CLASSIFICATION DES INCIDENTS	EXEMPLES D'INCIDENTS	DESCRIPTION	Temps de réponse max	Priorité
Contenu abusif	Pourriel (SPAM)	E-mails non sollicités et dont le destinataire n'a pas accordé une autorisation vérifiable pour l'envoi du message.	48 Heures	Faible
	Discours nuisible	Discréditation ou discrimination à l'égard de quelqu'un (ex : cyberharcèlement, racisme et menaces à l'encontre d'une ou plusieurs personnes)	24 Heures	Moyenne
	Enfant / Sexuel / Violence /...	Pornographie juvénile/Pédopornographie, promotion de la violence ...	6 Heures	Très élevée
Code malicieux	Virus/ ver / Cheval de Troie	Logiciel qui est intentionnellement inclus ou inséré dans un système à des fins nuisibles. Une interaction de l'utilisateur est normalement nécessaire pour activer le code.	12 Heures	Elevé
	Ransomware		12 Heures	Elevé
	Rootkit / Backdoor		12 Heures	Elevé
	Logiciel Espion		12 Heures	Elevé
La collecte illégale d'informations	Balayage (scanning)	Envoi de requête à un système pour en découvrir les points faibles. Cela inclut également certains types de processus de test visant à recueillir des informations sur les hôtes, les services et les comptes.	48 Heures	Faible
	Analyseur de Paquets (sniffing)	Enregistrement et analyse du trafic réseau (écoutes téléphoniques).	24 Heures	Moyenne
	Ingénierie Sociale	Lorsqu'une personne recueil des informations auprès d'une autre en employant une manière non technique (par ex. mensonges, ruses, pots-de-vin ou menaces).	48 Heures	Faible
Tentatives d'intrusion	Exploitation de vulnérabilités connues	Compromission ou perturbation d'un système ou un service en exploitant des vulnérabilités avec un identifiant standardisé tel que le CVE, etc.	12 Heures	Elevé
	Tentatives de connexion	Tentatives de connexion multiples (craquer les mots de passe, brute force).	12 Heures	Elevé
	Nouvelle signature d'attaque	Une tentative utilisant un exploit inconnu.	6 Heures	Très élevée
Les intrusions	Compromis de compte privilégié	Une compromission réussie d'un système ou d'une application (service). Cela peut être causé à distance par une vulnérabilité connue ou nouvelle, mais aussi par un accès local non autorisé. Comprend également le fait de faire partie d'un réseau de BOTNET.	6 Heures	Très élevée
	Compromis de compte sans privilèges		12 Heures	Elevé
	Compromis d'application		12 Heures	Elevé
	Bot		24 Heures	Moyenne
Atteinte à la disponibilité	Attaque par déni de service (DOS)	Envoi massif de paquets conduisant au retardement des opérations ou au crash du système Les attaques par déni de service distribué sont souvent basées sur des attaques par déni de service provenant de bots informatiques, mais il existe également d'autres scénarios comme les attaques par amplification DNS. Cependant, la disponibilité peut également être affectée par des actions locales (destruction, interruption de l'alimentation électrique, etc.) - ou par un cas de force majeure, des défaillances spontanées ou une erreur humaine, sans qu'il y ait malveillance ou négligence.	12 Heures	Elevé
	Attaque par déni de service distribué (DDoS)		6 Heures	Très élevée
	Sabotage			
	Panne (sans malveillance)		48 Heures	Faible
Sécurité de l'information	Accès non autorisé à l'information	Utilisation locale abusive des données et des systèmes, résultant sur une compromission réussie d'un compte ou d'une application. De plus, il est possible que des attaquants interceptent et accèdent aux informations pendant leur transmission (écoutes téléphoniques, usurpation d'identité ou détournement). Une erreur humaine / de configuration / logicielle peut également en être la cause.	48 Heures	Faible
	Modification non autorisée des informations		48 Heures	Faible
Fraude	Utilisation non autorisée des ressources	Utilisation de ressources à des fins non autorisées, y compris des entreprises à but lucratif (par exemple, l'utilisation du courrier électronique pour participer à des chaînes de lettres illégales ou à des systèmes pyramidaux).	48 Heures	Faible
	Droits d'auteur	Offrir ou installer des copies de logiciels commerciaux sans licence ou d'autres matériels protégés par le droit d'auteur (Warez).	48 Heures	Faible

	Usurpation d’identité	Type d'attaques dans lesquelles une entité prend illégalement l'identité d'une autre afin d’en tirer profit.	48 Heures	Faible
	Hameçonnage	Se faire passer pour une autre entité afin de persuader l'utilisateur de révéler un identifiant privé.	24 Heures	Moyenne
Actifs vulnérables	Ouvert aux abus	Résolveurs ouverts, imprimantes lisibles dans le monde entier, vulnérabilité apparente des scans Nessus, etc., signatures de virus non mises à jour, etc.	48 Heures	Faible