Stakeholder Briefing

On Feb 27, 2026, abnormal login activity was detected against an SSH service in the lab environment. Centralized monitoring in Elastic helped surface the activity quickly, and the team confirmed it as suspicious. A containment action was executed using CrowdSec to block the source, and the block was verified immediately.

On Feb 28, 2026, a controlled security test demonstrated that additional exposed services (Samba) on the target system were vulnerable. Using a standard security testing framework, the team was able to obtain remote access, showing that leaving legacy services exposed can lead to full compromise.

Performance metrics for the Feb 27 response were strong:
Detection: ~1 minute
Response: ~5 minutes
Total attacker window before containment: 5 minutes 30 seconds

Recommended improvements include restricting administrative access (SSH), applying secure baseline configurations, and reducing exposed services to minimize attack surface.