Phishing Email Detection

1. Brief / Purpose

This workflow detects and responds to phishing email detection. It receives alerts via a webhook, enriches the event, decides whether it's suspicious, and notifies the SOC team if necessary.

2. Components

• Webhook Trigger: Receives incoming alerts or events via HTTP POST.

• Enrichment Node: Calls an external API or threat intel to get reputation/context (e.g., VirusTotal, AbuseIPDB, PhishTank, GeoIP).

• IF / Decision Node: Examines enrichment results and decides whether to alert.

• Slack Alert Node: Posts a formatted message to #soc-alerts for SOC analysts.

• Log Clean Event Node: Records benign events for audit and reduces noise.

3. Workflow Flow

Webhook → Enrichment → IF Decision → [Slack Alert | Log Clean Event]

Perfect ✅ thanks for showing the style you want.
Here's the same structured **setup guide** but for your **Phishing Email workflow**:

Setup Guide – Phishing Email Detection Workflow

1. Configure Credentials

This workflow needs external integrations:

- **Slack API**
  - **Node:** Send Slack Alert.
  - Configure with your Slack account.
  - Set the channel (e.g., `#soc-alerts`).

---

2. Webhook Security

- **Webhook Trigger node** listens on:
  `/webhook/phishing-email`
- It validates incoming requests using:
- `if ($headers["x-siem-token"] !== $env.SIEM_SECRET) {`
- `throw new Error("Invalid Webhook Secret");`
- `}`
- **Setup:**
  - In your n8n environment variables, set:
  - `SIEM_SECRET=your_shared_secret`
  - Ensure your SIEM/security system sends:
    - `sender` (email address of sender)
    - `url` (suspicious link)
    - `subject` (optional, email subject)
    - **Header:** `x-siem-token: your_shared_secret`

---

3. Workflow Logic

1. **Webhook Trigger** → receives phishing email payload.
2. **Validate Payload** → ensures authenticity and required fields.
3. **Check URL in PhishTank** → queries if the URL exists in phishing database.
4. **Is Phishing?** → checks if PhishTank reports URL in database.
   - ✅ **If phishing** → Send Slack Alert.
   - ❌ **If clean** → Log Clean Email.

---

4. Testing

Send a test POST request:

```
curl -X POST "https://your-n8n-url/webhook/phishing-email" \
  -H "Content-Type: application/json" \
  -H "x-siem-token: your_shared_secret" \
  -d '{
    "sender": "phisher@evil.com",
    "url": "http://phishingsite.com",
    "subject": "Fake Bank Alert"
```

```
}'
```

- Replace `phishingsite.com` with a real phishing test URL if available.
- If detected → Slack alert is sent.
- If not → Workflow logs clean email status.

---

5. Deployment Notes

- Keep your **SIEM_SECRET** safe — it prevents unauthorized use of the webhook.
- Consider adding extra alerting destinations (e.g., email, Jira, ServiceNow).
- PhishTank API is community-based and may not cover all phishing attempts; use alongside other threat intel feeds if possible.