Chris Fullerton

AI Use in Security Operations

This system uses AI tools to help identify phishing attempts, suspicious logins, and unusual network activity. The purpose is to improve security by detecting threats faster and reducing manual review time. When the AI flags an alert, users will see a clear explanation of what was detected (e.g., “possible phishing link” or “login from unusual location”).

AI decisions are not final. A security analyst can review, confirm, or override any alert. Users may also appeal a decision if they believe an email or activity was flagged in error. Appeals are reviewed within 24 hours, with a written response provided.

The system only processes the minimum information needed (like sender, subject line, and metadata) and removes or redacts unnecessary personal details. Alerts and related data are stored for 90 days before secure deletion.

We track false positives and false negatives, as well as average appeal response time, to ensure fairness and accuracy. Performance and training data are reviewed quarterly, and the AI model is retrained at least once a year.