

# SOC lab – Brute Force Attempt Incident Report

Emma

August 18<sup>th</sup>, 2026

## Incident Report

**Date of Incident:** August 17<sup>th</sup>, 2026

**Type of Incident:** Physical Breach, Remote Access Attempt, Brute Force Attempt

**Description of Event:** At 6:45pm CST we identified multiple failed login attempts against our Domain Controller at 192.168.122.241 and physical attempts at Workstations A and B. Totaling 104 attempts between 6:45pm and 7:30pm CST.

**Detection:** Wazuh SIEM System

**Action Taken:** Required all users to change passwords, blocked external device IP 192.168.122.113. This IP was identified as an unauthorized device on our network. Multiple physical login attempts were logged on Workstations A and B, so we advised stricter physical security implementations.