PLAYER 1

HIGHSCORE 2500

SEUL À LA GUERRE : COMMENT SURVIVRE ?

START

MENU

HACKFEST 2024 - 16 BITS

MENU 01 07 12

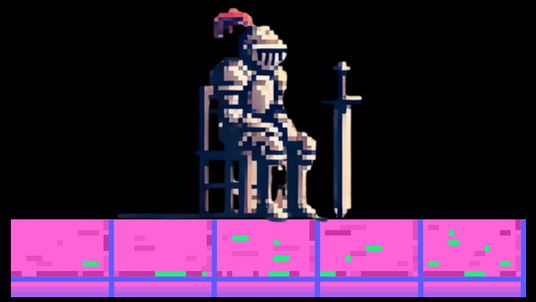
QUI SUIS-JE ?

- DANNY BOIVIN \ $NARCOMED
- 7 ANS SYSADMIN
- 5 ANS ANALYSTE EN CYBERSÉCURITÉ
- COUTEAU SUISSE\GÉNÉRALISTE
- ADORATEUR D'OLIVE
- AMATEUR DE RPG

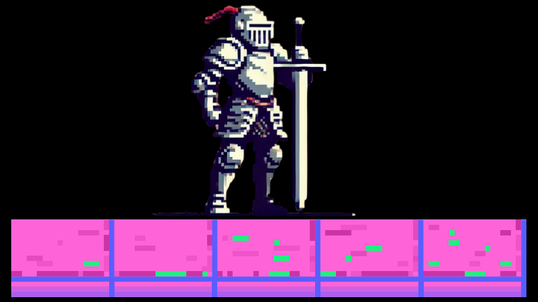
MENU 01 07 12

AGENDA

TOPICS COVERED



COMPRENDRE LA SOLITUDE



LES DÉFIS

LES CLÉS DE LA REUSSITE

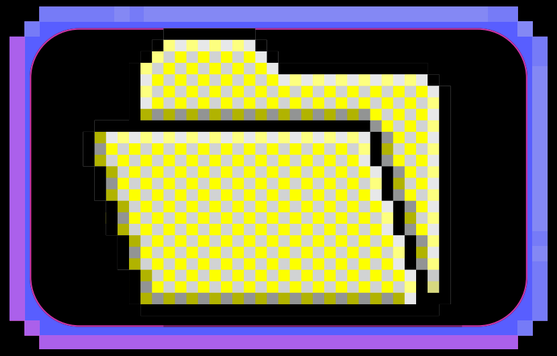
EXPÉRIENCE ET LEÇONS APPRISES

MENU

POURQUOI SOMMES-NOUS SEULS ?

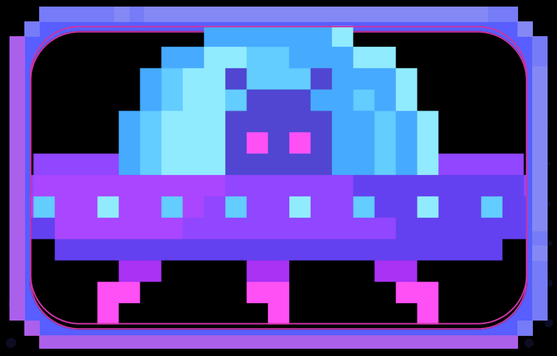
MANQUE DE RESSOURCES

Manque de budget
Manque de personnel ‘‘qualifié’’
Taille de l’entreprise



CULTURE ET PRIORITÉS

Manque de compréhension
Priorités différentes
Faible maturité organisationnelle



DÉPENDANCE EXTERNE ET CROYANCES

Source externe
Croyance en la technologie
Aveuglement volontaire

ET BEAUCOUP D’AUTRES .....


LES DÉFIS

01 07 12

ISOLEMENT ET CHARGE DE TRAVAIL

- MULTITÂCHE, PRIORITÉ CONCURRENTES
- BURN-OUT, MANQUE DE DÉCONNEXION
- MANQUE DE COLLABORATION

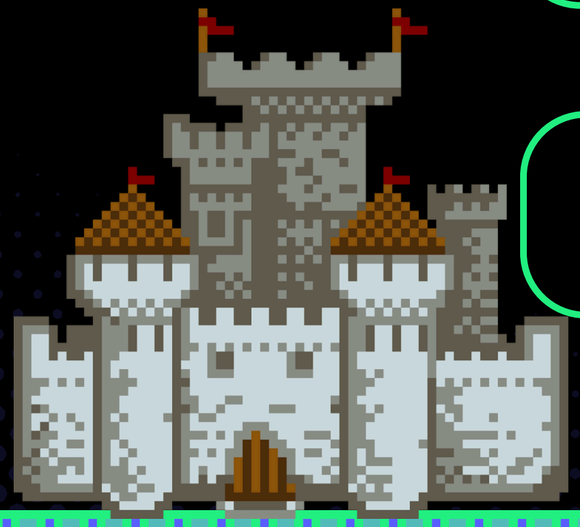
01 07 12

COMPLEXITÉ CROISSANTE DES MENACES

- ÉVOLUTION RAPIDE DES MENACES ET DE LA TECHNOLOGIE
- NÉCESSITÉ DE SE TENIR CONSTAMMENT INFORMÉ ET À JOUR
- DIVERSITÉ DES VECTEURS D'ATTAQUES

CULTURE, GOUVERNANCE ET ORGANISATION

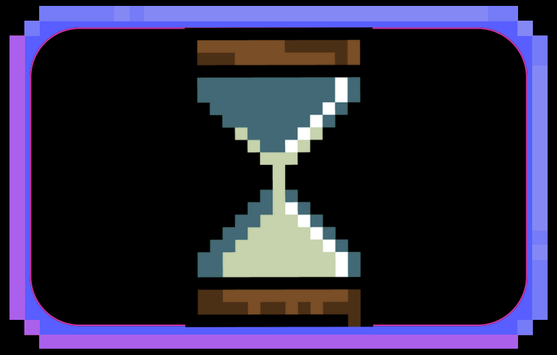
- MÊME BESOIN QUE LES GRANDES ENTREPRISES
- RESPONSABILITÉ ACCRUE
- MANQUE DE CULTURE DE LA SÉCURITÉ AU SEIN DE L'ENTREPRISE



LES CLÉS DE LA REUSSITE

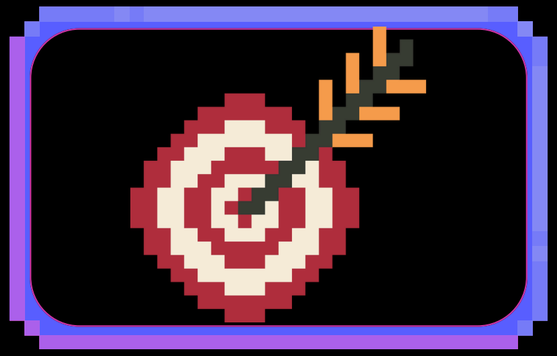
MENU

GESTION DU TEMPS ET DES PRIORITÉS



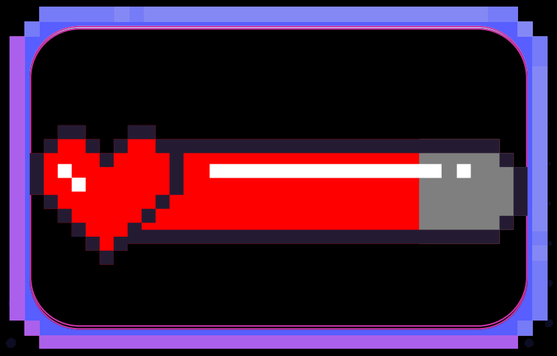
TECHNIQUES DE GESTION DU TEMPS

Utiliser la matrice d'Eisenhower, la technique Pomodoro, Kanban etc.



PRIORISATION DES TÂCHES

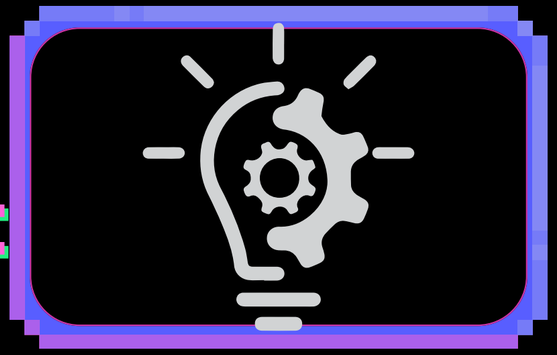
Se concentrer sur les tâches critiques et urgentes



DÉCONNEXION POUR LA SANTÉ MENTALE

S’accorder des moments de déconnexion totale afin de préserver sa santé mentale et éviter le surmenage

UTILISATION D'OUTILS ET DE MÉTHODOLOGIES



ANALYSE DES BESOINS AVEC DES FRAMEWORKS

Utiliser, CyberSecure Canada, CIS Controls v8, NIST, etc.

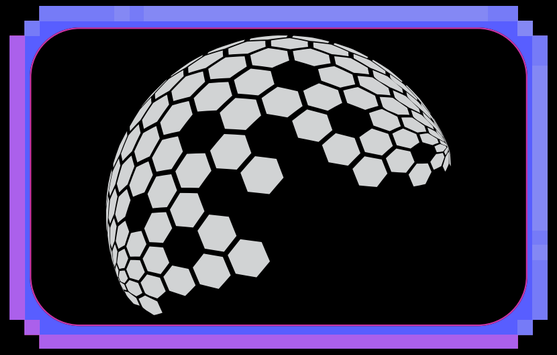
GESTION DES RISQUES AVEC DES OUTILS DÉDIÉE

Mettre en place des outils pour identifier, évaluer et suivre les risques dans les projets ou les processus.

UTILISATION DES OUTILS DE GESTION DES TÂCHES

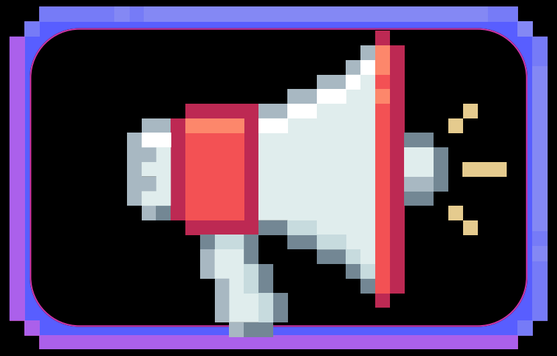
Adopter des outils de gestion des tâches ou de projets pour suivre et organiser les tâches efficacement.

COLLABORATION ET COMMUNICATION



CONSTRUIRE DES RÉSEAUX DE SOUTIEN

Collaborer avec d'autres départements et participation à des groupes de travail et des forums



COMMUNICATION EFFICACE

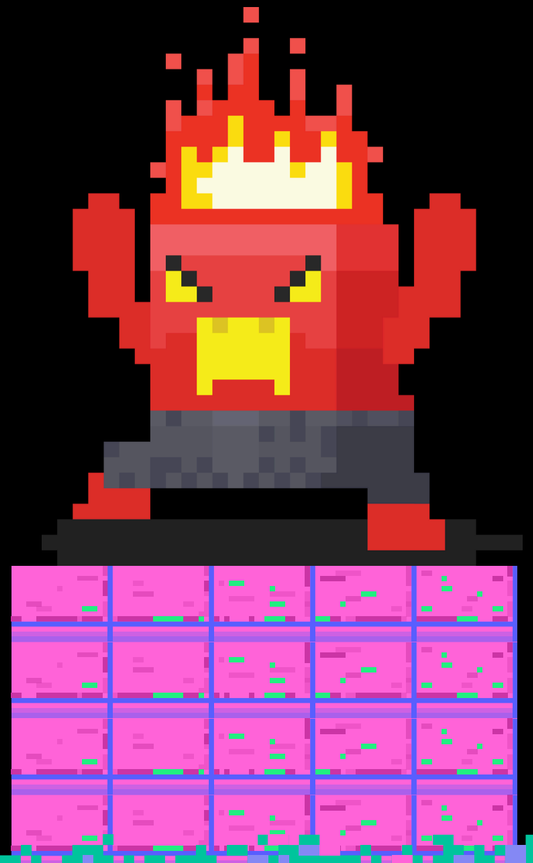
Communiquer efficacement les risques et les incidents de sécurité à la direction. Préparer et présenter des rapports de sécurité clairs et concis.

MISE EN PLACE DE “SECURITY CHAMPION”

Selon le type d’entreprise mettre en place le concept de “security champion”

EXPÉRIENCE ET LEÇONS APPRISES

HISTOIRES VRAIES



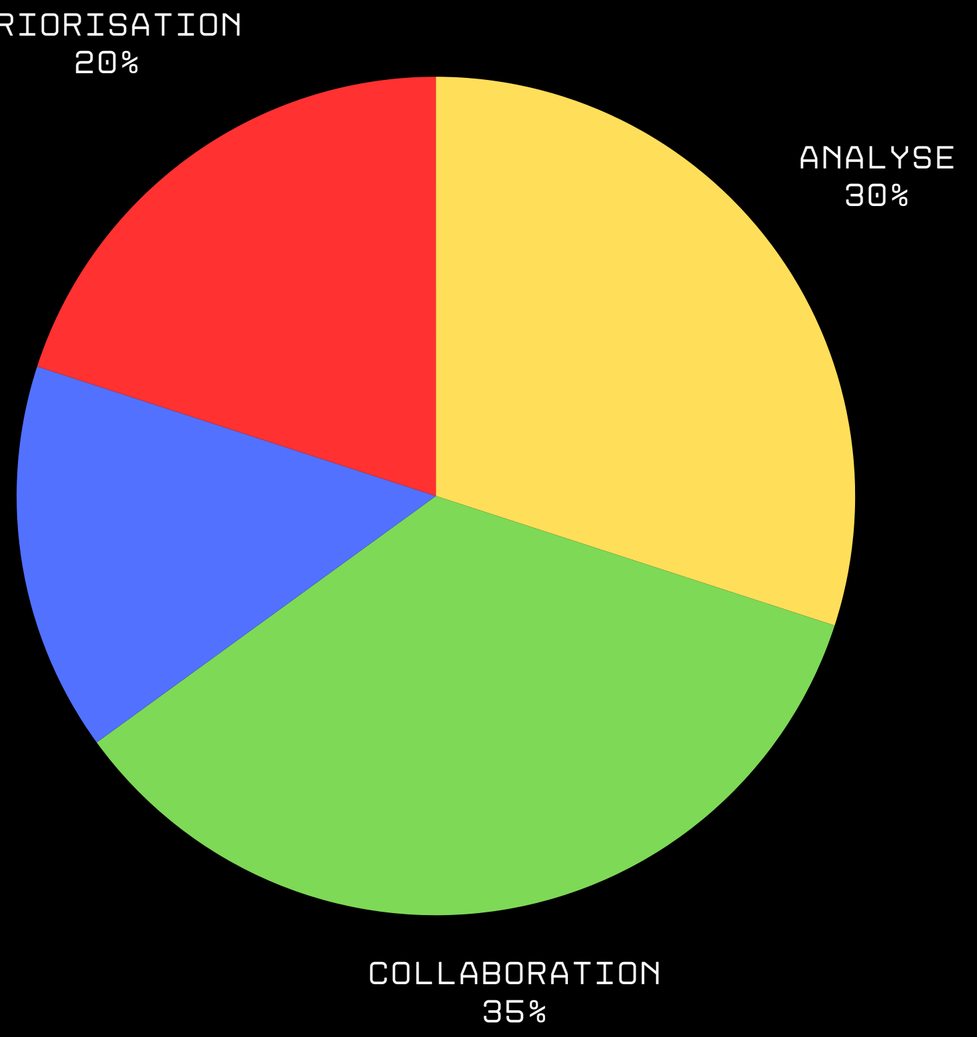
SEULEMENT RÉACTIF
ATTAQUE / PEUR D'ÊTRE "BREACHÉ"
PEU PRIS EN CONSIDÉRATION PAR LA HAUTE DIRECTION
PROCHE D'UN BURN-OUT

HIGHSCORE 2500

PLAYER

PAR OÙ COMMENCER ?

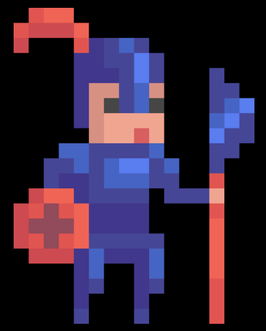
- ADAPTER SELON VOTRE RÉALITÉ



BRAINSTORM PLAN D'ACTION !

Mes recommandations

BAISSER LES ATTENTES (ÊTRE RÉALISTE)

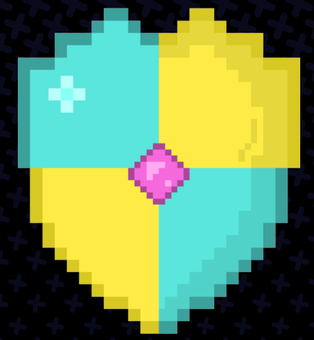


UNE BONNE FONDATION

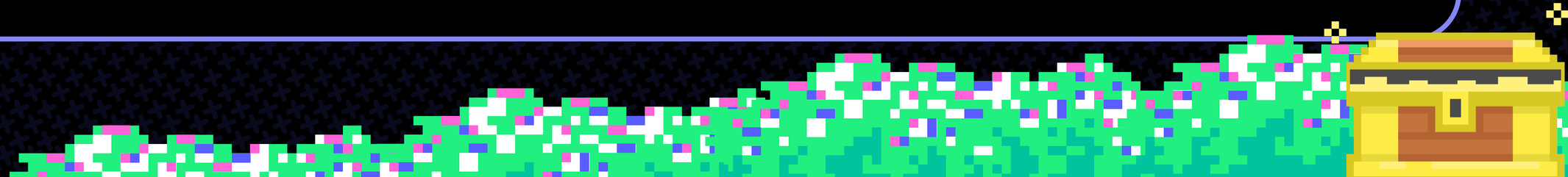
Collaboration	Audit	Identification des actions prioritaire (quick wins)
Rencontre d'équipe (IT,RH, Gestion, Devs, etc)	Inventaire des actifs	Mises à Jour et correctifs
Identifier les points de contacts clés	Identifier les systèmes critiques et obsolètes	Sauvegardes (Vérifier que les sauvegardes sont régulières, sécurisées et FONCTIONELLES)
Encourager une culture de sécurité au sein de l'entreprise.	Évaluation de la maturité a l'aide de frameworks (CyberSecure Canada, CIS Controls v8, etc)	Sensibilisation des employés

Documentation

VUE GLOBAL



COLLABORATION	ANALYSE	PRIORISATION	OPÉRATION
Communication inter-équipe	**Bien identifier les besoins d'entreprise**	**Utilisation de la pyramide d'hiérarchisation de sécurité**	**Réservation de temps horaire pour focus**
Implantation du concept de “Security Champion”	Utilisation d'un framework pour identifier les manquements (exemple CIS v8)	Implantation des KPI	Automatisation des tâches répétitives
Création d'un "Security Steering Committees" (ou comités de pilotage de la sécurité)	Identification des “quick-win”	Alignement avec les objectifs de l'entreprise	Utilisation d'outils\framrwork\plateforme
Rechercher un mentor	Avec l'aide des “security champion” identifier les problématiques	Évaluation des risques	Formation\sensibilisation



GESTION DU TEMPS\TÂCHES

Matrice d'Eisenhower

Technique Pomodoro

Méthode Kanban

Méthode Scrumban

Trello

Planka

OpenProject

RÉFÉRENTIEL

CyberSecure Canada

CISv8

NIST RMF

OWASP Top Ten

MITRE ATT&CK

MISP Threat Sharing

La hiérarchie de la réponse aux incidents

OUTIL

RealCiso

CISO Assistant

Web-Check

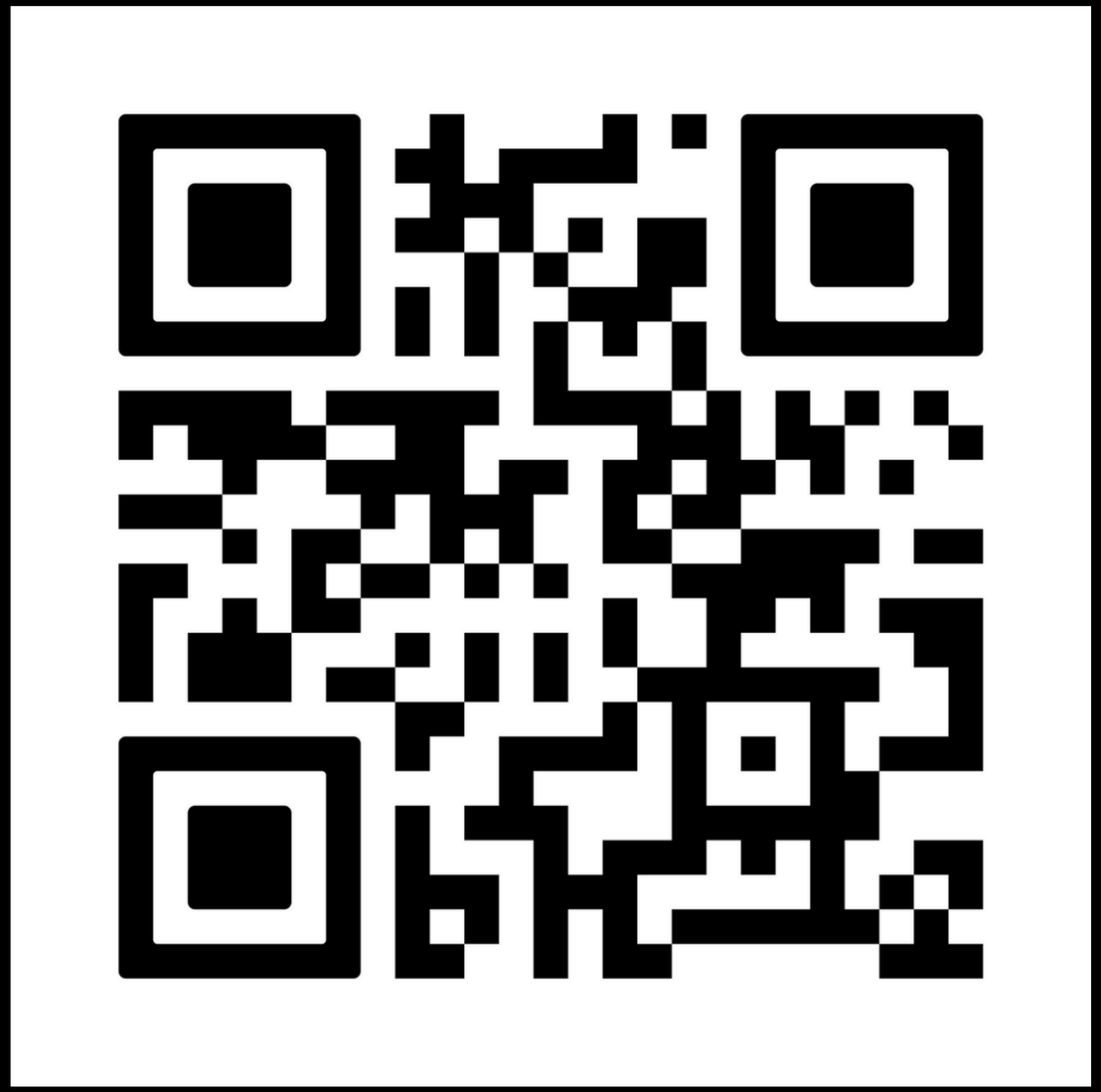
DefectDojo

SecurityOnion

Wazuh

Stride GPT

Lansweeper



https://github.com/Narc0med/presentation

MENU

MERCI

VOUS N'ÊTES PAS RÉELLEMENT SEUL !