FRANSEC

SECURING FRANCE FROM CYBER THREATS

FranSec: French IT Security Conference

1st – 2nd December 2021 // Virtual Event

WELCOME TO FRANSEC 2021

@tbillaut

https://fr.linkedin.com/in/thomasbillaut

COMMENT OPERER UN SOC DE FAÇON EFFICACE ?

ENTRE APPROCHES TRADITIONNELLES BASÉES SUR LA COUVERTURE DES RISQUES ET APPROCHES CENTRÉES SUR LA DONNÉE

THOMAS BILLAUT

FRANSEC 2021

AGENDA

- SOC et “modern” SOC
- Opérer un SOC
- Les limites du modèle
- La data et le Machine Learning, la solution ?
- Des approches vertueuses ?
- Et demain ?

AGENDA

- SOC et “modern” SOC
- Opérer un SOC
- Les limites du modèle
- La data et le Machine Learning, la solution ?
- Des approches vertueuses ?
- Et demain ?

> **A SECURITY OPERATIONS CENTER (SOC) CAN BE DEFINED BOTH AS A TEAM, OFTEN OPERATING IN SHIFTS AROUND THE CLOCK, AND A FACILITY DEDICATED TO AND ORGANIZED TO PREVENT, DETECT, ASSESS AND RESPOND TO CYBERSECURITY THREATS AND INCIDENTS, AND TO FULFILL AND ASSESS REGULATORY COMPLIANCE.**
>
> GARTNER
>
> HTTPS://WWW.GARTNER.COM/EN/NEWSROOM/PRESS-RELEASES/2017-10-12-SECURITY-OPERATIONS-CENTERS-AND-THEIR-ROLE-IN-CYBERSECURITY

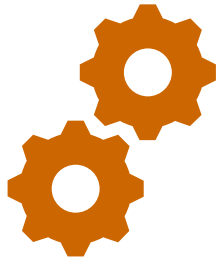
SOC ET « MODERN SOC » 1/2

LA SUPERVISION SÉCURITÉ EST UN PROCESSUS PAS UNE SOLUTION

- Concept du Security Operations Center (SOC) crée en 1990
- Créé pour centraliser l'expertise autour de la Détection et Réponse
- Mission enrichie au fil du temps avec de la protection (via retex), du pilotage de crise et des fonctions auxiliaires (problématiques de fraude, clients, techniques résultantes d'un manque d'expertise des métiers, …), de la connaissance de la menace…
- La mission d'un SOC reste de protéger l'organisation des menaces en détectant et remédiant rapidement dans un objectif de réduction de l'impact
- Des défis importants : surface d'attaque croissante résultante de la digitalisation, pénurie de talents, nouvelles technos, cadre réglementaire et législatif,…

Prevention et protection

Par influence via les retex et retours terrains

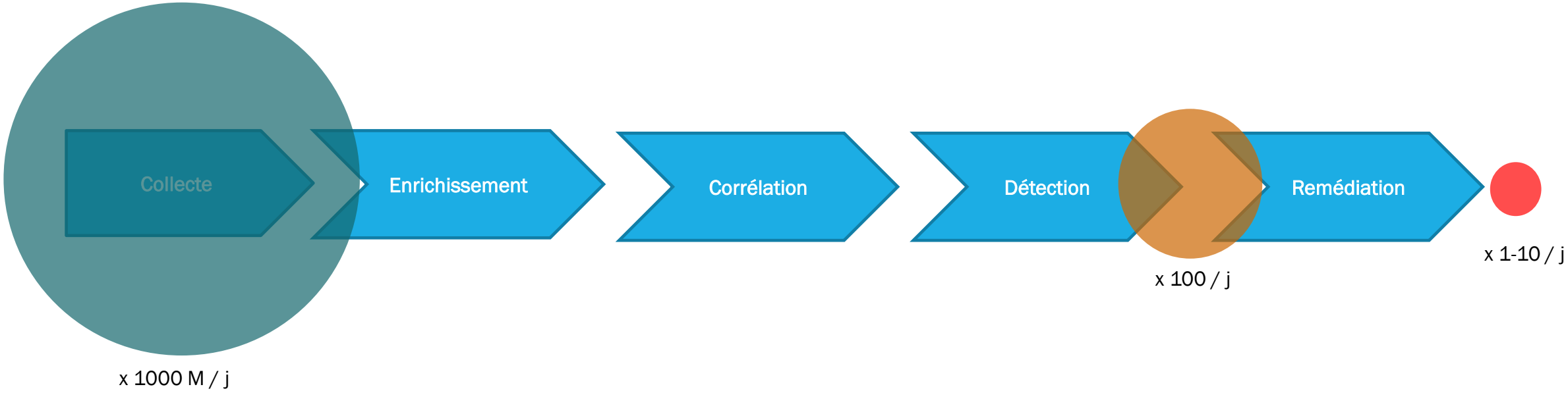


Détection

Réponse

SOC ET « MODERN SOC » 2/2

LA SUPERVISION SÉCURITÉ EST UN PROCESSUS PAS UNE SOLUTION



La supervision est un processus de bout en bout

La capacité à prendre en charge les détections et à remédier aux incidents fait partie de l'équation

AGENDA

- SOC et “modern” SOC
- Opérer un SOC
- Les limites du modèle
- La data et le Machine Learning, la solution ?
- Des approches vertueuses ?
- Et demain ?

OPERER UN SOC
AU QUOTIDIEN

Surface d'attaque et menaces

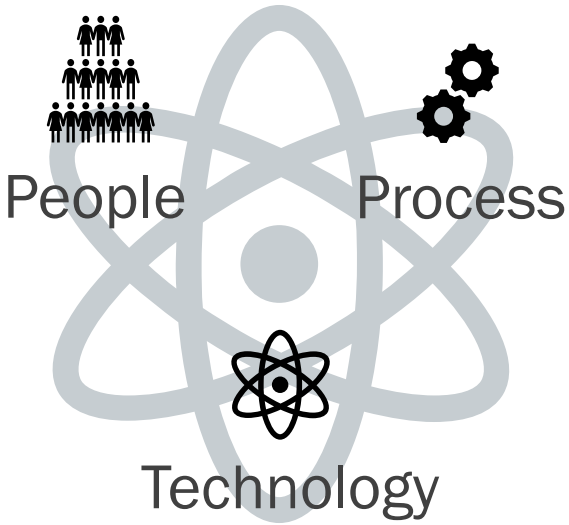
Pénurie de talents

Rupture techno

Couverture de chemins d'attaques

Conformité

« j'ai besoin de mettre en supervision » (?!)



Volume d'alerte important – non qualifié – et remédiation non automatisé

Run

Capacité à mettre en supervision sécurité insuffisante

Build

“HAVING THE RIGHT PEOPLE CAN OFTEN HAVE THE MOST PROFOUND IMPACT ON THE OVERALL CAPABILITY OF & SOC

STATE OF SECURITY OPERATIONS WITH 2016 REPORT OF CAPABILITIES AND MATURITY OF CYBER DEFENSE ORGANIZATIONS BUSINESS WHITE PAPER

HTTPS://SSL.WWW8.HP.COM/US/EN/SSL/LEADGEN/SECURE_DOCUMENT.HTML?OBJID=4AA6-3593ENW&SIEBELID=560013401

AGENDA

- SOC et “modern” SOC
- Opérer un SOC
- Les limites du modèle
- La data et le Machine Learning, la solution ?
- Des approches vertueuses ?
- Et demain ?

LES LIMITES DU MODELE ACTUEL

LA DISRUPTION SINON…

- Une activité en très forte croissance (run & build)
- Absence de priorité claire basée sur les risques (pas ou trop)
- Des collaborateurs qui montent en compétence et manquant d'expertise sur le cloud…
- Une activité en bout de chaîne : des formats de logs, de collecte, d'urbanisme, etc… non standards
- Collecter, collecter, collecter…sans idée précise de scénario de détection
- Des contraintes budgétaires, des contraintes sur le modèle de licensing
- Confusion entre conformité et sécurité
- Un retour sur investissement basé sur la réduction du risque…

AGENDA

- SOC et “modern” SOC
- Opérer un SOC
- Les limites du modèle
- La data et le Machine Learning, la solution ?
- Des approches vertueuses ?
- Et demain ?

“it’s a kind of magic…

LA DATA ET LE MACHINE LEARNING
LES PROMESSES DU MARCHÉ ACTUELLES …ET LA PERCEPTION DU TERRAIN

Les promesses du marché

- La solution aux problèmes du SOC
- Faciliter d'implémentation (plug'n play)
- Amélioration de la détection (run & build)
- Technologie idoine

VS

La perception du terrain

- Détection d'anomalie fonctionnelle
- UBA (User Behavior Analysis) fonctionnelle (sur IAM notamment)
- Des promesses lorsque le Use case est identifié et défini précisément
- Un Investissement important pour un passage à l'échelle sans date de visibilité

LA DATA ET LE MACHINE LEARNING
LA MACHINE À BULLE

x 1000 M / j

Logs/flows

Sup à 98 %

taux de prédiction

Finalement pas tant que ça...pour quel niveau de maîtrise?

LA DATA ET LE MACHINE LEARNING
UNE QUESTION DE MATURITÉ

- L'approche de détection d'anomalie ne nécessite-t-elle pas de maitriser complètement son périmètre ?
- Les usages et pratique d'administration sont-elles uniformes et standardisé avec une déviance faible?
- Capacité à pouvoir qualifier chaque alarme et à customiser le moteur de détection à son environnement
- Potentiellement très consommateur de temps de comprendre une anomalie ? Et très frustrant lorsque la conclusion n'est pas au bout
- Qu'est-ce qui est normale lorsqu'une situation est anormale (cf télétravail massif suite à la crise du covid)?

Basic CIS controls

1-6 basics
7-16 foundational
16-20 organizational

AGENDA

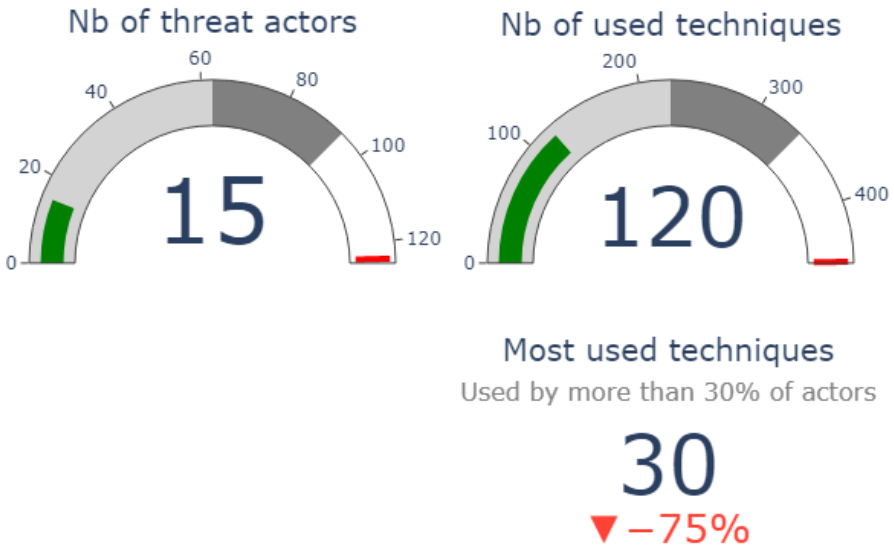
- SOC et “modern” SOC
- Opérer un SOC
- Les limites du modèle
- La data et le Machine Learning, la solution ?
- Des approches vertueuses ?
- Et demain ?

DES APPROCHES VERTUEUSES ?
MOINS D'AMBITION, PLUS DE PRAGMATISME

- Commencer par utiliser les données disponibles pour prioriser:
  - Connaissance de la menace : comprendre les TTPs prioritaires
  - Contextualisation de la menace : utiliser les feeds en osint (top 1 m Alexa, …) et de threat intel (gratuit/premium)
  - Adresser les principaux UC de détection en fonction de la menace, un après l'autre, de bout en bout jusqu'à la remédiation automatisée

- Utiliser les solutions du marché ou home made sur des UC dédiés en les intégrant de bout en bout à son environnement (People, process, techno)
  - La classification par niveau de risque des connexions (à l'AD, à l'AAD)
  - La classification des processus d'exécution de commande
  - La classification des créations de process

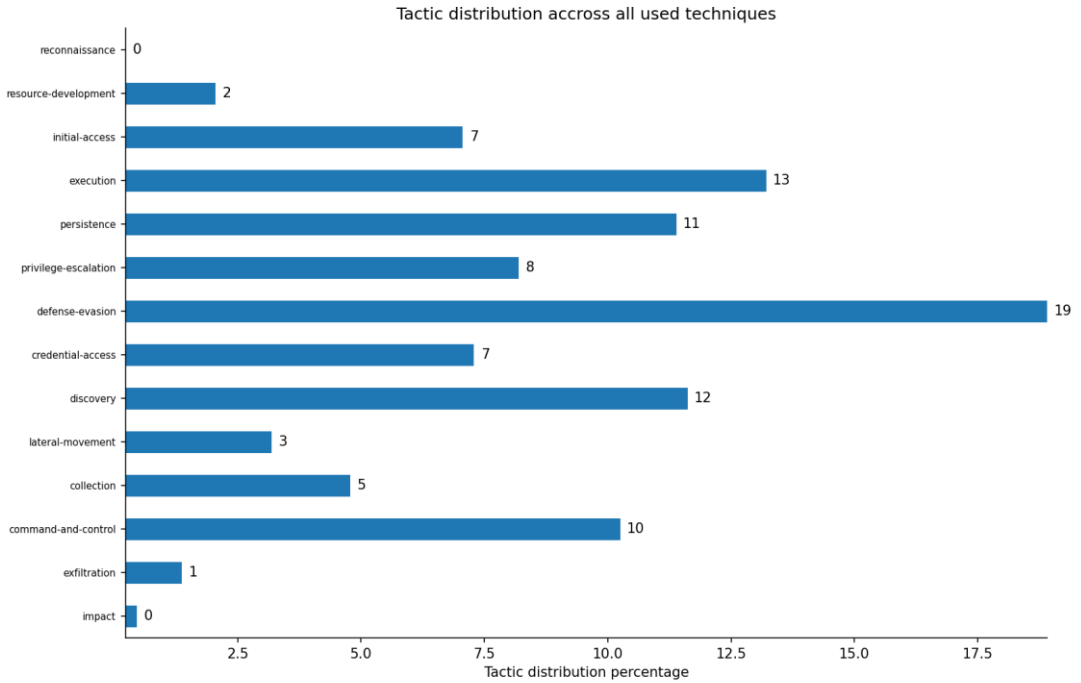
DES APPROCHES VERTUEUSES ?
UTILISER LA DONNÉE POUR MIEUX PRIORISER



Groupe d'attaquants

menaçant le secteur telecom worldwide

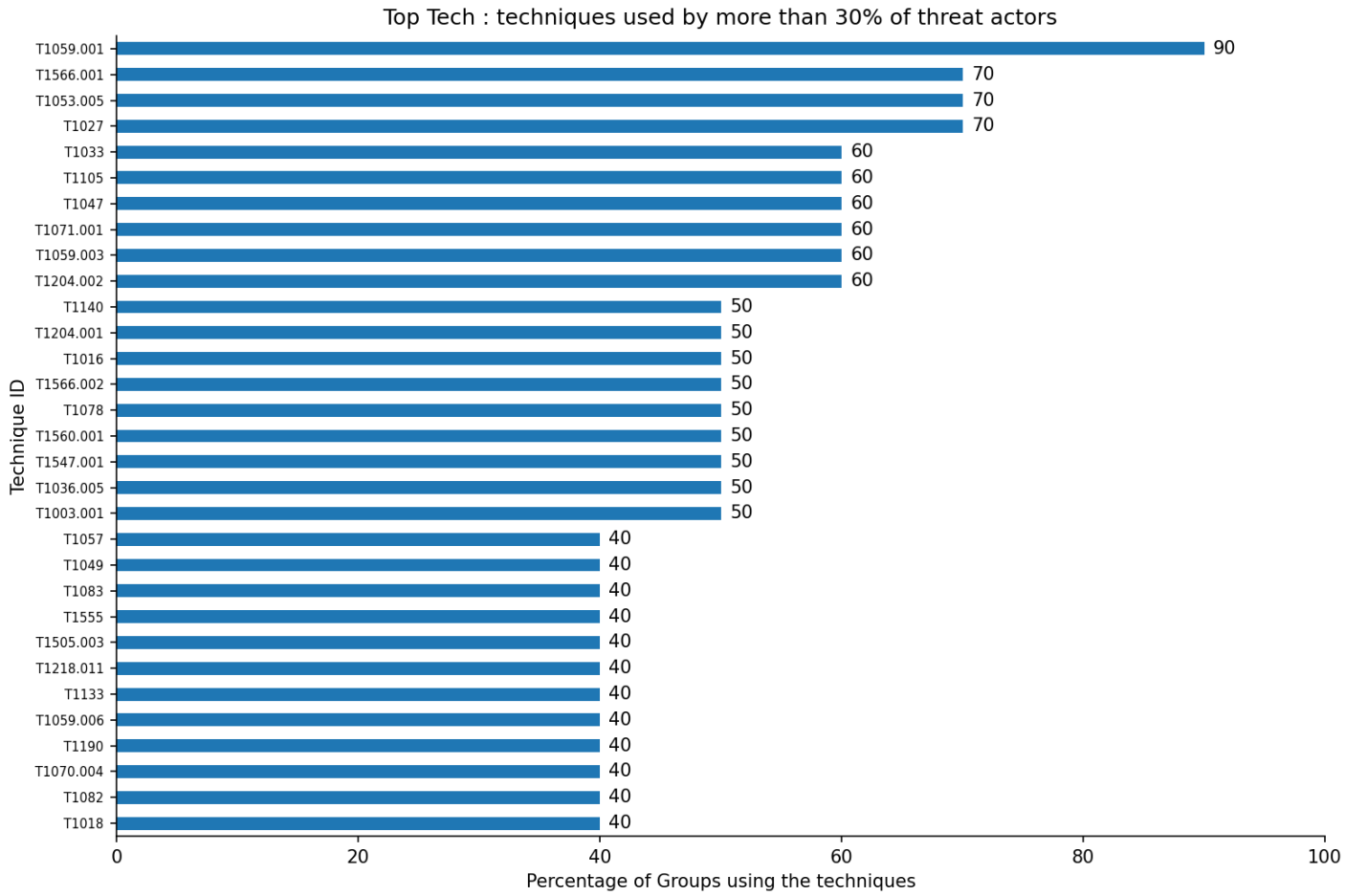
source Mitre Att&ck

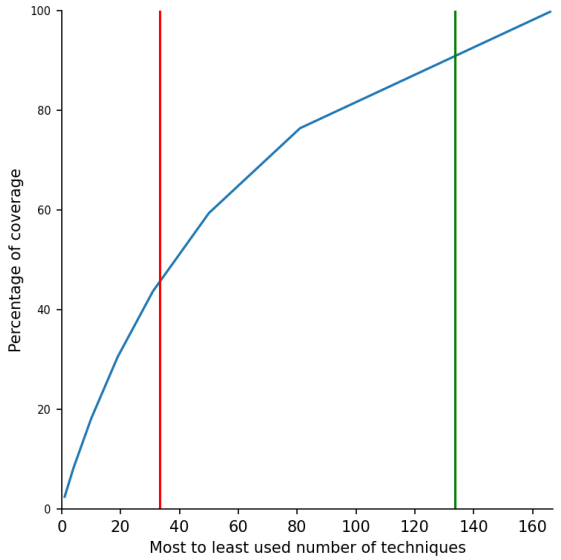


Répartition des tactiques pour l'ensemble des groupes d'attaquants

source Mitre Att&ck

DES APPROCHES VERTUEUSES ?
ADRESSER LES TECHNIQUES LES PLUS UTILISÉES





Techniques les plus utilisées par les groupes d'attaquants menaçant le secteur telecom : très loin du Pareto

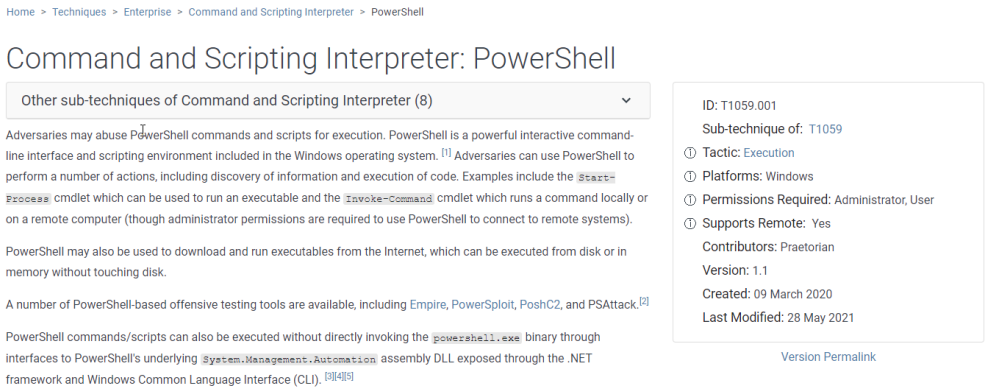
source Mitre Att&ck

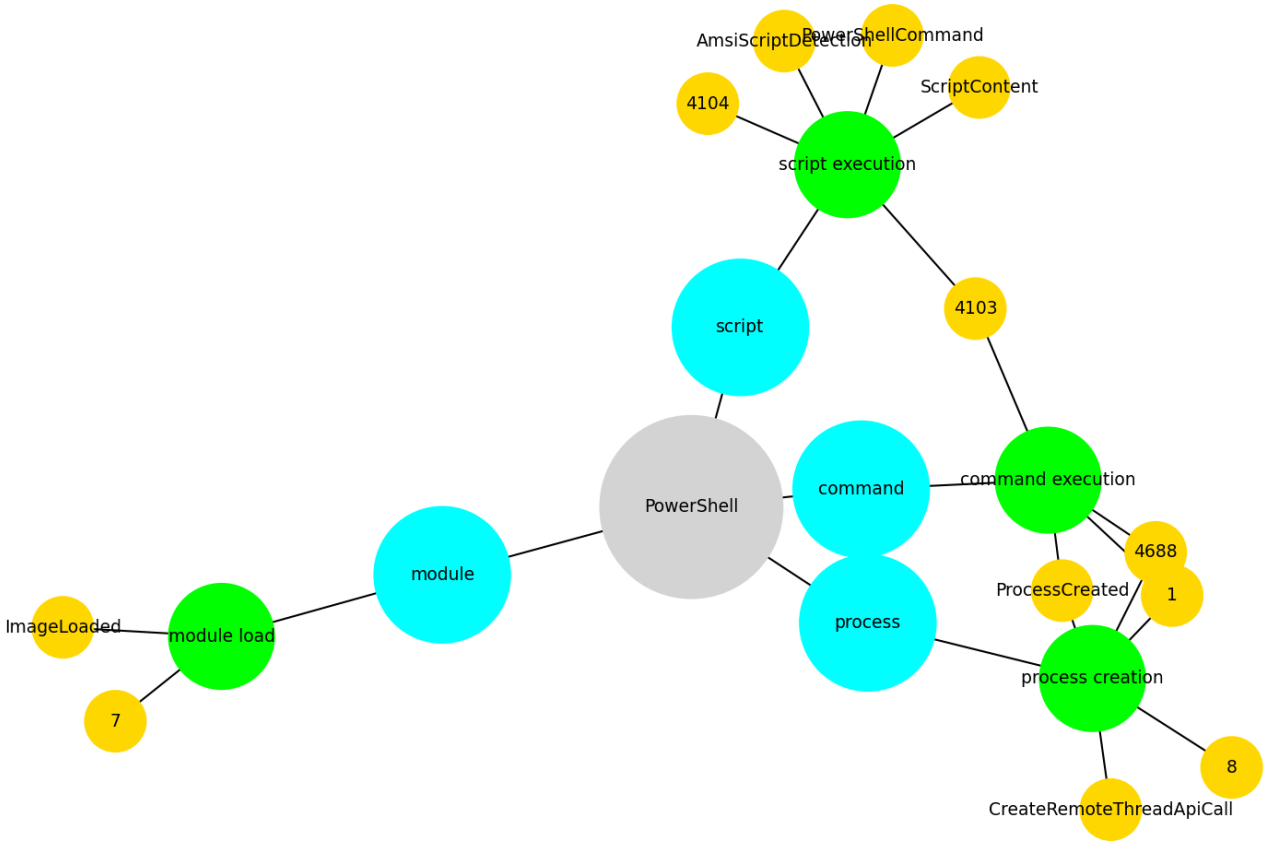
DES APPROCHES VERTUEUSES ?
COLLECTER LES LOGS NECESSAIRES POUR DETECTER

T1059.001

technique utilisée par 90% des groupes d'attaquants menaçant le secteur telecom

source Mitre Att&ck

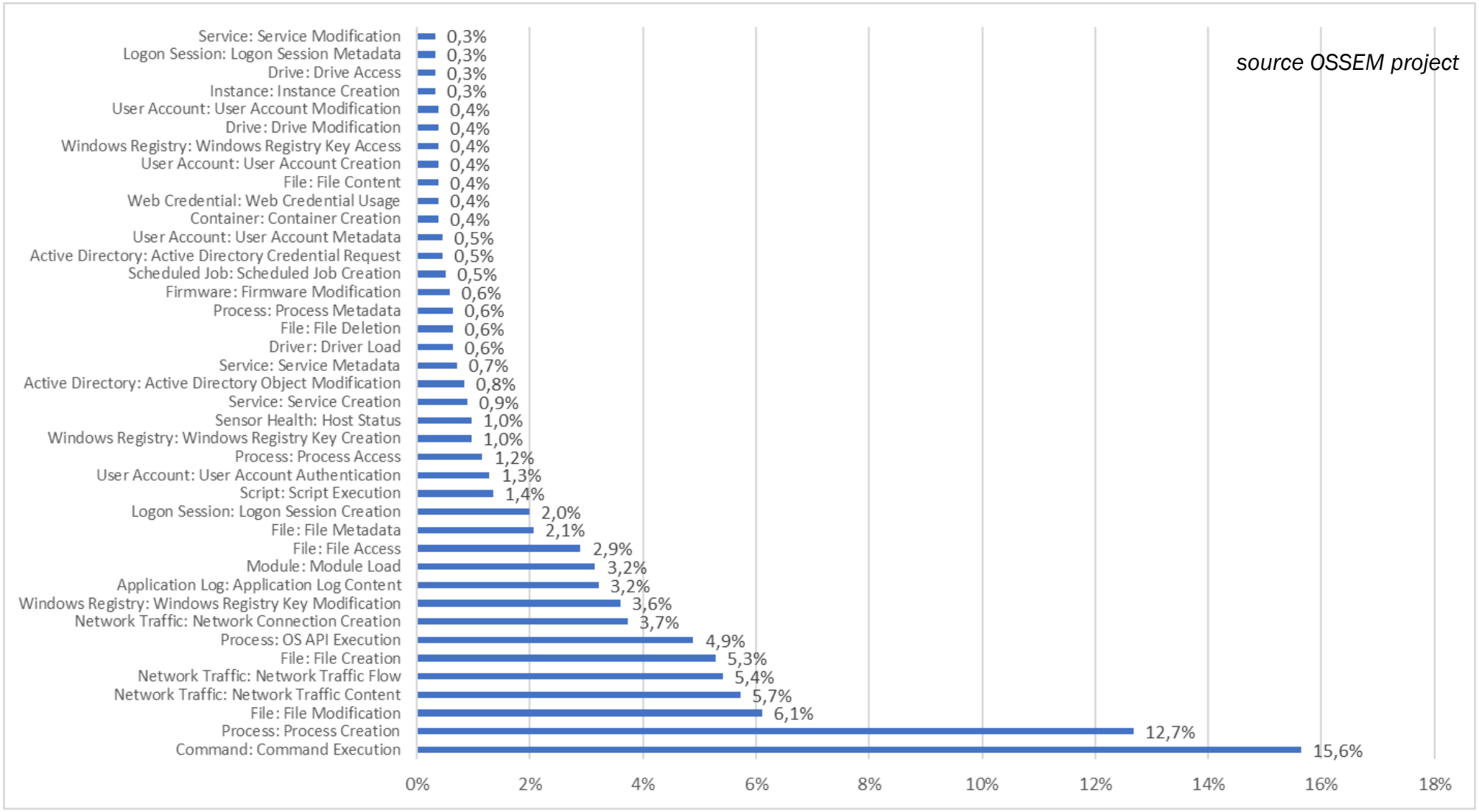




source OSSEM project

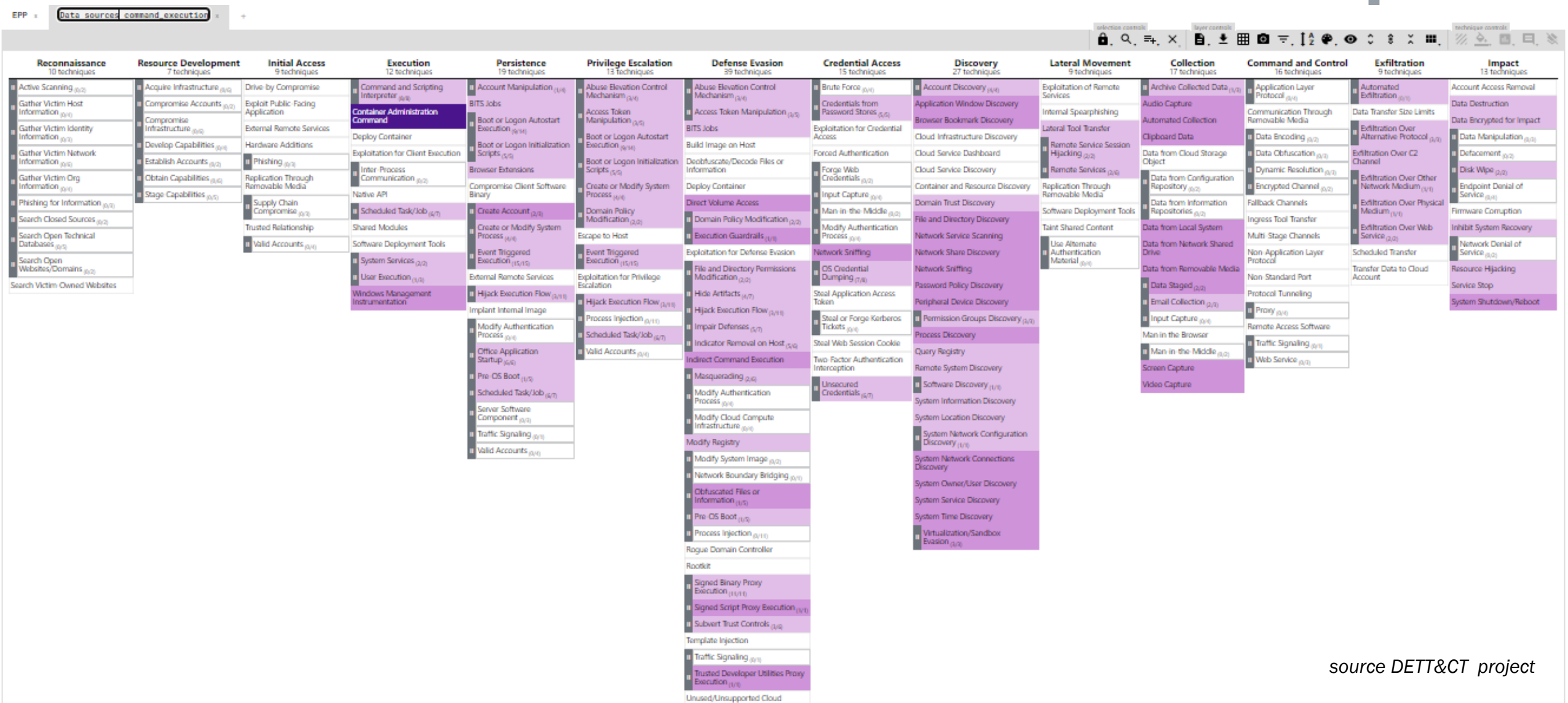
DES APPROCHES VERTUEUSES ?

S'APPUYER SUR UN FRAMEWORK POUR COUVRIR LES UC PERTINENTS



DES APPROCHES VERTUEUSES ?

MITRE ATTACK COVERAGE ON COMMAND EXECUTION ONLY



source DETT&CT project

DES APPROCHES VERTUEUSES ?
UTILISER L'APPRENTISSAGE AUTOMATIQUE (ML) DE FAÇON PRECISE SUR DES UC

- Une approche par UC (use case) en les intégrant de bout en bout à son environnement (People, process, techno)
- En s'appuyant sur les solutions de marché, la classification par niveau de risque des connexions (à l'AD, à l'AAD)
  - Solutions UBA pour connexions AD (via SIEM par ex)
  - Solutions disponibles dans le cloud
- En développant ses propres algorithlmes pour catégoriser - ou détecter les anomalies – sur UC identifié et maitrisé (known good par ex)
  - Permet d'accélérer la phase de qualification
  - Permet d'acculturer le personnel et de créer une courbe d'apprentissage vertueuse

Sign-in Activity	Risk Level
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical location	Medium
Users with leaked credentials	High

Sign in activity with corresponding Risk.

Exemple de solutions de catégorisation des connexions dans le cloud public

source Microsoft

AGENDA

- SOC et “modern” SOC
- Opérer un SOC
- Les limites du modèle
- La data et le Machine Learning, la solution ?
- Des approches vertueuses
- Et demain ?

ET DEMAIN ?

CONTINUER A PERSEVERER

- L'utilisation de la donnée (en source ouverte et payante) à l'échelle est un élément clé dans l'efficacité des activités de supervision sécurité (SOC)
- L'utilisation de certaines technologies d'UBA intégré de bout en bout à l'activité du SOC permet également une amélioration de l'efficacité
- Définir et implémenter ses propres UC de data permet d'acculturer et faciliter la montée en compétence des collaborateurs – et de mieux comprendre le marché et les solutions disponibles
- La promesse d'une IA améliorant significativement la détection et la remédiation dans des processus end2end déjà existants restent à concrétiser
- Travailler la complémentarité homme/machine…de façon à éviter les échanges philosophiques sur la capacité du ML/IA à détecter les APTs…

“AVEC UN TALENT ORDINAIRE ET UNE PERSÉVÉRANCE EXTRAORDINAIRE, ON PEUT TOUT OBTENIR

THOMAS FOXWELL BUXTON

MERCI

@tbillaut

https://fr.linkedin.com/in/thomasbillaut

FRANSEC

SECURING FRANCE FROM CYBER THREATS

FranSec: French IT Security Conference

1st – 2nd December 2021 // Virtual Event

ANNEXES ET REFERENCE

- **Autonomic Security Operations**
  10 x Transformation of the security Operations Center
  Iman Ghanizada, Dr. Anton Chuvakin
  - https://github.com/redcanaryco/atomic-red-team

- **MITRE ATTACK**
  - https://attack.mitre.org/

- **DETT&CT**
  - https://rabobank-cdc.github.io/dettect-editor/#/home
  - https://github.com/rabobank-cdc/DeTTECT

- **OSSEM PROJECT**
  - https://ossemproject.com
  - https://github.com/OTRF/OSSEM