Business Email Compromise BEC

1. Brief / Purpose

This workflow detects and responds to business email compromise bec. 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]

4. Notes / Improvements

- Configure credentials in n8n for external APIs and Slack.

- Protect webhooks with a shared secret or IP allowlist.

- Consider adding payload validation to prevent malformed inputs.

- Optionally integrate automated remediation (EDR quarantine, firewall block) for high-confidence alerts.

5. How to Set Up

Here is a step-by-step guide to implement this workflow in your n8n instance.

1. Prepare Your Credentials

HIBP API Key: You need to get an API key from haveibeenpwned.com. This key is required to access the API.

Slack Credential: Create a Slack credential in n8n. Note the Channel ID of your security alert channel (e.g., `#security-alerts`).

2. Import the Workflow JSON

* Create a new workflow in n8n and import the JSON code (which was provided in a previous response).

3. Configure the Nodes

Scheduled Check (Cron): Set the schedule according to your preference (e.g., every Monday at 8:00 AM).

List Emails to Check (Code): Open this node and edit the `emailsToCheck` array . Enter the list of company email addresses you want to monitor.

Query HIBP API (HTTP Request): Open this node and in the "Headers" section, add the header `hibp-api-key` with the value of your HIBP API key.

Send High-Priority Alert (Slack): Select your Slack credential and replace `YOUR_SECURITY_ALERT_CHANNEL_ID` with your actual Channel ID .

4. Test and Activate

Manual Test: Run the workflow manually. You can test with a known breached email address (you can find examples online) to ensure the alert is triggered.

Verify Output: Check your specified Slack channel to confirm that the alert is sent with the correct information.

Activate: Once you're confident in its function, activate the workflow. n8n will now automatically monitor your important accounts for data breaches on the schedule you set.