

Table décisionnelle SOC (1 page) — CVE-2025-62221 (UTILISATEUR → SYSTEM)

Date: 2025-12-22

■ Incident confirmé

Règle : (1 OUI) + (au moins un parmi 3 / 4 / 5 / 7 OUI)

Explication : Élévation UTILISATEUR → SYSTEM confirmée et au moins un signe d'exploitation active observé (persistance, vol d'identifiants, communication externe ou propagation).

Action : Containment immédiat

■ Incident probable

Règle : (1 OUI) + (2 OU 6 OUI)

Explication : Élévation UTILISATEUR → SYSTEM confirmée, mais seulement des indices préparatoires (binaire suspect ou payload sur disque) sans exploitation active observée.

Action : Containment conditionnel + collecte de preuves

■ Faux positif confirmé

Règle : (1 NON) OU (outil IT légitime + preuve de change)

Explication : Le signal est expliqué par un outil IT/maintenance documentée, ou l'élévation n'est pas confirmée.

Action : Clôture FP + tuning

■ Mémo rapide SOC

- Incident confirmé = SYSTEM obtenu et utilisé
- Incident probable = SYSTEM obtenu mais pas encore utilisé