De la CyberSecurité vers la CyberResilience

Louis Vieille-Cessay

Sales Engineering manager France & BeLux –
Micro Focus Cyber Resilience Solutions

Reimagine Cyber Resilience.

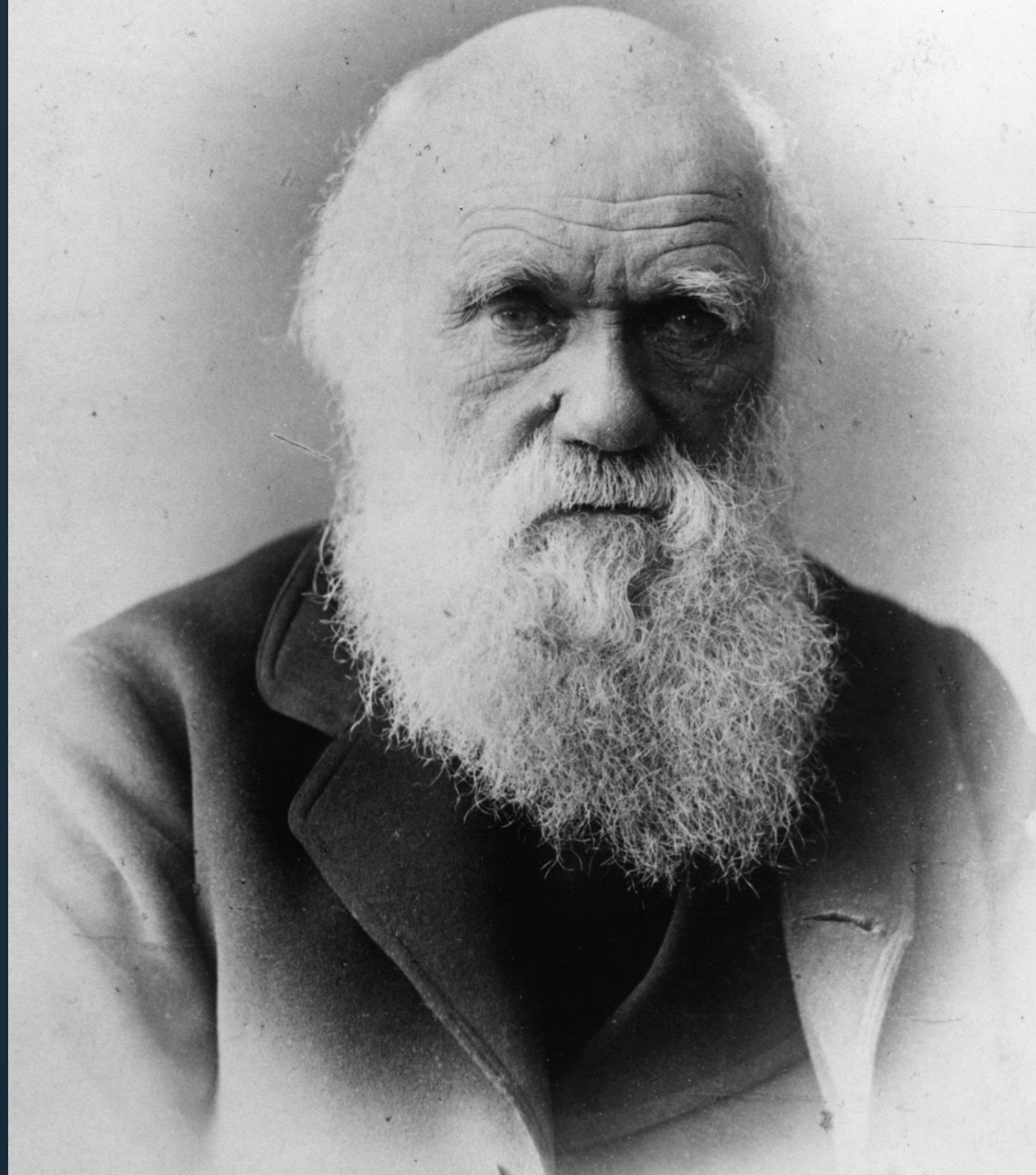
“résilience

Aptitude d'un individu à se construire et à vivre de manière satisfaisante en dépit de circonstances traumatiques. Capacité d'un écosystème, d'un biotope ou d'un groupe d'individus (population, espèce) à se rétablir après une perturbation extérieure (incendie, tempête, défrichement, etc.).”

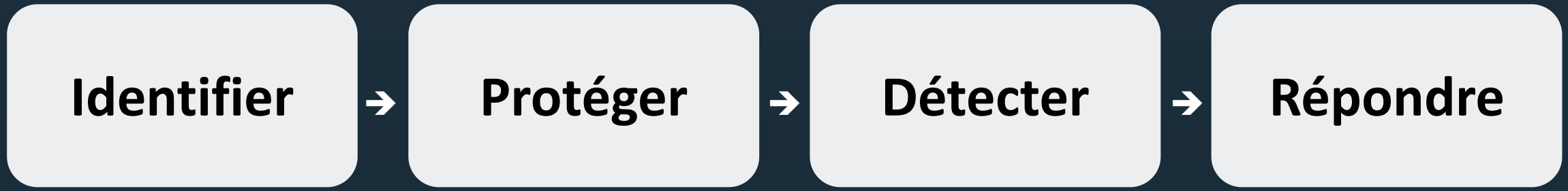
Dictionnaire Larousse

« Les espèces qui survivent ne sont pas les espèces les plus fortes, ni les plus intelligentes, mais celles qui s'adaptent le mieux aux changements. »

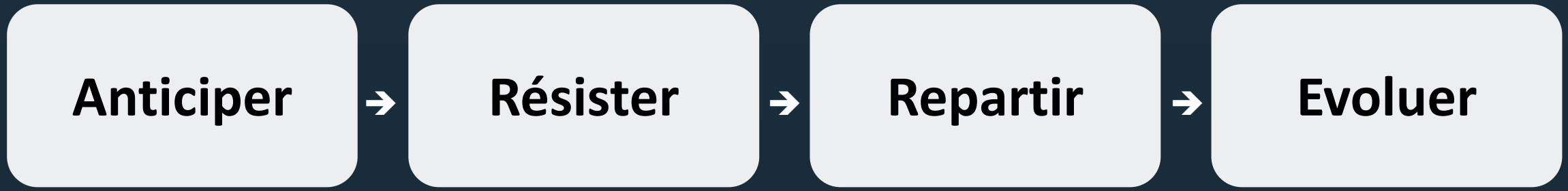
Charles Darwin



La CyberSecurité



La CyberRésilience



Une CyberRésilience Reussie

Centre de Sécurité Opérationnel

Nos Identités

Nos applications

Nos Données

Une gestion d’identité réussie

Portefeuille NetIQ

Les classiques de l’IAM

- Qui fait quoi?
- Quelles fonctions et quels droits associés?
- Quelle réalité par rapport au modèle que l’on créé?
- Quel contrôle d’accès?

Mais aussi:

- Comment protéger mes identités sensibles contre des usurpations?
- De l’analytique et de l’IA pour mieux connaitre et mieux protéger les identités. (en lien avec le SOC et les menaces connues du moment)
- Sécurisation et simplification de gestion des configurations de ces systèmes

Des données qui portent leur propre sécurité

Portefeuille Voltage

<u>Sécuriser ses données de manière homogène, où qu'elles soient:</u>

- Chez vous
- Chez un hébergeur tiers
- Sur une plateforme cloud

➔ la fin d'une logique de sécurisation des données dans un silo

<u>Quel que soit le type type de la donnée ou sa sensibilité</u>

- Données structurées
- Données non-structurées
- Communications

➔ Une meilleure sécurité, mais aussi une meilleure conformite

Un SOC moderne

Portefeuille ArcSight

Un SOC construit autour d'une capacite de comprendre

- Comment fonctionne l'organisation qu'il protège, (UEBA intégré, intégrations avec un EDR…)
- La nature des menaces actuelles (intégrations Threat-Intel, notamment MISP)

Un SOC qui détecte et remédie a des attaques

- Analyses et investigations multicouches (requête/corrélation/analytics)
- Logique/contenu de détection d'ordre méthodologique (MITRE ATT&CK)
- Un SOAR intégré, pour remédier plus vite.

Merci!