Une image contenant Graphique, capture d’écran, Police, graphisme

Description générée automatiquement

|  |
| --- |
| <CLIENT> |
| **Qualification d’incident** |
| **Diffusion : Confidentiel** |

|  |
| --- |
| Auteur : <AUTEUR>  09/02/2024 |

Maitrise du document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Classification | | Public [ ] – **Restreint [X]** – Diffusion Restreinte [ ]– Secret [ ] | | |
| Référence | | **PRO-AVV-PRIS-01-Formulaire de qualification de réponse aux incidents** | | |
| Propriétaire | | Jonathan MERESSE | | |
| Destinataires | | Les clients d’APIXIT et les collaborateurs du pôle AUDIT et CONSEIL | | |
| Historique des mises à jour | | | | |
| Version | Auteur | | Date | Description de la mise à jour |
| V0.1 | Jonathan MERESSE | | 09/02/2024 | Première version |
| V0.2 | Jean OUDOT | | 25/07/2024 | Ajout de la partie Maitrise du document |
| V0.3 | Jean OUDOT | | 13/01/2025 | Simplification du document client |

# ***Une image contenant symbole Description générée automatiquementUne image contenant symbole Description générée automatiquement*Compréhension de l’incident**

Noter les premiers éléments essentiels.

**Objectif**

**Contexte**

***Une image contenant symbole

Description générée automatiquement***

**Réglementation applicable, SIIV, contraintes métier et/ou techniques, sous-traitance, etc, ainsi que la localisation géographique**

* Exemple : Pas de backup disponible
* Exemple : Service essentiel à l’activité de l’entreprise
* Etc …
* **<Client> souhaite une investigation numérique pour :**
  + Identifier le point d'entrée utilisé par l'attaquant pour sécuriser l'accès et prévenir toute récidive.
  + Déterminer les motivations de l'attaquant afin de comprendre pleinement l'ampleur de l'impact.
  + Tenter d’identifier les traces de persistance mis en place par l'attaquant pour éliminer le risque d'une récidive.
  + Objectif 4
* **Complément**
  + **Complément 1**

**Contrainte(s)**

**Périmètre**

***Une image contenant symbole

Description générée automatiquement*t**

Le périmètre impacté ne montre aucun écart dans le protocole de temps réseau (NTP) ? :

* Oui
* Non

Si « Non », merci de préciser le nom des équipements ayant un écart dans le NTP : Asset 1, Asset2, Etc …

**Périmètre**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| TYPE | VERSION | NOM DE L’EQUIPEMENT | IP/DNS | FONCTIONS | TIME ZONE |
| **Serveur** | **Exemple :** Windows serveur 2019 | **Exemple :** AD-01 | **Exemple :** 10.10.10.1 | **Exemple :**   * AD * DHCP * DNS | **Exemple : GMT+1** |
| Choisissez un élément. |  |  |  |  |  |
| Choisissez un élément. |  |  |  |  |  |
| Choisissez un élément. |  |  |  |  |  |
| Choisissez un élément. |  |  |  |  |  |
| Choisissez un élément. |  |  |  |  |  |

**Actions client**

|  |  |
| --- | --- |
| Heure | Action |
|  | Lister les actions cliente ayant été effectuées à la suite de la découverte de la compromission et avant l’appel vers le CSIRT Apixit |
|  | Lister les actions cliente ayant été effectuées à la suite de la découverte de la compromission et avant l’appel vers le CSIRT Apixit |

***Une image contenant symbole

Description générée automatiquement***

**Liste des actions**

|  |  |  |
| --- | --- | --- |
| IOC | ACTION SUR L’IOC | DETAILS |
| **Exemple :** TeamViewer | **Exemple :** Suppression de l’application le 01/01/2024 par <nom utilisateur> | **Exemple :** TeamViewer n’est pas utilisé sur le SI. |
|  |  |  |
|  |  |  |
|  |  |  |

**INDICES DE COMPROMISSION**

***Une image contenant symbole

Description générée automatiquement***

**IOC**

Un IOC, qu'il s'agisse d'un malware ou d'un logiciel non conforme à la politique desécurité de l'entreprise, est un indice technique révélateur d'une possible compromission du système informatique par une menace ou d'une utilisation non autorisée de logiciels

# **Communication**

***Une image contenant symbole

Description générée automatiquement***

**Contacts**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Apixit | | | <Client> | | |
| Nom | Mail/téléphone | Rôle | Nom | Mail/téléphone | Rôle |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |