Formula 1

Content placeholder

Formula 2

Content placeholder

Related Content

Title	Type	Slug
Emergency Response Planning for Blasting Incidents	lesson	blasting-emergency-response-planning
Blast Design Excel Template v4.2	resource	blast-design-excel-template
Drill Rig Maintenance Inspection Checklist	resource	drill-rig-maintenance-checklist
Rock Mass Rating (RMR) Field Survey Sheet	resource	rmr-field-survey-sheet
Drilling Energy Benchmarking Dashboard (Power BI)	resource	drilling-energy-dashboard

Detailed Explanation

The AHS Cyber Incident Response Playbook addresses the unique threat landscape faced by autonomous mining haul trucks, which integrate real-time embedded systems, GPS/RTK navigation, wireless telemetry (e.g., LTE/5G, Wi-Fi 6, private radio), and centralized dispatch platforms. Unlike generic IT incident response playbooks, it accounts for safety-critical constraints—such as the inability to 'reboot' a 400-ton moving vehicle mid-shift—and prioritizes fail-safe operational continuity alongside forensic integrity. The playbook is structured around the NIST SP 800-61r2 incident response lifecycle (Preparation, Detection & Analysis, Containment, Eradication & Recovery, Post-Incident Activity), but adapts each phase to AHS-specific assets: e.g., Preparation includes secure boot validation for onboard

ECUs and air-gapped firmware update protocols; Detection leverages behavioral anomaly detection on CAN bus traffic and telematics metadata rather than traditional endpoint logs. It further defines cross-functional coordination between OT engineers, mine control room operators, cybersecurity analysts, and OEM support teams—emphasizing time-bound escalation paths, pre-approved communication templates, and offline response checklists for low-connectivity pit environments. Crucially, the playbook integrates regulatory alignment with standards such as IEC 62443-3-3 (security risk assessment), ISO/SAE 21434 (road vehicle cybersecurity engineering), and MINExpo Cybersecurity Guidelines, ensuring compliance across jurisdictional and contractual boundaries.

Key Components

#	Component
1	Incident Classification Matrix (AHS-Specific Severity Tiers)
2	Role-Based Response Playbooks (e.g., Fleet Controller, OT Security Analyst, OEM Liaison)
3	AHS Asset Inventory & Criticality Registry with Communication Path Maps

Applications

#	Application
1	Rapid isolation of compromised haul truck controllers during lateral movement attempts
2	Coordinated response to GPS spoofing or jamming events impacting autonomous navigation accuracy
3	Forensic preservation of CAN bus logs and motion telemetry following unauthorized remote access to dispatch systems

Related Concepts

#	Concept
1	Mine Automation Cybersecurity Framework

#	Concept
2	IEC 62443-4-2 (Secure Product Development Lifecycle)
3	SAE J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)

Tags

> autonomous mining, OT security, incident response, AHS, cyber-physical systems, mining cybersecurity