Matrice de communication Mini SOC AEGIS – DUNDER MIFFLIN, INC

1. ENGAGEMENTS DE SERVICE ET SLA

Sévérité	SLA Notification	SLA Qualification	SLA Investigations complémentaires
LOW	N/A	12h	N/A
MEDIUM	N/A	8h	N/A
HIGH	2h	4h	72h
CRITICAL	2h	4h	72h

Note : Le non-respect des SLA pourra, s'il n'est pas jugé justifié par le client, engendrer un malus sur la note de service.

2. MATRICE DE COMMUNICATION PAR SÉVÉRITÉ

INCIDENT CRITICAL

Délai de notification : 2 heures maximum (pour toute intrusion avérée)

Délai de qualification : 4 heures (première version du rapport d'investigation)

Délai investigation complémentaire : 72 heures

Parties prenantes concernées :

- VIPs (Regional Manager + Assistant to Regional Manager)
- AD-Admins (J.Halpert, R.Howard + VIPs)
- Servers-Admins (A.Martin, K.Kapoor, A.Bernard)
- Manager SOC MSSP

Canaux de communication :

- Téléphone (appel direct si situation urgente)
- Email vers conversation Teams dédiée aux sollicitations client
- Portail client (mise à jour temps réel du statut)

Contenu de la notification (sous 2h) :

- Brève synthèse de l'investigation en cours
- Nature de l'intrusion détectée
- Périmètre potentiellement affecté
- Actions immédiates entreprises par le SOC
- Prochaines étapes prévues

Contenu du rapport de qualification (sous 4h) :

- Première synthèse justifiant la qualification de l'incident
- Timeline des événements identifiés
- Analyse technique préliminaire
- Indicateurs de compromission (IOCs)
- Actions de containment appliquées
- Recommandations immédiates

Contenu du rapport complémentaire (sous 72h) :

- Éléments d'investigation supplémentaires
- Analyse root cause approfondie
- Support pour cellule de crise si activée
- Plan de remédiation complet
- Recommandations de sécurisation

Exemples d'incidents CRITICAL :

- Ransomware actif sur le SI
- Compromission de contrôleur de domaine
- Exfiltration de données confirmée
- Mouvement latéral d'un attaquant
- Backdoor persistant identifié

INCIDENT HIGH

Délai de notification : 2 heures maximum

Délai de qualification : 4 heures (première version du rapport)

Délai investigation complémentaire : 72 heures

Parties prenantes concernées :

- Desktop-Admins (Dev-DevOps : P.Beesly, P.Vance, O.Martinez, S.Hudson)
- Servers-Admins si infrastructure concernée
- Manager SOC MSSP
- Contact technique principal client

Canaux de communication :

- Email vers conversation Teams dédiée
- Portail client
- Téléphone si nécessaire

Contenu de la notification :

- Description de la menace détectée
- Systèmes ou comptes potentiellement impactés
- Actions de détection et réponse initiées

Contenu du rapport de qualification :

- Analyse technique de l'incident
- Périmètre d'impact confirmé
- IOCs identifiés
- Actions correctives recommandées
- Évaluation du risque résiduel

Exemples d'incidents HIGH :

- Malware détecté sur postes de travail
- Tentative d'élévation de privilèges
- Compte privilégié compromis
- Exploitation de vulnérabilité critique
- Activité anormale sur serveur critique

INCIDENT MEDIUM

Délai de qualification : 8 heures

Parties prenantes concernées :

- Contact technique concerné (Desktop-Admins ou Servers-Admins selon périmètre)
- Analyste SOC en charge

Canaux de communication :

- Email
- Portail client
- Conversation Teams dédiée

Contenu de la communication :

- Description de l'alerte et contexte
- Analyse de corrélation effectuée
- Recommandations de sécurisation
- Actions suggérées

Exemples d'incidents MEDIUM :

- Comportement suspect isolé

- Violation de politique de sécurité
- Scan de vulnérabilité détecté
- Tentative de phishing ciblée

INCIDENT LOW

Délai de qualification : 12 heures

Parties prenantes concernées :

- Contact technique client (Desktop-Admins ou Servers-Admins)
- Analyste SOC N1

Canaux de communication :

- Email notification automatique
- Portail client

Contenu de la communication :

- Notification standardisée de l'événement
- Contexte et règle de détection
- Consolidation dans rapports périodiques

Exemples d'incidents LOW :

- Alerte de corrélation informative
- Événement de sécurité bénin
- Tentative de connexion échouée répétée

3. FLUX DE COMMUNICATION ET ESCALADE

Règles d'escalade :

Niveau 1 - Analyste SOC N1

Rôle : Détection, triage initial, qualification de base

Délai d'action : Immédiat (monitoring 24/7)

Escalade vers N2 : Si incident MEDIUM ou supérieur

Niveau 2 - Analyste SOC N2

Rôle : Investigation approfondie, corrélation, containment

Délai d'intervention : 30 minutes maximum

Escalade vers N3 : Si incident HIGH ou CRITICAL

Niveau 3 - Expert SOC N3

Rôle : Analyse forensique, remédiation avancée, threat hunting

Délai d'intervention : 1 heure maximum

Escalade vers Manager : Tous incidents CRITICAL

Manager SOC

Rôle : Coordination, décision stratégique, interface client VIP

Intervention : Systématique sur incidents CRITICAL

4. CANAUX DE COMMUNICATION

Conversation Teams dédiée aux sollicitations client

Usage : Canal principal pour toutes notifications et rapports

Participants : Équipes SOC MSSP + Admins client concernés selon périmètre

Disponibilité : 24/7

Avantages : Traçabilité, historique, collaboration en temps réel

Email

Usage : Notifications formelles, rapports structurés

Format : Selon templates définis par sévérité

SLA réponse : Selon niveau de sévérité

Téléphone

Usage : Incidents CRITICAL en phase urgente uniquement

Numéro d'astreinte SOC : [À COMPLÉTER]

Disponibilité : 24/7

Portail client sécurisé

Usage : Consultation statut incidents, rapports historiques, KPIs

Accès : Selon profils AD Groups

Mise à jour : Temps réel

5. GESTION DE CRISE (INCIDENTS CRITICAL)

Activation cellule de crise

Déclenchement : Décision Manager SOC en accord avec VIPs client

Composition :

- Manager SOC MSSP (coordinateur)
- Expert N3 SOC
- Regional Manager (M.Scott)
- AD-Admins concernés
- Servers-Admins si infrastructure impactée

Communication en mode crise

- Point de situation : Toutes les 2 heures minimum
- Canal dédié : Conférence Teams permanente
- Mise à jour rapport : Continue (toutes les 4h minimum)
- Synthèse exécutive : Toutes les 6 heures vers VIPs

Sortie de crise

- Debriefing post-incident : Sous 48h après résolution
- Rapport final détaillé : Sous 72h (SLA investigations complémentaires)
- Lessons learned : Partagées avec toutes parties prenantes
- Plan d'action correctif : Validé conjointement

6. INDICATEURS DE PERFORMANCE

KPIs de communication suivis mensuellement :

- Taux de respect des SLA notification (objectif : 100%)
- Taux de respect des SLA qualification (objectif : 100%)
- Taux de respect des SLA investigations complémentaires (objectif : 100%)
- Délai moyen de première réponse par sévérité
- Taux de satisfaction client sur la qualité de communication
- Nombre d'escalades tardives (objectif : 0)

Ces indicateurs sont reportés dans le rapport mensuel exécutif et discutés lors des QBR.

7. POINTS DE CONTACT

Côté SOC MSSP :

- SOC 24/7 : [email à compléter] | [téléphone à compléter]
- Manager SOC : [email à compléter] | [téléphone à compléter]
- Astreinte urgence : [téléphone 24/7 à compléter]

Côté Client (selon AD Groups) :

- VIPs : M.Scott (Regional Manager), D.Schrute (Assistant)
- AD-Admins : J.Halpert, R.Howard
- Servers-Admins : A.Martin, K.Kapoor, A.Bernard
- Desktop-Admins (Dev-DevOps) : P.Beesly, P.Vance, O.Martinez, S.Hudson

8. RÈGLES ESSENTIELLES

Communication proactive

Le SOC communique systématiquement selon les SLA sans attendre de sollicitation client.

Transparence totale

Toute information pertinente, même défavorable, est communiquée au client dans les délais impartis.

Adaptation du message

Le niveau de détail technique est adapté à l'interlocuteur (VIPs vs Admins techniques).

Traçabilité complète

Toutes les communications sont documentées dans la conversation Teams dédiée et le portail client.

Respect strict des SLA

Les délais contractuels sont impératifs. Tout risque de dépassement est escaladé immédiatement en interne.

Confidentialité

Les informations d'incident sont partagées uniquement avec les AD Groups concernés selon le principe du besoin d'en connaître.

Document à valider conjointement entre le SOC et le client.

Version applicable à compter de : 3.12.2025

Prochaine revue prévue : 3.05.2026