IKare©

My Business Monitoring in Real Time

an innovative solution by ITrust

ITrust…

Fondateurs

Jean-Nicolas Piotrowski
Fondateur et CEO
Former SCO in BNP Paribas Front office
Telecom engineer, IUP STRI Toulouse

Henri Piotrowski
Associé
Former EADS ATR CEO
Supaero Engineer

Siège social situé à Toulouse

Trophées de l'innovation

- 1e prix des DSI aux IT-Days de Lyon
- 2e prix aux Trophées de l'Innovation aux Assises de la Sécurité
- label TIC 2009, catégorie E-entreprise
- label Jeune Entreprise Innovante (JEI)
- soutien spécifique de Oséo et Midi-Pyrénées Innovation.

Métiers

Une expertise de classe mondiale

Ingénieurs CISSP et LeadAuditor 27001
- audits de vulnérabilité
- tests de pénétration en mode intrusif
- enquêtes forensiques après incident
- sécurisation informatique Confidentiel Défense
- sécurisation des entreprises étendues (cloud)
- certification ARJEL (Autorité de Régulation des Jeux en Ligne)
- cryptographie, PKI, IAM
- normes et certifications Bâle II, ITIL, EBios, 27001.
- membre fondateur de la FPTI (Federation des professionnels des tests d'intrusion)

Clients

La sécurité des SI

Chiffres clés

ITrust amène une liste de clients satisfaits, un niveau de performance de ses services, un volume d'activité et une expérience propres à convaincre les clients les plus exigeants.

50 clients dont 6 grands comptes du CAC 40
20.000 vulnérabilités identifiées chez des Clients
10.000 adresses IP scannées de manière automatique
100% de taux de succès des certifications ARJEL (*)
90% de taux de réussite des audits intrusifs
50% de taux de récupération des data confidentielles

Ikare

La **Solution Ikare**, développée par les ingénieurs ITrust, propose une solution complète, intégrée et facile d'usage permettant de détecter les vulnérabilités informatiques.
La Solution Ikare inclut également des services associés tels que des **Audits intrusifs** et un label de sécurité : **ITrust Security Metrics**.

"Pour une protection du patrimoine informationnel de l'entreprise"

(*) Autorité de Réglementation des Jeux en Ligne

Des risques et pertes en augmentation exponentielle

- 6 entreprises françaises sur 10 ont subi au moins un **incident de sécurité** en 2011. (50% d'augmentation), dont 5 ayant subi des pertes financières directes. (PWC 2011)
- le coût moyen d'un incident de sécurité est de **40.000 €** (Clusif 2010)
- dans 20% des cas, les entreprises mettent plus d'une semaine pour revenir à une situation de fonctionnement normal. (Clusif 2010)
- En 2010, **80%** des entreprises françaises (de plus de 200 personnes) estiment avoir une dépendance forte vis à vis de leur système d'information,
- et 3/4 considèrent qu'une indisponibilité de 24h et moins de leur Système d'information serait lourde de conséquences.

De nouveaux besoins

- L’entreprise étendue / le cloud
- Le nomadisme
- BYOD (Bring your own device)
- Vie privée / vie professionnelle et réseaux sociaux
- Persistant threats

Focus sur **IKare Security**

La **Solution Ikare** fournit une solution complète en SaaS, intégrée et facile d'usage permettant de détecter les vulnérabilités informatiques.

La Solution Ikare inclut également des services associés tels que des **Audits intrusifs** et un label de sécurité : **ITrust Security Metrics**.

Solution en SaaS externe ou interne

90 % des failles de sécurité (tous types d'entreprises) et des vulnérabilités rencontrées par nos clients proviennent de 3 sources :

- Mots de passe par défaut ou faibles,
- Mauvaise configuration des équipements et serveurs,
- Systèmes et applications non mises à jour.

Ikare DETECTE ces failles et augmente alors de 90% votre sécurité

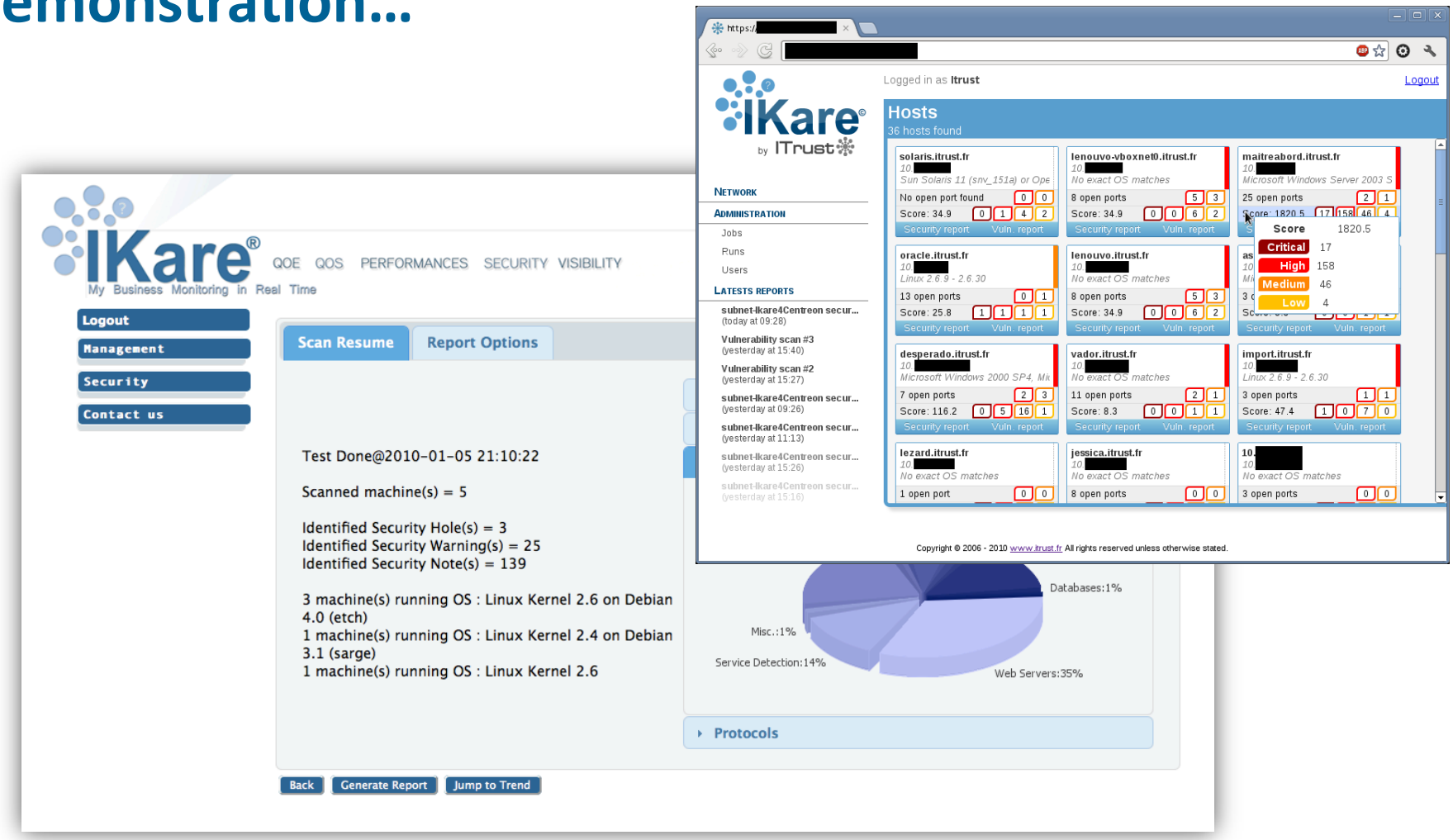
Ikare traite 100% des 10 failles les plus constatées
Soit **10 fois plus** qu'un IDS/IPS (système de prévention d'intrusion)
Là où un antivirus ou un Firewall ne traite pas plus de 10%

Représentant plus de 90% des menaces dans une PME.

Retour d'expérience Top 10 des failles de sécurité. Itrust de 2007 à 2012

Domaine et faille	% présence failles dans l'entreprise	Risques couverts ? Couvert / testé par Ikare	Couvert par un Antivirus	Couvert par un Firewall	IDS
Gestionnaire de domaines trop verbeux	95%	OUI	NON	NON	?
Mots de passe evidents ou faibles	95%	OUI	NON	NON	?
Partages et droits d'en connaitre	80%	OUI	NON	NON	Non
Relations de confiance : propagation de la compromission	50%	OUI	NON	NON	Non
Serveurs de bases de données	80%	OUI	NON	Partiellement	Non
Serveurs DNS trop verbeux pour les domaines internes	95%	OUI	NON	Partiellement	Non
Partages de fichiers	95%	OUI	NON	Partiellement	Non
Protocoles d'administration en clair ou mal configurés	95%	OUI	NON	Partiellement	Non
Serveurs développement, Serveurs à l'abandon	80%	OUI	NON	Partiellement	Non
Failles historiques	50%	OUI	NON	Partiellement	OUI

Démonstration…



ITrust Security Metrics

Critères / Exigences	Certified	Niveau 1	Niveau 2	Niveau 2+	Niveau 3	Niveau 4
Scan de Vulnérabilités via IKare	①	1/semaine	2/semaine	2/semaine	1/jour	1/jour
Contrôle de sécurité via IKare	①	2/semaine	1/jour	1/jour	2/jour	2/jour
Délais de correction des vulnérabilités	Pas de vulnérabilité critique	1 semaine	3 jours	3 jours	48H	24H
Sécurité physique	①			Tous les trimestres	√	√
Gestion des actifs	①			√	√	√
Gestion des communications et des opérations	①			√	√	√
Contrôle d'accès	①				√	√
Gestion des incidents	①				√	√
Politique de sécurité	①				√	√
Organisation de la fonction sécurité	①				√	√
Ressources humaines	①				√	√
Reprise et continuité d'activité	①				√	√
Conformité	①				√	√
Accréditation client ISO 27001	①					√

Une mise en place du label SIMPLE

- Label ITrust Security Metrics « **Certified** » : Revue ponctuelle

  Dès 3 000 Euros/an

- **Label 1 et 2** : contrôles de sécurité technique

- **Label 2+ à 4** : contrôles organisationnels (vers Cible ISO 27001)

- **Ikare seul** : Monitoring et contrôle de sécurité

Nouveaux besoins et réponses IKare

Nouveaux besoins	Solution IKare
éloignement géographique des éditeurs	proximité des équipes R&D (100% France)
faible orientation vers les besoins des PME	focalisation PME industrielles et de service
pas de vue métier possible	ajouts de vues métiers (ex : marketing)
pas de spécialisation sectorielle	expertise sectorielle (ex : aéronautique)
trop grande complexité de la prise en main	simplicité de la prise en main
impossibilité d'exploiter sans informaticien	exploitation des résultats sans informaticien
lourdeur de la certification ISO 27001	simplicité du label ITrust Security Metrics
pas d'intégration de la QOS du réseau	intégration de la QOS du réseau
obligation de délocaliser les rapports sécurité	pas de délocalisation des rapports sécurité
absence d'outils simples de management	outils simples de reporting et management
pas de boucle de contrôle des actions	boucles automatiques de contrôle permanent

Fonctionnalités techniques de Ikare

- **Audit des vulnérabilités temps réel**
- **Identification proactive des problèmes de sécurité**
- **Découverte de l'infrastructure et des applications**
- **Corrélation intelligente :**

  La détection de vulnérabilités devient beaucoup plus fiable. Ces moteurs diminuent le nombre de faux positifs et
  permettent de détecter des *comportements anormaux inconnus tels que les* ***virus « 0 day »***
- **Maintien en conditions opérationnelles**
- **Détermination des zones de responsabilité**
- **Alertes de sécurité**
- **Trending, Evolution dans le temps de la sécurité**
- **Gestion de Business units**
- **Groupes virtuels permettant une vue décisionnelle de la sécurité**
- **Conformité CNIL et E-Privacy**

Avantages clés 1/2

« Vous mettre en conformité réglementaire : Package Telecom, Loi Escoffier. »

L'Ordonnance du 26 aout 2011 (Loi Escoffier) stipule : « en cas de faille et de violation de données à caractère personnel, le fournisseur de services devra notifier l'existence de cette faille à la CNIL et, potentiellement aux « personnes intéressées »…sauf si elle peut prouver que son système d'information est bien protégé et sécurisé selon les meilleures pratiques, ce que procure IKare.

« Vous mettre au niveau des meilleures pratiques, Hervé Schauer Consultants »

« Les antivirus ne sont plus efficaces face aux nouvelles menaces informatiques. Maintenir une bonne politique de sécurité en temps réel en évitant les mots de passe par défaut et en supervisant les failles des sécurité reste la meilleure pratique de sécurité actuelle pour les PME » : Hervé Schauer, Consultant Expert en Sécurité Informatique (http://www.hsc.fr/). C'est justement le service que procure IKare de manière fiable et automatisée.

« Réduire fortement l'exposition aux vulnérabilités et risques informatiques. »

« La mise en place de la Solution Ikare réduit jusqu'à 90% le taux de vulnérabilité informatique de l'entreprise. 90% est le taux de réussite des audits intrusifs réalisés par les Experts de ITrust chez ses clients. »

« Augmenter votre productivité et vos marges commerciales. »

« Le label de sécurité ITrust établit de manière indépendante le niveau de sécurité de votre système d'information, selon des critères objectifs et des normes internationales. L'affichage de ce label rassure vos propres clients, qui réduisent leur propre niveau de risque global en contractant de préférence avec des fournisseurs évalués et labellisés, plutôt qu'avec ceux qui ne le seraient pas. »

Avantages clés 1/2

« Automatiser complètement vos processus d'analyse de vulnérabilité. »

« La Solution Ikare permet une automatisation totale des actions entreprises pour déployer la politique de sécurité, ce qui peut amener un bénéfice égal à 2 fois le coût de cette politique (exemple de la société déjà sécurisée ci-dessous). »

« Mettre à disposition de votre management des outils d'action et de contrôle. »

« La Solution Ikare transforme des informations techniques éparpillées, parcellaires et fragmentées, en tableaux de bord détaillés et présentés de manière managériale, décisionnaire et actionnable. De plus, le caractère automatique de la détection des vulnérabilités par IKare permet au management de contrôler le résultat des actions prises en réparation et en prévention des failles de sécurité. »

« Baisser vos coûts opérationnels de déploiement et d'exploitation. »

« variabilisation (« opexisation ») des coûts fixes de la sécurité informatique
absence de perturbation de la production lors du scan sécurité
meilleure utilisation des infrastructures de sécurité informatique
baisse des primes d'assurance de la production et des opérations. »

« Gagner du temps sur votre déploiement et votre exploitation. »

« gain de temps sur l'installation et la mise à jour de la solution
gain de temps sur les déploiements à grande échelle et multi-sites
gain de temps en cas d'évolution de la base informatique physique
gain de temps en cas d'évolution des applications informatiques
gain de temps en cas d'introduction de nouvelles applications
gain de temps lors des ajustements du nombre d'adresses IP. »

Roadmap

- Available:
  - IKare Security v1.7
    - Ouverture a l'OEM : export via API XML-RPC
    - SOC ITrust with Ikare
    - Refonte IHM
    - Sensor universel
  - IKare4Centreon
- Mars 2012 :
  - Ikare en SaaS Externe
  - Trending (évolution entre scans)
  - Business Unit
  - Vue métier et décisionnelle
- Q2 2012:
  - IKare Cloud (QoS)
  - IKare Cloud (QoE)
  - Moteur de correlation par scénarios
- S2 2012:
  - IKare IT = SIEM avec analyse comportementale

CONTACT

www.ikare-monitoring.com
www.itrust.fr

contact@itrust.fr
ITrust – Immeuble ACTYS 1 – 55 Avenue l'Occitane, 31673 Labège
Fixe Sdt. : 05.67.34.67.80 – **Fax :** 09.80.08.37.23
Cabinet de conseil en sécurité informatique

Jean Nicolas Piotrowski, Dirigeant
Mail : jn.piotrowski@itrust.fr
Tel. 06.76.40.88.41

Julien Lavesque, Directeur Technique IKare®
Mail : j.lavesque@itrust.fr

QUESTIONS ?

ANNEXES

Notre technologie : IKare Vsec

- **Scanner de vulnérabilités temps réel et non intrusif**
- **Scanner de sécurité**
- **Cartographie d'infrastructure et applications**
- **Génération de rapports**
  - Rapports PDF synthétiques
  - Rapports PDF détaillés
  - Tableaux de bord récapitulatifs
- **Interface d'administration**
  - Planifications des scans
  - Gestion des cibles (hotes/plage/blacklist)
  - Gestion des utilisateurs

Le moteur de corrélation intelligent

ALARM REPORT :11/11/2011 11:11:11
STATUS : CRITICAL
COMMENTS : INCIDENTS RUNNING
BU : DMZ ITRUST

-LATEST VSEC MAP SCANS SHOW
ALERT(10.1.0.161): WARNING - SERVICE DOWN : 34778/(oracle) Oracle TNS Listener
ALERT(10.1.0.161): WARNING - SERVICE DOWN : 55801/(oracle) Oracle TNS listener
ALERT(10.1.0.161): WARNING - SERVICE DOWN : 711/(status) 1 (rpc #100024)
ALERT(10.1.0.200): NOTICE - HOST DISCOVERED : Apple Mac OS X 10.7.0 (Lion) (Darwin 11.0.0)
ALERT(10.1.0.200): NOTICE - SERVICE DISCOVERED : 123/(ntp) NTP v4
ALERT(10.1.0.200): NOTICE - SERVICE DISCOVERED : 2048/(monitor) Unknown Daemon
ALERT(10.1.0.200): NOTICE - SERVICE DISCOVERED : 138/(dgm) Unknown Daemon
ALERT(10.1.0.200): NOTICE - SERVICE DISCOVERED : 4500/(ike) Unknown Daemon
ALERT(10.1.0.200): NOTICE - SERVICE DISCOVERED : 52147/(skype2) Skype
ALERT(10.1.0.200): NOTICE - SERVICE DISCOVERED : 137/(ns) Microsoft Windows XP netbios-ssn
ALERT(10.1.0.200): NOTICE - SERVICE DISCOVERED : 1023/(unknown) Unknown Daemon
ALERT(10.1.0.200): NOTICE - SERVICE DISCOVERED : 177/(xdmcp) Unknown Daemon
ALERT(10.1.0.200): NOTICE - SERVICE DISCOVERED : 2000/(sccp) Unknown Daemon
ALERT(10.1.0.200): NOTICE - SERVICE DISCOVERED : 5353/(zeroconf) Unknown Daemon
ALERT(10.1.0.161): NOTICE - SERVICE DISCOVERED : 135/(msrpc) Microsoft Windows RPC
ALERT(10.1.0.161): NOTICE - SERVICE DISCOVERED : 22/(ssh) OpenSSH 5.8p1-hpn13v10 (protocol 2.0)
ALERT(10.1.0.161): NOTICE - SERVICE DISCOVERED : 443/(https) Apache httpd
ALERT(10.1.0.163): NOTICE - HOST DOWN : Microsoft Windows 2000 Server SP4 or Windows XP Professional SP3

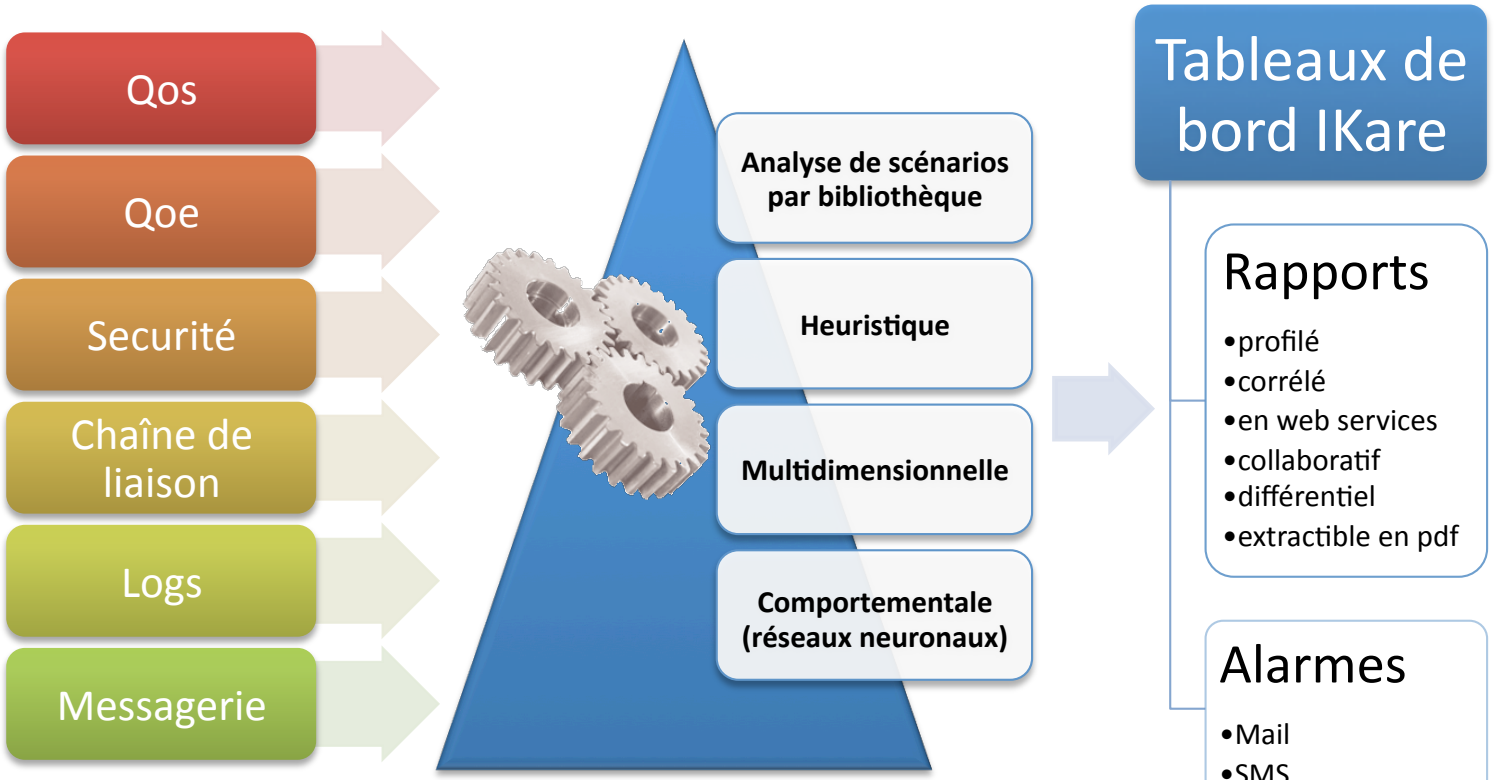
-LATEST VSEC SCANS
ALERT(10.1.0.161): CRITICAL - 443/(https) Apache httpd - Certificate signature validity: KO: error 18 at 0 depth lookup:self signed certificate,OK,
ALERT(10.1.0.161): WARNING - 135/(msrpc) 0|SMB|Anonymous access: Warning: Allowed anonymous access

-LATEST VULNERABILITIES SCANS
ALERT(10.1.0.100): WARNING - CVSS SCORE CHANGE : 30.5 (+10.0)
ALERT(10.1.0.100): WARNING - NEW VULNERABILITIES DISCOVERED : 2 Medium
ALERT(10.1.0.100): WARNING - OLD VULNERABILITIES FIX : 1 Critical
ALERT(10.1.0.100): WARNING - OLD VULNERABILITIES UNFIX : 1 High - 1 Low

-CORRELATION ALERTS
ALERT(10.1.0.161): CRITICAL - **POSSIBLE ATTACK ON HOST : too much new critical services open and down with CRITICAL VSEC Notifications.**
ALERT(10.1.0.100): WARNING - VULNERABILITIES UNFIX since 1 month now
ALERT(10.1.0.163): NOTICE - Typical Workstation shutdown.
ALERT(10.1.0.200): NOTICE - Should be a Nomad Workstation ... waiting to see if host runtime match workhours.

Prochainement : **IKare Cloud & IKare IT**

Collecteurs/Sensors non intrusifs	Moteur de corrélation IKare	"La bonne information à la bonne personne"



IKare©

My Business Monitoring in Real Time

ITrust

Présentation Technique

La sécurisation classique d'un SI

- Elle est basée sur un P.D.C.A
  - Un tour de roue est effectué par an et
  - Ne comprend qu'une seule vérification indépendante du niveau de sécurité.
- Il peut s'agir
  - De tests d'intrusions et/ou
  - D'audits de configurations.
  - Ils doivent être accompagnés de recommandations
    - Pour améliorer et conserver le niveau de sécurité du SI.

Le niveau de sécurité classique d'un SI

- Le niveau de sécurité augmente rapidement après chaque audit.
- Mais au jour le jour il peut grandement varier :
    - Lors d'éditions d'avis de sécurité,
    - Lors de changements de versions d'OS ou de logiciels ou
    - Lors de changements de configuration.
- Le niveau de sécurité doit rester optimal 365 jours par an :
    - Pour éviter les vols, modifications ou destructions de données confidentielles,
    - Pour éviter les problèmes de disponibilité du SI,
    - etc.

Conserver le niveau optimum de sécurité du SI

- Il est possible de multiplier les audits
    - Mais il faudrait en faire toutes les semaines…
    - Le coût serait prohibitif.
- Au jour le jour il s'agit plus de surveiller le niveau de sécurité que de l'évaluer :
    - La méthode doit être plus simple,
    - Automatisable et
    - Ne doit pas forcément tout couvrir :
        - l'application WEB n'a pas besoin d'un T.I. quotidien.

Evaluer le niveau de sécurité du SI

- Des tests de types « cartographie » peuvent recenser
    - Ses systèmes, ses services, ses versions, ses configurations
- Il est possible de s'inspirer du scellement de fichiers :
    - Une image du système est prise et
    - Quotidiennement le système vérifie qu'elle n'a pas changé.
- Puisqu'après un audit le niveau de sécurité est connu
    - Pourquoi ne pas réaliser un « scellement réseau » ?

Le scellement réseau

- Aucun système ne devrait apparaitre ou disparaitre.
- Aucun port ne devrait s'ouvrir ou se fermer.
- Aucune propriété de service ne devrait changer :
    - Logiciel, version, configuration.
- Détecter pro-activement les problèmes :
    - Renouvellements de certificats, de domaines DNS…
- S'assurer que le SI fonctionne correctement: temps de réponse
- Détecter certaines compromissions, par exemples :
    - Un serveur SSH sur un port ésotérique
    - Un nouvel utilisateur placé administrateur local
- Compléter ceci par des scans de vulnérabilités.

IKare Security

- Permet de *monitorer* en temps réel le système d'information.
- Inclut le support de différents modules de sécurité
    - VSec, Nessus, OpenVAS…
- Avec une périodicité choisie, par exemple :
    - Chaque heure pour VSec et
    - Quotidienne pour les autres.
- D'en obtenir des rapports bruts
    - Ou des rapports incrémentaux.
- D'en gérer des tickets d'actions à mener
    - Patches à appliquer, configurations à corriger…

VSec

- Originellement un ensemble de scripts pour accélérer les audits intrusifs internes
    - Netbios, LDAP, SNMP, FTP, NFS, MSSQL, MySQL, Oracle…
- Complété pour les serveurs externes
    - HTTP, SSL, WEBApps, DNS, SMTP, SSH…
- Développés pour être « légers » par défaut
    - Minimisation des ressources réseau et système,
    - Rapidité des tests effectués (« temps réel ») et
    - Cible les « failles » faciles à exploiter.
- Peut comporter des recherches par force brute à la demande
    - Par ex : tests de mots de passe par défaut ou évidents…

VSec

- Récupère des données pour aider l'intruseur, par ex :
  - Netbios : listes de comptes, d'administrateurs, de partages, de logiciels…
  - Oracle : listes de bases, de comptes, d'administrateurs, de tables…
- Dans IKare ces données permettent de détecter des changements inopportuns, par exemples :
  - Nouvel utilisateur devenu administrateur,
  - Partage avec des restrictions amoindries…
- VSec n'effectue que des tests anonymes
  - Ou avec des comptes par défaut.

Scanners de vulnérabilités

- Ils requièrent plus de ressources sur le réseau et les systèmes testés
    - et ne peuvent pas être lancés aussi souvent.
- Ils peuvent générer de nombreux faux-positifs
    - IKare permet de limiter leurs impacts
        - Par la corrélation des événements,
        - Par l'action des administrateurs.
- Ils peuvent utiliser un compte privilégié (ssh, netbios) pour
    - Accéder à la configuration complète du système,
        - Versions des navigateurs, lecteurs PDF, clients de messagerie…
    - Minimiser les faux positifs et les risques de DoS.

Scans

- Gestion des réseaux
    - Fonction de découverte
    - Hôtes, réseaux, listes noires.

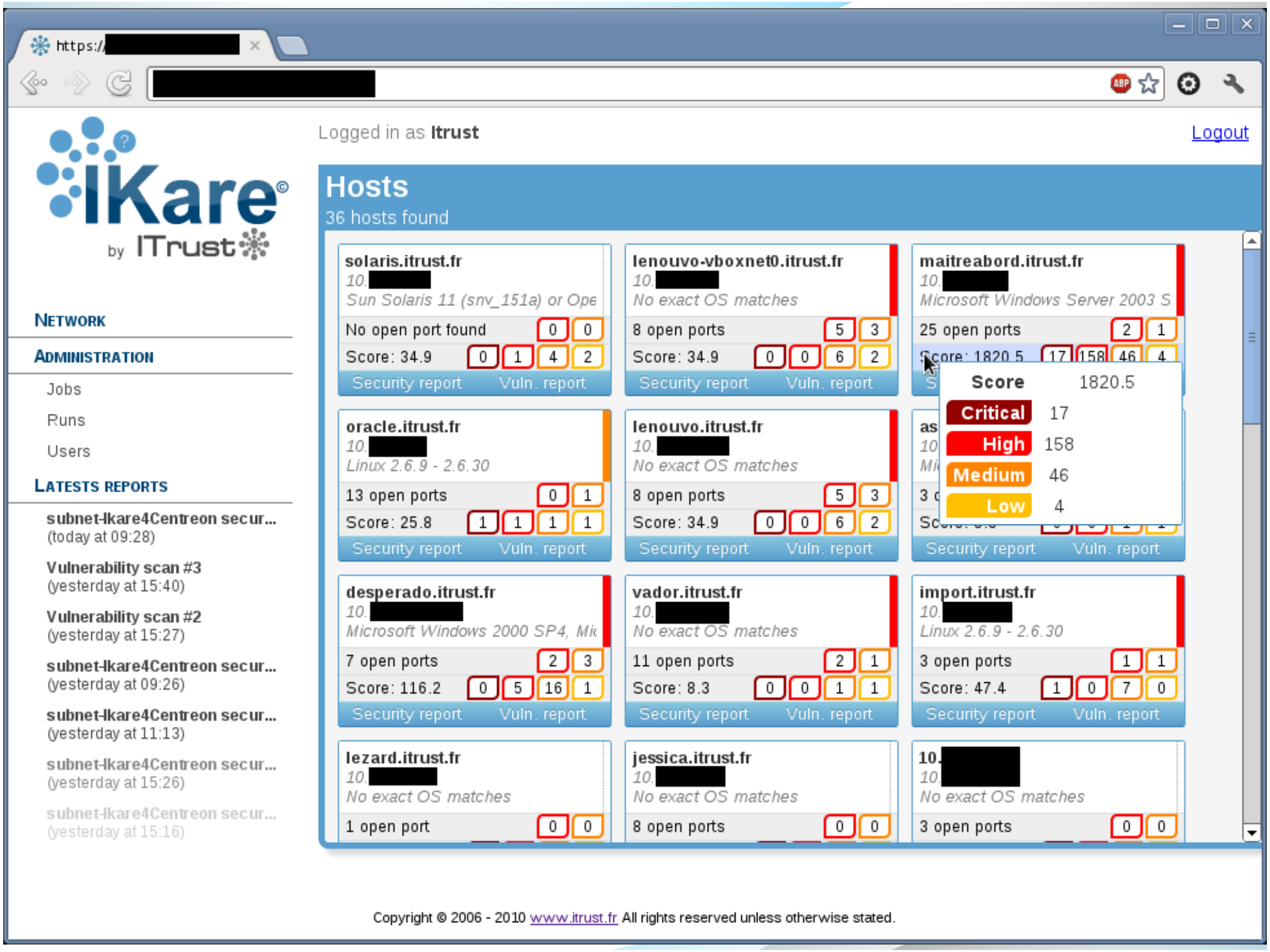
- Gestion des scans
    - Leurs périodicités (jour et/ou heure) et
    - Leurs propriétés
        - Scanners,
        - Intervalles de ports,
        - Comptes privilégiés

Rapports

- Les administrateurs ont accès aux rapports complets et incrémentaux
    - Pouvant être limités aux niveaux d'alertes souhaités,
    - Par système ou par réseau.

- Les alertes sont envoyées par mail aux administrateurs.

- Les rapports peuvent être triés :
    - Par systèmes (CVSS et criticité) ou
    - Par faille (CVSS et occurrences)
- Pour optimiser le temps de sécurisation du réseau.


https://[redacted]
Logged in as Itrust
Logout
IKare by ITrust
NETWORK
ADMINISTRATION
Jobs
Runs
Users
LATESTS REPORTS
subnet-Ikare4Centreon secur... (today at 09:28)
Vulnerability scan #3 (yesterday at 15:40)
Vulnerability scan #2 (yesterday at 15:27)
subnet-Ikare4Centreon secur... (yesterday at 09:26)
subnet-Ikare4Centreon secur... (yesterday at 11:13)
subnet-Ikare4Centreon secur... (yesterday at 15:26)
subnet-Ikare4Centreon secur... (yesterday at 15:16)
Hosts
36 hosts found
solaris.itrust.fr
10.[redacted]
Sun Solaris 11 (snv_151a) or Ope
No open port found 0 0
Score: 34.9 0 1 4 2
Security report Vuln. report
lenouvo-vboxnet0.itrust.fr
10.[redacted]
No exact OS matches
8 open ports 5 3
Score: 34.9 0 0 6 2
Security report Vuln. report
maitreabord.itrust.fr
10.[redacted]
Microsoft Windows Server 2003 S
25 open ports 2 1
Score: 1820.5 17 158 46 4
Score 1820.5
Critical 17
High 158
Medium 46
Low 4
Security report Vuln. report
oracle.itrust.fr
10.[redacted]
Linux 2.6.9 - 2.6.30
13 open ports 0 1
Score: 25.8 1 1 1 1
Security report Vuln. report
lenouvo.itrust.fr
10.[redacted]
No exact OS matches
8 open ports 5 3
Score: 34.9 0 0 6 2
Security report Vuln. report
desperado.itrust.fr
10.[redacted]
Microsoft Windows 2000 SP4, Mi
7 open ports 2 3
Score: 116.2 0 5 16 1
Security report Vuln. report
vador.itrust.fr
10.[redacted]
No exact OS matches
11 open ports 2 1
Score: 8.3 0 0 1 1
Security report Vuln. report
import.itrust.fr
10.[redacted]
Linux 2.6.9 - 2.6.30
3 open ports 1 1
Score: 47.4 1 0 7 0
Security report Vuln. report
lezard.itrust.fr
10.[redacted]
No exact OS matches
1 open port 0 0
jessica.itrust.fr
10.[redacted]
No exact OS matches
8 open ports 0 0
10.[redacted]
No exact OS matches
3 open ports 0 0
Copyright © 2006 - 2010 www.itrust.fr All rights reserved unless otherwise stated.