# DOCUMENTATION TECHNIQUE

## Outils et configurations - Stage BMS Circuits

**EBERHARD Nicolas | BTS SIO SISR | Mai - Juin 2025**
Tuteur : REVEL Cedric | BMS Circuits, Mouguerre (64)


*Environnement technique utilise durant le stage*

*Outils documentes : GLPI | Active Directory | DSP (Semperis) | WithSecure | TeamViewer | PowerShell*

# 1. GLPI - Gestion des tickets d'incidents

GLPI (Gestionnaire Libre de Parc Informatique) est l'outil ITSM utilise par BMS Circuits pour assurer le suivi des incidents et des demandes d'assistance. Il permet de centraliser et de prioriser les interventions du service informatique.

## 1.1 Fonctionnement general

- Les utilisateurs soumettent leurs demandes via le Helpdesk (source de la demande)
- Chaque ticket est categorise par Type (Incident ou Demande), Urgence, Impact et Priorite
- Les techniciens traitent, commentent et resolvent les tickets, avec historique complet des echanges
- Le statut evolue : En attente → En cours (Attribue) → Resolu

## 1.2 Exemple de ticket traite - Demande installation script

Ticket #8823 - Script Corim : demande d'installation d'un script de developpement interne. Urgence Haute, Impact Moyen, Priorite Haute.

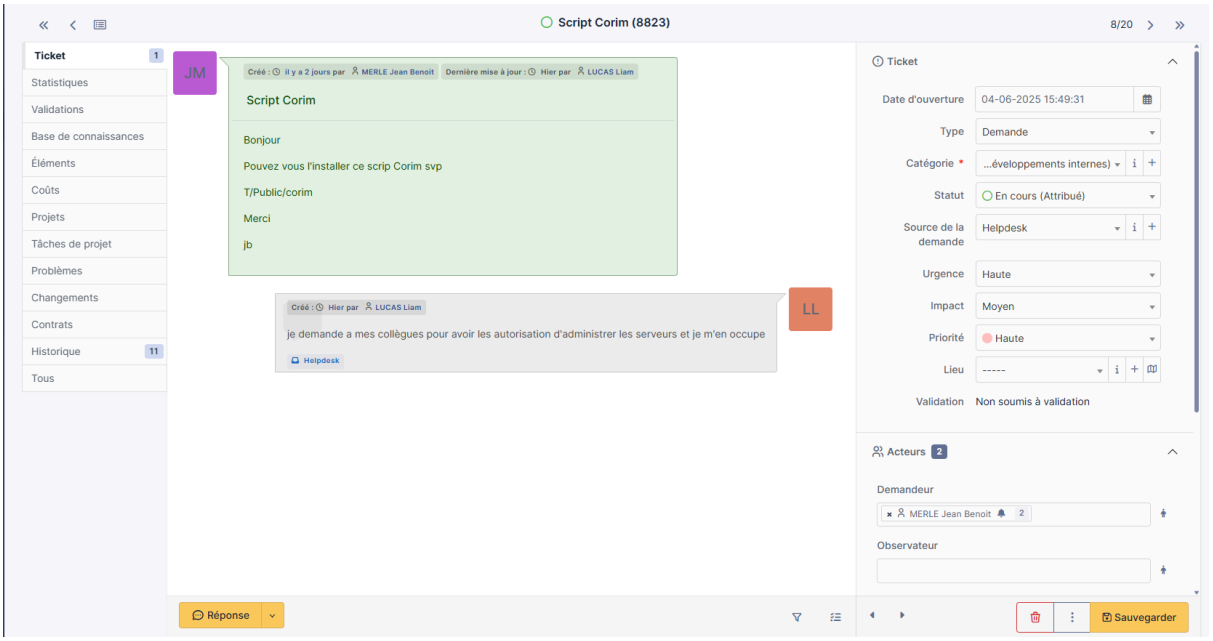



*Figure 1 - Ticket GLPI #8823 : demande d'installation d'un script (statut : En cours Attribue)*

## 1.3 Exemple de ticket resolu - Testeur fonctionnel TeamViewer

Ticket #8935 - Testeur fonctionnel MP2 : ajout d'un poste dans TeamViewer et gestion des droits d'acces groupe admin. Ticket resolu avec suivi des actions realisees.

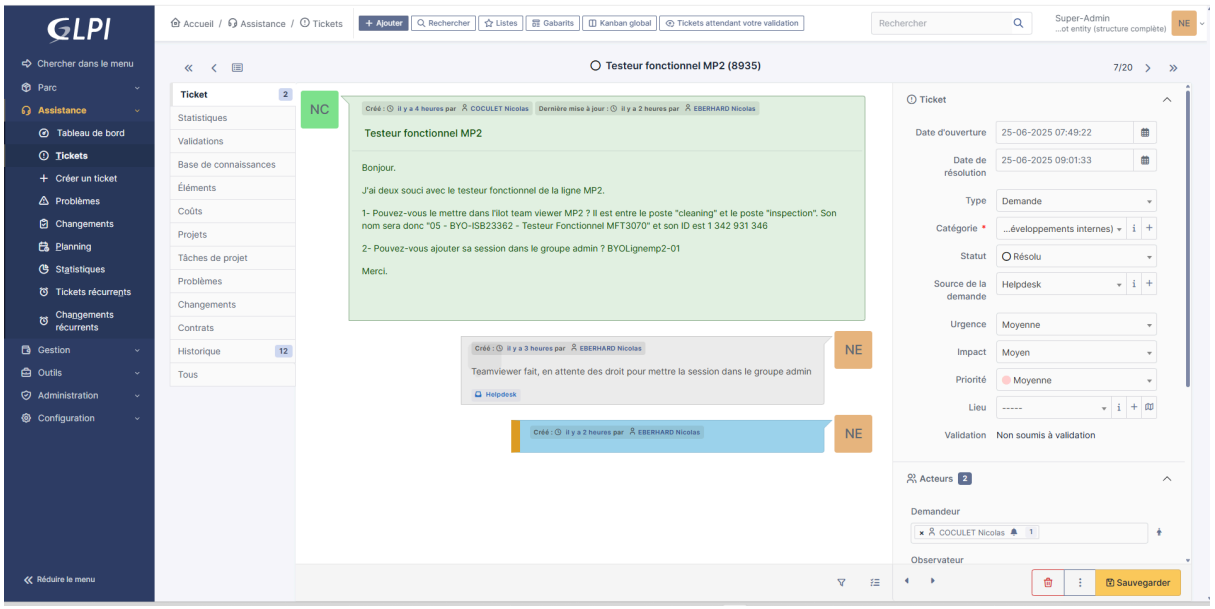



*Figure 2 - Ticket GLPI #8935 : integration TeamViewer et gestion des droits (statut : Resolu)*

**i Note :** Les tickets sont traces avec les initiales du technicien intervenant (NE = EBERHARD Nicolas). L'historique complet est conserve pour chaque ticket.

# 2. Active Directory - Gestion des identites et des acces

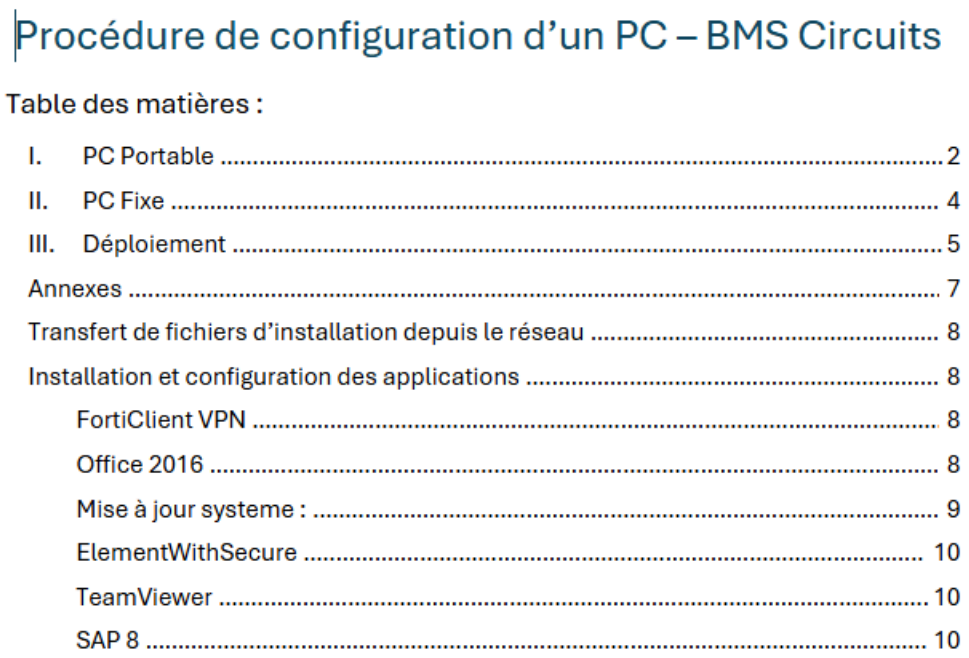
Active Directory (AD) est le service d'annuaire Microsoft utilise par BMS Circuits pour la gestion centralisee des comptes utilisateurs, des groupes de securite, des unites organisationnelles (OU) et des permissions reseau.

## 2.1 Missions realisees dans l'AD

- Creation et suppression de comptes utilisateurs dans les bonnes OU
- Gestion des groupes de securite (ajout/retrait de membres)
- Deplacement d'objets entre unites organisationnelles
- Diagnostic et correction d'incidents de synchronisation
- Verification des droits d'acces lors de l'audit RGPD

## 2.2 Procedure de configuration PC - BMS Circuits

Un document de procedure interne decrit la configuration standard des postes informatiques chez BMS Circuits. Il inclut les etapes pour PC Portable, PC Fixe et le deploiement des applications metier.



Procédure de configuration d'un PC – BMS Circuits

Table des matières :



*Figure 3 - Procedure interne de configuration d'un PC BMS Circuits (table des matieres)*

Les applications installes en standard sur chaque poste sont :

- FortiClient VPN - acces securise au reseau depuis l'exterieur
- Office 2016 - suite bureautique
- ElementWithSecure - agent de protection endpoint
- TeamViewer - prise en main a distance
- SAP 8 - ERP de gestion de production

## 2.3 Incident resolu - Perte d'acces utilisateur

Probleme : un utilisateur ne parvenait plus a acceder a son poste ni a ses partages reseau suite a un changement d'unite organisationnelle. Diagnostic via ADUC, correction de l'emplacement de l'objet → retablissement immediat de la session.

## 2.4 Incident RGPD - Fuite de droits accidentelle

Detection d'un utilisateur ayant acces a un repertoire confidentiel RH par erreur d'appartenance a un groupe de securite mal nomme. Correction immediate, puis proposition de refonte de la nomenclature des groupes et d'une revue mensuelle des droits.

# 3. Directory Services Protector (DSP) - Surveillance de l'AD

Semperis Directory Services Protector (DSP) est un outil ITDR (Identity Threat Detection and Response) reconnu par Gartner. Il surveille l'Active Directory en temps reel et detecte les modifications non autorisees, les comportements suspects et les vulnerabilites.

## 3.1 Architecture de la solution

Le DSP est compose de plusieurs elements travaillant ensemble :

- DSP Management : serveur central de gestion
- DSP Agents : agents deployes sur les controleurs de domaine
- Audit Agents & Audit Collectors : collecte des journaux d'evenements AD
- Database & Log Server : stockage des donnees d'audit
- Mail Server : envoi des alertes et notifications


*Figure 4 - Tableau de bord DSP : System Health avec 2 DSP Agents et 2 Audit Agents actifs (tous en vert = Responding)*

## 3.2 Partitions surveillees

Le DSP surveille l'ensemble des partitions LDAP de l'annuaire BMSCIRCUITS.LAN :

- DC=BMSCIRCUITS,DC=LAN - partition principale du domaine
- DC=DomainDnsZones,DC=BMSCIRCUITS,DC=LAN
- DC=ForestDnsZones,DC=BMSCIRCUITS,DC=LAN
- CN=Configuration,DC=BMSCIRCUITS,DC=LAN
- CN=Schema,CN=Configuration,DC=BMSCIRCUITS,DC=LAN

Toutes les partitions affichent un statut OK (coche vert) au moment de l'observation.

## 3.3 Tableau de bord - Activite recente

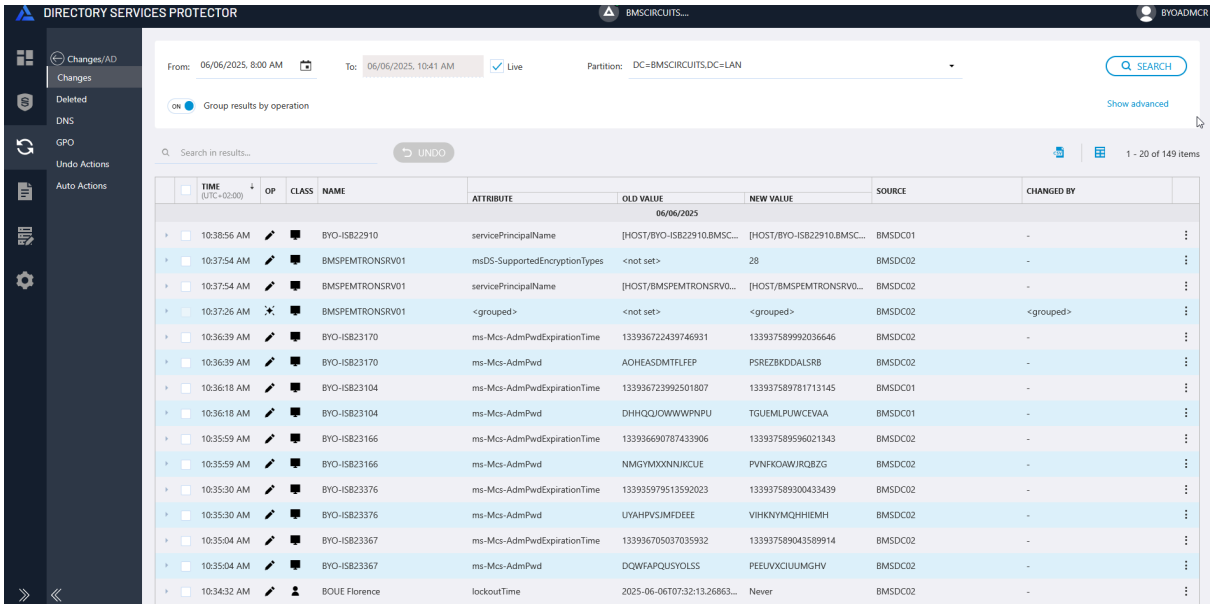



*Figure 5 - DSP : activite recente sur la periode Mai-Juin 2025 (creations, suppressions, modifications, deplacements)*

**i Note :** Le graphique montre des pics d'activite importants (jusqu'a 800 evenements/jour) correspondant aux periodes de maintenance et de mise a jour du parc informatique.

## 3.4 Regles de notification configurees

Le DSP dispose de regles d'alerte preconfigureees pour les evenements critiques de l'Active Directory :

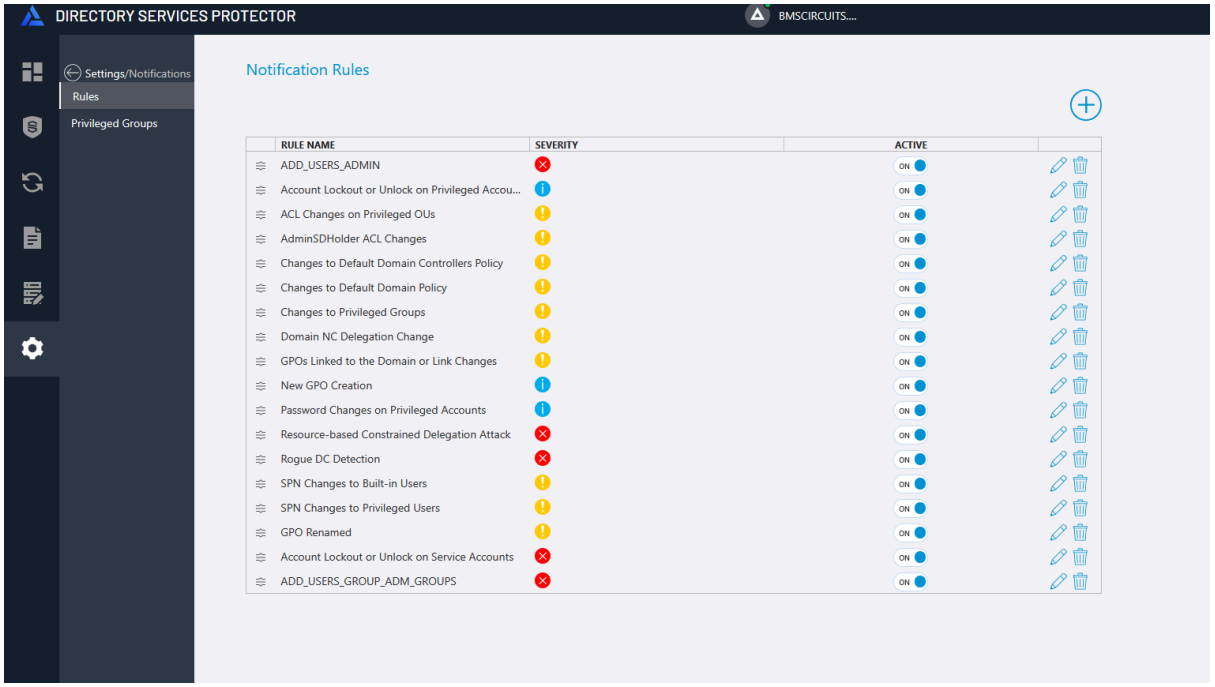



*Figure 6 - DSP : regles de notification avec niveaux de severite (rouge = critique, orange = avertissement, bleu = information)*

Les principales regles actives et leur niveau de severite :

| Regle | Severite | Statut |
|---|---|---|
| ADD_USERS_ADMIN | **Critique** | Active |
| Resource-based Constrained Delegation Attack | **Critique** | Active |

| | | |
|---|---|---|
| Rogue DC Detection | **Critique** | Active |
| Account Lockout on Service Accounts | **Critique** | Active |
| ADD_USERS_GROUP_ADM_GROUPS | **Critique** | Active |
| ACL Changes on Privileged OUs | **Avertissement** | Active |
| Changes to Default Domain Policy | **Avertissement** | Active |
| Changes to Privileged Groups | **Avertissement** | Active |
| GPOs Linked to the Domain or Link Changes | **Avertissement** | Active |
| New GPO Creation | **Information** | Active |
| Password Changes on Privileged Accounts | **Information** | Active |

# 4. WithSecure - Protection Endpoint

WithSecure (anciennement F-Secure Business) est la solution de securite des postes de travail et serveurs deploye chez BMS Circuits. Elle assure la protection antivirus, la detection comportementale, la gestion du pare-feu et la conformite du parc.

## 4.1 Tableau de bord - Vue d'ensemble du parc

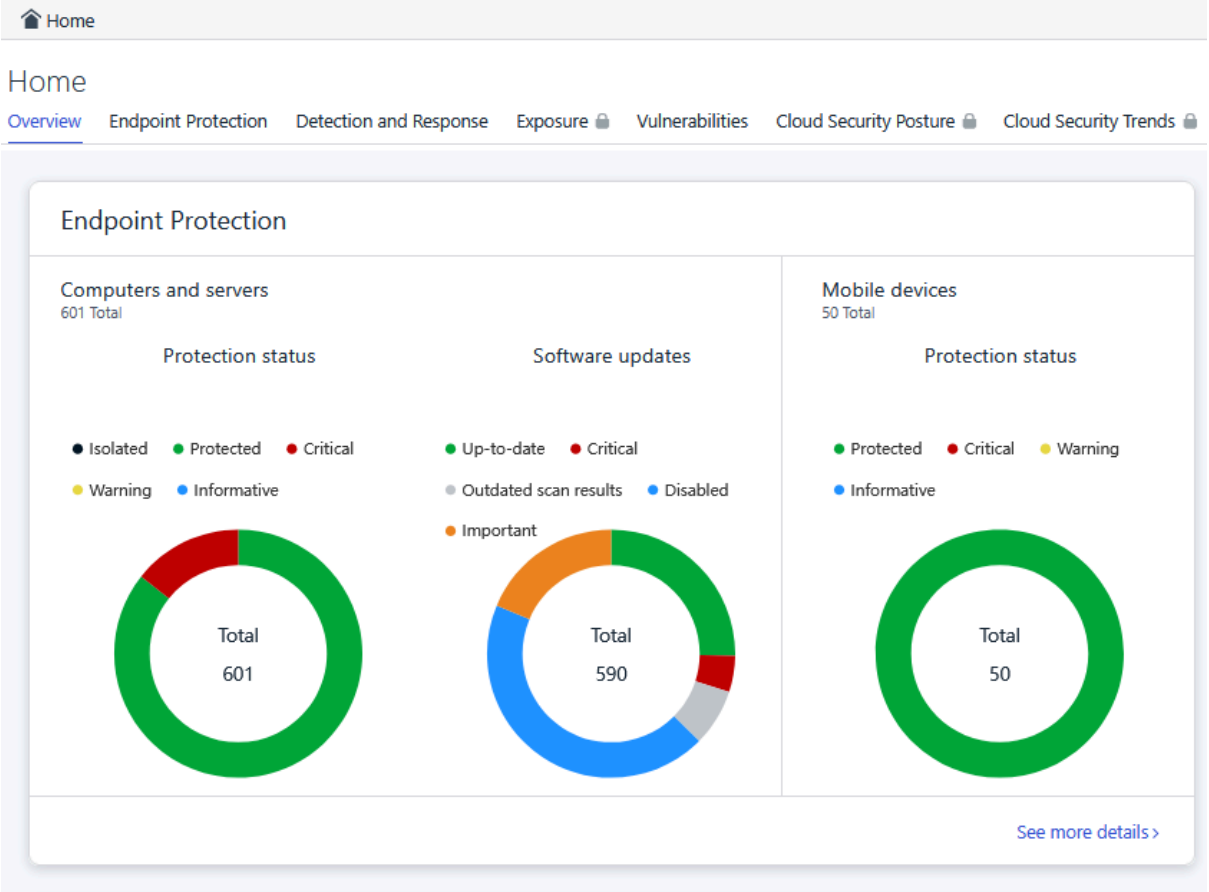



*Figure 7 - WithSecure : tableau de bord Endpoint Protection (601 postes, 50 appareils mobiles)*

## 4.2 Etat du parc au moment de l'observation

Ordinateurs et serveurs (601 au total) :

- Statut de protection : majorite des postes proteges (vert), quelques postes en etat critique
- Mises a jour logicielles : une partie des postes a jour, d'autres necessitant une mise a jour (bleu = Outdated scan results)

Appareils mobiles (50 au total) :

- Statut de protection : quasi-totalite des appareils proteges (vert)

## 4.3 Missions realisees avec WithSecure

- Analyse des alertes de logiciels malveillants et classification des evenements
- Verification du deploiement de l'agent WithSecure sur l'ensemble du parc
- Identification des postes sans agent installe ou avec agent non repondant
- Application de politiques de pare-feu sur des segments du reseau
- Documentation de l'etat de conformite des postes

## 4.4 Evenements bloques par le pare-feu

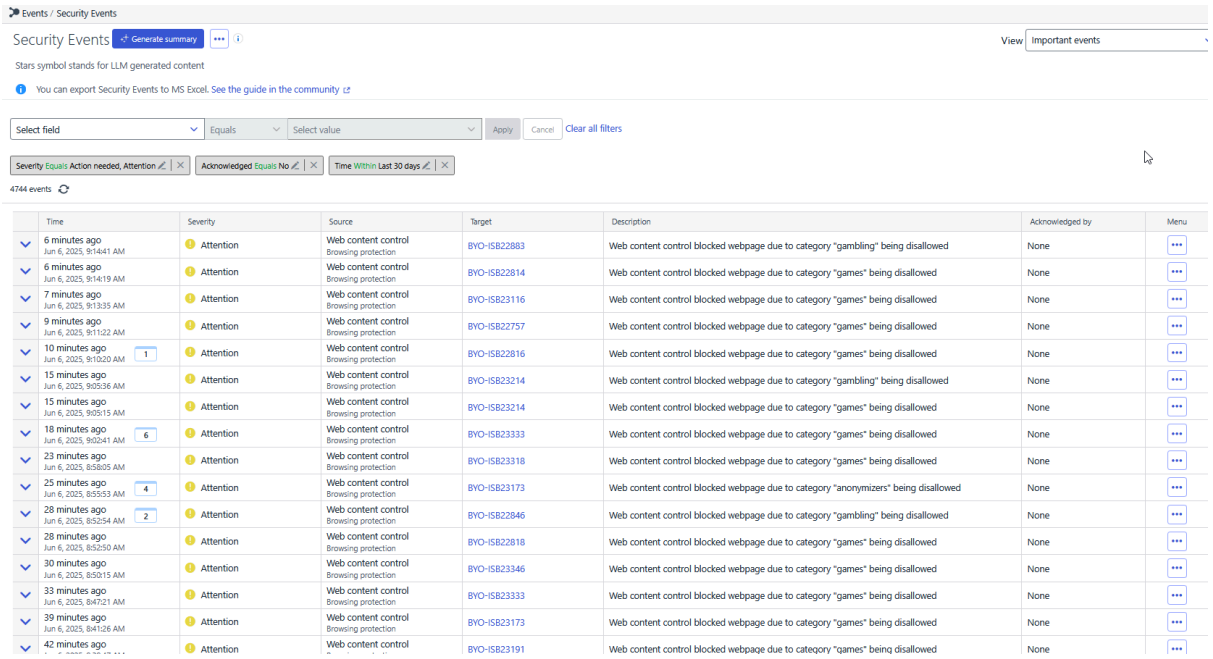



*Figure 8 - Exemple d'evenements bloques par le pare-feu WithSecure sur le reseau BMS Circuits*

**i Note :** Les evenements de pare-feu permettent de visualiser les tentatives de connexion bloquees et d'identifier d'eventuelles anomalies de comportement reseau.

# 5. Infrastructure reseau - Securisation des salles

BMS Circuits dispose d'une infrastructure reseau structuree autour d'un coeur de reseau Nexus N9K, avec des switches Cisco 48 ports distribuant la connectivite dans les differentes salles informatiques.

## 5.1 Architecture reseau - Solution de securisation

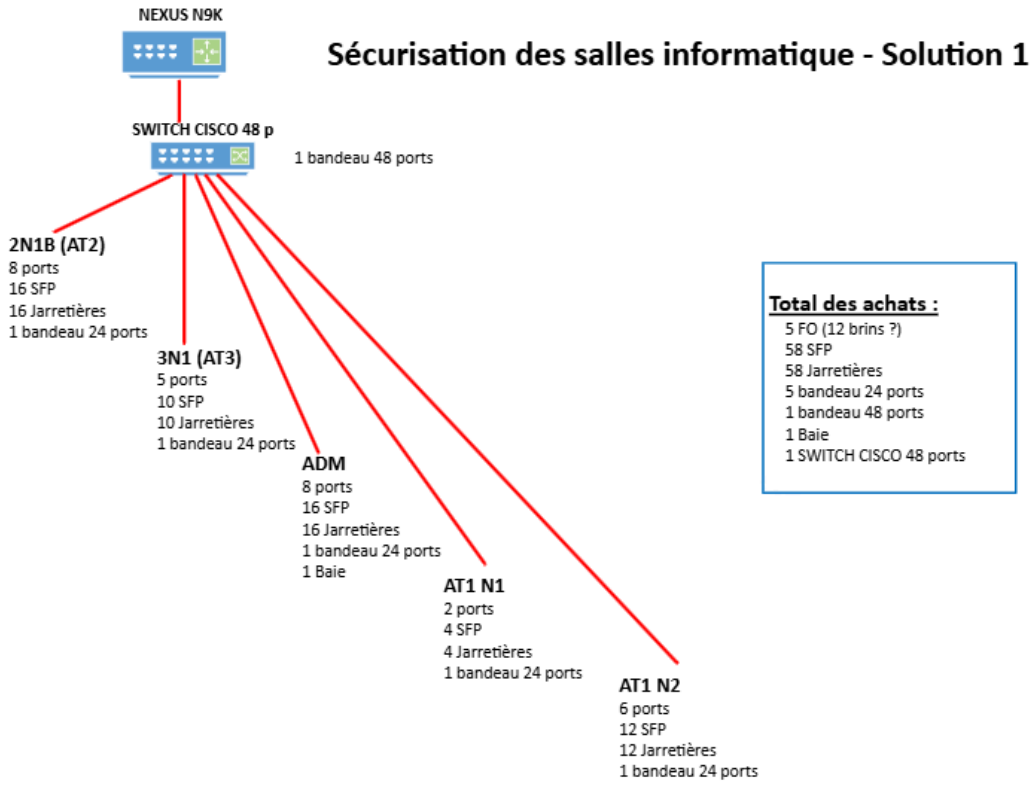



*Figure 9 - Schema de securisation des salles informatiques : architecture Nexus N9K + Switch Cisco 48 ports*

## 5.2 Detail de l'architecture

Le schema presente la solution 1 de securisation des salles informatiques :

- Coeur de reseau : NEXUS N9K (switch de distribution principal)
- Switch d'acces : CISCO 48 ports (1 bandeau 48 ports)
- Salles raccordees : 2N1B (AT2), 3N1 (AT3), ADM, AT1 N1, AT1 N2

Detail des equipements par salle :

| Salle | Ports | SFP | Jarretieres | Bandeaux | Baie |
|---|---|---|---|---|---|
| 2N1B (AT2) | 8 | 16 | 16 | 1 x 24p | - |
| 3N1 (AT3) | 5 | 10 | 10 | 1 x 24p | - |
| ADM | 8 | 16 | 16 | 1 x 24p | 1 Baie |
| AT1 N1 | 2 | 4 | 4 | 1 x 24p | - |
| AT1 N2 | 6 | 12 | 12 | 1 x 24p | - |

Total des achats identifies pour cette solution : 5 FO, 58 SFP, 58 Jarretieres, 5 bandeaux 24 ports, 1 bandeau 48 ports, 1 Baie, 1 Switch CISCO 48 ports.

# 6. Environnement de travail general

## 6.1 Poste de travail et acces

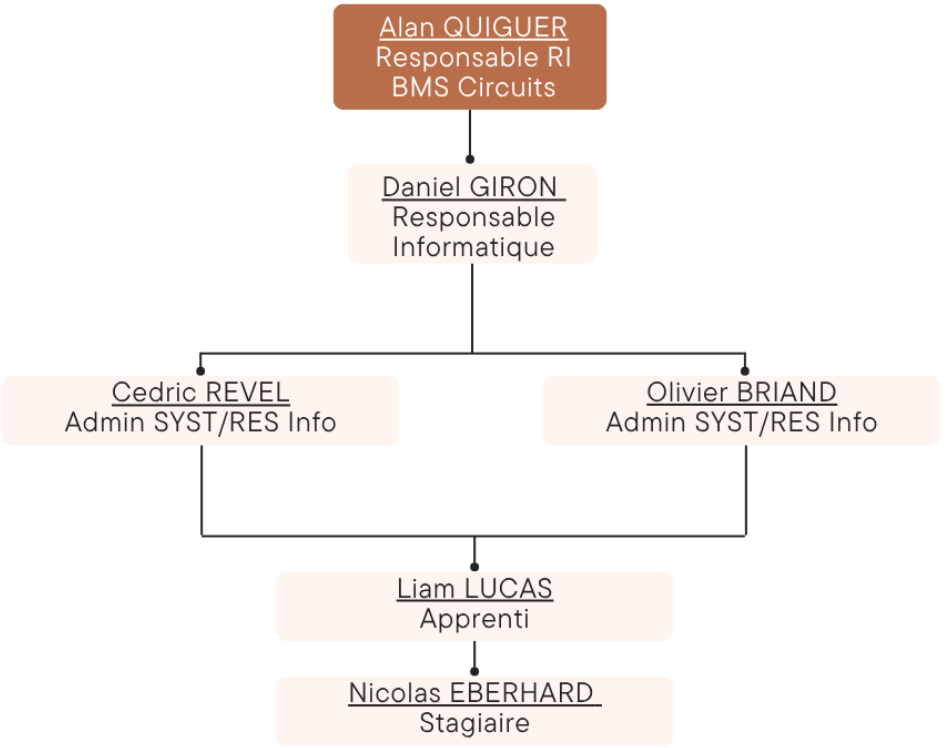



*Figure 10 - Poste de travail du stagiaire configure des la premiere semaine*

## 6.2 Infrastructure de production BMS Circuits

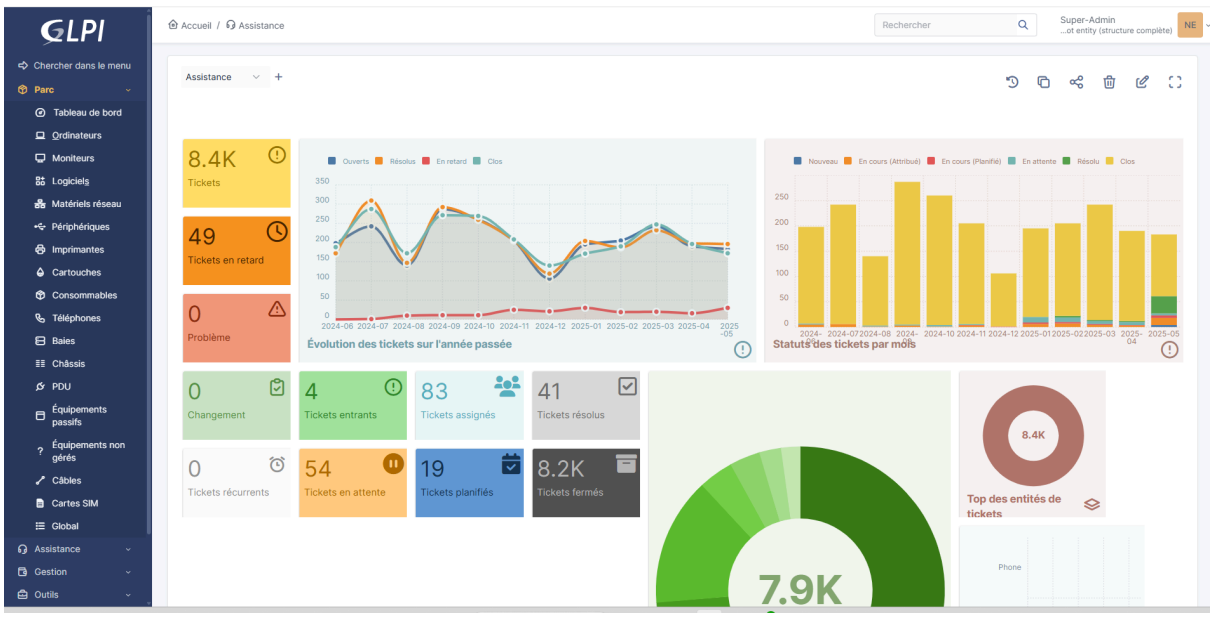



*Figure 11 - Vue de l'environnement de production BMS Circuits (ateliers electroniques)*

## 6.3 Organigramme du service informatique

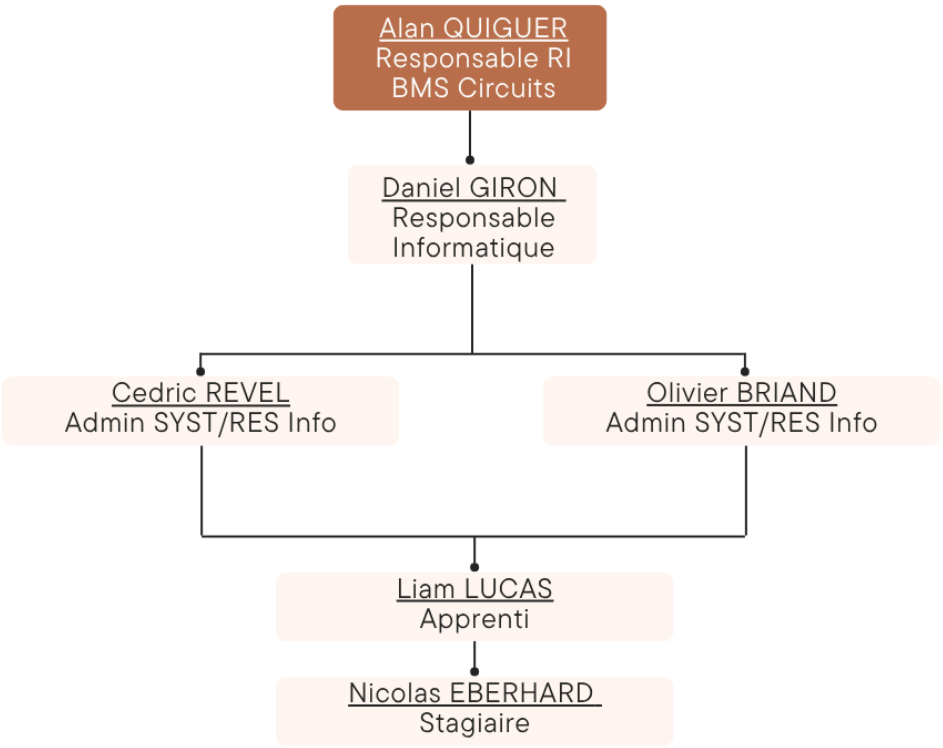



*Figure 12 - Organigramme du service informatique BMS Circuits (5 personnes)*

# 7. Script PowerShell - Automatisation de la creation de comptes

Dans le cadre du projet d'automatisation, j'ai developpe et teste un script PowerShell permettant d'automatiser la creation des comptes utilisateurs dans Active Directory, en reduisant les erreurs humaines et le temps de traitement.

## 7.1 Problematique

La creation manuelle des comptes etait source de plusieurs problemes recurrents :

- Oubli d'ajout aux groupes de securite obligatoires
- Boites mail Exchange non creees systematiquement
- Non-respect de la convention de nommage des logins
- Temps de traitement eleve pour chaque nouvelle arrivee

## 7.2 Fonctionnalites du script

- Generation automatique du Login selon la convention interne (Prenom.Nom)
- Creation de l'objet utilisateur dans la bonne Unite Organisationnelle (OU)
- Provisionnement de la boite aux lettres Exchange / Microsoft 365
- Attribution automatique des groupes de securite par defaut
- Gestion des doublons (verification de l'existence du compte)

## 7.3 Structure du script (exemple simplifie)

```
# Script de creation de compte utilisateur AD - BMS Circuits
param (
    [string]$Prenom,
    [string]$Nom,
    [string]$Service,
    [string]$OU
)

$Login = $Prenom.Substring(0,1).ToLower() + $Nom.ToLower()

# Verification doublon
if (Get-ADUser -Filter {SamAccountName -eq $Login}) {
    Write-Warning "Compte $Login deja existant"
    exit
}

# Creation du compte AD
New-ADUser -Name "$Prenom $Nom" -SamAccountName $Login \
    -Path "OU=$OU,DC=BMSCIRCUITS,DC=LAN" \
    -AccountPassword (ConvertTo-SecureString "TempPass123!" -AsPlainText
-Force) \
    -Enabled $true -ChangePasswordAtLogon $true

# Attribution des groupes par defaut
Add-ADGroupMember -Identity "GRP_$Service" -Members $Login
Add-ADGroupMember -Identity "GRP_ALL_USERS" -Members $Login

Write-Host "Compte $Login cree avec succes." -ForegroundColor Green
```

*Figure 13 - Extrait du script PowerShell de creation de comptes utilisateurs AD*

## 7.4 Bilan

- Gain de temps significatif : creation en < 1 minute contre 10-15 minutes manuellement
- Standardisation : tous les comptes respectent la meme convention de nommage
- Reduction des erreurs : aucun oubli de groupe ou de boite mail possible
- Script documente et teste en environnement controle avant deploiement

*Documentation realisee par EBERHARD Nicolas - BTS SIO SISR - Stage BMS Circuits 2025*