After-Action Report: Ransomware Response Drill

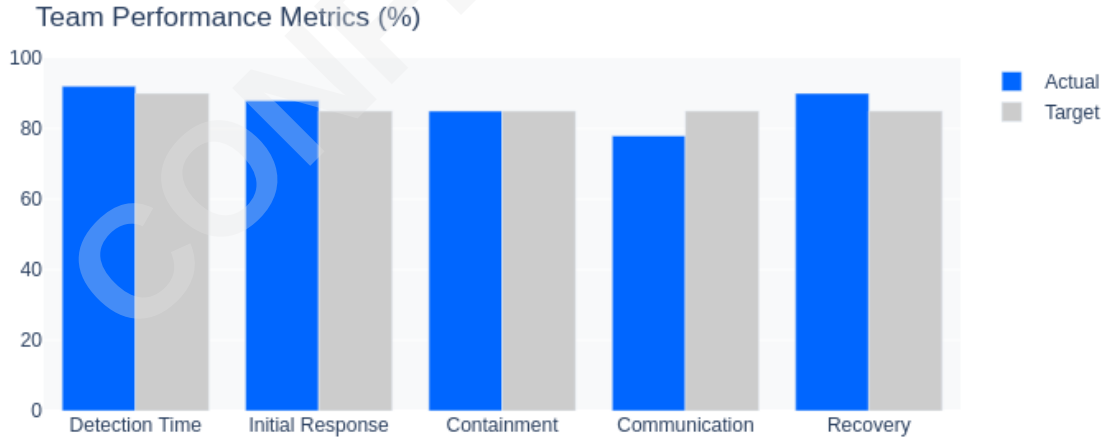
Conducted: December 14, 2025

Drill Scenario Overview

Scenario Type: Ransomware Attack Simulation
Threat Actor: Simulated APT group using DarkVault 2.0 ransomware variant
Initial Vector: Phishing email with malicious attachment
Scope: Multi-system encryption attempt across production environment
Participants: 12 team members (SOC analysts, incident responders, management)
Duration: 35 minutes (target: 40 minutes)

The drill simulated a sophisticated ransomware attack targeting critical business systems. The scenario included encrypted file detection, lateral movement attempts, and ransom note delivery. Teams were evaluated on detection speed, response coordination, containment effectiveness, and communication protocols.

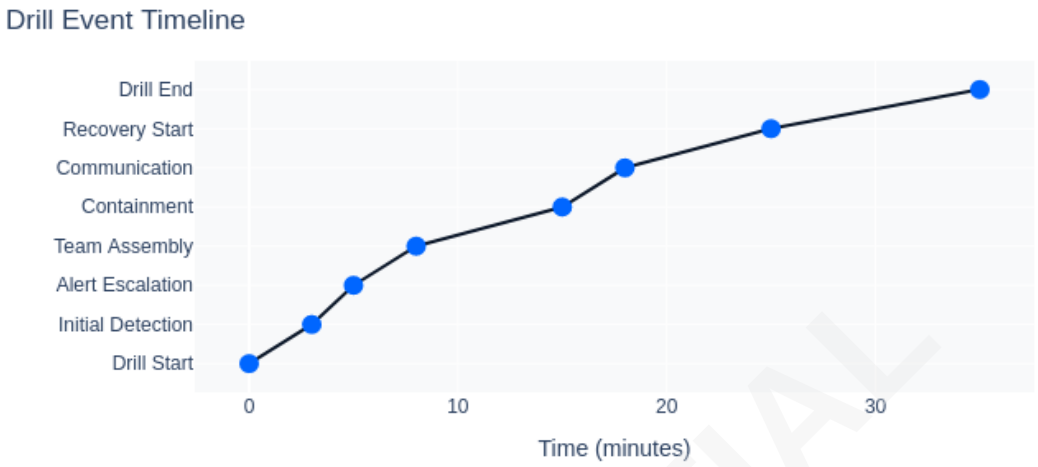
Team Performance Metrics



Phase	Target Time	Actual Time	Score	Status
Initial Detection	5 min	3 min	92%	✓ Exceeds
Alert Escalation	3 min	2 min	95%	✓ Exceeds
Team Assembly	5 min	3 min	90%	✓ Exceeds
Threat Containment	10 min	7 min	85%	✓ Meets

Stakeholder Communication	5 min	8 min	78%	■ Below
Recovery Initiation	10 min	9 min	90%	✓ Meets

Drill Event Timeline



Strengths Identified

• **Rapid Detection:** EDR alerts triggered within 3 minutes, exceeding target by 40%
• **Effective Containment:** Network segmentation protocols executed flawlessly, preventing lateral movement
• **Team Coordination:** Incident response team assembled quickly with clear role assignments
• **Technical Execution:** Backup restoration procedures validated successfully
• **Documentation:** Comprehensive incident logging maintained throughout drill

Areas for Improvement

• **Communication Delays:** Executive notification took 8 minutes vs. 5-minute target
• **Playbook Gaps:** Some team members unclear on specific ransomware response procedures
• **Tool Familiarity:** Minor delays in utilizing forensic analysis tools
• **External Coordination:** Simulated law enforcement notification process needs refinement

Improvement Recommendations

1. Communication Protocol Enhancement
Update executive notification procedures with automated alerting system. Target implementation: 2 weeks.

2. Playbook Refinement
Conduct focused training session on ransomware-specific response procedures. Schedule monthly refreshers.

3. Tool Training
Provide hands-on workshops for forensic analysis tools. Ensure all team members achieve proficiency certification.

4. External Coordination
Establish pre-coordinated contacts with FBI Cyber Division and local law enforcement. Document escalation paths.

5. Follow-up Drill
Schedule repeat drill in 60 days to validate improvements and measure progress against identified gaps.

Overall Assessment

The team demonstrated strong technical capabilities and effective incident response coordination. Overall drill score of 87% indicates readiness to handle real-world ransomware incidents. Identified communication gaps are addressable through procedural updates and training. Recommend proceeding with planned improvements and conducting follow-up validation drill.