# 👋 Hello, I'm Asad Dafalla

### SOC Analyst | Incident Responder | Blue Teamer

Welcome to my cybersecurity portfolio. Here, I document my journey in Security Operations, featuring real-world troubleshooting cases, lab investigations, and threat analysis reports.

## 📂 Featured Investigation: Suspicious Proxy Authentication

**Scenario:** Real-world incident troubleshooting & analysis.

### 🚨 Incident Overview

During routine system usage, a suspicious popup appeared requesting authentication for a proxy server (trout-west-1-us.maxxxcdn.com). This behavior was unexpected and indicated a potential unauthorized attempt to route network traffic.

### 🛠️ Investigation Methodology

I followed a structured SOC investigation lifecycle to analyze and remediate the issue:

1. **Observation:** Identified unusual behavior (unexpected authentication prompt).
2. **Verification (OSINT & DNS):** * Used nslookup to resolve the domain to an AWS IP (15.204.43.197).
    - **Analyzed the IP reputation using VirusTotal and Cisco Talos.**
3. **Root Cause Analysis (Endpoint):** * Investigated running processes and installed browser extensions.
    - Correlated the popup timing with active browser sessions.
4. **Discovery:** Identified a rogue browser extension ("Free VeePN") as the source of the traffic interception.
5. **Remediation:** Removed the extension and verified network settings were restored to default.

### 🛡️ Key Skills Demonstrated

- **Log & Traffic Analysis:** Understanding HTTP proxy requests.
- **DNS Analysis:** Using command-line tools (nslookup) to trace infrastructure.
- **Threat Intelligence:** Leveraging external reputation sources.
- **Endpoint Security:** Identifying Potentially Unwanted Programs (PUPs) / Extensions.

## 🔗 Connect with Me

- **LinkedIn:** www.linkedin.com/in/asad-dafalla
- **Email:** asad.cyper@gmail.com