CYBERDUDEBIVASH SIEM Detection Rules — 2026 Enterprise Blueprint

Advanced Detection Engineering Techniques, High-Fidelity Analytics, and SOC Playbooks.

This PDF contains the CyberDudeBivash SIEM Detection Blueprint for enterprise SOC teams.

For the full HTML version and detection packs, visit cyberdudebivash.com.

Sections Included:

1. Identity Compromise Detection Rules

2. RDP Abuse & Lateral Movement

3. Cloud IAM Attack Detection Rules

4. Ransomware Behavioral Detection

5. AI Phishing & Deepfake Detection

6. DFIR-Oriented Detection Rules