Security Blue Team Cheatsheet

Incident Response

- Establish clear roles and responsibilities (except Bob, he just brings donuts)
- Document everything meticulously (even bathroom breaks!)
- Isolate affected systems before investigating
- Preserve forensic evidence - never turn off infected machines, unless they're on fire

Monitoring

- Deploy SIEM solutions for real-time threat detection
- Configure alerts for suspicious activities (like developers working past 5pm)
- Monitor network traffic for unusual patterns
- Review logs daily, not weakly

Vulnerability Management

- Conduct regular scanning (like your ex scanning your social media)
- Prioritize patching based on risk - fix hole in roof before painting walls
- Document all known vulnerabilities in a central repositroy [sic]
- Establish remediation timelines that ignore holidays and weekends

Access Control

- Implement least privilege principles (executives need 37 access levels)
- Regularly audit user access rights - who the hack [sic] is this person?
- Use MFA everywhere possible - because passwords like "Password123!" aren't secure
- Revoke access immediately upon termination (before they get to the parking lot)

Security Awareness

- Train employees quarterly on social engineering tactics
- Run phishing simulations (Nigerian princes need love too)
- Create incident reporting procedures simple enough for management
- Celebrate security wins to boost moral [sic]