

EBIOS & Active Directory

La maîtrise des risques avec la méthode EBIOS

 par **Stéphane LARCHER**



Your digital fortress

 **cyberguard**
SOLUTIONS

Spécialiste de l'infrastructure et de la virtualisation

Depuis 2014

au sein de la DSI des hôpitaux de paris depuis mars 2014, j'ai été en charge de l'infrastructure virtuelle

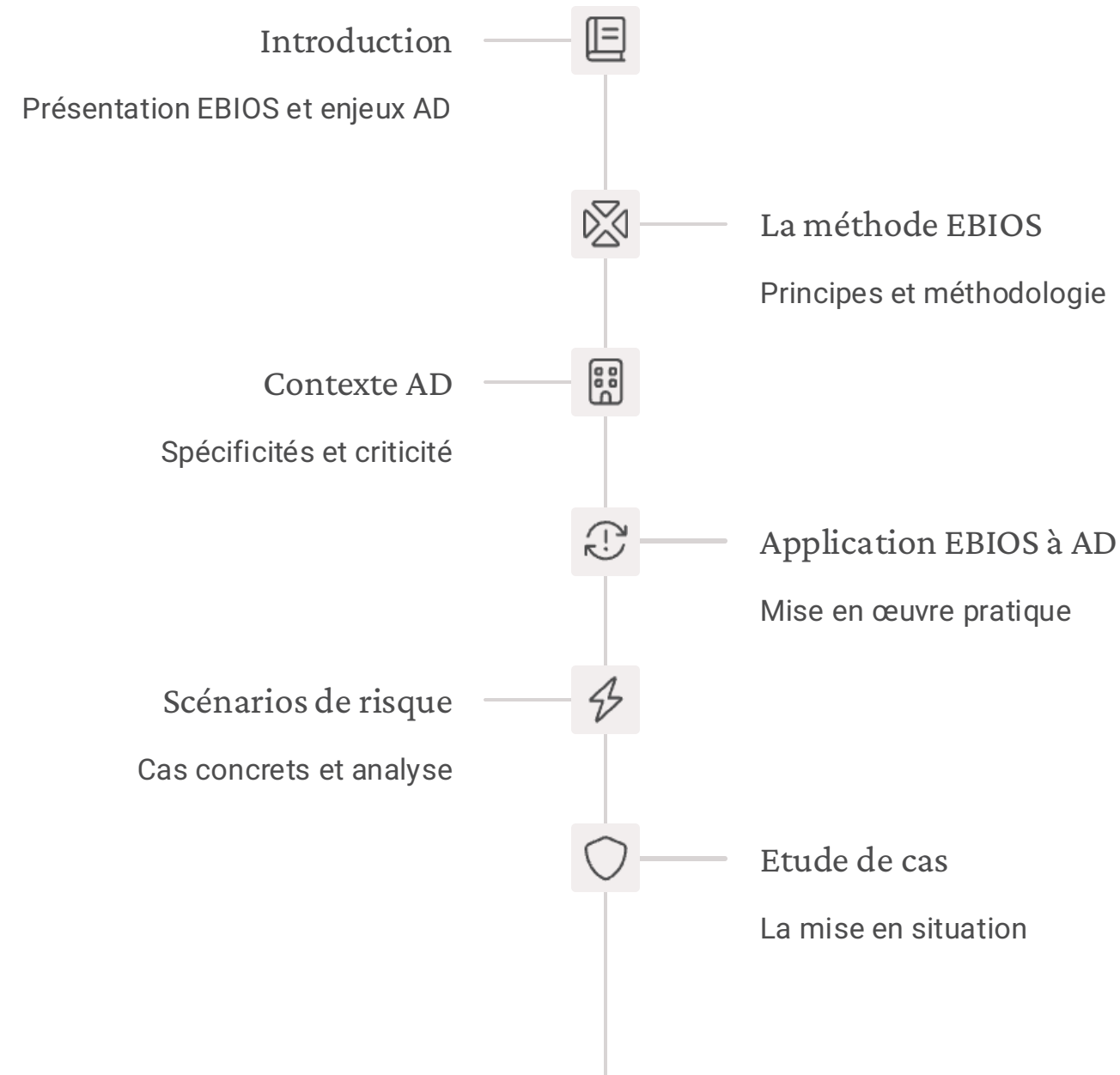
Depuis 2018

au sein du projet de consolidation des Datacenter, je suis en charge de la partie technique, de l'accompagnement des équipes pour l'utilisation de la nouvelle infrastructure mutualisée, et de l'inventaire matériel



Stéphane LARCHER
Stephane-larcher@outlook.com
Stephane.larcher2@lecnam.net
Mob : +33 6 60 98 63 41

Programme de la Conférence



Statistiques Alarmantes

74%

Cyberattaques

des cyberattaques ciblent l'identité

95%

Utilisation

des entreprises utilisent AD

23min

Compromission

compromission moyenne AD

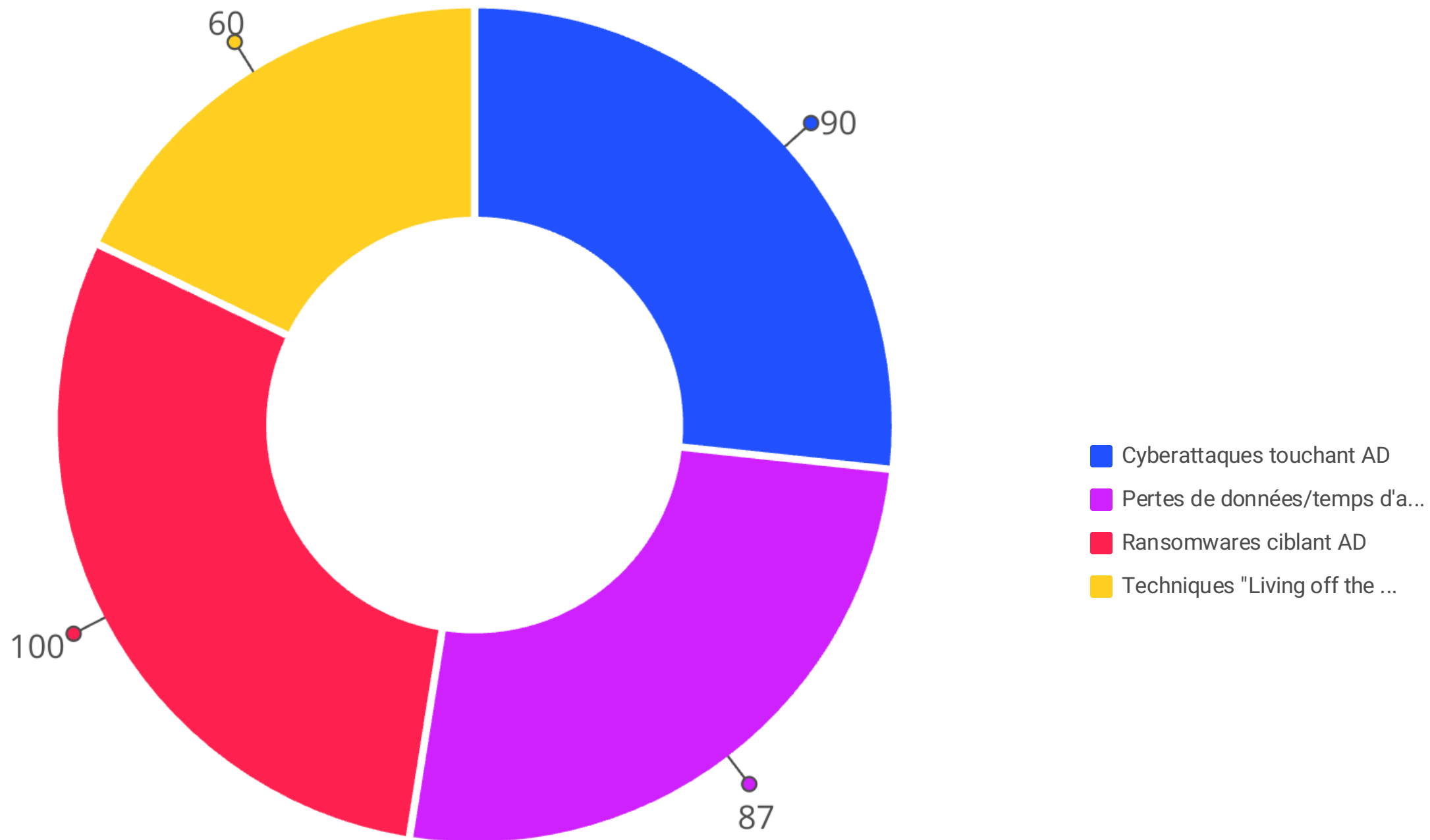
€4.5M

Coût

coût moyen incident AD

Constat critique : Active Directory est le "Saint Graal" des attaquants - une analyse de risque structurée est indispensable

Active Directory : La Cible N°1





Chronologie d'une attaque AD typique



3h

Compromission initiale



24h

Escalade privilèges



48h

Domain Admin



72h

Contrôle total

Impact Financier

€4.45M

Coût moyen d'une breach

+78%

Augmentation vs 2020

287 jours

Temps moyen de détection

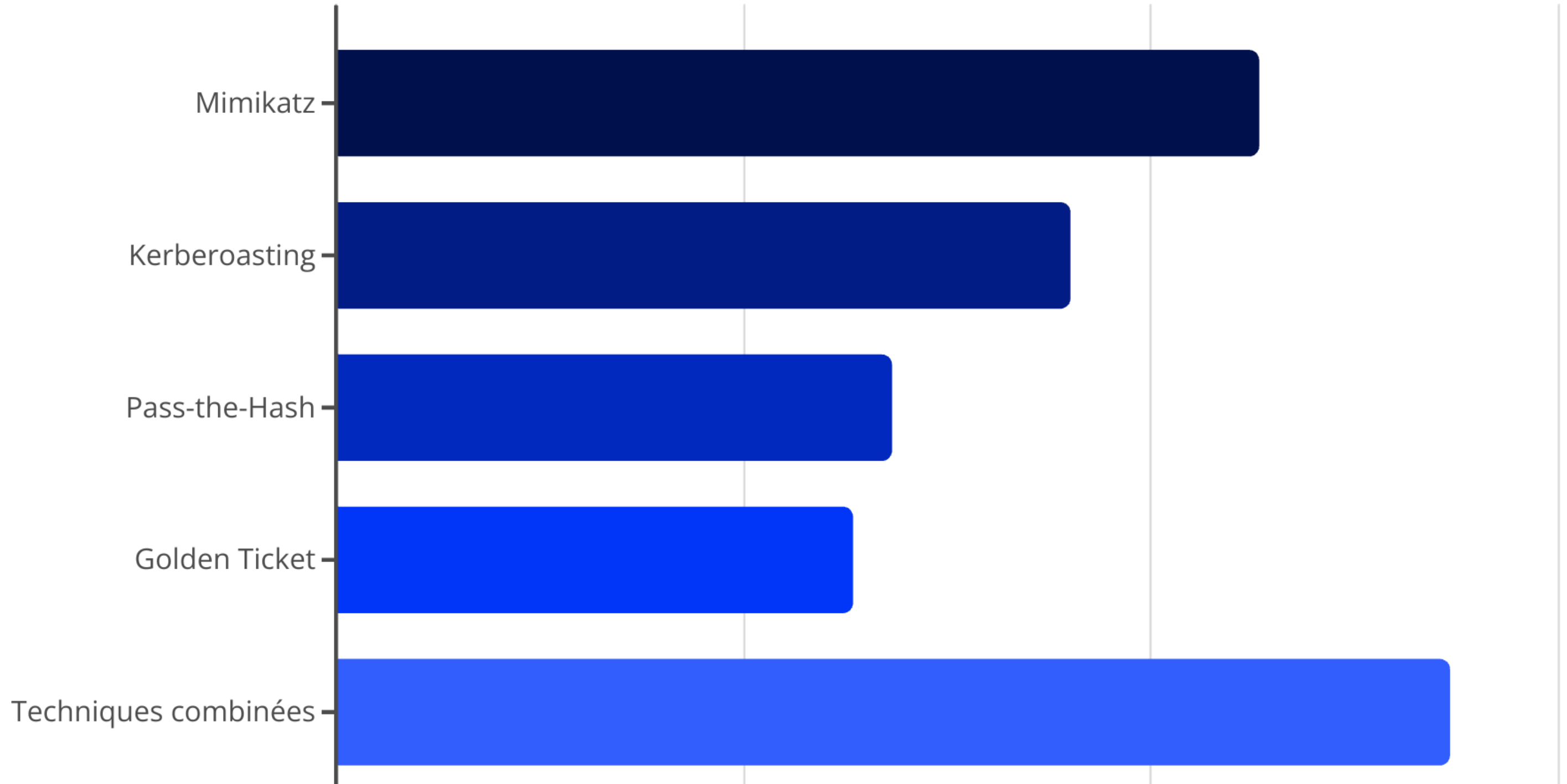
23%

Entreprises payent la rançon

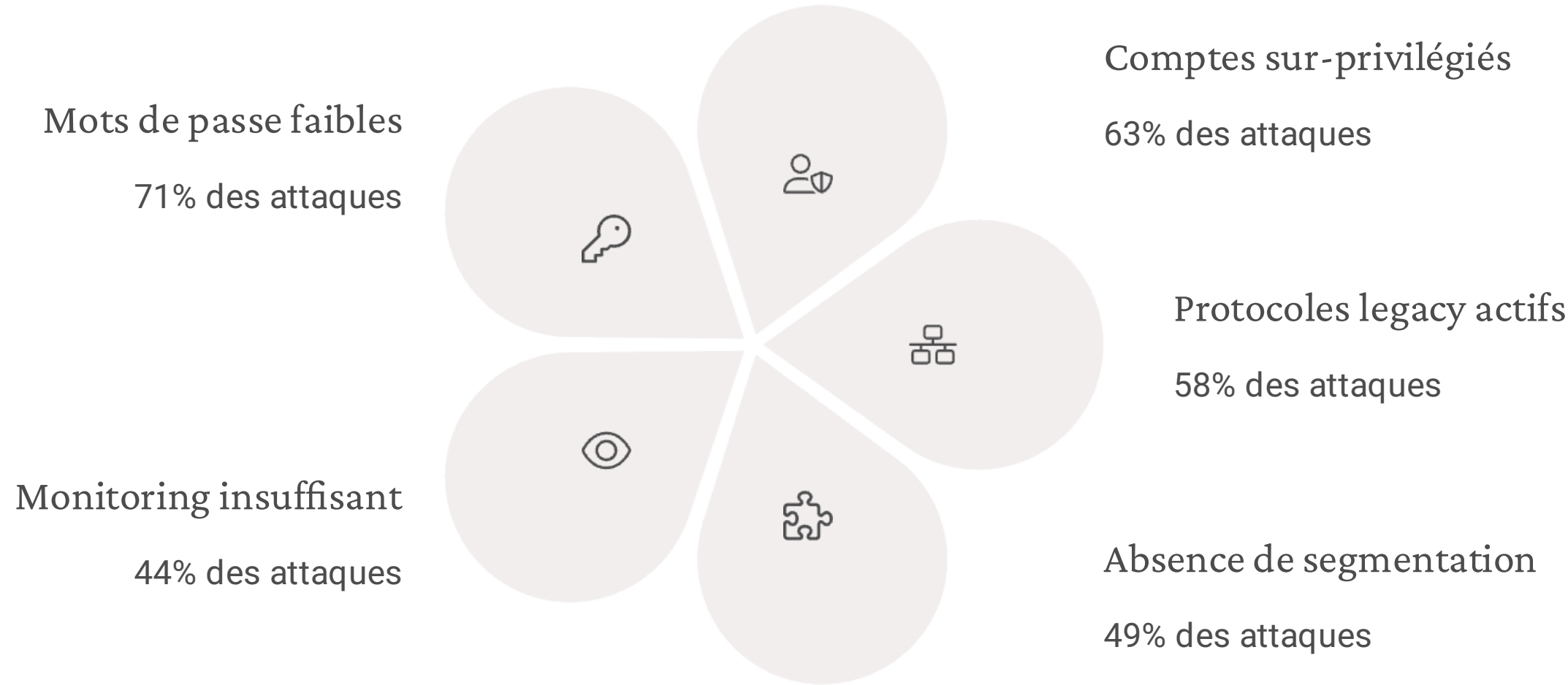
€8.2M

Record France (2023)

Techniques d'Attaque



Vulnérabilités Exploitées



Statistiques Critiques 2024-2025



9 attaques sur 10 touchent
Active Directory d'une
manière ou d'une autre



87% des attaques AD
provoquent des pertes de
données ou des temps d'arrêt
critiques



73% des entreprises ont au
moins une vulnérabilité
critique non corrigée dans AD



15 minutes suffisent pour compromettre une
Active Directory mal configurée



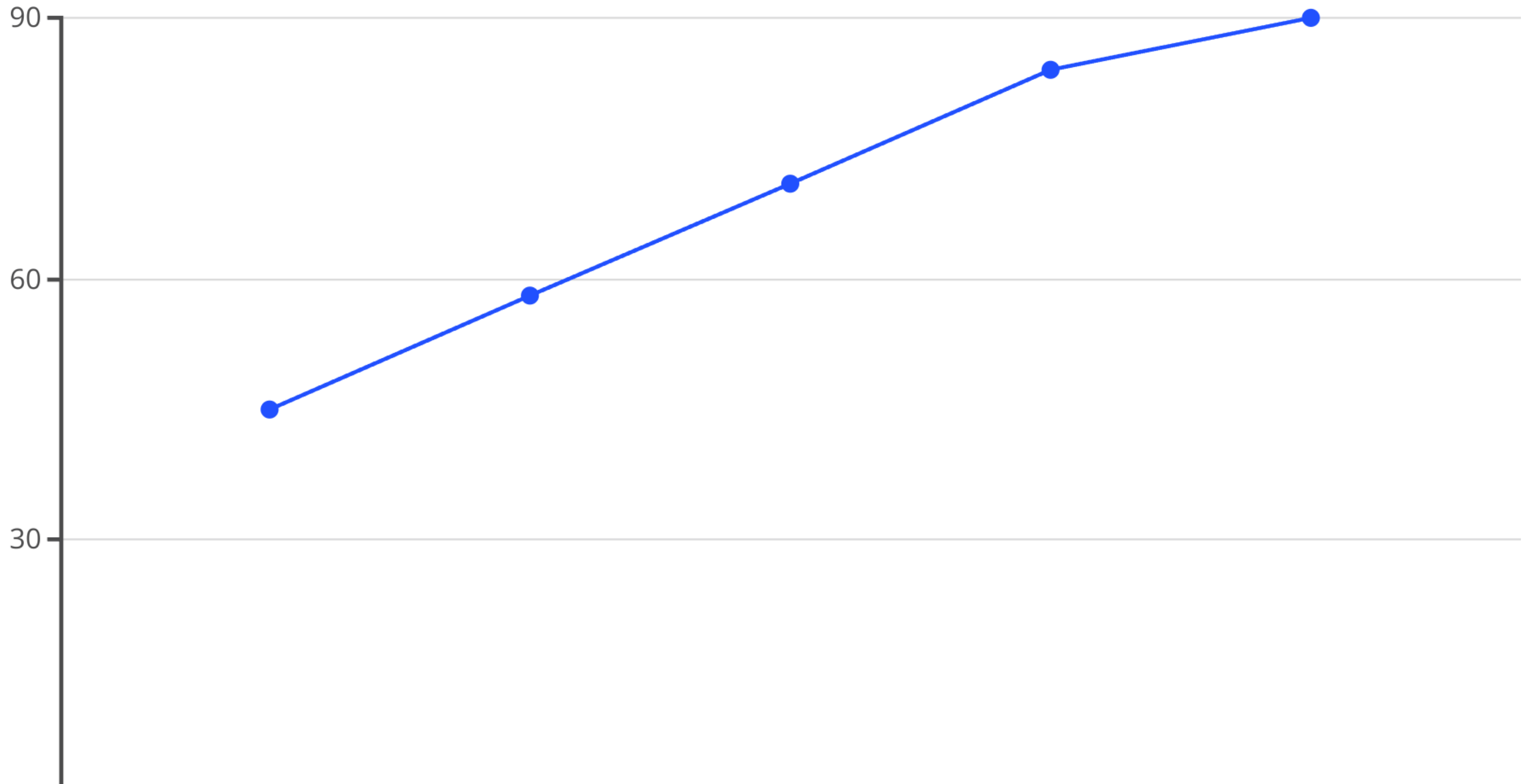
92% des ransomwares réussis ont exploité des
faiblesses AD



Top 10 des Groupes APT (Advanced Persistent Threat) ciblant AD

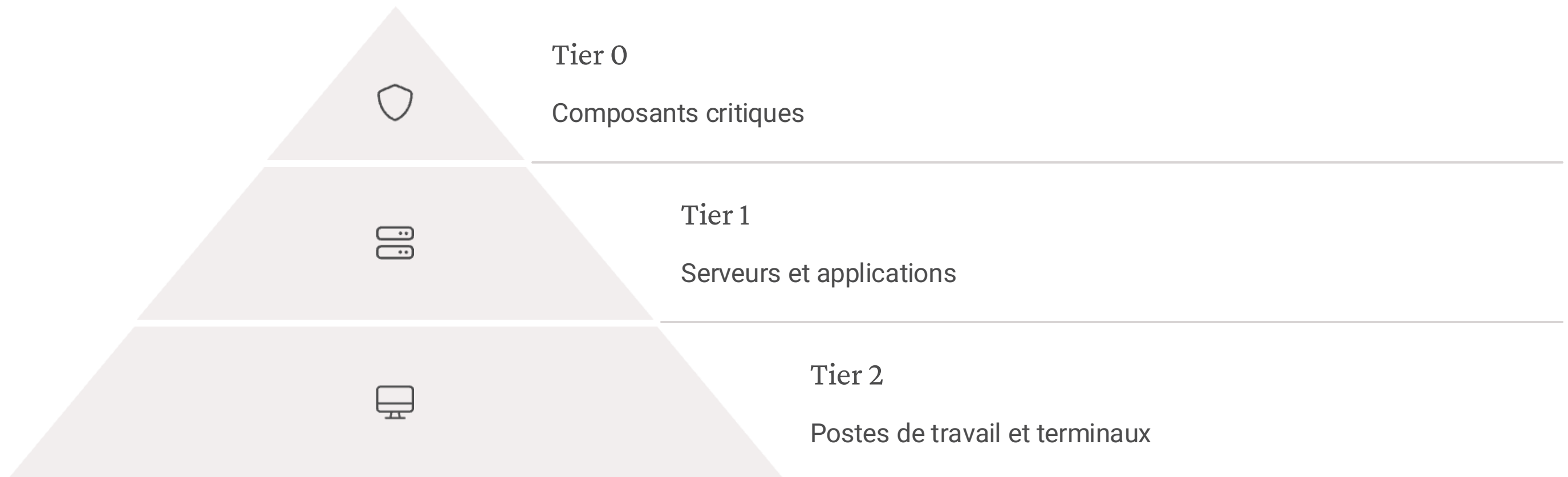
1. Lazarus Group	Corée du Nord - Finance/Crypto
2. APT28 (Fancy Bear)	Russie - Gouvernements
3. APT29 (Cozy Bear)	Russie - Espionnage
4. Carbanak	Finance - €1 milliard volé
5. APT1	Chine - Propriété intellectuelle
6. Equation Group	NSA - Cyber-espionnage
7. DarkHydrus	Moyen-Orient - Gouvernements
8. FIN7	Cybercrime - Retail/Hospitality
9. Cobalt Group	Banques - €1.2 milliard
10. Evil Corp	Ransomware - Dridex/WastedLocker

Évolution des Attaques AD (2020-2025)

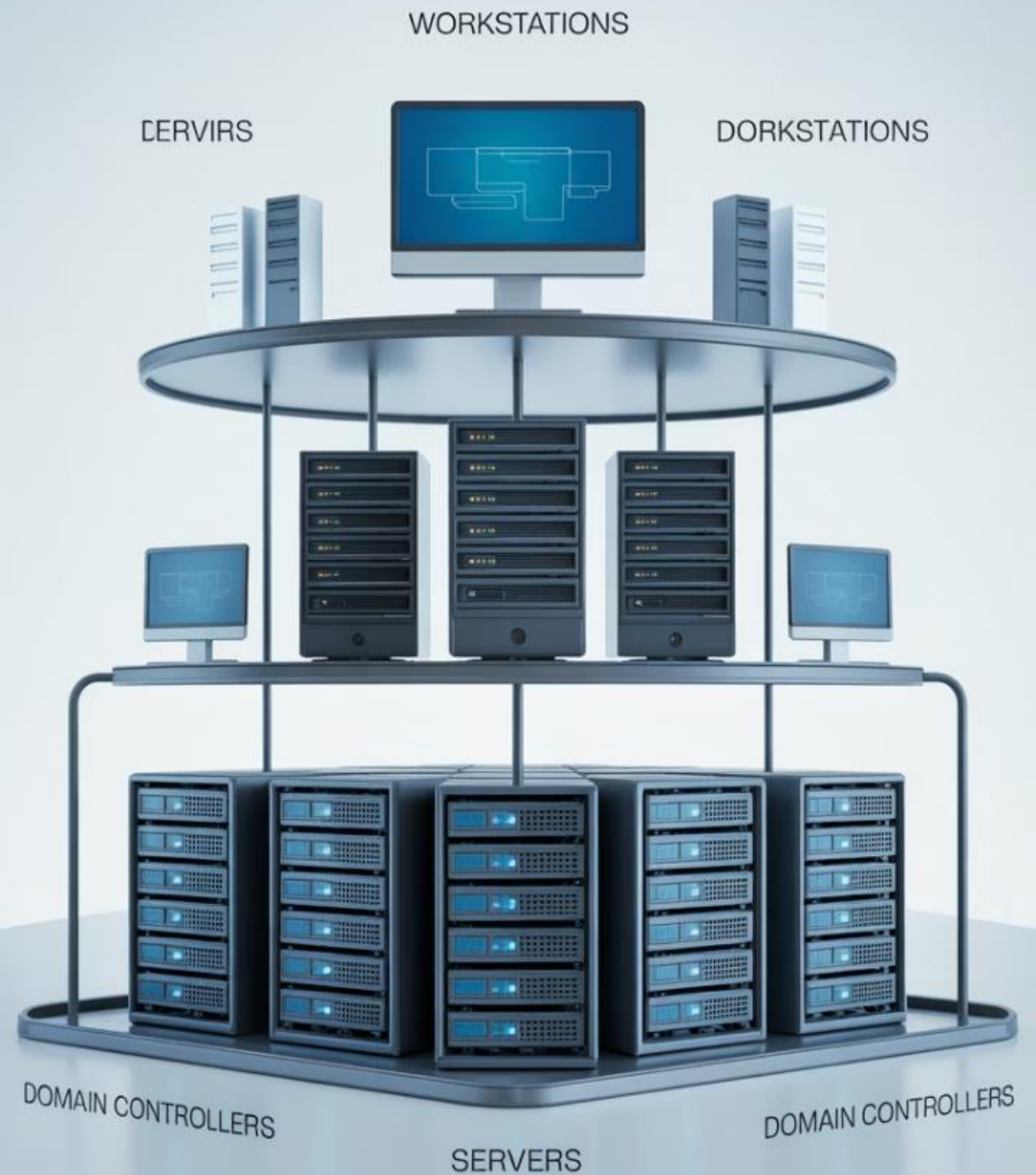


Le Tiering : Segmentation des niveaux d'accès

Le tiering consiste à segmenter les niveaux d'accès au sein de l'AD. La segmentation se fait en fonction de l'importance et de la sensibilité des composants. En règle générale, nous distinguons trois niveaux :



Le tiering permet donc d'isoler les couches d'administration et d'éviter les mouvements latéraux des attaquants. Cela passe par la mise en place d'une nouvelle organisation, de la délégation et du principe de moindre privilège.



Détails des niveaux de Tiering

Tier 0

Inclut les composants critiques. Par exemple les contrôleurs de domaine Active Directory, les serveurs PKI, et les systèmes de gestion des identités.

Tier 1

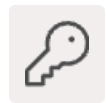
Comprend les serveurs et applications de l'entreprise, tels que les serveurs de gestion (SCCM, WSUS).

Tier 2

Regroupe les postes de travail des utilisateurs et les terminaux mobiles, qui sont les plus exposés aux risques.

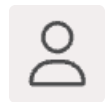
L'Hardening : Renforcement de la sécurité

L'hardening consiste à renforcer la sécurité des différents éléments de l'Active Directory. Cela peut inclure des éléments comme :



Stratégie de mot de passe

Le renforcement de la stratégie de mot de passe utilisateur



PSO

La mise en place de PSO en fonction de la population visée



Protocoles

La désactivation des anciens protocoles



Communication

Le renforcement des protocoles de communication

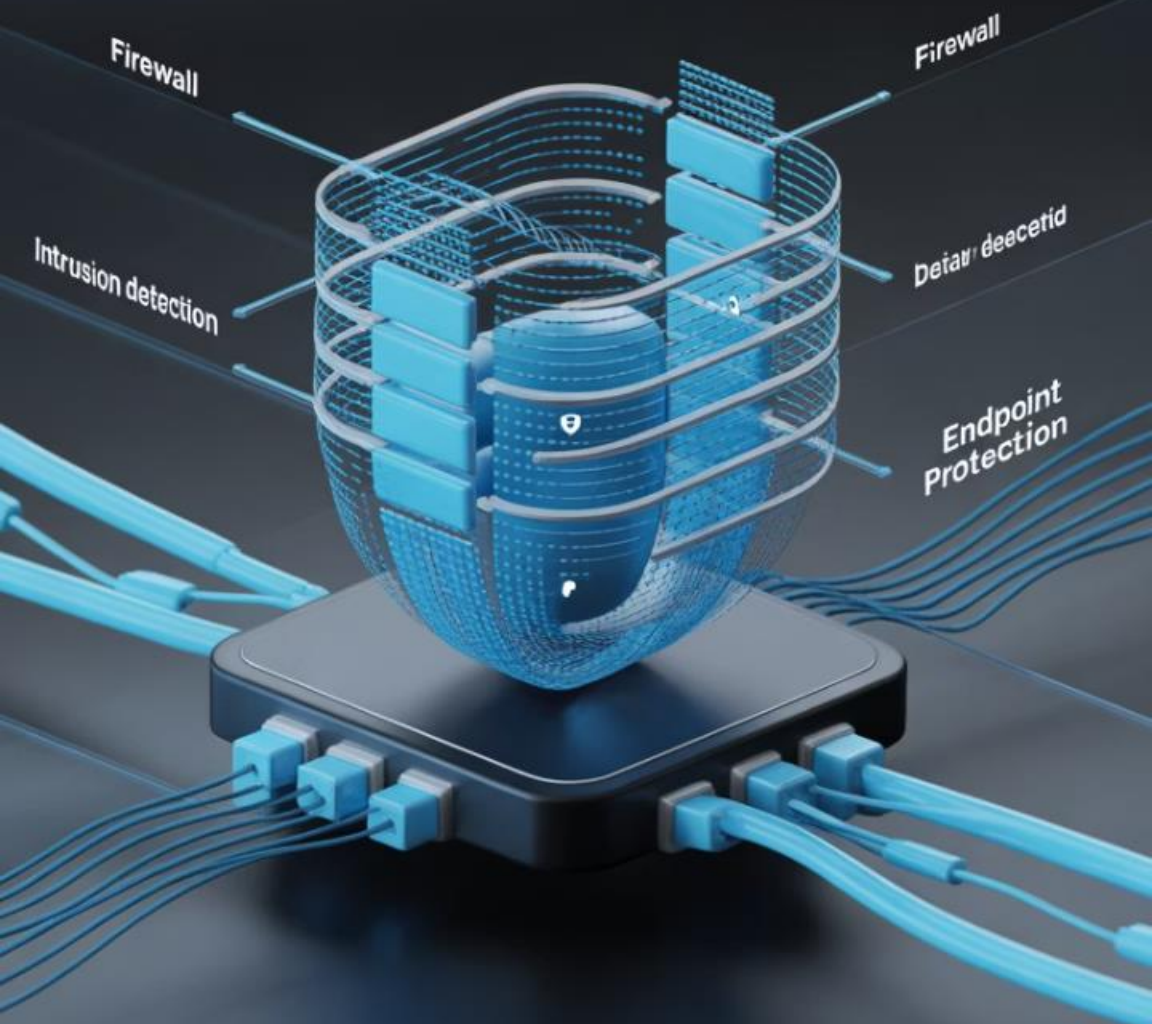
CYBERSECURITY FORTRESS



Layered Security Protection

A suite of tools and services that work together to protect your network and data from various threats. This comprehensive security solution includes advanced threat detection, intrusion prevention, and endpoint protection, all designed to provide a multi-layered defense against cyberattacks.

Activate Protection



Mesures d'Hardening supplémentaires



Silo d'authentification

La mise en place de silo d'authentification



Security baseline

La mise en place des security baseline de Microsoft

3

Solutions de protection

La mise en place d'AppLocker, Bitlocker ou LAPS



Restriction d'authentification

La mise en place de restriction d'authentification

Mesures d'Hardening complémentaires



Sécurité Logique

Définition

La sécurité logique concerne l'ensemble des moyens logiciels permettant d'assurer les DIC (Disponibilité, Intégrité et Confidentialité).

Exemples

Par exemple, les sauvegardes, les mises à jour, etc.





Sécurité Physique



Contrôle d'accès

La sécurité physique quant à elle implique la protection des serveurs et des infrastructures où l'AD est hébergé.



Protection

Cela garantit qu'ils sont à l'abri des accès non autorisés.

La Méthode EBIOS

Expression des Besoins et Identification des Objectifs de Sécurité



Socle de sécurité

Définir le périmètre et les enjeux



Sources de risque

Identifier les menaces



Scénarios stratégiques

Élaborer les scénarios



Scénarios opérationnels

Détailler les attaques



Traitement du risque

Définir les mesures

Objectifs d'EBIOS



Identifier et évaluer les risques cyber



Déterminer les mesures de sécurité nécessaires



Argumenter les décisions de sécurité



Suivre l'évolution du niveau de risque



Communiquer sur les risques

Avantages de la méthode



Approche structurée et méthodique



Vision stratégique et opérationnelle



Adaptable à tous contextes



Conforme ISO 27005



Reconnue par l'ANSSI

Cycle de vie

Analyse initiale complète

Amélioration continue



Révision annuelle

Mise à jour si changement majeur

Suivi continu des indicateurs



Active Directory : Contexte et Criticité

Pourquoi AD nécessite une analyse de risque approfondie

AD = Single Point of Failure

La compromission d'AD signifie la compromission totale de l'infrastructure IT

Rôle Central d'AD



Authentification

Tous les accès utilisateurs



Autorisation

Gestion des permissions



Configuration

GPO et paramètres



Services

DNS, DHCP, PKI



Applications

SSO et intégrations

Vulnérabilités Inhérentes



Protocoles legacy (NTLM, SMBv1)



Complexité des délégations



Dépendances multiples



Surface d'attaque étendue



Difficulté de monitoring

Impacts Business



Arrêt total de production possible



Vol de données sensibles



Usurpation d'identité massive



Non-conformité réglementaire



Perte de confiance clients



Évaluation de la criticité AD dans votre contexte

Critère	Niveau	Impact
Nombre d'utilisateurs	< 100 100-1000 1000-5000 > 5000	●●●
Applications critiques intégrées	< 5 5-20 20-50 > 50	●●●●
Données sensibles accessibles	Faible Moyen Élevé Critique	●●●●●

Application d'EBIOS à Active Directory

Méthodologie adaptée au contexte AD



Phase 1
Socle



Phase 2
Sources



Phase 3
Scénarios Strat.



Phase 4
Scénarios Op.



Phase 5
Traitement

Phase 1 : Socle de sécurité AD

□ Missions AD

- Authentifier les utilisateurs
- Autoriser les accès
- Gérer les identités
- Appliquer les politiques
- Auditer les activités

□ Valeurs métier

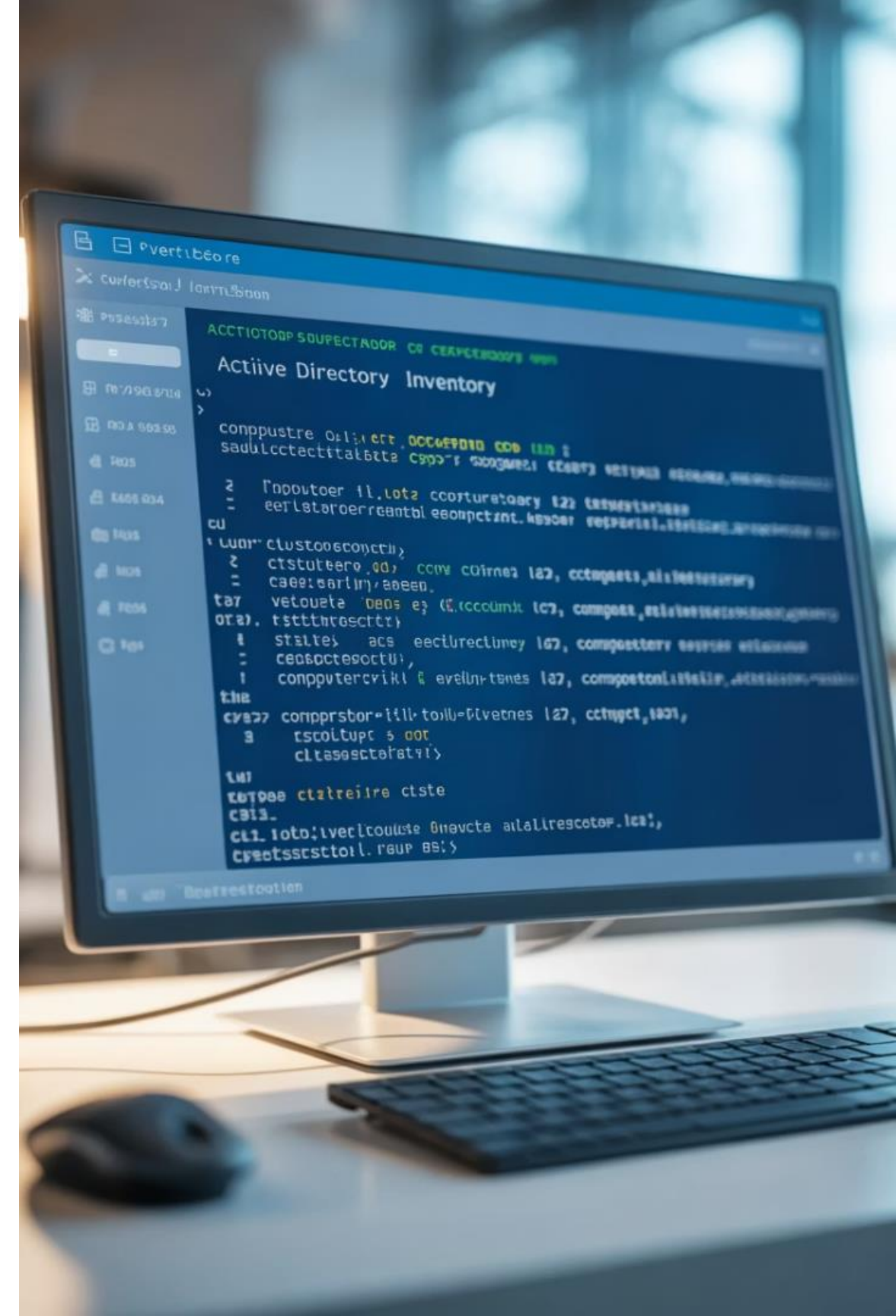
- Disponibilité 24/7
- Intégrité des identités
- Confidentialité des accès
- Traçabilité des actions
- Conformité réglementaire

□ Biens supports

- Contrôleurs de domaine
- Infrastructure PKI
- Serveurs RADIUS/NPS
- Systèmes de sauvegarde
- Liens de réplication

Script d'inventaire pour Phase 1 EBIOS

```
# Script d'inventaire pour Phase 1 EBIOS# Collecte des informations AD pour l'analyse# Informations Forest/DomainGet-ADForest | Select-Object Name, ForestMode, RootDomain, SchemaMasterGet-ADDomain | Select-Object Name, DomainMode, PDCEmulator, RIDMaster# Inventaire des DCsGet-ADDomainController -Filter * | Select-Object Name, IPv4Address, OperatingSystem, IsGlobalCatalog# Statistiques objets@{ Users = (Get-ADUser -Filter *).Count Computers = (Get-ADComputer -Filter *).Count Groups = (Get-ADGroup -Filter *).Count OUs = (Get-ADOrganizationalUnit -Filter *).Count}# Comptes privilégiésGet-ADGroupMember -Identity "Domain Admins" -Recursive | Select-Object Name, SamAccountName, ObjectClass
```



Phase 2 : Sources de risque AD

Cartographie des menaces AD

☐ Menaces internes

- Administrateurs malveillants
- Utilisateurs compromis
- Prestataires avec accès
- Mouvements latéraux

☐ Menaces externes

- APT (Advanced Persistent Threat)
- Ransomware gangs
- Hacktivistes
- Cybercriminels opportunistes

☐ Vulnérabilités techniques

- Protocoles legacy
- Misconfigurations
- Patches manquants
- Mots de passe faibles

Méthode MITRE ATT&CK

Méthode

Utiliser MITRE ATT&CK pour identifier systématiquement les techniques adverses ciblant AD

Mitre ATT&CK for Active Directory





Phase 3 : Scénarios stratégiques

AD

Matrice de risque AD

Impact →	Faible	Moyen	Élevé	Critique
Très probable	PS	PH	RW	APT
Probable	-	LL	KB	GT
Possible	-	SR	DC	AH
Peu probable	-	-	DS	SK

Strategic Attack Scenarios against Active Directory



Scénarios Stratégiques



Compromission totale

Attaquant obtient Domain Admin

Impact : Critique - Contrôle total

Vraisemblance : Moyenne



Vol d'identités

Exfiltration base AD

Impact : Élevé - Données sensibles

Vraisemblance : Élevée



Déni de service

AD rendu indisponible

Impact : Critique - Arrêt production

Vraisemblance : Faible

Phase 4 : Scénarios opérationnels AD

Exemple : Kill Chain "Compromission Domain Admin"



Bloodhound



Simulation de détection des chemins d'attaque

```
# Simulation de détection des chemins d'attaque (BloodHound-like)#  
Identifier les chemins vers Domain Admin# Recherche des comptes avec  
délégation non contrainteGet-ADComputer -Filter {TrustedForDelegation -eq  
$true} | Select-Object Name, DNSHostName, OperatingSystem# Comptes de  
service avec SPN (Kerberoastable)Get-ADUser -Filter {ServicePrincipalName -  
ne "$null"} -Properties ServicePrincipalName | Where-Object {$_.Enabled -eq  
$true} | Select-Object SamAccountName, ServicePrincipalName# Groupes avec  
membres privilégiés indirects$PrivGroups = @("Domain Admins", "Enterprise  
Admins", "Schema Admins")ForEach ($Group in $PrivGroups) { Get-  
ADGroupMember -Identity $Group -Recursive | Select-Object Name, ObjectClass,  
@{N="ViaGroup";E={$Group}}}
```

Phase 5 : Traitement du risque AD

□ Mesures préventives

- Tier Model / Red Forest
- Privileged Access Workstations
- Just-In-Time administration
- Désactivation protocoles legacy
- Hardening configurations

□ Mesures de détection

- SIEM avec use-cases AD
- Microsoft ATA/ATP
- Honey tokens
- Behavioral analytics
- Threat hunting régulier

□ Mesures de réaction

- Playbooks incidents AD
- Isolation automatique
- Reset krbtgt d'urgence
- Forensics AD
- Communication de crise

Active Directory Risk Treatment Strategy

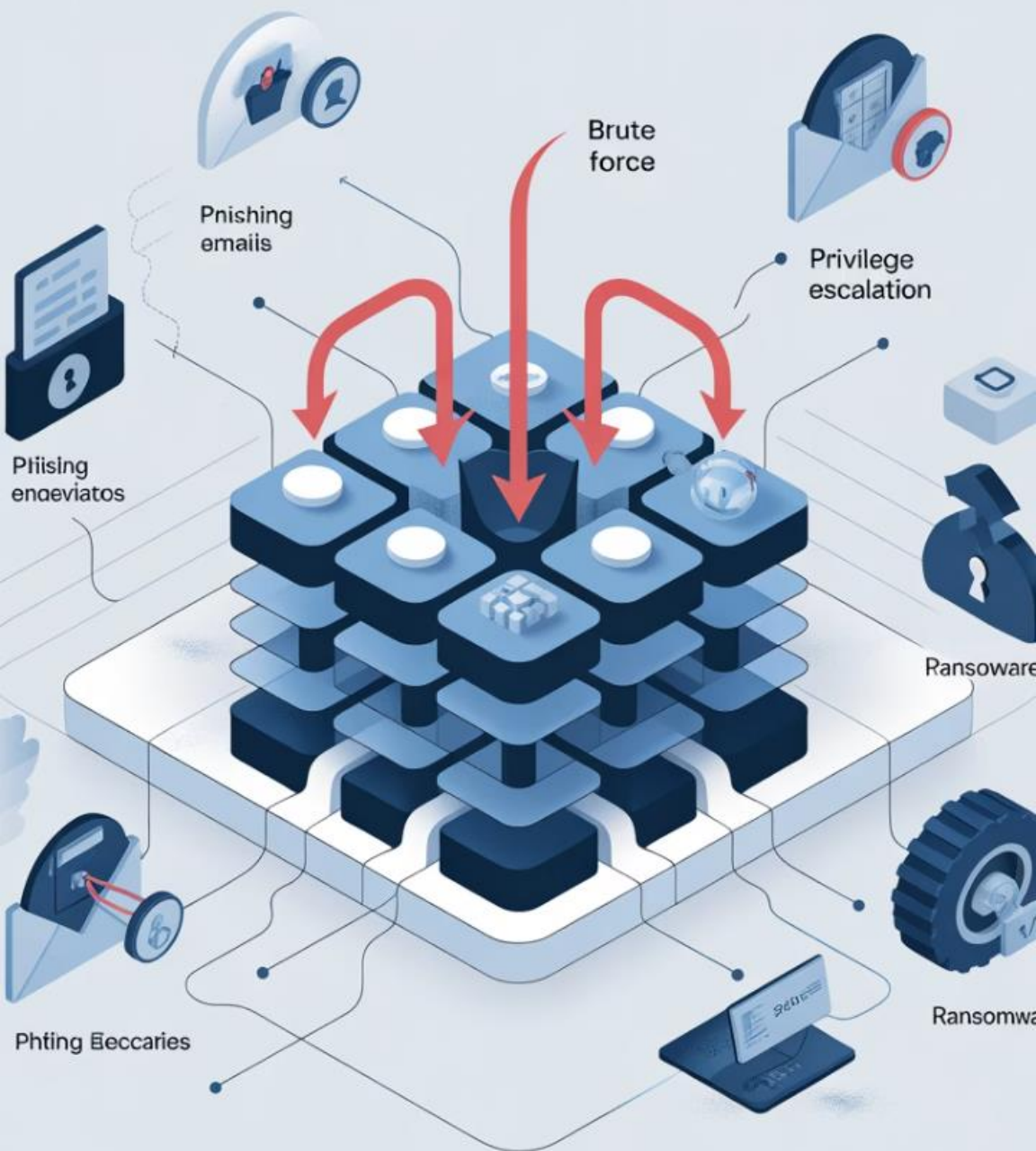


Stratégie de traitement du risque

Stratégie recommandée

Combiner réduction (hardening), évitement (architecture), transfert (cyber-assurance) et acceptation (risque résiduel)

Active Directory Security Risk Scenarios



Scénarios de Risque Détaillés

Analyse approfondie des menaces AD avec EBIOS



Ransomware



Menace Interne

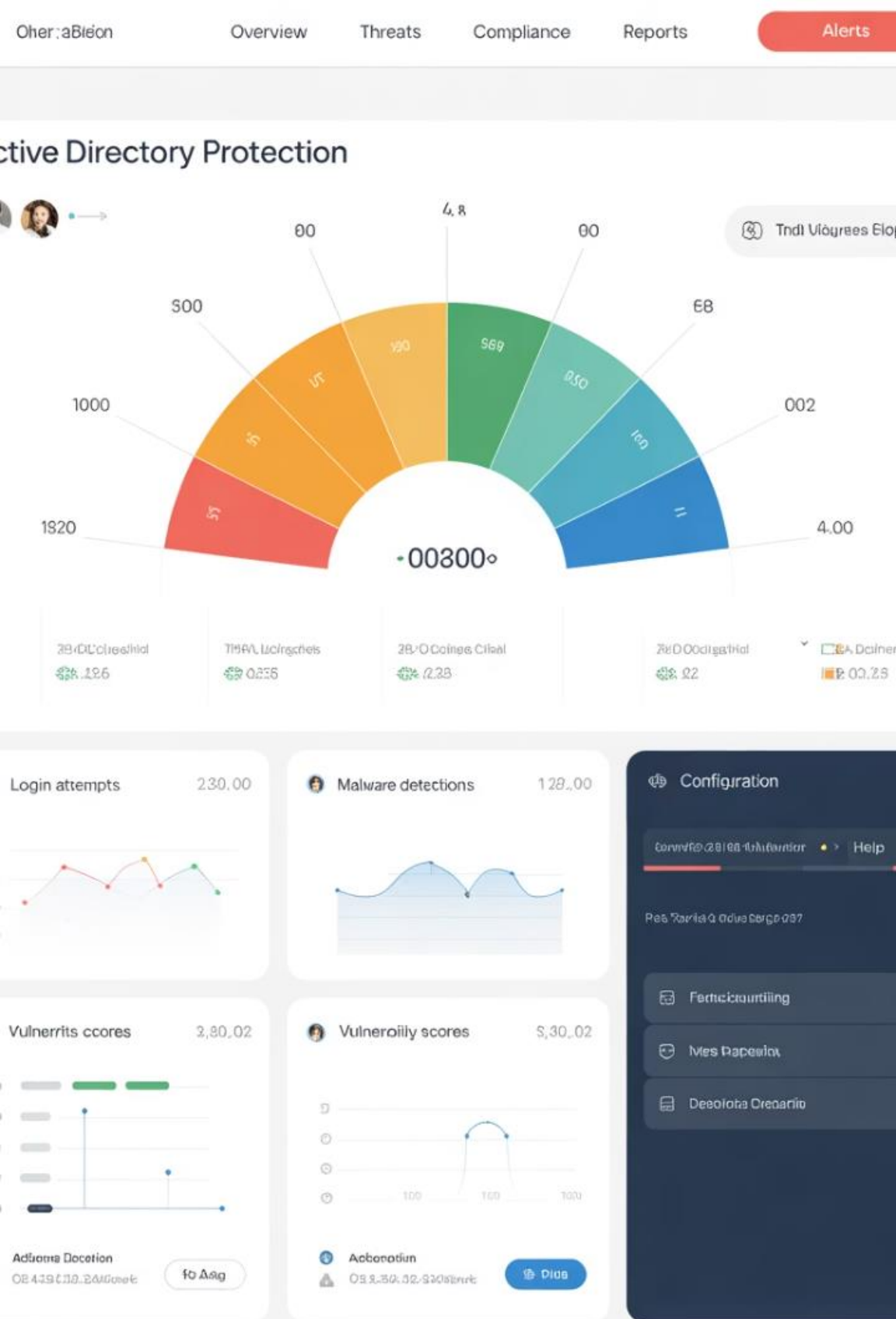


Supply Chain



APT

Sélectionnez un scénario pour voir l'analyse EBIOS complète



Statistiques des scénarios

12

Scénarios critiques
identifiés

47

Modes opératoires
recensés

156

Mesures de sécurité

€2.3M

Budget sécurité AD

Top 3 des scénarios critiques



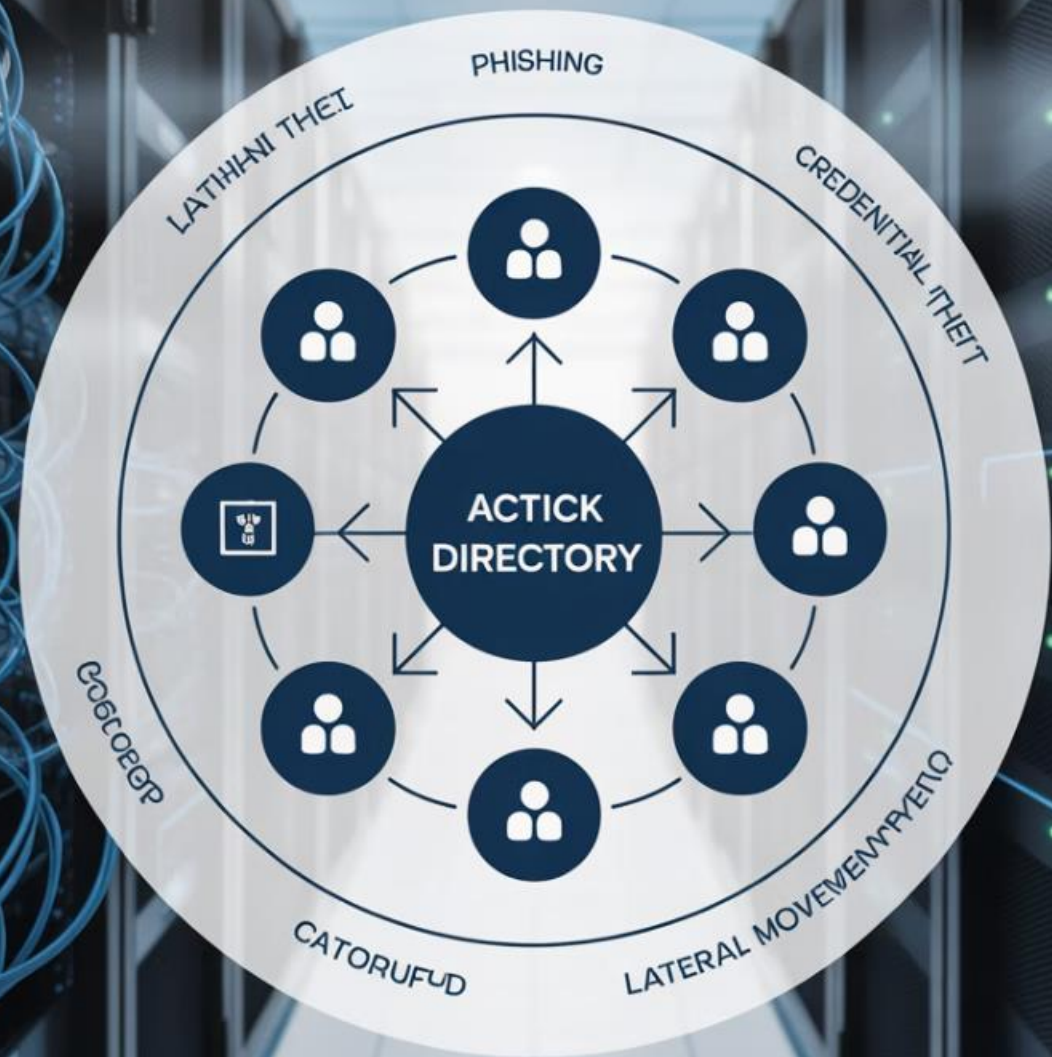
Compromission Domain
Admin via Kerberoasting
+ Pass-the-Ticket



Ransomware avec
propagation via GPO
malveillante

3

Exfiltration silencieuse via DCSync par APT



Mesures de Sécurité EBIOS pour AD

Plan d'action issu de l'analyse de risque



Quick Wins



Architecture



Détection



Réponse



Roadmap

Quick Wins - Mesures immédiates

□ Semaine 1

- ✓ Désactiver SMBv1
- ✓ Activer audit avancé
- ✓ Implémenter LAPS
- ✓ Restreindre RDP
- ✓ Scanner vulnérabilités

□ Mois 1

- ✓ Protected Users group
- ✓ Désactiver LLMNR/NetBIOS
- ✓ GPO hardening baseline
- ✓ Inventaire comptes service
- ✓ Formation équipes

□ Trimestre 1

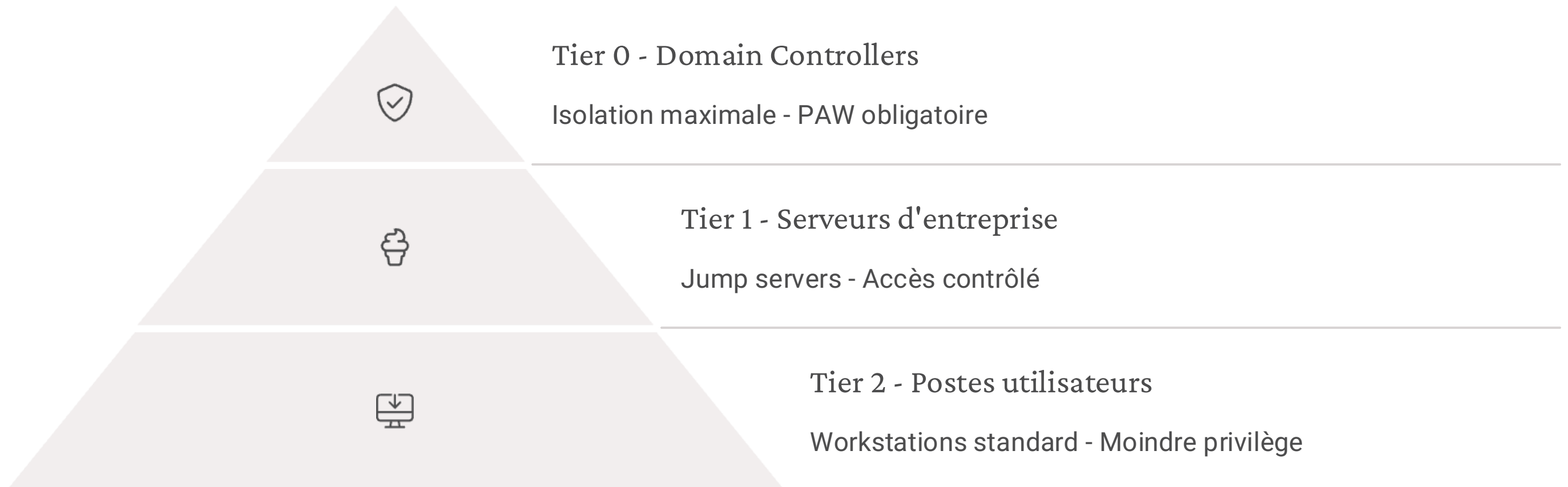
- ✓ Credential Guard
- ✓ Azure AD Connect sécurisé
- ✓ PKI renforcée
- ✓ MFA administrateurs
- ✓ Segmentation réseau

Script Quick Win - Audit et Hardening de base

```
# Script Quick Win - Audit et Hardening de base# À exécuter sur tous les DCs# 1. Configuration audit de sécuritéauditpol /set /category:"Account Logon" /success:enable /failure:enableauditpol /set /category:"Account Management" /success:enable /failure:enableauditpol /set /category:"DS Access" /success:enable /failure:enableauditpol /set /category:"Logon/Logoff" /success:enable /failure:enable# 2. Désactivation protocoles vulnérables# SMBv1Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force# LLMNRNew-ItemProperty -Path "HKLM:\\SOFTWARE\\Policies\\Microsoft\\Windows NT\\DNSClient" \ -Name "EnableMulticast" -Value 0 -PropertyType DWORD -Force# 3. Configuration sécurité KerberosSet-ADDefaultDomainPasswordPolicy \ -ComplexityEnabled $true \ -MinPasswordLength 14 \ -MaxPasswordAge "60.00:00:00" \ -LockoutThreshold 5 \ -LockoutDuration "00:30:00"
```

Mesures architecturales

Modèle de sécurité en couches (Tiering Model)



Mesures de détection avancées

□ Monitoring continu

- SIEM avec règles AD spécifiques
- Microsoft Defender for Identity
- Surveillance honey tokens
- Analyse comportementale
- Alertes temps réel

□ Use Cases prioritaires

- Détection Kerberoasting
- DCSync attempts
- Golden/Silver tickets
- Mouvements latéraux
- Élévations privilèges

□ KPIs de détection

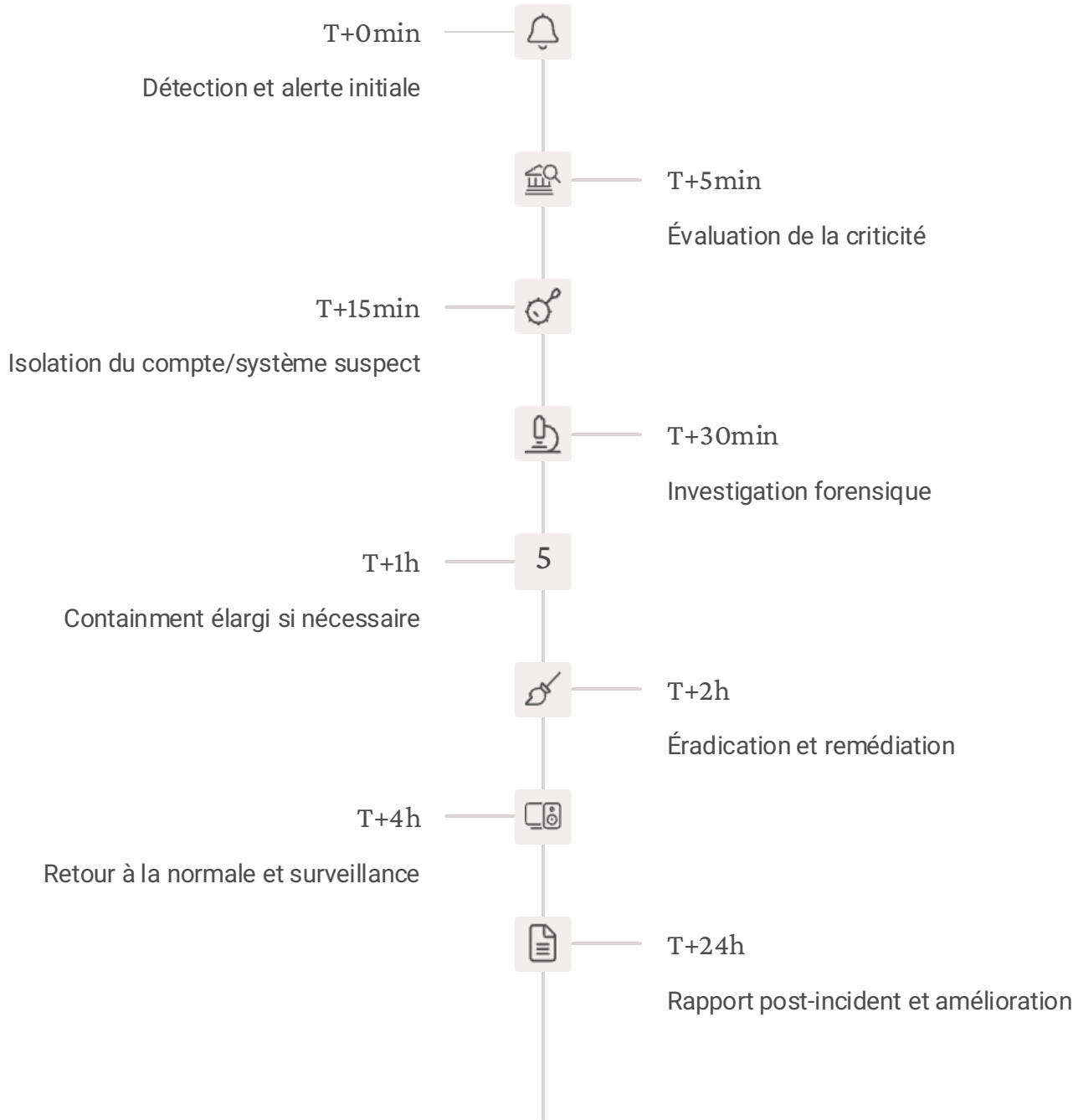
- MTTD < 15 minutes
- Couverture MITRE 85%
- False positive < 5%
- Alertes critiques < 1h
- Investigation < 4h

Requêtes Azure Sentinel pour détection avancée AD

```
// Requêtes Azure Sentinel pour détection avancée AD// Détection de KerberoastingSecurityEvent| where EventID == 4769| where  
ServiceName !endswith "$" and ServiceName != "krbtgt"| where TicketEncryptionType == "0x17"| summarize StartTime =  
min(TimeGenerated), EndTime = max(TimeGenerated), ServiceCount = dcount(ServiceName), ServiceNames = make_set(ServiceName) by  
Account| where ServiceCount > 5| project StartTime, EndTime, Account, ServiceCount, ServiceNames// Détection de  
DCSyncSecurityEvent| where EventID == 4662| where ObjectType == "19195a5b-6da0-11d0-afd3-00c04fd930c9"| where AccessMask in  
("0x100", "0x100000000")| where SubjectUserName !endswith "$"| project TimeGenerated, SubjectUserName, ObjectName, AccessMask
```

Plan de réponse aux incidents AD

Playbook : Compromission AD suspectée



Criticité temps

Criticité temps

En cas de compromission Domain Admin confirmée, considérer le reset immédiat de krbtgt et l'isolation de tous les DCs





Roadmap de sécurisation EBIOS

Plan sur 18 mois

Phase	Période	Actions clés	Budget
1. Fondations	M1-M3	Quick wins, Audit, Baseline	150k€
2. Architecture	M4-M9	Tier model, PAW, Segmentation	500k€
3. Détection	M7-M12	SIEM, MDI, SOC integration	350k€
4. Résilience	M10-M15	Red Forest, JIT/JEA, Zero Trust	800k€
5. Maturité	M13-M18	Threat hunting, Amélioration continue	300k€

Laboratoire Pratique EBIOS-AD

Mise en application de la méthode



Lab 1: Analyse EBIOS Express

Réaliser une analyse EBIOS simplifiée de votre AD

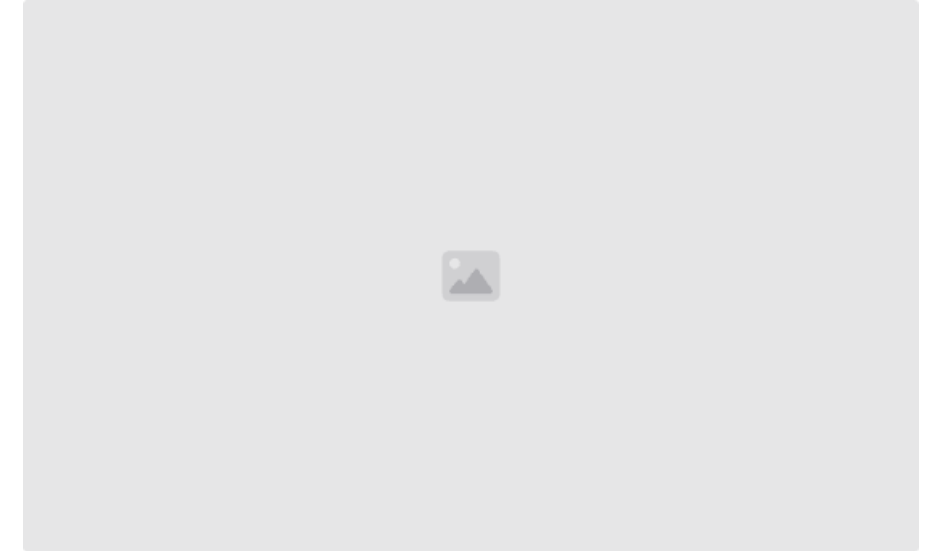
- Identifier 5 valeurs métier critiques
- Lister 10 biens supports essentiels
- Définir 3 scénarios de risque majeurs
- Évaluer vraisemblance et impact
- Proposer 5 mesures prioritaires



Lab 2: Matrice de Risque AD

Construire votre matrice de risque spécifique

- Utiliser le template fourni
- Placer vos scénarios identifiés
- Ajuster selon votre contexte
- Identifier zones rouges
- Prioriser les actions



Lab 3: Plan d'Action

Créer votre roadmap de sécurisation

- Partir des risques identifiés
- Définir mesures court terme
- Planifier actions long terme
- Estimer efforts et coûts
- Créer planning projet