
🚨 SOC Automation Project: End-to-End Email & Network Threat Detection (Power Automate + n8n + Google Sheets + AI)

Project Overview

A practical SOC automation project for monitoring and responding to phishing emails and network traffic threats—built entirely with accessible, no-cost tools:
Power Automate (Cloud), n8n (open-source workflow automation), Google Sheets, Slack, OpenAI, and Looker Studio.

What makes this project unique:
It shows how anyone can build meaningful security automation by combining Power Automate, n8n, and Google Sheets—even without access to expensive enterprise SOC platforms. This approach helped me understand real-world SOC workflows and the integration challenges teams often face with limited resources.

Key Features

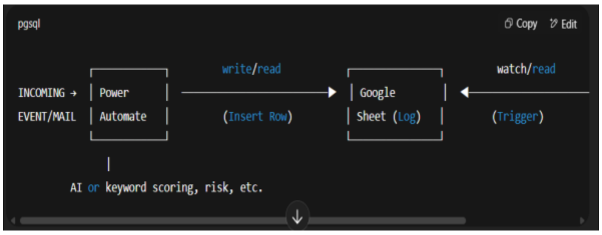
- **Phishing/malware email detection** and automated triage
- **Network log ingestion** & enrichment with AI-driven risk scoring
- **Central incident log** via Google Sheets (see below for why/how!)
- **Slack notifications** for critical events
- **Real-time Looker Studio dashboard** for SOC analytics

🔗 Integration Architecture: Power Automate ↔ Google Sheets ↔ n8n

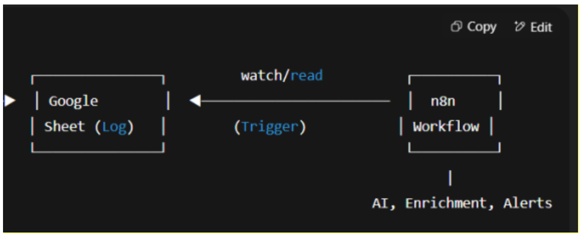
How It Works

Power Automate and n8n do *not* talk to each other directly.
Instead, Google Sheets acts as the “data bus”—a simple but effective shared log that connects the two workflows.

Flow Diagram



```
                ┌─────────┐    write/read             ┌──────────┐   watch/read
INCOMING →      │ Power    │ ──────────────────────▶  │ Google    │ ◀──────────────
EVENT/MAIL      │ Automate │      (Insert Row)        │ Sheet (Log)│    (Trigger)
                └─────────┘                           └──────────┘
                    |
            AI or keyword scoring, risk, etc.
```



```
  ┌───────────┐       watch/read           ┌─────────┐
▶ │ Google     │ ◀────────────────────────  │   n8n    │
  │ Sheet (Log)│        (Trigger)          │ Workflow │
  └───────────┘                             └─────────┘
                                                 |
                                       AI, Enrichment, Alerts
```

Typical Sequence

1. **Power Automate** receives a new email and inserts a row into Google Sheets.
2. **n8n** triggers on new rows in Google Sheets, analyzes, enriches, and notifies.
3. **Looker Studio** visualizes all incident data from Google Sheets.

Why Use This Pattern?

- **Free:** Google Sheets is free, accessible, and supports both Power Automate and n8n natively.
- **Modular:** Either automation can be upgraded/swapped independently.
- **Loose Coupling:** Follows industry integration patterns ("log bus").

Industry-Grade Alternative

Workflow Step	Project Tool (Free)	Enterprise Tool (Easy/Pro)
Event/Alert Logging	Google Sheets	SIEM (Splunk, Sentinel, ELK, QRadar)
Cross-platform trigger	Google Sheets row	API Webhooks, Message Bus (Kafka, Azure Service Bus)
Email monitoring	Power Automate (Gmail/Outlook trigger)	Microsoft Defender for O365, Graph API, Secure Email Gateway
Incident enrichment	n8n + OpenAI	SOAR (XSOAR, Sentinel Playbooks), ML/Threat Intel integrations
Notifications	Slack via n8n	SIEM/SOAR Alerts, PagerDuty, Teams, ServiceNow
Dashboarding	Looker Studio	SIEM Dashboards, Power BI, Kibana

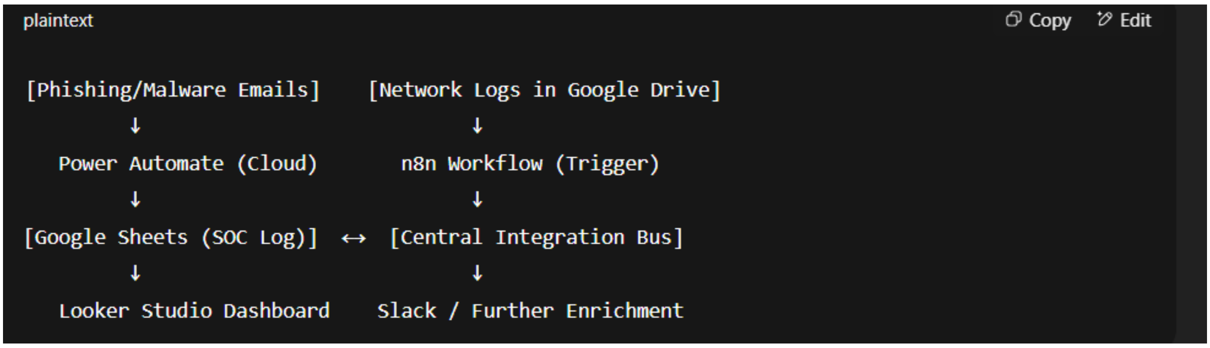
How It’s Faster/Easier with Enterprise Tools

- **No need for Google Sheets as an intermediary:** Direct webhook/API integrations or native SIEM ingest.
- **Log correlation, retention, search, and reporting** are built-in (no custom Apps Script or polling needed).
- **Prebuilt connectors** for email, threat feeds, ticketing, and notifications.

🗺️ Table of Contents

---

1. Project Architecture



```
[Phishing/Malware Emails]    [Network Logs in Google Drive]
          ↓                              ↓
   Power Automate (Cloud)        n8n Workflow (Trigger)
          ↓                              ↓
[Google Sheets (SOC Log)]  ↔  [Central Integration Bus]
          ↓                              ↓
   Looker Studio Dashboard     Slack / Further Enrichment
```

*In this project, **Google Sheets** is the heart of cross-tool integration.*
In a true enterprise SOC, a SIEM (Splunk/Sentinel/ELK) would fill this role.

---

2. Power Automate Email Threat Detection

Objective:

Monitor emails for threats, extract indicators, triage, and log to Google Sheets.

Actual Flow:

Step	Action	Purpose	Enterprise-Grade Equivalent
1	When a new email arrives	Trigger on new Gmail emails	Defender for O365, Graph API trigger
2	Get email details	Pull sender, subject, body, etc.	SIEM/Defender API, direct mail flow ingest
3	Html to text	Converts email to plain text	Ingest pipeline with built-in parser
4	Compose	Extract keywords/URLs	Threat detection module/regex, ML filter
5	Initialize variable	Store computed risk level	ML risk scoring, Threat Score API
6	Condition	Checks for threats/flags risk	SOAR playbook or SIEM correlation rules
7	Insert row (Google Sheets)	Log to incident sheet (integration bus)	SIEM database/incident table
8	Send email (V2)	Alert (optional)	PagerDuty, ServiceNow, Teams alert
9	Insert row 2	Log non-critical/misc events	Triage queue, alternative log index

---

3. n8n Network Log Ingestion & AI Analysis

Purpose:

Ingest, enrich, and triage network logs (from firewall/SIEM export) with AI risk scoring.

Key Steps:

- **Trigger:** New file or row in Google Sheets (log record).
- **Parse/Enrich:** Extract fields, enrich IP with ipinfo.io, threat feeds.
- **AI Triage:** OpenAI node provides SOC-style summary, risk score, and recommended action.

- **Alert:** High-risk events trigger Slack notifications.
- **Log:** All results are appended to Google Sheets.

Enterprise-Grade Equivalent:

- Trigger on log event: SIEM agent, cloud connector, or API.
- Enrichment: SIEM built-in, Threat Intel integration, SOAR playbooks.
- AI/ML: Native or integrated (e.g., Sentinel ML analytics, Splunk Phantom, Cortex XSOAR).
- Alerting: SIEM/SOAR action modules.

---

4. Google Sheets as Integration Bus

Role in Project:

- Serves as the central log and data bus for both automations.
- Enables modular, loosely-coupled workflow integration without custom APIs.

Enterprise Alternative:

- SIEM or dedicated event/message bus (Kafka, Azure Service Bus, RabbitMQ).
- Direct webhook/API integration between products.

How an Enterprise Makes This Fast/Easy:

- No polling or Apps Script needed—instant, robust event-driven integrations via native connectors.

---

5. Looker Studio Dashboard

- **Connects to Google Sheets** for real-time analytics on incident logs.
- **Charts:** By time, type, country, risk, etc.

Enterprise Alternative:

- SIEM-native dashboards, Power BI, Grafana, Kibana—directly on security data.

---

6. Sample n8n Workflow JSON

SOC_Network_Log_Ingestion_Flow.json

---

7. Deployment Instructions

1. **Power Automate:**
   - Import/create flow, connect Gmail and Google Sheets.
2. **n8n:**
   - Import/copy workflow JSON, connect Sheets, Slack, OpenAI.
3. **Google Sheets:**
   - Create SOC_Incident_Log with required columns (see README).
4. **Looker Studio:**
   - Connect to Google Sheet, build dashboards.

---

8. Security, Privacy, and "What Real SOCs Use"

- **No credentials/tokens in shared files.** Always use environment secrets.
- Use OAuth2 for all integrations.
- Do NOT upload sensitive info to public repos.
- **In enterprise/SOC:**
  - Replace Sheets with SIEM/secure DB/message bus.
  - Use production APIs, secured endpoints, and native eventing.
  - All workflows are monitored, audited, and managed centrally.

---

9. Contact & Credits

Author:
Manish

[Manish | LinkedIn]
