Incident Response Plan

Detection Method

Log & Behavior Monitoring:
The CLI tool logs every command and response. Unusual activity such as unknown outbound connections, unexpected recon runs, or input/output mismatches will trigger alerts and flag potential misuse.

Type of Cyber Attack: Malware

The CLI tool could be altered (e.g., by a malicious pull request or dependency hijacking) to include malware that logs keystrokes, sends data to external servers, or provides backdoor access.

Containment Strategy

Immediately:

- Disable access to the compromised build or repository
- Revoke tokens/API keys
- Notify users to stop using the affected version

Eradication & Recovery

- Investigate and remove the malicious code
- Rebuild and audit all tool dependencies
- Release a new, secure version with patch notes
- Resume normal operations after testing recovery integrity

Legal and Ethical Compliance

Legal Requirements

1. **Computer Fraud and Abuse Act (CFAA)** – U.S. law prohibiting unauthorized access to computers.

2. **GDPR** – European data privacy regulation applicable to any collected user data.

Ethical Considerations

- **Responsible Disclosure**: If a vulnerability is found through the tool, the user is ethically bound to report it, not exploit it.

- **Tool Misuse**: Includes warnings and restrictions against targeting unauthorized systems.

Plan Compliance

- Limits tool usage to authorized systems with permission

- Includes logging and audit trails for accountability

- Shares incident findings responsibly through coordinated disclosure