Executive Briefing - SOC Capstone Project

Date: September 29, 2025

✔ Attack simulated: Samba exploitation (T1210)

✔ Detection time: <1 second (vs industry avg 280s)

✔ Response time: 72.75 minutes (vs industry avg 73.5 days)

✔ 100% detection rate, 0 false positives

✔ SOAR automation: CrowdSec IP blocking

✔ Case tracking: TheHive Case #3

✔ Critical gap identified: lack of network segmentation

Conclusion: SOC exercise demonstrated world-class detection and response with actionable recommendations for strengthening training lab security.