SOC Decision Table (1 page) — CVE-2025-62221 (USER ➜ SYSTEM)

Date: 2025-12-22

🟥 Confirmed Incident

Rule: (Check 1 = YES) + (at least one of Checks 3 / 4 / 5 / 7 = YES)
Explanation: USER ➜ SYSTEM escalation is confirmed and at least one active exploitation sign is observed (persistence, credential access, outbound communication, or propagation).
Action: Immediate containment

🟧 Probable Incident

Rule: (Check 1 = YES) + (Check 2 OR Check 6 = YES)
Explanation: USER ➜ SYSTEM escalation is confirmed, but only preparatory indicators exist (suspicious binary or payload on disk) with no active exploitation observed yet.
Action: Conditional containment + evidence collection

🟩 Confirmed False Positive

Rule: (Check 1 = NO) OR (legitimate IT tools + change evidence)
Explanation: The signal is explained by documented IT tooling/maintenance, or escalation is not confirmed.
Action: Close FP + tuning

■ SOC Quick Reminder

- Confirmed Incident = SYSTEM obtained and actively used
- Probable Incident = SYSTEM obtained but not yet used