

Gallus – Poste de Travail Sécurisé



Gallus est un logiciel open source offert par Eternilab.

Nous vous proposons une veille sécuritaire et des services spécialisés pour configurer, sécuriser, contrôler, maintenir vos postes de travail sécurisés basés sur Microsoft

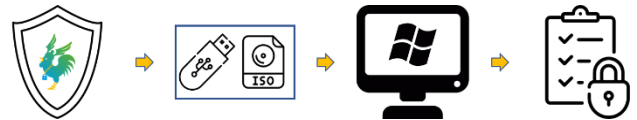


Gallus prépare un poste de travail sécurisé conforme au [GHI](#), au [PAMS](#), au [SecNumCloud](#) de l'ANSSI. Il met également en œuvre les recommandations du [CIS Benchmark](#). La version premium est conforme à l'[II901](#) pour atteindre le niveau Diffusion Restreinte.

Ce poste est un élément pivot des stratégies de défense qui adresse les points suivants :

1. **Isolation** : Créez une machine dédiée aux données sensibles.
2. **Authentification forte** : Déployez vos solutions.
3. **Chiffrement** : Chiffrez les configurations, mots de passe et clés d'accès. Chiffrez les communications.
4. **Accès restreint** : Contrôlez les accès aux machines et aux infrastructures via des protocoles maîtrisés.
5. **Gestion des sessions** : Restreignez l'utilisation des sessions privilégiées. Contrôlez les capacités des machines.
6. **Protection** : Lutte contre les logiciels malveillants. Contrôlez l'intégrité du poste.
7. **Surveillance** : Tracez et analysez les actions effectuées par les administrateurs.
8. **Mises à jour et correctifs** : Assurez une mise à jour régulière du système d'exploitation et des logiciels.


Gallus permet de déployer des outils de durcissement et de produire un rapport de conformité utilisable comme preuve.



Exemple de Rapport

A chaque installation, un rapport est produit pour vérifier que les outils de durcissement ont bien été déployés et que le poste est conforme au référentiel choisi. Une liste de non-conformités est mise en avant afin d'aider les équipes à les corriger rapidement.

Gallus Audit Report



Generated by Hardening Kit on 31/03/2025 12:16:46

| ID | Category | Name | Severity | Result |
|----------|------------------------|--|----------|---|
| 2.2.14.2 | User Rights Assignment | Create symbolic links (Hyper-V) | Medium | BUILTIN\Administrators |
| 2.2.29.2 | User Rights Assignment | Log on as a service (Hyper-V) | Medium | |
| 5.3.2 | System Services | Computer Browser (Browser) (Service Startup type) (Check for false positive for service "browser") | Medium | Manual |
| 5.7.2 | System Services | Infrared monitor service (irmon) (Service Startup type) | Medium | |
| 5.30.2 | System Services | Special Administration Console Helper (sacsv) (Service Startup type) | Medium | |
| 5.36.2 | System Services | Windows Media Player Network Sharing Service (WMPNetworkSvc) (Service Startup type) | Medium | |
| 2.3.1.4 | Security Options | Accounts: Rename administrator account | Low | Administrator |
| 2.3.1.5 | Security Options | Accounts: Rename guest account | Low | Guest |
| 2.3.7.5 | Security Options | Interactive logon: Message text for users attempting to log on | Low | |
| 2.3.7.6 | Security Options | Interactive logon: Message title for users attempting to log on | Low | |
| 1.1.1 | Account Policies | Length of password history maintained | Passed | 24 |
| 1.1.2 | Account Policies | Maximum password age | Passed | 365 |
| 1.1.3 | Account Policies | Minimum password age | Passed | 1 |
| 1.1.4 | Account Policies | Minimum password length | Passed | 14 |
| 1.1.5 | Account Policies | Password must meet complexity requirements | Passed | 1 |
| 1.1.6 | Account Policies | Relax minimum password length limits | Passed | 1 |
| 1.1.7 | Account Policies | Store passwords using reversible encryption | Passed | 0 |
| 1.2.1 | Account Policies | Account lockout duration | Passed | 15 |
| 1.2.2 | Account Policies | Account lockout threshold | Passed | 5 |
| 1.2.3 | Account Policies | Allow Administrator account lockout | Passed | 1 |
| 1.2.4 | Account Policies | Reset account lockout counter | Passed | 15 |
| 2.2.1 | User Rights Assignment | Access Credential Manager as a trusted caller | Passed | |
| 2.2.2 | User Rights Assignment | Access this computer from the network | Passed | BUILTIN\Administrators,BUILTIN\Remote Desktop Users |

www.eternilab.com

sales@eternilab.com

