THEIA SECURITY DATA NETWORK VOTRE

PARTENAIRE CYBERSECURITE

THEIA
SECURITY DATA NETWORK

WWW.THEIA-SDN.COM

Nos solutions de cybersécurités avancées

Découvrez notre gamme complète de solutions conçues pour protéger efficacement vos entreprises et collectivités

GUARDIA
BY THEIA-SDN

YAMI
BY THEIA-SDN

SPARTA
BY THEIA-SDN

ATTAQUE

SOC/SIEM souverain

Notre SOC, basé en France, assure une protection complète avec EDR et SIEM, une réponse rapide aux incidents, une détection en temps réel du chiffrement, plus de 3000 règles personnalisées pour une détection fine, une analyse des vulnérabilités et une conservation des données sur six mois.

SURVEILLANCE

Fuite de données sur le darknet

Notre système offre des alertes immédiates en cas de détection de fuites, identifie les données exposées pour des contre-mesures rapides, anticipe les cyberattaques par l'analyse des forums, et assure un accompagnement des services enquêteurs

www.theia-sdn.com

DEFENSE

Audits et tests d'intrusions

Notre service allie souveraineté technique et humaine, avec une expertise éprouvée et des certifications reconnues. Nous proposons un outillage packagé en interne et un entraînement régulier aux techniques de contournement. Les auditeurs ont accès à notre SOC/SIEM GUARDIA pour enrichir les analyses d'attaques

THEIA
SECURITY DATA NETWORK

GUARDIA

BY THEIA-SDN

Notre suite logicielle dédiée aux Centres d'Opérations de Sécurité, clé en main, dédiée aux entreprises et collectivités

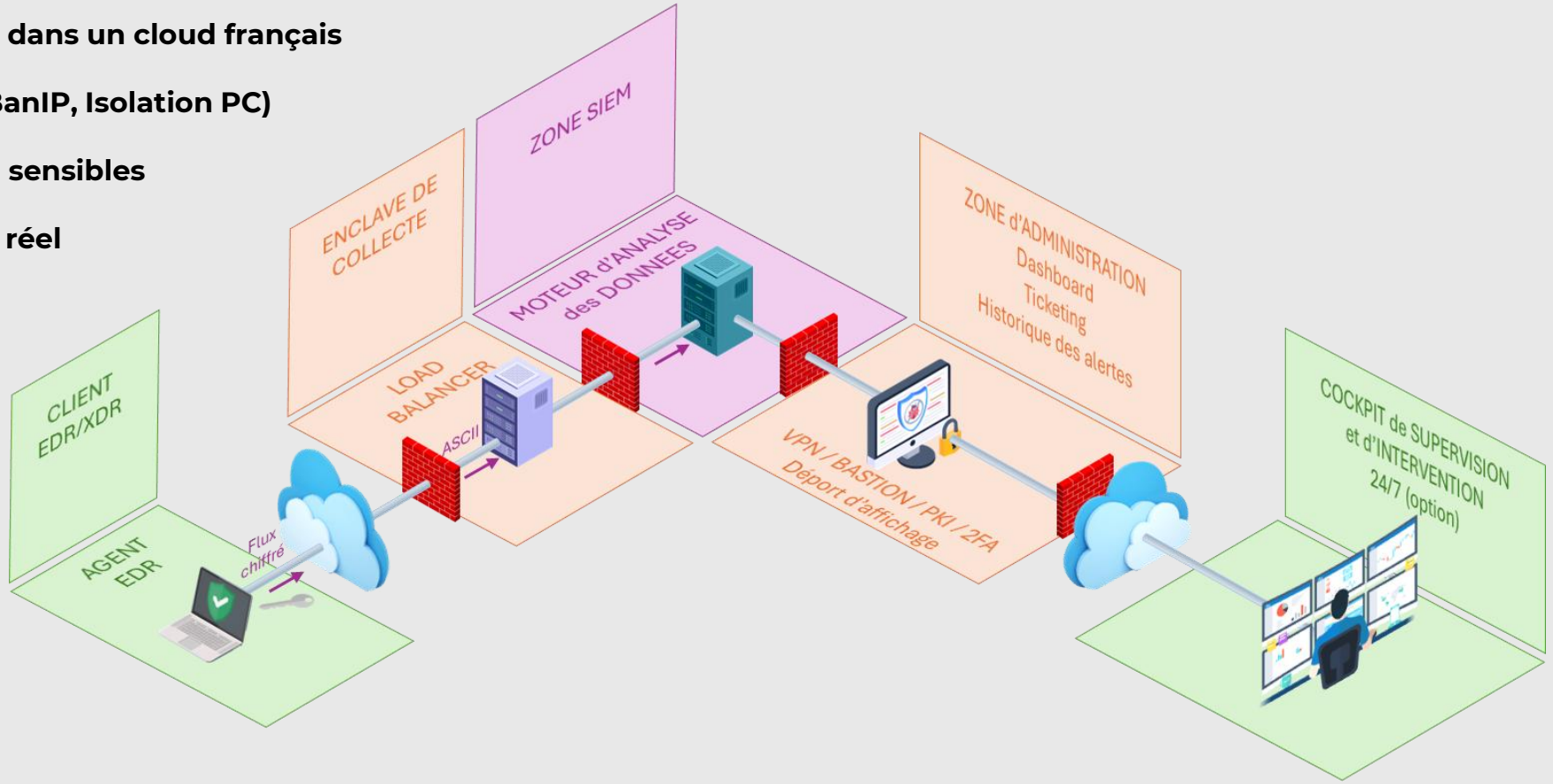
THEIA

SECURITY DATA NETWORK

Avec GUARDIA, votre SOC dédié localisé en France qui garantit une souveraineté technique et humaine

Respect du référentiel PDIS (ANSSI)

- EDR et SIEM souverains
- Collecte de tous les logs stockés dans un cloud français
- Réponse à incidents (Kill Proc., BanIP, Isolation PC)
- Intégrité des fichiers ou dossiers sensibles
- Détection chiffrement en temps réel
- >3000 règles personnalisées
- Analyse des configurations
- Gestion des vulnérabilités
- 6 mois d'historisation

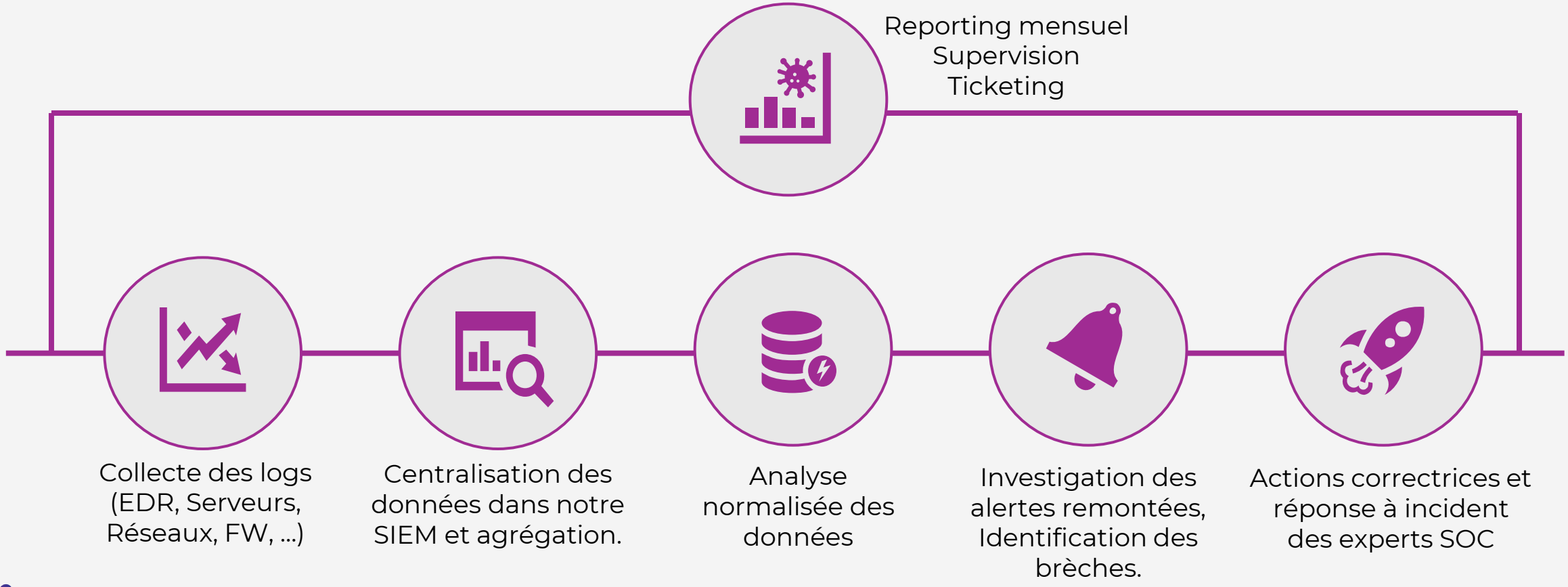


THEIA
SECURITY DATA NETWORK

Le SOC (Security Operation Center) est la tour de contrôle qui surveille et détecte les suspicions d'attaques

THEIA
SECURITY DATA NETWORK

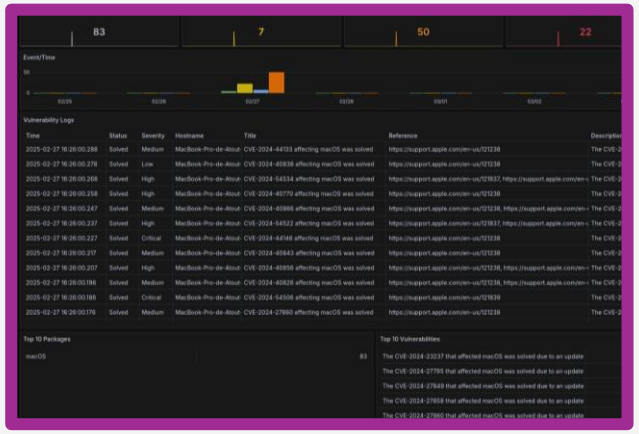
Notre SIEM - Security information and event management



THEIA
INFORMATION TECHNOLOGY

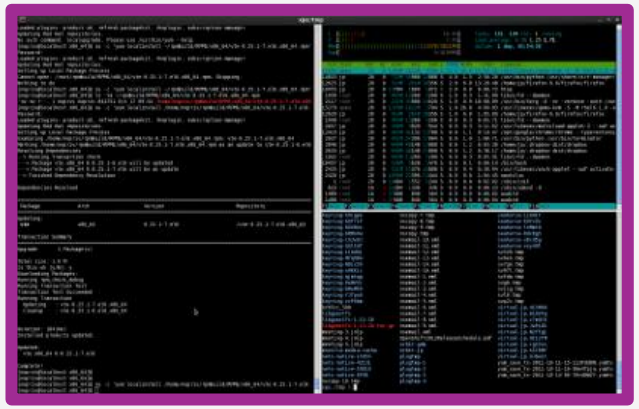
Plus que des mots : démonstration

Console SIEM

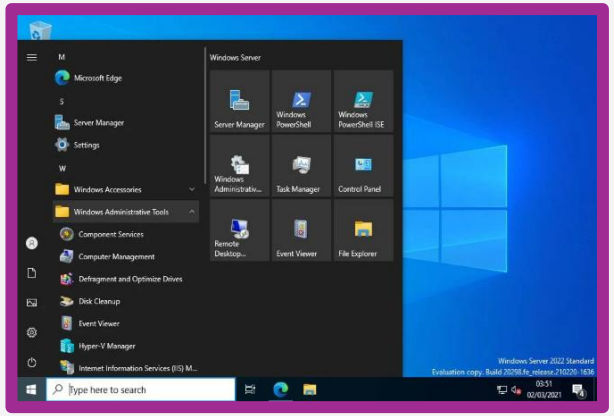


- Détection
- Tentatives d'intrusions
- Isolation de la machine
- Historisation des évènements

Cybercriminel



- Attaques depuis Internet
- Brute force sur le compte Admin
- Requêtes sur l'Active Directory
- Envoi d'un ransomware
- Instructions en Pipe SMB pour contourner l'AntiVirus

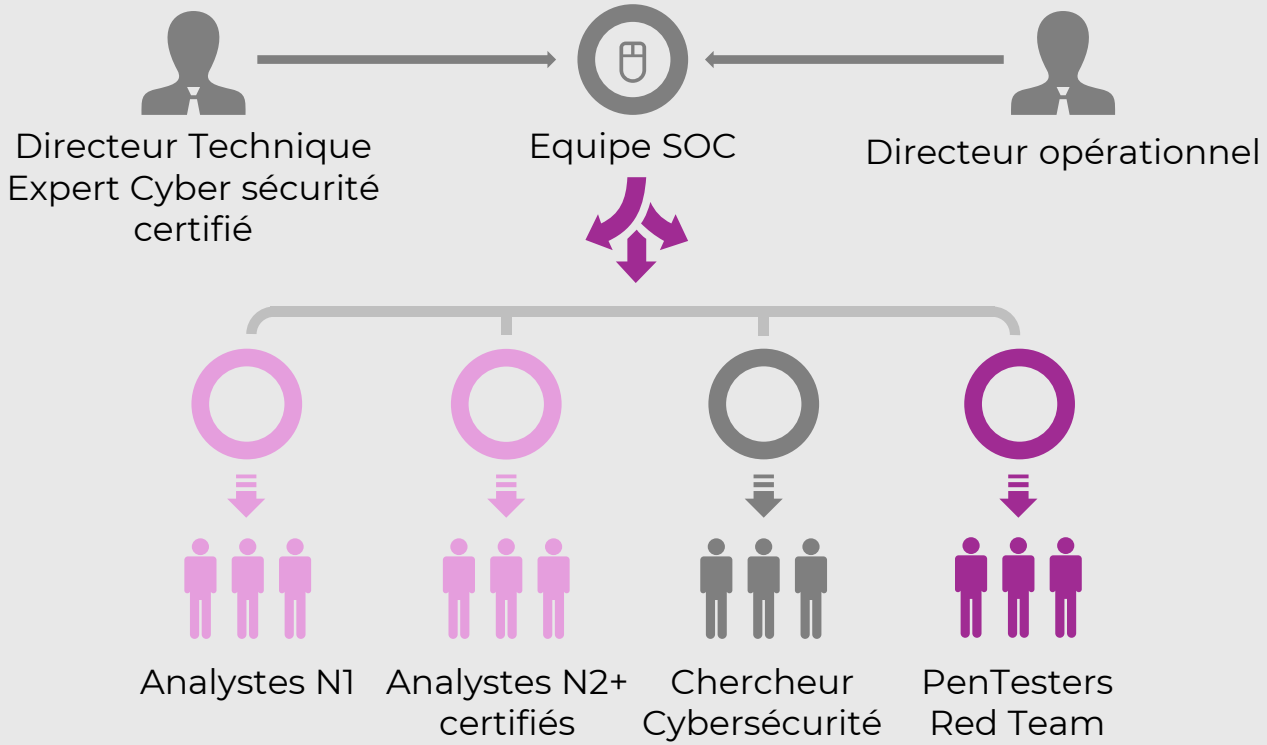


- Windows Server 2022
- Active Directory déployée
- Agent EDR
- Antivirus Windows Defender

Serveur de production

THEIA
SECURITY DATA NETWORK

Organisation de notre équipe d'experts SOC GUARDIA



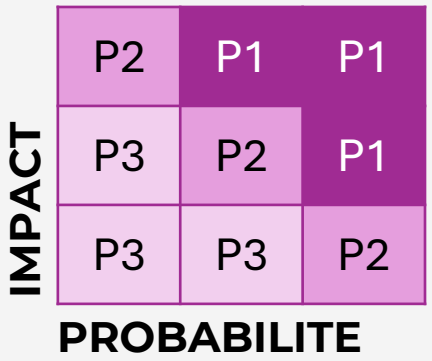
- **Une équipe certifiée et expérimentée**
- **Une organisation éprouvée**
- **Des engagements clairs**
- **Des analystes N1 qui se forment aux PenTests**
- **En cours de qualification PASSI**
- **Comité de pilotage trimestriel**

THEIA
SECURITY DATA NETWORK

Nos engagements de niveaux de service SLAs

Criticité de l'incident	Evènement *	Prise en compte après évènement **	Information client après prise en compte ***	Plage de service ****
P1	T0	+ 30 min	+15 min	9h00 – 18h00
P2		+ 60 min	+ 60 min	9h00 – 18h00
P3		+ 120 min	+ 120 min	9h00 – 18h00

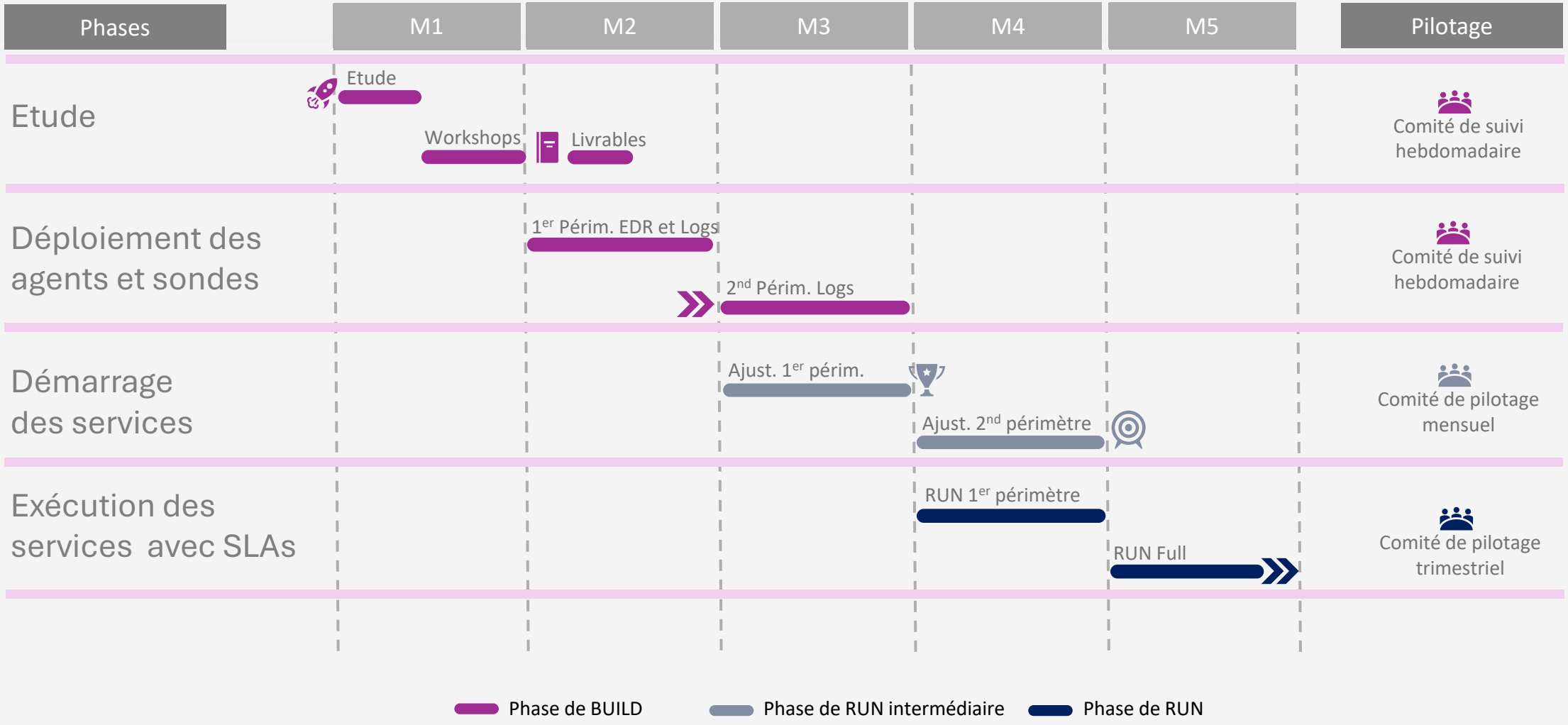
* Constat par nos outils ou équipes d'un évènement qui peut être qualifié de risque sécuritaire
** Prise en compte après l'évènement : démarrage de l'analyse avec une première levée de doute
*** Information client après prise en compte : Création d'un ticket couplé par appel téléphonique pour les incidents de priorité P1
**** Plage de service en 24/7 en option



Exemples :
P1 : Panne totale du réseau ou indisponibilité d'une application essentielle
P2 : Problème de performance d'une application ou dysfonctionnement d'un service secondaire
P3 : Problème mineur de configuration ou demande de renseignements

THEIA
SECURITY DATA NETWORK

GUARDIA : Planning de onboarding d'une nouvelle organisation



THEIA
SECURITY DATA NETWORK

Quelques références pour notre SOC en Région Centre-Val de Loire et en France

Equipementier industriel (45)

1200 postes

Logisticien (37)

150 postes

Industrie pharmaco. (IdF)

200 postes

Avec plus de 4000 postes en surveillance

THEIA
SECURITY DATA NETWORK

THEIA SECURITY DATA NETWORK VOTRE

PARTENAIRE CYBERSECURITE

THEIA
SECURITY DATA NETWORK

WWW.THEIA-SDN.COM