vumetric
CYBERSECURITY

LA CYBERSÉCURITÉ À L'ÈRE DE L'INFONUAGIQUE ET DE L'INDUSTRIE 4.0

26 septembre 2018

PRESENTÉ PAR

Patrick Chevalier

CISSP, CISA, CSSLP, GIAC, CPTE, CEH

Associé, conseiller principal

Agenda

- Présentation
- Tendances en cybersécurité
- Réalité en entreprise
- Enjeux spécifiques
  - Sécurité de l'infonuagique / Cloud
  - Sécurité des réseaux industriels
- Recommandations
- Conclusion / Questions

vumetric CYBERSECURITY

Qui suis-je ?

- Patrick Chevalier
  - > CISSP, CISA, CSSLP, GIAC, etc.
- Associé et conseiller principal @ Vumetric
- 20 ans d'expérience en cybersécurité
  - > Consultation, Audits, Plan directeur, etc.
- Conférencier dans ses temps libres !

vumetric CYBERSECURITY

À propos de Vumetric

- Entreprise dédiée à la cybersécurité
  - > Québec et Montréal
  - > 300+ projets annuels
  - > À votre service depuis plus de 10 ans !
- Clientèle variée:
  - > Manufacturier, technologie, services financiers, énergie, alimentation, SaaS, assurance, gouvernements, pharma, etc.
- Entreprise 100% indépendante
  - > Aucune activité de revente de solutions (pare-feu, antivirus, etc.)
  - > Approche agnostique et impartiale

vumetric CYBERSECURITY

Offre de services

Tests d'intrusion et audits de sécurité

Test d'intrusion réseau • Test d'intrusion Web • Revue de code • Audit de sécurité • Audit Cloud • Test d'hameconnage, etc.

Surveillance et impartition en sécurité

Surveillance de la sécurité • Détection des intrusions • Balayage est gestion des vulnérabilités • Veille sur les correctifs de sécurité, etc.

Services professionnels en cybersécurité

Accompagnement en sécurité • Mise en conformité • Plan directeur • Sécurité du Cloud • Sécurité applicative • Services conseils, etc.

vumetric CYBERSECURITY

vumetric
CYBERSECURITY

TENDANCES EN CYBERSÉCURITÉ

Tendances en cybersécurité

- Augmentation générale des cyberattaques
- Sensibilisation grandissante aux enjeux de sécurité
  - > Augmentation de la couverture médiatique, ransomware, etc.
  - > Demeure un enjeu technique pour plusieurs
- Augmentation générale des investissements
- Augmentation de la reddition de compte
  - > Questionnaires de conformité et normes (ex: GDPR, PCI, etc.)
- Éclatement du « périmètre de sécurité »
  - > Mobilité, BYOD, Cloud, Télétravail, Impartition, etc.

vumetric CYBERSECURITY

Augmentation des cyberattaques

AIR CANADA

30 août 2018

L'application d'Air Canada aurait été piratée

7 septembre 2017

143 millions de clients d'Équifax touchés par un piratage

13 septembre 2018

La MRC de Mékinac est la proie de pirates informatiques

23 janvier 2018

Près de 100 000 clients de Bell Canada victimes de piratage

14 septembre 2017

Un faux fournisseur dérobe 3,3 millions à Future Electronics

30 septembre 2016

Piratage informatique: lourde facture pour la CS des Appalaches

1 avril 2018

La Baie d'Hudson victime de pirates

17 septembre 2018

La CS des Chênes aux prises avec un virus informatique

31 mars 2017

Le site d'embauche de McDonald's Canada piraté

25 septembre 2018

Artopex victime de pirates informatiques

vumetric CYBERSECURITY

Tendances des menaces

- Ingénierie sociale
- Ransomware
- Cryptomining
- Mots de passe faibles
- Sécurité du Cloud
- Menaces internes
- BYOD
- Sécurité Webapp
- Botnets
- APT / Malware ciblé

vumetric CYBERSECURITY

vumetric
CYBERSECURITY

RÉALITÉ EN ENTREPRISE

Réalité en entreprise

- Plusieurs dépassées par les enjeux de sécurité
- Expertise généralement incomplète à l'interne
  - Équipes TI déjà débordées par les opérations courantes
  - Rareté des ressources en TI (et en sécurité !)
- Pas de planification stratégique / roadmap
  - Plusieurs directeurs TI ont de la difficultés à justifier les budgets requis
  - Mentalité « Ça n'arrive qu'aux autres » encore présente
- Manque de visibilité (Pas de KPI)

vumetric CYBERSECURITY

Réalité en entreprise

	Defeatists	Denialists	Realists	Egoists
	Their IT security is weak and underfunded	Their IT security is weak but they lack full awareness of this reality	Their IT security is fair and they strive to be better	Their IT security is good but they risk over-confidence
Percentage of organizations	23%	37%	23%	17%
Breaches compared to average	More	More	Fewer	Fewer
Percentage of IT budget on security	6%	8%	14%	12%
Confidence in security defenses	Low	High	Low	High
Focus areas	Trial and error/ little risk process	Technology over people/process	Employee training/ benchmarking with outside peers	Formal risk process/hiring topnotch staff
Level of maturity out of 5	1–2	2–3	3–4	4–5
Industry profile	Manufacturing/ resources	Public sector/ infrastructure/ telco	Retail/ distribution	Finance

Source: IDC Canada - Determining How Much to Spend on Your IT Security The Canadian Perspective (2015)
https://www-03.ibm.com/industries/ca/en/healthcare/documents/IDC_Canada_Determining_How_Much_to_spend_on_Security_-_Canadian_Perspective_2015.pdf

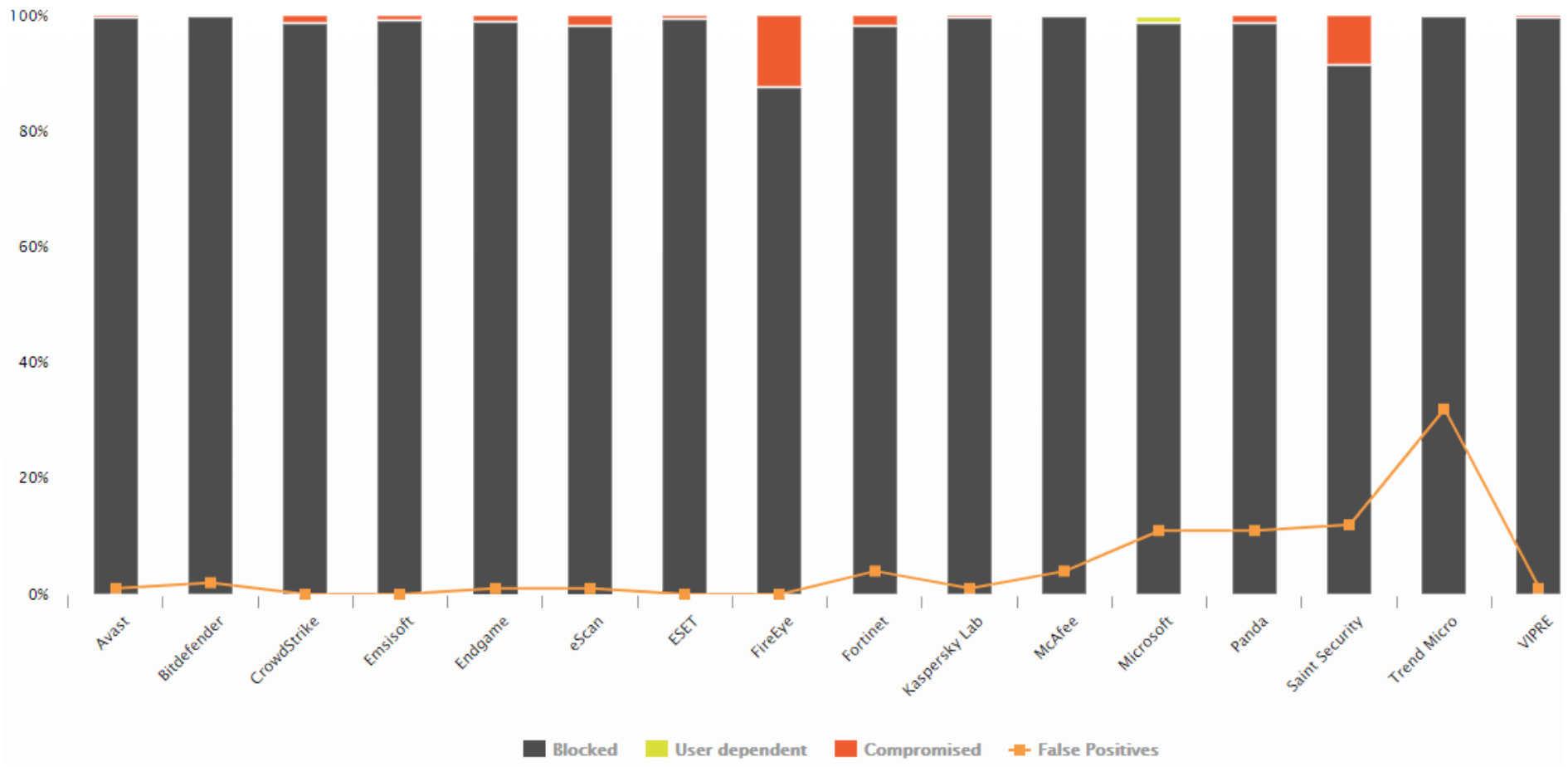
vumetric CYBERSECURITY

Réalité en entreprise

- Plusieurs s'appuient sur des entreprises spécialisées
  - > Tous veulent rentabiliser leurs investissements
- La sécurité *de base* est généralement en place
  - > Pare-feu, anti-spam, web filter, anti-virus, correctifs.
- Des solutions de sécurité… qui n'apportent pas de solution
  - > Mauvaise évaluation du TCO
  - > …ou solution simplement mal adaptée au contexte

vumetric CYBERSECURITY

Ex: Solutions antivirus…



Source: AV Comparatives – Antivirus Real-World protection Test Mar-Jun 2018
https://www.av-comparatives.org/enterprise/comparison/

vumetric CYBERSECURITY

Cybersécurité de base en 2018

Mécanismes

- Pare-feu
- Anti-Virus
- Anti-Spam
- Web Filter
- VPN

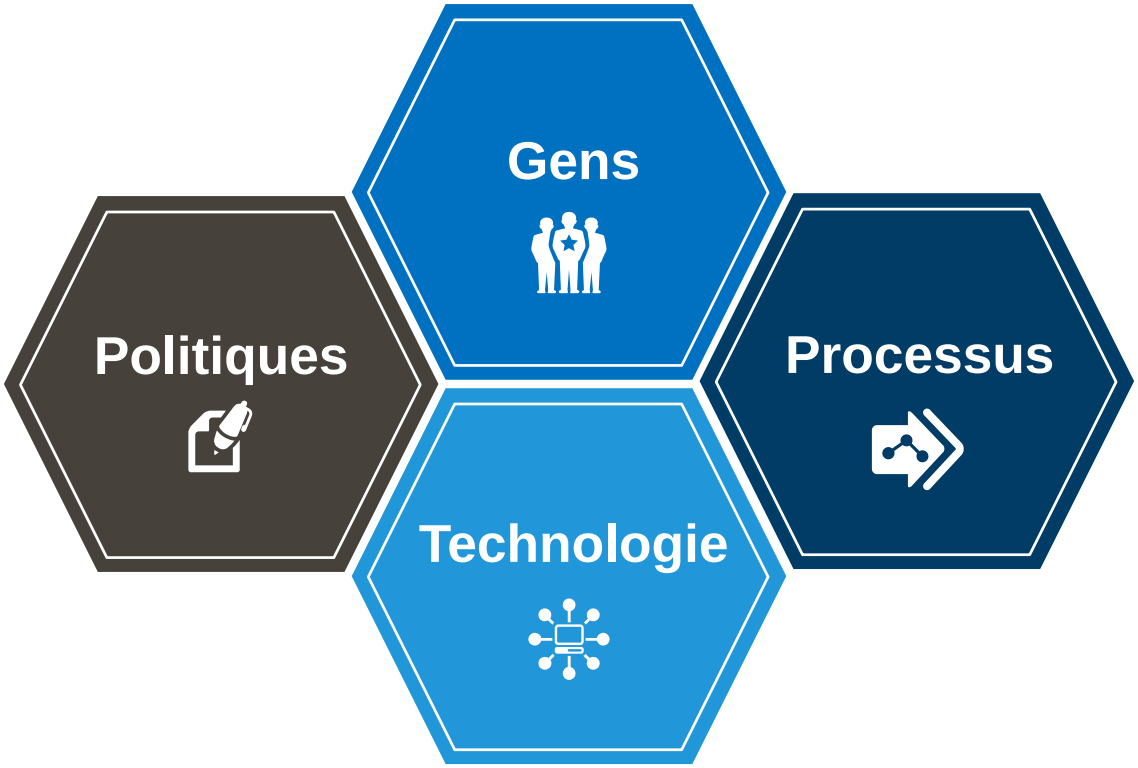
Activités

- Gestion des correctifs
- Gestion des vulnérabilités
- Inventaire
- Segmentation du réseau
- Gestion des accès
- Surveillance de la sécurité
- Gestion des sauvegardes
- Sensibilisation des employés

Notez qu'il n'y a pas d'"Intelligence artificielle" ou de "Machine Learning" ici…

vumetric CYBERSECURITY

Stratégie de cybersécurité intégrée



vumetric CYBERSECURITY

vumetric
CYBERSECURITY

SÉCURITÉ DU CLOUD / INFONUAGIQUE

Sécurité du cloud

- Adoption en constante progression !
- La sensibilisation aux enjeux de sécurité du Cloud est généralement adéquate
- Change les paradigmes de sécurité traditionnels
  - > Défense périmétrique, focus sur le réseau, etc.
- Domaine relativement récent
  - > Souvent des lacunes dans l'expertise disponible
  - > Mauvaise connaissance des fonctionnalités de sécurité offertes (ex: Office 365)
  - > Mauvaise compréhension des rôles et responsabilités

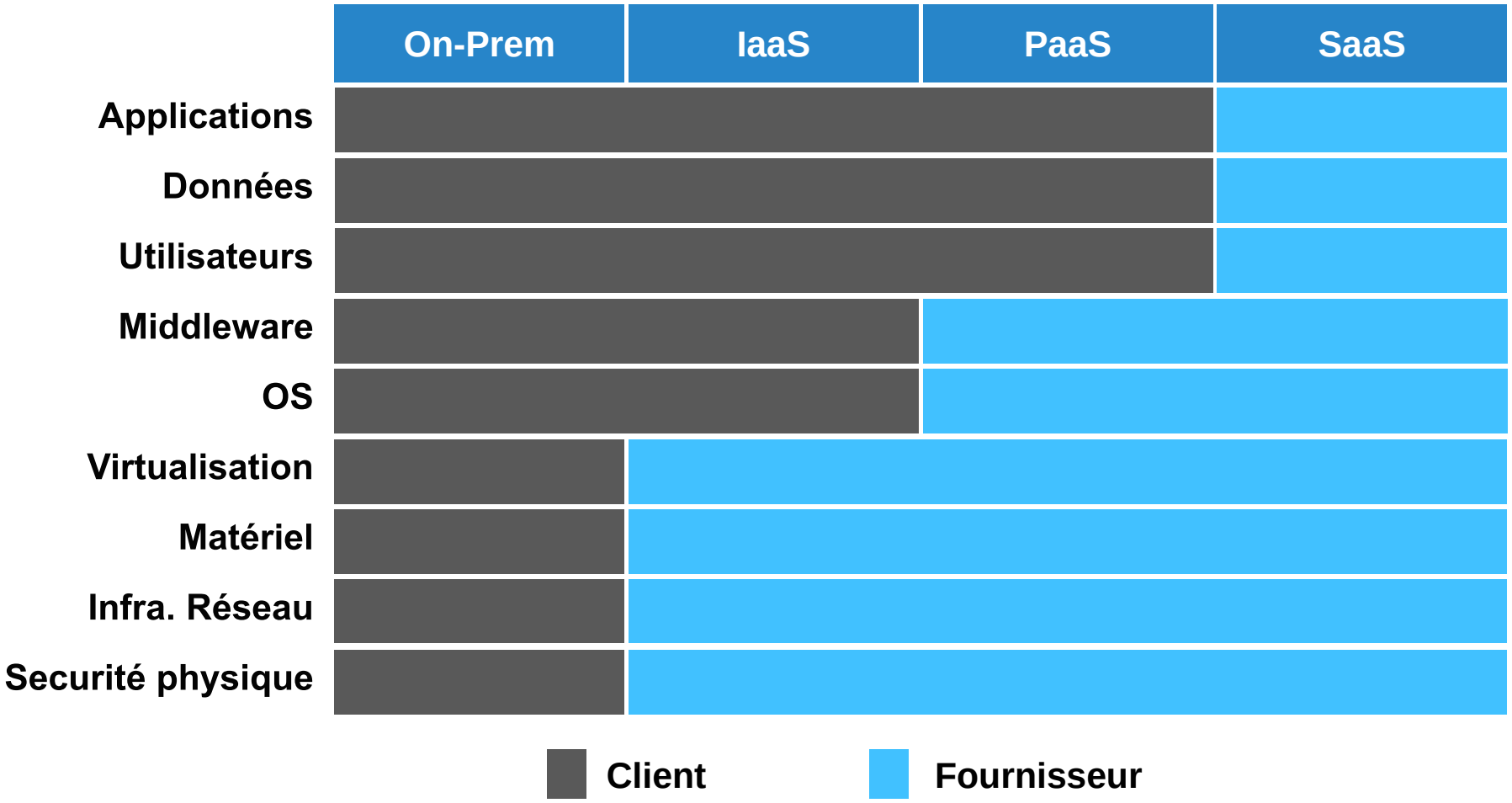
vumetric CYBERSECURITY

“Through 2020, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities. ”

Neil MacDonald, Gartner

vumetric CYBERSECURITY

Cloud: Responsabilités partagées



vumetric CYBERSECURITY

Cloud: Recommandations générales

- Valider les fournisseurs
  - > Conformité SOC1, SOC2, SSAE-16, etc.
- Intégrer la sécurité à même les projets
  - > Appel à expertise externe si requis
- Utiliser les fonctionnalités de sécurité natives
  - > Activer l'authentification multi-facteur
  - > Sécuriser les serveurs/composants
  - > Chiffrer les données
- Tester et corriger les vulnérabilités régulièrement

vumetric CYBERSECURITY

vumetric
CYBERSECURITY

SÉCURITÉ DES RÉSEAUX INDUSTRIELS

Sécurité des réseaux industriels

- Niveau de maturité général très faible
- Souvent une *boite noire* pour les équipes TI
  - > Aucune ou peu de visibilisé, géré par équipe distincte, etc.
- Impact sur les affaires facile à démontrer
  - > Perte de productivité, Arrêt de chaine de production, etc.
- Principales lacunes observées:
  - > Contrôles des accès
  - > Segmentation

vumetric CYBERSECURITY

Sécurité des réseaux industriels

- Débuter avec un audit/bilan
  - Identifier les actifs (systèmes, IP, données)
  - Identifier les vulnérabilités / lacunes de sécurité
  - Évaluer et quantifier les risques
- De façon générale:
  - Segmenter le réseau industriel du réseau TI
  - Contrôler les accès (fournisseur, support, etc.)
  - Sensibiliser les équipes de production
  - Adopter une stratégie de *défense en profondeur*
  - S'aligner sur les principaux standards (NIST 800-82, ISO/IEC-62443)

vumetric CYBERSECURITY

vumetric
CYBERSECURITY

RECOMMANDATIONS GÉNÉRALES

Recommandations: administratives

- Planifier et budgétiser les dépenses de sécurité
  - > 8-14 % du budget TI, 1 ressource dédiée par 500 employés
  - > Réviser la planification sur une base annuelle
- Identifier et mesurer les KPI
  - > Intégrer la sécurité au niveau exécutif
- Sensibiliser les employés
  - > Newsletter OUCH!, test d'hameçonnage, etc.
- Considérer l'impartition pour certaines activités clés

SANS Institute OUCH! Newsletter
https://www.sans.org/security-awareness-training/ouch-newsletter

vumetric CYBERSECURITY

Recommandations: techniques

- Identifier et focuser sur les *quick-wins* !
- Adopter une stratégie de *défense en profondeur*
  - > Combiner les contrôles de prévention et de détection
- Tester et corriger régulièrement les vulnérabilités
  - > Test d'intrusion, audit de sécurité, etc.
- Évaluer les solutions de sécurité adéquatement
  - > Faite abstraction des *buzzwords du jour*
  - > Sources: Gartner, NSS Labs, AV-Comparatives, etc.
  - > Considérer le TCO !

vumetric CYBERSECURITY

" *If you spend more on coffee than on IT security, you will be hacked.*
What's more, you deserve to be hacked. "

Source: Richard Clarke, White House Cyber Security Advisor

vumetric CYBERSECURITY

vumetric
CYBERSECURITY

MERCI DE VOTRE ATTENTION !

QUESTIONS ?

Patrick Chevalier
Associé, conseiller principal
pchevalier@vumetric.com
1-877-805-RISK