الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Tunisian Computer Emergency Response Team

Overview

SMII Mondher

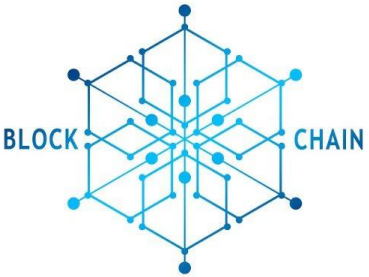
Cyber Security Analyst | Pentester | Bug Hunter

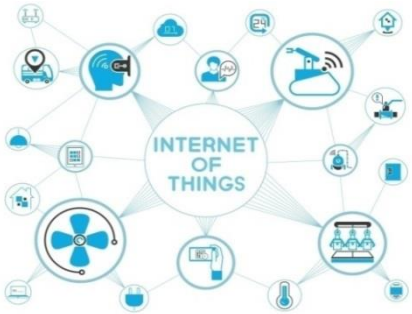
Information Sharing & Analysis Center – ISAC

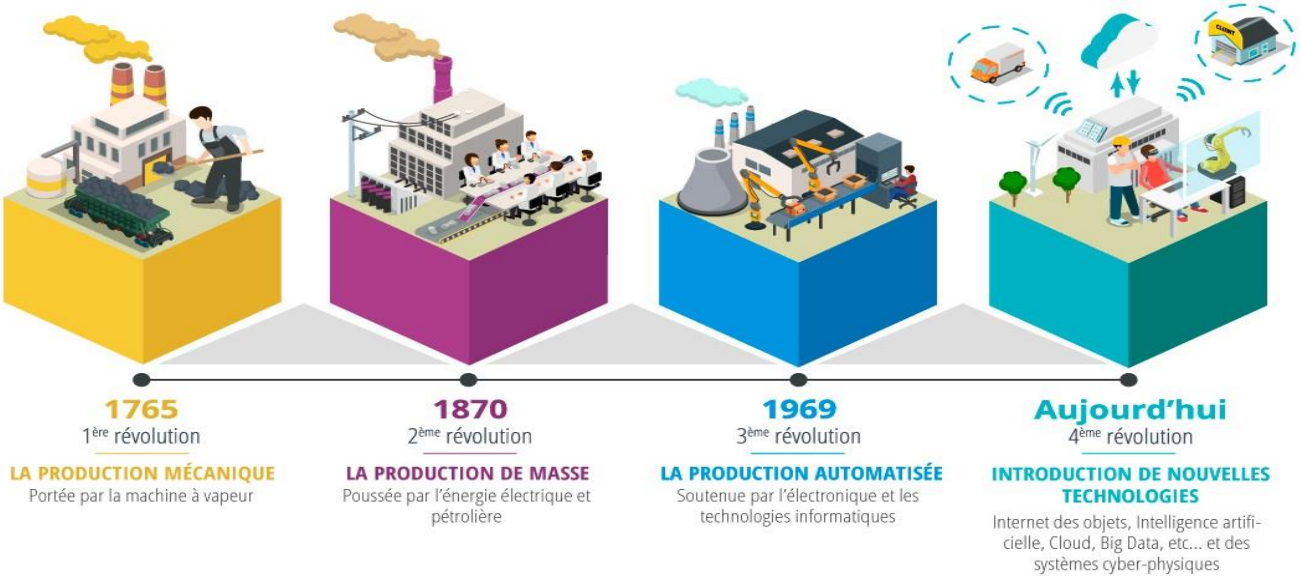
ISO 27001 LI | ISO 22301 LI | Penetration Testing and Ethical Hacking

smii.mondher@ansi.tn

Révolution numérique

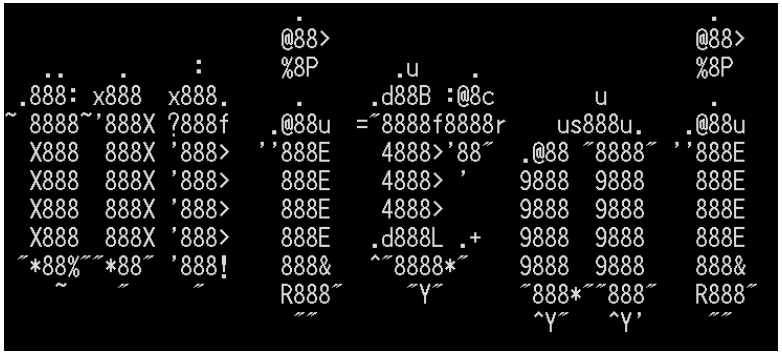






الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique

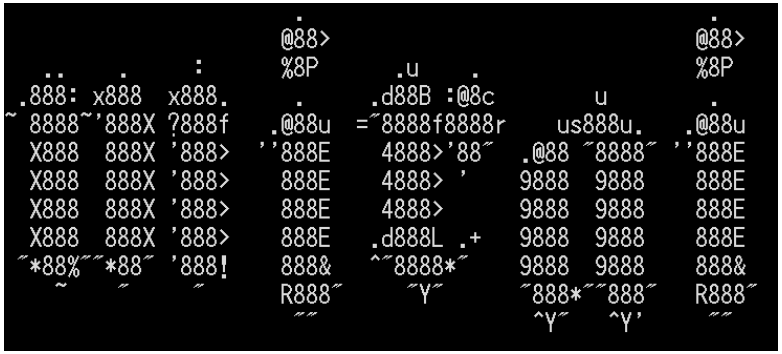
Révolution numérique



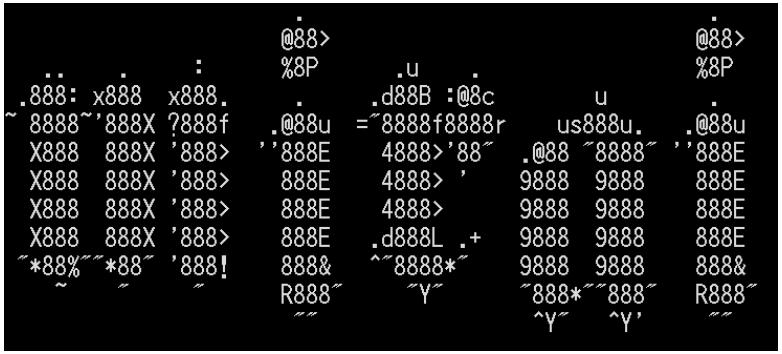
الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Révolution numérique

Révolution numérique



Révolution numérique



الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Révolution numérique

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Computer Emergency Response Team

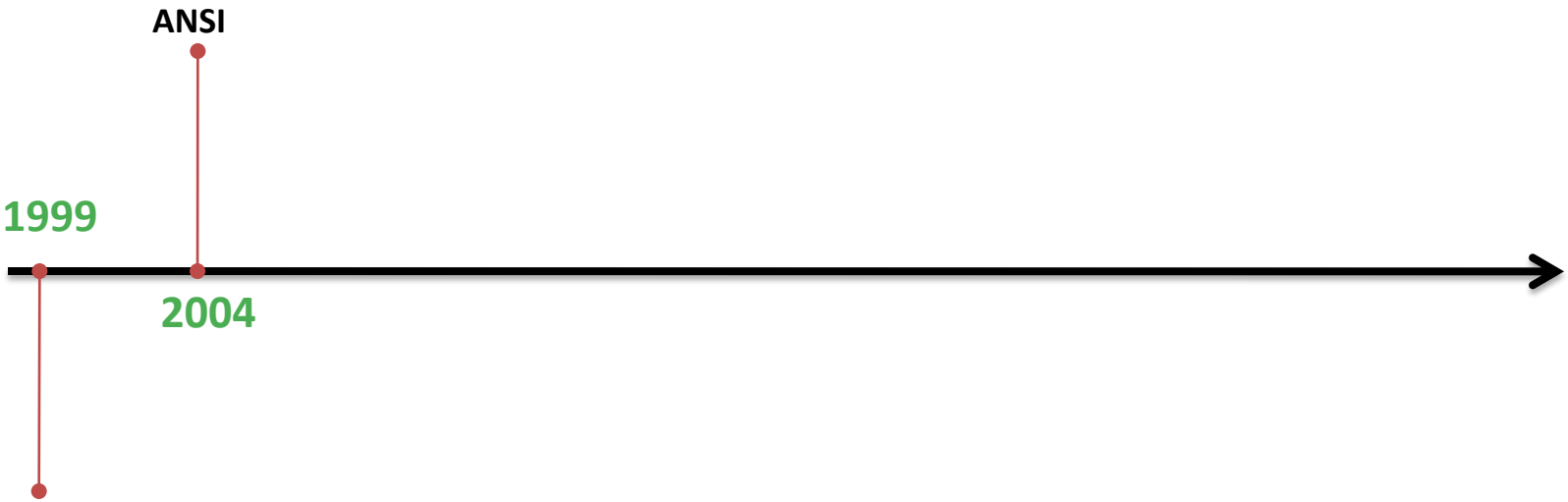
Un **computer emergency response team** (**CERT**) ou **computer security incident response team** (**CSIRT**) est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations.

L'appellation CSIRT est privilégiée en Europe, CERT étant une marque déposée aux États-Unis par l'université Carnegie-Mellon.

Timeline

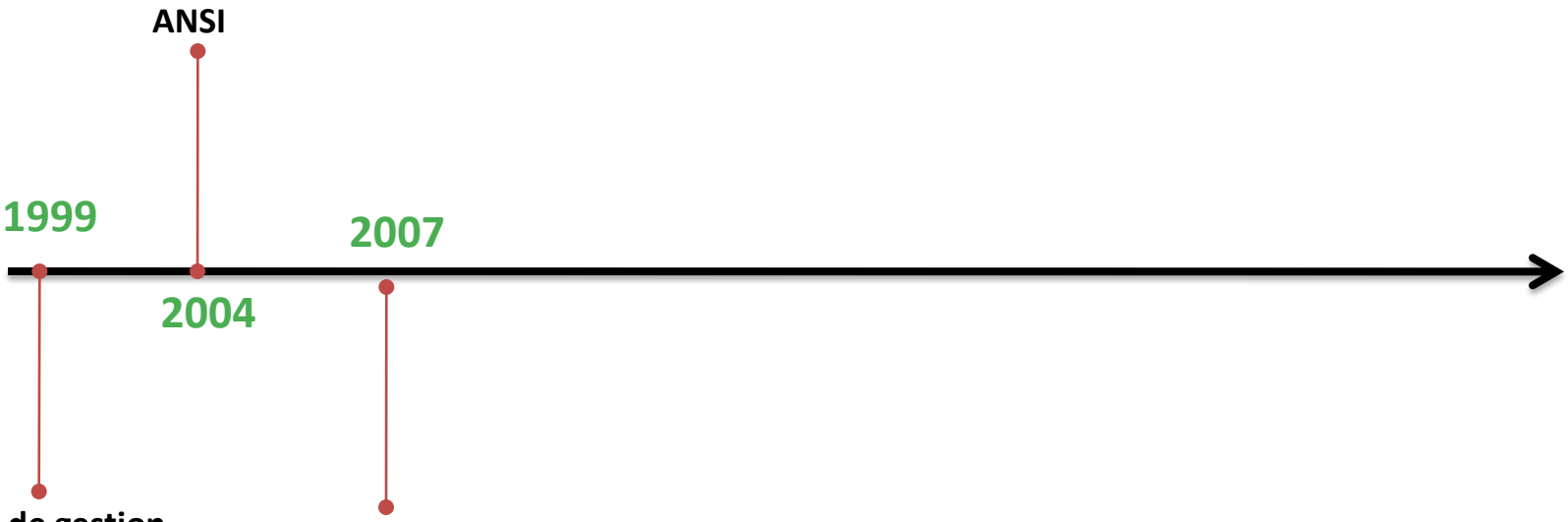
Timeline

promulgation du cadre réglementaire
Création de l'ANSI



Timeline

promulgation du cadre réglementaire
Création de l'ANSI



Unité de gestion par objectifs

FIRST

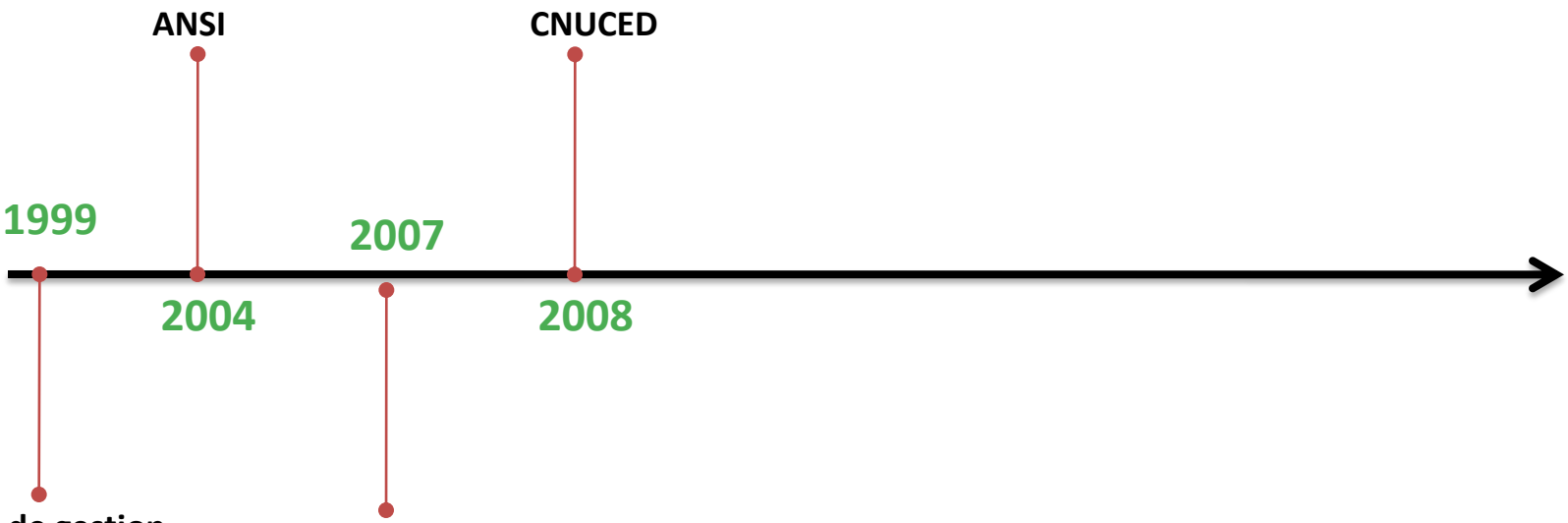
Adhésion au Forum of Incident Response and Security Teams

الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique

Timeline

promulgation du cadre réglementaire
Création de l'ANSI

Adhésion au réseau des centres d'excellence



Unité de gestion par objectifs

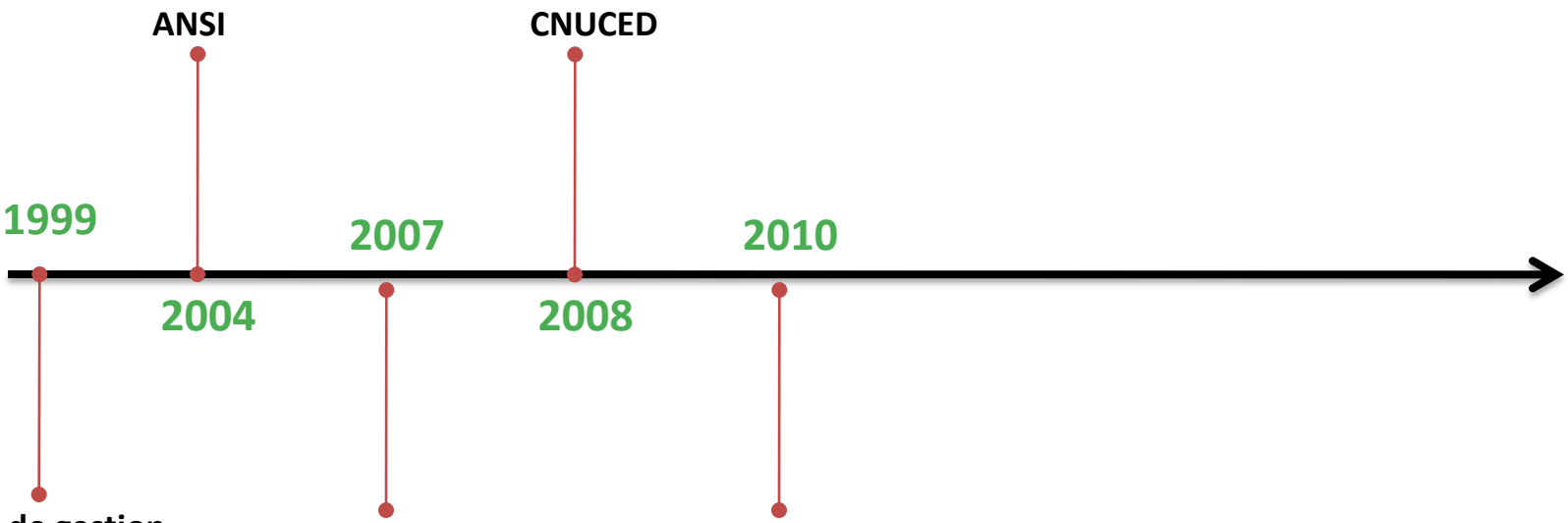
FIRST

Adhésion au Forum of Incident Response and Security Teams

Timeline

promulgation du cadre réglementaire
Création de l'ANSI

Adhésion au réseau des centres d'excellence



Unité de gestion par objectifs

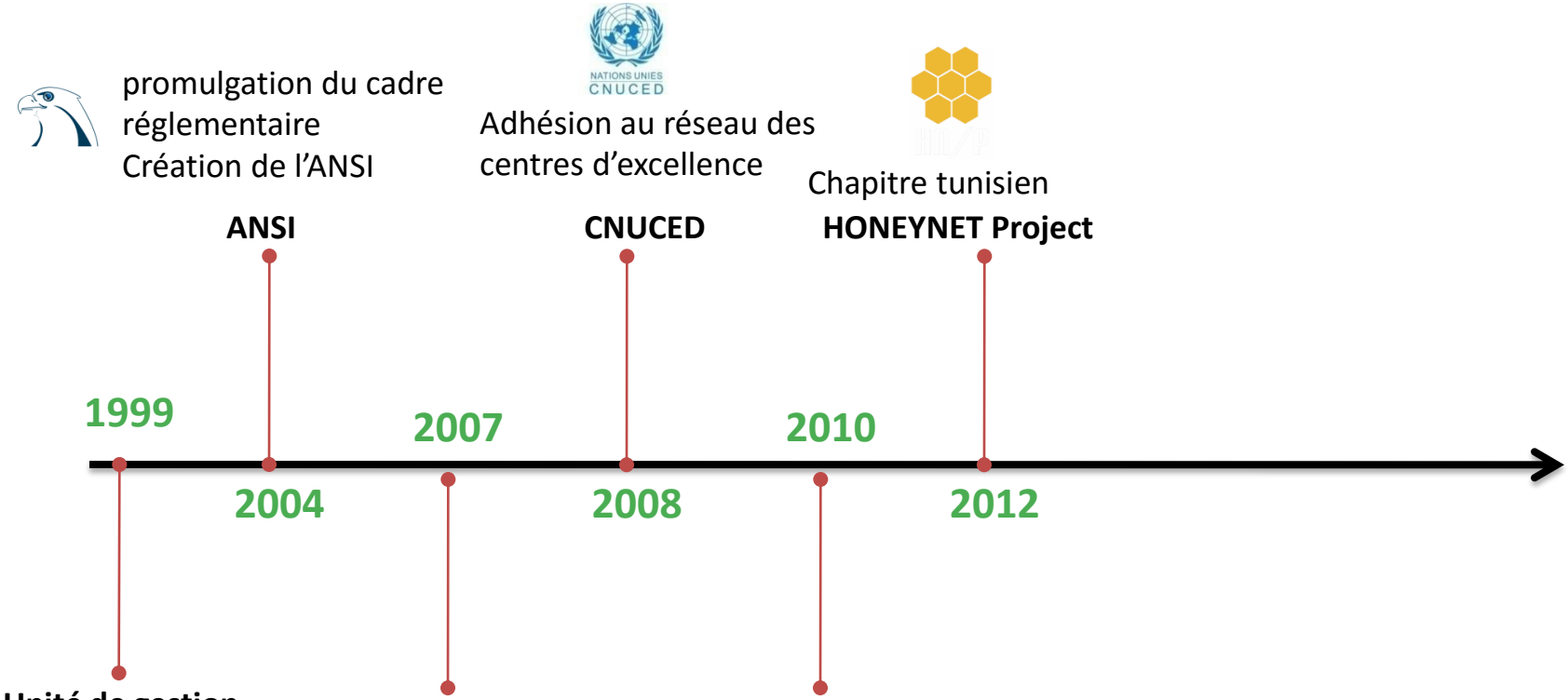
FIRST

Adhésion au Forum of Incident Response and Security Teams

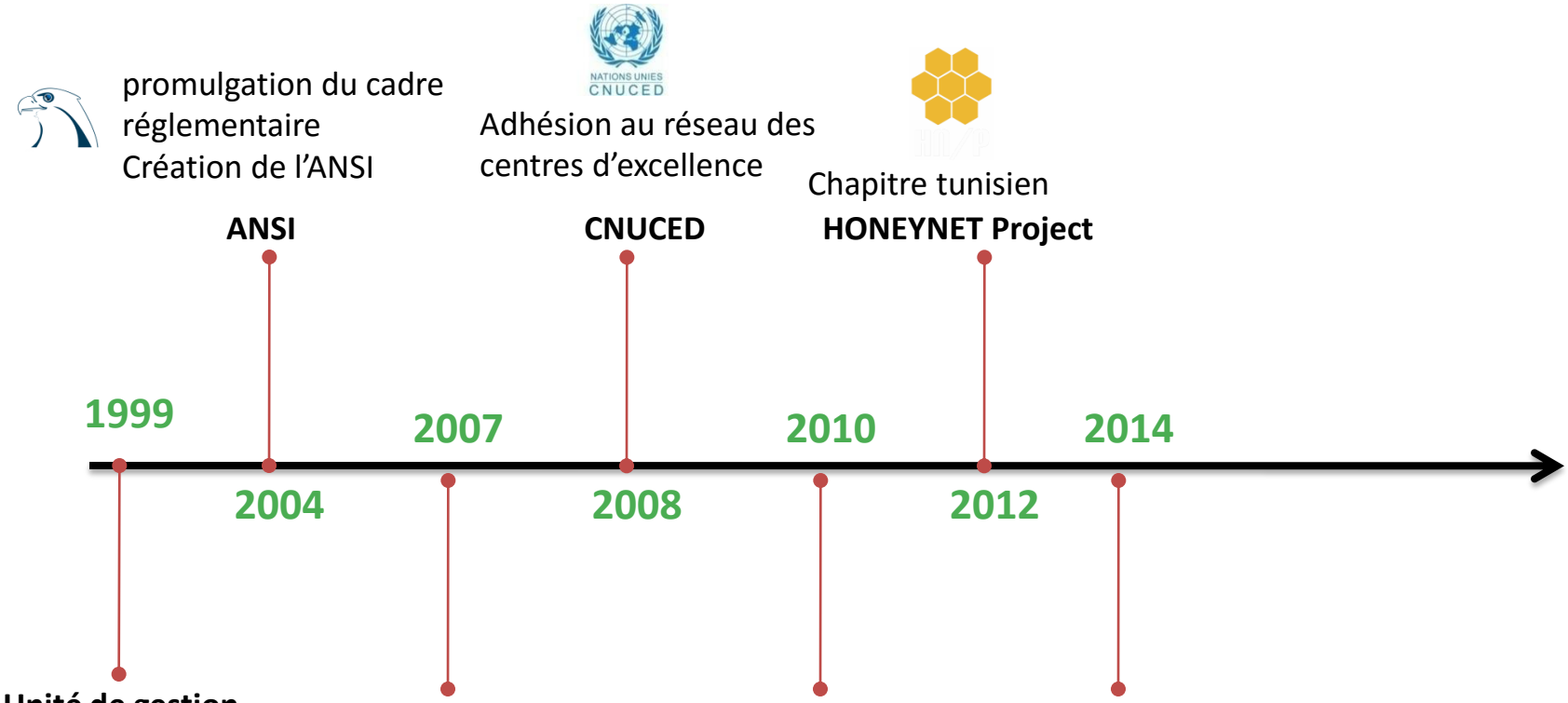
Afrique du sud

Assistance à la création du CERT sud africain et accompagnement à l'adhésion au FIRST

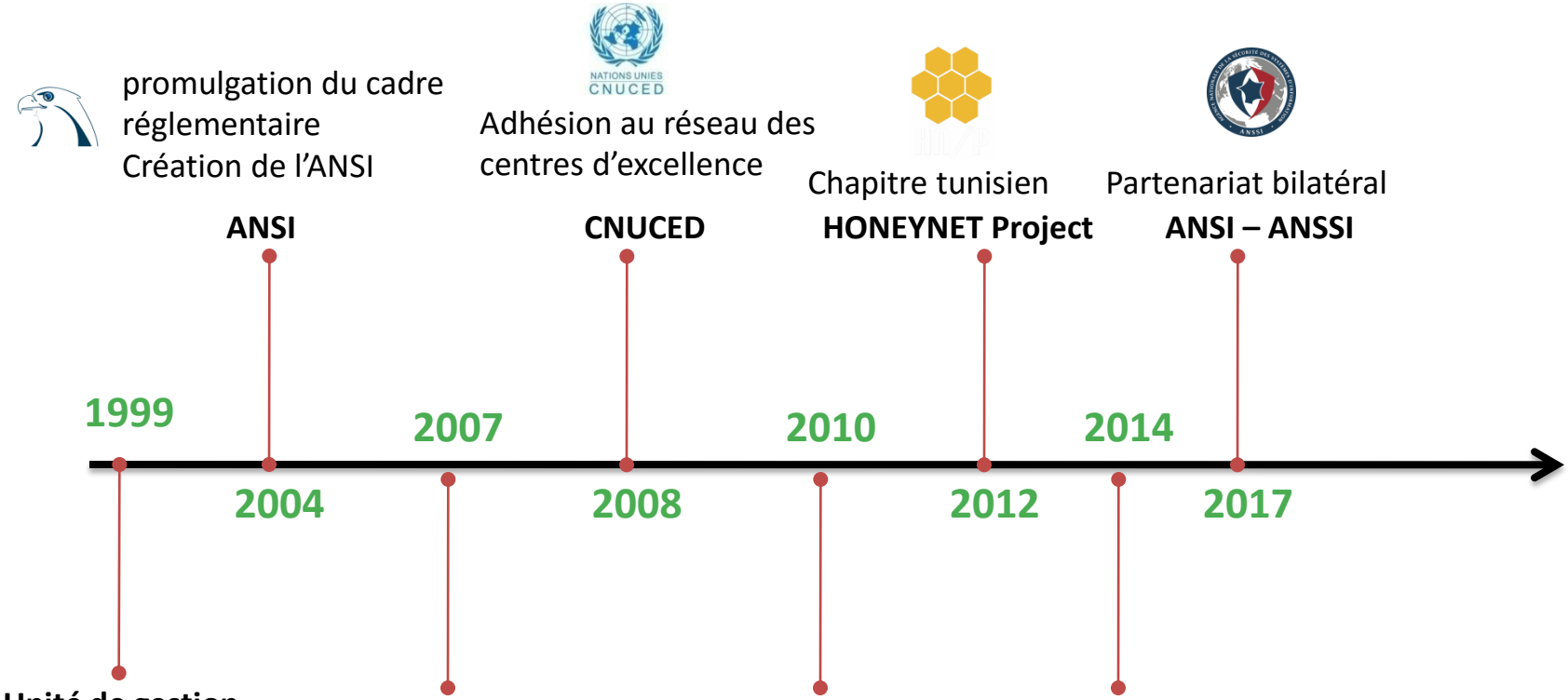
Timeline


promulgation du cadre réglementaire
Création de l'ANSI
ANSI
1999
2004
Unité de gestion par objectifs
Adhésion au réseau des centres d'excellence
CNUCED
2007
2008
FIRST
Adhésion au Forum of Incident Response and Security Teams
Chapitre tunisien
HONEYNET Project
2010
2012
Afrique du sud
Assistance à la création du CERT sud africain et accompagnement à l'adhésion au FIRST

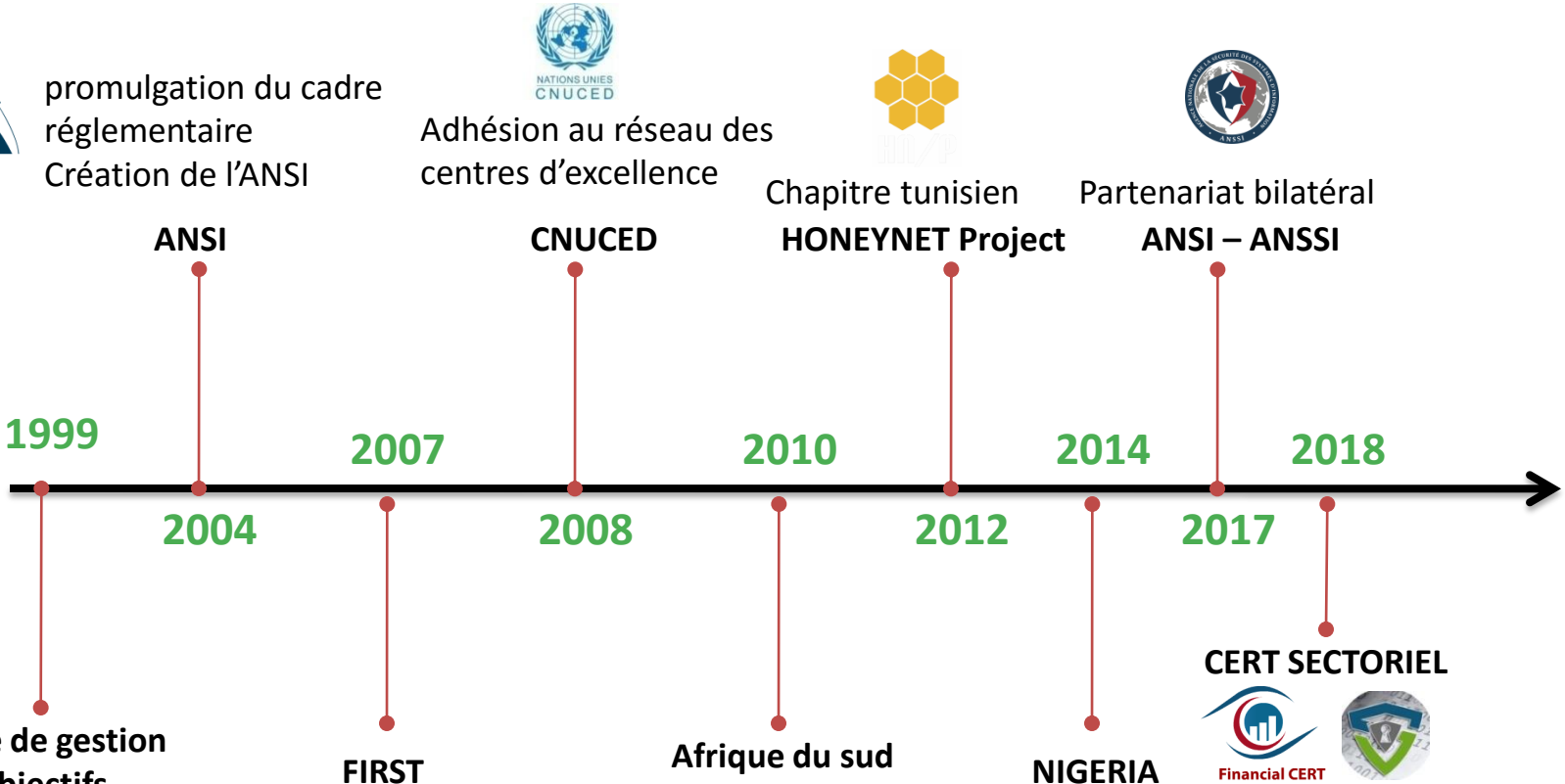
Timeline


promulgation du cadre réglementaire
Création de l'ANSI
Adhésion au réseau des centres d'excellence
Chapitre tunisien
ANSI
CNUCED
HONEYNET Project
1999
2004
2007
2008
2010
2012
2014
Unité de gestion par objectifs
FIRST
Adhésion au Forum of Incident Response and Security Teams
Afrique du sud
Assistance à la création du CERT sud africain et accompagnement à l'adhésion au FIRST
NIGERIA
Assistance à la création du CERT Nigérien et accompagnement à l'adhésion au FIRST

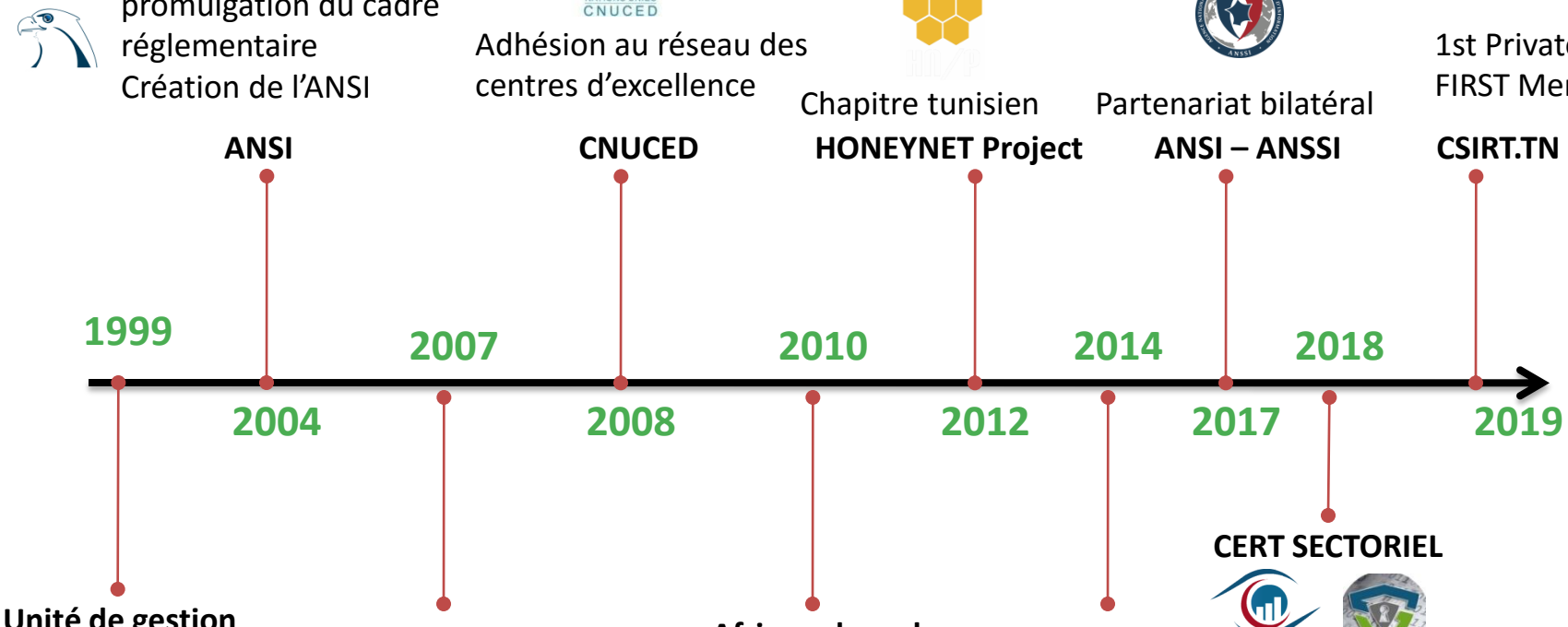
Timeline


promulgation du cadre réglementaire
Création de l'ANSI
ANSI
Adhésion au réseau des centres d'excellence
CNUCED
Chapitre tunisien
HONEYNET Project
Partenariat bilatéral
ANSI – ANSSI
1999
2004
2007
2008
2010
2012
2014
2017
Unité de gestion par objectifs
FIRST
Adhésion au Forum of Incident Response and Security Teams
Afrique du sud
Assistance à la création du CERT sud africain et accompagnement à l'adhésion au FIRST
NIGERIA
Assistance à la création du CERT Nigérien et accompagnement à l'adhésion au FIRST

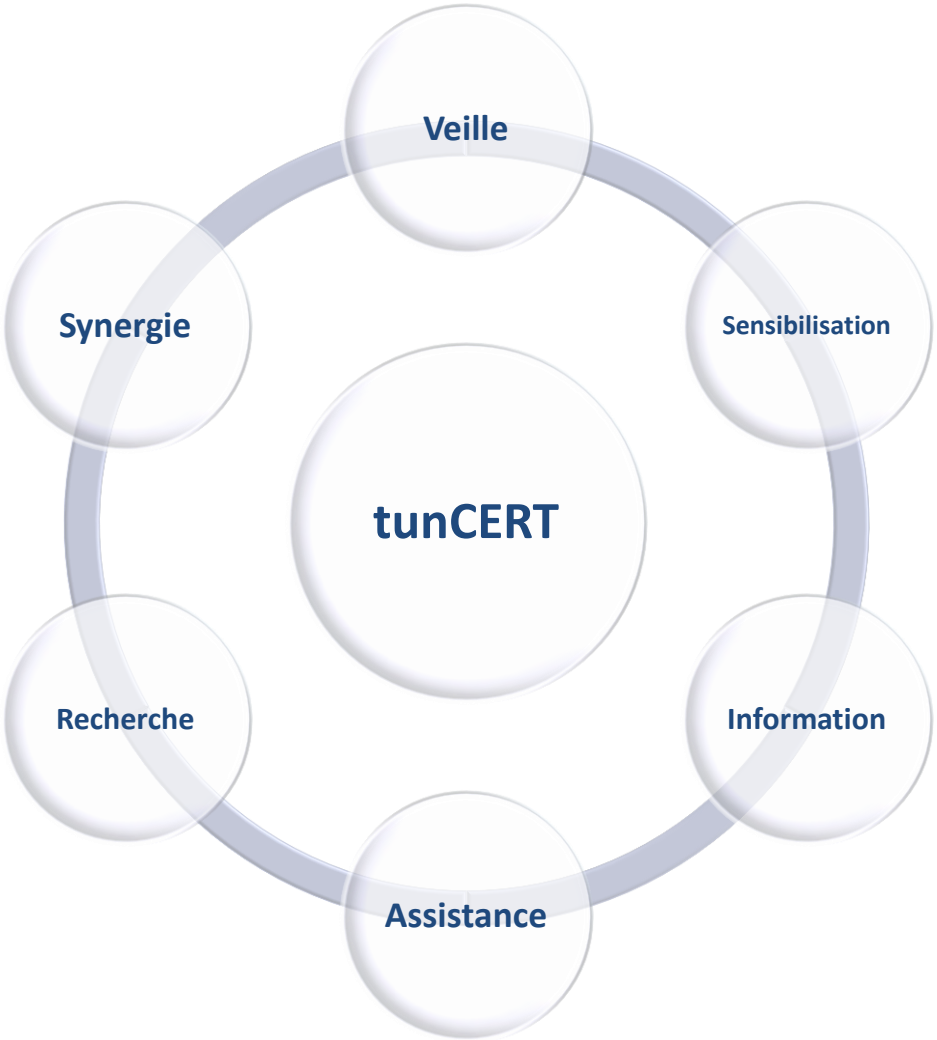
Timeline


1999
promulgation du cadre réglementaire
Création de l'ANSI
ANSI
2004
Unité de gestion par objectifs
2007
FIRST
Adhésion au Forum of Incident Response and Security Teams
2008
CNUCED
Adhésion au réseau des centres d'excellence
2010
Afrique du sud
Assistance à la création du CERT sud africain et accompagnement à l'adhésion au FIRST
2012
HONEYNET Project
Chapitre tunisien
2014
NIGERIA
Assistance à la création du CERT Nigérien et accompagnement à l'adhésion au FIRST
2017
ANSI – ANSSI
Partenariat bilatéral
2018
CERT SECTORIEL
Financial CERT

Timeline


1999
promulgation du cadre réglementaire
Création de l'ANSI
ANSI
2004
2007
FIRST
Adhésion au Forum of Incident Response and Security Teams
CNUCED
2008
Adhésion au réseau des centres d'excellence
2010
Afrique du sud
Assistance à la création du CERT sud africain et accompagnement à l'adhésion au FIRST
HONEYNET Project
2012
Chapitre tunisien
2014
NIGERIA
Assistance à la création du CERT Nigérian et accompagnement à l'adhésion au FIRST
ANSI – ANSSI
2017
Partenariat bilatéral
2018
CERT SECTORIEL
CSIRT.TN
2019
1st Private CERT
FIRST Member
Unité de gestion par objectifs

tunCERT : Missions



tunCERT : Services

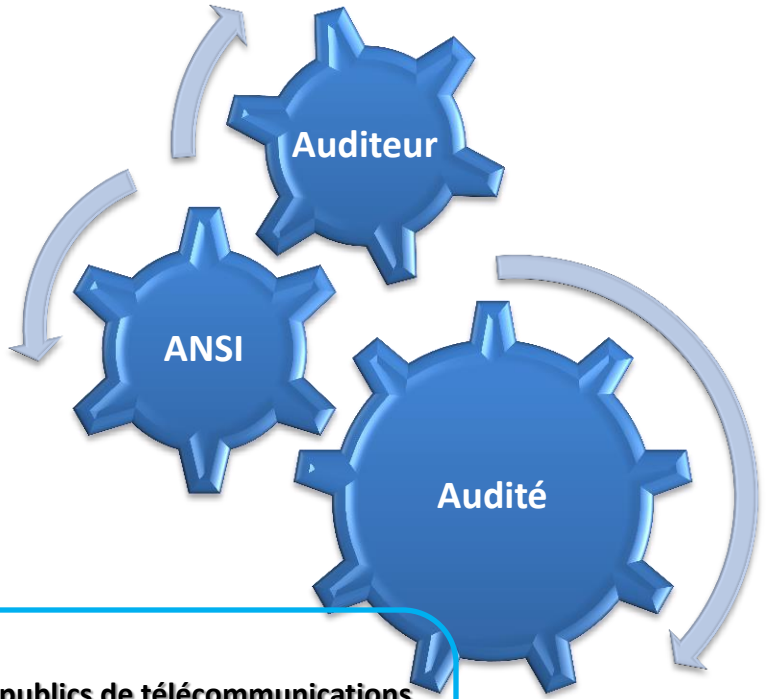
- assuré par tunCERT
- partiellement assuré par tunCERT
- Non assuré par tunCERT

Services proactifs

Audit de la sécurité des SI

Décret n° 2004-1250 du 25 mai 2004, fixant les systèmes informatiques et les réseaux des organismes soumis à l'audit obligatoire périodique de la sécurité informatique et les critères relatifs à la nature de l'audit et à sa périodicité et aux procédures de suivi de l'application des recommandations contenues dans le rapport d'audit.

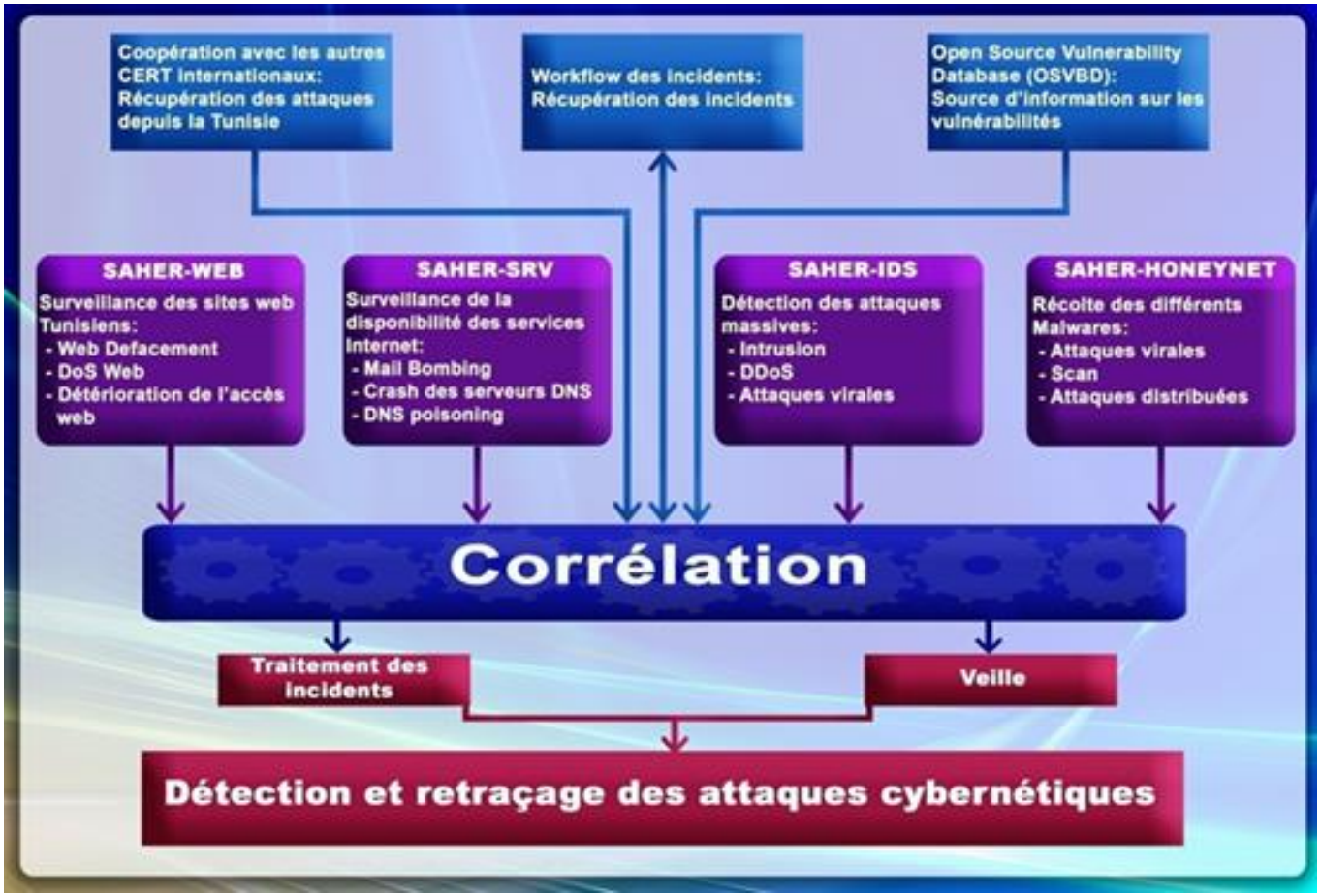
Décret n° 2004-1249 du 25 mai 2004, fixant les conditions et les procédures de certification des experts auditeurs dans le domaine de la sécurité informatique.



- Entreprises publiques
- Opérateurs de réseaux publics de télécommunications et FSI
- Entreprise dont les réseaux informatiques sont interconnectés, à travers des réseaux externes
- Entreprise qui procèdent au traitement automatisé des données personnelles de leurs clients

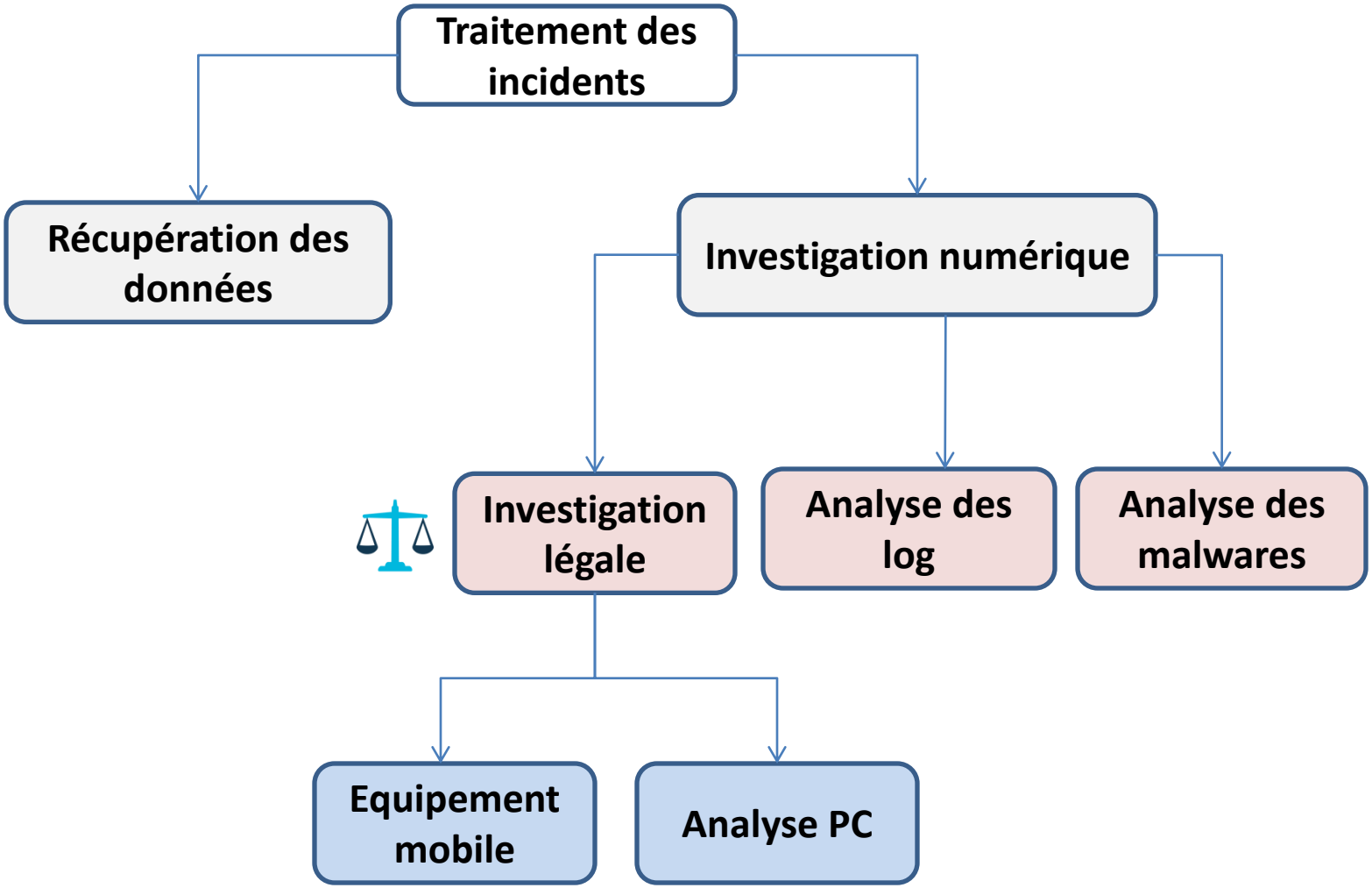
Services proactifs

Monitoring du cyberespace : SAHER CTI



Services reactifs

Réponse aux incidents



الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique

Gestion de la qualité de la cybersécurité

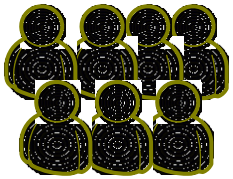
Sensibilisation

Managers, Decision makers

Réunions B to B
Séminaires ciblés
Programme de formation orienté Management de la sécurité (exemple : CISM, etc)

Web masters, Security Admin., Developers

Workshops
Séminaires orientés RSSI, FSI, etc
Formations techniques (CISSP, CEH, ECSA, etc)
Avis de vulnérabilités
Guides techniques

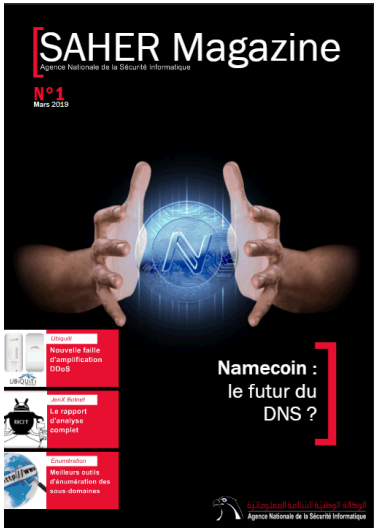


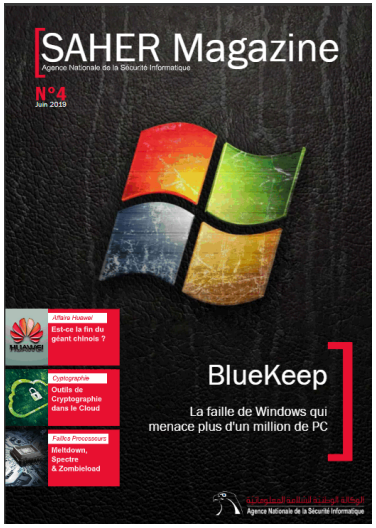
Internet Community

Foires
Spot Télé et Radio
Evénements en collaboration avec la société civile
Brochures, etc

Gestion de la qualité de la cybersécurité

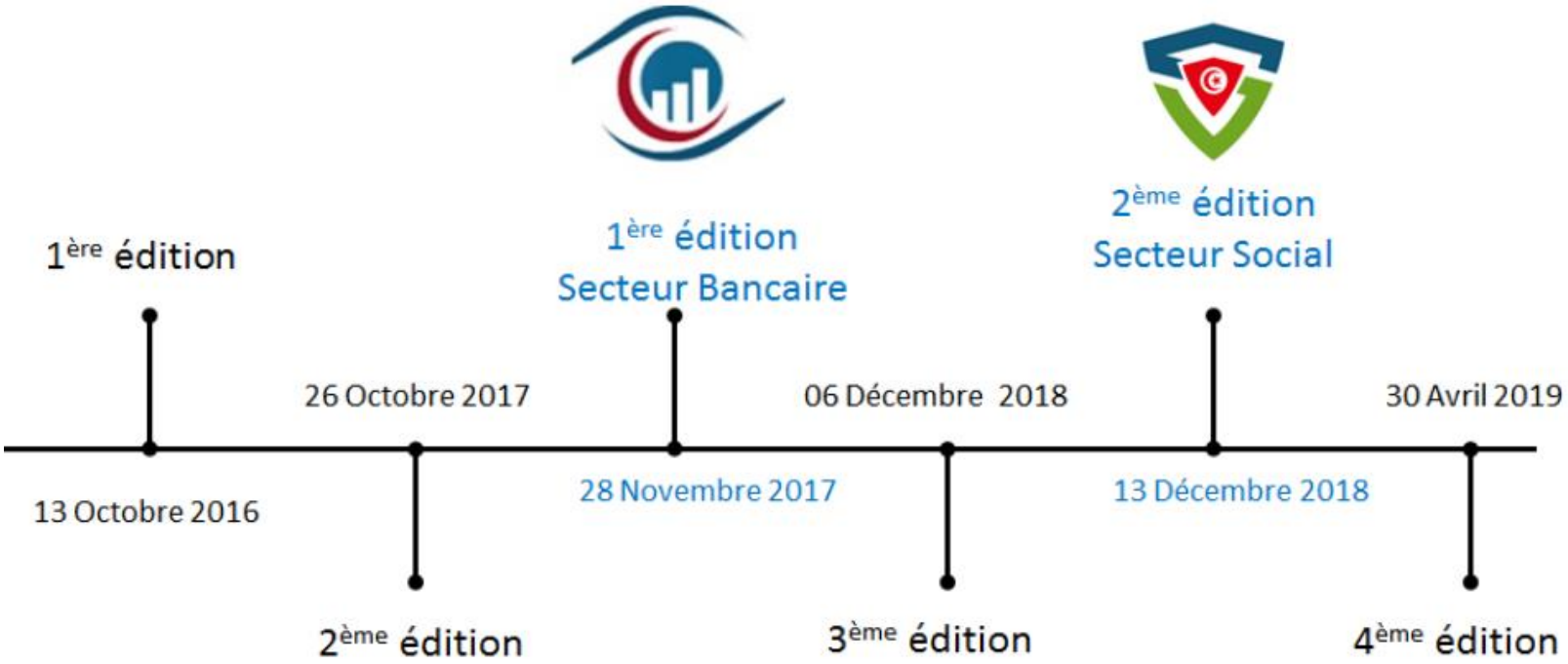
SAHER Magazine





Gestion de la qualité de la cybersécurité

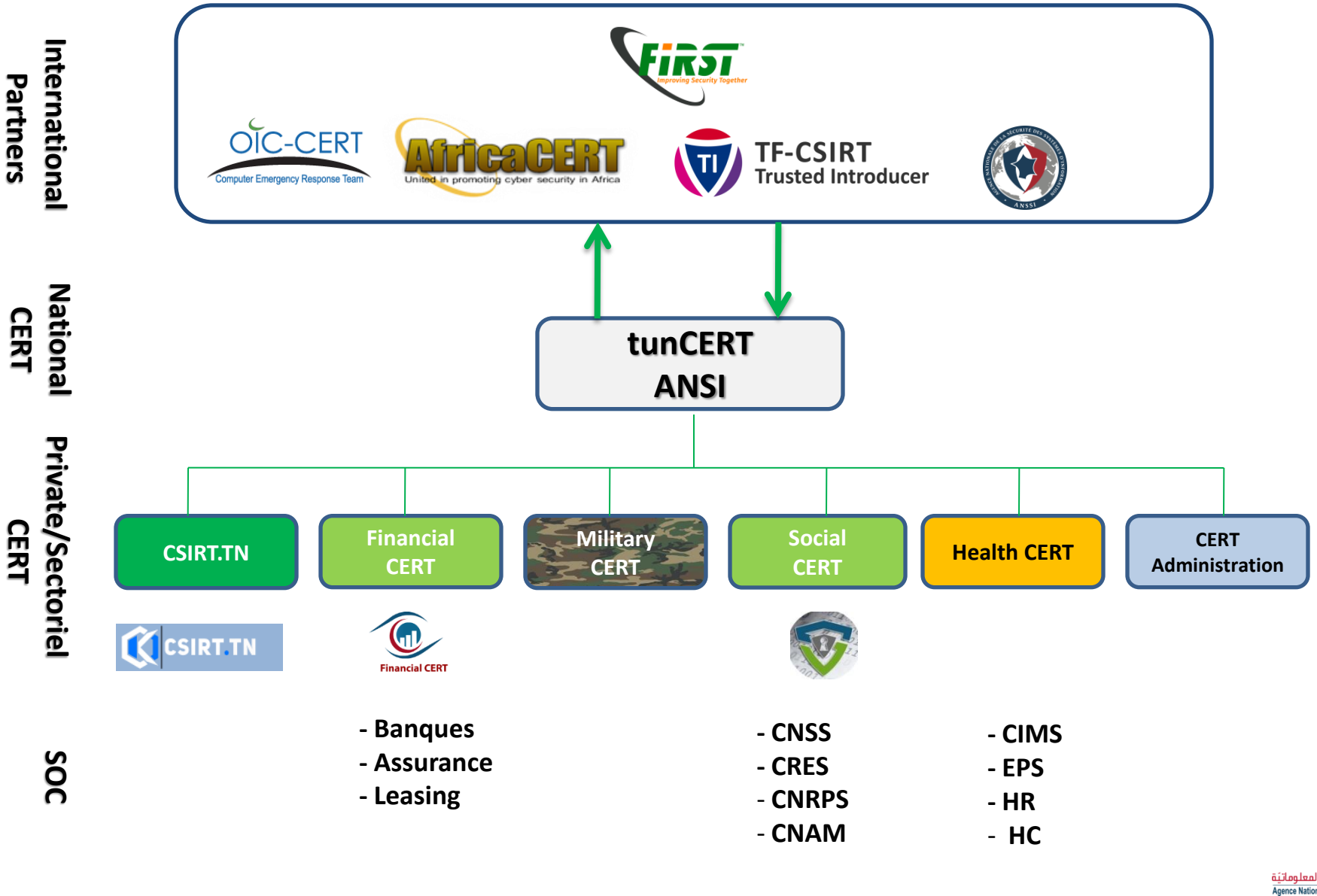
Cyberdrill



Gestion de la qualité de la cybersécurité

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

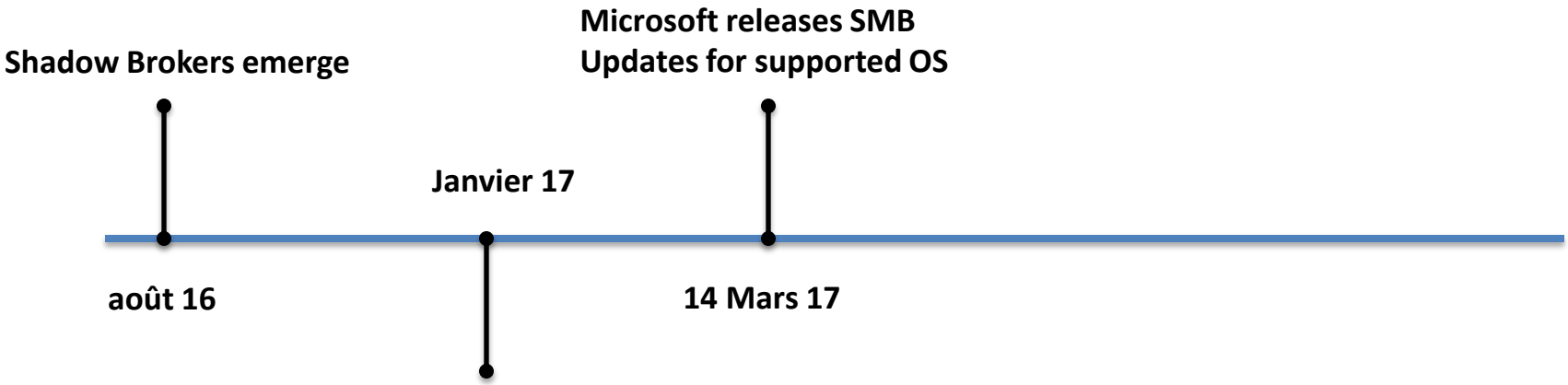
Notre Vision : Communauté CERT



الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique

Ransomware Wannacry : Etude de cas

Wannacry : Comportement tunCERT

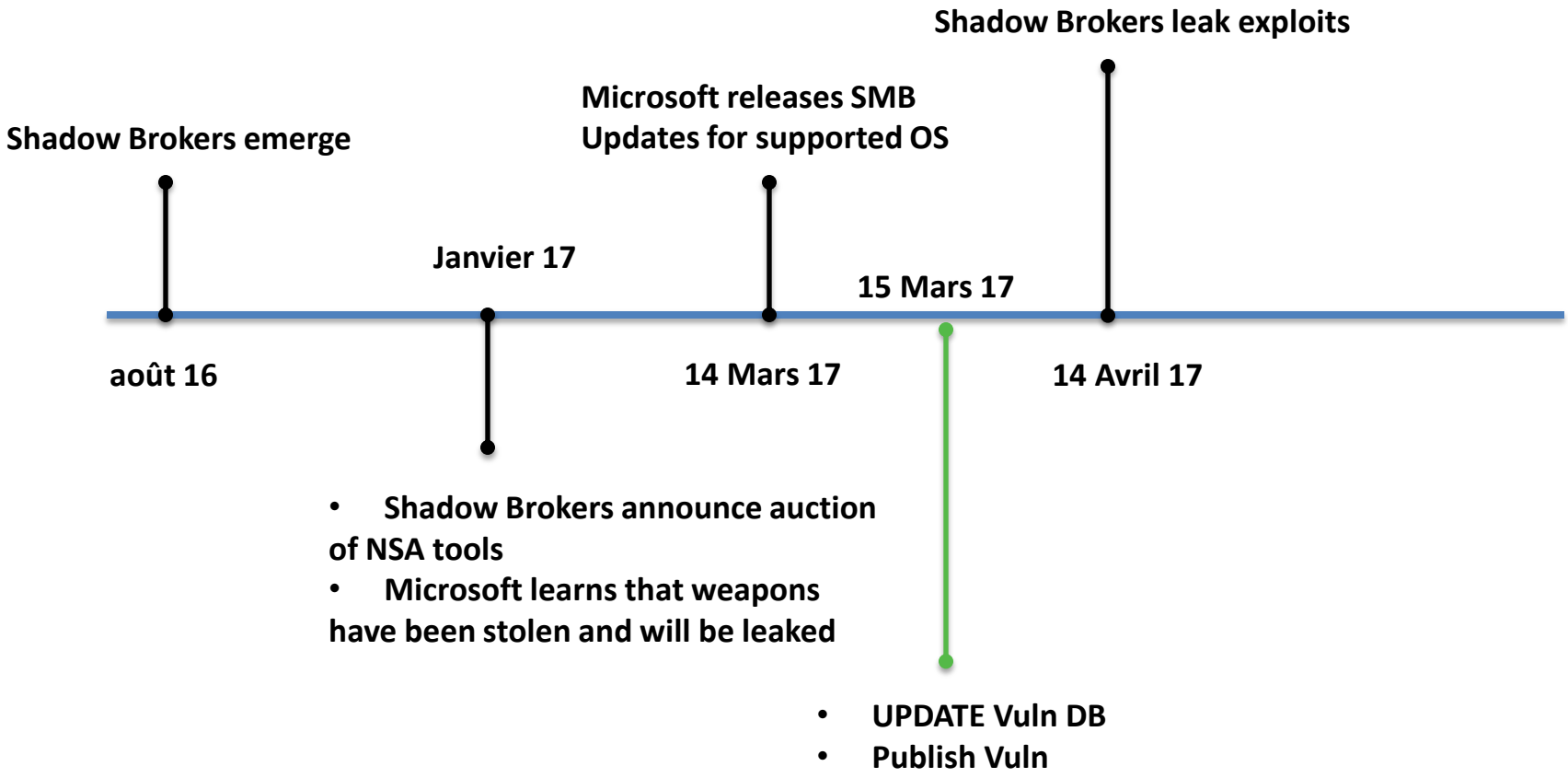


- Shadow Brokers announce auction of NSA tools
- Microsoft learns that weapons have been stolen and will be leaked

Wannacry : Comportement tunCERT

https://tuncert.ansi.tn/publish/module/vulnerabilite.asp?id_vul=5000

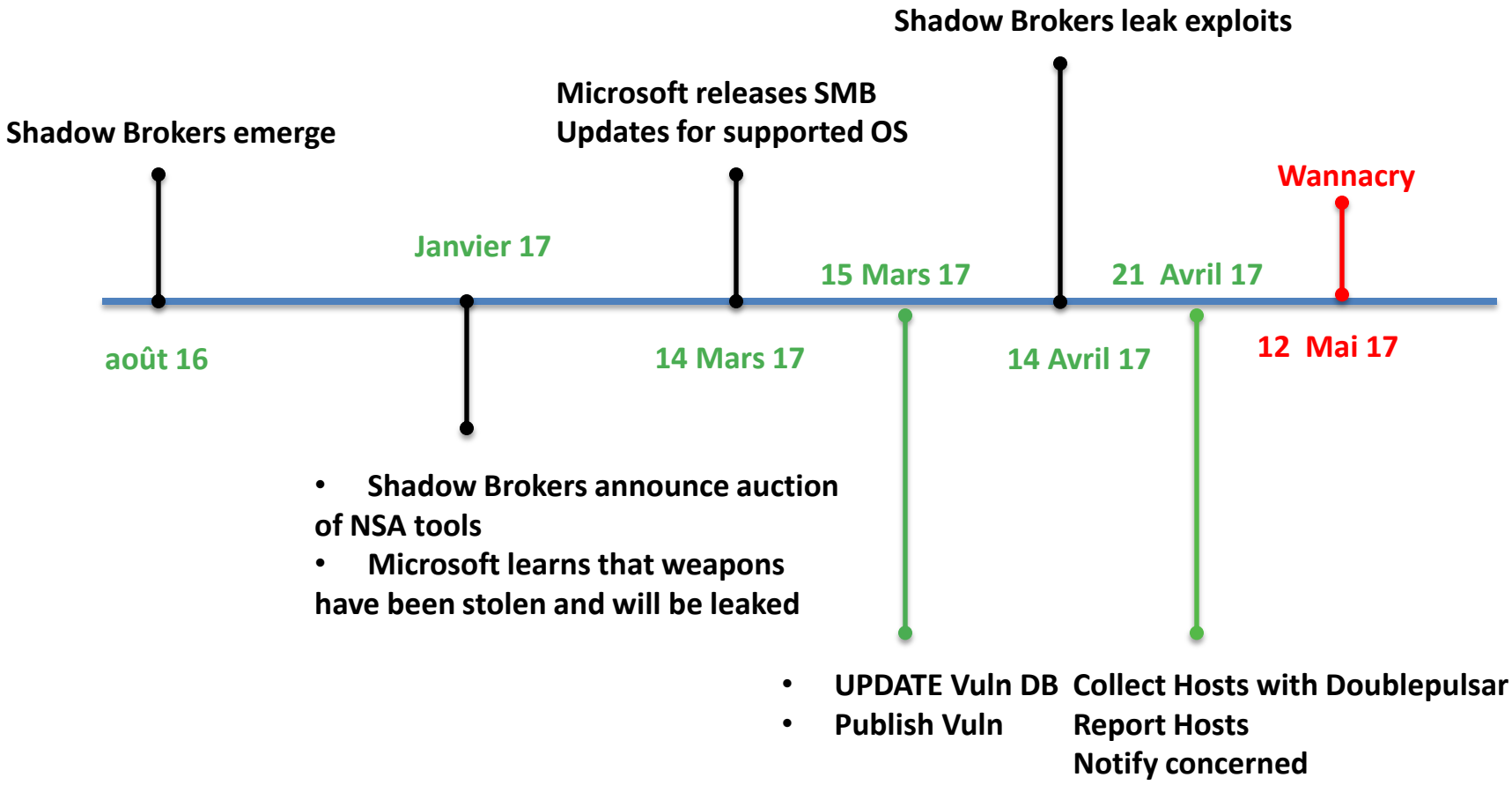
Wannacry : Comportement tunCERT



Wannacry : Comportement tunCERT

```
┌─[root@parrot]─[/home/pentesting/doublepulsar-detection-script]
└──╼ #python detect_doublepulsar.py --file test.txt
[-] [41.224.246.210] No presence of DOUBLEPULSAR
[-] [41.224.250.121] No presence of DOUBLEPULSAR
[-] [41.224.253.116] No presence of DOUBLEPULSAR
[-] [41.224.250.213] No presence of DOUBLEPULSAR
[ERROR] [41.224.184.199] - [Errno 111] Connection refused
[-] [41.224.245.1] No presence of DOUBLEPULSAR
[ERROR] [41.224.246.211] - [Errno 113] No route to host
[-] [41.228.170.219] No presence of DOUBLEPULSAR
[+]                  DOUBLEPULSAR DETECTED!!!
[-] [41.228.175.40] No presence of DOUBLEPULSAR
[-] [41.224.249.163] No presence of DOUBLEPULSAR
[-] [41.224.255.67] No presence of DOUBLEPULSAR
[-] [41.228.164.25] No presence of DOUBLEPULSAR
[-] [41.224.247.179] No presence of DOUBLEPULSAR
[-] [41.228.160.135] No presence of DOUBLEPULSAR
[+]                  DOUBLEPULSAR DETECTED!!!
[ERROR] [41.224.241.7] - [Errno 113] No route to host
[-] [41.224.241.204] No presence of DOUBLEPULSAR
[ERROR] [41.224.242.131] - [Errno 113] No route to host
[ERROR] [41.224.71.239] - [Errno 110] Connection timed out
[ERROR] [41.224.14.62] - [Errno 110] Connection timed out
[ERROR] [197.27.34.203] - [Errno 110] Connection timed out
[ERROR] [41.224.173.23] - [Errno 110] Connection timed out
[ERROR] [197.27.91.19] - [Errno 110] Connection timed out
[ERROR] [197.27.13.209] - [Errno 110] Connection timed out
┌─[root@parrot]─[/home/pentesting/doublepulsar-detection-script]
└──╼ #
```

Wannacry : Comportement tunCERT



Wannacry : Comportement tunCERT

Agence nationale de sécurité informatique ANSI - Officiel
15 mai ·

Récemment, une campagne massive de Spam, portant comme pièce jointe un nouveau ransomware baptisé « WannaCry », a été détectée sur le net. Connu aussi sous les noms Wana Decrypt0r, ce malware est capable d'exploiter la faille « MS17-10 » du composant « Microsoft Server Message Block SMBv1 » pour obtenir des privilèges élevés, crypter les données personnelles des victimes et aussi se propager sur d'autres machines vulnérables.
Pour s'en protéger, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :

-Vérifier l'authenticité et la fiabilité des expéditeurs avant la lecture de chaque message reçu par e-mail ou affiché sur votre mûr de Facebook / Twitter et en cas de doute n'y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu'il contient et supprimer le immédiatement.
-Mettre à jour régulièrement votre solution antivirale.
-Activer la mise à jour automatique de votre système Windows.
Sauvegarder régulièrement vos données sensibles sur des disques durs externes.
-Créer chaque semaine des points de restauration pour récupérer les fichiers système en cas d'infection.
-Installer des Addons dans votre navigateur web pour vous renseigner sur la fiabilité des sites web visités (Exemples:Netcraft).
Utiliser un compte utilisateur avec des privilèges limités pour se connecter à Internet.

Tunisian Computer Emergency Response Team

ACTUALITES

15/05/2017 : Attention au ransomware « WannaCry » et ses variantes.

Attention au ransomware « WannaCry » et ses variantes.

Vendredi dernier, une ***attaque massive de ransomware*** a ciblé plusieurs pays du monde. Baptisé «***WannaCry***», ce malware a été principalement répandu ***via des Spams*** envoyés par des cybercriminels. Une fois que la victime clique sur une pièce jointe, WannaCry commence à ***crypter les données présentes sur les disques durs*** puis ***se propager automatiquement***, en exploitant la ***faille « Microsoft Server Message Block SMB - MS17-10 »***, afin ***d'infecter plusieurs systèmes Windows sur les réseaux interconnectés***.

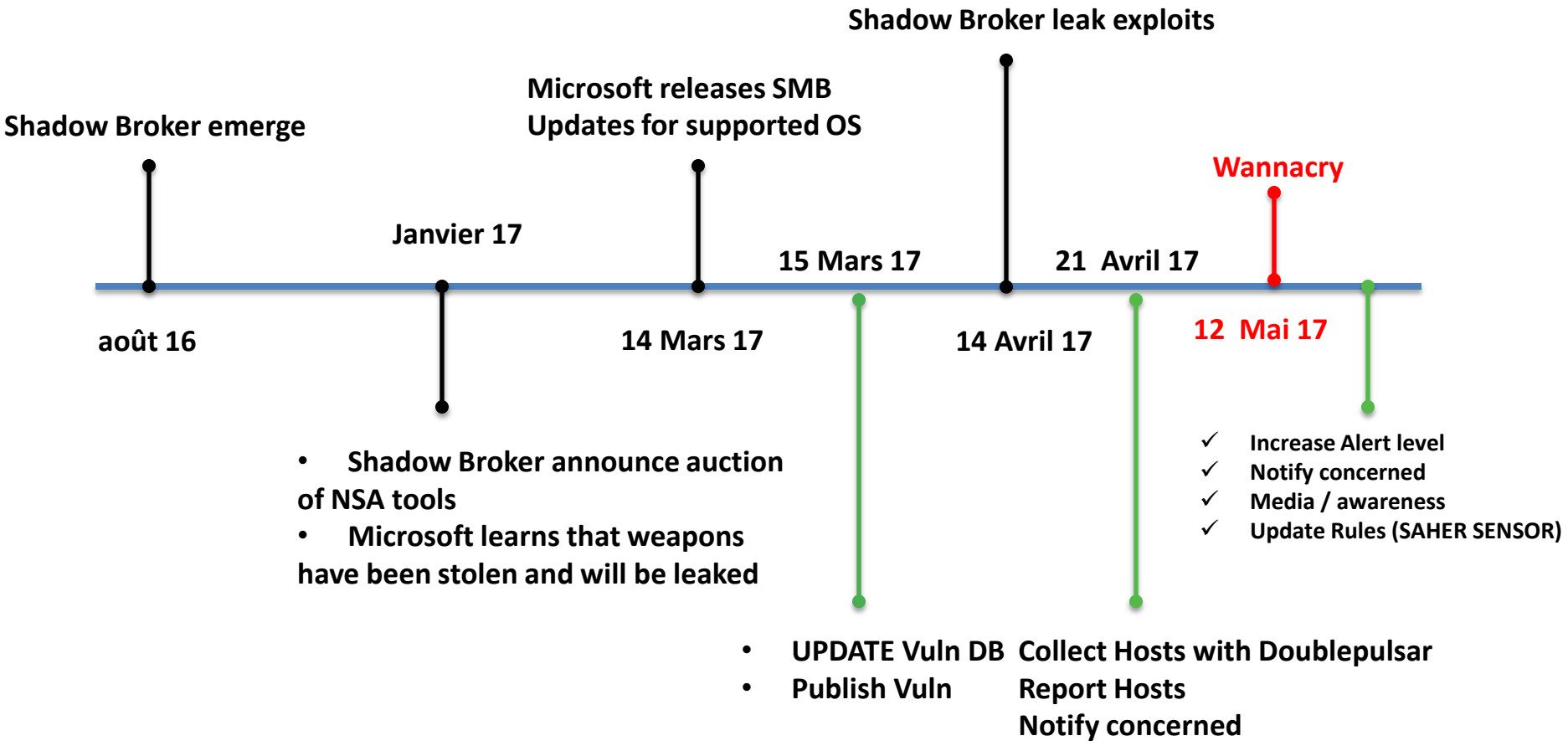
Récemment, des informations publiées sur le net annoncent que ***des nouvelles variantes de «WannaCry »*** comme « ***Uiwix*** » arriveront bientôt et seront capables d'exploiter d'autres vulnérabilités sur les systèmes Windows.

Pour protéger vos données personnelles face à ces menaces, nous vous conseillons d'être **vigilant** et de **suivre généralement les mesures préventives suivantes** :

- ***Mettre à jour aussitôt votre système Windows*** **pour** ***corriger la vulnérabilité de SMB et toute autre pourrant exister.***
- ***Mettre à jour immédiatement votre solution antivirale.***
- ***Vérifier l'authenticité et la fiabilité des expéditeurs*** *avant la lecture de chaque message reçu par* ***e-mail*** *ou affiché sur votre mûr de* ***Facebook / Twitter*** *et en cas de doute* ***ne télécharger pas les pièces jointes, n'y répondez pas, ne cliquez pas*** *sur les liens hypertextes ou les images qu'il contient et* ***supprimer le immédiatement.***
- ***Sauvegarder régulièrement vos données sensibles*** *sur des disques durs externes.*

https://tuncert.ansi.tn/publish/content/news.asp?idn=117&

Wannacry : Comportement tunCERT



Wannacry : Comportement tunCERT

L'ANSI met en garde contre le virus WannaCry

16 mai 2017 **Mots-clefs :** actualité, Agence Nationale de Sécurité Informatique, ansi, ransomware, reseau sociaux, Spam , technologie, tunisie, virus wannacry

Partager Sur Facebook | Partager Sur Twitter | Partager Sur Google+

L'Agence Nationale de Sécurité Informatique (ANSI) attire l'attention de tous les utilisateurs du système d'exploitation Windows à une nouvelle attaque virulente.

Wannacry : Comportement tunCERT

Pré-attaque

Post-attaque

2 months interval

Shadow Broker leak exploits

Microsoft releases SMB
Updates for supported OS

Shadow Broker emerge

Wannacry

Janvier 17

15 Mars 17

21 Avril 17

août 16

14 Mars 17

14 Avril 17

12 Mai 17

- Shadow Broker announce auction of NSA tools
- Microsoft learns that weapons have been stolen and will be leaked

- ✓ Increase Alert level
- ✓ Notify concerned
- ✓ Media / awareness
- ✓ Update Rules (SAHER SENSOR)

- UPDATE Vuln DB Collect Hosts with Doublepulsar
- Publish Vuln Report Hosts
  Notify concerned

الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique

Dans le Cyberespace, Personne ne Vous Entend Crier