CS TELECOM

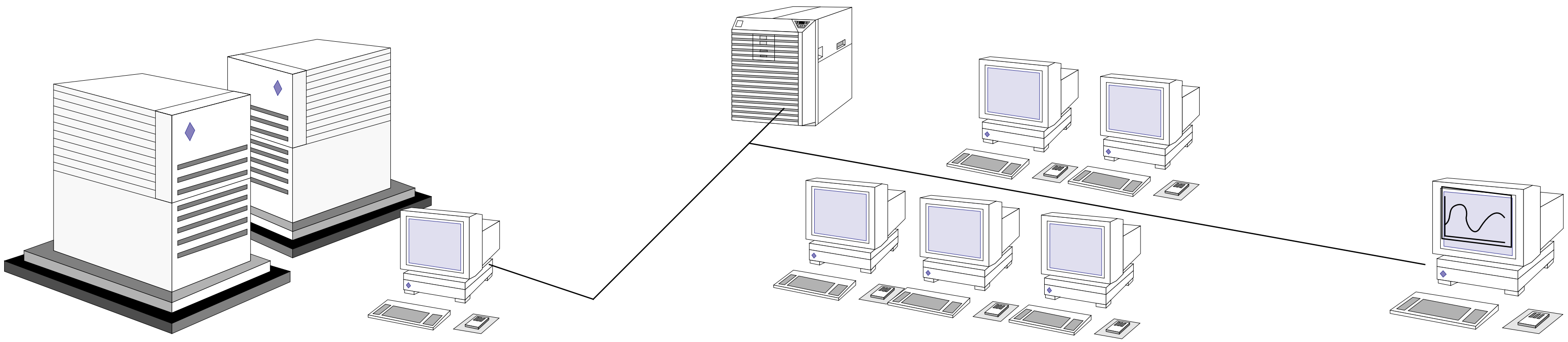
HYPERVIEW 2.0

PrésentationJanvier 1995

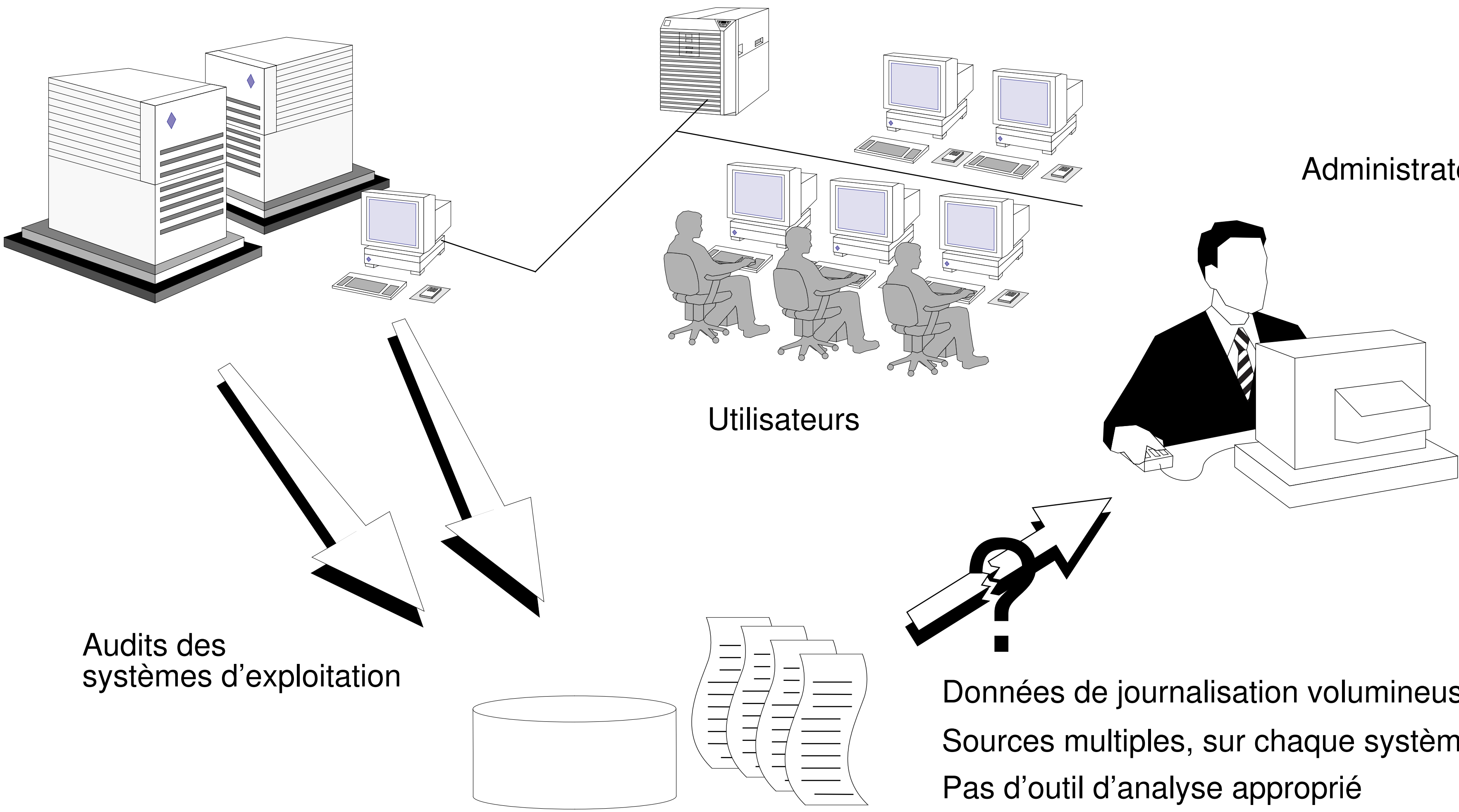
SURVEILLANCE CENTRALISEE DES SYSTEMES D'INFORMATION

ADMINISTRATION DES SYSTEMES D'INFORMATION				
configurations	anomalies	comptabilite	securite	performances

H Y P E R V I E W



COMMENT SURVEILLER UN SYSTEME D’INFORMATION COMPLEXE ?



Données de journalisation volumineuses

Sources multiples, sur chaque système

Pas d’outil d’analyse approprié

FACILITER LA SURVEILLANCE

HYPERVIEW : Système de détection d'Intrusion ou IDS

Donner une vision synthétique de l 'utilisation quantitative et qualitative de l'utilisation des systèmes

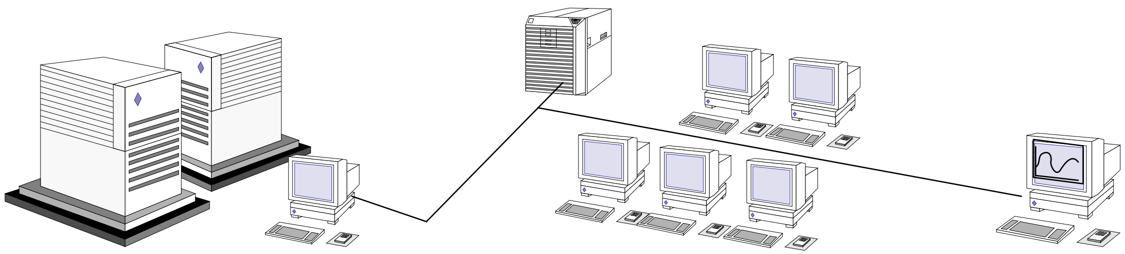
Rechercher des facteurs de risque : configuration fragile ou complexe, degré d'utilisation d'un système

Détecter des utilisations inhabituelles, irrégulières ou atypiques

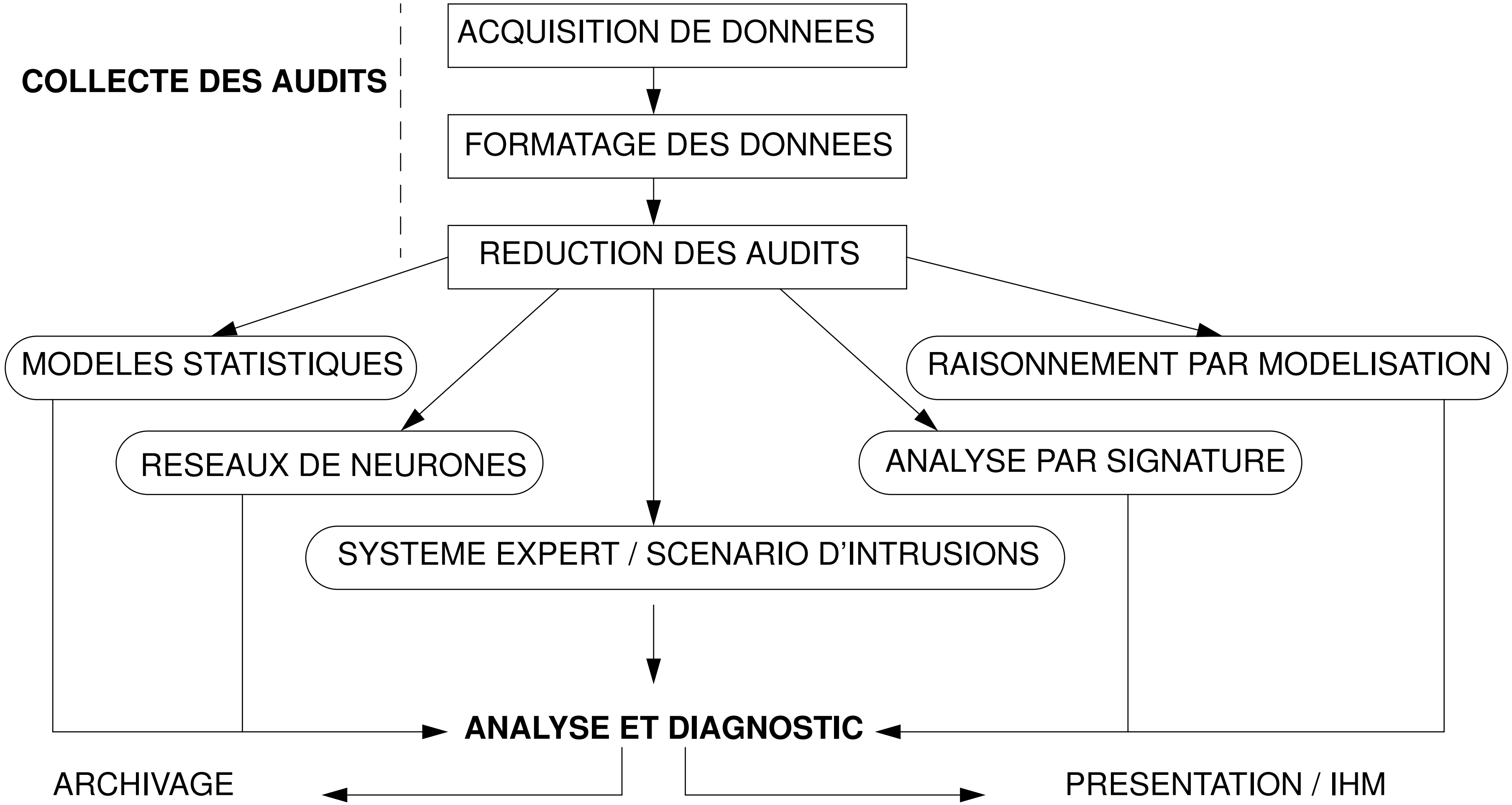
Déceler des présomptions de fraude : utilisation dans des conditions inhabituelles, actions alarmantes

Archiver des traces exploitables à des fins d'analyse ou d'investigation

Centraliser et automatiser la surveillance



Architecture Fonctionnelle d'un IDS



ARCHITECTURE GLOBALE -1- Le dialogue Plateforme/Agent

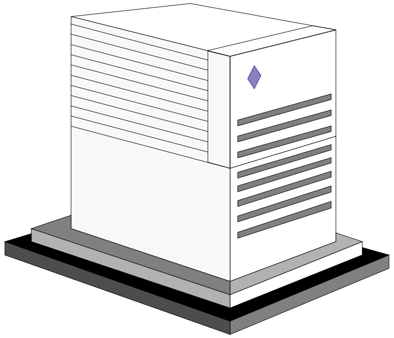
Serveur(s) Surveillé(s)

Acquisition d'audits natifs

Création d'audits spécifiques

Formatage des données

Réduction des Audits



AGENT Hyperview

Réseau TCP/IP

Rapatriement des audits

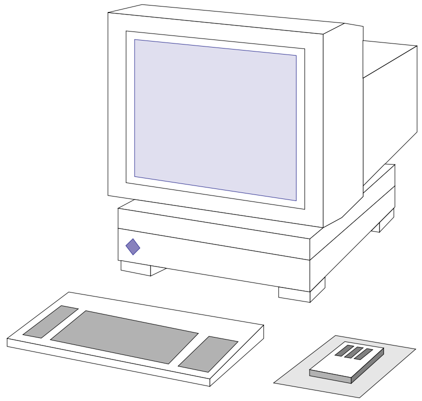
Plateforme Hyperview

Réduction des audits

Analyse et diagnostic des audits

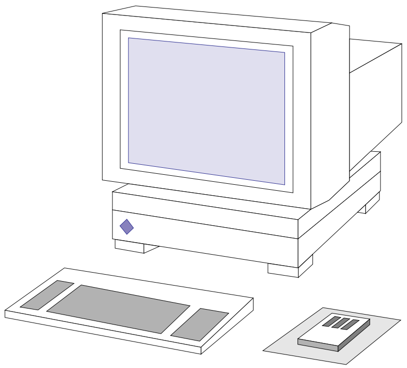
Archivage

Interface administrateur Securité

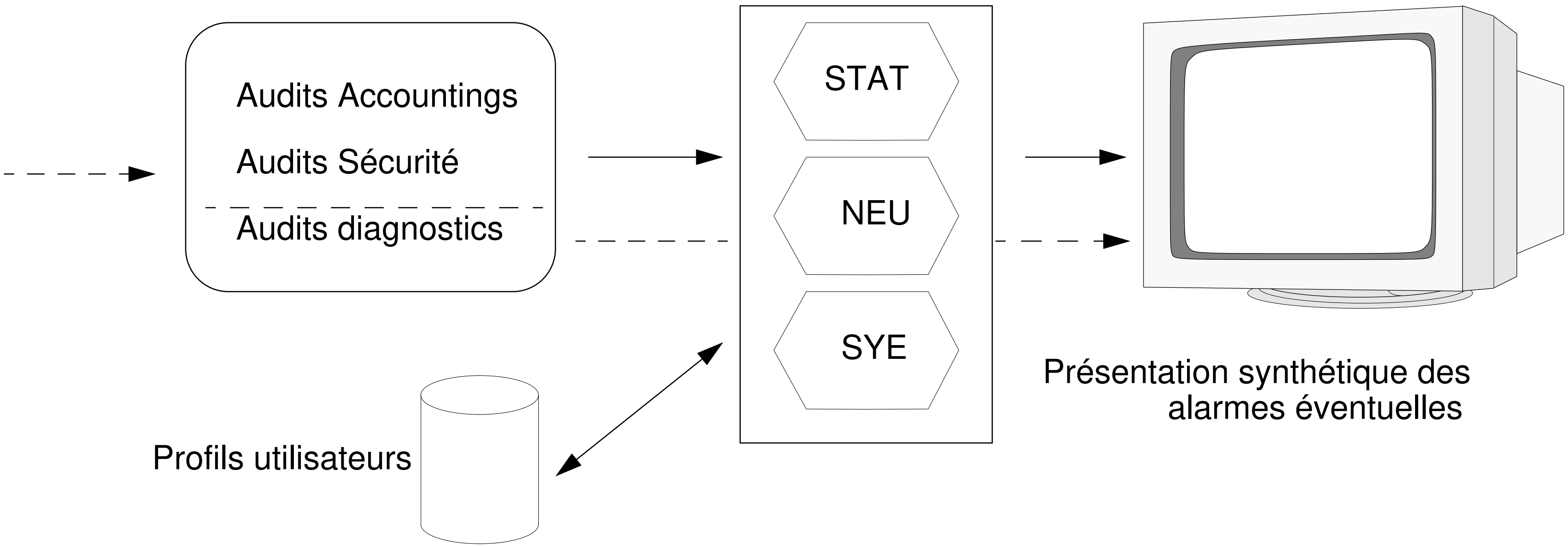


protocole Hyperview

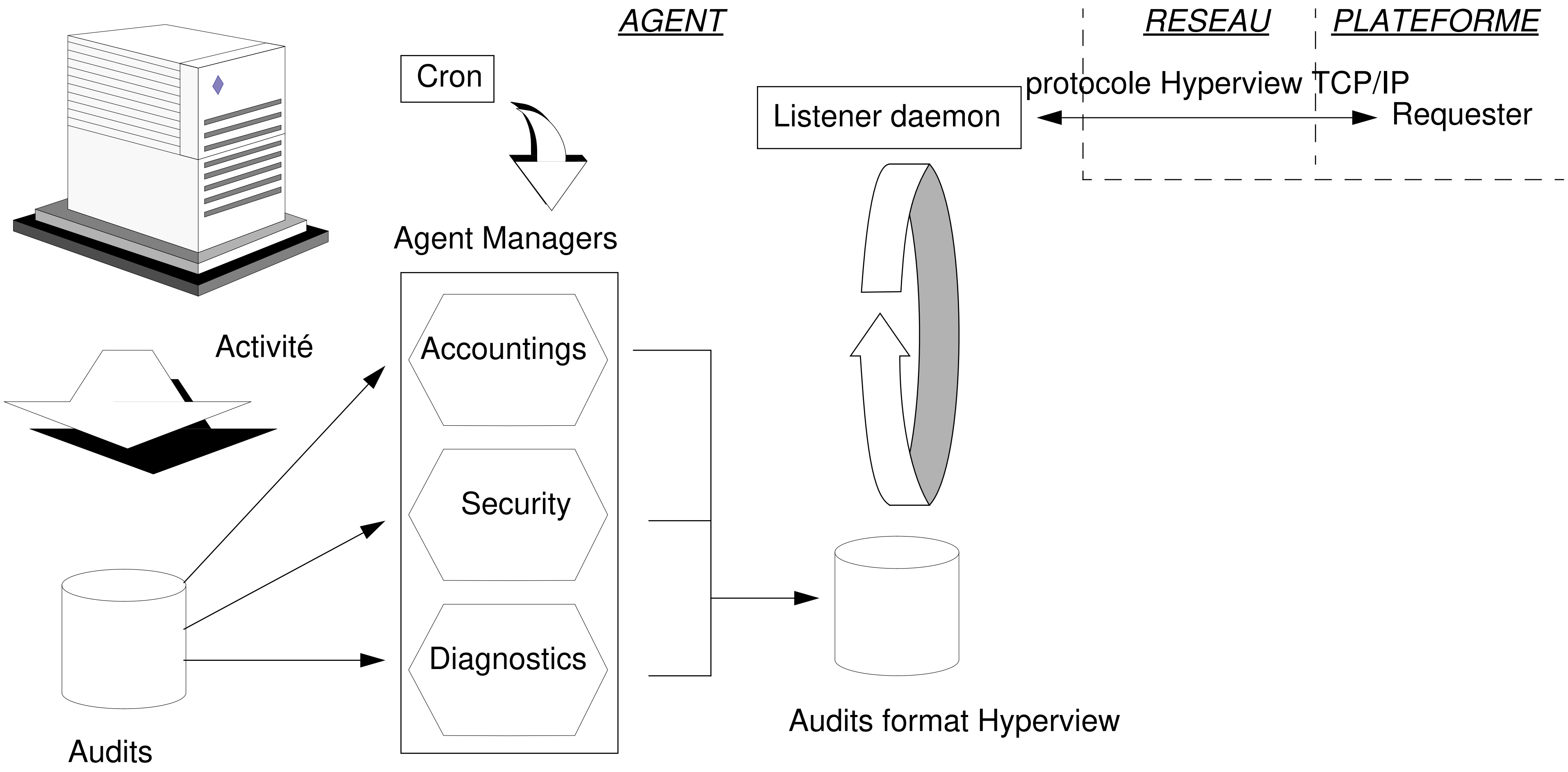
ARCHITECTURE GLOBALE -2- La Plateforme Hyperview



L’analyse et la synthèse sont réalisées par :
- une composante statistique,
- une composante réseau de neurones,
- un système expert



ARCHITECTURE GLOBALE -3- L'AGENT



L'ANALYSEUR STATISTIQUE

Objectif

Analyser des variables caractéristiques des utilisateurs.

Modélisation de comportements par statistiques

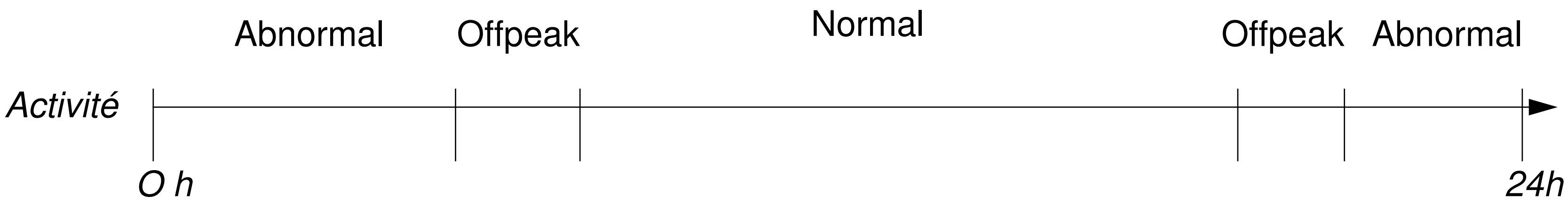
Déduire les déviations de comportement par rapport aux profils construits

Source d'information multiple

- accountings
- audits de sécurité

Principes de construction des profils statistiques des utilisateurs

- autoapprentissage
- la modélisation suit une fenêtre glissante dans le temps
- choix des variables caractéristiques : CPU, IO, fréquence des appels système
- découpage de la journée en périodes caractéristiques : plusieurs profils par utilisateur



L'ANALYSE PAR LE RESEAU NEURONAL

Objectif

Analyser les séquences de commandes réalisées par les utilisateurs ▶ Modélisation de comportements ▶ Déduire les déviations de comportement par rapport aux profils construits

Principes de construction des profils neuronaux

- autoapprentissage
- les déviations sont évaluées par rapport aux prédictions du Réseau Neuronal
- le modèle du réseau est un réseau récurrent simple avec architecture de GENT

Quelques résultats :

$<a,b>^{50}<c,d><a,b>^{50}$ génère une alarme

<login> <appli> <logout> apprise en une centaine de sessions

puis <login> <appli> <sh> <ftp> <logout> génère 2 alarmes

LE SYSTEME EXPERT

Objectif

Détection d'audits alarmants

- acquisition de privilèges
- changement de droits d'accès
- modification de fichiers systèmes
- montage de volumes
- ...

Principe

Base de règles portant sur l'enchainement des appels systèmes et la référence à des objets sensibles. (description de cibles potentielles).

Liste de ressources sensibles : fichiers suid, fichiers du répertoire $HOME des utilisateurs, répertoires sensibles, comptes sensibles.

Exemples

Sur SunOS 4.1.3. environ 60 règles, 120 ressources sensibles, 5 niveaux de gravité d'alarmes

☞ L'utilisateur (aid) a exécuté le fichier système sensible (objectfile) appartenant au propriétaire (ownerid) dans son répertoire $HOME.

☞ L'utilisateur (aid) a modifié l'heure et la date système.

Distributed DiagnosticTool

Objectif

Action préventive : détecter les problèmes de configuration, les failles de sécurité reconnues, éviter les régressions lors d’installations de nouveaux packages ou logiciels

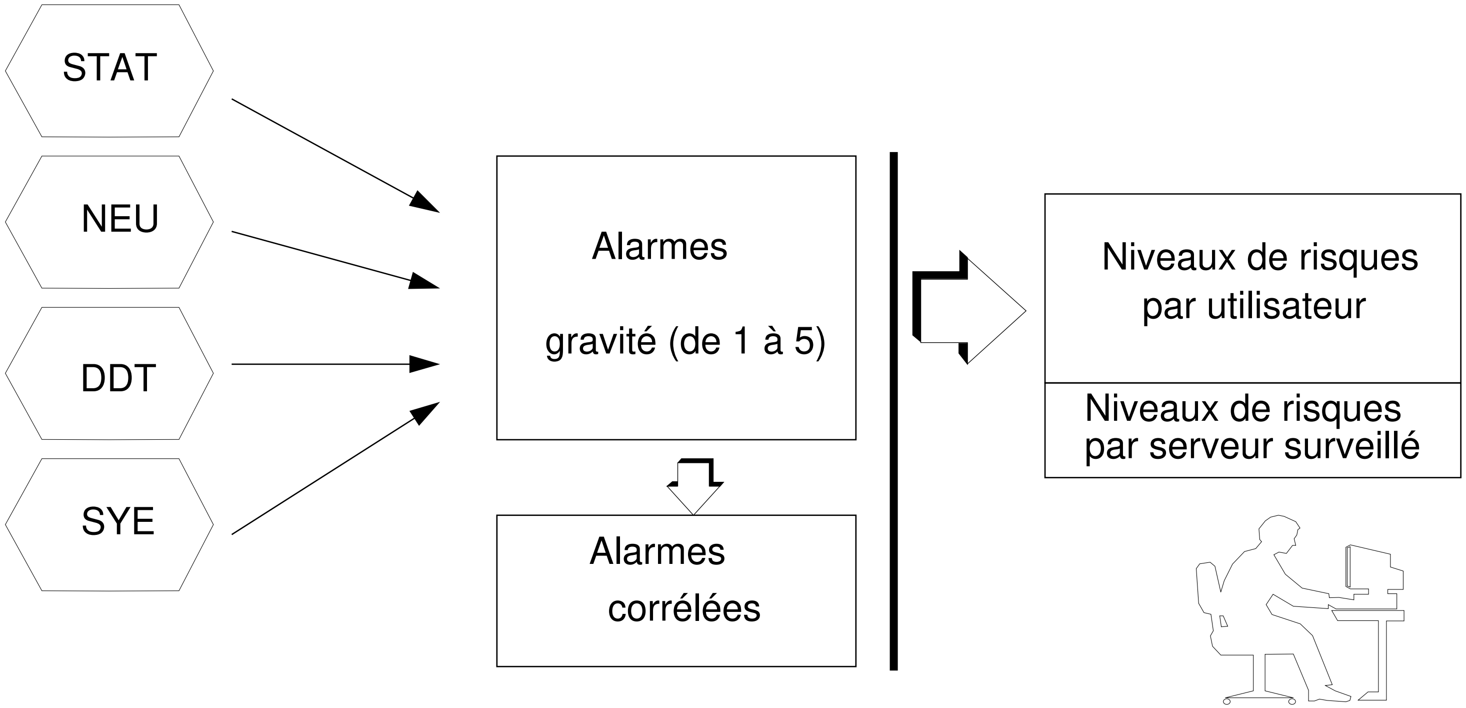
Accompagne le suivi sécurité des serveurs
permet un suivi régulier des machines au cours d’exploitation et d’installations de logiciels

Principe

Le diagnostic porte sur :

- l’intégrité du système d’exploitation (références aux avis du CERT)
- droits d’accès aux fichiers, aux devices
- vérification de la trivialité des mots de passe
- paramétrage de la configuration Réseau
- ...

SYNTHESE et AGREGATS DES ALARMES

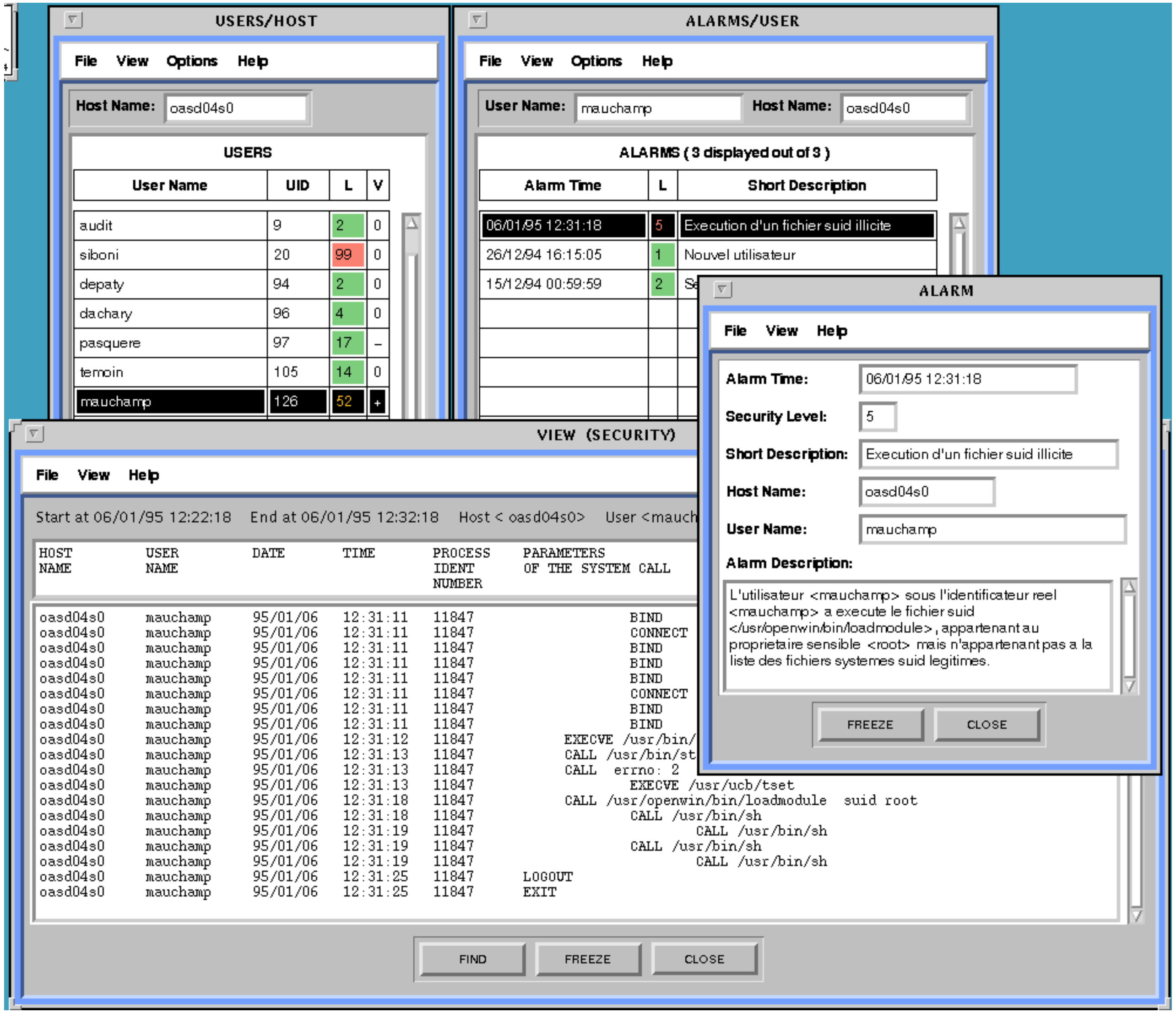


Flux d'alarmes

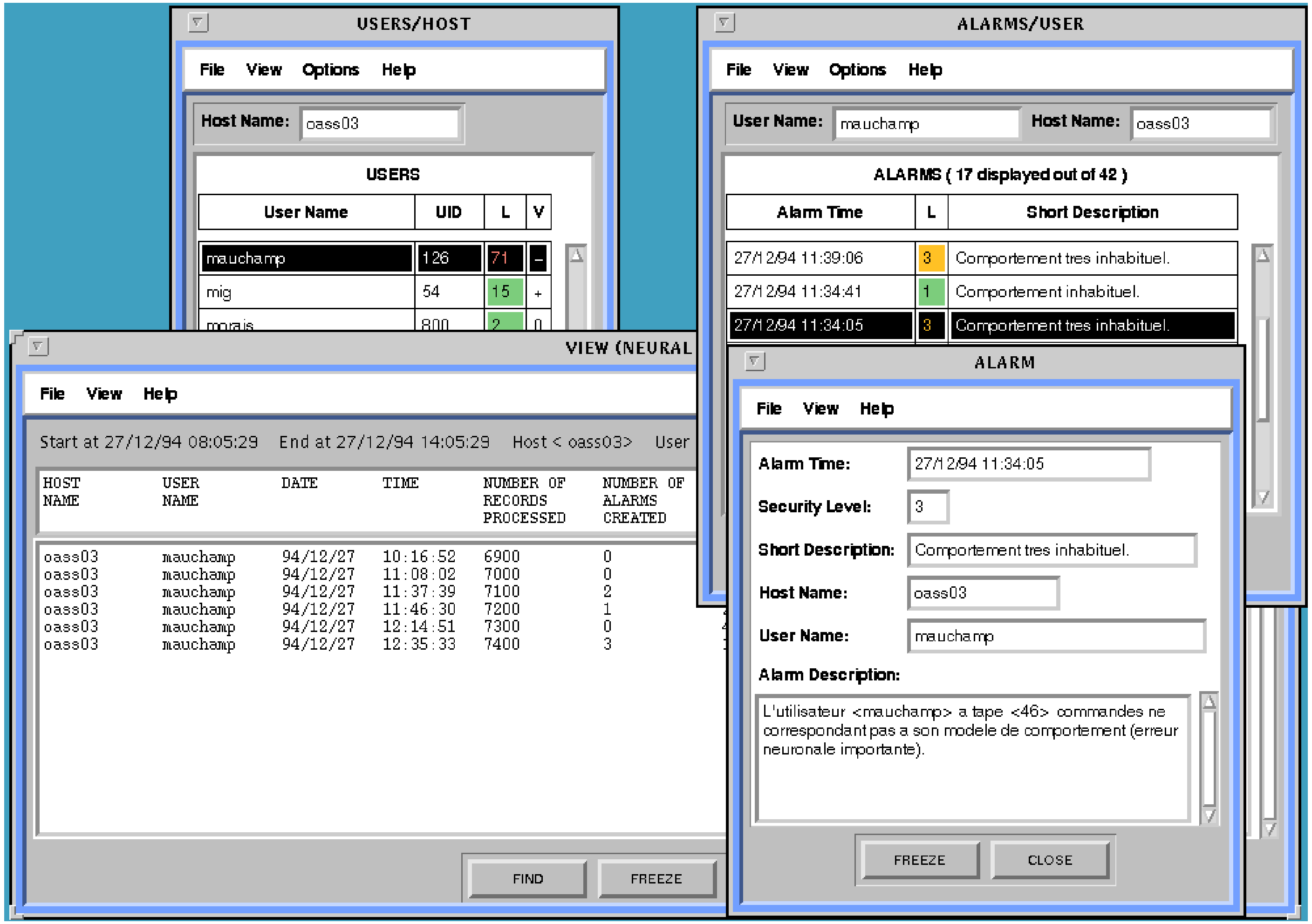
Flux d'alarmes corrélées

Synthèse des informations

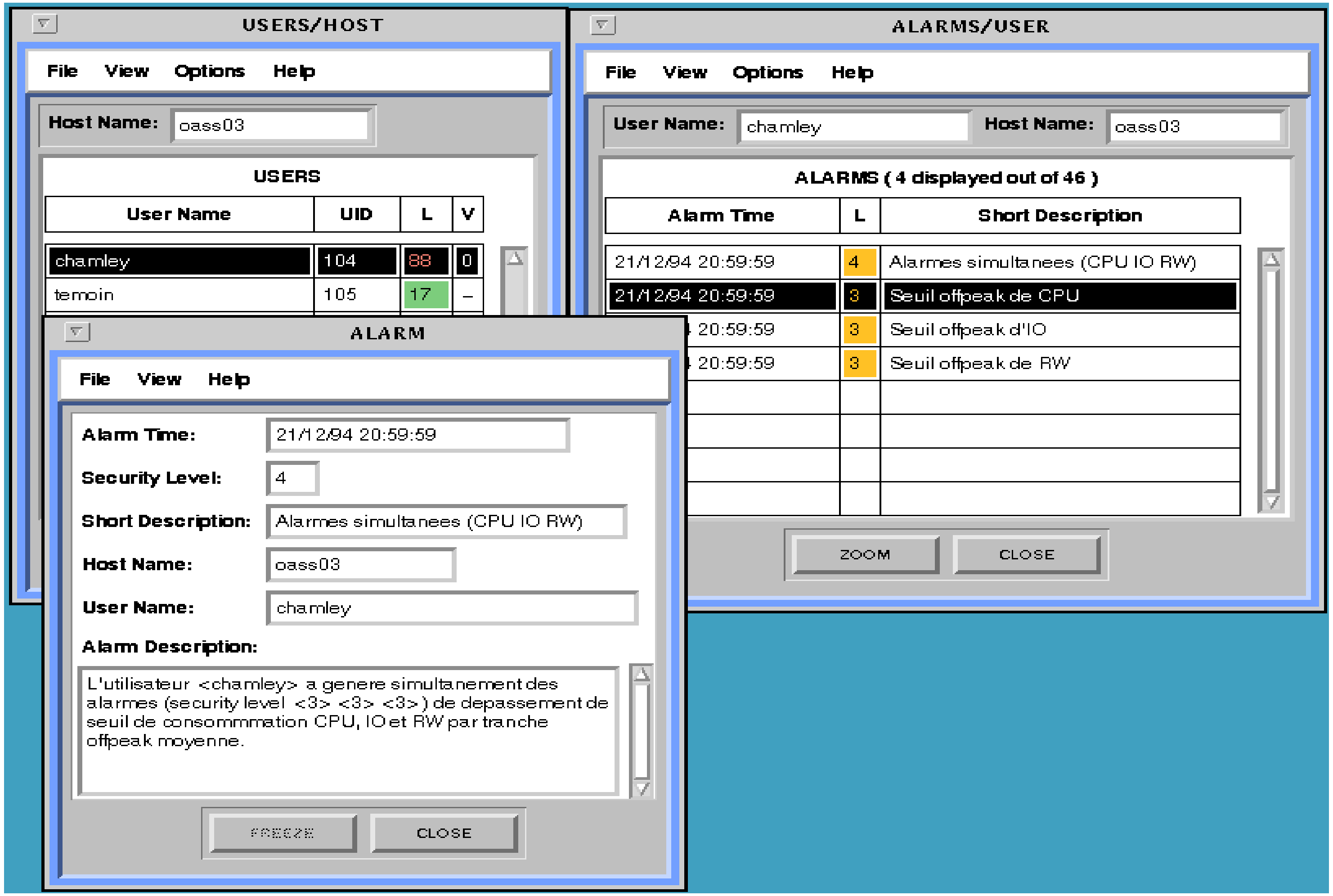
Un exemple d'exploitation : alarme du système expert



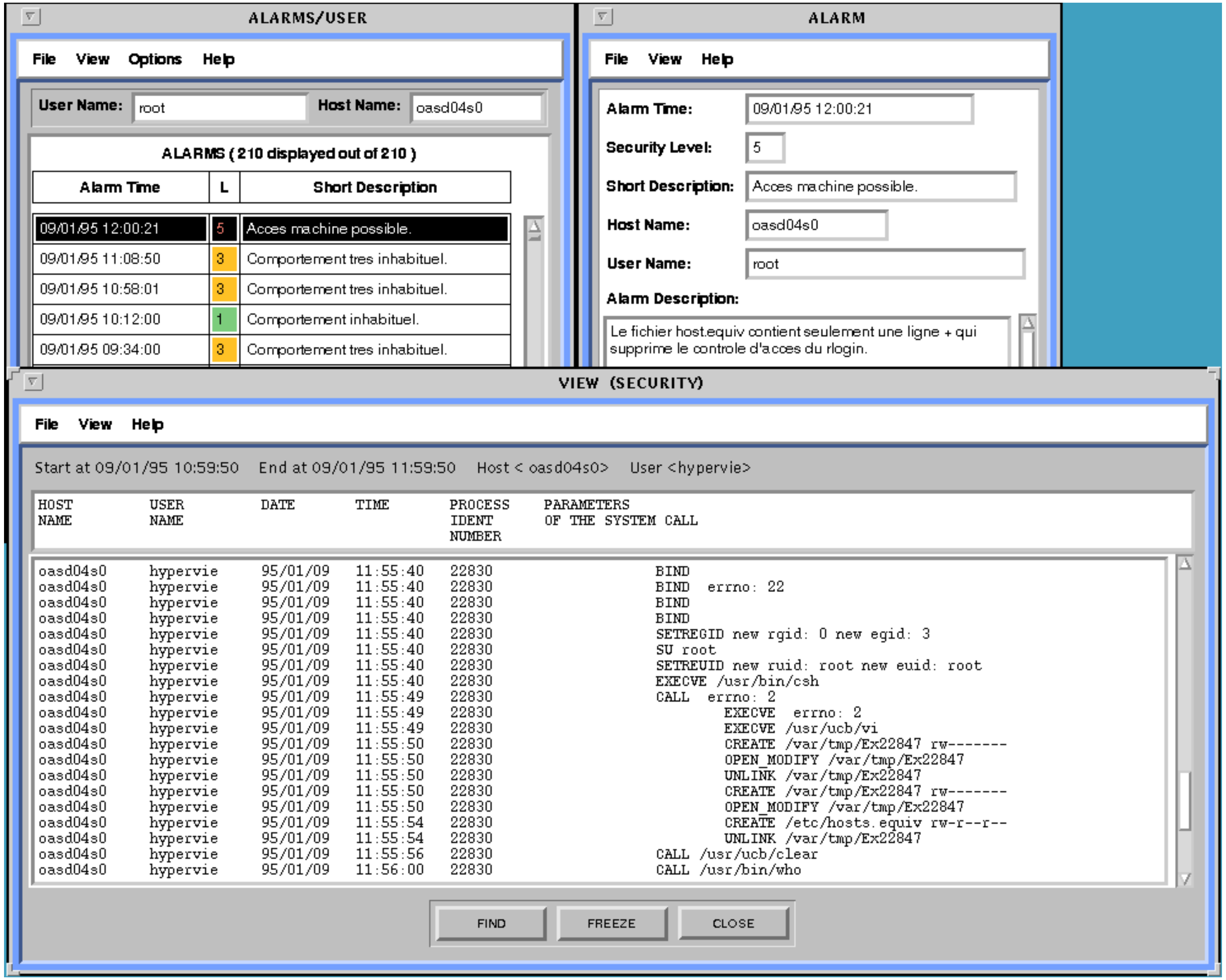
Un exemple d'exploitation : alarme neuronale



Un exemple d’exploitation : alarme statistique



Un exemple d'exploitation : alarme diagnostic



REFERENCES ET PERSPECTIVES

Références :

Hyperview UNIX 2.0 : installation chez Aérospatiale

Hyperview France Telecom : surveillance d'une application de gestion des comptes-clients

Perspectives :

Surveillance d'équipements de réseau (routeurs, commutateurs...)

Surveillance d'outils "middle-ware" : SGBD...

Surveillance d'applications

Surveillance de systèmes spécifiques : contrôle d'accès physique...

Ressources coûteuses, sensibles

Autres projets IDS sur Unix ou Unix-like

IDES, NIDES (Denning, Lunt)	depuis 1980 par SRI & marine Americaine (non commercial)	Modèles statistiques	Réseau neuronal simple exploratoire
Haystack & DIDS (Smaha, Snapp)	US air force Haystack Labs (Stalker)	Approche Système Expert	P 1003.6 format CAT
Wisdom & Sense, NADIR (Vaccaro, Jackson)	Los Alamos Labs (88)	Base de règles arborescentes	Fonctionnement par dépassement de seuils

MENACES ET ANALYSE DU COMPORTEMENT

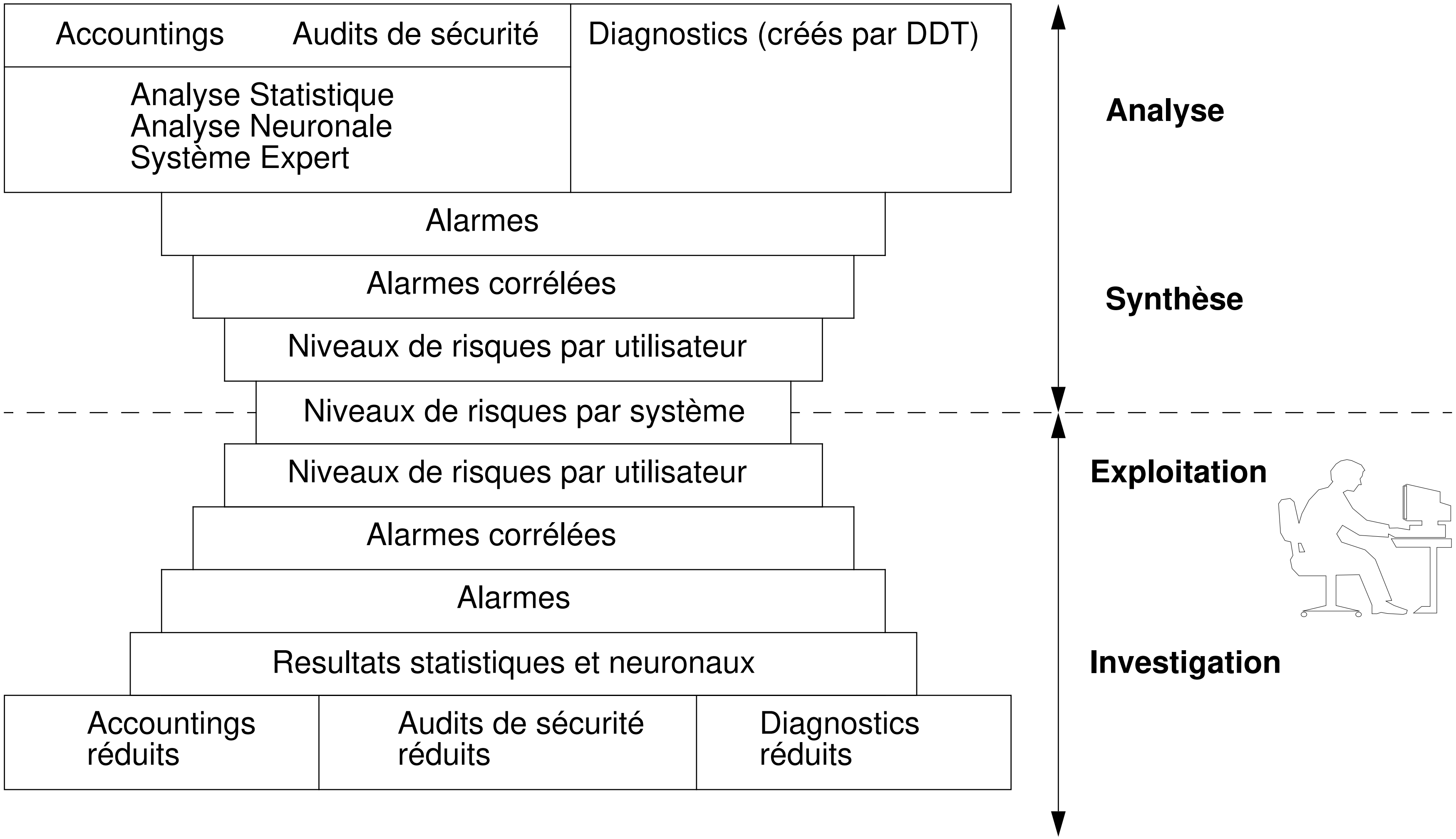
Des menaces liées à la configuration du système

Menaces	Techniques d'analyse	Modèle
Mise à profit d'une faille du système	Diagnostic : analyse de la configuration	Base de connais-sance des faiblesses

Des menaces liées à l'utilisation du système

Menaces	Techniques d'analyse	Modèle
Vol de ressource Vol d'information	Analyse stat. de variables caract.	Profil statistique
Usurpation d'identité	Apprentissage du comportement par RN détection de comportements inhabituels	Modèle de comportement
Actions alarmantes	Détection et analyse de séquences suspectes par système expert	Base de règles d'actions alarmantes

FACILITER L'EXPLOITATION



Quelques points de configuration ...

Gestion des alarmes, du niveau de risque:

seuils de claquage des alarmes statistiques
Stat.CPUUsageM.ValueRatioLevel1= 1
Stat.CPUUsageM.ValueRatioLevel2= 2
Stat.CPUUsageM.ValueRatioLevel3= 4

Stat.CPUUsageM.ValueRatioLevel5= 16
Stat.CPUUsageM.ValueRatioLevel6= 32

formulation du calcul du niveau de risque
UpdateRiskLevel.fadingFactor= 1
UpdateRiskLevel.powerFactor= 2
UpdateRiskLevel.weigthFactor= 2
UpdateRiskLevel.frequencyFactor= 1

configuration des périodes de références des profils statistiques
Stat.RefPeriodDurationInDay= 90
Stat.RefPeriodDurationInPeriod= 1080
Stat.RefPeriodDurationInHours= 180
Stat.DailyPeriodDuration= 2
Stat.NormalHoursStart= 9
Stat.NormalHoursEnd= 18
Stat.OffPeakHoursStart= 6
Stat.OffPeakHoursEnd= 20

Configuration DDT

exemple de configuration de fichiers sensibles :

File Name	owner	group	rights	level	CRC
/	root	*	-d-?r?xr-xr-x	5	
/bin	root	*	?d-?r?xr-xr-x	5	
/boot	root	*	----r??-------	4	True

exemple de configuration de références CERT verifiées :

/usr/ucb/rdist	1991/10/23	CA-91:20
/usr/etc/restore	1989/07/26	CA-89:02
/sys/sun4c/OBJ/cons.o	1990/12/17	CA-90:12
/sys/sun4c/OBJ/crt.o	1991/09/18	CA-91:16
/sys/sun4c/OBJ/nfs_subr.o	1991/12/06	CA-91:21

la configuration réseau recouvre :
- les hosts autorisés dans les ".rhosts" des utilisateurs,
- l'intégrité des fichiers du type "inetd.conf", "services"

on peut également définir un dictionnaire pour la fonction de détection de mots de passe triviaux, l'existence et les droits autorisés des fichiers $HOME/.xxxxx.,

DEVELOPPEMENT D'HYPERVIEW

Etapes :

90-92 : maquettage avec des partenaires industriels. Evaluation des méthodes d'analyse

92-94 : réalisation de la version 2.0 UNIX

94-95 : développement de compléments spécifiques pour France Telecom

Méthodes de développement :

Spécification et conception orientées objet : OMT

Codage en C++

Gestion de configuration multi-utilisateurs, multi-projets

Outils :

LOV / OMT

Base de données INGRES, Générateur de systeme expert IlogRules

Environnements de développement SparcWorks C++ et HP SoftBench