

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

Qui sommes-nous ?

La plus importante société
de test & mesure au monde

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

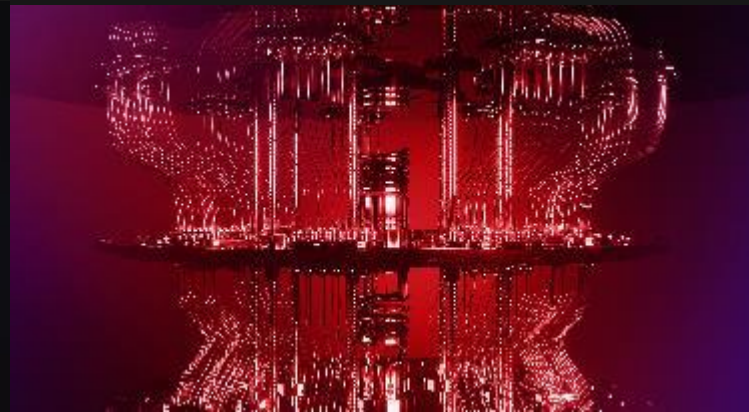


Keysight fournit des outils de test et de mesure dans de nombreux domaines qui seront votre quotidien de demain

Software for NASA



Quantum Computing



5G and 6G



Autonomous vehicles



Industrial IoT



Digital systems in hospitals



+ 20 ans d'expérience dans les réseaux

+ 10 ans dans la cybersécurité auprès des R&D de Constructeurs/Editeurs de solutions de Sécurité

Visibilité des réseaux



Tests réseaux / cybersécurité



Sécurité de l'IoT

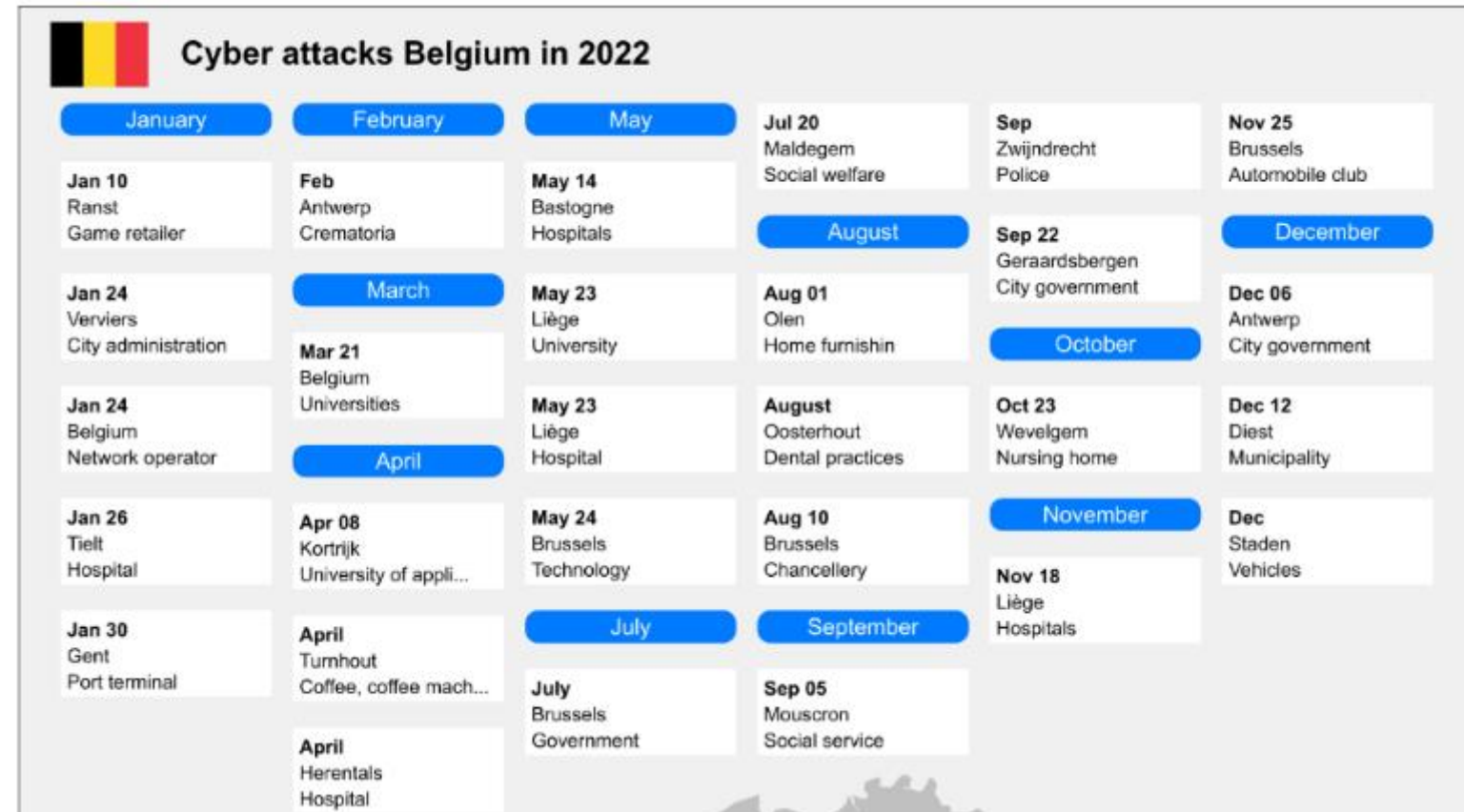


Simulation d'attaques



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

Comment éviter au maximum de faire la Une des journaux ?



Credits: KonBriefing Research



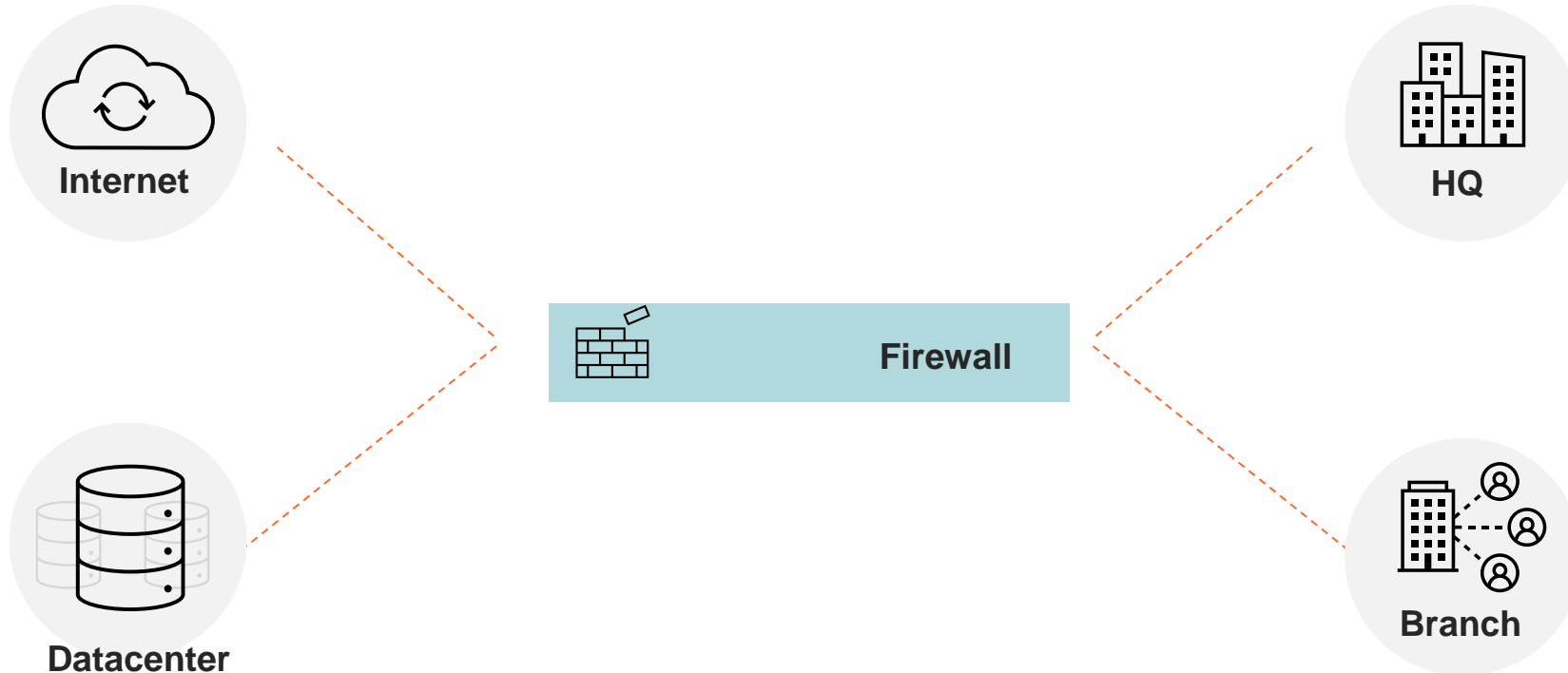
Vous avez une chance sur 8.000 d'être victime d'un incendie, **une chance sur cinq de subir une cyberattaque.** Pourtant, **38% des entreprises belges** ne disposent d'encore aucune stratégie de sécurité active ? *Rapport de Proximus 2022*

21/08/2023 – **Le Centre Public d'Action Sociale (CPAS) de Charleroi (BEL).**

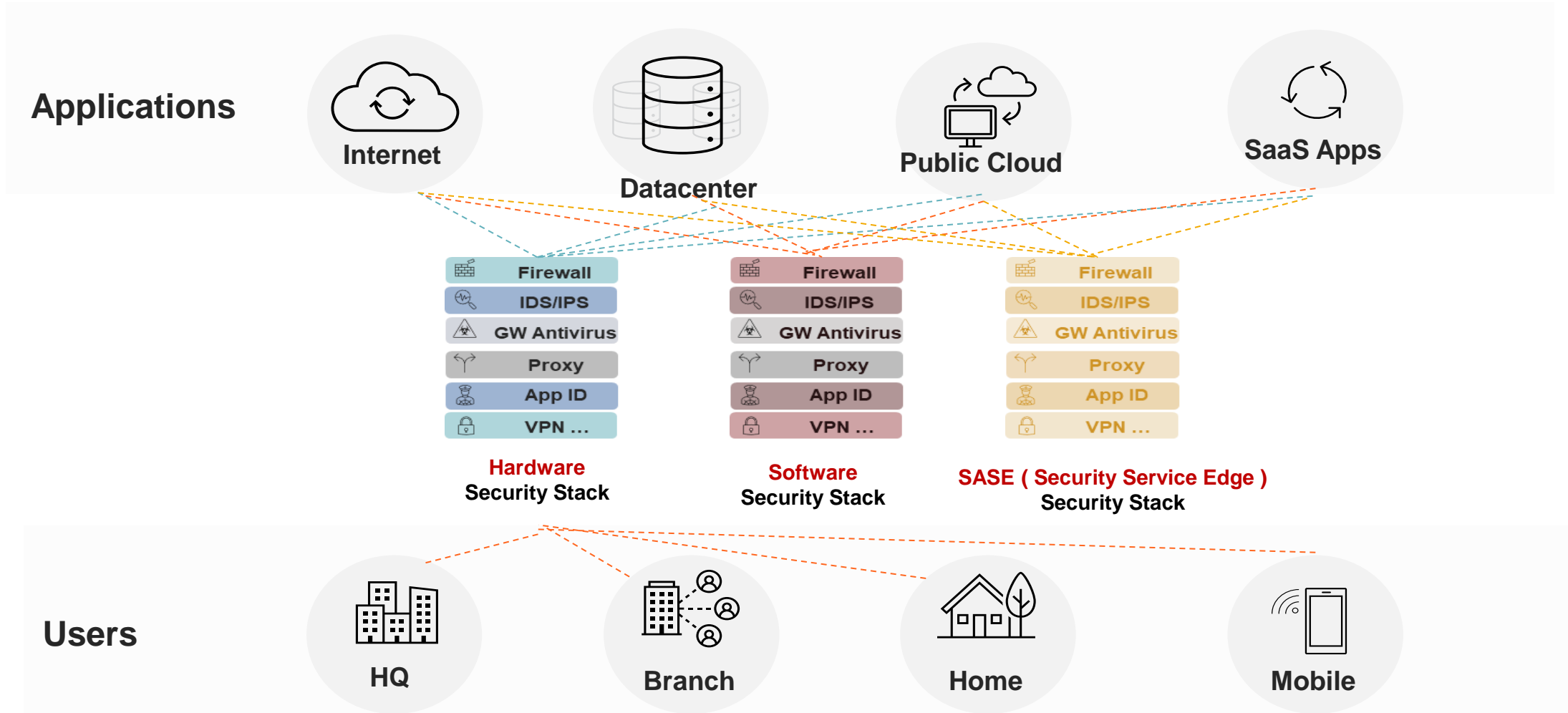
*Ce lundi 21 août, les services informatiques du CPAS carolo ont été victimes d'une cyberattaque, paralysant complètement le site*⁵

L'évolution de la sécurité des réseaux :

Au commencement , une sécurité centralisée avec des “firewall”

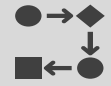


Aujourd'hui : L'approche de la sécurité devient hybride et hétérogène avec l'essor de la DIGITALISATION des services qui peuvent s'exécuter en local &/ou en remote





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 Gouvernance

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).



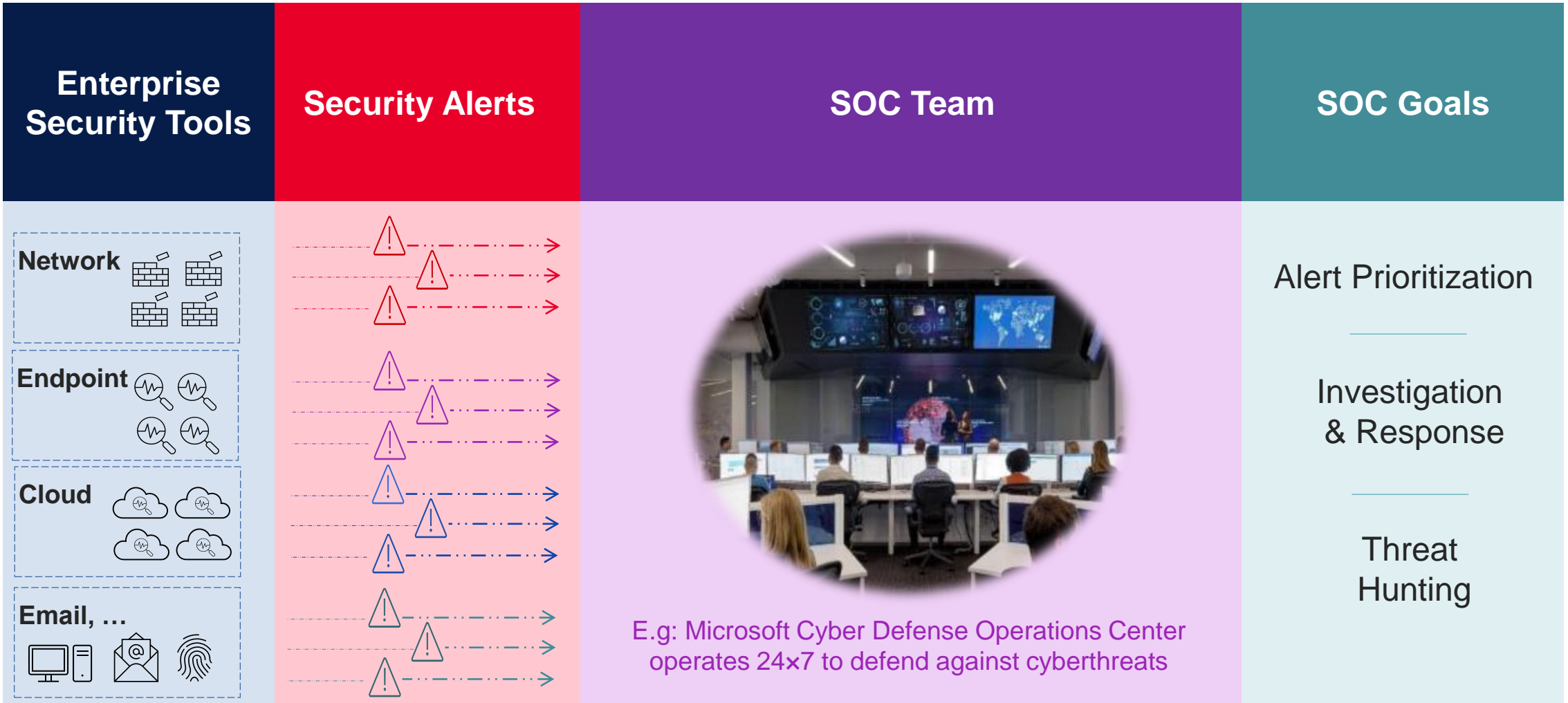
SUPPOSITION #6

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



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 » - People , Process & Technology

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



Une démarche Pro-Active "Ready To Use" :

Notre proposition de Valeur



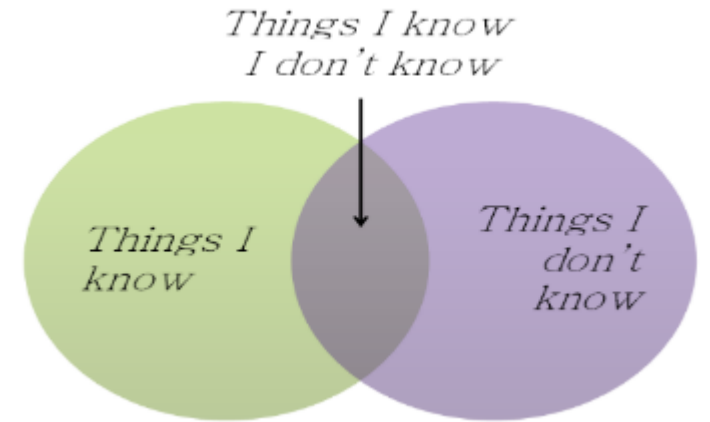
Simuler en toute sécurité des scénarios de cyberattaques



Évaluer avec précision votre niveau de sécurité



Améliorer votre posture de sécurité

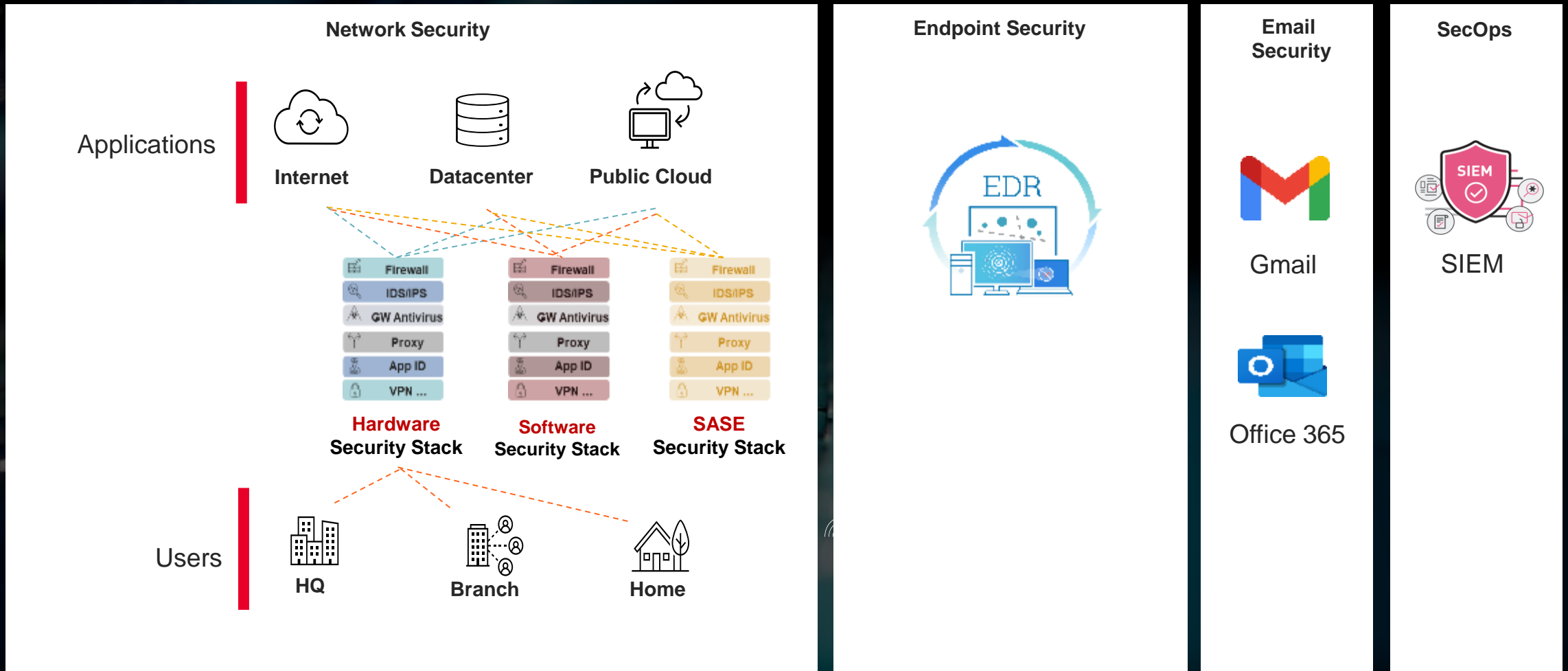


Si vous ne pouvez pas le **mesurer**, vous ne pouvez pas **l'améliorer**.

Kelvin. Physicien, Scientifique (1824 - 1907)

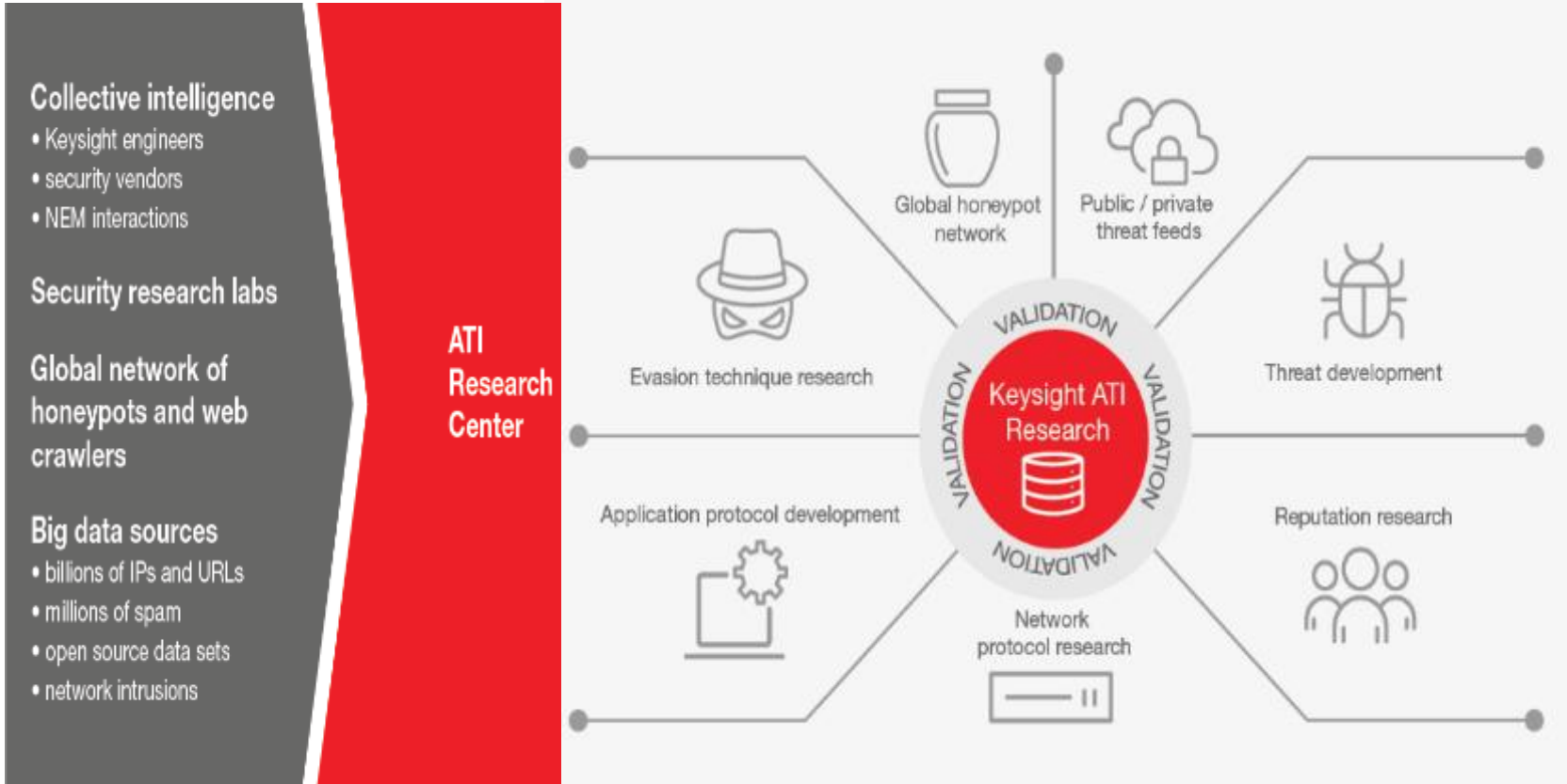
[Comment mesurer son niveau de sécurité IT ?](#)

Les vecteurs d'attaque



Application And Threat Intelligence (ATI)

Keysight's Research Center



Collective intelligence

- Keysight engineers
- security vendors
- NEM interactions

Security research labs

Global network of honeypots and web crawlers

Big data sources

- billions of IPs and URLs
- millions of spam
- open source data sets
- network intrusions

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

ars TECHNICA | [HOME](#) | [TECH](#) | [SCIENCE](#) | [POLICY](#) | [GAMES](#) | [GAMING & CULTURE](#) | [STORE](#) | [FORUMS](#) | [SUBSCRIBE](#) | [SIGN IN](#)

BEAR ATTACK —
Russia-linked hackers accused of targeting COVID-19 vaccine developers
 UK, US, and Canada attribute attacks to group “almost certainly” working for Moscow.
HELEN MARRELL, CLIVE COOKSON, HENRY FOX — FINANCIAL TIMES / 7/16/2020, 10:42 AM

Enlarge / Test doses of another potential SARS-CoV-2 vaccine.

118
 Hackers backed by the Russian state are targeting pharmaceutical companies and academic institutions in the UK, US, and Canada that are working on potential COVID-19 vaccines, British intelligence officials have warned.

The UK's National Cyber Security Centre, working with Canada's Communications Security Establishment, attributed the attacks to hacking group **APT29**, also known as **Cozy Bear**, which it alleged was “almost certainly” working for Russian intelligence services. The findings have been endorsed by the US National Security Agency.

Dominic Raab, UK foreign secretary, said it is “completely unacceptable that the Russian intelligence services are targeting those working to combat the coronavirus pandemic.”

Adversary Emulation Plan – APT29 / CozyBear / CozyCar

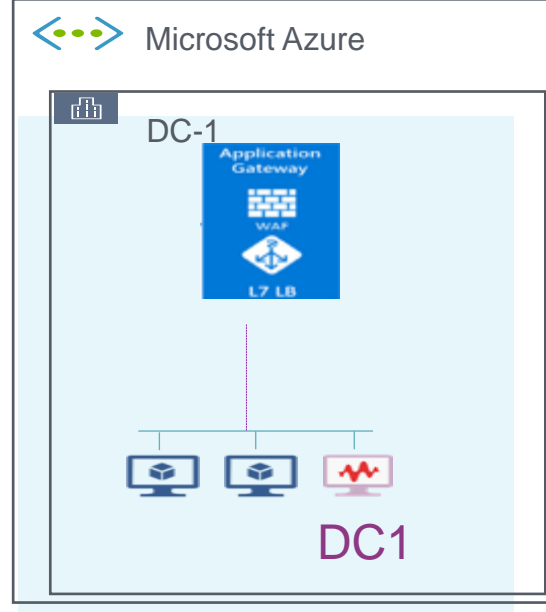
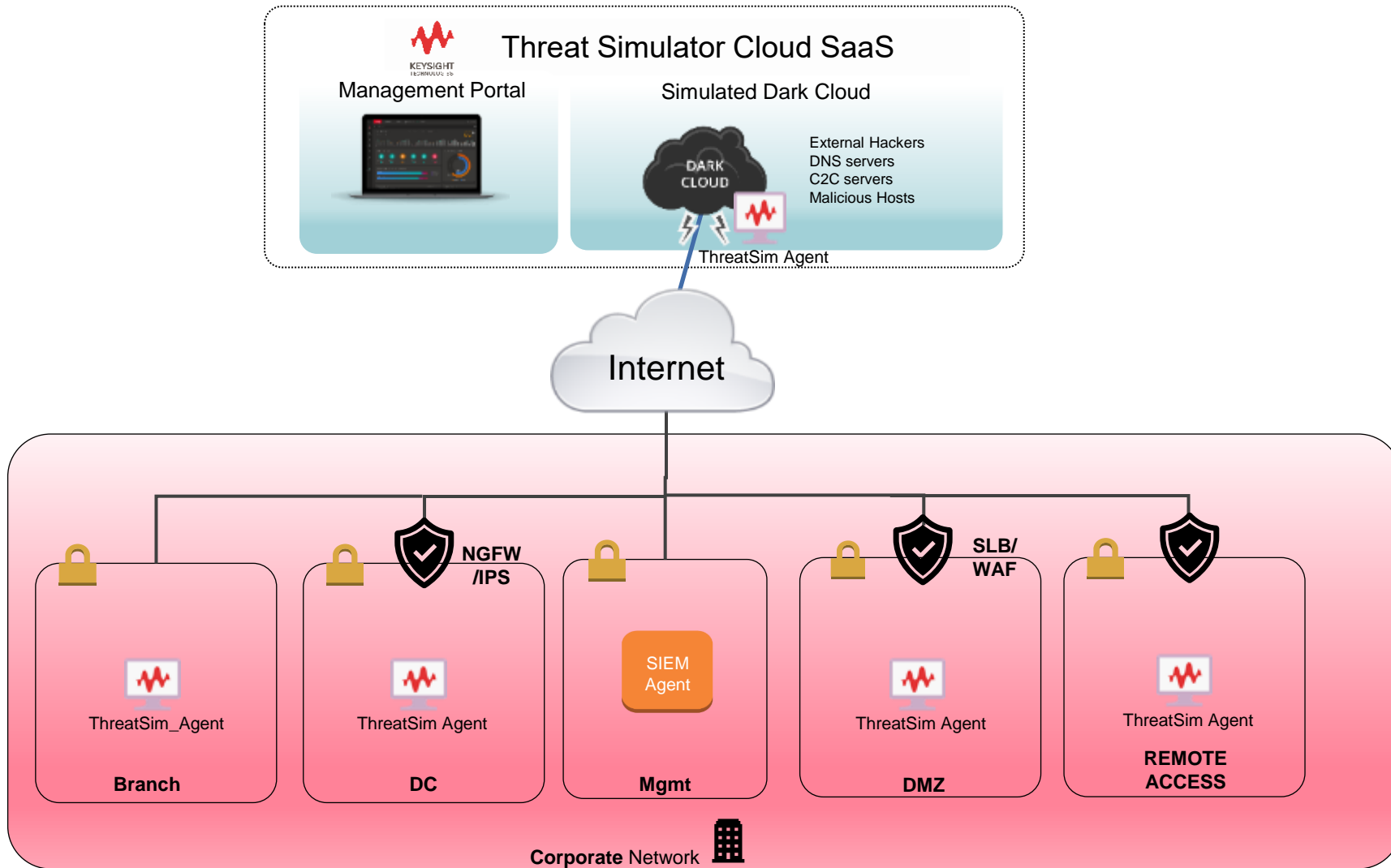


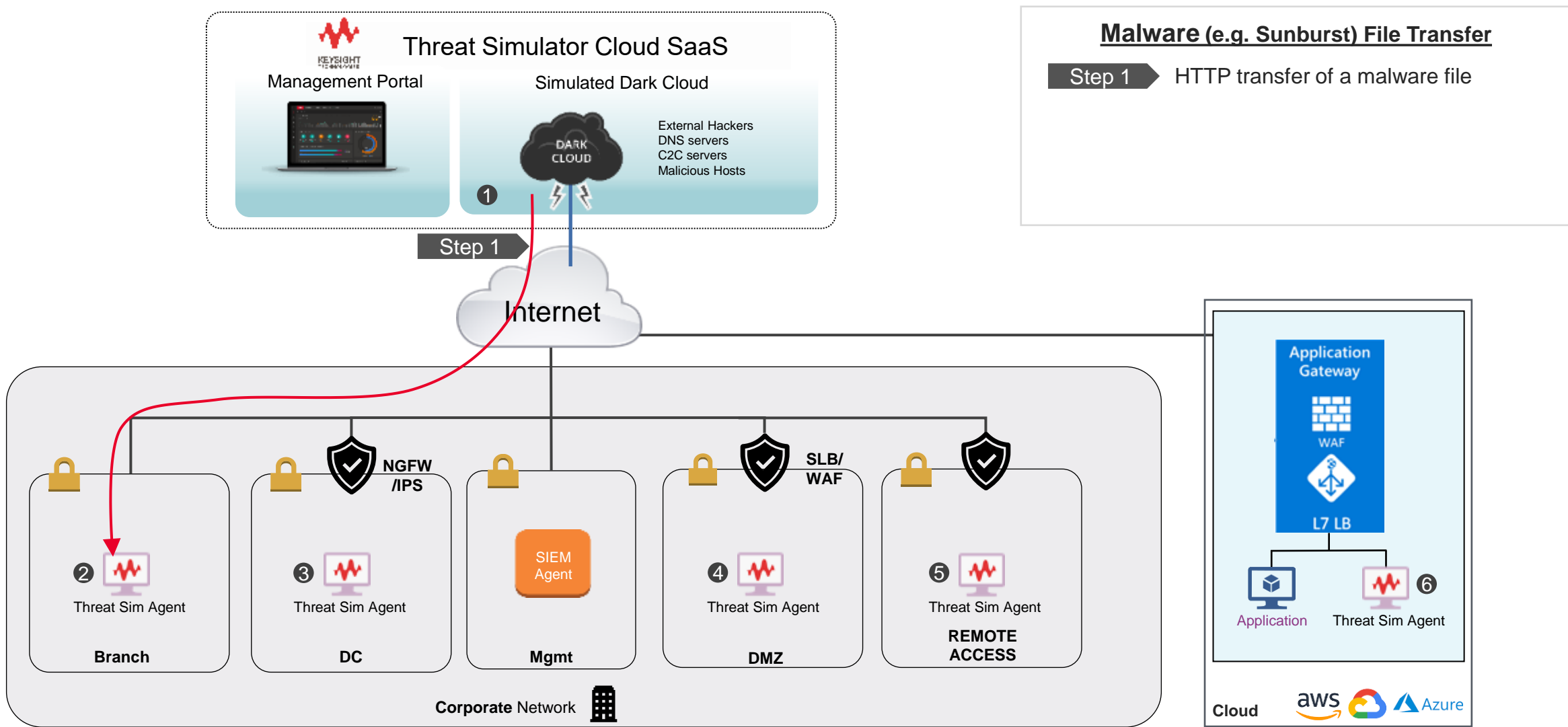
- Malware detonation
- **IoCs collection**



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

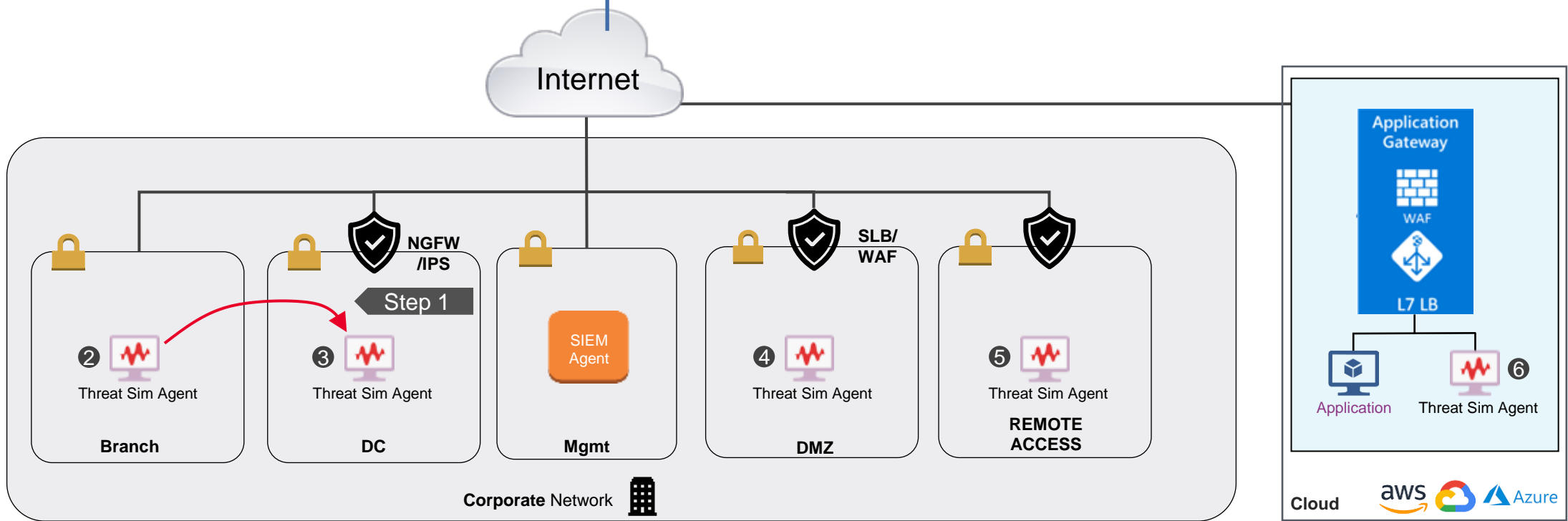
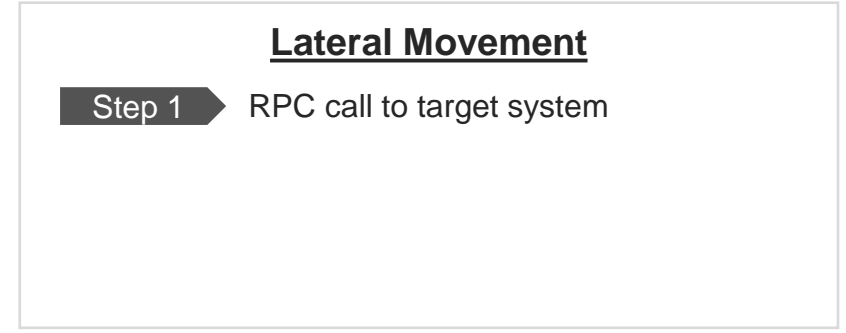
Exemple d'architecture





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).

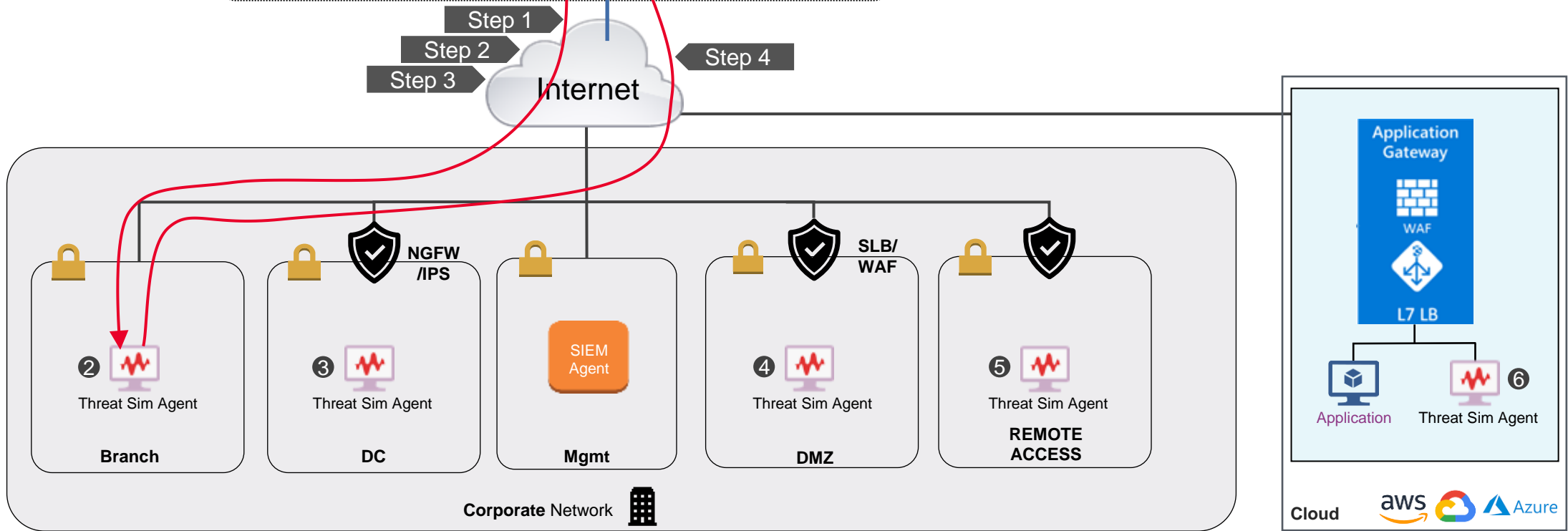
Tels que Sunburst (utilisé par SolarWinds), Darkside, Hafnium, Maze, CLOP, Ryuk, Revil, BotenaGo, etc.



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 récupérer 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

 NETWORK WAF, IPS, GAV, DLP, URL Filtering, DLP	 EMAIL	 ENDPOINT HIPS, HIDS, DLP and AV
Web Application Security / OWASP <ul style="list-style-type: none">-- Cross Site Scripting-- SQL Injection-- Remote File Inclusion-- Local File Inclusion-- Server-Side Script Injection-- OS Command Injection-- Reflected XSS Efficiency-- Stored XSS Efficiency-- SQL Injection Efficiency LAN Perimeter <ul style="list-style-type: none">-- Web browser vulnerabilities-- File format vulnerabilities-- Malware file transfer-- Command and control (C&C) Post-Breach <ul style="list-style-type: none">-- Lateral movement-- Data exfiltration	Policy Assessments <ul style="list-style-type: none">-- Anomalous Archives-- Compressed files-- Corrupted files-- Encrypted archives and documents-- Encrypted content-- Executable binaries-- Executable scripts-- Microsoft Office documents Corporate Email Security <ul style="list-style-type: none">-- Malicious attachments-- Malicious links-- CISA Top-10-- EICAR Validation Email integrations <ul style="list-style-type: none">-- Microsoft Office 365 Email	MITRE ATT&CK Tactics & Techniques <ul style="list-style-type: none">-- TA001 Initial Access-- TA002 Execution-- TA003 Persistence-- TA004 Privilege Escalation-- TA005 Defense Evasion-- TA006 Credential Access-- TA007 Discovery-- TA008 Lateral Movement-- TA009 Collection-- TA010 Command & Control-- TA011 Exfiltration-- TA040 Impact Endpoint Security Controls <ul style="list-style-type: none">-- Host based EPP/EDR/IDS/IPS-- Host based AV-- Host based DLP

Full Kill Chain & APT scenarios | SIEM Integration: Splunk, QRadar, and LogZ.io

Assessments vision MITRE ATT&CK

LaunchPad Threat Campaigns **MITRE ATT&CK Tactics** Assessments [Create Assessment from Selections](#)

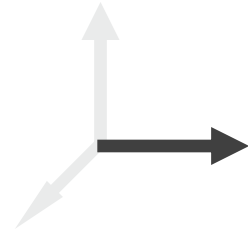
INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY
TECHNIQUES (9)	TECHNIQUES (8)	TECHNIQUES (16)	TECHNIQUES (18)	TECHNIQUES (26)	TECHNIQUES (12)	TECHNIQUES (26)
Supply Chain Compromise T1135 Sub-Techniques(1) Audio Selected	Command and Scripting Interpreter T1059 Sub-Techniques(5) Audio Selected	Account Manipulation T1098 Sub-Techniques(2) Audio Selected	Abuse Elevation Control Mechanism T1548 Sub-Techniques(3) Audio Selected	Abuse Elevation Control Mechanism T1548 Sub-Techniques(2) Audio Selected	Brute Force T1110 Sub-Techniques(1) Audio Selected	Account Discovery T1087 Sub-Techniques(5) Audio Selected
	Exploitation for Client Execution T1203 Audio Selected	BITS Jobs T1137 Audio Selected	Access Token Manipulation T1134 Sub-Techniques(1) Audio Selected	Access Token Manipulation T1134 Sub-Techniques(1) Audio Selected	Credentials from Password Stores T1555 Sub-Techniques(2) Audio Selected	Application Windows T1018 Audio Selected
	Inter-Process Communication T1558 Sub-Techniques(2) Audio Selected	Boot or Logon Autostart Execution T1547 Sub-Techniques(9) Audio Selected	Boot or Logon Autostart Execution T1547 Sub-Techniques(9) Audio Selected	Boot or Logon Autostart Execution T1547 Sub-Techniques(9) Audio Selected	Exploitation for Credential Access T1212 Audio Selected	Browser Bookmarks T1217 Audio Selected
	Native API T1106 Audio Selected	Boot or Logon Initialization Scripts T1037 Sub-Techniques(2) Audio Selected	Boot or Logon Initialization Scripts T1037 Sub-Techniques(9) Audio Selected	Boot or Logon Initialization Scripts T1037 Sub-Techniques(9) Audio Selected	Forced Authentication T1187 Audio Selected	Debugger Evasion T1622 Audio Selected
	Scheduled Task/Job T1053 Sub-Techniques(3) Audio Selected	Browser Extensions T1176 Audio Selected	Boot or Logon Initialization Scripts T1037 Sub-Techniques(9) Audio Selected	Deobfuscate/Decode Files or Information T1134 Audio Selected	Direct Volume Access T1006 Audio Selected	Domain Trust Discovery T1482 Audio Selected
	Shared Modules T1128 Audio Selected	Compromise Client Software Binary T1354 Audio Selected	Create or Modify System Process T1137 Sub-Techniques(3) Audio Selected	Direct Volume Access T1006 Audio Selected	Execution Guardrails T1430 Audio Selected	File and Directory Discovery T1083 Audio Selected
	System Services T1088 Sub-Techniques(3) Audio Selected	Create Account T1126 Sub-Techniques(2) Audio Selected	Event Triggered Execution T1136 Sub-Techniques(9) Audio Selected	Event Triggered Execution T1136 Sub-Techniques(9) Audio Selected	File and Directory Permissions Modification T1222 Sub-Techniques(2) Audio Selected	File and Directory Permissions Modification T1222 Sub-Techniques(2) Audio Selected
	User Execution T1204 Sub-Techniques(2) Audio Selected	Create or Modify System Process T1137 Sub-Techniques(3) Audio Selected	Hijack Execution Flow T1574 Sub-Techniques(1) Audio Selected	File and Directory Permissions Modification T1222 Sub-Techniques(2) Audio Selected	Hide Artifacts T1564 Sub-Techniques(1) Audio Selected	Hide Artifacts T1564 Sub-Techniques(1) Audio Selected
	Windows Management Instrumentation T1047 Audio Selected	Event Triggered Execution T1136 Sub-Techniques(9) Audio Selected	Process Injection T1574 Sub-Techniques(1) Audio Selected	Hide Artifacts T1564 Sub-Techniques(1) Audio Selected	Hijack Execution Flow T1574 Sub-Techniques(1) Audio Selected	Hijack Execution Flow T1574 Sub-Techniques(1) Audio Selected
		Hijack Execution Flow T1574 Sub-Techniques(1) Audio Selected	Scheduled Task/Job T1053 Sub-Techniques(3) Audio Selected	Hijack Execution Flow T1574 Sub-Techniques(1) Audio Selected	Impair Defenses T1562 Sub-Techniques(9) Audio Selected	Impair Defenses T1562 Sub-Techniques(9) Audio Selected
		Modify Authentication Process T1556 Sub-Techniques(1) Audio Selected	Indicator Removal on Host T1070 Sub-Techniques(4) Audio Selected	Indicator Removal on Host T1070 Sub-Techniques(4) Audio Selected	Scheduled Task/Job T1053 Sub-Techniques(3) Audio Selected	Scheduled Task/Job T1053 Sub-Techniques(3) Audio Selected
		Office Application Corruption T1135 Sub-Techniques(1) Audio Selected		Indicator Removal on Host T1070 Sub-Techniques(4) Audio Selected	Unsecured Credentials T1133 Sub-Techniques(1) Audio Selected	Unsecured Credentials T1133 Sub-Techniques(1) Audio Selected



T1021 Sub-Techniques(2) Audio Selected	T1185 Audio Selected	Dynamic Resolution T1558 Sub-Techniques(2) Audio Selected	T1048 Sub-Techniques(3) Audio Selected
T1090 Audio Selected	Clipboard Data T1115 Audio Selected	Encrypted Channel T1572 Sub-Techniques(2) Audio Selected	Defeat Mitigation T1585 Sub-Techniques(2) Audio Selected
T1086 Audio Selected	Data from Local System T1085 Audio Selected	Fallback Channels T1008 Audio Selected	Disk Wipe T1561 Sub-Techniques(2) Audio Selected
T1083 Audio Selected	Data Staged T1074 Sub-Techniques(2) Audio Selected	Ingress Tool Transfer T1105 Audio Selected	Scheduled Transfer T1025 Audio Selected
T1046 Audio Selected	Email Collection T1114 Sub-Techniques(1) Audio Selected	Multi-Stage Channels T1104 Audio Selected	Resource Hijacking T1495 Sub-Techniques(1) Audio Selected
T1114 Audio Selected	Network Share Discovery T1048 Audio Selected	Non-Application Layer Protocol T1085 Audio Selected	Service Stop T1489 Audio Selected
T1048 Audio Selected	Password Policy Discovery T1261 Audio Selected	Traffic Signaling T1205 Sub-Techniques(1) Audio Selected	
T1046 Audio Selected	Peripheral Device Discovery T1179 Audio Selected	Remote Access Software T1219 Audio Selected	
T1046 Audio Selected	Permission Groups Discovery T1089 Sub-Techniques(2) Audio Selected		
T1046 Audio Selected	Process Discovery T1057 Audio Selected		
T1046 Audio Selected	Query Registry T1057 Audio Selected		

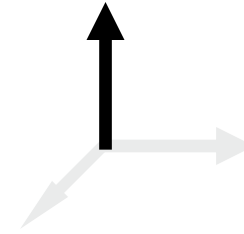
Quelques cas d'usage

De la PME aux Services Managés



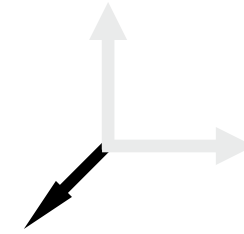
Taille

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

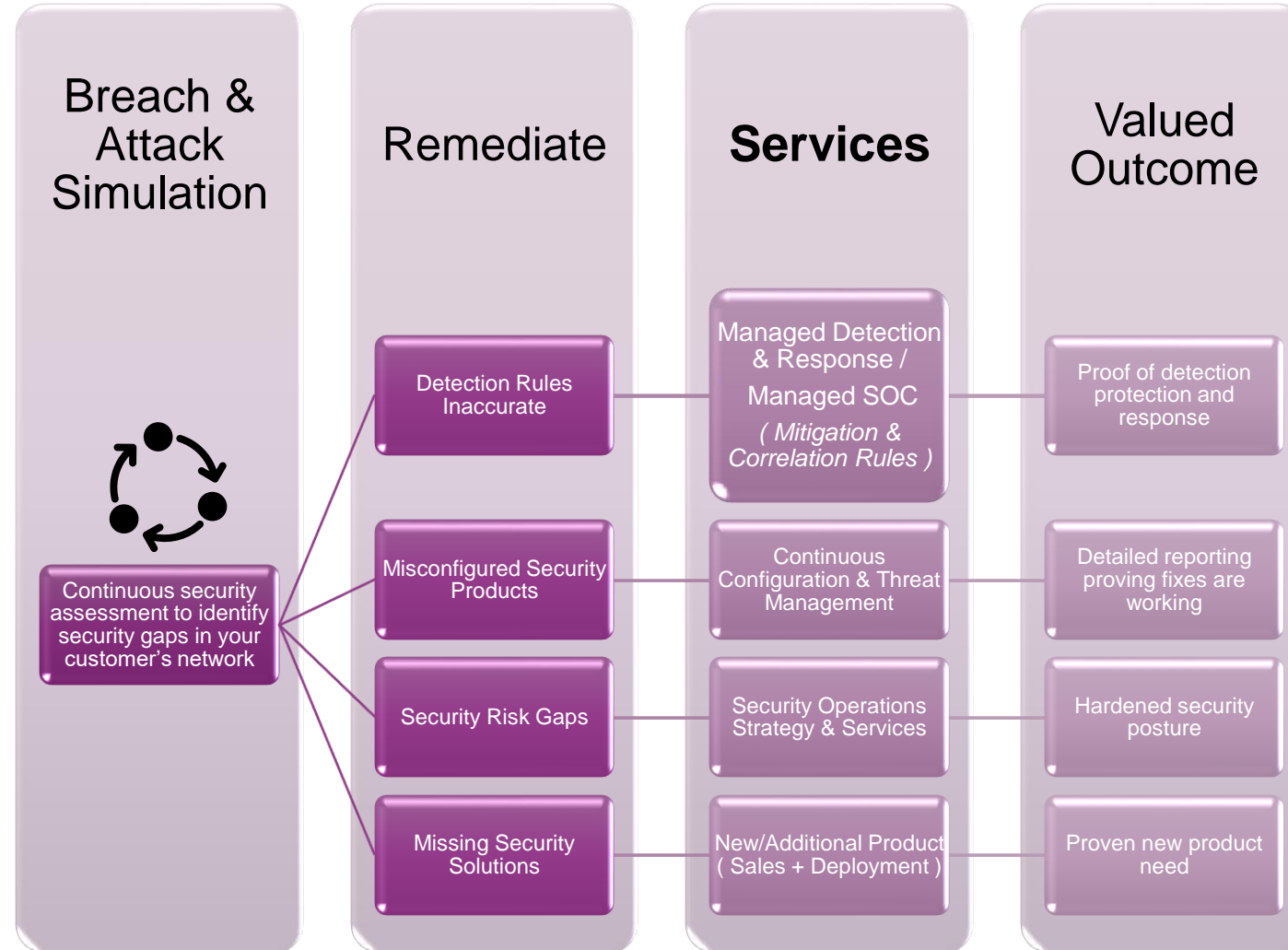
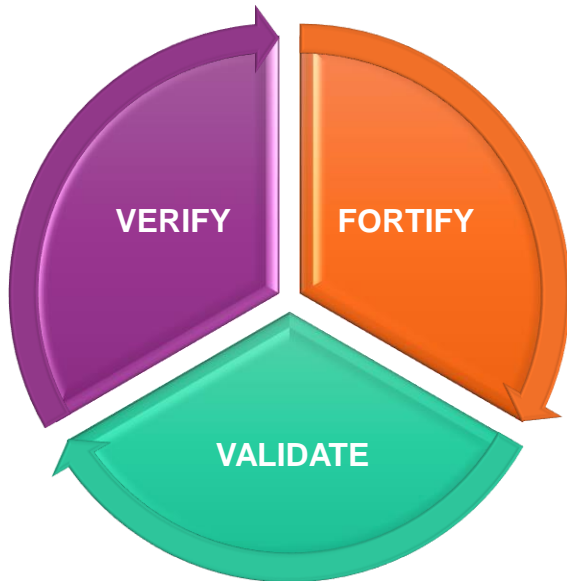
Threat Simulator

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

Complète 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



Tuner & Améliorer votre portefeuille existant

Challenger vos Services 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

george.zscheru@keysight.com



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%	210	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

george.zscheru@keysight.com



OVERALL NETWORK SECURITY



SECURITY SCORES BY LOCATION (SORTED BY PREVENTION SCORE)

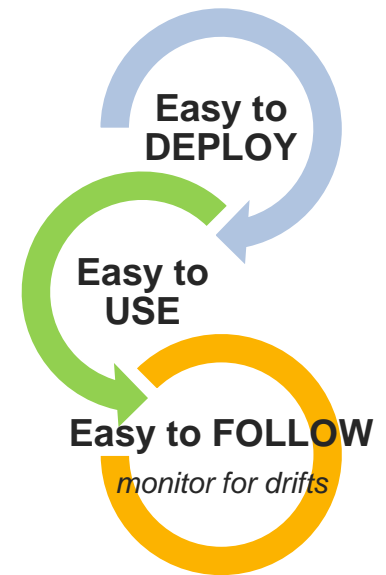
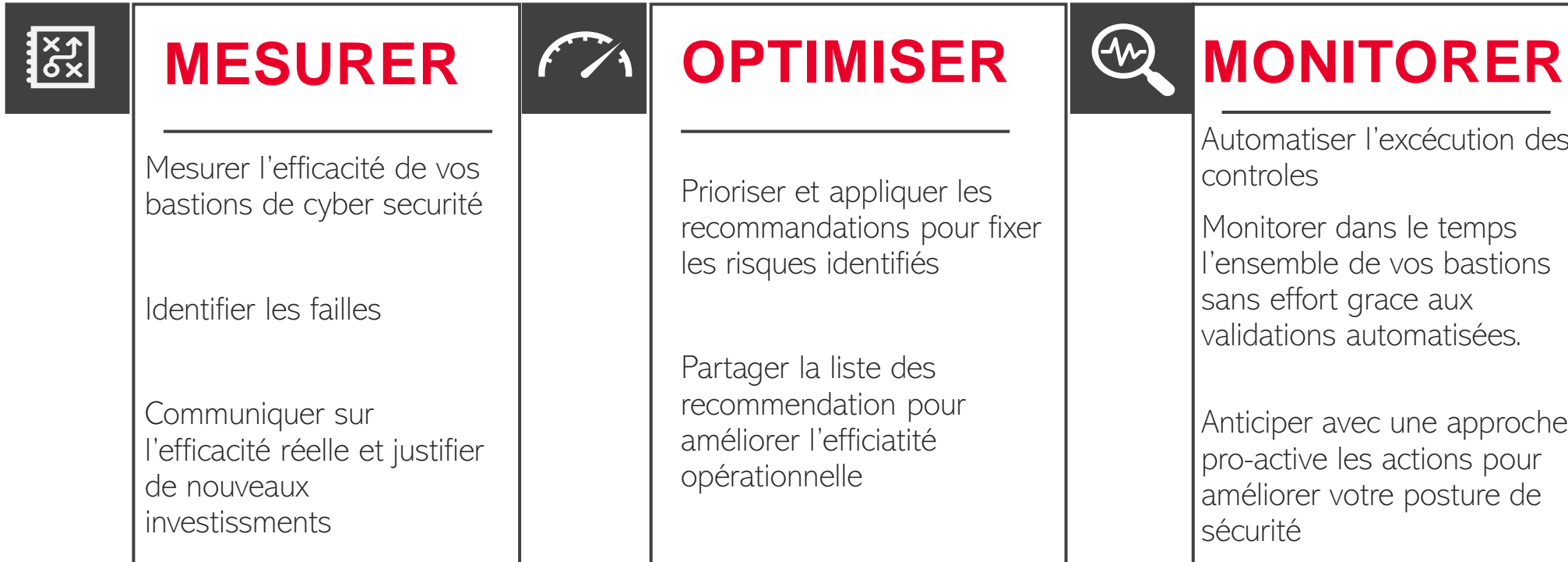
LOCATION	PREVENTION SCORE	DETECTION SCORE	AUDITS RUN	AGENTS ASSESSED	LAST 7-DAYS PREVENTION (MIN/AVG/MAX)	LAST 7-DAYS DETECTION (MIN/AVG/MAX)
Branch-Austin	85%	85%	200	1	15% 29% 85%	75% 77% 85%
Branch-London	85%	85%	200	1	15% 29% 85%	75% 77% 85%
Branch-Singapore	85%	85%	200	1	15% 29% 85%	75% 77% 85%
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)

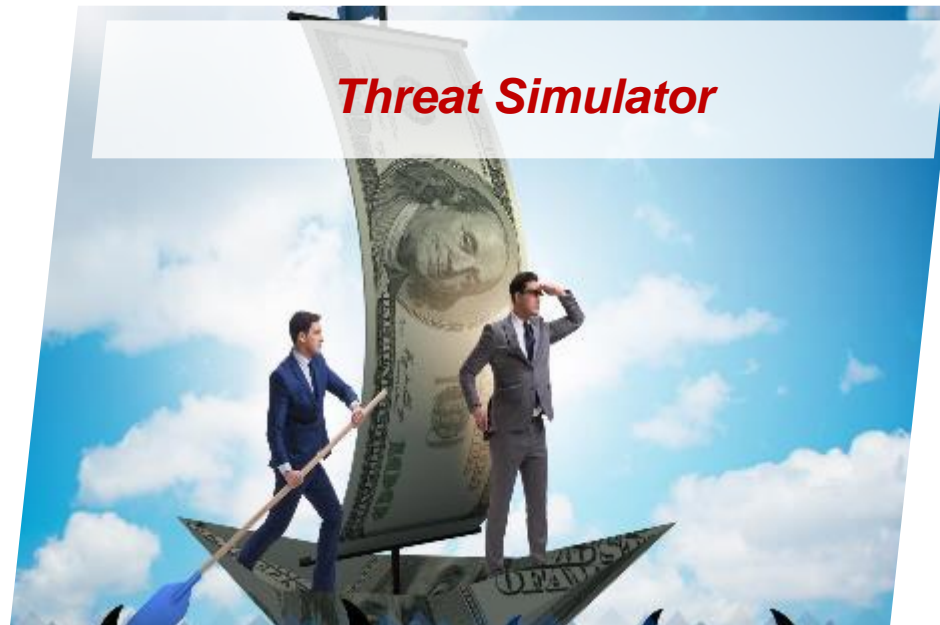
SCENARIO NAME	PREVENTION SCORE	DETECTION SCORE	AUDITS RUN	AGENTS ASSESSED	LAST 7-DAYS PREVENTION (MIN/AVG/MAX)	LAST 7-DAYS DETECTION (MIN/AVG/MAX)
Branch-CISA-Top-10 Exploits	71%	71%	21	1	0% 14% 71%	71% 83% 86%
Branch-CISA-Top-10-Malware	73%	73%	33	1	9% 22% 73%	73% 87% 91%
Branch-Top-File-Vulnerabilities	79%	79%	210	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



La confiance n'exclut pas le contrôle



Questions ?

Une démonstration / Une évaluation de la solution