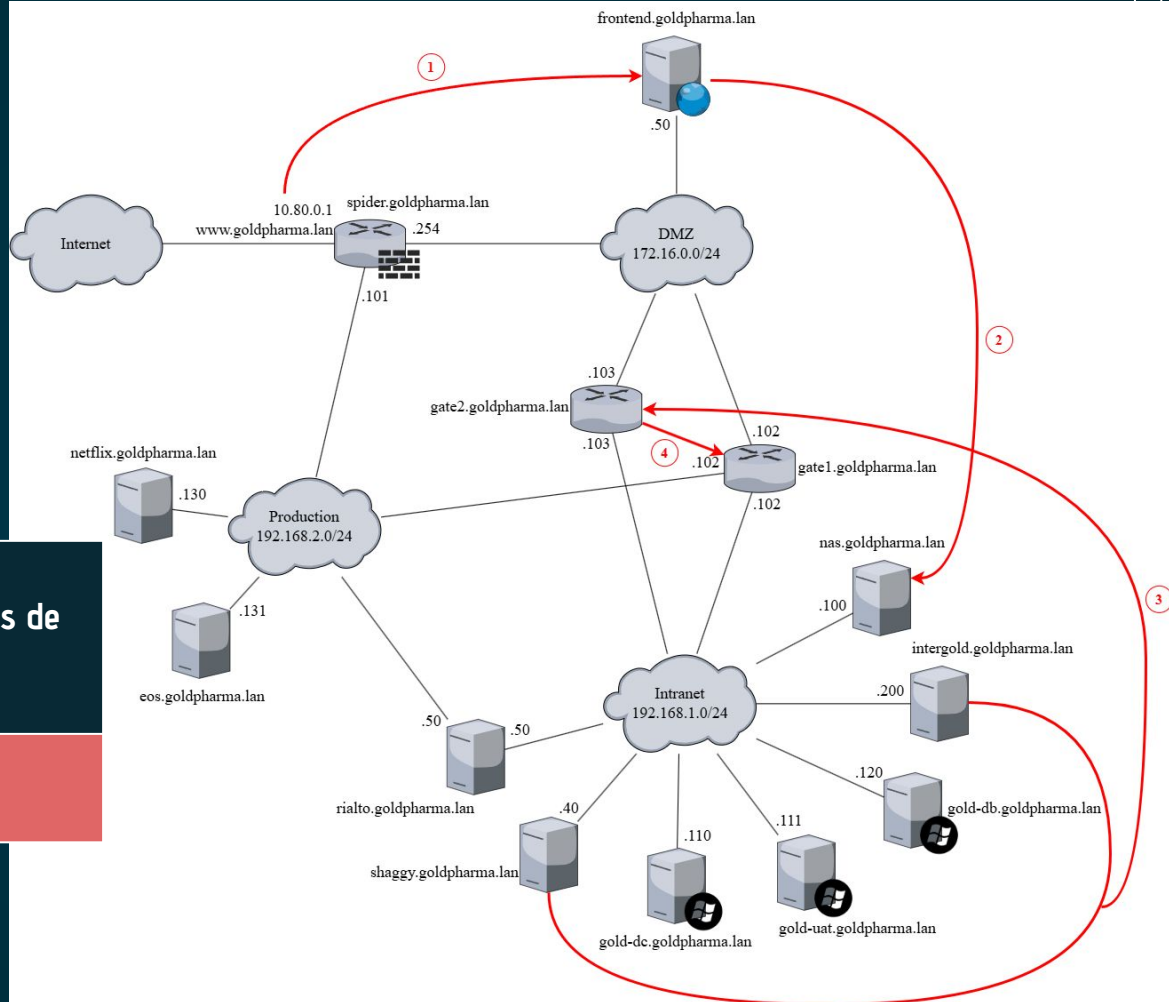
CHEMIN D'INTRUSION EXPLOITÉ

Présentation de vulnérabilités remarquables

[Gates-1] Réutilisation systématique des mots de passe

Criticité

Haute



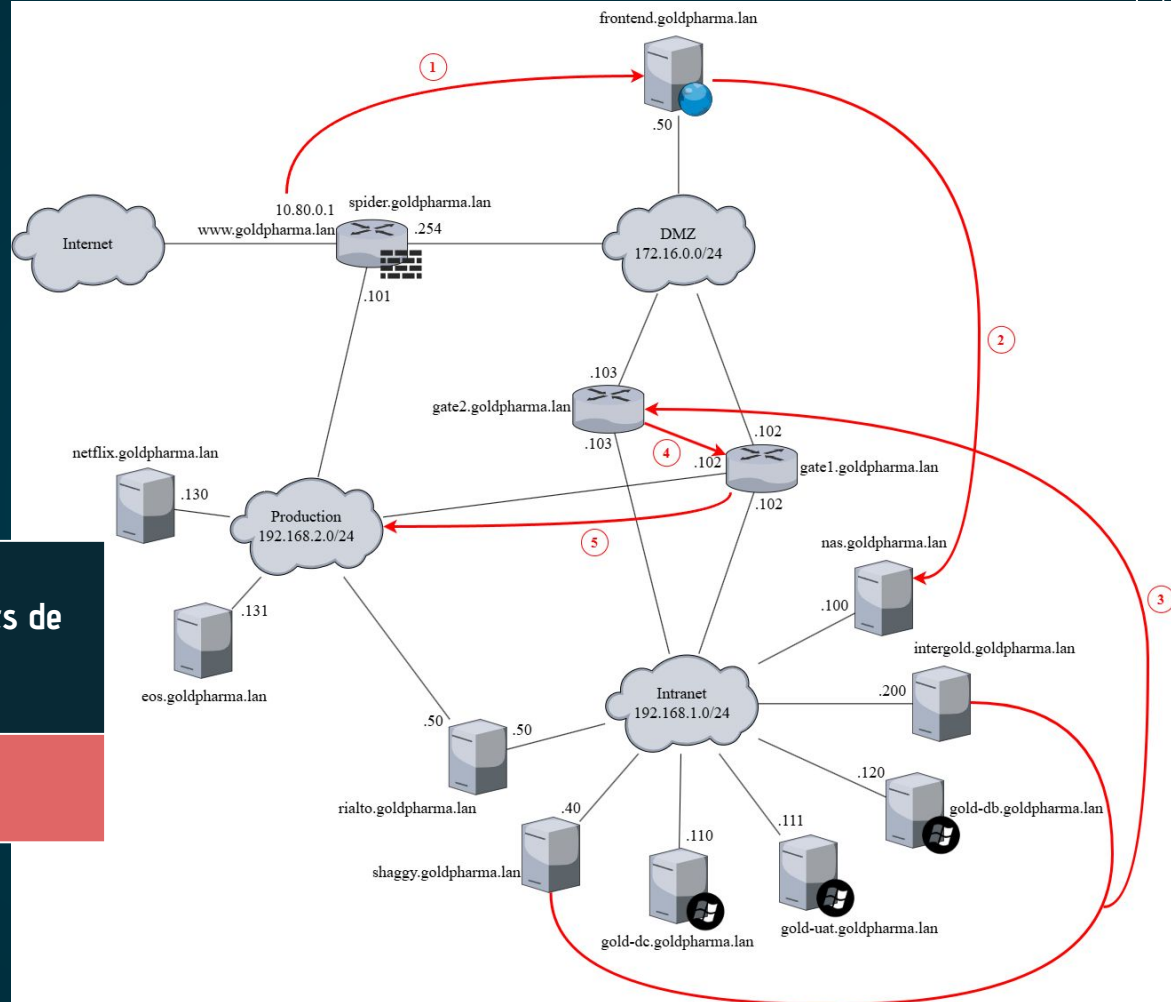
CHEMIN D'INTRUSION EXPLOITÉ

Présentation de vulnérabilités remarquables

[Gates-1] Réutilisation systématique des mots de passe

Criticité

Haute



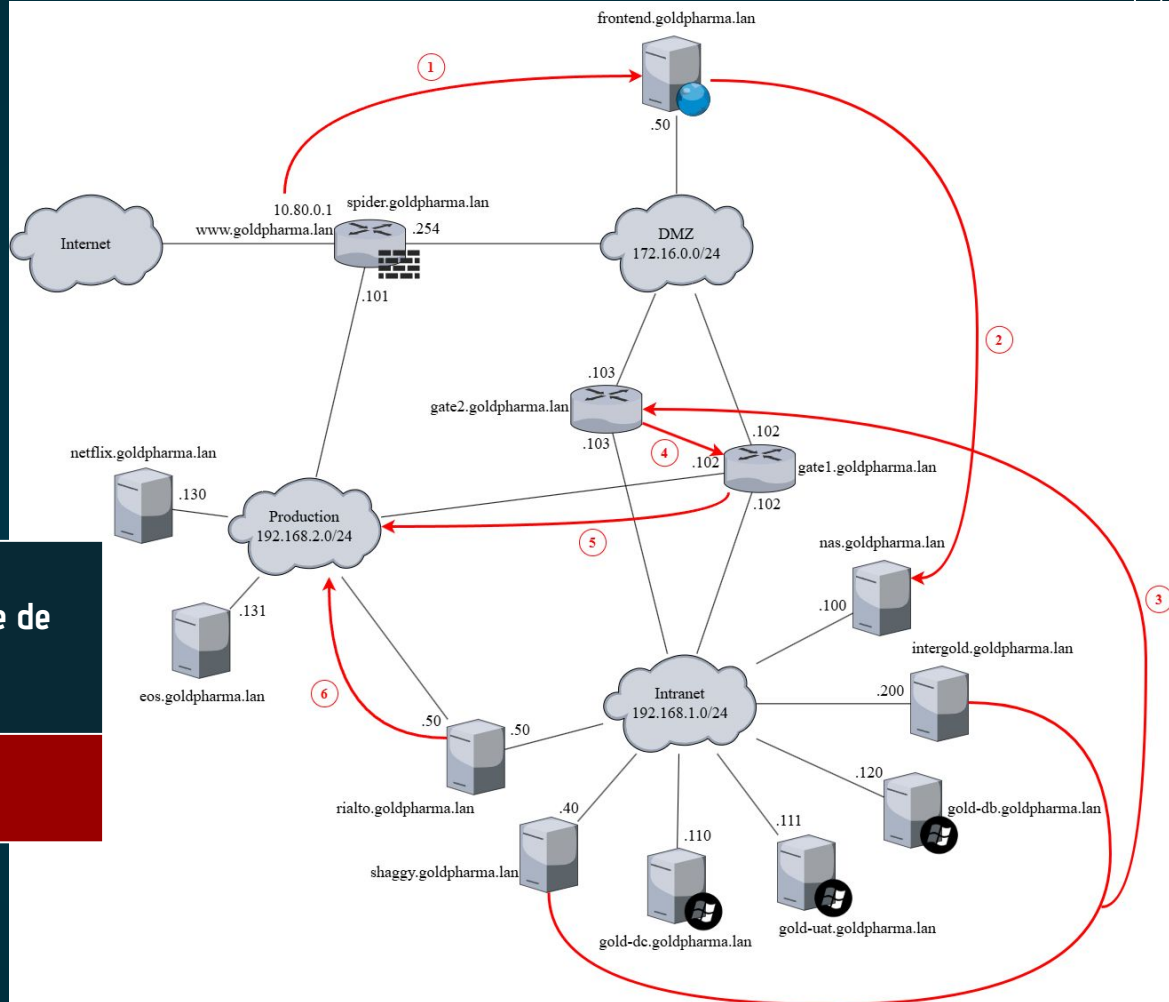
CHEMIN D'INTRUSION EXPLOITÉ

Présentation de vulnérabilités remarquables

[Rialto-1] Utilisation d'une version vulnérable de Nginx

Criticité

Critique



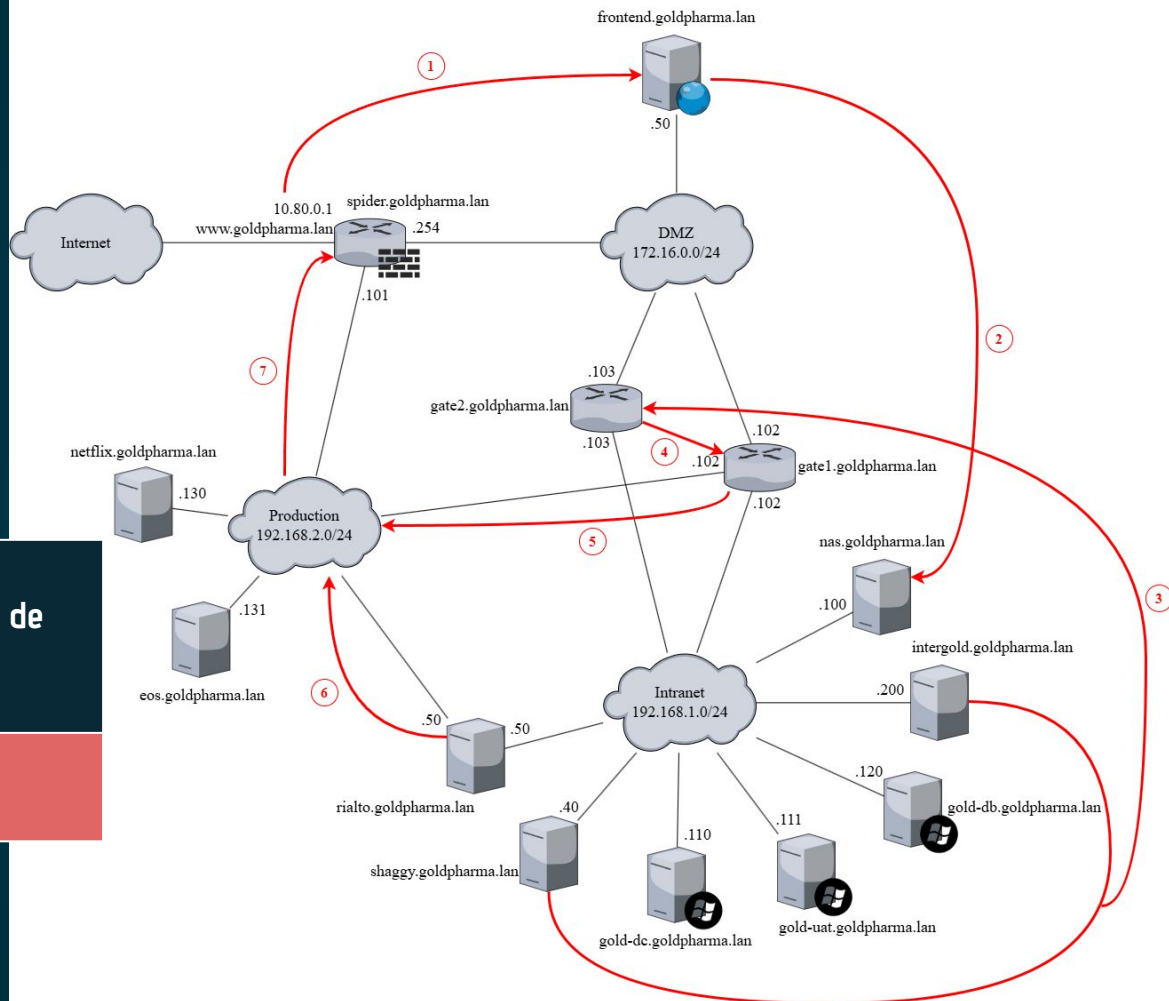
CHEMIN D'INTRUSION EXPLOITÉ

Présentation de vulnérabilités remarquables

[Spider-1] Utilisation d'une version obsolète de pfSense

Criticité

Haute

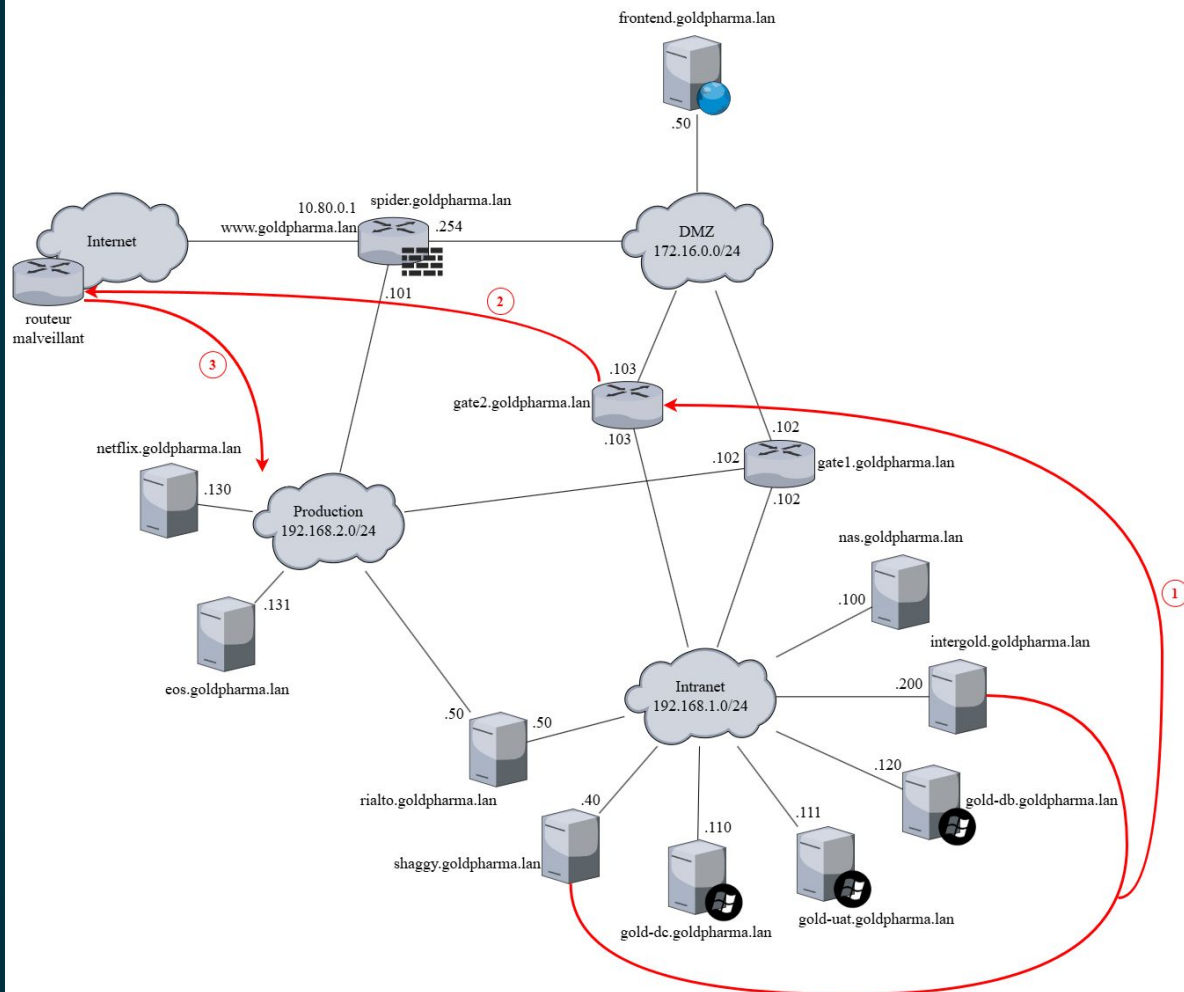


AUTRE CHEMIN D'INTRUSION

1 : Utilisation des informations sur Intergold et Shaggy pour obtenir les identifiants du routeur Gate2

2 : Création d'un routeur virtuel prioritaire à partir des fichiers de configuration de Gate2

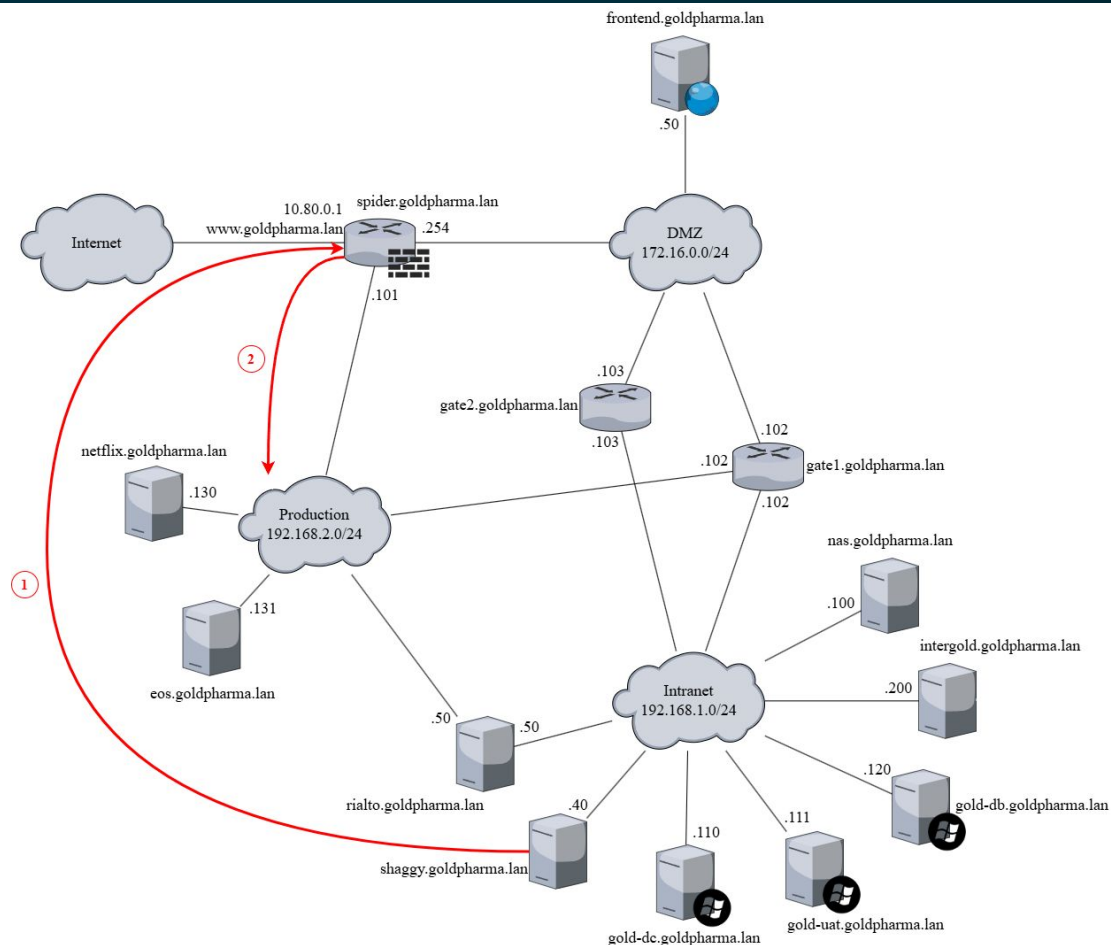
3 : Modification du protocole KeepAlive pour modifier la priorité des routeurs (accès au réseau Production)



AUTRE CHEMIN D'INTRUSION

1 : Connexion à Spider depuis la machine Shaggy à l'aide des identifiants obtenus des challenges des affiches

2 : Accès au réseau Production depuis la machine Spider





03

Synthèse de l'analyse des risques

MISSIONS

MISSION	Vente de médicament	Opérations interne
ACTIF CRITIQUE	Serveur Web et son backup (Frontend à 172.16.0.50 et NAS à 192.168.1.100)	Active Directory (Gold-DC à 192.168.1.110 et Gold-DB à 192.168.1.120)
ÉVÈNEMENTS REDOUTÉS	<ul style="list-style-type: none">• Fuite des données personnelles ou médicales des clients• Indisponibilité du serveur web	<ul style="list-style-type: none">• Indisponibilité de l'Active Directory

SOURCES DE RISQUE

SOURCE DE RISQUE	OBJECTIF VISÉ
Concurrent déloyal	Espionnage
Cybercriminel	Lucratif
Vengeur	Entrave au fonctionnement

POINTS D'INTRUSION

1

Compromission de
l'infrastructure

○○○

2

Compromission d'un
compte employé
(phishing)

○○○

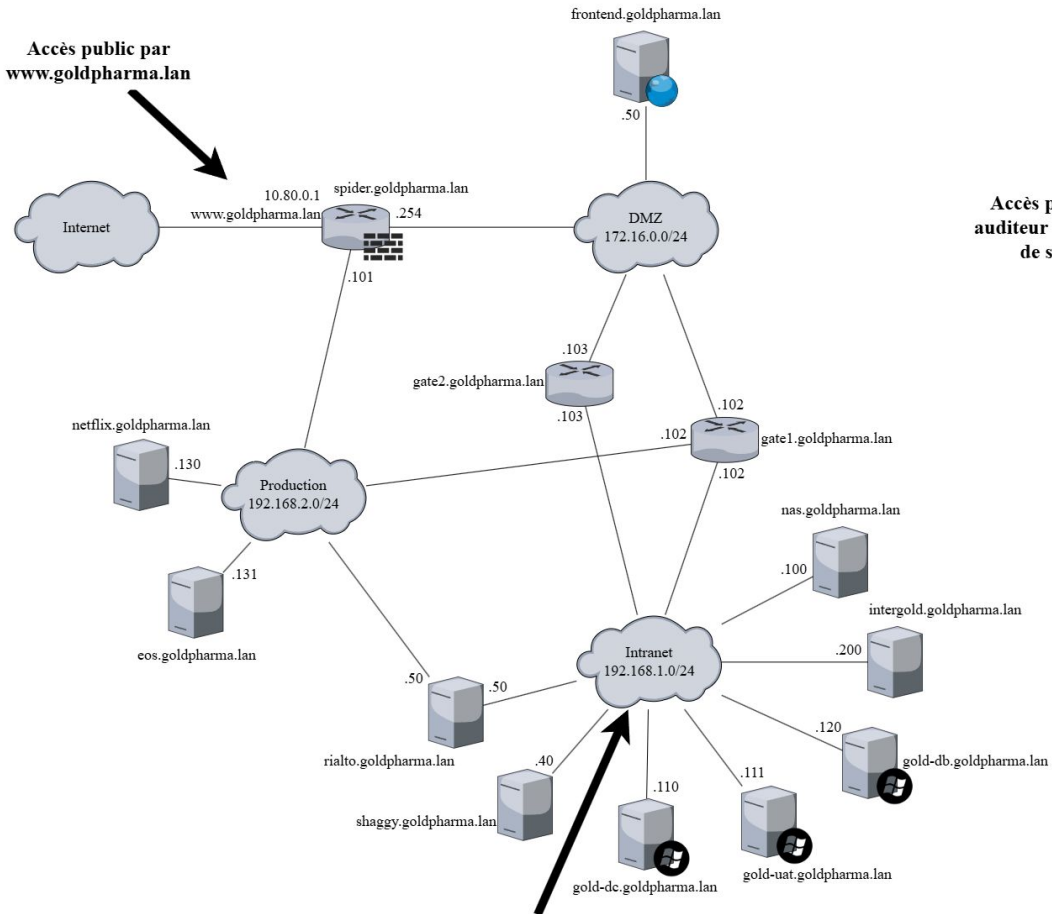
3

Corruption d'un
prestataire

○○○



Accès public par
www.goldpharma.lan















Accès physique par un
auditeur (accès dépendant
de ses missions)

Compromission d'un
compte employé (phishing)

SCÉNARIOS D'ATTAQUE

	CONCURRENT	CYBERCRIMINEL	VENGEUR
DESCRIPTION	Exfiltration des données de vente et des données de stratégie de l'entreprise	Mise en place d'un rançongiciel ou vol des données clients	Mise en indisponibilité du serveur web ou de l'Active Directory
INFRASTRUCTURE	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
COMPTE EMPLOYÉ	<input checked="" type="radio"/> <input checked="" type="radio"/>	<input checked="" type="radio"/> <input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/>
PRESTATAIRE	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

RISQUES DES SCÉNARIOS D'ATTAQUE

	CONCURRENT	CYBERCRIMINEL	VENGEUR
DESCRIPTION	Exfiltration des données de vente et des données de stratégie de l'entreprise	Mise en place d'un rançongiciel ou vol des données clients	Mise en indisponibilité du serveur web ou de l'Active Directory
INFRASTRUCTURE	  	 	 
COMPTE EMPLOYÉ	 		
PRESTATAIRE	 		



04

Plans d'action



FRONTEND, COURT TERME (0-15 JOURS)

Désactiver l'option de réinitialisation du mot de passe admin	Révocation des secrets exposés	Déploiement d'un Web Application Firewall
<ul style="list-style-type: none">• Gain : Empêcher le premier accès• Coût : 0,5 j-h	<ul style="list-style-type: none">• Gain : Empêcher l'accès non autorisés aux systèmes connectés à partir des clés d'API et mots de passes exposés• Coût : 2 j-h• Outils : GitGuardian	<ul style="list-style-type: none">• Gain : Protection contre les attaques web connues• Coût : 10 j-h• Outils : Cloudflare, Palo Alto Networks, ModSecurity• Impact métier : Faible, risque de faux positifs à gérer

FRONTEND, MOYEN TERME (1-3 MOIS)

Implémentation d'un système de gestion des secrets	Intégration d'analyses de sécurité dans le CI/CD	Refonte du mécanisme d'authentification	Correction des vulnérabilités critiques du code
<ul style="list-style-type: none">● Gain : Gestion centralisée et sécurisée des secrets d'API, credentials, etc.● Coût : 8 j-h● Outils : Script PowerShell avec module AD	<ul style="list-style-type: none">● Gain : Détection des mauvaises pratiques et des vulnérabilités lors de la phase de développement● Coût : 12 j-h + licences● Outils : SAST (SonarQube), DAST (OWASP ZAP)	<ul style="list-style-type: none">● Gain : Prévention contre le contournement de l'authentification● Coût : 30 j-h● Outils : Bibliothèques TOTP standards● Impact métier : Moyen, la formation des utilisateurs est nécessaire	<ul style="list-style-type: none">● Gain : Prévention d'exploitation immédiate des failles critiques● Coût : 30 j-h développeurs

NAS, COURT TERME (0-15 JOURS)

Mise à jour du système d'exploitation	Sécurisation des scripts utilisant tar avec des caractères génériques
<ul style="list-style-type: none">• Gain : Élimination de vulnérabilités connues• Coût : 3 j-h• Outil : Procédures de mise à jour du fabricant	<ul style="list-style-type: none">• Gain : Élimination d'un vecteur d'élévation de privilège• Coût : 1 j-h• Outil: Réécriture des scripts avec contrôles appropriés

ACTIVE DIRECTORY (AD), COURT TERME (0-3 MOIS)

Correction des modèles de certificats vulnérables (ESC4)	Nettoyage des champs de description des utilisateurs contenant des mots de passe	Révocation des droits dangereux
<ul style="list-style-type: none">● Gain : Critique, empêcher l'élévation des privilèges en tant qu'administrateur de domaine● Coût : Moyen, 2 j-h admin système● Outils : Certipy pour audit	<ul style="list-style-type: none">● Gain : Élevé, élimination des secrets exposés● Coût : Faible, 0.5 j-h● Outils : Script PowerShell avec module AD	<ul style="list-style-type: none">● Gain : Élevé, suppression d'un chemin d'attaque● Coût : Faible, 0.5 j-h● Outils : Script PowerShell avec module AD

ACTIVE DIRECTORY (AD), MOYEN TERME (3-6 MOIS)

Révision des relations d'approbation entre domaines

- Gain : Limitation de la propagation latérale
- Coût : 21 j-h
- Outils : Microsoft AD Trust Security Assessment Tool

GLOBAL (DÉVELOPPEMENT), LONG TERME (3+ MOIS)

Formation sécurité pour l'équipe de développement	Refonte du code avec sécurité by design
<ul style="list-style-type: none">• Gain : Montée en compétences et prévention proactive des vulnérabilités• Coût : 5 j-h développeurs + formateurs• Outils :<ul style="list-style-type: none">○ Sessions de formation OWASP Top 10○ Workshops secure coding spécifiques PHP/JavaScript	<ul style="list-style-type: none">• Gain : Élimination structurelle des classes entières de vulnérabilités et amélioration de la robustesse du code• Coût : 45+ j-h• Outils : Audit complet du code et restructuration sécurisée• Utilisation de bibliothèques sécurisées auditées certifiées

GLOBAL (CONTRÔLE D'ACCÈS), LONG TERME (3+

MOIS)

Déploiement d'une solution de surveillance des accès privilégiés

- Gain: Détection des comportements malveillants liés aux élévations de privilèges
- Coût: licence + 10 j-h
- Outil: Microsoft Defender for Identity (qui fait partie de Microsoft Defender XDR) ou CyberArk

Mise en place d'une surveillance des émissions de certificats

- Gain: Détection des tentatives d'exploitation
- Coût: 3 j-h + open source solution (graylog, wazuh +pki...)
- Outil: Microsoft Sentinel ou Splunk

GLOBAL (GOUVERNANCE), MOYEN TERME (0-3 MOIS)

Mise en place d'une politique de mots de passe

- Gain : Meilleure sécurité et gestion des mots de passes
- Coût : 7 j-h
- Outils : Guide ANSSI

Chapitre 4 : Facteur de connaissance (« ce que je sais ») du
GUIDE ANSSI RECOMMANDATIONS RELATIVES À
L'AUTHENTIFICATION MULTIFACTEUR ET AUX MOTS DE PASSE

GLOBAL (GOUVERNANCE), LONG TERME (3+ MOIS)

Mise en place d'un Système de Management de la Sécurité de l'Information (SMSI)	Formation sur le phishing et mots de passe avec sensibilisation régulière pour tous les employés
<ul style="list-style-type: none">● Gain :<ul style="list-style-type: none">○ Résilience aux cyberattaques○ Préparation aux nouvelles menaces○ Intégrité, confidentialité et disponibilité des données○ Protection de l'ensemble de l'organisation○ Économies de coûts○ Amélioration continue● Coût : 140 € document + investissements et recrutements● Outils : Normes ISO/IEC 27001 (et 27002)	<ul style="list-style-type: none">● Gain : Réduction du risque de compromission des comptes employés● Coût :<ul style="list-style-type: none">○ Formation initiale : 350€ - 850€, 0,5 j-h○ Sensibilisation interne régulière : 2 j-h tous les quelques mois
<ul style="list-style-type: none">● Audits blancs et audit de certification ISO 27001	

GLOBAL (ARCHITECTURE), LONG TERME (3+ MOIS)

Segmentation du réseau avancée	Mise en place d'une architecture à haute disponibilité	Mise en place d'un SIEM + XDR	Mise en place d'un processus de gestion de vulnérabilités
<ul style="list-style-type: none">• Gain : Réorganisation ordonnée et réduction de la surface d'attaque• Coût : 30 j-h	<ul style="list-style-type: none">• Gain : Résilience face aux DDoS et surcharges• Coût : 20 j-h	<ul style="list-style-type: none">• Gain : Récolte des logs pour détecter les comportements suspects et automatisation de la réponse aux comportements• Coût : 20 j-h• Outils : Wazuh, HarfangLab EDR	<ul style="list-style-type: none">• Gain : Réduction du délai de prise de connaissance entre la découverte et la correction des vulnérabilités• Coût : 15 j-h• Outils : Nessus, OpenVAS

A collection of isometric icons in shades of teal and blue. It includes a large shield with a checkmark, a padlock, several cloud shapes, and speech bubbles. The background is dark blue with decorative patterns of white circles and a large teal ring on the left.

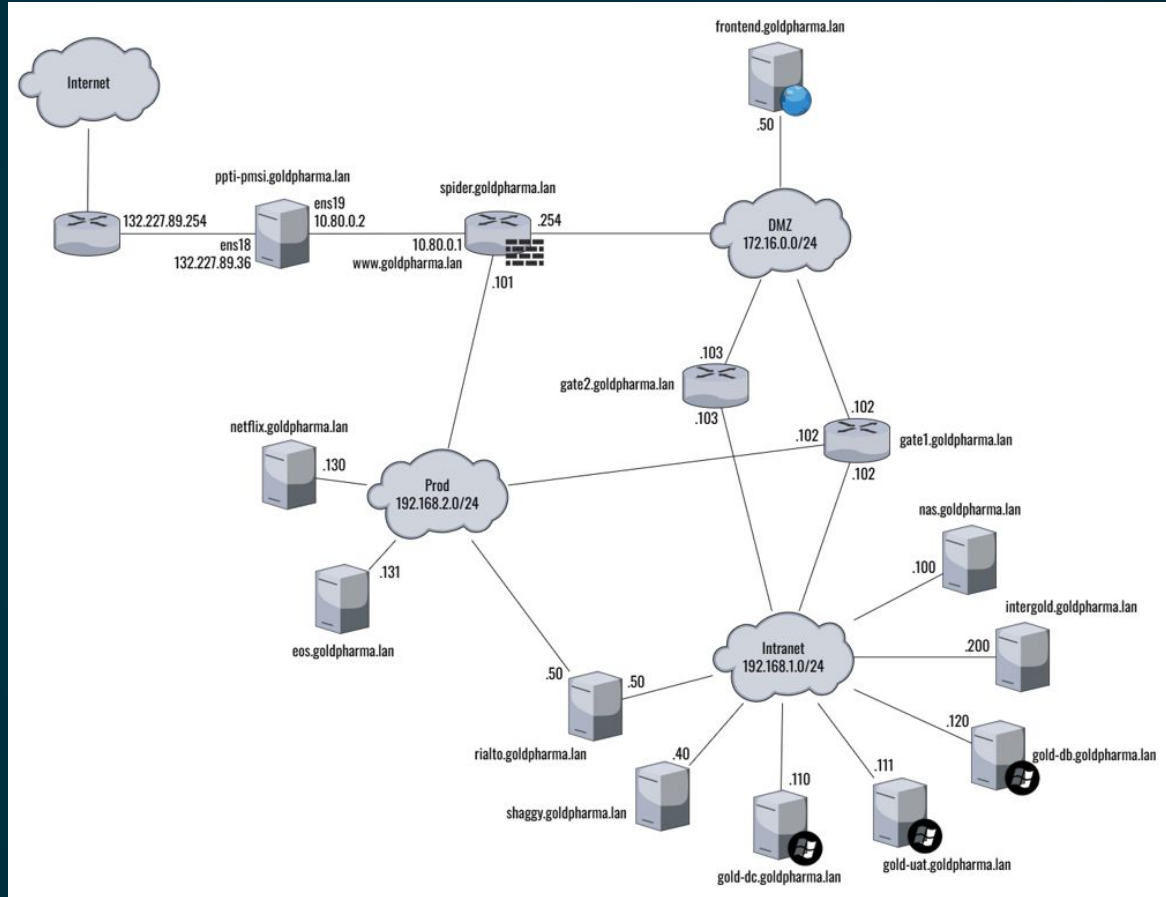
05

Proposition d'une nouvelle architecture

INFRASTRUCTURE ACTUELLE

Principaux défauts :

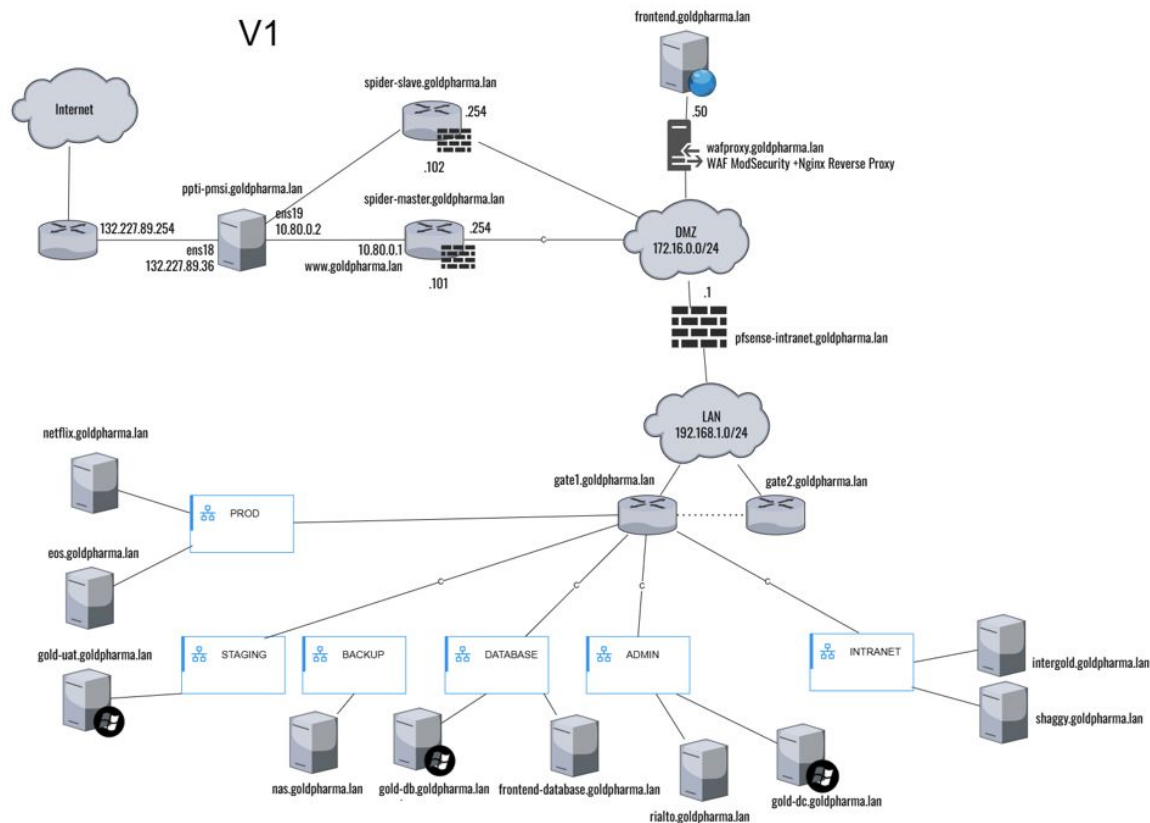
- Point de défaillance unique
- Frontend exposée
- Mauvaise segmentation



INFRASTRUCTURE RÉSEAU (COURT TERME)

Ajouts :

- Segmentation
- Redondance (Spider)
- Filtrage de flux



INFRASTRUCTURE RÉSEAU (LONG TERME)

Ajouts :

- Haute disponibilité
- Redondance (stockage)
- Surveillance et détection

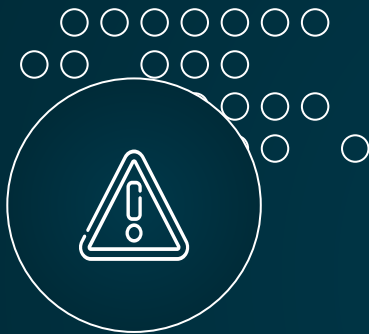


06

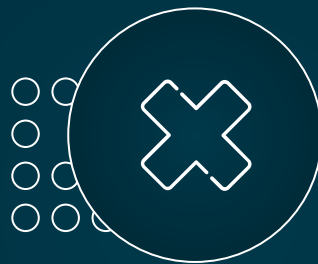
Conclusion



CONCLUSION



FAIBLE SOCLE
DE SÉCURITÉ



RISQUE DE
COMPROMISSION
TOTALE



SÉCURISER À
L'AIDE DES PLANS
D'ACTION

“Effective cybersecurity is not a product, but a process”

— JIM LANGEVIN





MERCI !

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**

VECTORS: Cyber security instagram stories template