1. CrowdStrike Integration Architecture

text

[Endpoint] → [Falcon Agent] → [AI Model (AWS/Docker)] → [Falcon Alerts]

↓ ↑

(Event Stream via API) [Custom IOC/Detection]

2. Prerequisites

CrowdStrike Falcon instance with API access (requires Falcon X or Spotlight license).

API Credentials:

FALCON\_CLIENT\_ID (OAuth2 client)

FALCON\_CLIENT\_SECRET

FALCON\_BASE\_URL (e.g., https://api.crowdstrike.com)

3. Step-by-Step Implementation

A. Set Up CrowdStrike API Access

python

# Install CrowdStrike SDK

pip install crowdstrike-falconpy

B. Real-Time Event Streaming (Falcon Event Streams API)

python

from falconpy import EventStreams

# Authenticate

auth = EventStreams(client\_id=FALCON\_CLIENT\_ID, client\_secret=FALCON\_CLIENT\_SECRET)

# Stream endpoint events (process executions, file modifications)

for event in auth.stream\_events():

if event["event\_type"] == "ProcessRollup2":

process\_name = event["event"]["ImageFileName"]

command\_line = event["event"]["CommandLine"]

# Send to AI model for ransomware detection

if detect\_ransomware(process\_name, command\_line):

trigger\_containment(event["device\_id"])

C. AI Model Integration

1. Ransomware Detection (Behavioral Analysis)

python

import joblib

from falconpy import Detects

# Load pre-trained model

model = joblib.load("ransomware\_model.pkl")

def detect\_ransomware(process\_name, cmdline):

# Feature extraction (example)

features = {

"encryption\_keywords": int("encrypt" in cmdline.lower()),

"shadow\_copy\_deletion": int("vssadmin" in cmdline.lower()),

"entropy": calculate\_entropy(process\_name)

}

return model.predict([list(features.values())])[0] == 1 # 1=malicious

2. DDoS Detection (Network Anomalies)

python

from falconpy import Spotlight

def check\_ddos\_participation(device\_id):

# Query network connections

spotlight = Spotlight(client\_id=FALCON\_CLIENT\_ID, client\_secret=FALCON\_CLIENT\_SECRET)

connections = spotlight.query\_network\_connections(device\_id)

# Analyze for DDoS patterns (high outbound packets)

if connections["total\_packets"] > 1000/second:

return True

D. Automated Containment

python

from falconpy import Hosts

def trigger\_containment(device\_id):

# Isolate endpoint

hosts = Hosts(client\_id=FALCON\_CLIENT\_ID, client\_secret=FALCON\_CLIENT\_SECRET)

hosts.perform\_action(action\_name="contain", ids=[device\_id])

# Create detection in Falcon console

detects = Detects(client\_id=FALCON\_CLIENT\_ID, client\_secret=FALCON\_CLIENT\_SECRET)

detects.create\_detection(

name="AI-Detected Ransomware",

severity="Critical",

behaviors=[{"tactic": "TA0040", "technique": "T1486"}]

)

E. Custom IOC Management

python

from falconpy import IOC

def add\_ransomware\_ioc(file\_hash):

ioc = IOC(client\_id=FALCON\_CLIENT\_ID, client\_secret=FALCON\_CLIENT\_SECRET)

ioc.create\_indicator(

type="sha256",

value=file\_hash,

platforms=["Windows"],

action="detect",

severity="High"

)

4. Key CrowdStrike-Specific Optimizations

Reduce API Calls:

Use Falcon Streaming API instead of polling to minimize rate limits.

Focus on High-Value Events:

Filter for critical event types:

python

event\_types = ["ProcessRollup2", "DiskWrite", "NetworkConnect"]

Leverage Falcon ML Insights:

Combine your AI model with CrowdStrike’s built-in ML (e.g., Overwatch).

5. Example Workflow

Falcon Agent detects encrypt.exe spawning from a suspicious path.

AI Model receives process event → predicts ransomware with 98% confidence.

Automated Response:

Isolates endpoint via Hosts API.

Creates detection with MITRE tactic T1486.

Adds file hash to Falcon IOCs.

6. Monitoring & Alerting

python

# Send alerts to SIEM (Splunk/Sentinel)

import requests

def send\_to\_siem(alert):

requests.post(

"https://your.siem.com/api/alerts",

json={

"source": "CrowdStrike+AI",

"message": alert

}

)

7. Deployment Options

Method Use Case Example

AWS Lambda Serverless real-time analysis Lambda Guide

Docker + Kubernetes Scalable on-prem deployment docker build -t falcon-ai .

Falcon Horizon Cloud workload protection Horizon API Docs

8. Validation Checklist

Test Detection:

Simulate ransomware using MITRE CALDERA.

Measure Performance:

False positives/negatives.

Endpoint impact (CPU/memory).

Verify Containment:

Confirm isolation via Falcon console.

9. Troubleshooting Tips

API Limits: Use exponential backoff for rate limits.

Model Drift: Retrain monthly with new Falcon Detections data.

Logging: Log all predictions to S3 for audit trails.

10. Sample Output in Falcon Console

json

{

"detection\_id": "ldt:ABCD1234",

"name": "AI-Detected Ransomware",

"severity": "Critical",

"device\_id": "12345678",

"behaviors": [

{"tactic": "Impact", "technique": "Data Encrypted"}

]

}

This integration enhances CrowdStrike’s native capabilities with your AI models while leveraging Falcon’s real-time visibility and response APIs.