WE'VE GOT A LOCK ON THE FUTURE

TOTAL STREAM PROTECTION IS THE KEY

CYBERGUARD WORLDWIDE

Les critères communs et la certification

Christian Damour
christian.damour@aql.fr

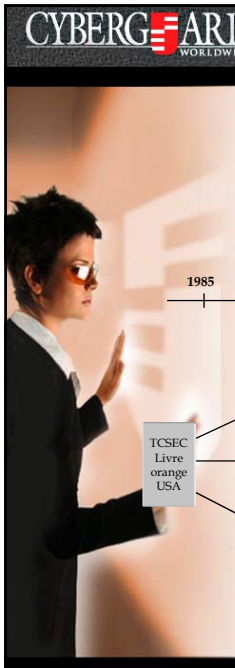
Yann Berson
yann@webwasher.com

SILICOMP-AQL

webwasher
A CYBERGUARD COMPANY

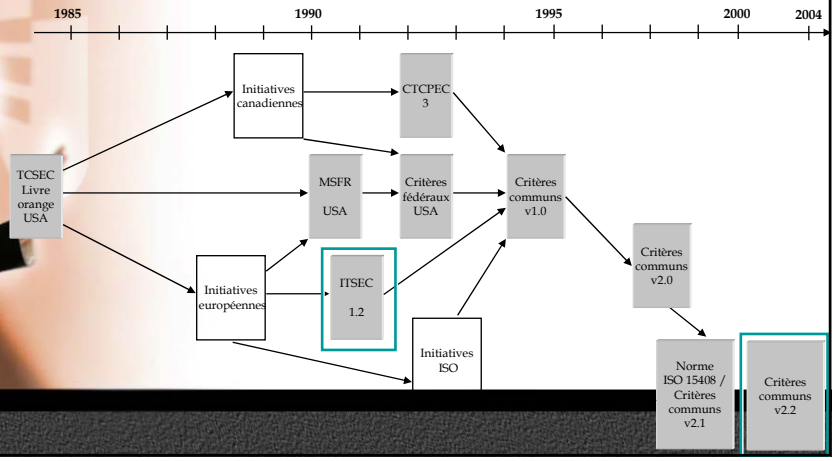
Agenda

- **Historique des critères communs**
- **Que sont les critères communs**
- **Reconnaissance internationale**
- **Les niveaux de confiance**
- **La cible d'évaluation**
- **Les profils de protection (PP)**
  - Le projet Mélèze
- **Le schéma Français**
  - La DCSSI
  - Les CESTI
- **Expérience de certification : Cyberguard**
  - Historique
  - « Assurance continuity »
  - Zéro vulnérabilité
  - TSP (Firewall/VPN v6.1.2)
- **Plus d'infos : Les liens**
- **(BS 7799 Section 8.1.1)**



Historique des CC

- **Uniformisation de ITSEC (EU), TCSEC (US) et CTCPEC (Can.)**



CYBERGUARD WORLDWIDE

Que sont les critères communs

- **Définissent une référence quant à la sécurité apportée (ou pas) par un produit ou système**
- **En référence à sa cible de sécurité**
- **Sur la base d'un niveau d'évaluation (ou niveau de confiance)**
- **Critères génériques applicables à tout type de produit (logiciel et/ou matériel)**

CYBERGUARD WORLDWIDE

Que sont les critères communs

- **Anti-Virus**
- **Key Recovery**
- **PKI/KMI**
- **Switches and Routers**
- **Biometric**
- **Remote Access**
- **System Access Control**
- **Certificate Management**
- **Mobile Code**
- **Secure Messaging**
- **Tokens**
- **Firewalls**
- **Multiple Domain Solutions**
- **Security Management**
- **Trusted DBMS Guard**
- **Network Mgmt**
- **Sensitive Data Protection**
- **VPN**
- **IDS/IPS**
- **Operating System**
- **Single-Level Web Server**
- **WLAN**
- **Peripheral Switch**
- **Smart Cards**

CYBERGUARD WORLDWIDE

Reconnaissance internationale

- **Standard ISO 15408**
- **Valeur réciproque (CCRA : Common Criteria Recognition Arrangement) pour tout certificat émis par l'Australie (et Nouvelle-Zélande), le Canada, la France, l'Allemagne, le Royaume Unis, les Etats-Unis,** *(*)la Finlande, la Grèce, l'Italie, l'Israël, le Japon, la Hollande, la Norvège et L'Espagne* **jusqu'au niveau EAL4**
- **Valeur réciproque jusqu'au niveau EAL7 entre les pays européens**

(*) Ces pays de disposent pas de centres d'évaluation agréés

CYBERGUARD WORLDWIDE

Les niveaux de confiance

- **Niveaux de confiance (d'assurance) prédéfinis : Evaluation Assurance Level (EAL1-EAL7) :**
  - Niveau d'assurance de l'évaluation 2 (EAL2) : testé structurellement
  - Niveau d'assurance de l'évaluation 4 (EAL4) : conçu, testé et revu méthodiquement

Les niveaux de confiance

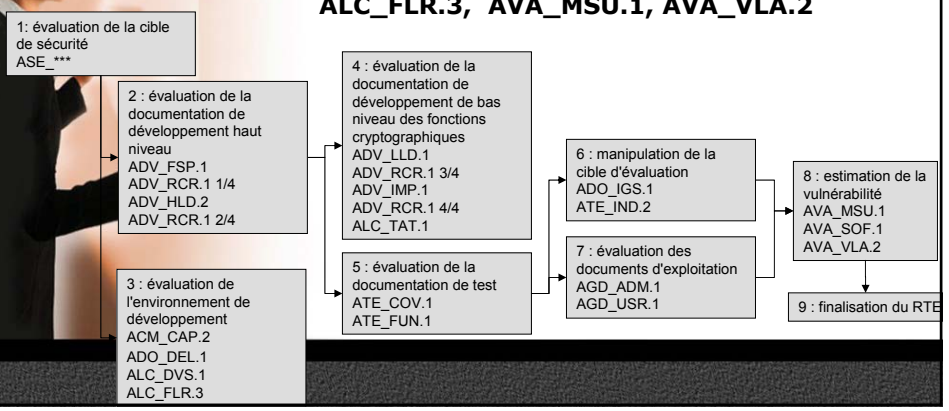
Classe d'assurance	Famille d'assurance	Composants d'assurance par niveau d'assurance de l'évaluation							niveau retenu pour le paquet EAL2+ de qualification au niveau
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	
	ACM_AUT				1	1	2	2	
Gestion de configuration	ACM_CAP	1	2	3	4	4	5	5	**2**
	ACM_SCP			1	2	3	3	3	
	ADO_DEL		1	1	2	2	2	3	**1**
Livraison et exploitation	ADO_IGS	1	1	1	1	1	1	1	**1**
	ADV_FSP	1	1	1	2	3	3	4	**1**
Développement	ADV_HLD		1	2	2	3	4	5	**2**
	ADV_IMP				1	2	3	3	**1**
	ADV_INT					1	2	3	
	ADV_LLD				1	1	2	2	**1**
	ADV_RCR	1	1	1	1	2	2	3	**1**
	ADV_SPM				1	3	3	3	
	AGD_ADM	1	1	1	1	1	1	1	**1**
Guides	AGD_USR	1	1	1	1	1	1	1	**1**
	ALC_DVS			1	1	1	2	2	**1**
Support au Cycle de vie	ALC_FLR								**3**
	ALC_LCD				1	2	2	3	
	ALC_TAT				1	2	3	3	**1**
	ATE_COV		1	2	2	2	3	3	**1**
Tests	ATE_DPT			1	1	2	2	3	
	ATE_FUN		1	1	1	1	2	2	**1**
	ATE_IND	1	2	2	2	2	2	3	**2**
	AVA_CCA					1	2	2	
Estimation des vulnérabilités	AVA_MSU			1	2	2	3	3	**1**
	AVA_SOF		1	1	1	1	1	1	**1**
	AVA_VLA		1	1	2	3	4	4	**2**

Les packages

- **Les augmentations, « + » ou packages**
  - ALC_FLR.3
  - ADV_IMP.2
  - ALC_DVS.2
  - AVA_VLA.2
  - …

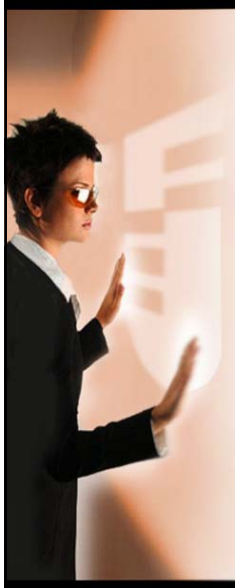
Exemple

- **Exemple « Qualification niveau standard » EAL2 augmenté des composants d'assurance suivants : ADV_HLD.2, ADV_LLD.1, ADV_IMP.1, ALC_TAT.1, ALC_DVS.1, ALC_FLR.3, AVA_MSU.1, AVA_VLA.2**



La cible d'évaluation

- **Ou TOE (Target Of Evaluation)**
- **Elément primordial**
- **Périmètre de l'évaluation : quels éléments de son produit le commanditaire souhaite faire certifier et comment**
- **Explicité dans la cible de sécurité / le rapport de certification**



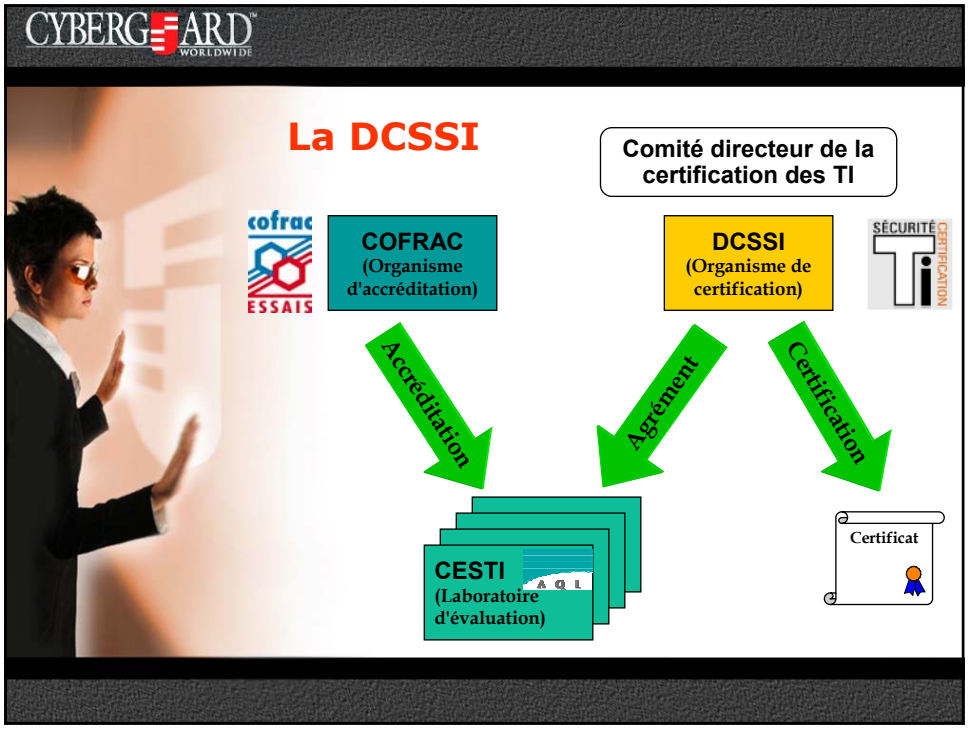
Les profils de protection (PP)

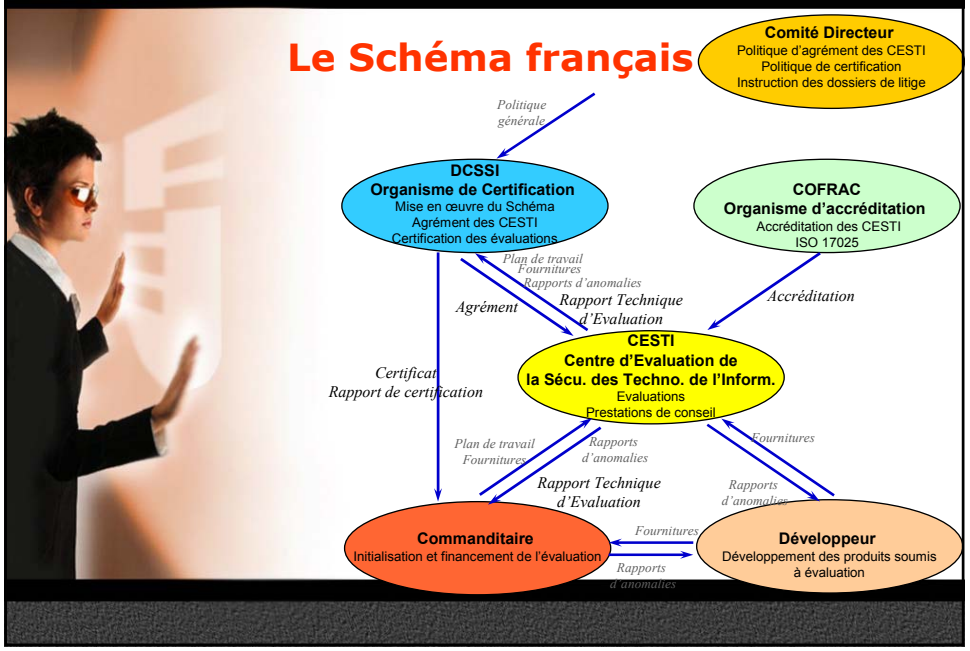
- **Définissent des objectifs et exigences de sécurité**
- **Cibles d'évaluation communes, définies dans le cadre des CC**
- **Les PP eux-même peuvent être certifiés**
- **Communs et réutilisables :**
  - Homogénéisation
  - Comparaison
  - Réduction des délais et des coûts

Le projet Mélèze

- **A la demande du gouvernement français**
- **En cours de définition**
- **Base de discussion industrielle**
- **Firewall d'interconnexion de réseaux IP**
- **Piloté par Arkoon/AQL/Oppida**
- **Groupes de travail utilisateurs et développeurs**
- **EAL2+ (qualification niveau standard)**
- **A terme : Norme nationale AFNOR**


CYBERGUARD
WORLDWIDE
La DCSSI
• Direction Centrale de la Sécurité des Systèmes d'Information
• Organisme français
• Dépend du Premier Ministre
• http://www.ssi.gouv.fr
• Forte expertise dans le domaine des cartes à puces


CYBERGUARD
WORLDWIDE
La DCSSI
Comité directeur de la certification des TI
cofrac
ESSAIS
COFRAC
(Organisme d'accréditation)
DCSSI
(Organisme de certification)
SÉCURITÉ
CERTIFICATION
Accréditation
Agrément
Certification
CESTI
(Laboratoire d'évaluation)
AQL
Certificat



Les CESTI

- **Les CESTI (Centre d'Evaluation de la Sécurité des Technologies de l'Information), organismes indépendants conduisent les évaluations :**
  - **AQL** (Groupe Silicomp), Rennes
  - **Oppida**, Versailles
  - **Algoriel**, Paris
  - **CEA/LETI**, Grenoble
  - **CEACI**, Toulouse
  - **Serma Technologies**, Bordeaux

http://www.ssi.gouv.fr/fr/confiance/cesti.html

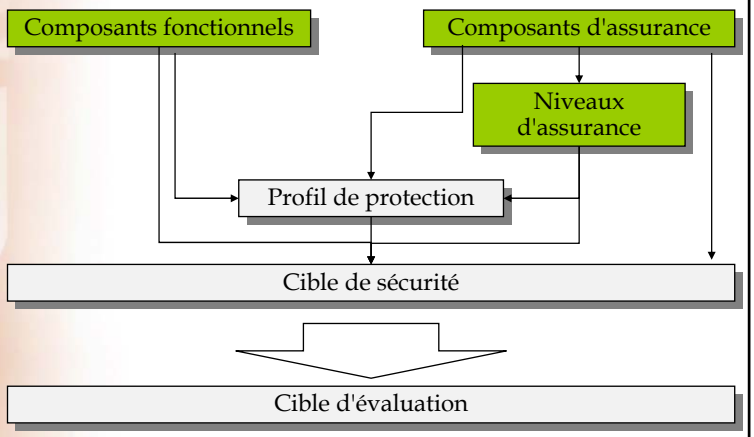
Le CESTI AQL

- **Vers la certification de vos produits ou systèmes selon des critères normalisés**

Agréé DCSSI

ACCREDITATION N° 1-1528
Section Laboratoires
Portée communiquée
sur demande

En résumé



CyberGuard : Historique de 30 ans

- 1974 : **Harris Computer Systems** crée un Département de recherche qui deviendra **CyberGuard**
- 1990 : **SIEMENS** crée un département de recherche qui deviendra **Webwasher**
- 1994 : Filiale de Harris Computer Sytems Corporation
- 1996 : **Spin Off** de HCSC: devient **CyberGuard** Corporation
- *1999 : **Spin Off** de SIEMENS : devient **Webwasher***
- *1999 : Webwasher prend la présidence Technique du Forum ICAP*
- 2000 : technologie FW Proxy sur boîtier APPLIANCE
- 2004 : WebWasher intègre le **groupe CyberGuard**

Historique des certifications

- **TCSEC B1 (Secure Operating System)**
  - 3 Years (1987-1990)
  - RAMP Maintenance Scheme (1990 -1995)
- **ITSEC E3 (CyberGuard Firewall Release 2.1.1e)**
  - 18 Months (1995 -1997)
  - Certificate Maintenance Scheme - (1998 - 2000)
- **ITSEC E3 (CyberGuard Firewall Release 4.3)**
  - 12 months (1999)
  - Certificate Maintenance Scheme (CMS) - **(1999-)**
- **Common Criteria EAL4 (CyberGuard Firewall Release 4.3/Premium Appliance Firewall)**
  - 6 months (2000)
  - Certificate Maintenance Scheme (AMA) - **(2001-)**
    - Interim Releases & Patches for Release 4.3 (2001-)
    - Provides Certification for Release 5.x (introduced Dec 2001)
    - Latest Release 5.2.1 is Certified

CYBERGUARD WORLDWIDE

« Assurance continuity »

- **AMA : Assurance Maintenance**
- **Augmentation**
- **Ré-évaluation permanente**
- **Suivi de processus à chaque étape du produit**
- **(Oblige la qualité et la rigueur)**
- **Coûteux à mettre en place**
- **Le dernière version du produit est certifiée**

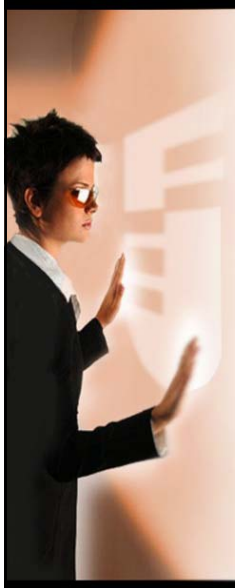
CYBERGUARD WORLDWIDE

Zéro vulnerabilité

Discover the power of zero vulnerability security.

Sources Dated: 03/24/04	CERT	CIAC	BugTraq	X-Force	CVE	Total Reported ** Vulnerabilities
CyberGuard	-	-	-	-	-	0
WatchGuard FireBox	-	-	14	9	10	14
NetScreen	-	-	18	2	2	18
Secure Computing WebShield Gauntlet	1	1	9	6	6	9
Cisco PIX Firewall	2	1	17	3	3	17
Check Point Firewall 1	3	2	28	11	13	29
SonicWall SOHO	-	-	7	3	3	9
Symantec Enterprise Raptor	-	-	11	2	2	11
Nokia Check Point	2	-	2	1	1	4
Border Ware	-	-	1	1	1	1

* **The numbers listed in the "Total Reported Vulnerabilities" column reflect the total number of individual vulnerabilities reported, not the total across all columns, as single vulnerability may be reported by more than one source.

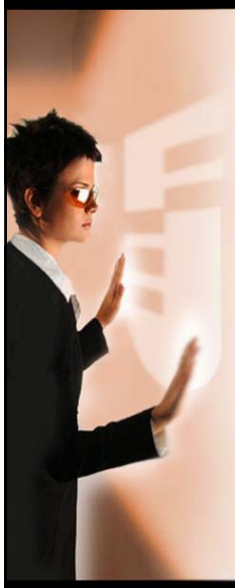


En cours : TSP (Firewall/VPN v6.1.2)

- **Début de l'évaluation : 24 Août 2004**
  - EAL4
  - Augmenté de AVA_VLA.3 (Analyse de vulnérabilités) et ALC_FLR.3 (Correction d'erreurs systématique)
- **4 Profils de Protection, dont :**
  - Application-level Firewall PP for Medium Robustness Environments v1.0 June 28, 2000
  - Traffic Filter Firewall PP for Medium Robustness Environments, v1.4 May 4, 2000

En cours : TSP (Firewall/VPN v6.1.2)

- **Management Software**
- **Packet Filter Engine**
- **NAT**
- **Multiple Authentication Mechanism**
- **Audit subsystem**
- **RSBAC**
- **Telnet, FTP, HTTP and SMTP Proxies**
- **Kernel Extensions (SHIM) (relevant parts of OS)**



Plus d'infos : Les liens

http://www.commoncriteriaportal.org

http://www.ssi.gouv.fr/

http://niap.nist.gov

Merci,
Questions / Réponses

SILICOMP-AQL

webwasher
A CYBERGUARD COMPANY