Alizé – Solution d'Enterprise Security & Asset Management

Supervision centralisée – Corrélation de logs – Cartographie réseau – Gestion de parc

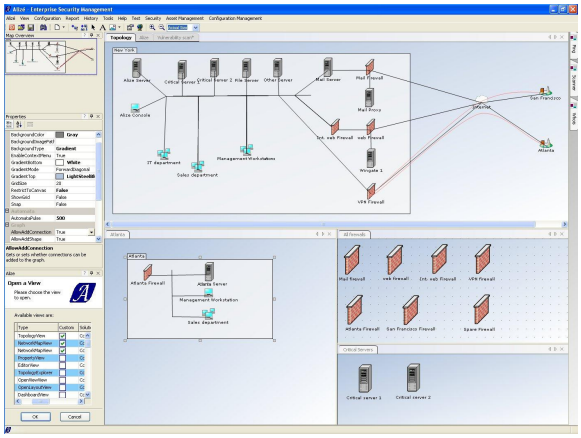
Palliez l'insuffisance des équipements de sécurité actuels

Les dispositifs traditionnels de sécurité (firewalls, antivirus, log Windows et Unix…) ont montré leurs limites :

- Ils n'ont qu'une vision limitée de la sécurité et de l'entreprise,
- Ils ne parlent pas entre eux,
- Ils inondent l'entreprise d'informations de sécurité inexploitables en l'état,
- Ils génèrent autant de fausses alertes ('faux positifs') qu'ils en ratent de réelles ('faux négatifs').

Au total, ces dispositifs ne permettent pas d'avoir une vision globale de la sécurité et des risques, ni de détecter en temps réel les problèmes et donc de s'en prévenir, ni encore de savoir en cas d'intrusion ou de virus l'étendue et la gravité des dégâts et donc de réagir rapidement.

Par analogie avec le système d'alarme d'un immeuble, une organisation ne dispose en informatique que de détecteurs hétérogènes et isolés mais pas d'une centrale d'alarme pour piloter le tout. C'est ce besoin que comble notre produit Alizé.



Avec Alizé, supervisez graphiquement votre réseau.

Centralisez et automatisez la gestion de votre sécurité et de votre parc informatique

Alizé est un framework modulaire et administrable facilement dont les principales fonctions sont de :

- **Superviser la sécurité informatique de tout ou partie de votre organisation**, y compris postes de travail et sites distants.
- **Analyser et corréler les logs** en temps réel de vos équipements, logiciels, et potentiellement de vos applications maison.
- **Cartographier votre système d'information**, y compris VLAN, VPN, NAT…, et détecter/avertir de tout changement.
- **Gérer votre parc informatique**, en inventoriant matériel, OS, patchs, logiciels…, détectant les pannes, identifiant les tendances…

Maîtrisez votre parc et gérez votre risque informatique efficacement

Alizé fournit une vue complète de l'état du système d'information et des menaces réelles qui pèsent dessus. Il renforce et simplifie la gestion de bout en bout de votre sécurité et de votre parc en vous aidant à :

- **Evaluer en temps réel votre niveau de sécurité** par rapport à vos besoins métier.
- **Piloter et communiquer sur votre gestion du risque**, grâce aux rapports et tableaux de bord que vous pouvez créer – graphiquement – avec Alizé.
- **Protèger l'intégrité et la confidentialité de vos données business**. Alizé améliore votre niveau de service en détectant proactivement les défaillances et les menaces.
- **Pérenniser vos investissements passés et futurs** – antivirus, firewalls, OS, base de données… – en les intégrant dans le périmètre sécurisé par Alizé.
- **Maîtriser votre parc logiciel et matériel**, grâce aux outils de cartographie et aux statistiques d'évolution fournies par Alizé.

Une solution fonctionnellement riche, conçue pour répondre aux attentes des entreprises

- **Une surveillance étendue aux postes de travail et sites distants**. Alizé protège tout le SI, quelles qu'en soient la taille et la configuration, sans laisser de zone d'ombre.
- **Une supervision globale de la sécurité, des performances et de la configuration des systèmes**. Alizé fait converger en un outil modulaire de nombreuses fonctions de monitoring.
- **Une supervision en temps réel ou a posteriori intégrant un mode « replay »**. Le temps réel vous permet d'agir quand l'attaque survient et non quand il est trop tard, et le mode 'replay' de rejouer toute séquence passée comme avec un magnétoscope.
- **Une gestion des équipements et sous-réseaux par profil**. L'annuaire d'Alizé reflète votre politique de sécurité et vous permet de détecter tout écart avec celle-ci.
- **Une interface graphique intuitive et personnalisable**. Alizé permet de créer des vues ou groupes de vues spécialisées sur tout ou partie de votre SI : cartes de votre réseau, tables d'évènements, matrices des logiciels installés ou en écart…
- **Un moteur de reporting avancé**. Avec Alizé, vous pouvez créer et publier vos propres rapports (en pdf, html), du tableau de bord synthétique au rapport détaillé.
- **Un système ouvert et évolutif**. Superviser un nouveau type d'équipement ou intégrer un nouveau moteur d'analyse se fait en quelques jours : Alizé peut être enrichi à tous niveaux par des modules additionnels et ses API sont publiques.




Un système simple d'utilisation et pourtant bâti sur des technologies avancées

- **Un système distribué souple**. Alizé repose sur un framework de collecte et de routage de messages, adaptable à toute topologie réseau. Les informations sont collectées à distance (SNMP, syslog…) ou par des agents distribués.
- **Un déploiement et une administration facilités**. Tous les composants d'Alizé sont installables et administrables à distance, depuis la ou les Consoles d'administration.
- **Scalability et respect des ressources**. Les composants distribués d'Alizé pré-filtrent et analysent en local l'information collectée, ce qui réduit le trafic réseau et protège Alizé des problèmes de performance.
- **Un système redondant et tolérant aux pannes**. En cas de machine ou de réseau indisponible, les composants d'Alizé se reconfigurent, stockent ou reroutent leurs messages et se resynchronisent automatiquement, sans intervention de l'administrateur mais en prévenant celui-ci…
- **Un système sécurisé**. L'architecture d'Alizé est bâtie sur une PKI, transparente pour l'administrateur, qui garantit l'identification et l'authentification de chaque équipement, et le chiffrement des communications.
- **Portabilité**. Développés en .NET, les composants d'Alizé tournent sur Windows ou Unix/Linux, à l'exception de la Console qui sera portée en 2006 sous Linux.

" Tracer la propagation d'une attaque ou détecter un virus réseau inconnu "

Grâce à ses agents distribués intégrant firewall et host IDS, Alizé a une connaissance globale du SI qui lui permet non seulement **une analyse approfondie des cas observés**, comme par exemple de tracer la propagation d'une attaque, mais aussi **l'application de règles de supervision simples** qu'un outil traditionnel ne peut pourtant pas implémenter.

Exemple : Avec une unique règle – un poste de travail ne communique qu'avec des serveurs à quelques exceptions près – Alizé détecterait instantanément tout nouveau virus réseau du genre Slammer ou Zotob ou toute attaque réseau massive lancée depuis un poste de travail.

De la supervision à la prévention

Alizé agit aujourd'hui uniquement en mode supervision et détection : les firewalls intégrés à ses agents distribués ne font qu'alerter, et les équipements réseaux remonter leurs informations.

La version 2 d'Alizé, en développement, offrira en option un mode préventif. Avec notre approche, sans toucher au parc existant, l'administrateur aura la possibilité d'isoler tout PC non conforme à sa politique de sécurité et de le mettre en quarantaine sur le réseau.

A propos d' Aulofée Infrastructures Sécurité

Société innovante, Aulofée est une jeune société spécialisée en sécurité des systèmes d'information, fondée par deux associés cumulant plus de 35 ans d'expérience dans l'informatique, l'audit et la sécurité.

Notre vocation est d'aider PME, grandes entreprises et administrations à évaluer et gérer à moindre coût le risque lié à la sécurité informatique. Autour d'Alizé, notre produit phare, nous offrons une gamme étendue de services et de produits en sécurité, directement ou via notre réseau de partenaires spécialisés, afin d'accompagner nos clients dans leur démarche de maîtrise des risques : audit et conseil, politique de sécurité, intégration formation en sécurité.

Pour plus d'information, appelez au +33 (0)1 30 43 40 88 ou rendez vous sur www.aulofee.com