Executive Briefing

On 2025-08-18 a simulated attack was detected and contained by the SOC during a capstone exercise. Key metrics: MTTD 2 hours, MTTR 4 hours, no production data impacted. Actions: automated playbook blocked malicious IPs, SOC analysts isolated affected VM, and escalation procedures were executed. Recommendations: invest in enhanced email filtering, expand threat feed integration, and apply playbook updates to shorten response time. This simulation demonstrates current SOC capabilities and provides a roadmap for targeted improvements to reduce business risk.