Anatomie d’une attaque ransomware

retour d’expérience et points essentiels à retenir

© 2001-2022 APPROACH

Speaker

Laurent Deheyer

SOC Director

Approach Belgium

© 2001-2022 APPROACH

Anatomie d’une attaque ransomware

- Retour d’expérience CSIRT: ransomware
- Points essentiels à retenir
  - Evaluer votre surface d’attaque
  - Patcher intelligemment
  - Activer l’authentification forte
  - Augmenter votre visibilité et automatisation
  - Préparez-vous au pire
- Conclusion

© 2001-2022 APPROACH

Retour d’expérience CSIRT

Ransomware

© 2001-2022 APPROACH

Retour d’expérience CSIRT : ransomware

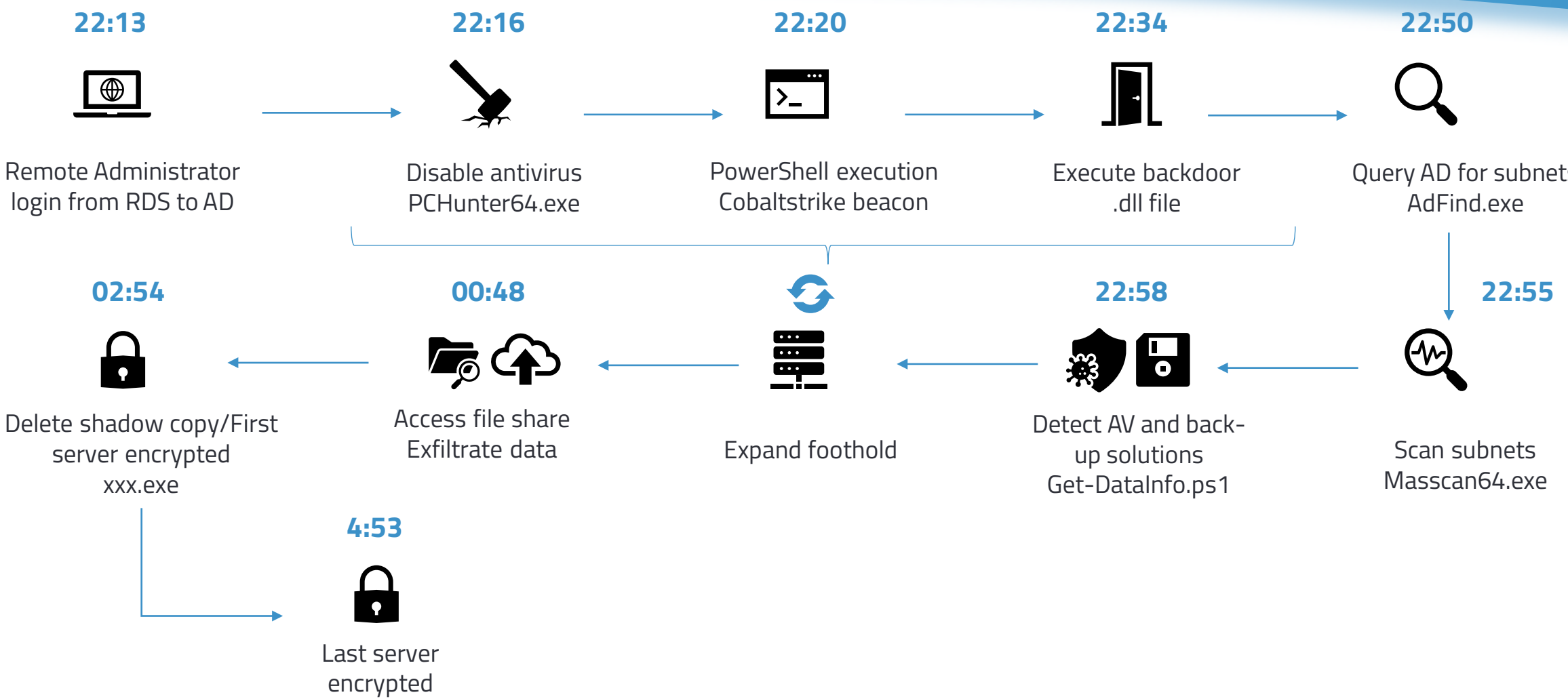
Contexte de l’organisation victime

- 350 postes de travail
- 20 serveurs
- Active Directory local
- Utilisation de M365
- Mesure de sécurité traditionnelle (AV, firewall, VPN, backup)
- Service d’accès bureau distant
- Fournisseur IT externe

© 2001-2022 APPROACH

Retour d'expérience CSIRT : ransomware

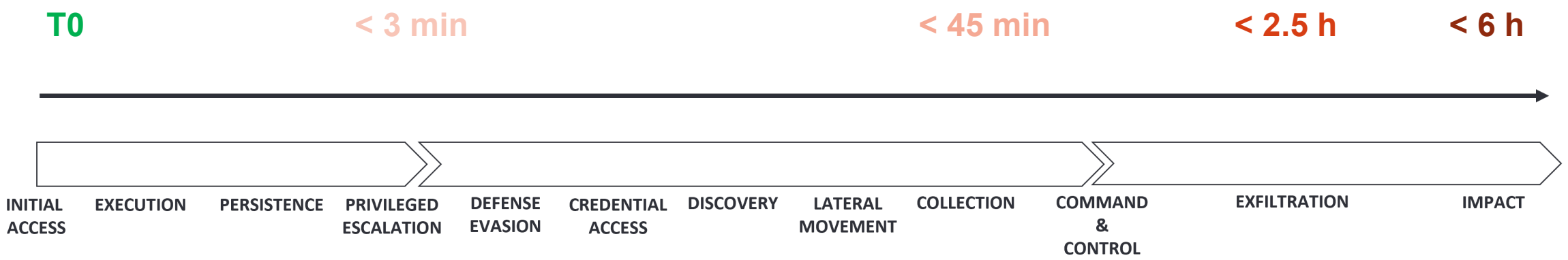
Ce qu'il s'est passé



© 2001-2022 APPROACH

Retour d'expérience CSIRT : ransomware

FAIT N°1 : La ligne de temps



© 2001-2022 APPROACH

Retour d'expérience CSIRT : ransomware

FAIT N°2 : l'accès initial

Pas d'artefact expliquant l'accès initial et escalade de privilège.

Potentiellement :

- Vol d'identifiants
- Brute force
- Exploit de CVE

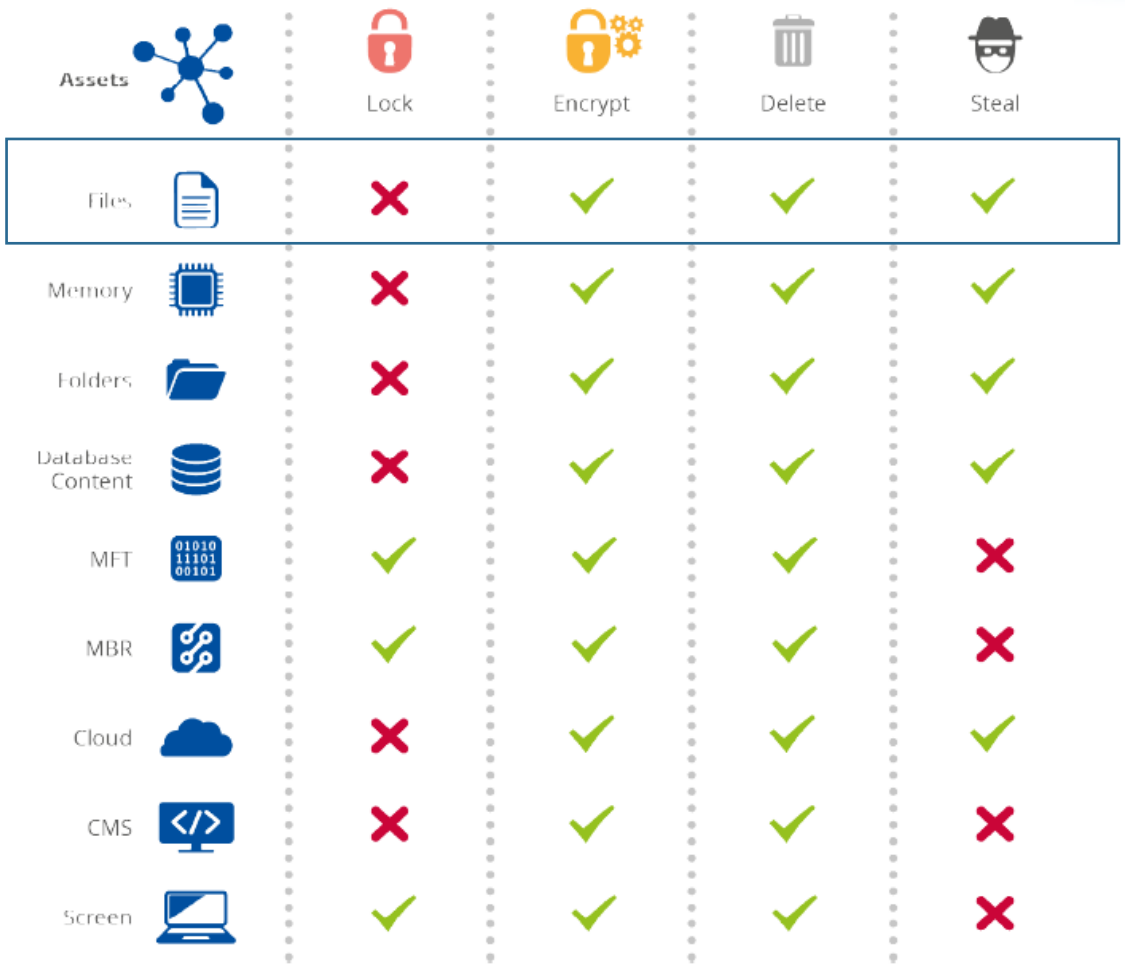
*In **95.3%** of the incidents, it is not known how threat actors obtained initial access into the target organization**

*ENISA THREAT LANDSCAPE FOR RANSOMWARE ATTACKS July 2022

© 2001-2022 APPROACH

Retour d'expérience CSIRT : ransomware

FAIT N°3 : le type d'action du ransomware



*ENISA THREAT LANDSCAPE FOR RANSOMWARE ATTACKS July 2022

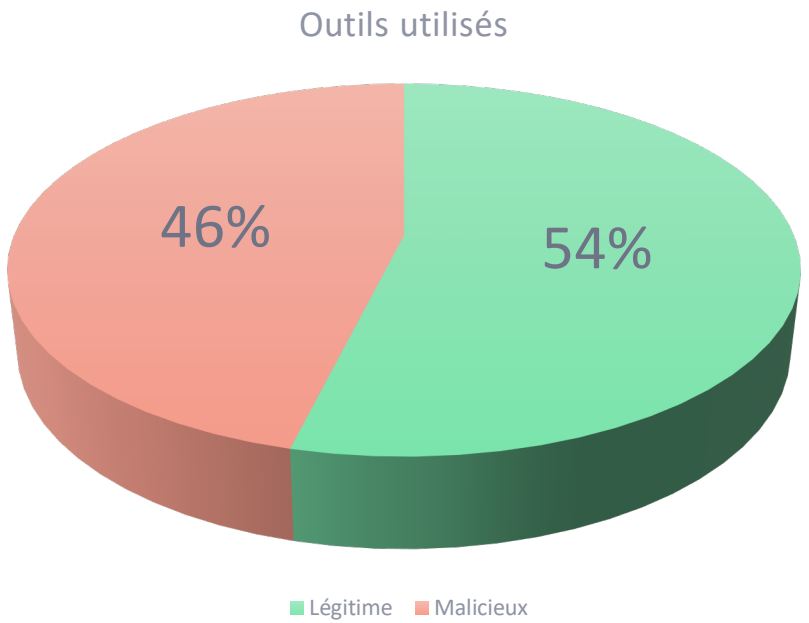
© 2001-2022 APPROACH

Retour d'expérience CSIRT : ransomware

FAIT N°4 : les outils utilisés

Outil légitime	MITRE ATT&CK	
binaire natif de l'OS	technique	tactique
powershell	T1056.001 T1564.003	EXECUTION
net.exe	T1056.003	EXECUTION
cmd.exe	T1218.011	EXECUTION
outils d'administration	technique	tactique
ADFind.exe	T1016	DISCOVERY
Filezilla	T1048.003	EXFILTRATION
chrome.exe mspaint.exe	T1039	COLLECTION

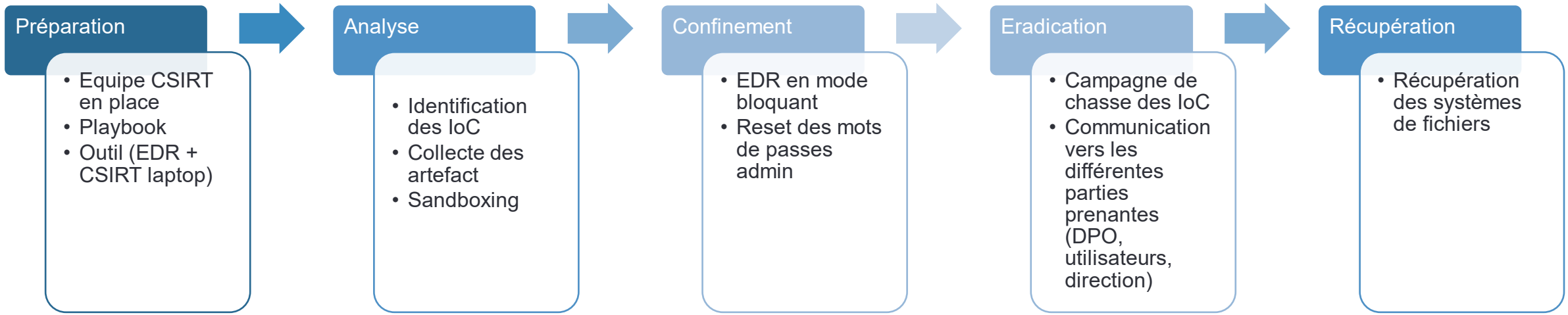
Outil malvaillant	MITRE ATT&CK	
	technique	tactique
PowerTool64.exe PCHunter64.exe	T1562.001	DEFENSE EVASION
masscan64.exe	T1046	DISCOVERY
getdata-info.ps1	T1518.001	COLLECTION
xxx.exe	T1486	IMPACT
ss.dll	T1218.011	DEFENSE EVASION



© 2001-2022 APPROACH

Retour d'expérience CSIRT : ransomware

Stratégie de gestion de l'incident



© 2001-2022 APPROACH

Points essentiels à retenir

© 2001-2022 APPROACH

Points essentiels à retenir

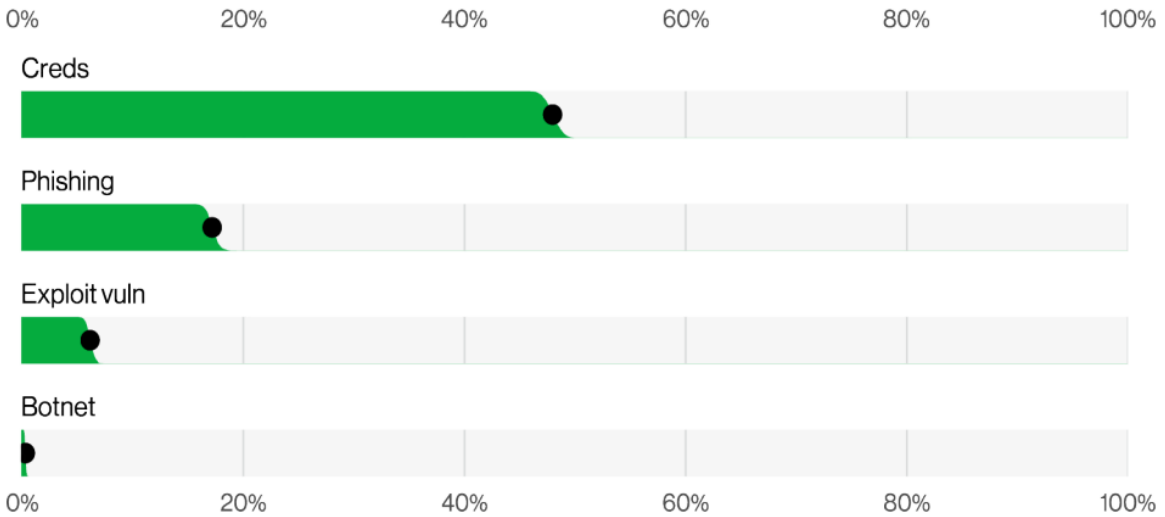
ACTION 1 : Evaluer votre surface d'attaque

- Exploitation de CVE

CVE-2021-34523	CVE-2021-26084
CVE-2021-34473	CVE-2010-2861
CVE-2021-31207	CVE-2021-36942
CVE-2021-26855	CVE-2021-34523

  - Quelques exemples:
    - SMBv1
    - MS Exchange
    - Log4J
  - Local Privilege Escalation
  - Remote Code Execution

- Vol, divulgation d'identifiants



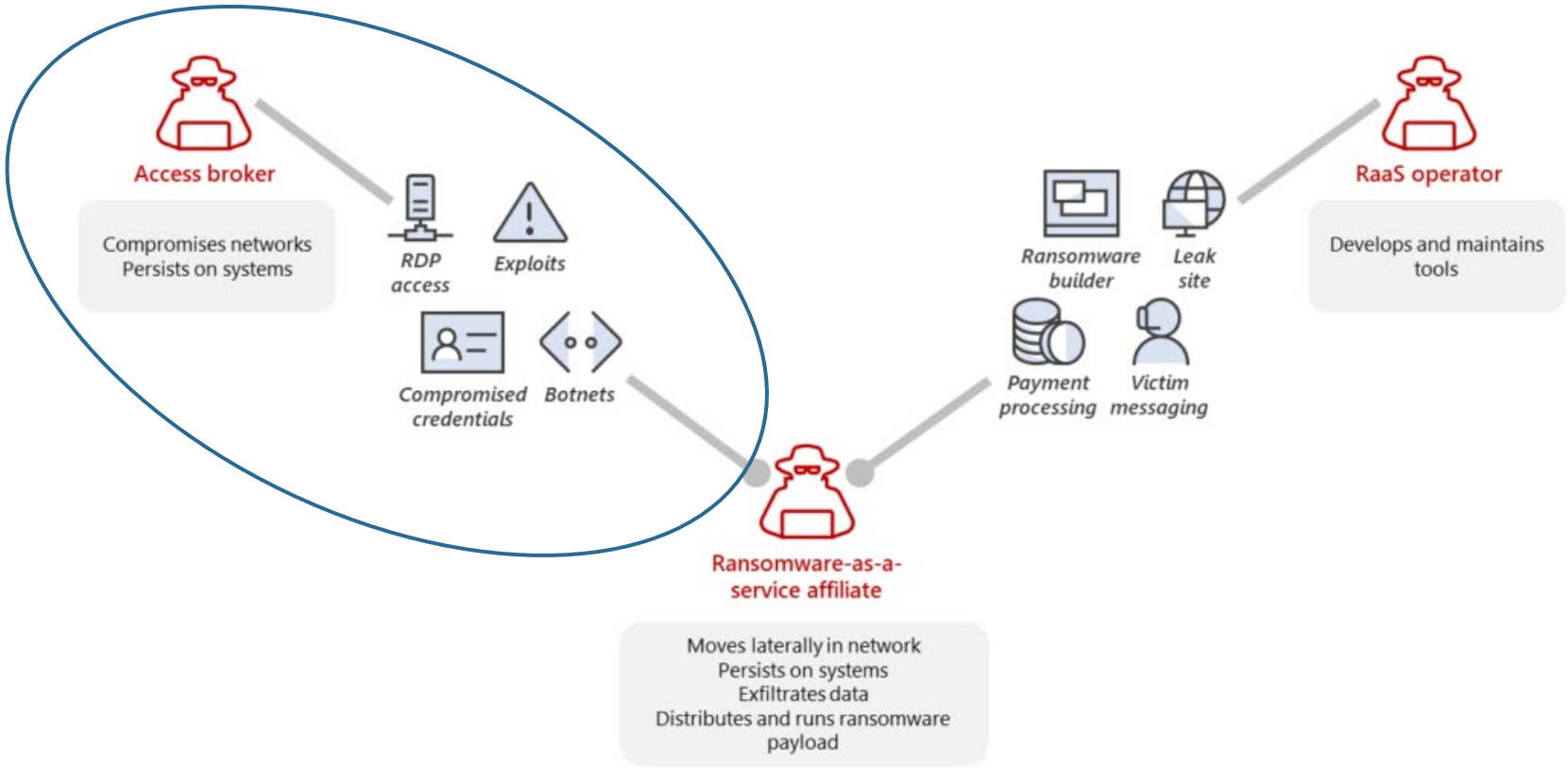
Source: Verizon Databreach Investigation Report 2022

© 2001-2022 APPROACH

Points essentiels à retenir

ACTION 1 : Evaluer votre surface d'attaque

Ransomware as a service: Understanding the cybercrime gig economy



Source: https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

© 2001-2022 APPROACH

Points essentiels à retenir

Patcher vos systèmes

Les Ransomware as a Service visent les low hanging fruits ..
Et donc des CVE connus.

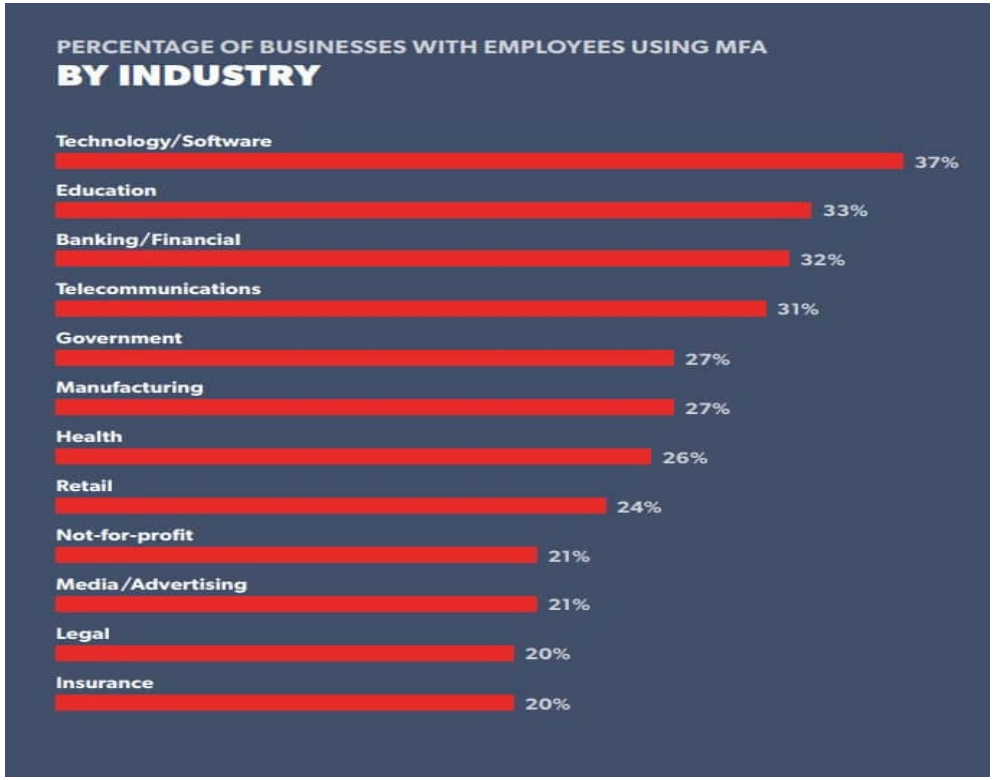
…. MAIS …. Adopter une stratégie de patching « risk based ».

Priorisez les vulnérabilités qui comptent réellement, en fonction de votre contexte métier (et de votre surface d'attaque).

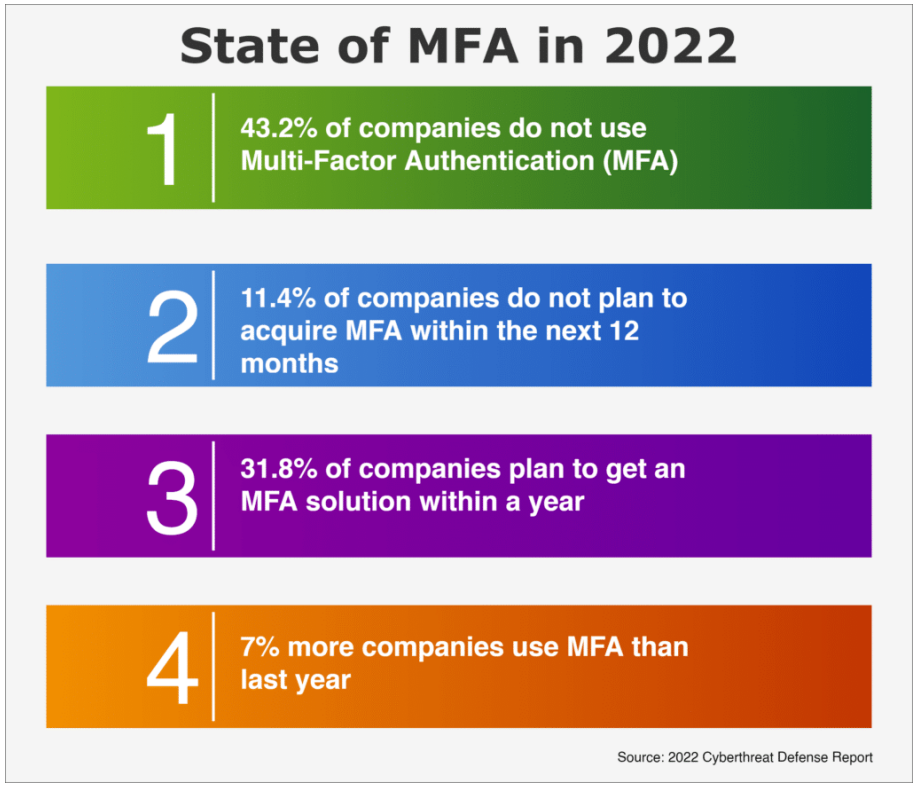
© 2001-2022 APPROACH

Points essentiels à retenir

ACTION 2 : activer le MFA



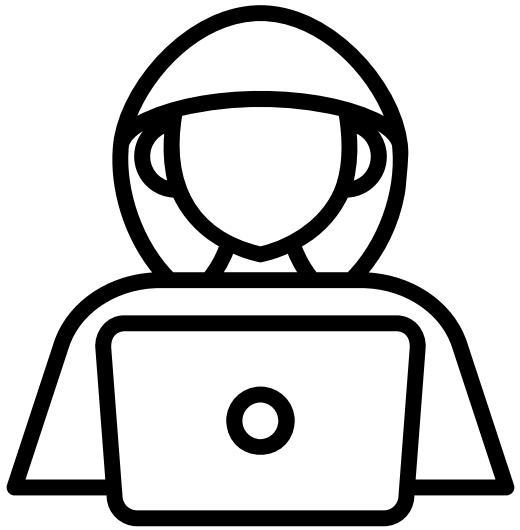
Source: LastPass



© 2001-2022 APPROACH

Points essentiels à retenir

ACTION 3 : augmenter votre visibilité et automatisation

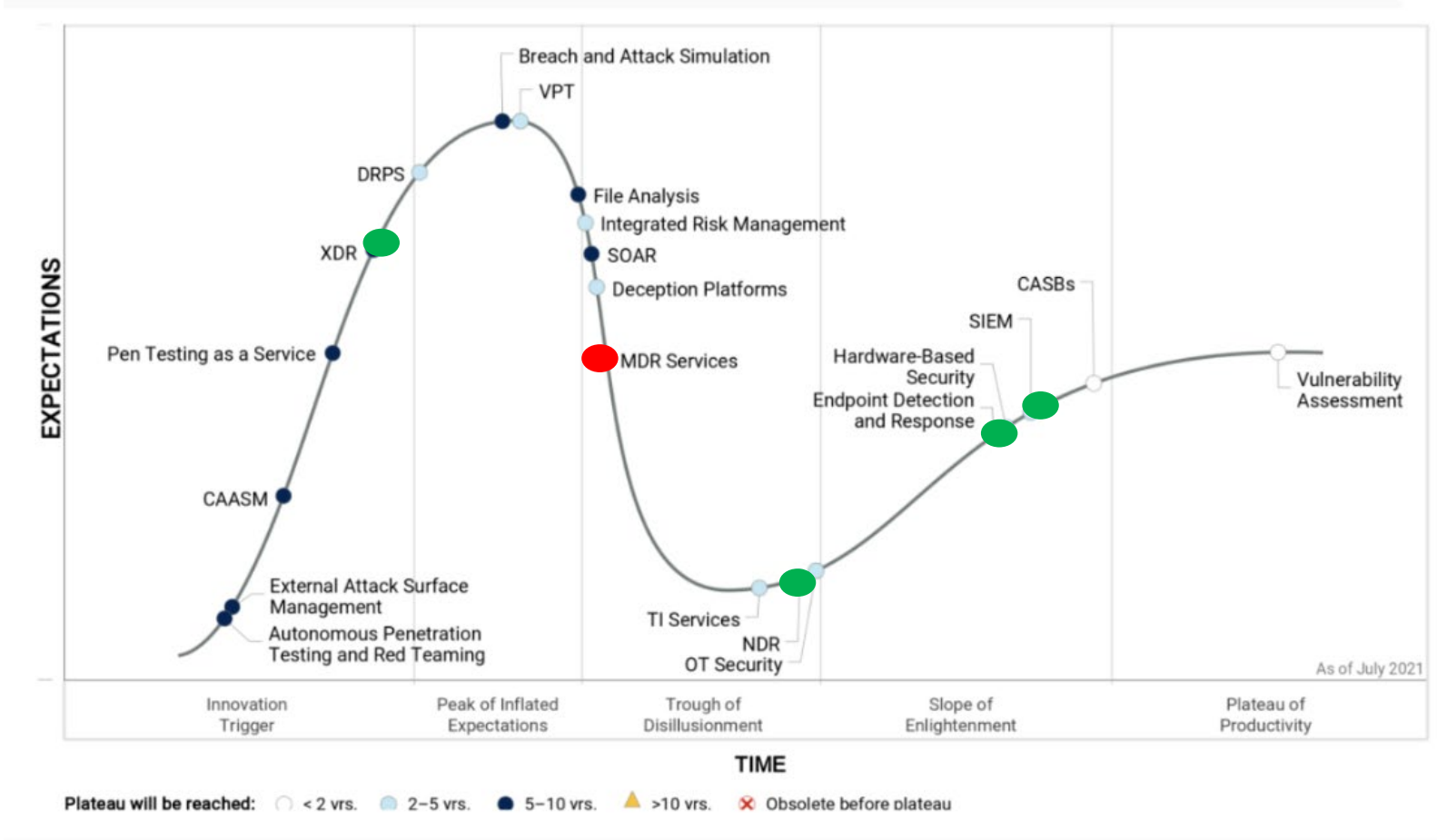


- **+ 60 %** des attaques ne sont pas liées à des logiciels malveillants
- Augmentation des exploitations de vulnérabilités critiques de type **"0-day"** et à large diffusion : Log4shell, Hafnium, PwnKit, Solarwinds
- **2 logiciels malveillants sur 3** restent sous le radar des anti-malware traditionnels
- Les solutions de sécurité traditionnelles se **focalisent sur les fichiers malicieux uniquement**
- Le mode « détection » ou « monitoring » uniquement **n'est plus suffisant**

© 2001-2022 APPROACH

Points essentiels à retenir

ACTION 3 : augmenter votre visibilité et automatisation

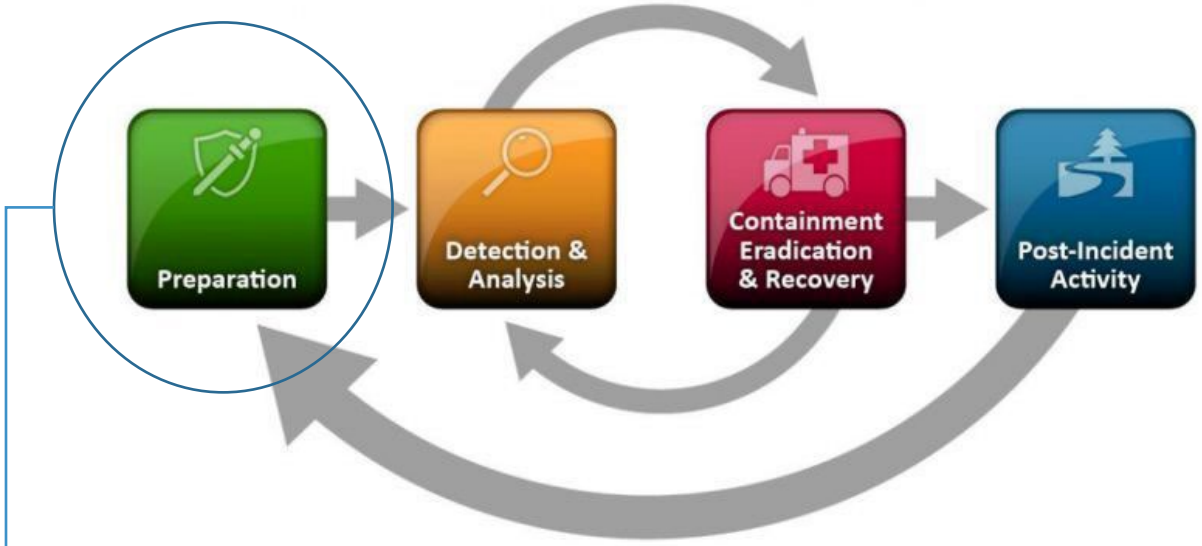


Source: Gartner Hype Cycle cyber ops 2021

© 2001-2022 APPROACH

Points essentiels à retenir

ACTION N°4 : Préparez-vous au pire



- Equipe de réponse
- Communication & Facilités
- Matériaux
- Documentation asset
- DRP et sauvegardes
- Playbooks

- Experts CSIRT
- Disponibilité 24/7
- SLA sur temps d'intervention

© 2001-2022 APPROACH

Résumé

Votre plan d’action :

- Faites évaluer votre surface d’attaque (régulièrement)
- Patchez vos systèmes de manière intelligente
- Activez le MFA sur tous vos comptes (utilisateur et à privilèges)
- Adoptez une solution MDR (SOC) pour garantir une couverture de surveillance complète et une réponse automatisée
- Documentez votre plan de réponse et souscrivez à un service d’expert de réponse aux incidents avec un SLA (à distance et sur site)

© 2001-2022 APPROACH

Conclusion

Ne jouez pas avec votre chance …

… ni aux apprentis sorciers !!!

Faites appel à des experts !!

© 2001-2022 APPROACH

Nos Services

How we can help

Consultance & Audit

Nous évaluons et conseillons avec pragmatisme & précision

Formation & Coaching

Un catalogue complet de formations et de certifications

Technologie Design & Build

Sélectionner, fournir, intégrer et déployer la meilleure technologie

Managed Security Services

Grâce à notre Security Operations Centre (SOC)

© 2001-2022 APPROACH

Merci !

APPROACH

Approach Belgium – Louvain-la-Neuve, Antwerp

EYRApproach Switzerland – Lausanne, Geneva, Zürich, Neuchâtel

+32 10 83 21 11 sales@approach.be www.approach.be Linkedin

ISO 27001 INFORMATION SECURITY MANAGEMENT VINÇOTTE

ISO 27701 PRIVACY INFORMATION MANAGEMENT VINÇOTTE

CYBERSECURITY MADE IN EUROPE

DIENSTVERLENER VOOR DE KMO-PORTEFEUILLE
Registratienummer DV.A237804

BRUSSELS ECONOMY AND EMPLOYMENT
BRUSSELS REGIONAL PUBLIC SERVICE

Chèques-entreprises

© 2001-2022 APPROACH