HoneyGuard Implementation Guide

1. Critical Infrastructure

Objective: Protect SCADA systems, network shares, and operational protocols from unauthorized access.

Step-by-Step Implementation:

1. Create SCADA Honeytokens:

- Deploy fake configuration files mimicking SCADA systems (e.g., scada-config.json).

- Embed trackers to capture access attempts.

2. Deploy Decoy Network Shares:

- Set up fake network folders labeled as 'Engineering Docs'.

- Add honeytoken files (e.g., PowerGridSettings.xlsx) to monitor unauthorized interactions.

3. Embed Phishing Defenses:

- Send simulated phishing emails to employees with honeytoken links.

4. Set Up Alert System:

- Integrate alerts with monitoring tools like Splunk or PagerDuty.

2. Financial Systems

Objective: Detect credential theft and fraudulent access attempts.

Step-by-Step Implementation:

1. Generate Fake Banking API Keys:

- Embed realistic-looking API keys in internal tools or repositories.

2. Deploy Decoy Payment Files:

- Create fake wire transfer instruction files (e.g., WireTransferDetails.pdf) with embedded trackers.

3. Monitor Database Credentials:

- Add honeytoken database credentials to config files.

4. Set Up Incident Response:

- Log all interactions and trigger Webhooks for security alerts.

3. Healthcare

Objective: Protect sensitive patient records and medical systems.

Step-by-Step Implementation:

1. Deploy Fake EMRs:

- Add honeytokens to patient record databases with realistic but fake patient data.

2. Create Decoy Medical Documents:

- Deploy fake research papers or sensitive documents (e.g., CancerStudyResults.pdf).

3. Monitor Medical Device Systems:

- Deploy honeytoken credentials for devices like MRI machines.

4. Track Phishing Emails:

- Send fake phishing emails to staff and monitor interaction with tracking links.

4. Cloud Services

Objective: Detect API key abuse and unauthorized resource access.

Step-by-Step Implementation:

1. Create Fake Cloud API Keys:

- Embed honeytoken keys in repositories or documentation.

2. Deploy Pre-Signed URLs:

- Generate decoy URLs for cloud storage and monitor unauthorized access.

3. Set Up Decoy IAM Users:

- Create fake IAM users and track login attempts.

4. Monitor Cloud Workloads:

- Deploy decoy cloud functions to detect unauthorized execution attempts.

5. Implement Alerting:

- Integrate alerts with CloudWatch, Azure Monitor, or similar tools.