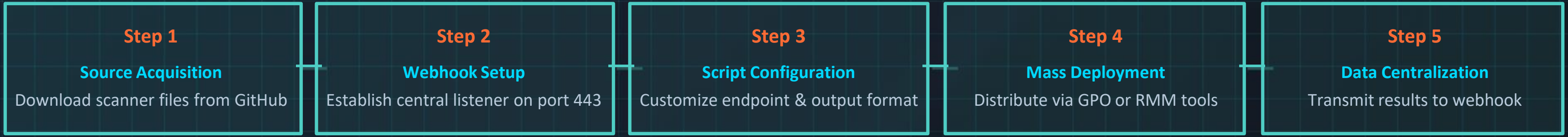
End-to-End Deployment & Data Flow Pipeline - Instructions



Step 1
Source Acquisition
Download scanner files from GitHub

Step 2
Webhook Setup
Establish central listener on port 443

Step 3
Script Configuration
Customize endpoint & output format

Step 4
Mass Deployment
Distribute via GPO or RMM tools

Step 5
Data Centralization
Transmit results to webhook

Step	Component	Action	Instructions
1	GitHub Repository	Download Scanner Files	find_impacted_packages.ps1 (Windows) & .sh (Linux/macOS) & impacted_packages.txt
2	Data Collection Server	Establish Central Listener	HTTP server on port 443 (python3 -m http.server 443)
3	Scanner Scripts	Customize Endpoint & Format	Edit scripts to point to webhook IP:port; select JSON or CSV
4	GPO or RMM	Distribute & Execute	Copy files to hosts and trigger script execution
5	Host → Webhook	Transmit Scan Results	Scan results (JSON/CSV) sent to central webhook for analysis

⚡ *Two parallel execution paths: Windows hosts (.ps1) and Linux/macOS hosts (.sh) | All data centralized for post-attack remediation analysis*

QMasters Cybersecurity Services 2025

QMASTERS
www.QMasters.co