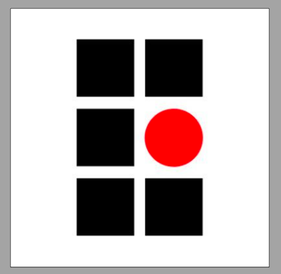
SYNACKTIV

25 novembre 2021

Retour d'expérience pour accélérer vos réponses aux incidents

A propos

Arnaud Pilon
Responsable activité réponse aux incidents
SYNACKTIV



- Responsable d’activité de traitement d’incidents

- Responsable de SOC

- Auditeur en sécurité & Tests d’intrusion

Synacktiv en quelques chiffres

Synacktiv
10 ans d'existence
100% française et indépendante

Croissance
12.2 millions de CA en 2020

Collaborateurs
90 passionnés
18 recrutements en 2020

R&D
45 publications en 2020
15% de la masse salariale

Missions
+ de 400missions réalisées en 2021

Locaux
4 bureaux régionaux
Paris
Rennes
Toulouse
Lyon

Reconnaissance
PASSI
CESTI
ANJ

Rétro-conception

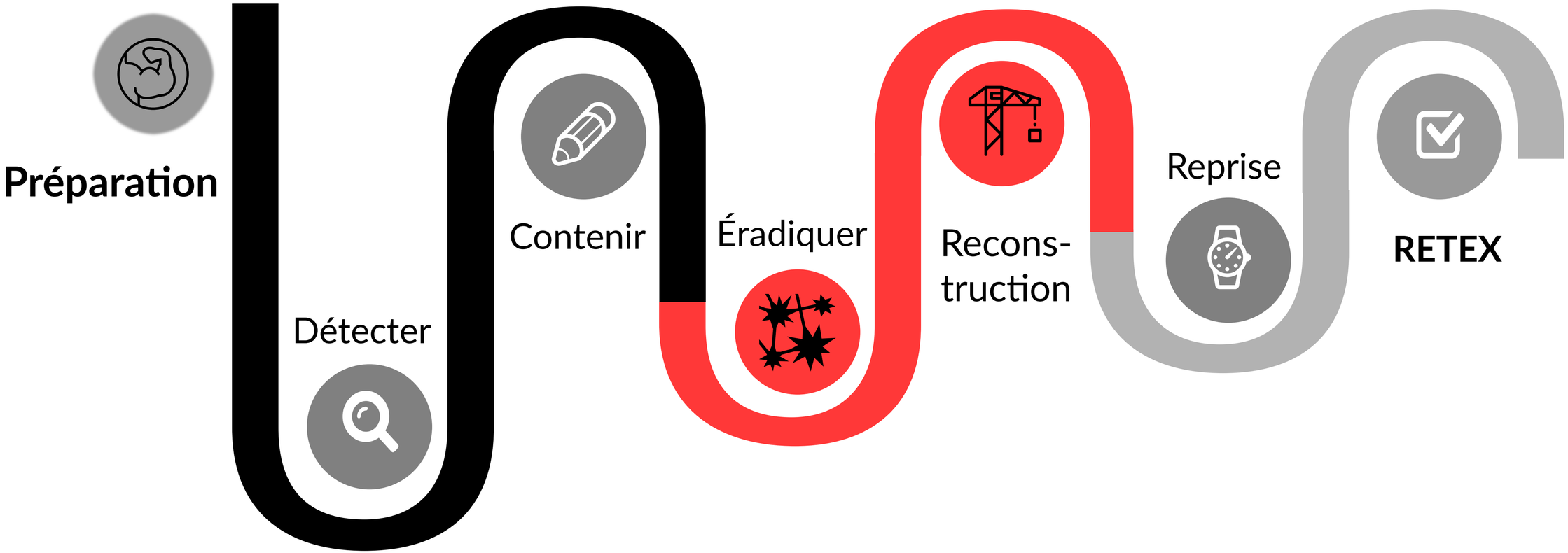
Tests d'intrusion

Dev. sécurité

Réponse aux incidents

Cycle de vie d'un incident

SANS Institute



Défiguration de site
Publicité détournée
SEO

Vol de données personnelles
Détournement de l'usage initial
Phishing

Espionnage
Prépostionnement
DDoS

Ransomware

Maturité des organisations face à un incident

- Configuration par défaut des outils (ex: aucune mise à jour)
- Pas d'équipe ou organisation sécurité
- Aucun outil de sécurité
- Pas de résistance à la crise
- Ne sais pas ce qui est externalisé ni où

- Possède une supervision
- Un savoir-faire, voir de l'expertise en interne
- Présence d'outils de sécurité
- Déjà expérimenté des situations de crise (pas forcément cyber)
- Hybride Cloud / Multi cloud

SYNACKTIV

- Possède un SOC / Outils-Equipe pour gérer la sécurité
- Déjà (sur)vécu à des incidents cyber => RETEX
- Capacité à mettre une organisation pour résoudre une crise
- Hybride Cloud / Multi cloud

Maturité des organisations face à un incident

Une entreprise n'est jamais complètement dans l'une ou l'autre de ces catégories

Cas particuliers des réseaux très vastes / hétérogènes

- Configuration par défaut des outils (ex: aucune mise à jour)
- Pas d'équipe ou organisation sécurité
- Aucun outil de sécurité
- Pas de résistance à la crise
- Ne sais pas ce qui est externalisé ni où

- Possède une supervision
- Un savoir-faire, voir de l'expertise en interne
- Présence d'outils de sécurité
- Déjà expérimenté des situations de crise (pas forcément cyber)
- Hybride Cloud / Multi cloud

- Possède un SOC / Outils-Equipe pour gérer la sécurité
- Déjà (sur)vécu à des incidents cyber => RETEX
- Capacité à mettre une organisation pour résoudre une crise
- Hybride Cloud / Multi cloud

Journaux

MEME utilisant une illustration
https://twitter.com/jkrillustration

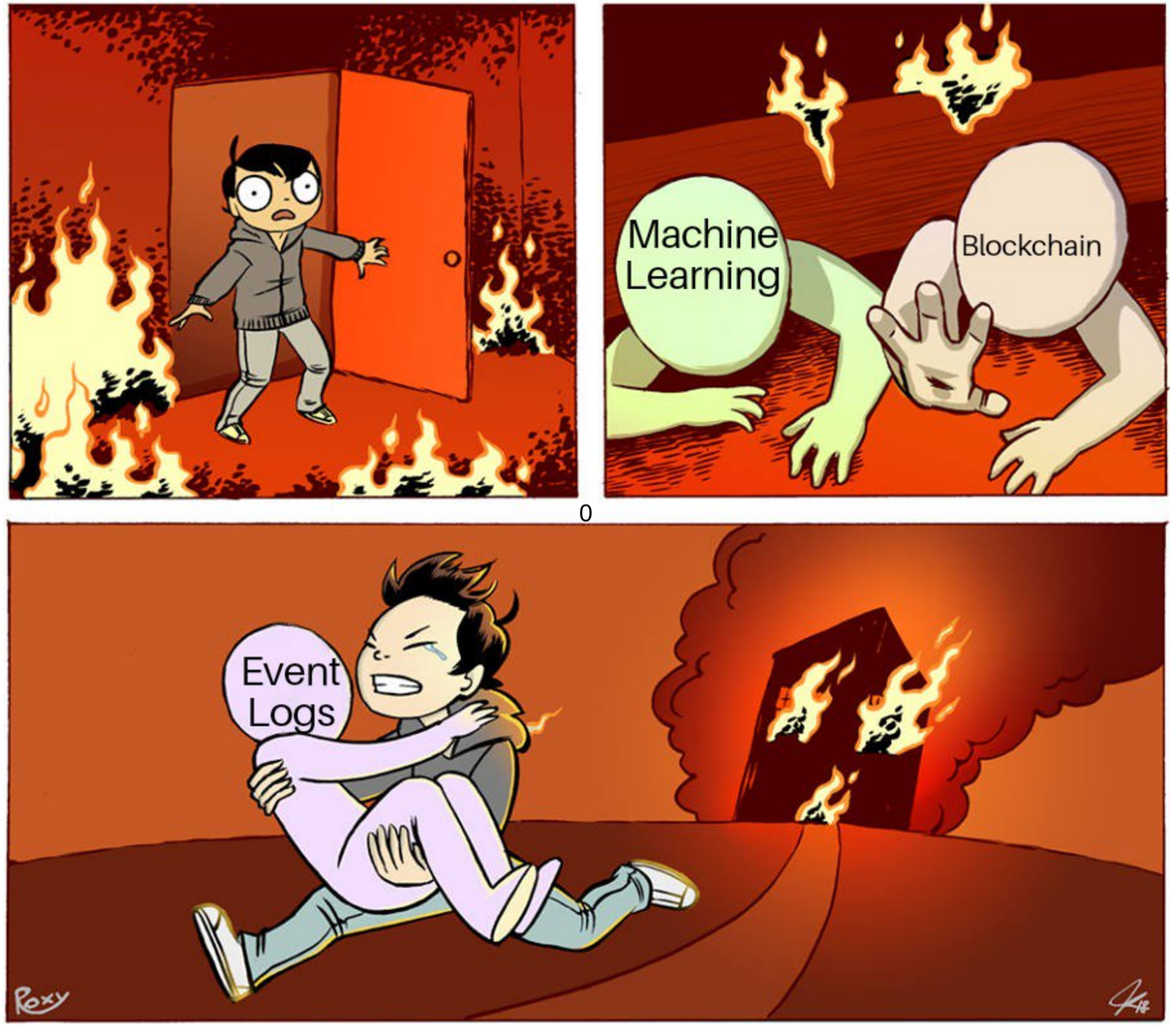
Journaux

Premier élément regardé : toutes(*) les attaques laissent des traces.

- ↣ Que se passe-t-il ?
- ↣ Depuis quand ?
- ↣ Quels impacts techniques/métiers ?
- ↣ Quel périmètre ?

- ↣ Que doit-on faire ? (pour rétablir la situation / pour ne plus que cela se reproduise)

.....Est-on sûr des résultats / interprétations ?



https://twitter.com/jkrillustration

Challenge autour des journaux

➔ Unification des journaux : dates (synchronisation/tz) et durée de rétention

- Éviter une mauvaise lecture / interprétation
- Équilibre entre sécurité / surveillance / risques / réalité technique
- Cas international / dispositifs externalisés

Challenge autour des journaux

➔ Unification des journaux : dates (synchronisation/tz) et durée de rétention

➔ Tous les journaux ne sont pas égaux devant un incident de sécurité : usage au bon moment / objectifs

FW	→	Périmètre à investiguer
Anti-malware	→	Signaux forts / Causalité
Journaux Windows	→	Privilège / Déplacement
Proxy	→	Périmètre à investiguer
Crash d'application	→	Tentative d'exploitation

Sysmon	→	Mode opératoire
Serveur messagerie	→	Destinataire du phishing
Supervision	→	Anomalie
Netflow	→	Volume échangé
VPN	→	Accès Externe

Challenge autour des journaux

➔ Unification des journaux : dates (synchronisation/tz) et durée de rétention

➔ Tous les journaux ne sont pas égaux devant un incident de sécurité : usage au bon moment / objectifs

FW → Périmètre à investiguer

Anti-malware → Signaux forts / Causalité

Journaux Windows → Privilège / Déplacement

Proxy → Périmètre à investiguer

Sysmon → Mode opératoire

Serveur messagerie → Destinataire du phishing

Supervision → Anomalie

Netflow → Volume échangé

Imprimante ? Routeur ? Téléphone ?

Challenge autour des journaux

➔ Unification des journaux : dates (synchronisation/tz) et durée de rétention

➔ Tous les journaux ne sont pas égaux devant un incident de sécurité

➔ “Puits” de journaux

- Difficulté à passer à l’échelle : sujet d’intégration SIEM x XDR x elk
- Bénéfices supplémentaires au quotidien : diagnostique des pannes plus rapide + meilleurs contrôles

Challenge autour des journaux

➔ Unification des journaux : dates (synchronisation/tz) et durée de rétention

➔ Tous les journaux ne sont pas égaux devant un incident de sécurité

➔ “Puits” de journaux

➔ Capacité à extraire certains journaux pour réaliser des traitements spécifiques

- Extraction dans des délais raisonnables (~ heure)
- Extraction exportable dans un format lisible (ex: clé/valeur)

Challenge autour des journaux

➔ Unification des journaux : dates (synchronisation/tz) et durée de rétention

➔ Tous les journaux ne sont pas égaux devant un incident de sécurité

➔ “Puits” de journaux

➔ Capacité à extraire certains journaux pour réaliser des traitements spécifiques

- Extraction dans des délais raisonnables (~ heure)
- Extraction exportable dans un format lisible (ex: clé/valeur)

➔ Intérêt exacerbé dans les situations d’urgence cas de DDoS ou de ransomware

(Mauvaises) pratiques d'administration

- ✘ Effacer les journaux
- ✘ Réinstaller un poste infecté avant l'analyse

  Retrouver des données effacées ou analyser des artefacts à la place de journaux prend du temps

- ✘ Un compte unique d'administration pour toutes les opérations
  - ➳ Question plus générale sur les pratiques d'administration : **décrire la normalité**

(Mauvaises) pratiques d'administration

- ✘ Effacer les journaux
- ✘ Réinstaller un poste infecté avant l'analyse

  Retrouver des données effacées ou analyser des artefacts à la place de journaux prend du temps

- ✘ Un compte unique d'administration pour toutes les opérations
  - ➳ Question plus générale sur les pratiques d'administration : **décrire la normalité**

➔ Action réflexe / Formation autour de la conduite à tenir

➔ Importance des exercices autour de mises en situation opérationnelle

Capacité à manoeuvrer durant un incident

- Déployer un agent type EDR / un programme de collecte / ...un SIEM – XDR - TIP

  SI trop complexe, trop de sous-traitants : personne ne sait vraiment comment adresser tout le SI

- Déployer une sonde en urgence (ou module de capture d'un FW)
  - Cas d'une attaque non comprise
  - le réseau ne ment pas :-)
- Modifier la configuration de son Firewall : flux / débit-qos

  Capacité à couper un prestataire (supply chain attack) / Couper Internet
  Limiter les communications d'un attaquant

- Contact (en urgence) des prestataires
  - Demander de l'aide
  - Ne pas être isolé du reste de vos partenaires
- Disposer de moyens d'échange sécurisé : fichiers ou messages

Focus sur les derniers arrivés dans le SI

Cloud

- Comprendre le niveau de souscription : couverture des offres de sécurité incluses
- Rétention des journaux (SaaS)
- Capacité (d'investigation) offerte par le prestataire de cloud : recherche / croisement (performance octroyée)
- Paramétrage par défaut

Focus sur les derniers arrivés dans le SI

Cloud

- Comprendre le niveau de souscription : couverture des offres de sécurité incluses
- Rétention des journaux (SaaS)
- Capacité (d'investigation) offerte par le prestataire de cloud : recherche / croisement (performance octroyée)
- Paramétrage par défaut

EDR

- Rétention des journaux (SaaS) : x mois / conservation d'un sous-ensemble de la télémétrie
- Capacité « Threat Hunting » / Réponse aux incidents à distance
- Connaitre les angles morts : zones non couvertes, vieux windows /linux/ imprimante/ cloud
- Paramétrage par défaut : type d'événement conservé/surveillé

Conclusion

- Un incident bien traité est un incident bien préparé
- Importance des mises en situation : pas seulement théorique ou orientée communication de crise (1/2 journée)
- Connaitre les capacités d’investigation offertes par son environnement (prestataire x produit)

https://www.linkedin.com/company/synacktiv
https://twitter.com/synacktiv
Nos publications sur : https://synacktiv.com

Cas des applications Web

- Difficulté à croiser les journaux de l'application / identité sur le réseau bureautique
  - SSO vs base locale
- Présence d'un Reverse Proxy / WAF / FW permet d'enrichir la chronologie des événements
  - Preuve de connexion
  - Volume échangé
- Journaliser certains types d'événements
  - Login / Logout
  - Opérations CRUD

- Rétention
  - Publication du 18/11/2021 :
    https://www.cnil.fr/sites/default/files/atoms/files/recommandation_-_journalisation.pdf