MEMO – COSC – 11/2018
INFORMATION SUR LES SCANS DE VULNERABILITE

GESTION DU DOCUMENT

Date de la version du mémo : 12/11/2018

Version : 1.0

Auteur : Centre Opérationnel de Sécurité et de Cyberdéfense

GESTION DU DOCUMENT

VALIDATIONS

Diffusion : *à l'ensemble du groupe*

Rédacteur	*Vérificateur*	*Approbateur*
Nom : A.Saltel Fonction : Ingénieur sécurité Date/ visa : 12/11/2018	Nom : S Carpentier Fonction : Responsable COSC Date/ visa : 12/11/2018	Nom : S Carpentier Fonction : Responsable COSC Date/ visa : 12/11/2018

DEMANDE DE SCAN DE SECURITE

RAPPEL

Tout incident de sécurité lié à des attaques ou à des suspicions de malveillance doit faire l'objet d'un incident de sécurité.

Toute demande de scan doit faire l'objet d'une demande :

- HPSM pour la DSI SN
- Redmine pour la DSI SC

Détail des demandes

Type	Env	Scope scanner	Périodicité	Demande	Délai
Qualys	Prod	Groupe	Hebdo	HPSM/Redmine	1 Semaine
Rapid 7	Tous	Groupe	Hebdo	HPSM/Redmine + formulaire	2j
Greenbone	Tous	DSI SN	Sur demande	HPSM	2j
Cyberwatch	Tous	Groupe	Sur demande	Redmine + Formulaire	N/A
Cenzic	NON Prod	Groupe	Sur demande	HPSM	2j

SCANNER DE VULNERABILITE DU COSC

L'objectif de ce mémo est de rappeler le fonctionnement des scans de vulnérabilité qui pourraient occasionner des évènements assimilables à des attaques malveillantes.

Les sources indiquées peuvent être amenées à changer

SCAN EXTERNE AUTOMATIQUE QUALYS

- Périodicité : Hebdomadaire
- Source : 64.39.96.0/20 (weekend), 80.15.71.48/32 (semaine), 62.116.156.85/32 (lundi)
- Type : Non intrusif, authentifié (sur demande), récupération d'informations, analyse des réponses du serveur.

SCAN EXTERNE AUTOMATIQUE RAPID 7

- Périodicité : Hebdomadaire (weekend)
- Source : 185.62.220.250, 185.62.220.251, 185.62.220.252
- Type : Non intrusif, non authentifié, récupération d'informations, analyse des réponses du serveur.

SCAN INTERNE GREENBONE – DSI SN

- Périodicité : Sur demande
- Source : 172.22.24.51
- Type : Non intrusif, authentifié, récupération des versions logicielles et remontée des vulnérabilités connues sur ces versions.

SCAN INTERNE CYBERWATCH

- Périodicité : Sur demande
- Source : 93.92.105.156, 93.92.105.157
- Type : Non intrusif, authentifié, récupération des versions logicielles et remontée des vulnérabilités connues sur ces versions.

SCAN INTERNE CENZIC

- Périodicité : Sur demande
- Source : 172.22.204.98
- Type : Intrusif, authentifié (sur demande), récupération d'informations, tests d'intrusion, analyse des réponses du serveur.