10 technologies

1. SIEM (Security Information and Event Management)
Remontée de logs, analyse automatique et alertes en temps réel. Indispensable pour identifier rapidement les incidents de sécurité et réagir avant que la situation ne s’aggrave.

2. Firewall
L’indispensable filtre qui t’évite de te prendre des attaques sur ton infra. Sans ça, autant laisser la porte ouverte et sortir les petits fours.

3. EDR (Endpoint Detection and Response)
Pour que ton système détecte quand quelque chose qui ne devrait pas se passer se passe.

4. Solutions de Sécurité Cloud
Ah, le cloud. Là où tout est censé être sécurisé et flou. En vérité, la grande majorité des attaques aujourd’hui cible le cloud, normal, c’est là où tout se passe !

5. VPN (Virtual Private Network)
Parce que travailler depuis un salon de thé en toute sécurité, c’est le rêve de tout “hacker”. Aussi parce que tout le monde en télétravail est sur VPN, et que c’est un bon vecteur d’attaque.

6. IDS/IPS (Intrusion Detection/Prevention Systems)
IDS observe ce qui passe sur le réseau, IPS agit. Ça se bypass, mais surtout, ça se met en place et ça se configure comme il se doit.

7. Antivirus / Anti-Malware
Parce qu’en 2024, les virus ne sont pas encore obsolètes, désolé de te décevoir. Mais la majorité des anti-malwares aujourd’hui sont des EDR, et comme les commerciaux en ont vendu à toutes les boîtes, on a inventé les XDR.

8. Technologie de Chiffrement
Parce que les données sensibles, c’est mieux quand elles ne sont pas stockées en clair. Encore mieux quand elles ne sont pas transférées en clair non plus…

9. IAM (Identity and Access Management)
Pour gérer qui accède à quoi, même si toi-même tu t’y perds un peu et que tu n’as accès à pas grand-chose.

10. DLP (Data Loss Prevention)
Empêche les fuites de données, quand ça marche bien. Parce que partager, c’est sympa, mais pas les infos sensibles à des personnes non autorisées.

Revision #1
Created 2024-11-01 20:14:06 UTC by Admin

Updated 2024-11-01 20:14:44 UTC by Admin