Supervision de sécurité – une évolution globalement timide depuis 20 ans

En bref – plusieurs contradictions gênent à atteindre l'objectif souhaité

Efficacité recherchée par la majorité

Face aux contradictions

Détecter au plus tôt
Comprendre et maîtriser ce qu'il se passe

Clients / bénéficiaires

Stratégies partielles et pilotage par les coûts

Sociétés de service

Industrialisation vs. expertise&initiative

Produits

Modularité vs. plateformes globales

Peut-on être satisfaits de la situation en 2022 ?

MODE commentaires

1. Les éditeurs de solution de supervision

Chaque année du ‘buzz’ autour de concepts (en apparence) nouveaux

- Deception, *DR, UBA, zero trust, etc.

On en oublie que ce n’est pas tant le produit que la manière de l’utiliser qui fait ou non sa valeur

Une tendance permanente à élargir les fonctionnalités pour construire des plateformes globales

- « qui est bon à tout devient propre à rien »…
- Eviter l’interopérabilité et rendre captif les utilisateurs

Des outils nécessitant toujours une expertise forte et des équipes spécifiques

2. Les fournisseurs de service de supervision de sécurité

Quid de l'efficacité de la supervision ?

- SLA
- Référentiels (qu’en dit PDIS ?)

Réponse à toutes les demandes des clients

- Opérer tous produits/technologies/modèles organisationnels
- Gérer la complexité des automatisations – le SOAR est au cœur du dispositif

Responsabilité parfois ambiguë

- Faire avec ce qui est donné
- RACI surprenants

Motivation à l’achat/revente et au millefeuille technologique

3. Les clients ou bénéficiaires de la supervision

Des mille-feuilles de technologies (CTI/UBA/IAM/CASB/NAC/EDR/etc.)

- Justification de budgets
- Transfert parfois naïf de responsabilités
- Réaction à incidents

Des stratégies parfois hasardeuses

- Diviser pour mieux gérer ne suffit pas
- Oubli que la défense doit rester un travail d'équipe
- Internaliser quelques très bonnes expertises est indispensable (ou aide par de très bons consultants spécialisés)

Des organisations qui restent complexes

- RSSI vs. DSI vs. directions d’usines…

MODE optimisme

Des défis pour avancer

Rendre l'existant efficace !

- Passer d'un concept ou d'une expertise pointue à une généralisation
- Optimiser les positions et fonctions de détection
- Pousser l’interopérabilité et la modularité

Mieux travailler la défense « active » - les briques sont là

- Leurres… jouer intelligemment avec (/contre) l'ennemi…
- Emulation des attaques pour s’entraîner et étalonner les solutions
- Vue réseau et vue système : faciliter l’agilité et la compréhension (rôle sonde/EDR à revoir?)
- Remédiation contrôlée (bonnes pratiques, tests, use cases)

Simplifier la construction et la compréhension d’une bonne stratégie

- Comment déléguer intelligemment des capacités de détection?
- Définition des capacités de supervision face aux menaces

S’adapter plus rapidement

- Virtualisation et couches d'abstraction relativement complexes
- « Living Off the Land »

De bonnes pistes tracées

Des modèles intéressants et à foison mais à mieux articuler

- D3fend/Att&ck/Dett&ct/OSSEM/Re&ct…

Des formats pour favoriser l'interopérabilité et les échanges

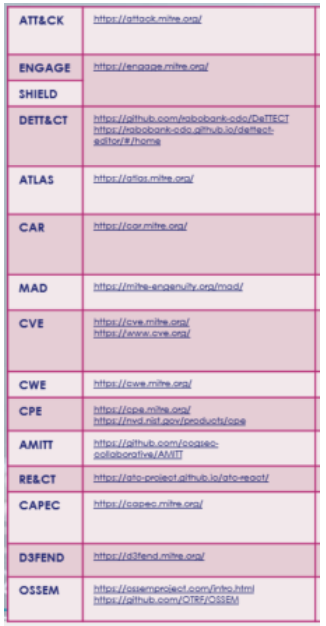
- Sigma, Yara, …

Des solutions qui se focalisent sur la simplification des usages

- Approches "no-code"
- Studios (IA, dev, etc.)

Des partages de connaissances

- Catalogue de playbooks



ATT&CK	https://attack.mitre.org/
ENGAGE	https://engage.mitre.org/
SHIELD	
DETT&CT	https://github.com/rabobank-cdc/DeTTECT https://rabobank-cdc.github.io/dettect-editor/#/home
ATLAS	https://atlas.mitre.org/
CAR	https://car.mitre.org/
MAD	https://mitre-engenuity.org/mad/
CVE	https://cve.mitre.org/ https://www.cve.org/
CWE	https://cwe.mitre.org/
CPE	https://cpe.mitre.org/ https://nvd.nist.gov/products/cpe
AMITT	https://github.com/cogsec-collaborative/AMITT
RE&CT	https://atc-project.github.io/atc-react/
CAPEC	https://capec.mitre.org/
D3FEND	https://d3fend.mitre.org/
OSSEM	https://ossemproject.com/intro.html https://github.com/OTRF/OSSEM

En conclusion

Des réussites

- Beaucoup de briques techniques et de modèles sont apparus ces dernières années et répondent à plusieurs besoins

Des frustrations

- Un usage globalement insuffisant et inefficace de ces capacités
- Une modularité qui devrait permettre d'insérer simplement des briques innovantes

Des échecs

- La pire des situations est de croire renforcer sa defense cyber mais de se rendre finalement plus vulnerable

Construire autour du postulat que 80% des utilisateurs et des bénéficiaires ne sont et seront pas des experts. Mais ce qu'ils font et utilisent en terme de supervision de sécurité doit être performant et utile.