Gestion des vulnérabilités du terrain au cloud

LES JOURNÉES DE LA CYBER

2 & 3 MARS 2023
Campus Région du Numérique

LES JOURNÉES DE LA CYBER

Gestion des vulnérabilités du terrain au cloud

Sylvain Cortes

VP Strategy @ Hackuity

Roch Auburtin

Directeur Sécurité des Systèmes d'Information Visiativ

Agenda

- Mais au fait, c'est quoi une vulnérabilité ?
- De la nécessité de mettre les vulnérabilités sous contrôle
- Les challenges liés au traitement des vulnérabilités
- Quelles actions concrètes ?
  - Dans les PMEs/PMIs
  - Dans les grandes organisations
- Conclusion

Agenda

- Mais au fait, c'est quoi une vulnérabilité ?
- De la nécessité de mettre les vulnérabilités sous contrôle
- Les challenges liés au traitement des vulnérabilités
- Quelles actions concrètes ?
  - Dans les PMEs/PMIs
  - Dans les grandes organisations
- Conclusion

LES JOURNÉES DE LA CYBER

Mais au fait, c'est quoi une vulnérabilité ?

Vulnérabilité (informatique)

30 langues

Article Discussion | Lire Modifier Modifier le code Voir l'historique

Cet article concerne la vulnérabilité en informatique. Pour une utilisation plus large du terme, voir Vulnérabilité.

Dans le domaine de la sécurité informatique, une **vulnérabilité** ou **faille** est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Ces vulnérabilités sont la conséquence de faiblesses dans la conception, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel du système, mais il s'agit souvent d'anomalies logicielles liées à des erreurs de programmation ou à de mauvaises pratiques. Ces dysfonctionnements logiciels sont en général corrigés à mesure de leurs découvertes, mais l'utilisateur reste exposé à une éventuelle exploitation tant que le correctif (temporaire ou définitif) n'est pas publié et installé. C'est pourquoi il est important de maintenir les logiciels à jour avec les correctifs fournis par les éditeurs de logiciels. La procédure d'exploitation d'une vulnérabilité logicielle est appelée exploit.

Source: https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9_zero-day

LES JOURNÉES DE LA CYBER

Mais au fait, c'est quoi une vulnérabilité ?

Finalement, pour attaquer un système, quel qu'il soit, l'attaquant n'utilise que deux types de vulnérabilités:

1

Vulnérabilité (erreur) de programmation

- Code développé en interne
- CVE non patchée ou système obsolète
- Zero-Day

2

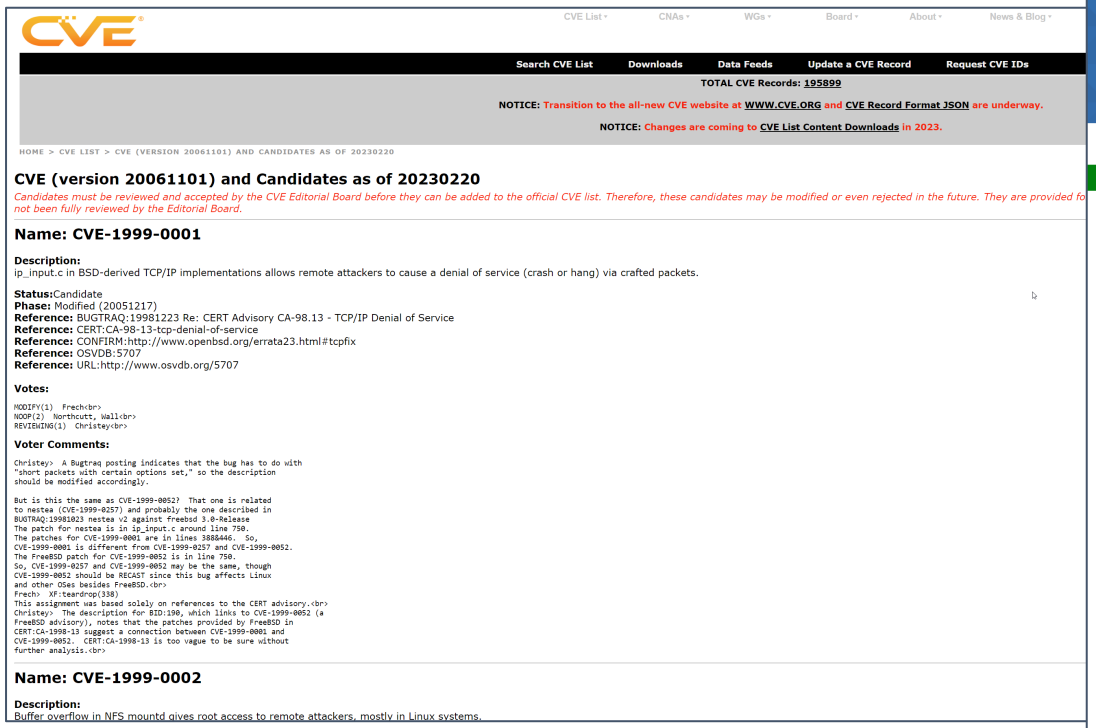
Vulnérabilité (erreur) de configuration

- Mauvaise config Firewall/VPN
- Mauvaise config AD
- Mauvaise config Cloud

LES JOURNÉES DE LA CYBER

Mais au fait, c'est quoi une vulnérabilité ?

CVEs



CVE

CVE List · CNAs · WGs · Board · About · News & Blog

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 195899

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Changes are coming to CVE List Content Downloads in 2023.

HOME > CVE LIST > CVE (VERSION 20061101) AND CANDIDATES AS OF 20230220

CVE (version 20061101) and Candidates as of 20230220

Candidates must be reviewed and accepted by the CVE Editorial Board before they can be added to the official CVE list. Therefore, these candidates may be modified or even rejected in the future. They are provided fo not been fully reviewed by the Editorial Board.

Name: CVE-1999-0001

Description:
ip_input.c in BSD-derived TCP/IP implementations allows remote attackers to cause a denial of service (crash or hang) via crafted packets.

Status: Candidate
Phase: Modified (20051217)
Reference: BUGTRAQ:19981223 Re: CERT Advisory CA-98.13 - TCP/IP Denial of Service
Reference: CERT:CA-98-13-tcp-denial-of-service
Reference: CONFIRM:http://www.openbsd.org/errata23.html#tcpfix
Reference: OSVDB:5707
Reference: URL:http://www.osvdb.org/5707

Votes:

MODIFY(1) Frech
NOOP(2) Northcutt, Wall
REVIEWING(1) Christey

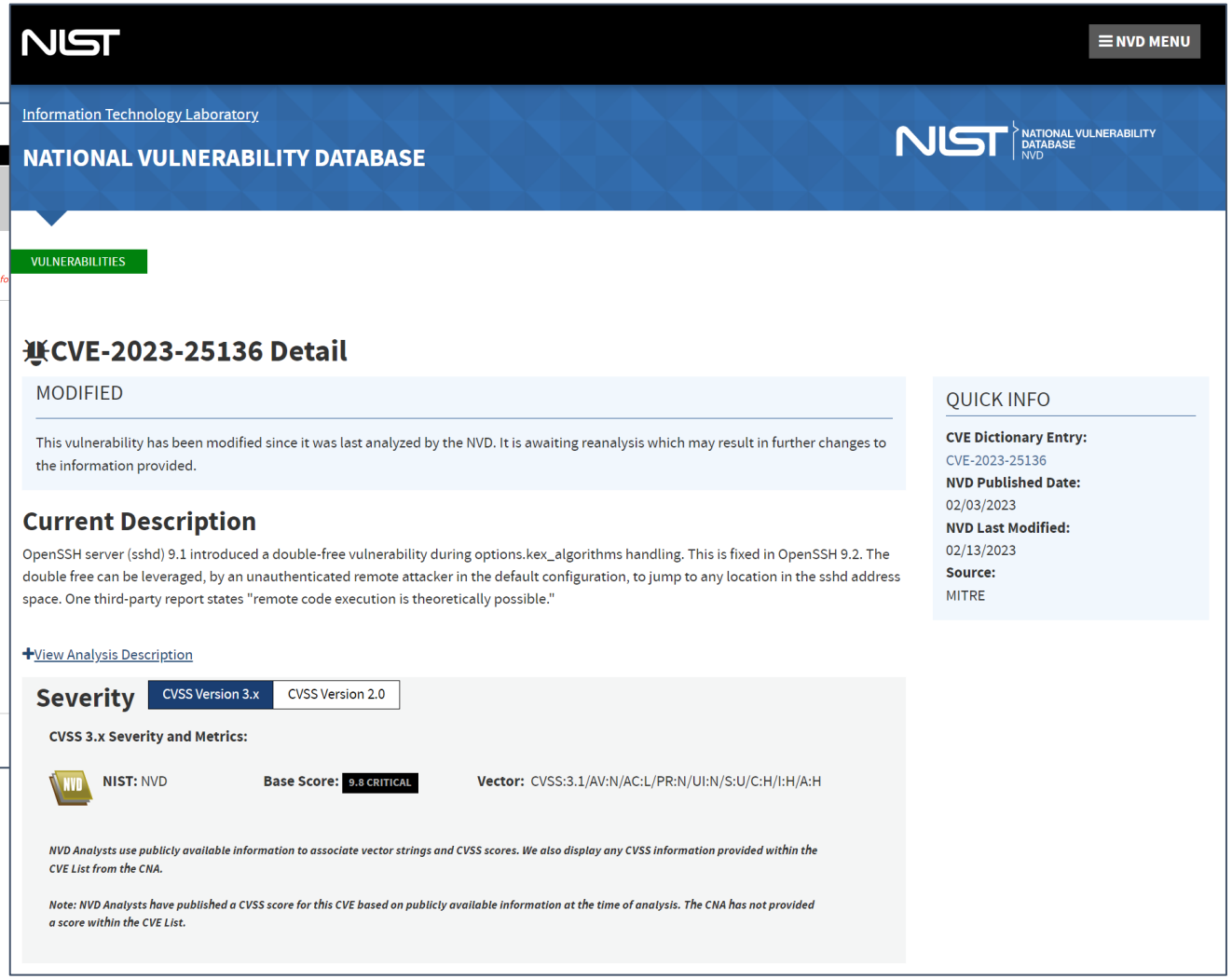
Voter Comments:

Christey> A Bugtraq posting indicates that the bug has to do with
"short packets with certain options set," so the description
should be modified accordingly.

But is this the same as CVE-1999-0052? That one is related
to nestea (CVE-1999-0257) and probably the one described in
BUGTRAQ:19981023 nestea v2 against freebsd 3.0-Release
The patch for nestea is in ip_input.c around line 750.
The patches for CVE-1999-0001 are in lines 3888446. So,
CVE-1999-0001 is different from CVE-1999-0257 and CVE-1999-0052.
The FreeBSD patch for CVE-1999-0052 is in line 750.
So, CVE-1999-0257 and CVE-1999-0052 may be the same, though
CVE-1999-0052 should be RECAST since this bug affects Linux
and other OSes besides FreeBSD.
Frech> XF:teardrop(338)
This assignment was based solely on references to the CERT advisory.
Christey> The description for BID:190, which links to CVE-1999-0052 (a
FreeBSD advisory), notes that the patches provided by FreeBSD in
CERT:CA-1998-13 suggest a connection between CVE-1999-0001 and
CVE-1999-0052. CERT:CA-1998-13 is too vague to be sure without
further analysis.

Name: CVE-1999-0002

Description:
Buffer overflow in NFS mountd gives root access to remote attackers, mostly in Linux systems.



NIST

NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2023-25136 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

OpenSSH server (sshd) 9.1 introduced a double-free vulnerability during options.kex_algorithms handling. This is fixed in OpenSSH 9.2. The double free can be leveraged, by an unauthenticated remote attacker in the default configuration, to jump to any location in the sshd address space. One third-party report states "remote code execution is theoretically possible."

+View Analysis Description

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NVD **NIST:** NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

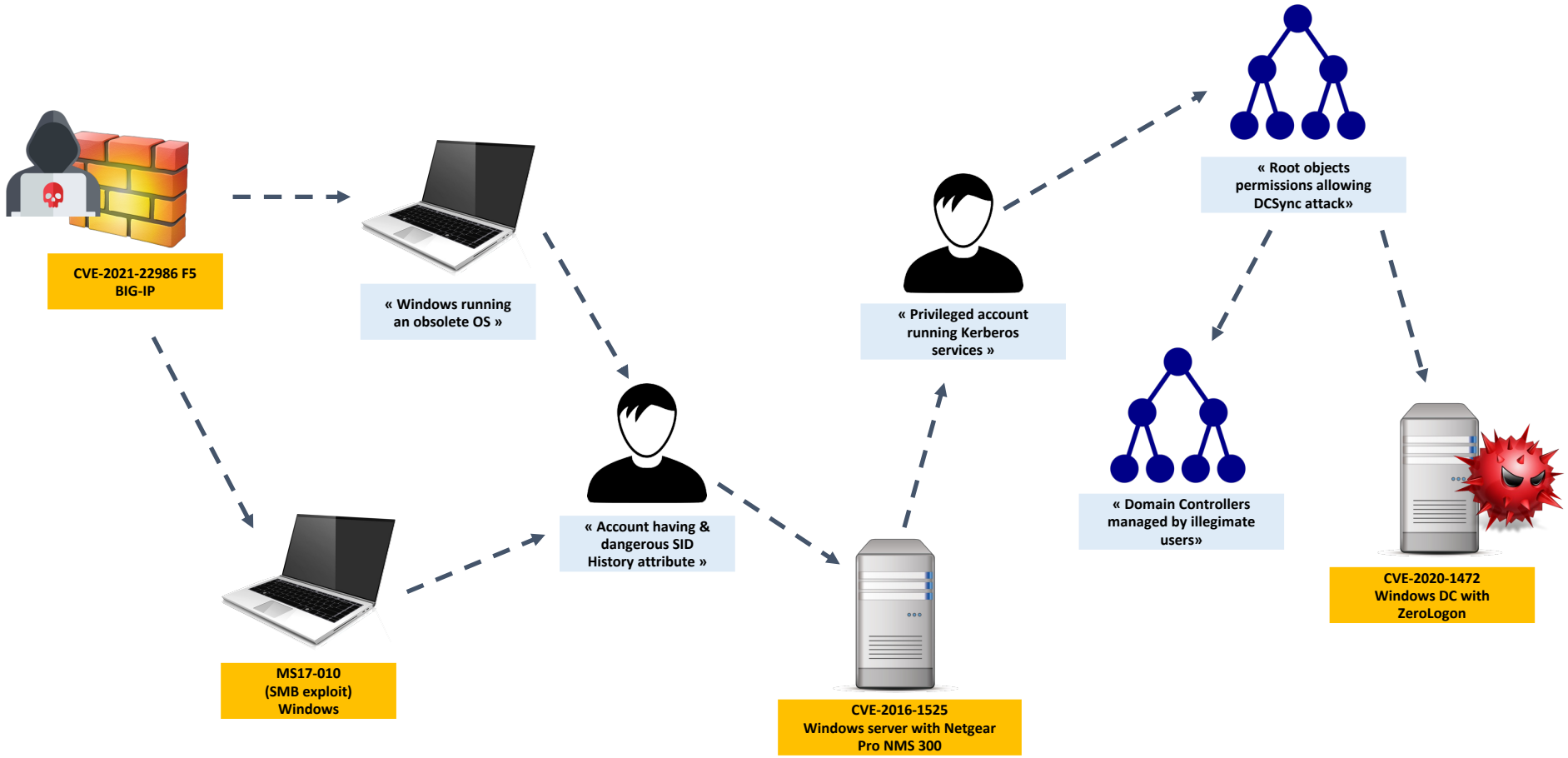
CVE Dictionary Entry:
CVE-2023-25136
NVD Published Date:
02/03/2023
NVD Last Modified:
02/13/2023
Source:
MITRE

Sources: https://cve.mitre.org & https://nvd.nist.gov

LES JOURNÉES DE LA CYBER

Mais au fait, c'est quoi une vulnérabilité ?

Notion de **chemin d'attaque** exploitant des CVEs non patchées et des mauvaises configurations AD



Primo-infection & Pivoting | **Mouvement lateral et escalade des privilèges** | **Compromission de domaine**

LES JOURNÉES DE LA CYBER

Mais au fait, c'est quoi une vulnérabilité ?

Exemple avec un Ransomware très connu: RYUK

TEMPS MOYEN D'EXECUTION DE LA SEQUENCE: 7 HEURES

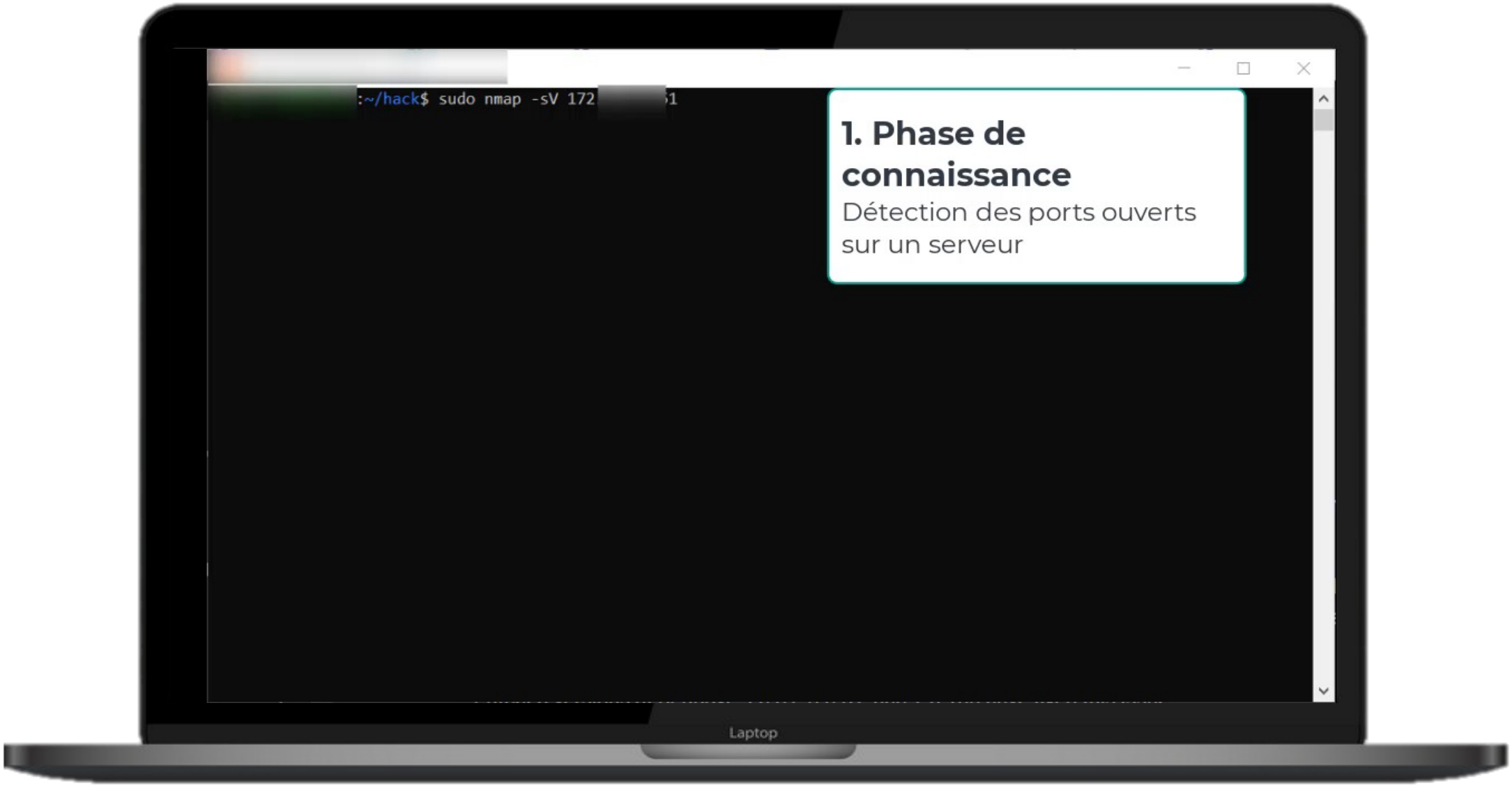
CVE-2018-1156	CVE-2021-40444	MS17-010	Computer objects	SYSVOL User objects
Mikrotik RouterOS is vulnerable to stack buffer overflow. This vulnerability allows for arbitrary code execution on the system.	Remote code execution (RCE) vulnerability in Windows allows attackers to craft malicious Microsoft Office documents	Wormdll uses an SMB exploit (MS17-010) & Sharedll drops payload copies in administrative shares C$ or ADMIN$	"pysmb" script leverages NTLM protocol in older Windows systems and IPC shares	"DomainGabber" (domainDll32) is used for LDAP harvesting of domain controller configuration via ADSI

Agenda

- Mais au fait, c'est quoi une vulnérabilité ?
- De la nécessité de mettre les vulnérabilités sous contrôle
- Les challenges liés au traitement des vulnérabilités
- Quelles actions concrètes ?
  - Dans les PMEs/PMIs
  - Dans les grandes organisations
- Conclusion

LES JOURNÉES DE LA CYBER

De la nécessité de mettre les vulnérabilités sous contrôle : Démo

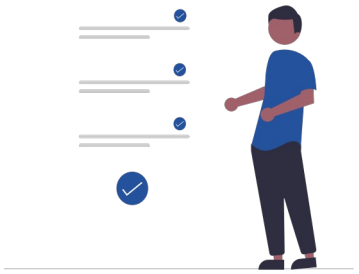


Agenda

- Mais au fait, c'est quoi une vulnérabilité ?
- De la nécessité de mettre les vulnérabilités sous contrôle
- Les challenges liés au traitement des vulnérabilités
- Quelles actions concrètes ?
  - Dans les PMEs/PMIs
  - Dans les grandes organisations
- Conclusion

LES JOURNÉES DE LA CYBER

Les challenges liés au traitement des vulnérabilités

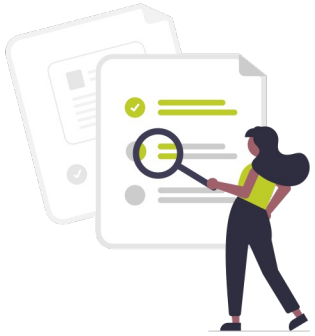


Avoir un inventaire à jour

- Nombre très important de logiciels, d'OS, d'appareils, et de composants
- Dépendance très difficile à obtenir

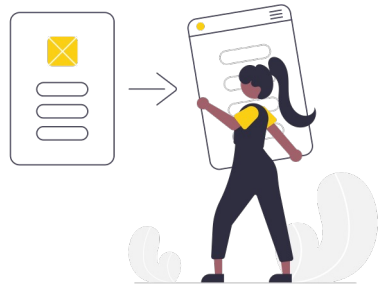
Maintenir les systèmes à jour

- La mise à jour d'un système (OS, Logiciel) peut impacter un autre logiciel
- La mise à jour des applications et des systèmes d'exploitation peut être très longue et complexe



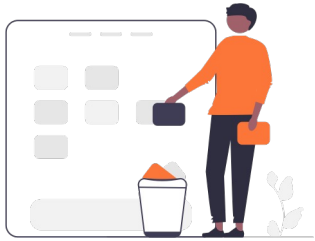
Réaliser une veille efficace

- Une Zero-Day peut être exploitée très vite (Log4j a été exploitée 2 ou 3 h après sa publication)
- De très nombreuses sources d'informations, des explications complexes et très techniques qui rendent très difficile la compréhension en terme d'exploitabilité et remédiations



Vérifier que les remédiations ne pénalisent pas les usages

Des mises à jour incomplètes ou de mauvaise qualité peuvent avoir des impacts importants sur les usages (ex: des fonctionnalités qui ne sont plus disponibles pour les utilisateurs)



Être sûr que les fournisseurs traitent vulnérabilités

La mise en œuvre du plan de remédiation demande du temps, de l'argent et des connaissances. Il est impératif que les partenaires soient en mesure d'appliquer les correctifs

Agenda

- Mais au fait, c'est quoi une vulnérabilité ?
- De la nécessité de mettre les vulnérabilités sous contrôle
- Les challenges liés au traitement des vulnérabilités
- Quelles actions concrètes ?
  - Dans les PMEs/PMIs
  - Dans les grandes organisations
- Conclusion

LES JOURNÉES DE LA CYBER

Quelles actions concrètes pour protéger les PMEs ?

Mesures cybersécurité générales

- Faites des sauvegardes régulières « Offline » et testez-les
- Sensibilisez les employés
- Utilisez des logiciels de protection (antivirus performants type EDR, protection messagerie) et traitez les alertes
- **Mettez à jour vos logiciels et les systèmes d'information**
- Mettez en place le MFA et des mots de passe robustes
- Limitez les comptes administrateur locaux
- Chiffrez les disques dur de vos postes de travail
- Surveillez votre surface externe et cloisonnez votre réseau interne
- Mettez en place une procédure de gestion d'incident

Mesures cybersécurité pour réduire les vulnérabilités

- Faites un inventaire
- Installez un serveur WSUS et une stratégie de mise à jour automatique par GPO
- Faites de la veille à minima sur les alertes de CERT.FR
- Décommissionnez les systèmes d'exploitation et les logiciels non supportés
- Soyez exigeant vis-à-vis de vos prestataires (Web Agency, Solutions SaaS, …)
- Faites faire des pentests internes

Et faites-vous accompagner ! ☺

LES JOURNÉES DE LA CYBER

Quelles actions concrètes ?

Grandes organisations: Programme CTEM

1

Vulnérabilité (erreur) de programmation

- Code développé en interne
- CVE non patchée ou système obsolète
- Zero-Day

2

Vulnérabilité (erreur) de configuration

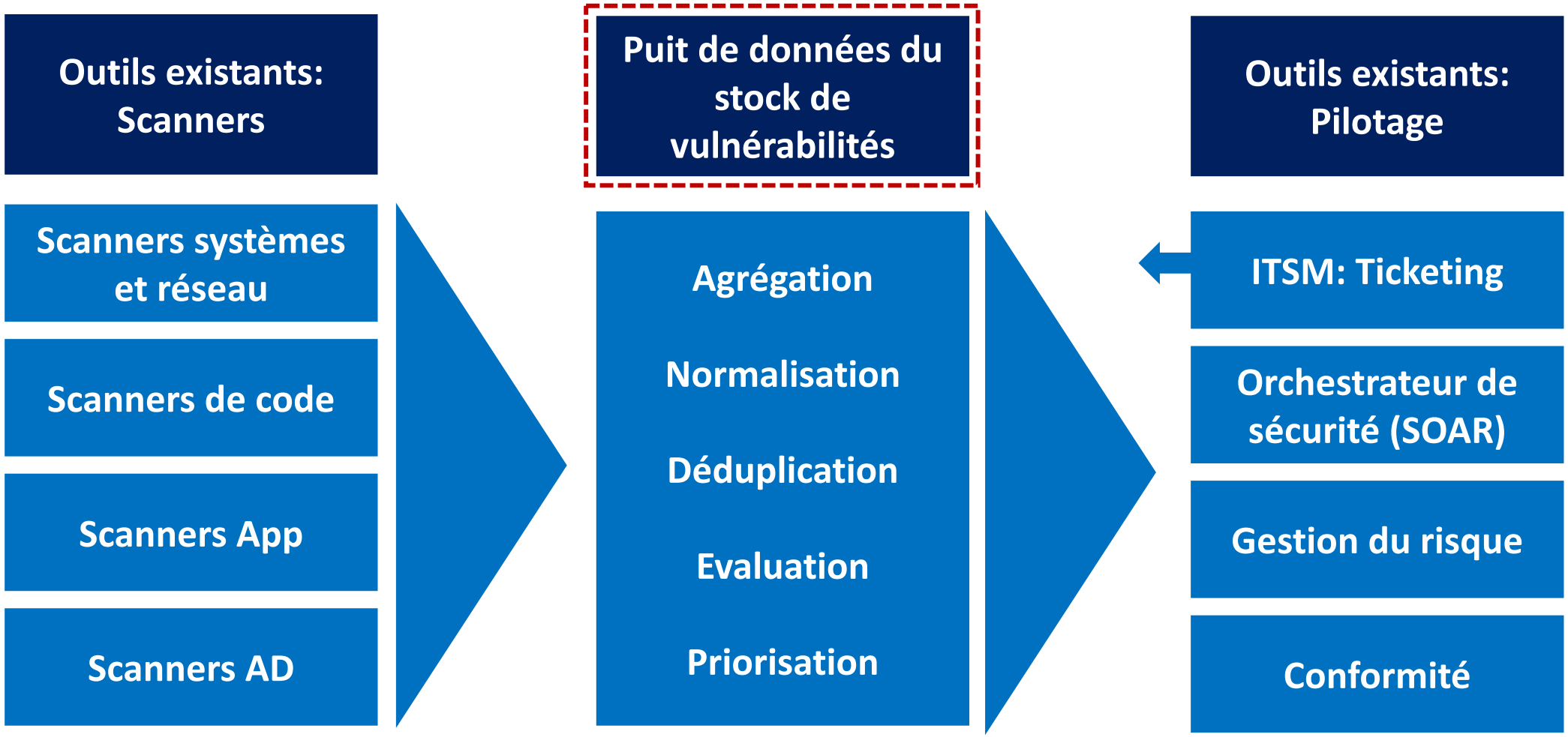
- Mauvaise config Firewall/VPN
- Mauvaise config AD
- Mauvaise config Cloud

Mettre en œuvre un programme CTEM:
« Gestion continue de l'exposition aux menaces »

LES JOURNÉES DE LA CYBER

Quelles actions concrètes ?

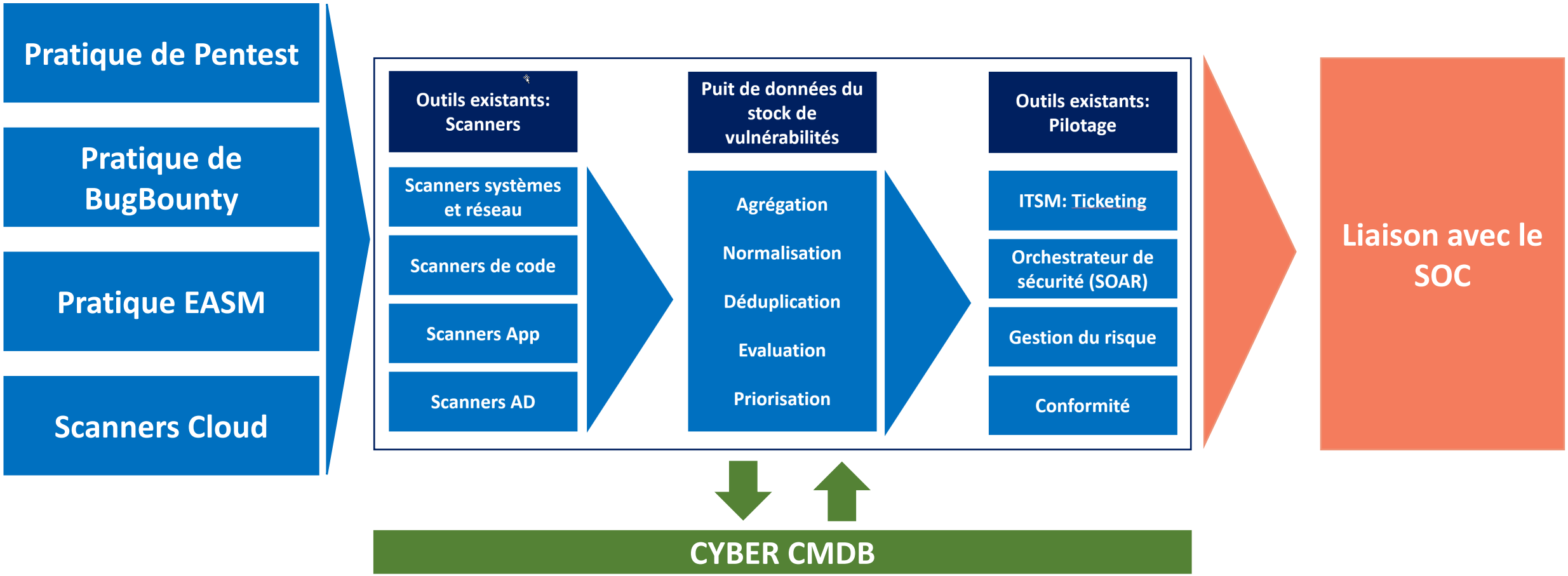
Grandes organisations: Pilotage des vulnérabilités, le minimum vital



LES JOURNÉES DE LA CYBER

Quelles actions concrètes ?

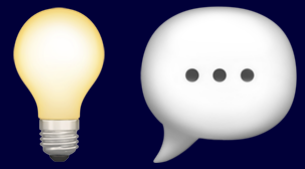
Grandes organisations: Vulnerability Operation Center (VOC) pour les organisations matures



Agenda

- Mais au fait, c'est quoi une vulnérabilité ?
- De la nécessité de mettre les vulnérabilités sous contrôle
- Les challenges liés au traitement des vulnérabilités
- Quelles actions concrètes ?
  - Dans les PMEs/PMIs
  - Dans les grandes organisations
- Conclusion

Cyber sécurité: « back to basics »



LES JOURNÉES DE LA CYBER