KEYSIGHT

# Attack yourself before the hackers do !

## Vérifier l’efficacité de vos dispositifs de sécurité en production …

EMEA
cyrille.vassant@keysight.com
5 Octobre 2023

Threat Simulator

Breach and Attack Simulation, Automated Red-teaming

KEYSIGHT

# Qui sommes-nous ?

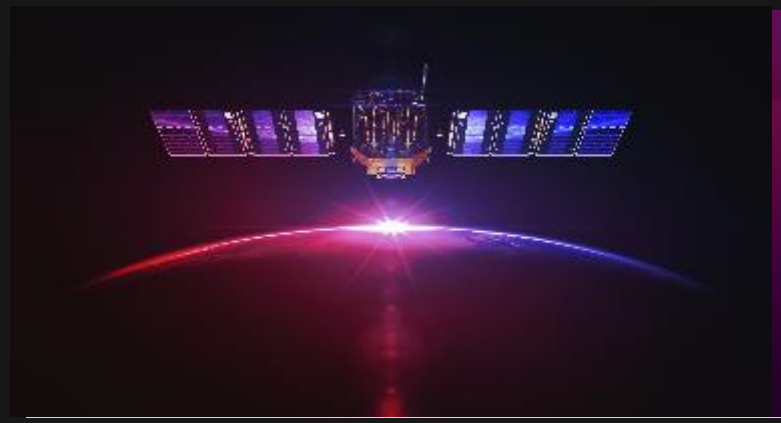
**La plus importante société de test & mesure au monde**

- C.A $5.42bn (2022)
- 32k clients
- 14k employés

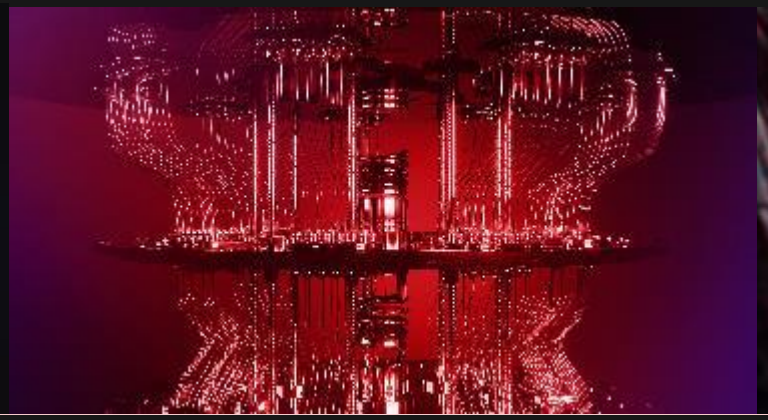
KEYSIGHT

# Keysight fournit des outils de test et de mesure dans de nombreux domaines qui seront votre quotidien de demain

Software for NASA

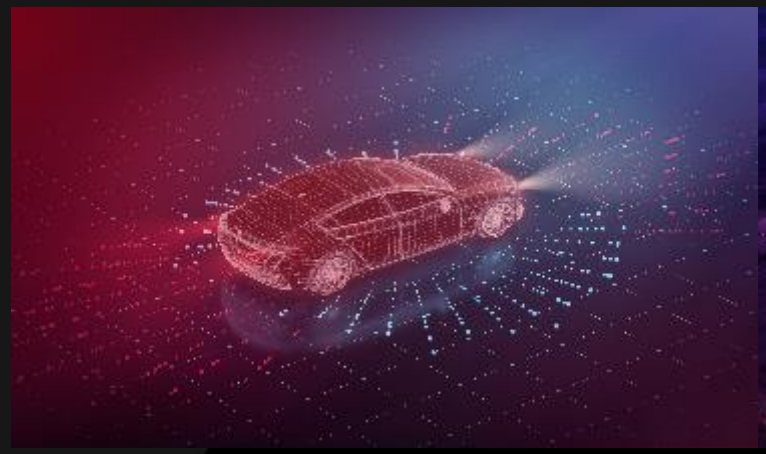


Quantum Computing



5G and 6G

Autonomous vehicles



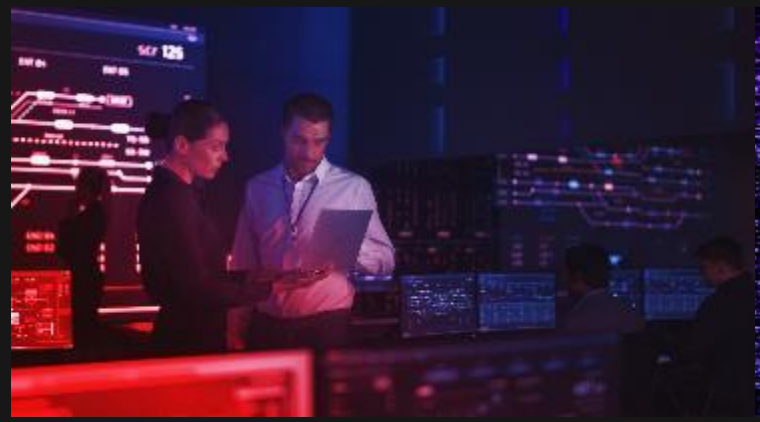
Industrial IoT

Digital systems in hospitals

KEYSIGHT

**+ 20 ans d’expérience dans les réseaux**
**+ 10 ans dans la cybersécurité auprès des R&D de Contructeurs/Editeurs de solutions de Sécurité**

## Visibilité des réseaux



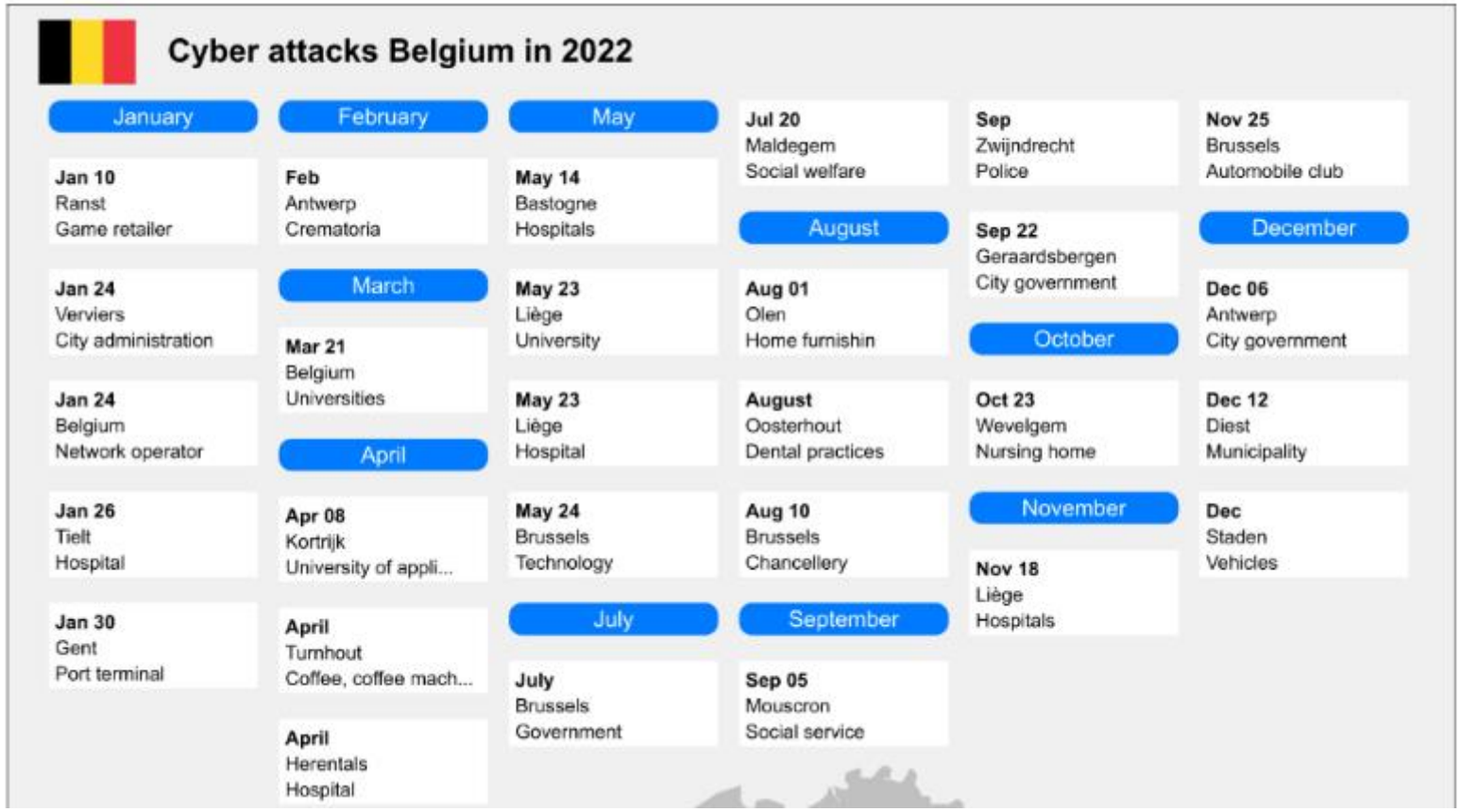
## Tests réseaux / cybersécurité

## Sécurité de l’IoT

## Simulation d’attaques

# Les problèmes/coûts Cyber ne cessent d'augmenter !!!

Comment éviter au maximum de faire la Une des journaux ?




*Credits: KonBriefing Research*

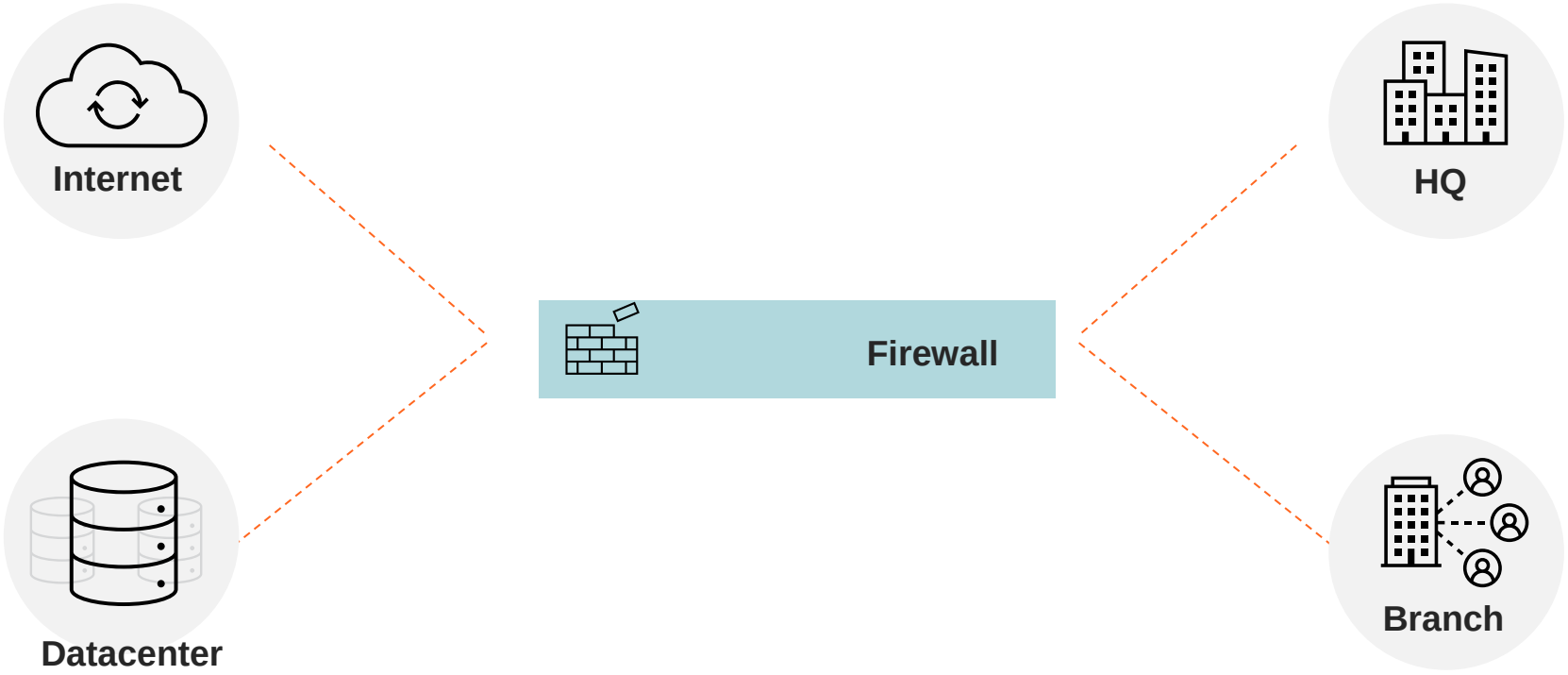

Vous avez une chance sur 8.000 d'être victime d'un incendie, **une chance sur cinq de subir une cyberattaque**.
Pourtant, **38% des entreprises belges** ne disposent d'encore aucune stratégie de sécurité active ? *Rapport de Proximus 2022*

21/08/2023 – **Le Centre Public d'Action Sociale (CPAS) de Charleroi** (BEL).
*Ce lundi 21 août, les services informatiques du CPAS carolo ont été victimes d'une cyberattaque, paralysant complètement le site*


CYBER SCAPE
2023
Network & Infrastructure Security
Advanced Threat Protection
NAC
SDN
DDoS Protection
DNS Security
Network Firewall
SASE
Deception
ICS + OT
Network Analysis & Forensics
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Data Centric Security
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Risk Quantification
Pen Testing & Breach Simulation
Security Ops & Incident Response
SIEM
Security Incident Response
Security Analytics
Momentum CYBER
Threat Intelligence
IoT
IoT Devices
Connected Home
Messaging Security
Digital Risk Management
Security Consulting & Services
Blockchain
Fraud & Transaction Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Cloud Security
Container
Infrastructure
CASB
Le problème n’est peut-être pas aussi simple !!!

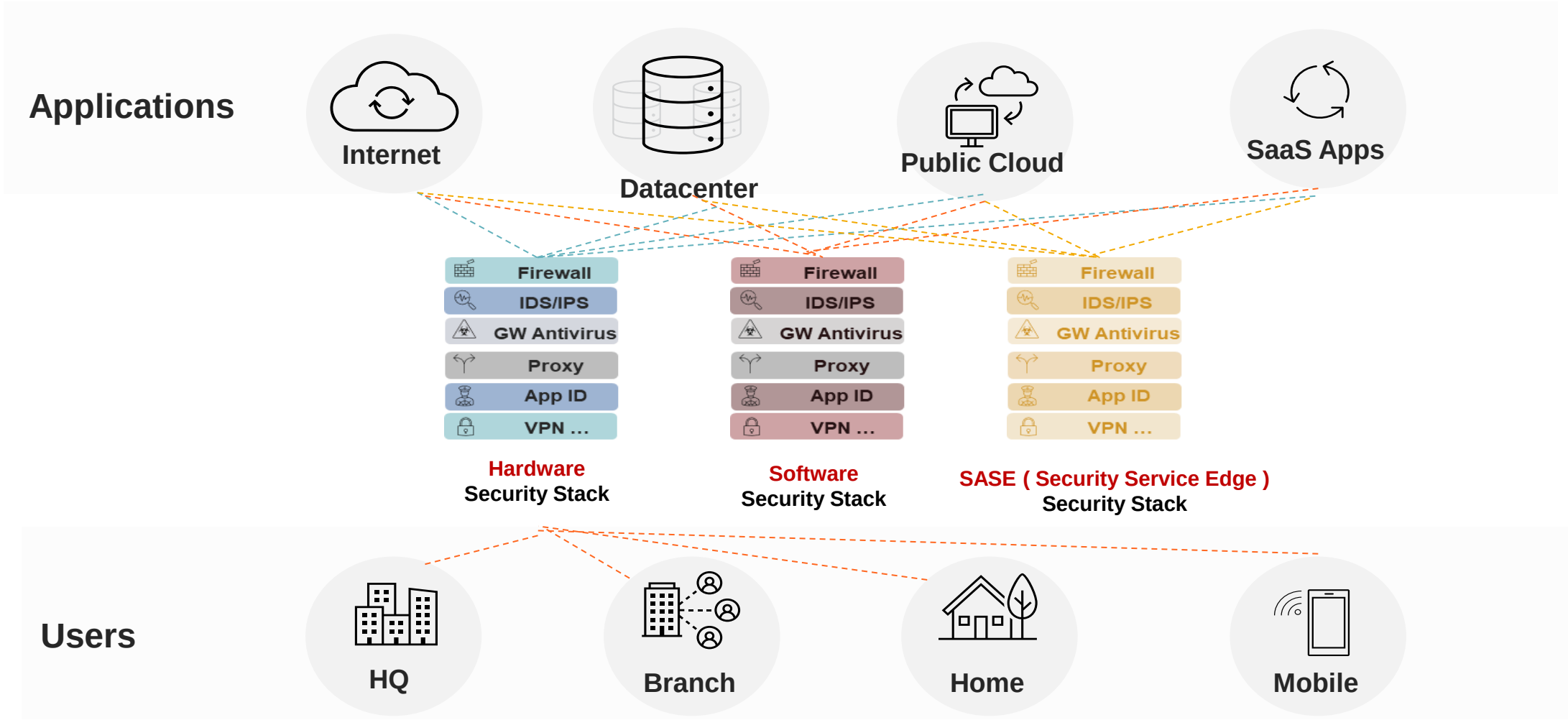
# L’évolution de la sécurité des réseaux :

## Au commencement , une sécurité centralisée avec des “firewall”




La digitalisation des entreprises  apporte ses bénéfices et la nécessite d’adapter son approche de la sécurité IT …

# **Aujourd'hui :** L'approche de la sécurité devient hybride et hétérogène avec l'essor de la DIGITALISATION des services qui peuvent s'exécuter en local &/ou en remote



KEYSIGHT

People
Process
Technology..

# ..ne sont jamais parfait tout le temps


Complexité Accrue

Environnement Dynamique

Une combinatoire qui peut laisser perplexe

**Find it before they do !.**

# Votre quotidien :
# Les Compétences - L'expertise Cyber - La Gouverance

1. **Pénurie** de compétences IT en Cyber Sécurité
2. Comportement de **l'utilisateur**
3. **Exceptions** à la politique de sécurité « temporaires » ou « poussées par les métiers ».
4. Menaces émergentes
5. Menaces internes
6. Mauvaise **configuration**

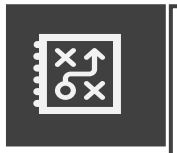

LACUNES DANS VOTRE COUVERTURE

« Un certain type d'attaque peut-il entrer ? »

MAUVAISES CONFIGURATIONS

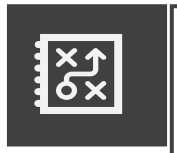
« Tous mes outils fonctionnent-ils correctement? »

# Les hypothèses qui vous rassurent … ???



## SUPPOSITION #1

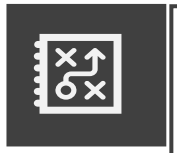
Les outils de sécurité font tout ce qu'il faut !



## SUPPOSITION #2

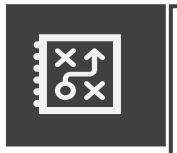
Les produits sont déployés correctement.

Set & Forget !



## SUPPOSITION #3

Les équipes de Dev et les équipes de Prod font confiance à la revue de code. DevSecOps



## SUPPOSITION #4

Le test d'intrusion fait une fois par an est suffisant pour sécuriser tous les réseaux.

## SUPPOSITION #5

Les scans de sécurité suffisent à prévenir les attaques ( patch virtuels ).

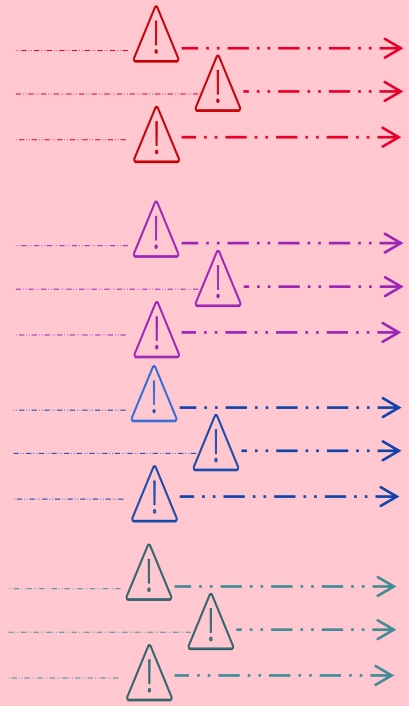
## SUPPOSITION #6

Les équipes SecOps sauront rapidement s'il y a eu une intrusion.

Sommes-nous aussi confiant ….

# La confiance n’exclut pas le contrôle

**Mise en place d’un “SOC” ou sous-traitance à travers un Service Managé**

| Enterprise Security Tools | Security Alerts | SOC Team | SOC Goals |
|---|---|---|---|
| Network<br>Endpoint<br>Cloud<br>Email, … |  |  <br>E.g: Microsoft Cyber Defense Operations Center operates 24×7 to defend against cyberthreats | Alert Prioritization<br>Investigation & Response<br>Threat Hunting |

# Un début de réponse pour minimiser le “Detect & Respond”


## 1 - Identify

- Risk assessments
- Business context modeling

## 2 - Protect

- Training
- Antivirus (AV)
- Firewalls (NGFW)
- Intrusion Prevention Systems (IPS)
- Endpoint Detection and Response (EDR)
- Web Application Firewalls (WAF)
- …..

## 3 - Detect

- SIEMs
- Intrusion Detection Systems
- Network Detection and Response
- Endpoint Detection and Response
- MITRE ATT&CK framework

## 4 - Respond

- Security Operations Center (SOC) teams
- Blue Teams

## 5 - Recover

- Backup and Restore
- Incident Response Planning
- Gap analysis and risk scoring
- Reporting

**Approche Pro-Active & Préventive**

« **Valider/Tester** » - **P**eople , **P**rocess & **T**echnology

What If ? Scenarios de tests – ( Before Hackers Find It For You ! )

# L’ Approche “Pro-Active”

**Nous pouvons vous aider à anticiper**

1. Développer un protocole utilisable en production permettant aux clients d'évaluer leur niveau de résistance face aux menaces.

2. Via des transactions « End To End »  pour traverser les couches de sécurité  .

3. Reproduire les routes et les « Behaviour » incluant le poste de travail .
   - Ext → Int
   - Int → Ext
   - Int → Int

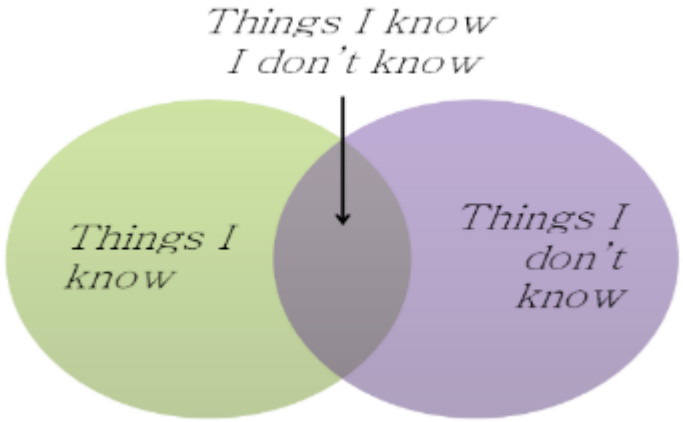
4. Proposer  des recommandations :
   1. - Bonne pratique
   2. - Recommandation Editeurs

*Vision de l’assaillant*

*Posture de défense*

KEYSIGHT

# Une démarche Pro-Active “Ready To Use” :




## Notre proposition de Valeur

**Simuler en toute sécurité des scénarios de cyberattaques**

**Évaluer avec précision votre niveau de sécurité**

**Améliorer votre posture de sécurité**

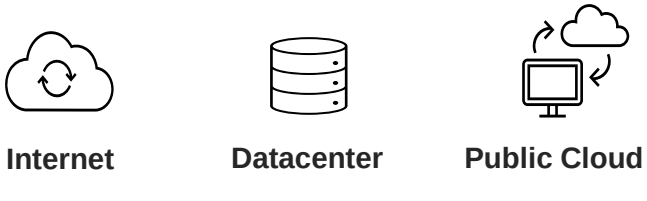
Si vous ne pouvez pas le **mesurer**, vous ne pouvez pas **l'améliorer**.
*Kelvin. Physicien, Scientifique (1824 - 1907)*

***Comment mesurer son niveau de sécurité IT ?***

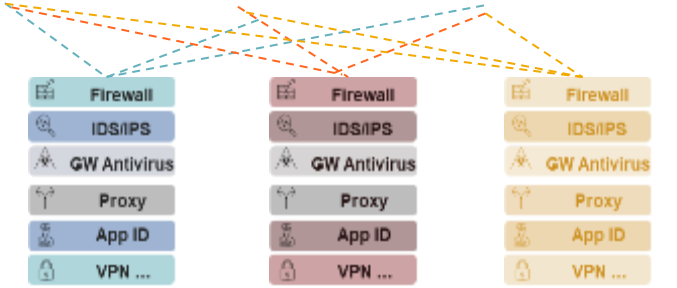
# Les vecteurs d'attaque

## Network Security

Applications



Internet Datacenter Public Cloud




**Hardware** Security Stack | **Software** Security Stack | **SASE** Security Stack

Users

HQ Branch Home

## Endpoint Security


## Email Security

Gmail

Office 365

## SecOps

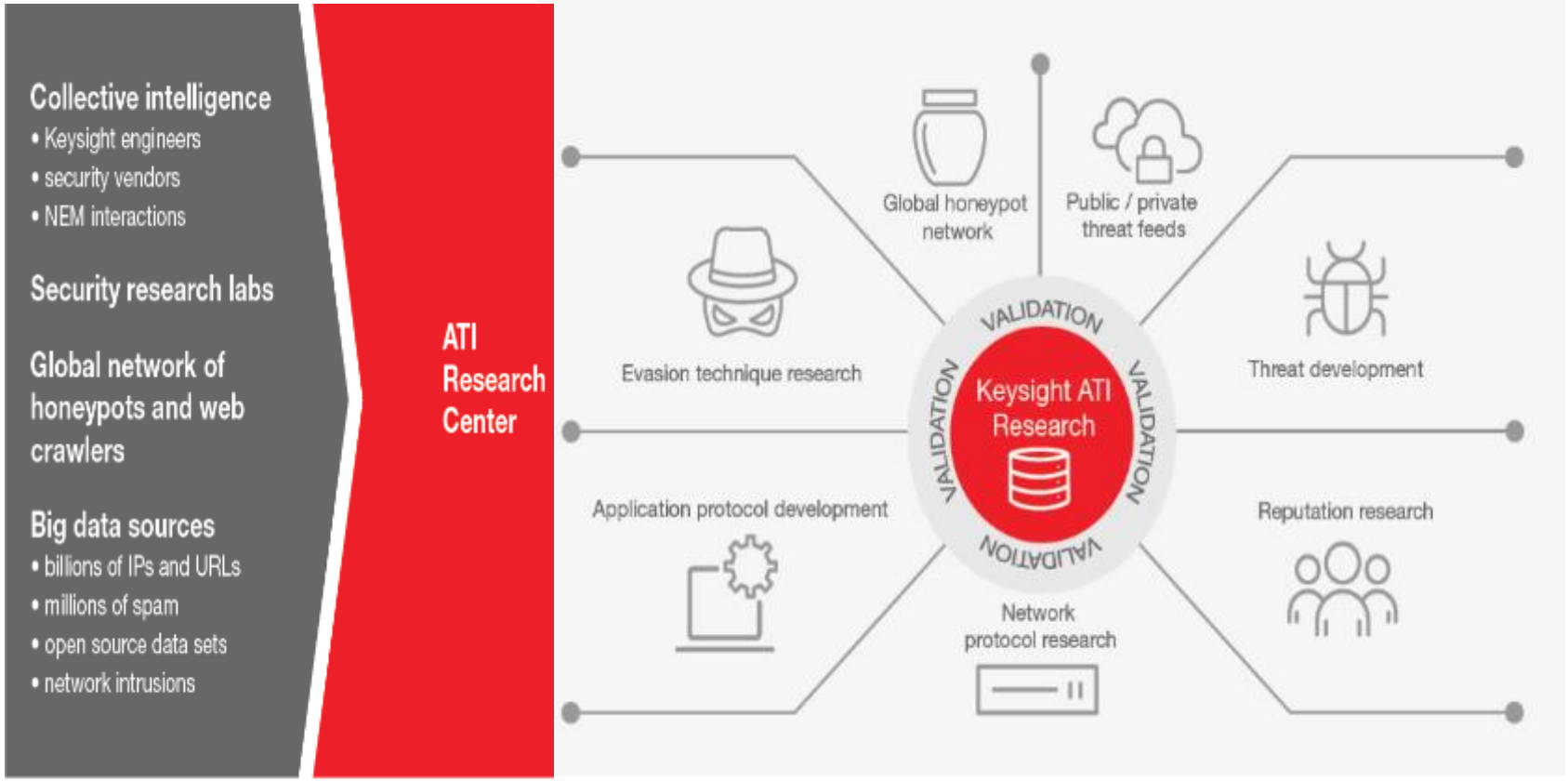

SIEM

*FW, IPS/IDS, DLP, Url filtering , . . .*

*HIDS/HIPS, AV, EPP, EDR, . . .*

# Application And Threat Intelligence (ATI)

## Keysight's Research Center




**Trusted library of attacks**

- 7000+ live security attacks, 41000+ malware techniques, 100+ evasions
- DDoS, botnet, APT simulations

**Leading source of known threats**

- Curated set of proprietary, opensource, commercial datasets
- Billions of IPs, URLs
- Millions of SPAM records

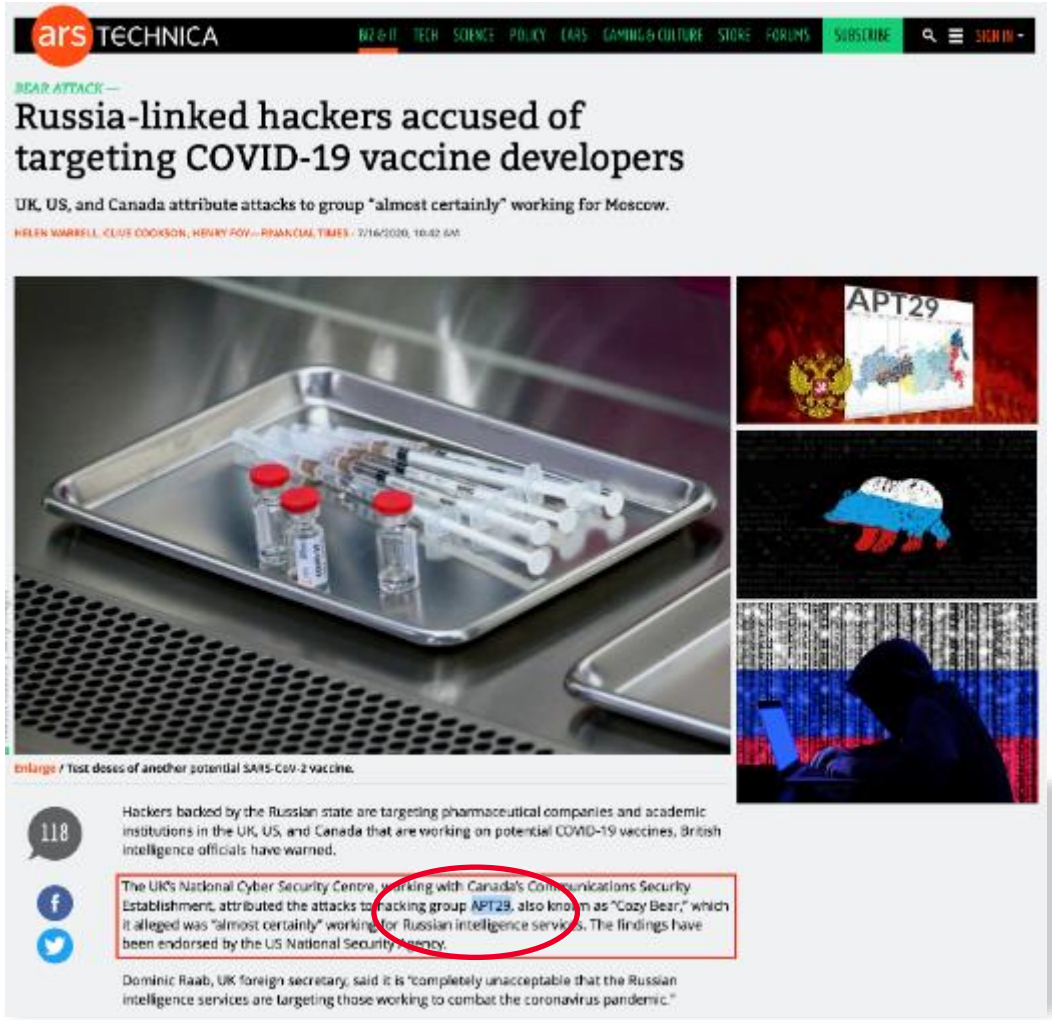
**Our work is never finished**

- Continuously updated, global network of honeypots, web crawlers and security research labs

# Adversary Emulation – APT29 / CozyBear / CozyCar

## Adversary Emulation

*"A type of Red Team engagement that mimics a known threat to an organization by blending in threat intelligence to define what actions and behaviors the red team uses".*
***– MITRE***



# Adversary Emulation Plan – APT29 / CozyBear / CozyCar

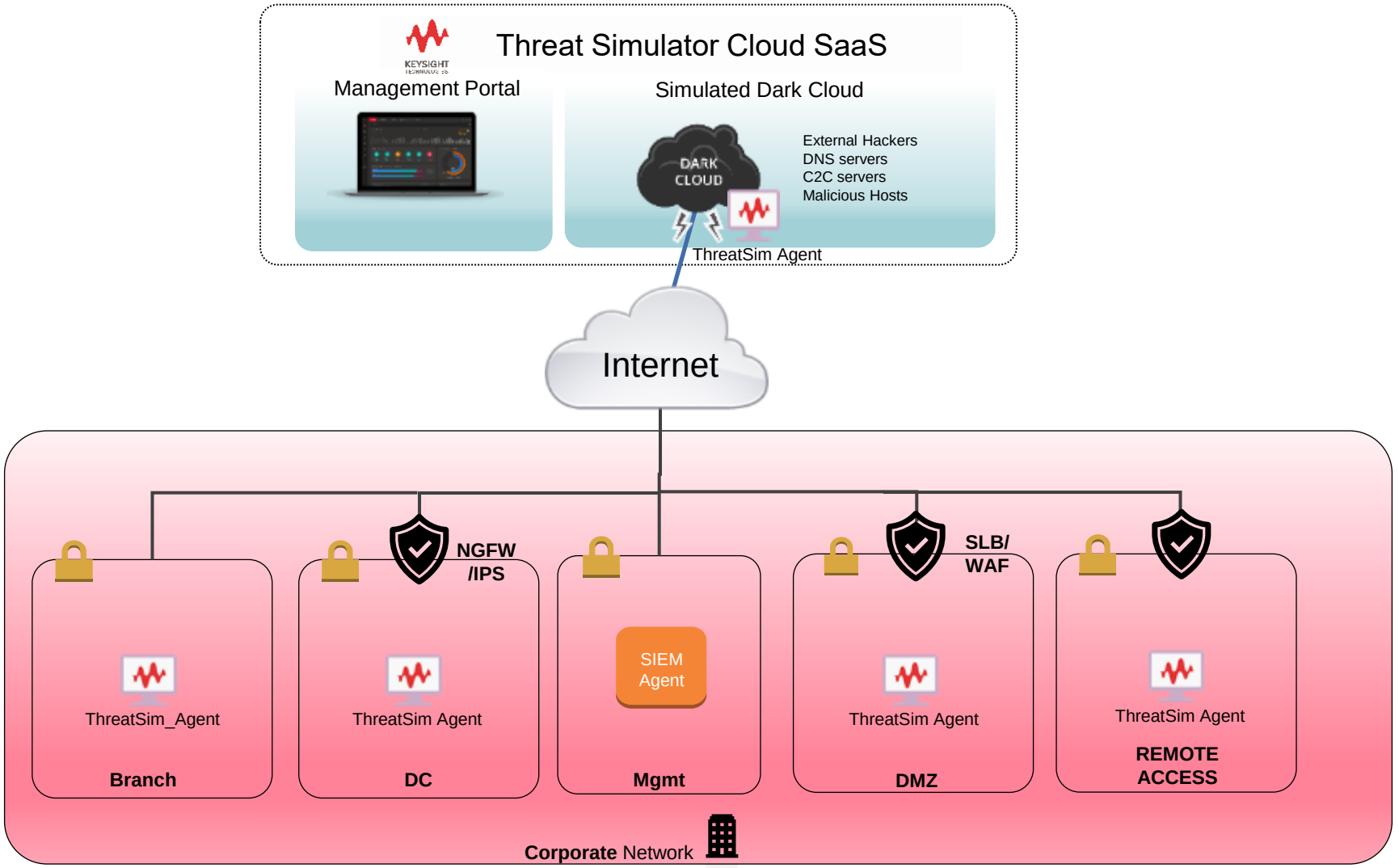
Threat Intelligence Acquisition → Extract Actionable Techniques → Develop tools → Setup Infrastructure → Emulate Adversary (APT29)

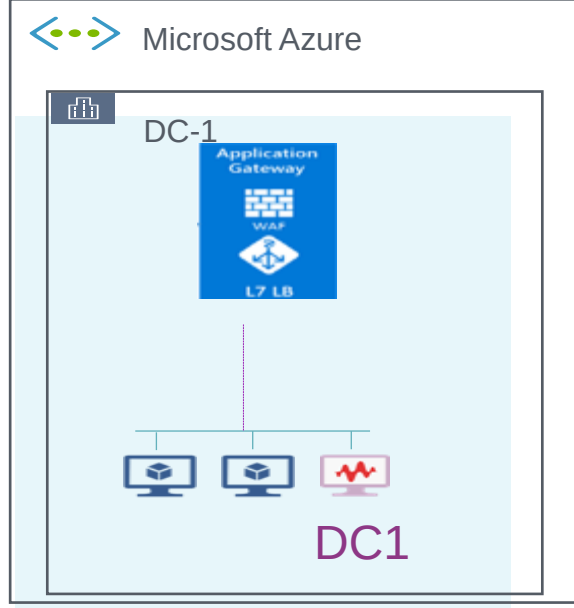

cuckoo

- Malware detonation
- IoCs collection


| # | Assessment | Category | Agents | Audits |
|---|---|---|---|---|
| 1 | APT-29 July 2020 SoreFang Campaign | | | 3 |
| 2 | APT-29 Sep 2020 WellMess Campaign | | | 3 |
| 3 | Endpoint - G0016: APT29 (macos) | | | 11 |
| 4 | Endpoint - G0016: APT29 (windows) | | | 803 |

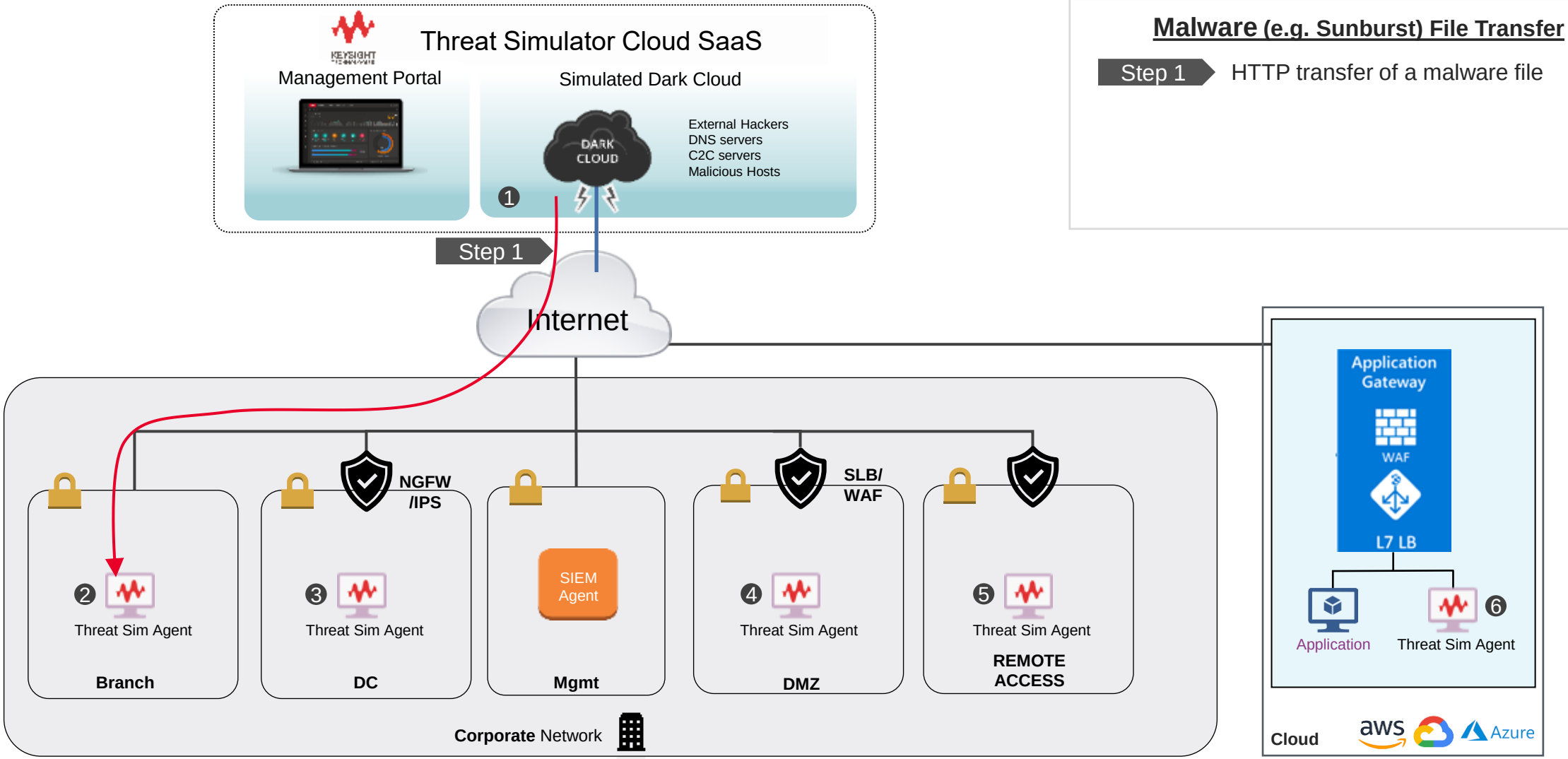
# Exemple d’architecture



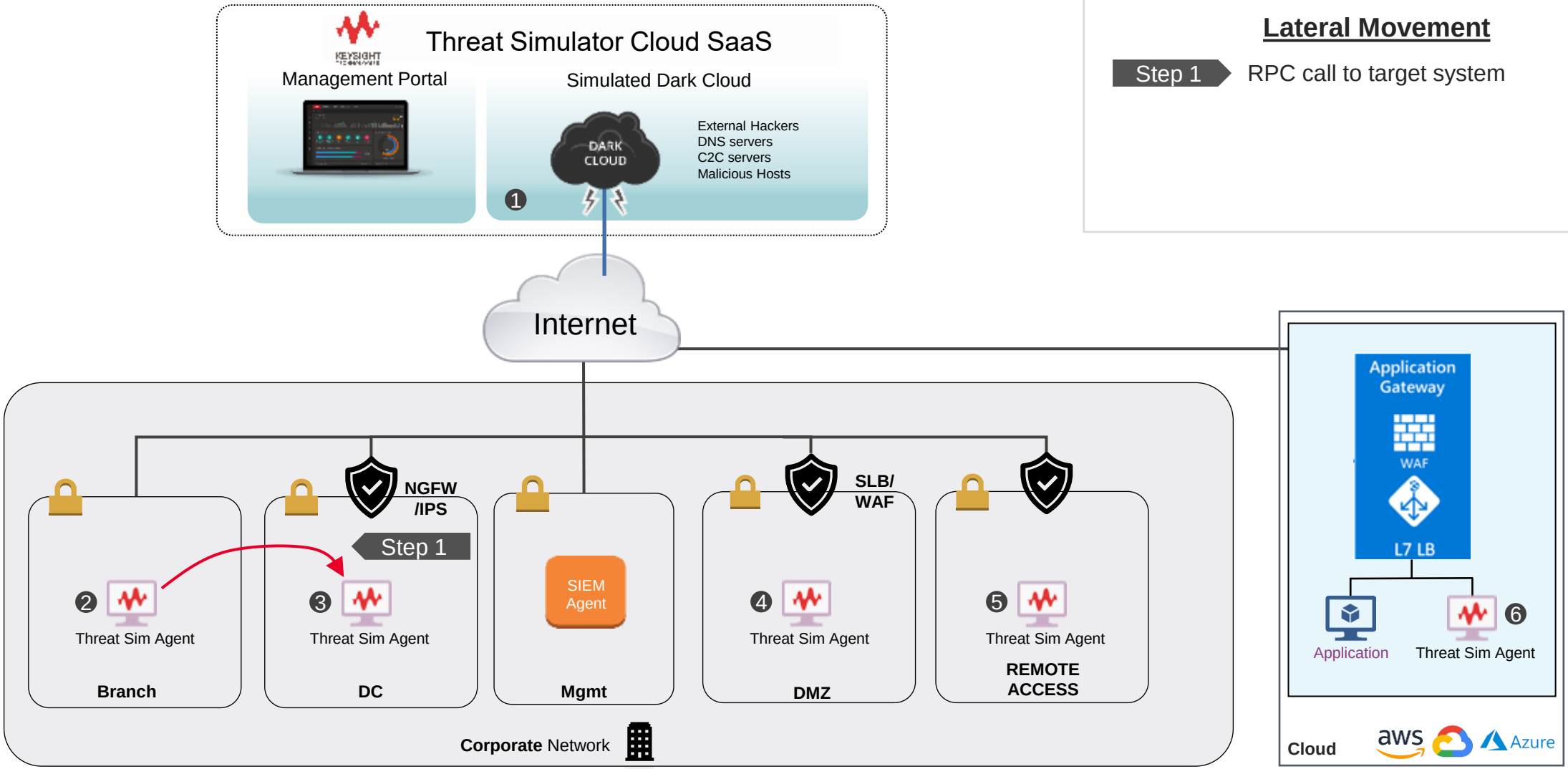

## Malware (e.g. Sunburst) File Transfer

Step 1 HTTP transfer of a malware file




Les assessments **MALWARE** sont conçus pour tester les contrôles de sécurité mis en place afin de prévenir le téléchargement de logiciels malveillants via HTTP(S).

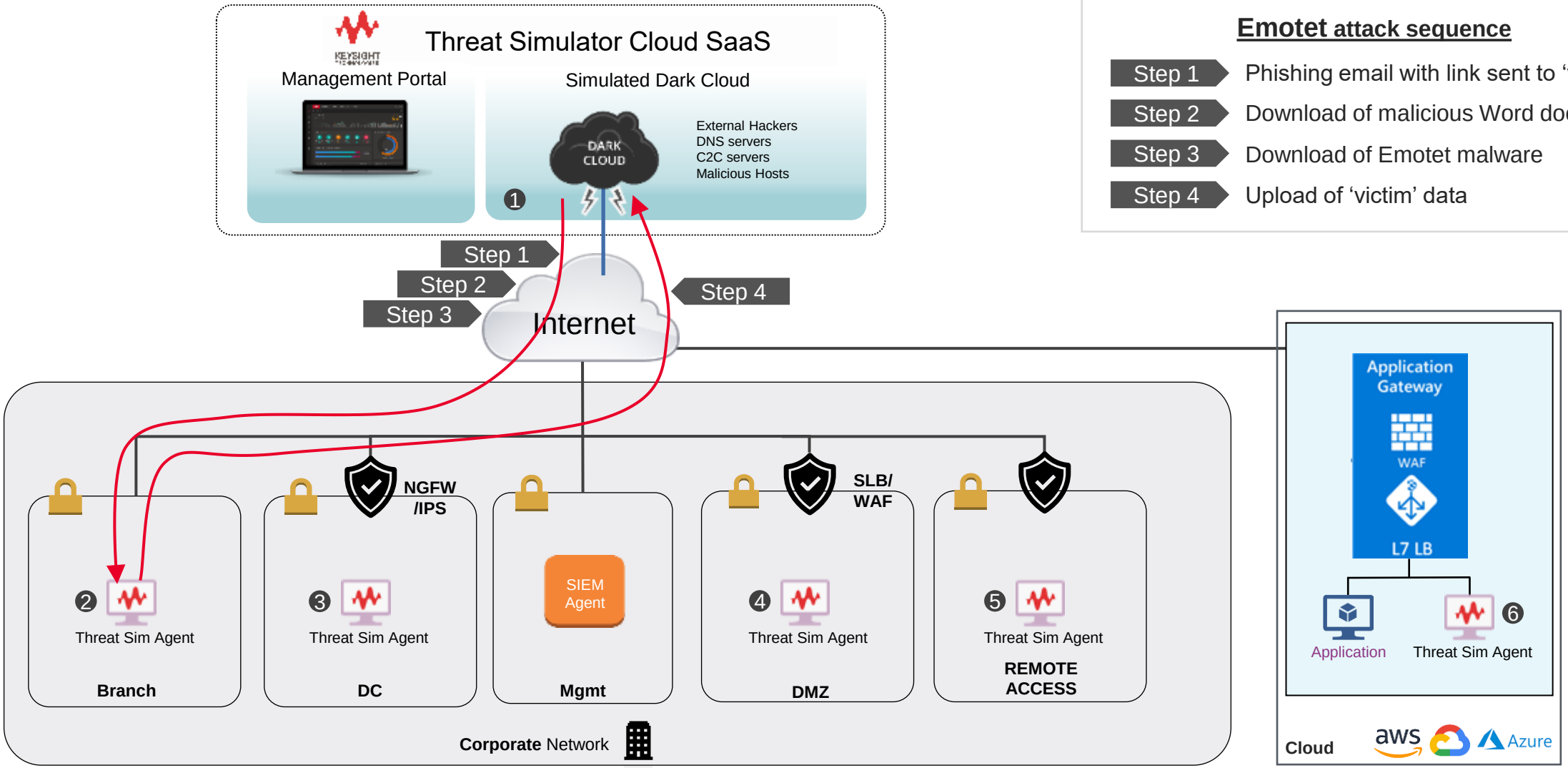
Tels que Sunburst (utilisé par SolarWinds), Darkside, Hafnium, Maze, CLOP, Ryuk, Revil, BotenaGo, etc.




## Lateral Movement

Step 1 RPC call to target system

**Mouvement Lateral** : L'attaquant lance une attaque depuis l'intérieur de votre réseau. Ces attaques ciblent des systèmes qui ne peuvent être exploités que par un attaquant se trouvant dans le réseau.Il peut-être utilisé pour faire des escalades de privilège une fois rentré dans le SI de la victime.




## Emotet attack sequence

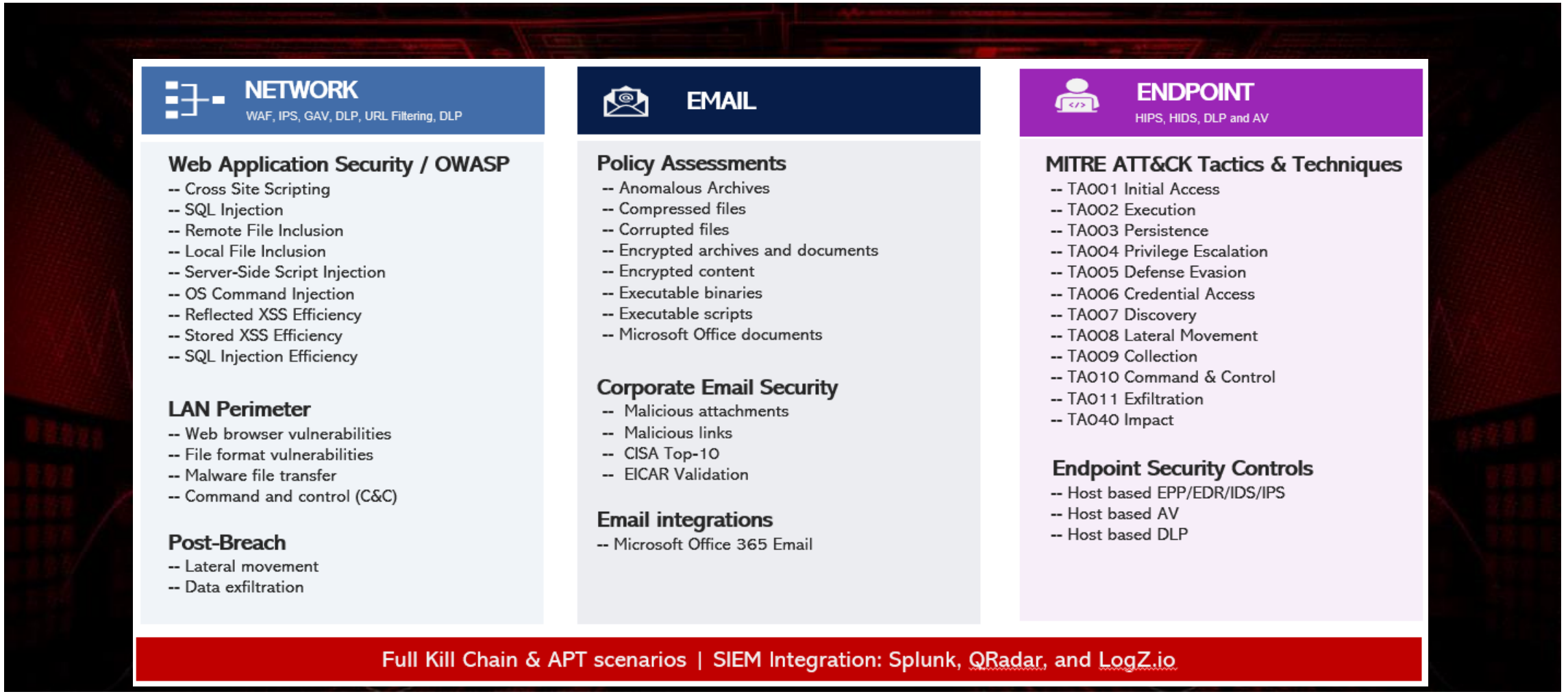
- Step 1 — Phishing email with link sent to ‘victim’
- Step 2 — Download of malicious Word document
- Step 3 — Download of Emotet malware
- Step 4 — Upload of ‘victim’ data

**Emotet** exemple d’un cheval de troie plus avancé dont le vecteur initial d’attaque est via un phishing email qui permet de récuperer ensuite un fichier dont l’objectif est de voler vos identifiants ( Email/User/pwd ) ..

# La bibliothèque prête à l'usage

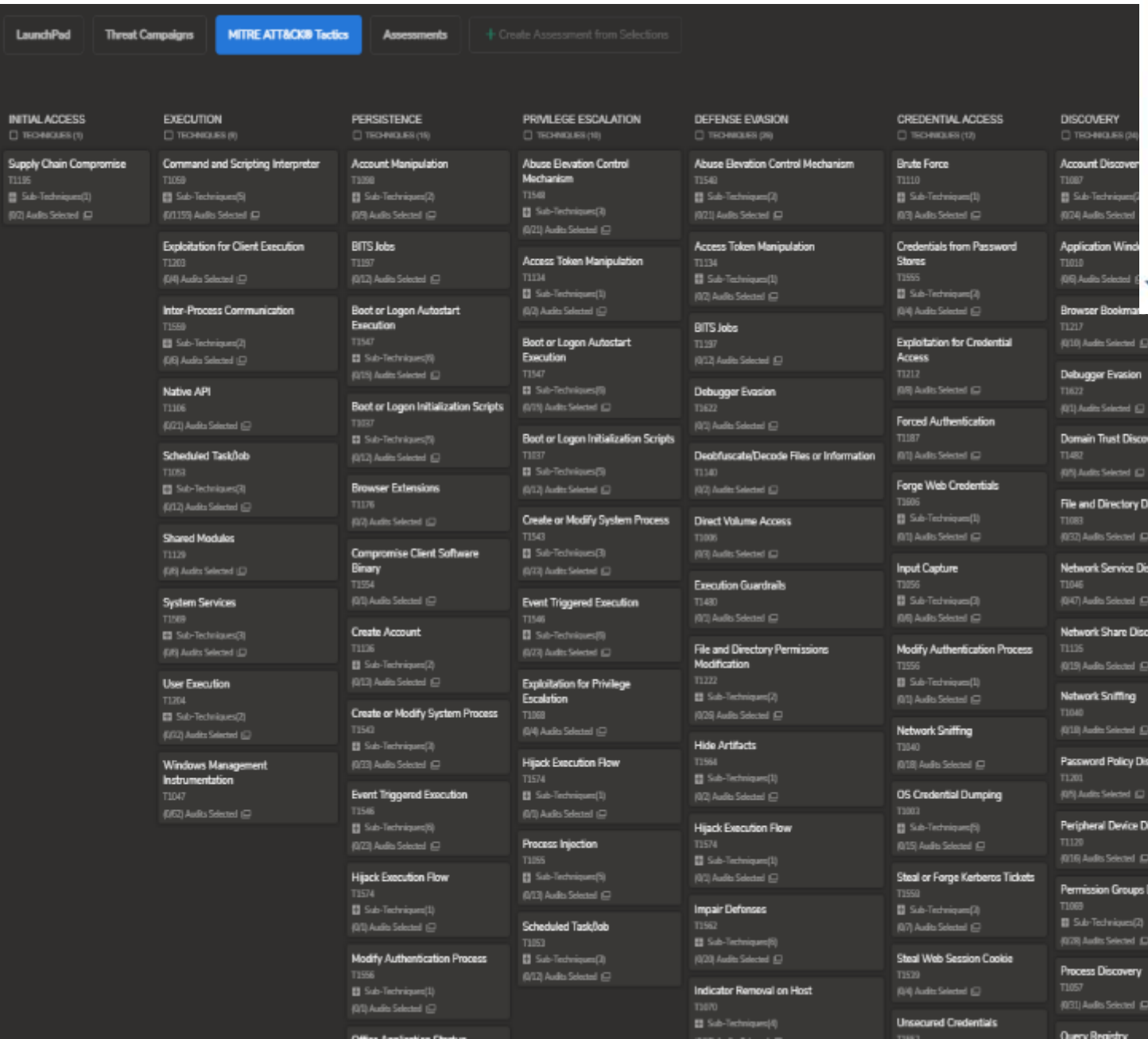
**Red (Attack) and Blue (Defense)**

**Les attaques sont à l'image de celles des hackers**



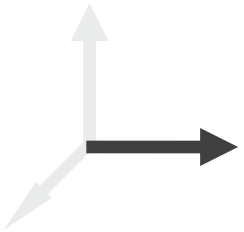

*Les attaques et les récommandations sont mises à jour régulierement*

# Assessments vision MITRE ATT&CK



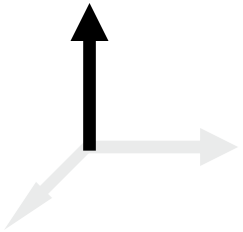
# Quelques cas d’usage

**De la PME aux Services Managés**



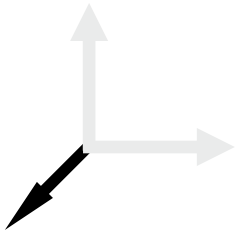
## Taille

How large is the network?
# of sites/security zones?



## Fréquence

How often will you test?
Daily, weekly, monthly?



## Périmètre

Network, Endpoint, and/or
Email testing?

**Modèle Flexible –**

Accompagner votre niveau de Maturité qui va grandir dans le temps

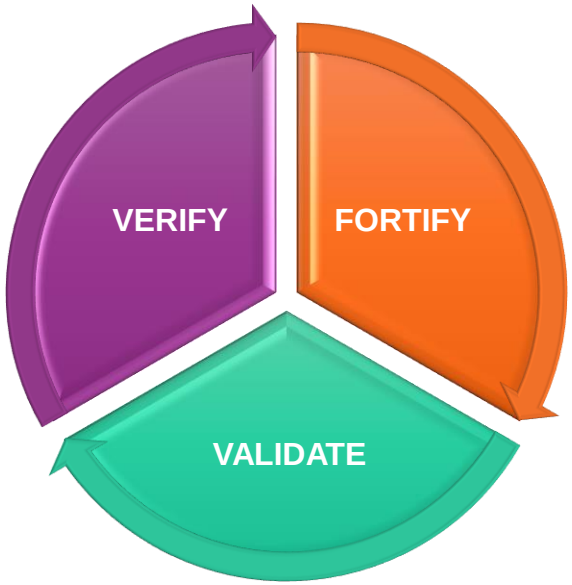
1. Usage Ponctuel
   - Audit / Mise en Production
2. Usage Mensuel
   - Contrôle tournant depuis les # zones
3. Usage Continu
   - Automatisation ( KPI )
     - Bloqué / Détecté
   - Durcissement des règles de detection

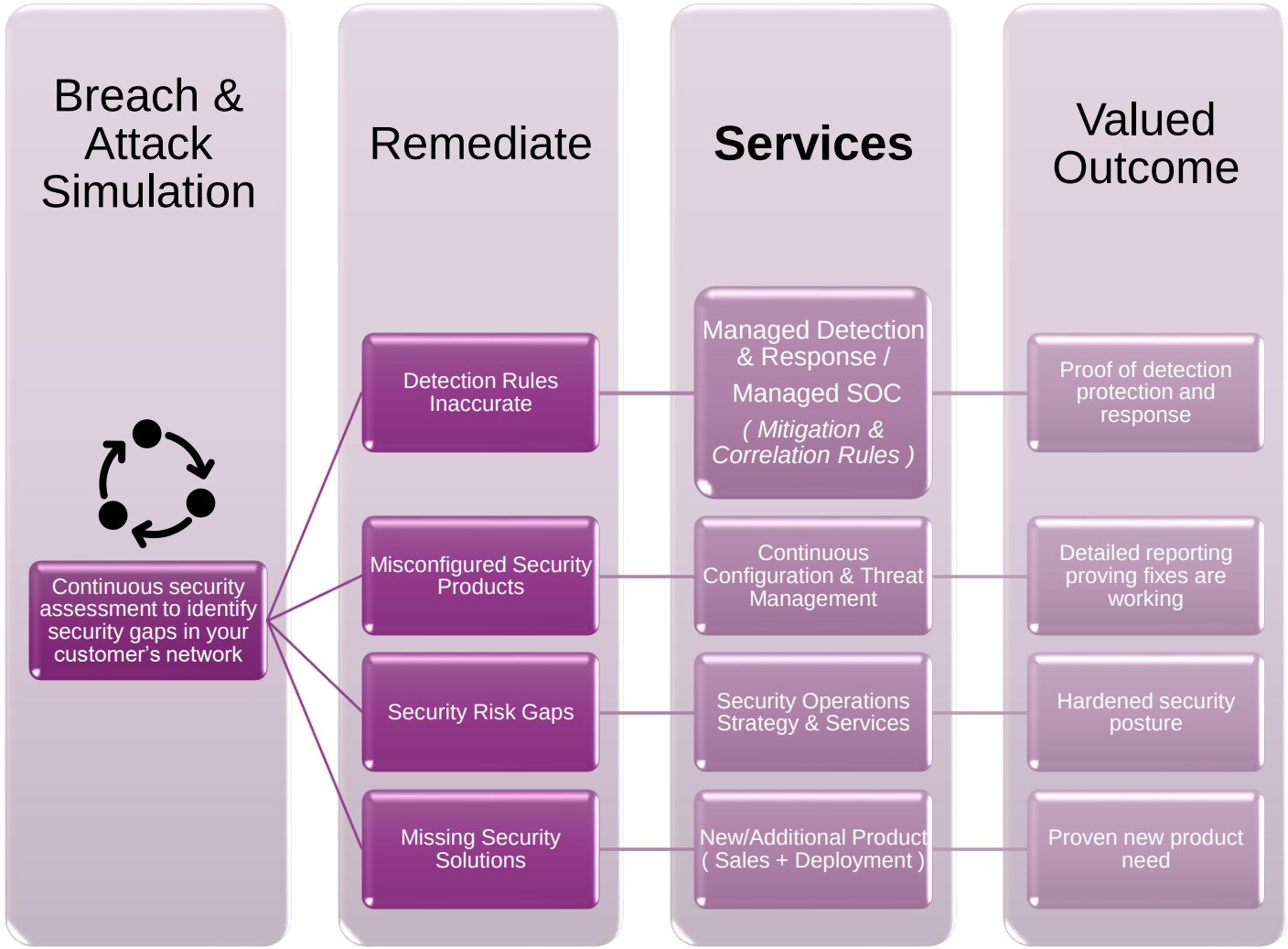
# Threat Simulator

## ADDITIONAL SERVICES AND PRODUCTS

***A Safe Offense***
**To check if tools you already have are actually protecting you !**

**Like an automated Virtual "Red Team"**



# MSSP Use Cases

## Compléte le catalogue des services MSSP

### UBV avec une nouvelle offre de service

- Identifier de manière proactive les dérives du niveau de protection grâce à une validation continue
- Identifier rapidement votre posture face aux dernières menaces
- « Cyber Range » en Production

### Maintenir son SOC à un niveau de robustesse maximal

- Formation & développement des compétences
- Utiliser nos IOC's pour chasser les menaces
- Optimiser les outils et les process
- Gestion des changements

**Threat Simulator**

KEYSIGHT

### Tuner & Améliorer votre portefeuille existant

Challenger vos Servcies Managés:

- IDS / IPS / DLP
- Firewall / WAF
- EDR / Email Gateway

### Augmenter votre capacité à délivrer des services

Optimiser & Enrichir :

- Pen test
- Red teaming
- Audits
- Projets de migrations

# RAPPORTS DE MATURITÉ DE SECURITÉ

EXECUTIVE REPORTS, SCENARIO (DETAILED REPORTS), RECOMMENDATIONS REPORTS

## AVANT OPTIMISATION

**Identifier** et **Corriger** les failles

### EXECUTIVE REPORT

KEYSIGHT TECHNOLOGIES

#### OVERALL NETWORK SECURITY


#### SECURITY SCORES BY LOCATION (SORTED BY PREVENTION SCORE)

| LOCATION | PREVENTION SCORE | DETECTION SCORE | AUDITS RUN | AGENTS ASSESSED | LAST 7-DAYS PREVENTION MIN/AVG/MAX | LAST 7-DAYS DETECTION MIN/AVG/MAX |
|---|---|---|---|---|---|---|
| Branch-Austin | 15% | 75% | 200 | 1 | 15% 15% 15% | 75% 75% 75% |
| Branch-London | 15% | 75% | 200 | 1 | 15% 15% 15% | 75% 75% 75% |
| Branch-Singapore | 15% | 75% | 200 | 1 | 15% 15% 15% | 75% 75% 75% |
| AWS-DC | 70% | 83% | 600 | 1 | 70% 70% 70% | 83% 83% 83% |
| Azure-DC | 80% | 83% | 600 | 1 | 80% 80% 80% | 83% 83% 83% |

#### SECURITY SCORES BY SCENARIO(SORTED BY PREVENTION SCORE)

| SCENARIO NAME | PREVENTION SCORE | DETECTION SCORE | AUDITS RUN | AGENTS ASSESSED | LAST 7-DAYS PREVENTION MIN/AVG/MAX | LAST 7-DAYS DETECTION MIN/AVG/MAX |
|---|---|---|---|---|---|---|
| Branch-CISA-Top-10 Exploits | 0% | 86% | 21 | 1 | 0% 0% 0% | 86% 86% 86% |
| Branch-CISA-Top-10-Malware | 9% | 91% | 33 | 1 | 9% 9% 9% | 91% 91% 91% |
| Branch-Top-File-Vulnerabilities | 11% | 74% | 270 | 1 | 11% 11% 11% | 74% 74% 74% |
| Branch-Email-Attachments-Policy | 11% | 89% | 111 | 1 | 11% 11% 11% | 89% 89% 89% |
| Branch-Web-Gateway-Protection | 22% | 96% | 81 | 1 | 22% 22% 22% | 96% 96% 96% |
| Branch-Data-Exfiltration | 32% | 29% | 84 | 1 | 32% 32% 32% | 29% 29% 29% |
| Datacenters-OWASP-Top10 | 75% | 83% | 1200 | 1 | 75% 75% 75% | 83% 83% 83% |

## APRES OPTIMISATION

**Automatiser** et **Mesurer** les dérives

### EXECUTIVE REPORT

KEYSIGHT TECHNOLOGIES

#### OVERALL NETWORK SECURITY


#### SECURITY SCORES BY LOCATION (SORTED BY PREVENTION SCORE)

| LOCATION | PREVENTION SCORE | DETECTION SCORE | AUDITS RUN | AGENTS ASSESSED | LAST 7-DAYS PREVENTION MIN/AVG/MAX | LAST 7-DAYS DETECTION MIN/AVG/MAX |
|---|---|---|---|---|---|---|
| Branch-Austin | 85% | 85% | 200 | 1 | 15% 29% 85% | 75% 77% 85% |
| Branch-London | 85% | 85% | 200 | 1 | 15% 29% 85% | 75% 77% 85% |
| Branch-Singapore | 85% | 85% | 200 | 1 | 15% 29% 85% | 75% 77% 85% |
| AWS-DC | 100% | 100% | 600 | 1 | 70% 76% 100% | 83% 86% 100% |
| Azure-DC | 100% | 100% | 600 | 1 | 80% 84% 100% | 83% 86% 100% |

#### SECURITY SCORES BY SCENARIO(SORTED BY PREVENTION SCORE)

| SCENARIO NAME | PREVENTION SCORE | DETECTION SCORE | AUDITS RUN | AGENTS ASSESSED | LAST 7-DAYS PREVENTION MIN/AVG/MAX | LAST 7-DAYS DETECTION MIN/AVG/MAX |
|---|---|---|---|---|---|---|
| Branch-CISA-Top-10 Exploits | 71% | 71% | 21 | 1 | 0% 14% 71% | 71% 83% 86% |
| Branch-CISA-Top-10-Malware | 73% | 73% | 33 | 1 | 9% 22% 73% | 73% 87% 91% |
| Branch-Top-File-Vulnerabilities | 79% | 79% | 270 | 1 | 11% 25% 79% | 74% 75% 79% |
| Branch-Email-Attachments-Policy | 84% | 84% | 111 | 1 | 11% 25% 84% | 84% 86% 89% |
| Branch-Web-Gateway-Protection | 100% | 100% | 81 | 1 | 22% 38% 100% | 96% 97% 100% |
| Branch-Data-Exfiltration | 100% | 100% | 84 | 1 | 32% 46% 100% | 29% 43% 100% |
| Datacenters-OWASP-Top10 | 100% | 100% | 1200 | 1 | 75% 80% 100% | 83% 86% 100% |

# Notre approche

**Automated BAS “Breach and Attack Simulation” for Live Networks**

## MESURER

Mesurer l’efficacité de vos bastions de cyber securité

Identifier les failles

Communiquer sur l’efficacité réelle et justifier de nouveaux investissments

## OPTIMISER

Prioriser et appliquer les recommandations pour fixer les risques identifiés

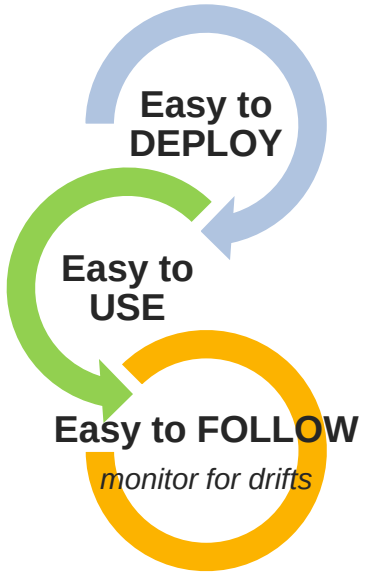
Partager la liste des recommendation pour améliorer l’efficiatité opérationnelle

## MONITORER

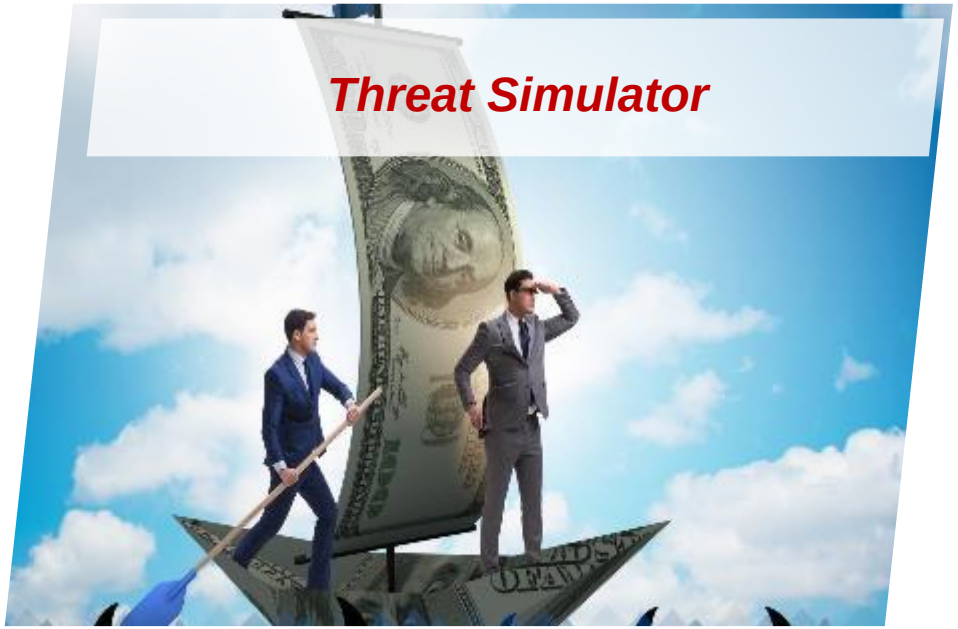
Automatiser l’excécution des controles

Monitorer dans le temps l’ensemble de vos bastions sans effort grace aux validations automatisées.

Anticiper avec une approche pro-active les actions pour améliorer votre posture de sécurité



# La confiance n’exclut pas le contrôle




## Questions ?

**Une démonstration / Une évaluation de la solution**