SYNACKTIV

RED TEAM

Succès, tendances et statistiques clés

RAPPORT 2024

35

MISSIONS

RED TEAM

EN 2024

1800 | **JOURS-HOMMES**
50 EN MOYENNE

12 | **AUDITEURS**
5+ ANNÉES XP

EFFORT

PAR TYPOLOGIE D'ENTREPRISE

35 JH

13 RED TEAM

SENSIBILITÉ À LA SÉCURITÉ RÉCENTE OU LIMITÉE

- Solutions de sécurité en cours de déploiement (EDR, cloisonnement)
- SOC récent, supervision ponctuelle via des outils non corrélés
- Audits ponctuels, surface d'attaque peu maîtrisée
- Premiers exercices red / purple team réalisés à titre exploratoire

50 JH

17 RED TEAM

PRISE DE CONSCIENCE DES ENJEUX, EN STRUCTURATION

- Principales solutions de sécurité déployées (EDR, MFA)
- SOC en horaires étendus ou externalisé avec supervision partielle
- Audits réguliers sur des périmètres spécifiques (externe, AD, Cloud)
- Quelques exercices red / purple team

100 JH

5 RED TEAM

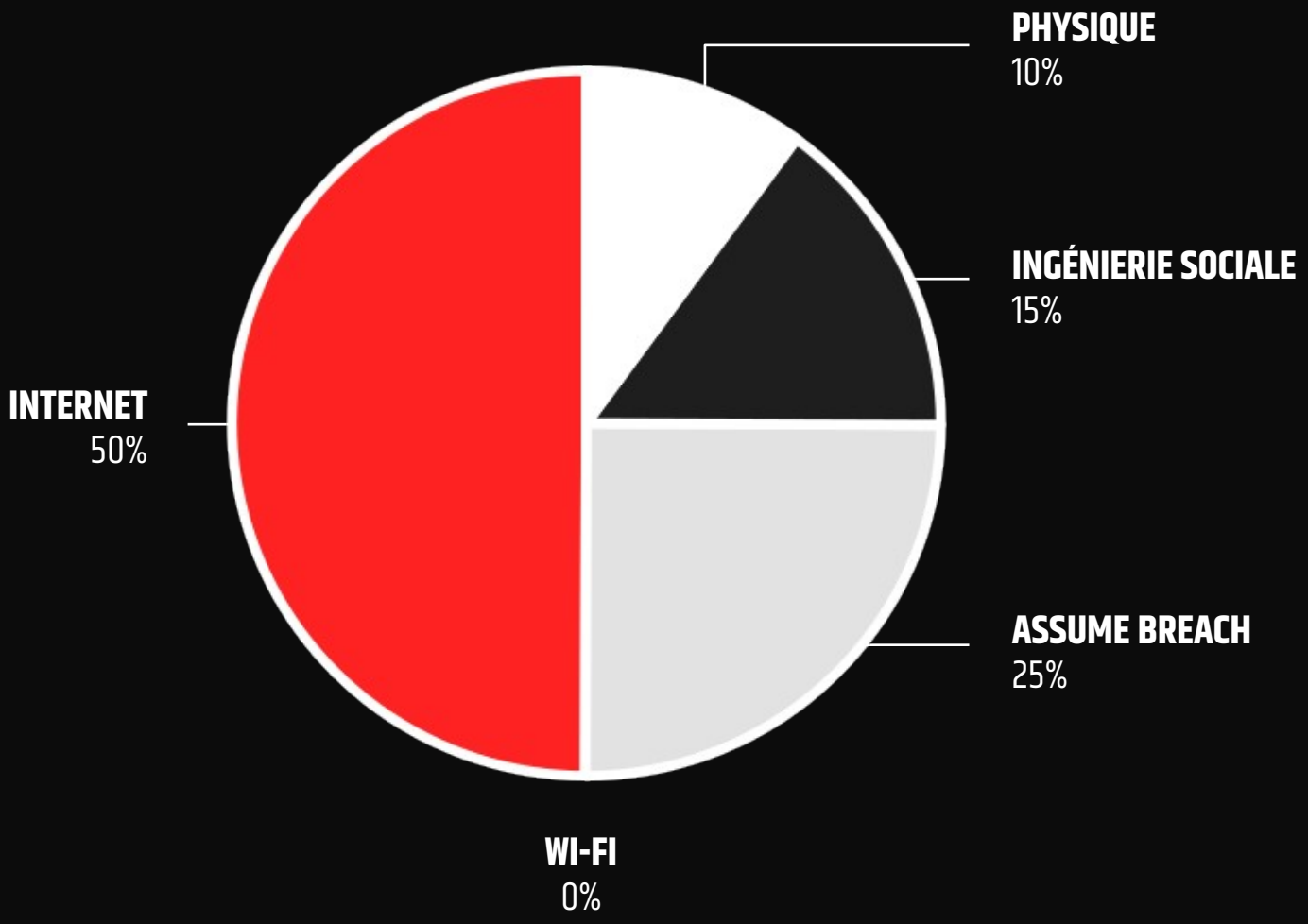
ENTITÉS MATURES AUX FORTS ENJEUX DE SÉCURITÉ

- Sécurité en profondeur (XDR, MFA, SmartCards, ZeroTrust)
- SOC 24/7 entraîné par des exercices purple réguliers
- Campagnes d'audits périodiques
- Red team annuel / semestriel

JH = Jours-Hommes

ACCÈS INITIAL

AUX RÉSEAUX D'ENTREPRISES



15 | **JOURS AVANT ACCÈS**

EN MOYENNE

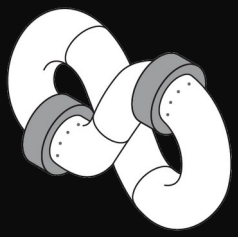
La compromission d'applications et de mots de passe demeure le principal vecteur d'accès initial, représentant 50 % des intrusions. L'ingénierie sociale et l'intrusion physique sont aussi impliquées, tandis que la sécurité Wi-Fi, désormais renforcée, reste un vecteur rare.

TENDANCES

VECTEURS D'ATTAQUE

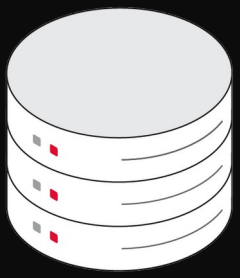
CONTOURNEMENT MFA

La compromission des mots de passe demeure une menace majeure en 2024, malgré l'adoption croissante de MFA. Cependant, de nombreuses failles de configuration dans les politiques d'accès permettent encore de contourner cette protection et d'accéder aux ressources critiques.



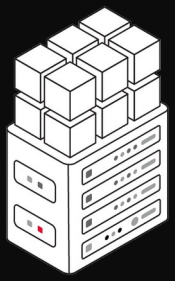
PIPELINES CI/CD

Les plateformes CI/CD telles que GitLab, GitHub et Azure DevOps gèrent des secrets critiques pour l'infrastructure, mais constituent souvent des angles morts en raison d'une faible visibilité sur leur cycle de vie. Ayant un rôle central, et une position réseau stratégique, elles deviennent les cibles privilégiées pour les attaquants les plus innovants.



SCCM / CONFIGMR & 0 DAYS

L'environnement SCCM rompt souvent le modèle d'architecture en 3 tiers, en gérant des ressources du tier 0. Cela a attiré l'attention de notre équipe et mené à la découverte d'une 0-day (CVE-2024-43468). Une fois compromis, SCCM offre de nombreuses opportunités de mouvement latéral et il est, malgré son rôle clé, fréquemment sous-surveillé.

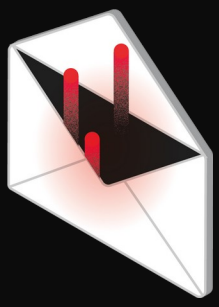


VSPHERE / HYPERVISORS

vSphere et ses équivalents sont de plus en plus ciblés, hébergeant des ressources du tier 0 comme les contrôleurs de domaine. Ils permettent d'extraire des données critiques et sont souvent sous-surveillés, avec peu d'intégration XDR ou de protection des identités. Les hyperviseurs offrent aussi des opportunités de mouvements latéraux, donnant accès à plusieurs réseaux et consoles, ce qui en fait une cible privilégiée.

TROPHÉES

LES PLUS MARQUANTS

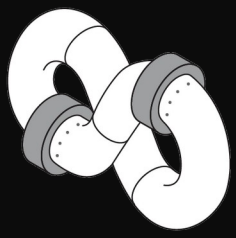


LIVRAISON DE PRODUITS

Faire livrer un produit pour 1€

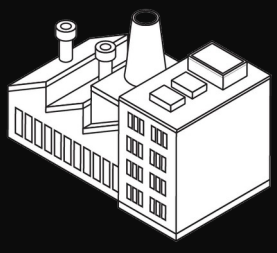
VOL D'ARGENT

Modifier un IBAN pour un virement



PUBLICATIONS LOGICIELLES

Modification du code publié via la CI/CD



SUPPLY CHAIN

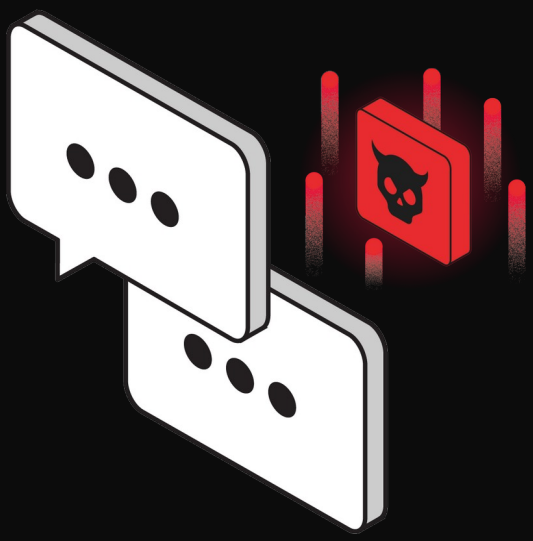
Accès initial via un fournisseur

RANSOMWARE

Alertes et simulation de ransomware

ÉTUDES DE CAS

INGÉNIERIE SOCIALE



USURPATION DU HELPDESK

Dans ce scénario, nous usurpons le support technique afin de convaincre la cible de changer son mot de passe. L'attaquant appelle en se faisant passer pour un agent du helpdesk, prétextant une activité suspecte sur le compte. Sous pression, la victime est poussée à réinitialiser son mot de passe via une application web malveillante. En jouant sur l'urgence et la confiance accordée au support, l'attaquant réduit la vigilance de la cible et obtient ses identifiants.

ÉTABLIR LA CRÉDIBILITÉ

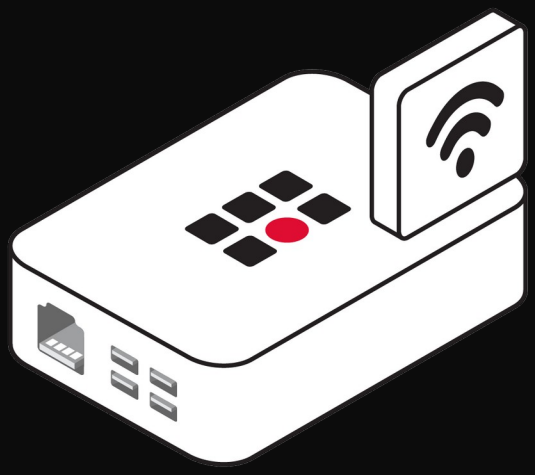
Faire vérifier l'agent usurpé dans l'annuaire et rappeler qu'on ne demande jamais de mot de passe au téléphone.

CONTOURNEMENT MFA

Contourner le MFA en utilisant un Agent-in-the-Middle pour capturer les sessions après l'authentification.

ÉTUDES DE CAS

INTRUSION PHYSIQUE



USURPATION DU PERSONNEL IT

Ce scénario s'est déroulé dans une zone industrielle, où un drone a été utilisé pour effectuer une reconnaissance des locaux de l'entreprise et observer les habitudes d'accès des employés. Le périmètre a été franchi en escaladant une clôture, avant d'approcher la réception en se faisant passer pour du personnel informatique, prétendant résoudre des problèmes réseau. Des polos de l'entreprise ont été portés pour renforcer la crédibilité. Un faux appareil de diagnostic a été installé à la réception, permettant en réalité un accès réseau à distance via 4G.

VÊTEMENTS OFFICIELS

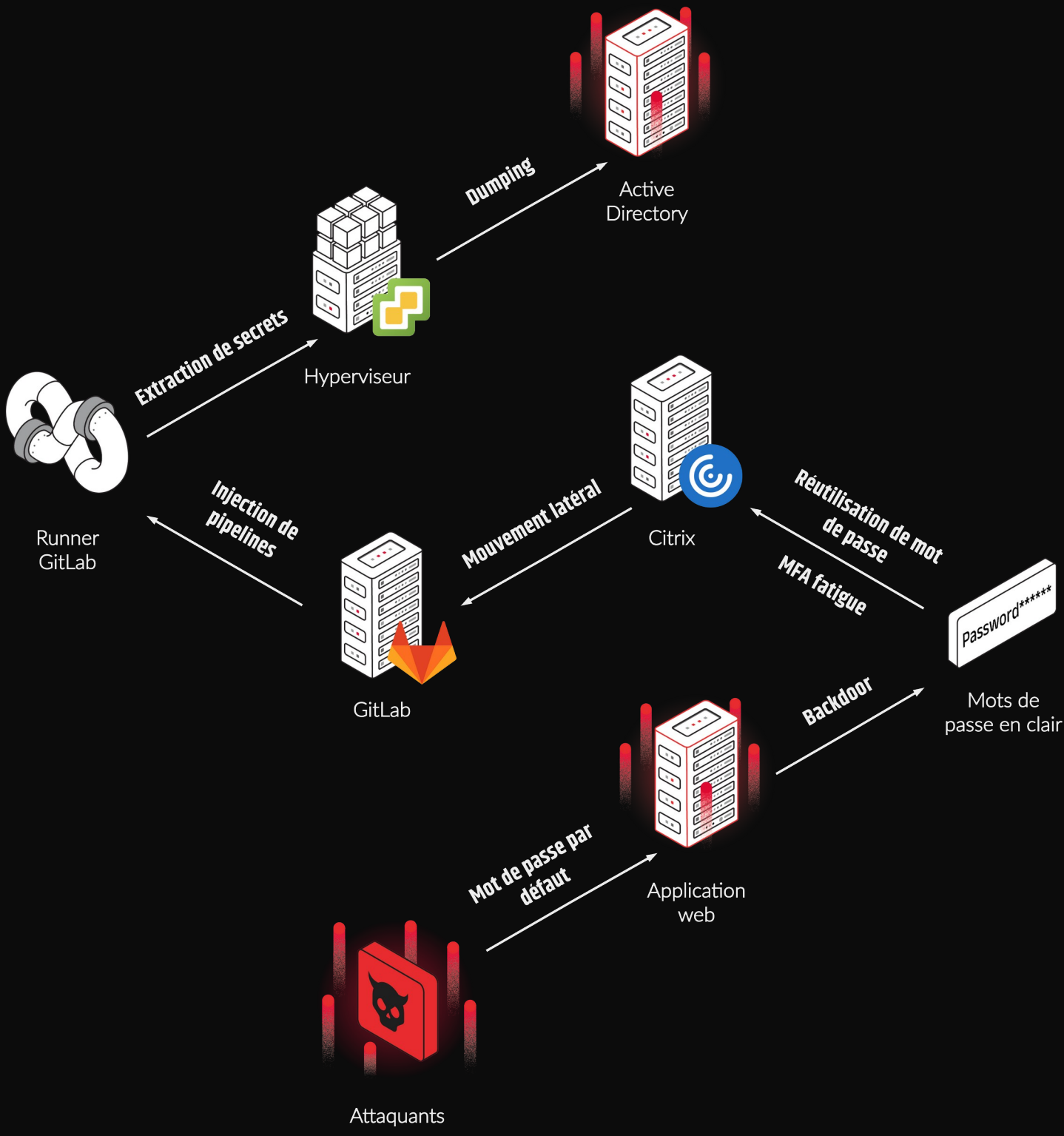
La crédibilité peut être renforcée en utilisant des articles achetés en ligne auprès d'anciens employés.

EXPLOITER LA CONFIANCE

L'accès aux zones non autorisées est généralement plus simple en abusant de la confiance qu'en forçant l'entrée.

ÉTUDES DE CAS

LIVING OFF THE LAND



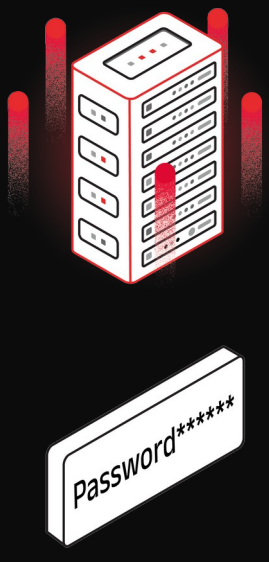
ÉTUDES DE CAS

LIVING OFF THE LAND

INTRODUCTION

Les derniers exercices red team montrent une évolution des stratégies d'attaque. Les méthodes traditionnelles — comme les attaques frontales sur l'Active Directory, la propagation via les protocoles SMB et RPC, ou le dump des secrets LSASS — sont devenues moins efficaces en raison du renforcement de la sécurité et de la surveillance. L'attention se porte donc davantage sur l'exploitation des angles morts, en abusant des applications collaboratives telles que SharePoint, Jira ou Confluence pour la collecte de secrets, des services tels que Citrix ou CyberArk pour les mouvements latéraux légitimes, et des plateformes critiques comme GitLab, SCCM ou les hyperviseurs en tant que points de rupture de cloisonnement. Ces tactiques de type Living Off The Land s'appuient sur les ressources internes de l'organisation, rendant la détection plus difficile et permettant aux attaquants de rester discrets.

Les étapes suivantes détaillent un scénario réel illustrant ces méthodes.



ACCÈS INITIAL

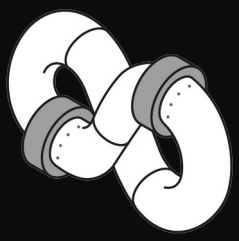
L'intrusion démarre par l'identification d'un mot de passe par défaut sur une interface d'administration d'une application Java, insuffisamment restreinte. En détournant les fonctionnalités natives de l'application, une backdoor est injectée en mémoire afin de réaliser des actions de post-exploitation comme le pivot réseau et l'interception de mots de passe, tout en contournant l'EDR.

ÉTUDES DE CAS

LIVING OFF THE LAND

MOUVEMENTS LATÉRAUX

Après la capture de plusieurs mots de passe, une instance Citrix est utilisée pour faciliter le mouvement latéral depuis le point d'entrée réseau. Bien qu'une authentification multi-facteurs soit configurée pour empêcher la réutilisation directe des identifiants compromis, des méthodes faibles comme les notifications push sans vérification de code ont été exploitées (MFA fatigue), permettant l'accès aux applications et VDI Citrix.



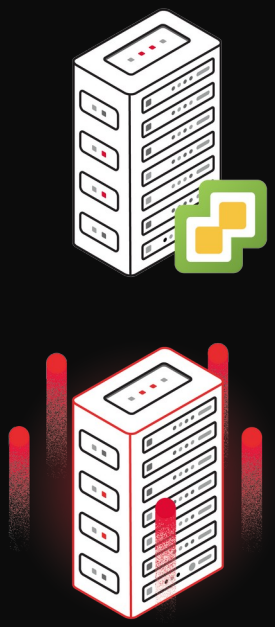
INJECTIONS DE PIPELINES CI/CD

Depuis Citrix, le service GitLab interne a été exploré à la recherche de secrets d'infrastructure. En exploitant les privilèges développeur sur plusieurs projets, les pipelines CI/CD ont été injectés et les runners GitLab compromis. Leur rôle critique dans le système d'information a permis l'extraction de secrets d'hyperviseurs et offert des opportunités d'accès réseau stratégiques.

ÉTUDES DE CAS

LIVING OFF THE LAND

HYPERVISEURS



Avec un accès privilégié aux hyperviseurs, les configurations ont pu être modifiées pour réduire la journalisation des événements, masquant ainsi les attaques suivantes. Les contrôleurs de domaine Active Directory ont été extraits afin de récupérer la base NTDS, donnant à l'attaquant un accès complet à l'ensemble des ressources fédérées par le domaine. Enfin, la manipulation du réseau et des machines virtuelles a permis un accès sans restriction au reste de l'infrastructure.

CONCLUSION

L'intrusion décrite dans ce scénario a duré plus d'un mois. Bien que des mesures de sécurité et de la surveillance étaient déjà en place, la nature discrète de ces attaques a permis de ne générer que des signaux faibles, rendant leur détection difficile. Dans ce contexte, plusieurs recommandations clés ont été proposées pour améliorer la posture de sécurité générale. Celles-ci incluent la mise en place du Single Sign-On (SSO) pour protéger les applications critiques, l'amélioration des mécanismes de détection pour le pivot réseau, le renforcement des configurations MFA, la révision de l'architecture de tiering, l'analyse approfondie de la segmentation et des configurations des runners GitLab, ainsi que le renforcement de la surveillance des hyperviseurs. En abordant ces points, les organisations pourront mieux se défendre contre de telles menaces et atténuer les risques associés à des intrusions subtiles et à long terme.

AU DELÀ

DU RED TEAM

SURFACE EXTERNE

Analyse approfondie
de la surface d'attaque

RÉSEAU INTERNE

Revue exhaustive
de l'Active Directory

PURPLE TEAM

Collaboration
entre les équipes red et blue

RED TEAM

Nouvelle itération
pour évaluer les améliorations

Le red teaming offre une évaluation réaliste de la posture de sécurité d'une organisation, mettant en lumière les angles morts à travers plusieurs vecteurs d'attaque. Cependant, pour améliorer encore la sécurité, les exercices de purple team et les audits ciblés, tels que ceux portant sur la surface externe, Active Directory, les environnements Cloud ou les pipelines CI/CD, sont essentiels. Ces audits viennent compléter les résultats du red team en couvrant de manière plus exhaustive les zones critiques, renforçant ainsi les actifs les plus importants.

CONTACT

SALES@SYNACKTIV.COM

Synacktiv

synacktiv.com

@Synacktiv