Real Threat Intelligence Integration Guide

Current Status: Hybrid System

Your CSIRT Command Center now runs in **hybrid mode**:

- **Without API keys**: Uses realistic simulated data based on real threat patterns
- **With API keys**: Integrates live threat intelligence from real security sources

🌐 Real Security Data Sources Available:

1. Free Threat Intelligence APIs:

AbuseIPDB (Malicious IP Database)

- **What**: Real malicious IPs reported globally
- **Free tier**: 1,000 requests/day
- **Get key**: https://www.abuseipdb.com/register
- **Provides**: Live malicious IPs, abuse confidence scores, geolocation

VirusTotal (Malware/URL Analysis)

- **What**: Real malware hashes, suspicious URLs
- **Free tier**: 500 requests/day
- **Get key**: https://www.virustotal.com/gui/join-us
- **Provides**: File reputation, URL scanning, malware family classification

Shodan (Internet Scanning)

- **What**: Real vulnerable devices on the internet
- **Free tier**: Limited searches
- **Get key**: https://account.shodan.io/register
- **Provides**: Open ports, vulnerable services, IoT device exposure

AlienVault OTX (Open Threat Exchange)

- **What**: Community threat intelligence sharing
- **Free tier**: Full access
- **Get key**: https://otx.alienvault.com/
- **Provides**: IOCs, threat actor TTPs, malware signatures

2. Public Security Datasets (No API Key Required):

CVE Database

- **What**: Real vulnerability disclosures
- **Access**: Free, no key required
- **Provides**: Latest CVEs, severity scores, affected products

MITRE ATT&CK

- **What**: Real adversary tactics and techniques
- **Access**: Free JSON API
- **Provides**: Attack patterns, threat actor profiles

How to Enable Real Data:

Step 1: Get Free API Keys (5-10 minutes each)

```
# 1. Visit these sites and register:
# - https://www.abuseipdb.com/register (for malicious IPs)
# - https://www.virustotal.com/gui/join-us (for malware data)
# - https://account.shodan.io/register (for vulnerable devices)
# - https://otx.alienvault.com/ (for threat indicators)
```

Step 2: Configure Your Environment

```
# Copy the example file
cp .env.example .env

# Edit .env and add your API keys:
nano .env
```

Step 3: Add API Keys to .env

```
# Real Threat Intelligence APIs
ABUSEIPDB_API_KEY=your_actual_api_key_here
VIRUSTOTAL_API_KEY=your_actual_api_key_here
SHODAN_API_KEY=your_actual_api_key_here
OTX_API_KEY=your_actual_api_key_here
```

Step 4: Restart the Application

```
# The system will automatically detect the keys and switch to real data
npm run dev
```

Real vs Simulated - What Changes:

Without API Keys (Current State):

- Realistic threat patterns based on real attack data
- Authentic IP ranges used by actual attackers
- Recent CVE references and vulnerability descriptions
- Proper severity classifications and timing patterns

With API Keys (Enhanced Mode):

- **Live malicious IPs** from global honeypot networks
- **Real CVEs** published in the last 7 days
- **Actual threat indicators** from security community
- **Live vulnerability scans** from internet-wide scanning
- **Real malware family classifications**

Data Sources Breakdown:

Source	Real Data Available	Free Tier Limit	Setup Time
AbuseIPDB	Malicious IPs	1,000/day	2 min
VirusTotal	Malware/URLs	500/day	2 min
Shodan	Vulnerable devices	Limited	3 min
AlienVault OTX	Threat indicators	Unlimited	2 min
CVE Database	Vulnerabilities	Unlimited	0 min
MITRE ATT&CK	Attack patterns	Unlimited	0 min

Enhanced Features with Real Data:

Real Malicious IP Detection:

```
// Example real incident with API integration:
{
  "sourceIP": "185.220.101.42",  // Real malicious IP from AbuseIPDB
  "country": "RU",               // Actually reported from Russia
  "abuseConfidence": 95,         // 95% confidence malicious
  "lastSeen": "2024-01-15",      // Last reported 3 days ago
  "type": "Malicious IP Connection"
}
```

Live Vulnerability Intelligence:

```
// Real CVE from last week:
{
  "cveId": "CVE-2024-21412",     // Actual CVE published
  "severity": "CRITICAL",        // Real CVSS score 9.8
  "description": "Microsoft Outlook Remote Code Execution Vulnerability",
  "publishedDate": "2024-01-09"  // Actually published this date
}
```

Security Best Practices:

API Key Security:

- Never commit .env files to git (already in .gitignore)
- Use environment variables in production
- Rotate API keys monthly
- Monitor API usage limits

Rate Limiting:

- Built-in request throttling (20-second intervals)
- Fallback to simulation if APIs fail
- Graceful error handling for all sources

Demo Script for Interviews:

"Pure Simulation" Mode (Current):

> *"This CSIRT dashboard demonstrates realistic threat detection patterns. The incidents you're seeing follow authentic attack signatures and timing patterns based on real threat intelligence, but are simulated for demo purposes."*

"Live Intelligence" Mode (With APIs):

> *"This dashboard is connected to live threat intelligence feeds. The malicious IPs you're seeing are actively being reported by security researchers worldwide. That CVE that just appeared was published 2 days ago. This is real-time cybersecurity data."*

Perfect for Portfolio:

Both modes are impressive for different reasons:

Simulation Mode: Shows you can create realistic, professional security tools
Live Intelligence Mode: Demonstrates real threat intelligence integration skills

Choose based on your interview context:

- **Technical interviews**: Show the live intelligence integration
- **General demos**: Simulation mode is more predictable and reliable

⚡ Quick Test:

Check if your APIs are working:

```
# Watch the server logs for real data indicators:
#       "Using simulated malicious IPs (AbuseIPDB not available)" - Simulation
#       "New CRITICAL incident: Real vulnerability CVE-2024-21412" - Live data
```

Your CSIRT Command Center is now ready for both demo and real threat intelligence scenarios!