CERT-IST
INDUSTRIE | SERVICES | TERTIAIRE

CERT-IST
290, Allée du Lac
31670 LABEGE
+33 5 34 39 44 88
info@cert-ist.com
www.cert-ist.com

CERT-IST

INDUSTRIE | SERVICES | TERTIAIRE

COMPUTER
EMERGENCY RESPONSE TEAM

Industrie Services Tertiaire

CERT-IST

INDUSTRIE | SERVICES | TERTIAIRE

Créé par un consortium d'entreprises françaises, le Cert-IST a été en 1999 l'un des trois premiers CERT en France, avec le Cert-Renater (communauté de l'enseignement et de la recherche) et CERT-FR.

Au niveau international, le Cert-IST est membre du FIRST (Forum for Incident Response and Security Teams) depuis 1999.

Le Cert-IST s'est constitué en 2003 en association de loi 1901 (publiée au JO le 26 avril 2003).

Au niveau européen, le Cert-IST est membre accrédité TI TF-CSIRT Level 2 depuis 2006. Il a été aussi le coordinateur du projet européen EISPP.

La base de vulnérabilités du Cert-IST est reconnue par MITRE comme produit compatible CVE, assurant ainsi un référencement unique des vulnérabilités pour l'ensemble de la communauté sécurité.

La Base de vulnérabilités du Cert-IST intègre également les informations CVSS et CPE.

Une équipe dédiée ayant plus de 20 ans d'expérience dans ce domaine assure la fourniture des services du Cert-IST et maintient sa base de connaissances.

OBJECTIFS & MISSIONS

Le Cert-IST (Computer Emergency Response Team – Industrie Services et Tertiaire) est un centre d'alerte et de réaction aux attaques informatiques destiné aux entreprises.

Il propose à ses adhérents des services de prévention des risques et d'assistance aux traitements d'incidents.

Le Cert-IST est indépendant vis-à-vis des éditeurs et des constructeurs. Il travaille pour la commnauté en assurant le partage d'expérience.

L'activité de prévention du Cert-IST s'appuie sur une analyse quotidienne des nouvelles vulnérabilités, de leurs criticités et des moyens de protection pour y répondre.
Le Cert-IST diffuse auprès de ses membres des avis et alertes de sécurité qui leur permettent d'être informés sur ces menaces et sur les parades.

Il entretient des relations privilégiées avec ses homologues.

Le Cert-IST peut s'appuyer sur le réseau mondial de plus de 690 CERTS affiliés au FIRST, ce qui lui donne accès à un système d'alerte unique au monde en fournissant les points de contact nécessaires à l'investigation des incidents trans-frontaliers et en offrant un accès privilégié aux informations non encore publiques. Le Cert-IST a parrainé plusieurs Certs (CERT National Tunisien, BNP-Paribas, l'Orange-CERT-CC) pour leur admission au FIRST.

Le Cert-IST assiste également les membres de l'association en cas d'incident de sécurité majeur.

Ce service apporte une expertise dans l'investigation de cet incident qui permet d'analyser les problèmes constatés (comportement anormal, perte de disponibilité ou de confidentialité…), pour en identifier les causes (volontaires ou involontaires) et l'origine. Il permet également de proposer des actions correctives et préventives en vue de permettre une remise en service opérationnelle et sécurisée.

SYNTHÈSE DE L'OFFRE

VEILLE SUR LES VULNÉRABILITÉS

Émission personnalisée d'avis de sécurité et d'alertes sous différents formats. Résulte de l'analyse et du recoupement des informations recueillies quotidiennement auprès de nombreuses sources et de la qualification selon des critères objectifs.

• Veille SCADA
En complément des avis de sécurité sur les produits SCADA, ce bulletin présente une synthèse de l'actualité sur la sécurité informatique des systèmes SCADA.

• Accès à la base de vulnérabilités
La base de vulnérabilités du Cert-IST, alimentée depuis 1997, couvre l'ensemble des composants matériels et logiciels les plus couramment utilisés dans les systèmes d'information.
Accès à un support téléphonique ou mail, en cas de demande d'informations complémentaires sur un avis émis.

VEILLE SUR LES ATTAQUES

Ce service a pour objectif de répertorier les attaques connues (les attaquants, leurs cibles, les TTP associés …) et les marqueurs techniques (i.e. IOC) qui permettent d'identifier ces attaques.

• Fiches attaques
Information consolidée sur un groupe d'attaquants et/ou une campagne d'attaque, incluant les TTP (Information sur les Tactiques, Techniques et Procédures utilisées par les attaquants) et des pointeurs sur des évènements et des IOC associés.

• Base d'IOC
Marqueurs techniques qualifiés permettant de caractériser une attaque ou un attaquant, enrichis avec des élèments de contextualisation.

INTERNET EXPOSURE

Collecte quotidienne et corrélation d'informations issues de sources de confiance (publiques et privées) afin de surveiller les dépots de nom de domaine (typosquatting, ...), d'identifier les machines suspectées d'être mal configurées et/ ou compromises et appartenant au Système d'Information de ses membres.

RÉACTION AUX ATTAQUES

• Assistance sur incident
Service d'assistance. Etablissement d'une relation de confiance permettant de traiter les problèmes de sécurité avec toutes les garanties de confidentialité requises.
Recommandations correctives pour pallier l'incident et générales pour améliorer le niveau global de sécurité. Utilisation si nécessaire des contacts Nationaux et Internationaux pour identifier et neutraliser les sources des attaques.

+2 100
Avis / an

+7 800
Mises à jour d'avis / an

+16
Alertes / an

+3 100
Produits suivis

+33 000
Versions associées

CERT-IST : UN PARTENAIRE DE CONFIANCE

La pérennité du Cert-IST est assurée par l'engagement de ses membres.
La confiance des membres du Cert-IST est renforcée chaque jour par :

- la véracité et la complétude des informations transmises
- la confidentialité des informations
- la garantie de l'objectivité
- la pérennité de l'activité