Unique
100%

Plagiarized
0%

Word: 623

Characters: 4677

Content Checked for Plagiarism

https://www.linkedin.com/in/matx104/
Implementing AI-Driven Security Operations Center (SOC)
with Automated Threat Hunting, SOAR Integration, and Machine Learning
for Enterprise Cybersecurity
Presenter: Muhammad Abdullah Tariq
Institution: AL NAFI International College
Diploma: EduQual Level 6 - AI Operations
Date: September 2025
The Security Crisis We Face
Daily Reality:
10,000+ security alerts per day
45% error rate in manual review
67% of advanced threats missed
82% breaches involve human error
Business Impact:
207 days average detection time
$4.88M average breach cost
65% analyst turnover rate
43% yearly increase in attacks

Traditional SOC processes only 10-50GB/day effectively

Traditional SOC AI-Driven SOC
207 days detection 3 minutes detection
67% threats missed 96.3% accuracy
Manual response 78% automated
10-50GB/day 1M+ events/second
Reactive approach Predictive analytics
An Automated AI-SOC Solution
Transforming Security Operations with AI

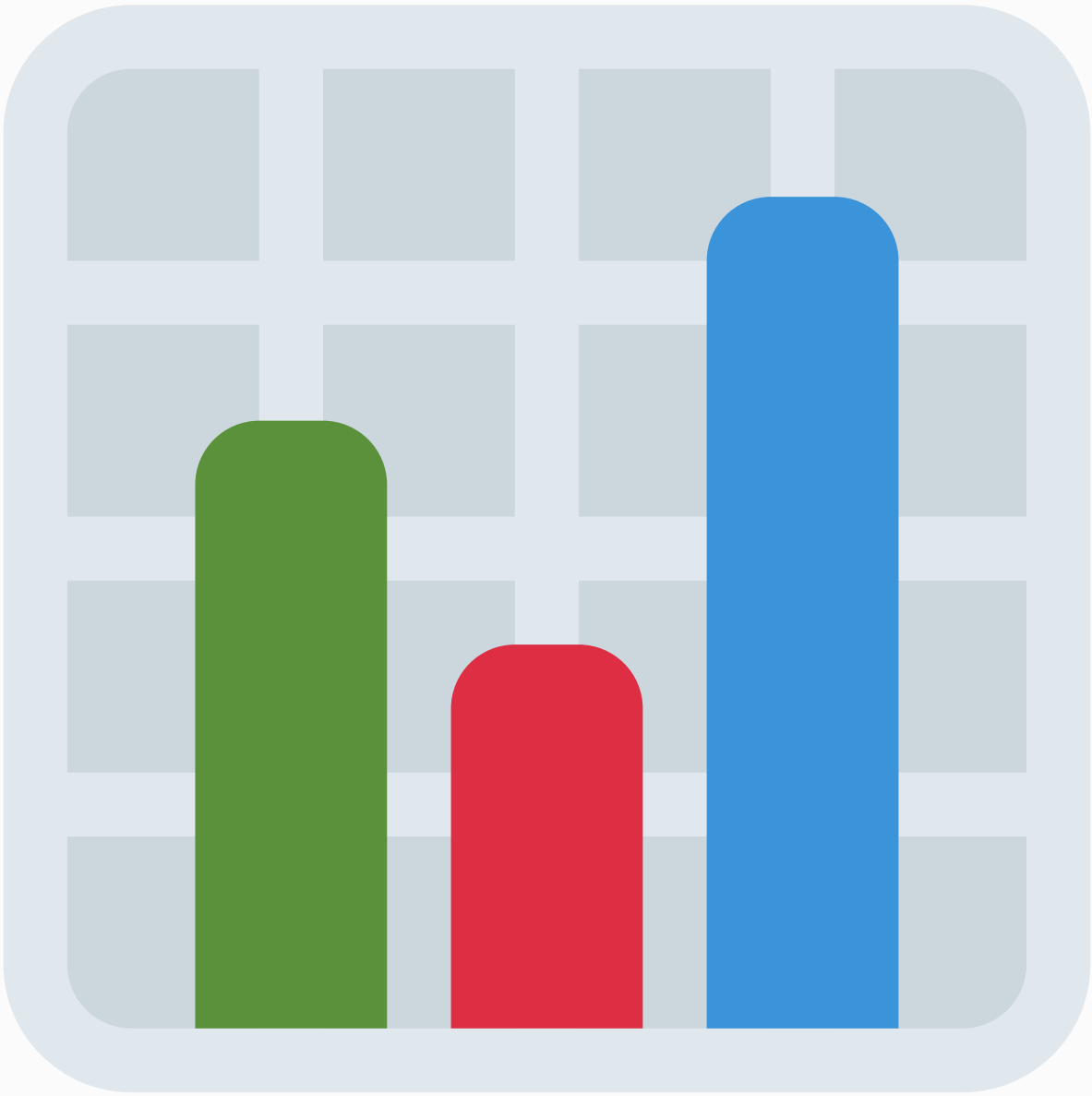
256% ROI in Year 1

Architecture Overview
4-Stage Security Pipeline
Tools per Stage:
1.Ingest: Elastic, Splunk, Wazuh
2.Analyze: TensorFlow, scikit-learn
3.Respond: TheHive, Phantom SOAR
4.Comply: Grafana, Automated Reporting
SIEM/Analytics SOAR Platforms Threat Intelligence

Elastic Security

TheHive

MISP



Splunk

Cortex

OpenCTI

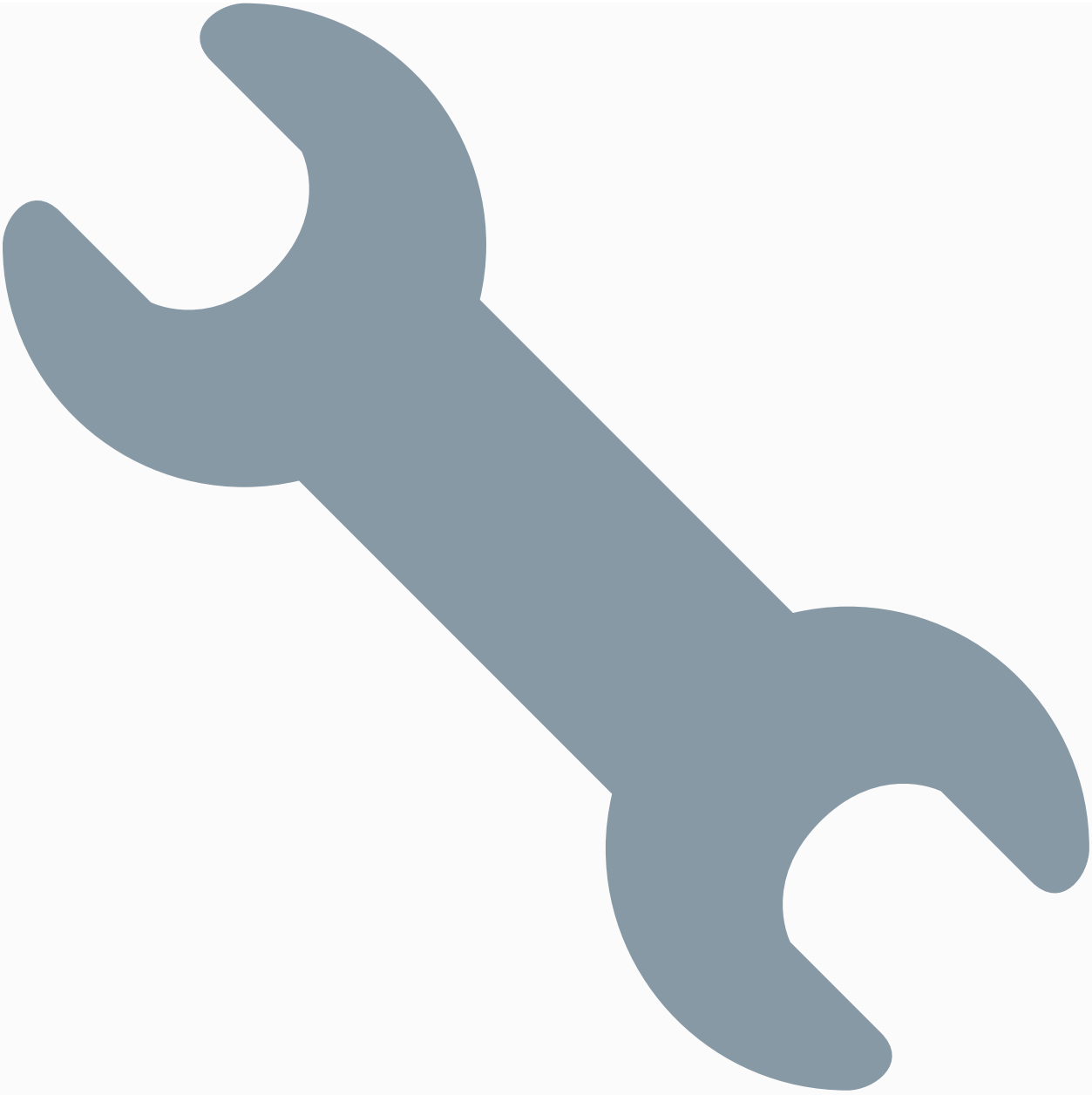
Wazuh &

Graylog

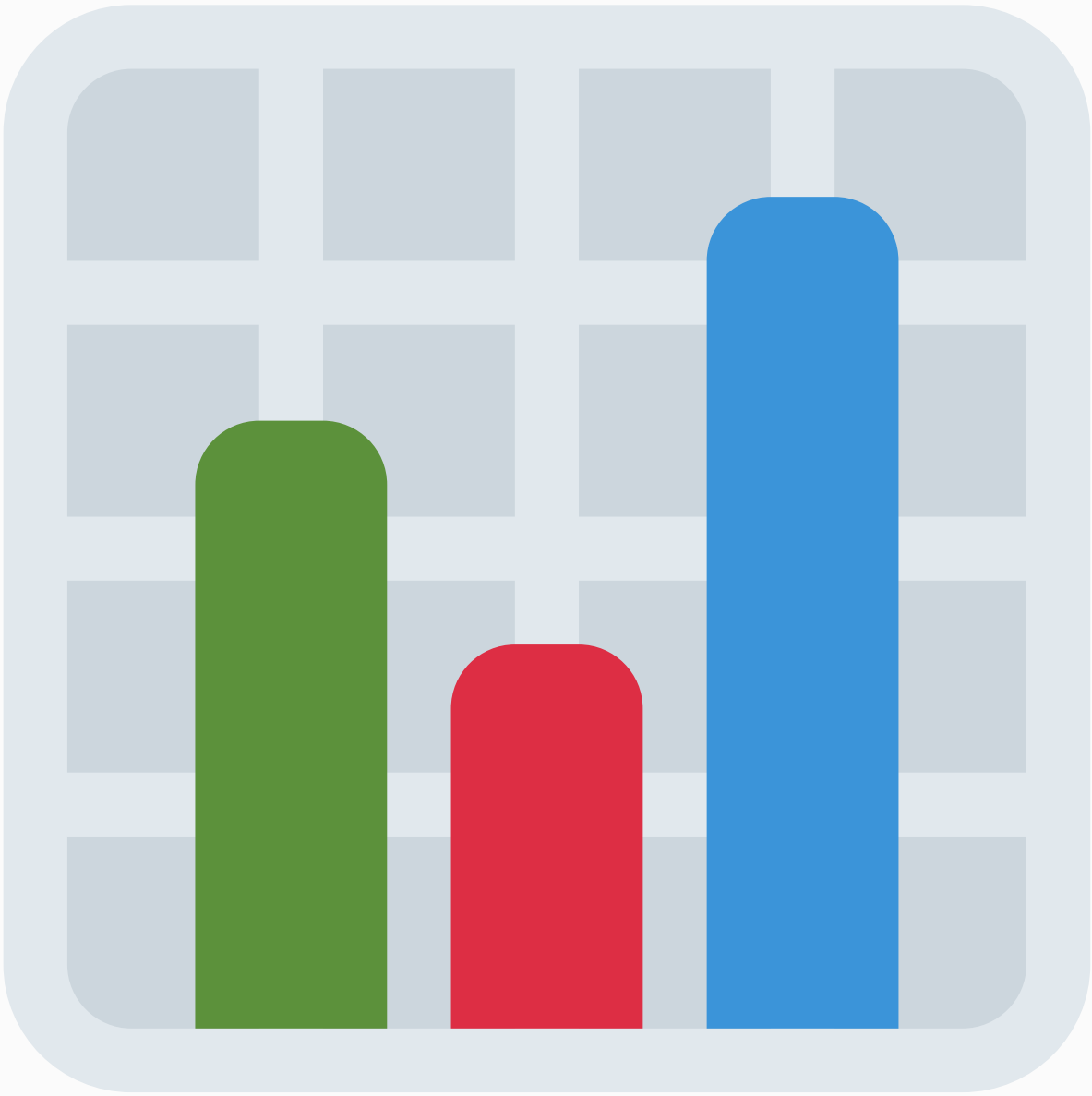
Phantom

YARA
ML/Analytics Automation Visualization

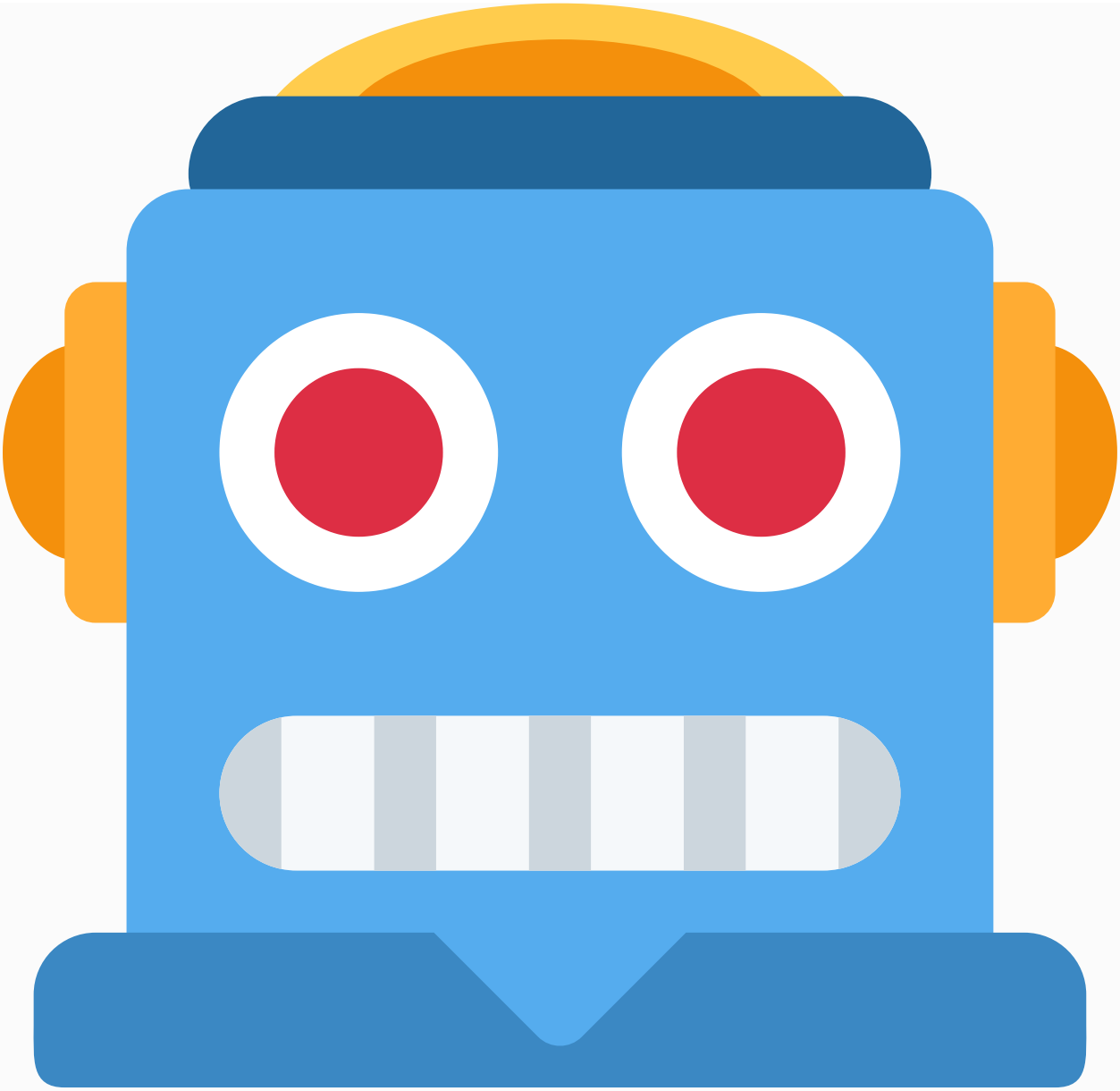
TensorFlow



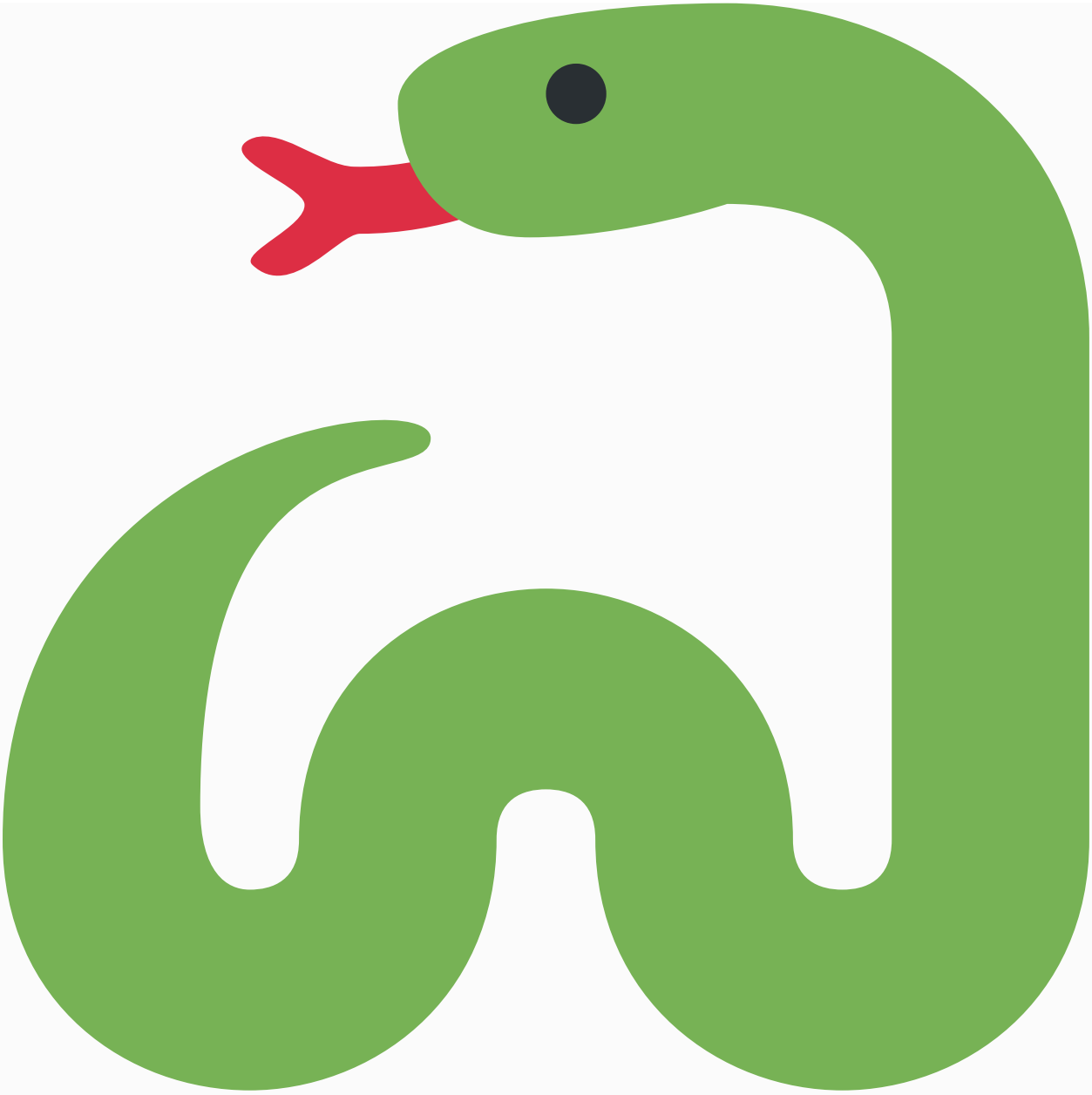
Ansible



Grafana



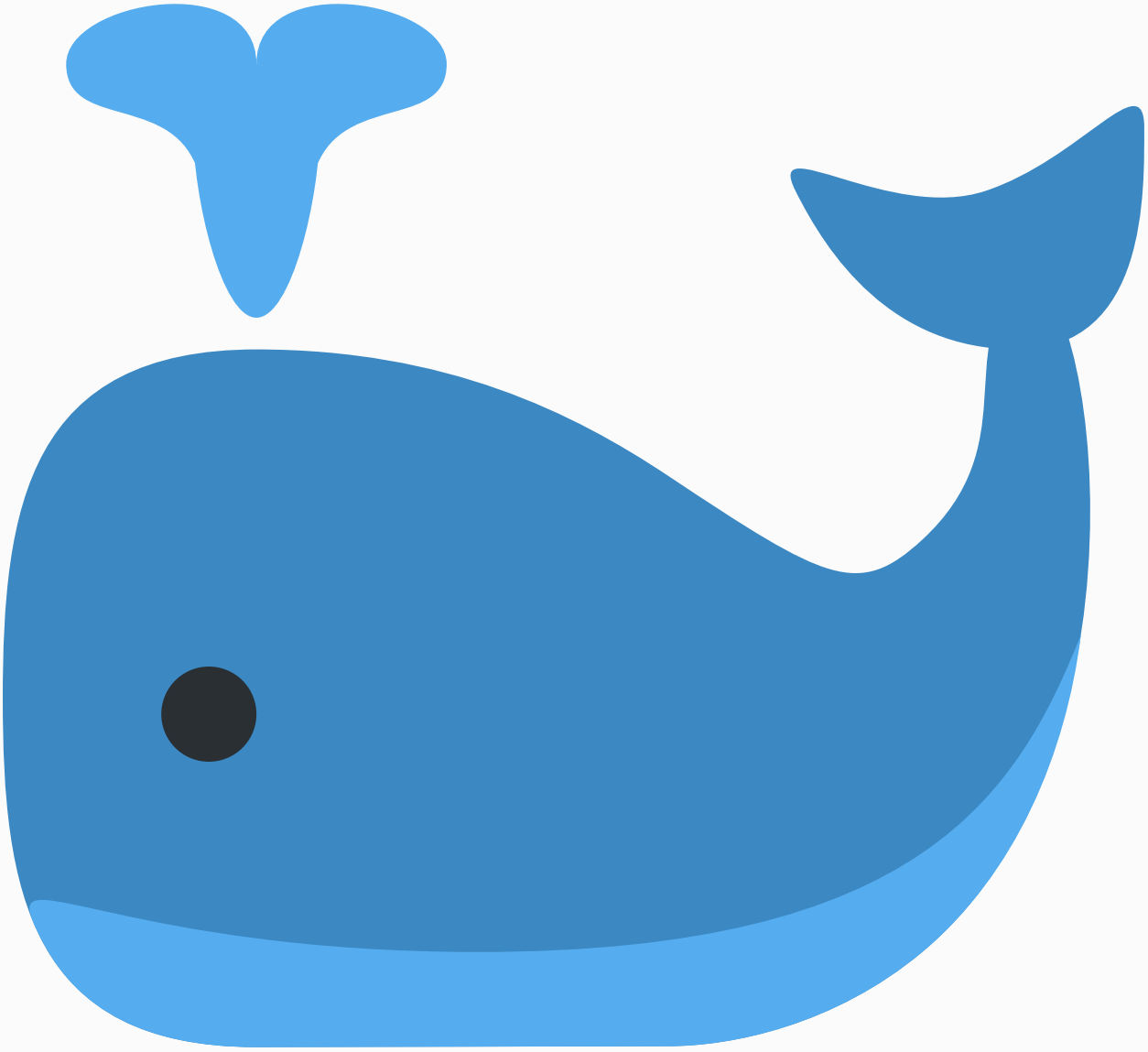
scikit-learn



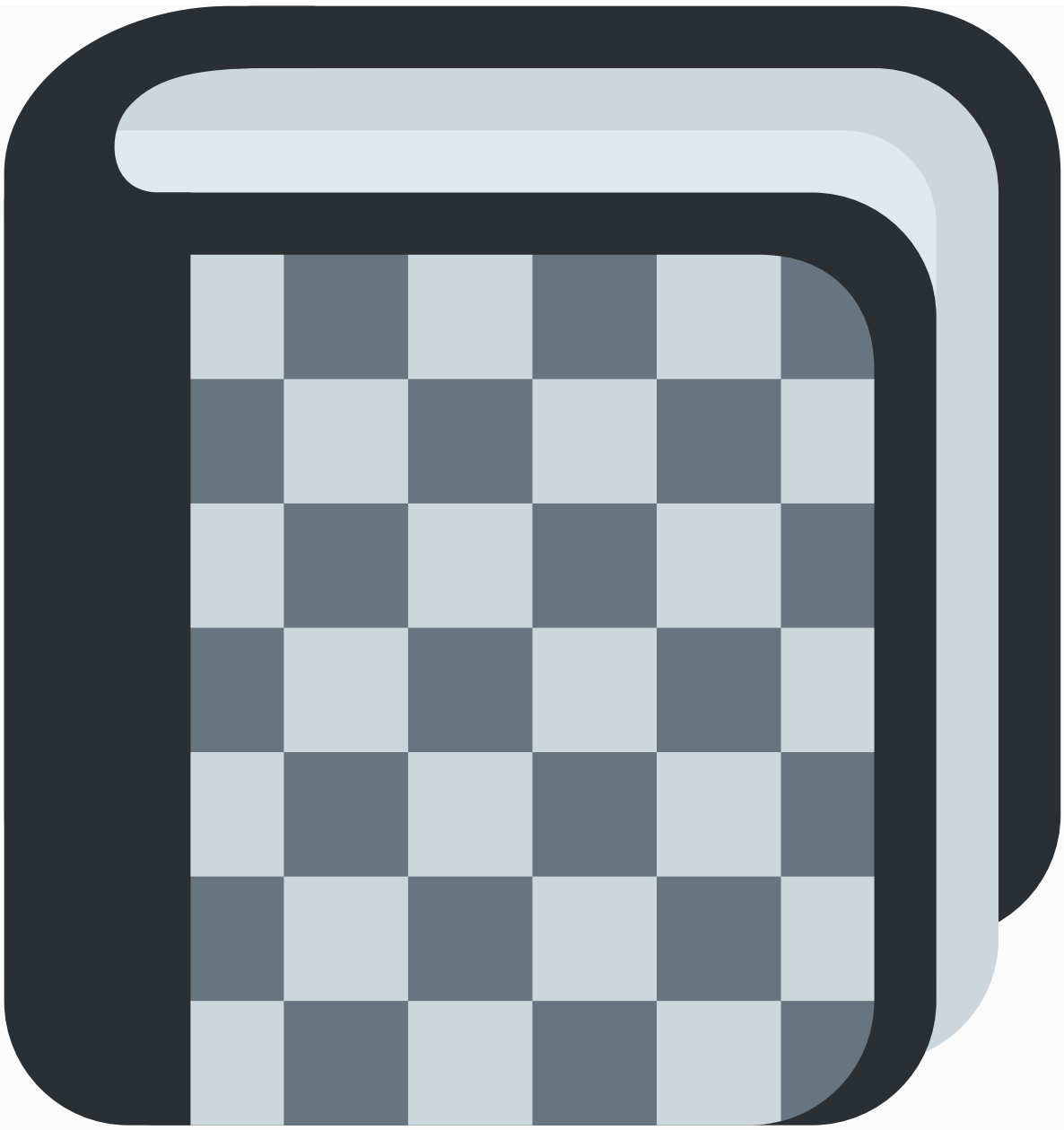
Python

Kibana

Apache Spark



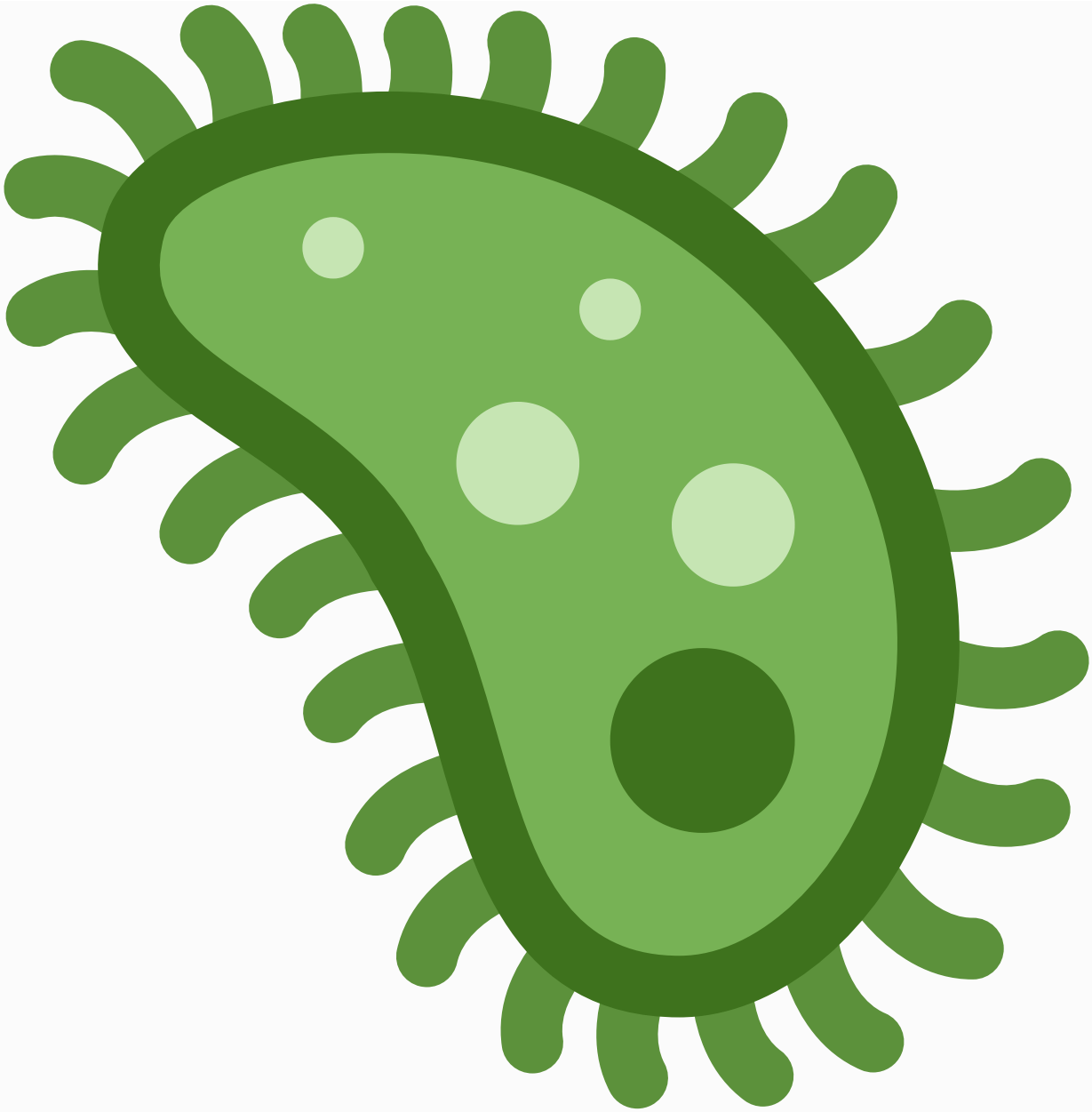
Docker/K8s



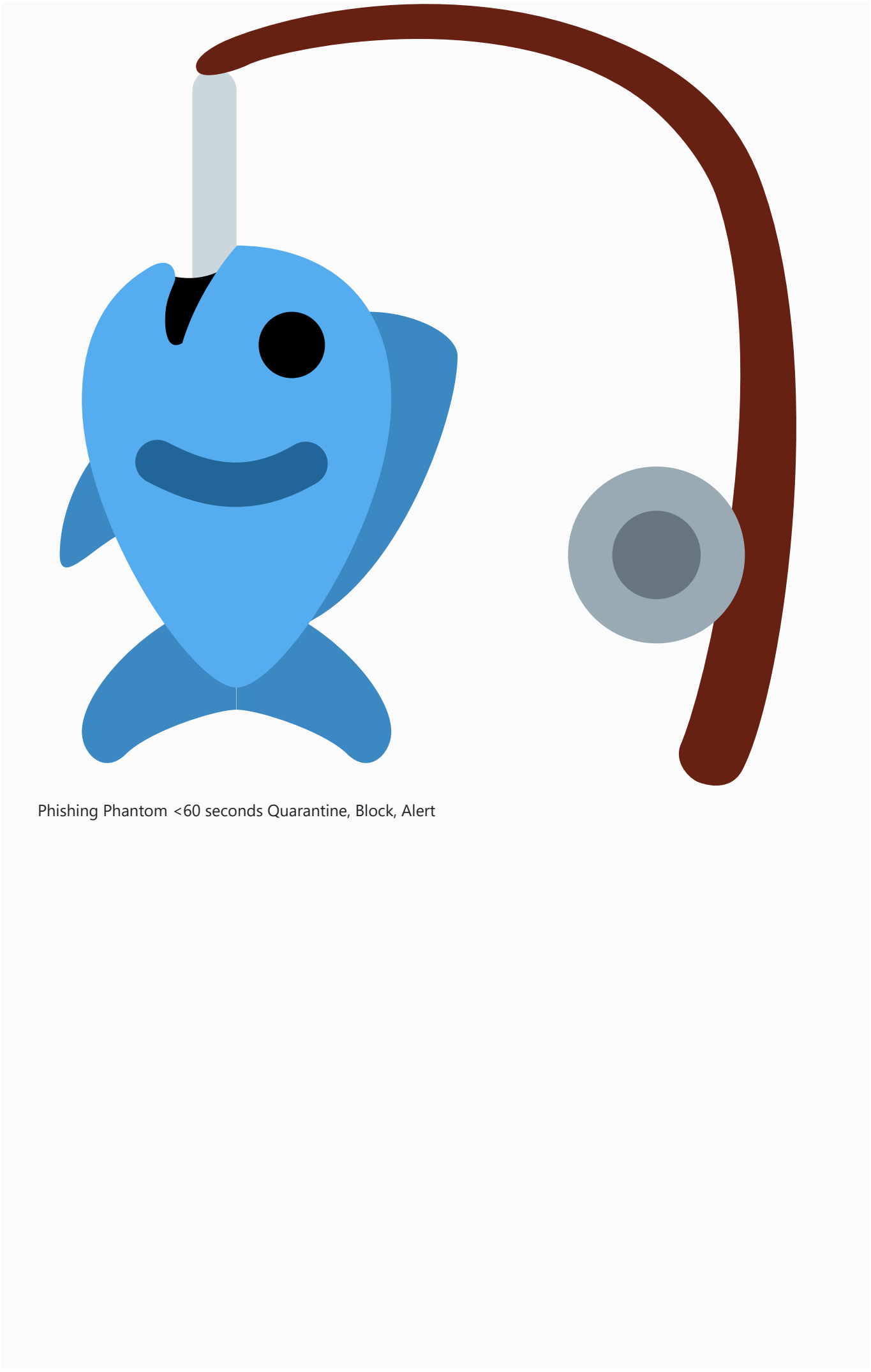
Jupyter
Open Source Technology Stack
Enterprise-Grade Open Source Stack
Open Source Technology Stack
AI-Powered Threat Detection
Ensemble Machine Learning Approach

From 10,000 alerts to 230 real threats daily

Automated Threat Hunting
MITRE ATT&CK Automated Hunting
Coverage Metrics:
Initial Access: 89% detected
Persistence: 92% detected
Lateral Movement: 87% detected
Exfiltration: 94% detected
Threat Type Tool Response Time Actions



Ransomware TheHive <30 seconds Isolate, Snapshot, Contain



Phishing Phantom <60 seconds Quarantine, Block, Alert

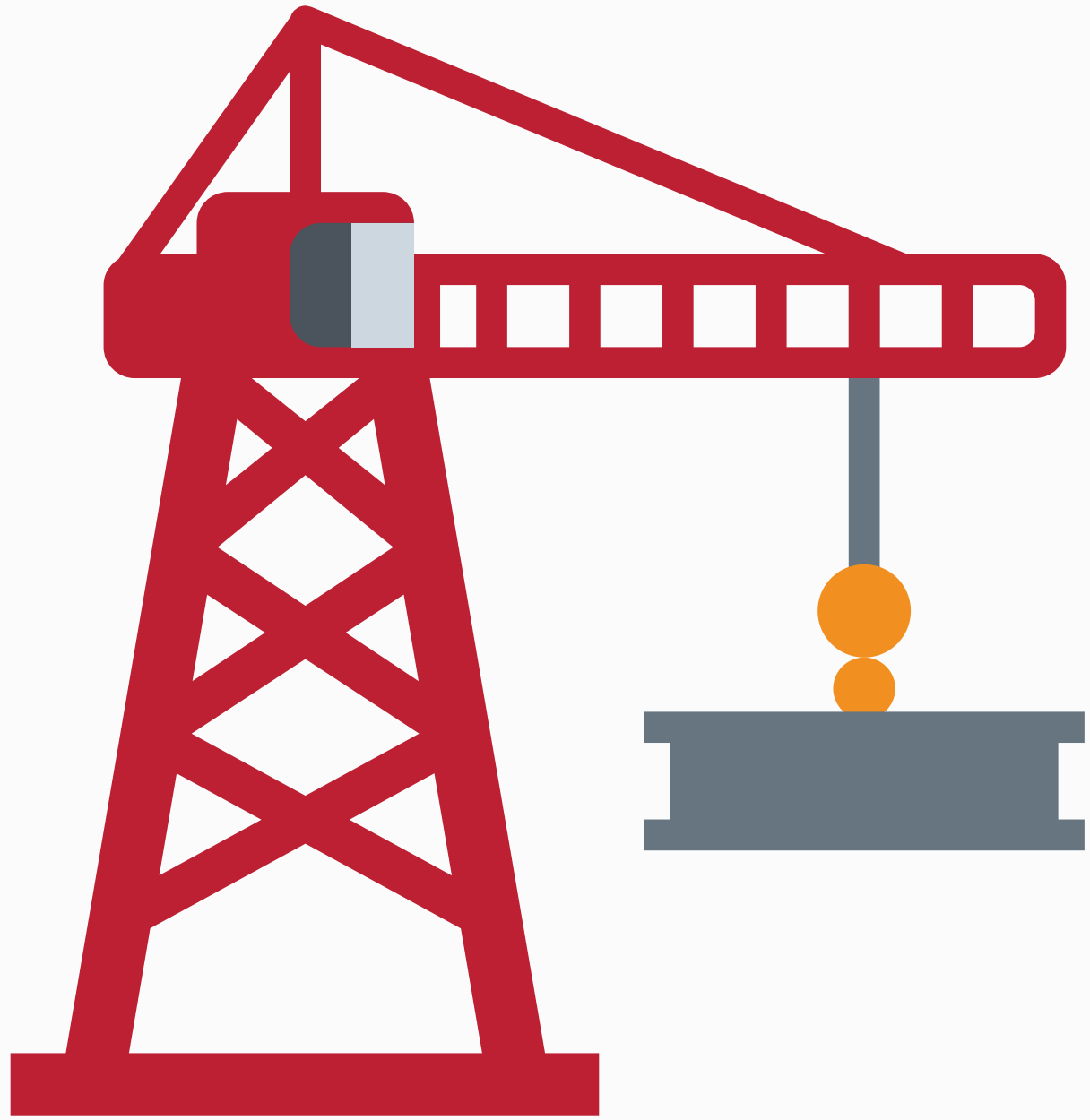
Insider Cortex <2 minutes Revoke, Monitor, Report

DDoS TheHive <45 seconds Reroute, Scale, Block
SOAR Integration
78% Incident Automation with SOAR
Connected Systems: SIEM + EDR + Threat Intel + Cloud Security
Framework Automation Evidence Audit Time
PCI DSS 4.0 100% Real-time <5 min
SOX 98% Continuous <10 min
GDPR 95% Automated <15 min
HIPAA 97% Immutable <10 min
ISO 27001 100% Daily <5 min
CIS Controls 94% On-demand <5 min
Compliance Automation
Multi-Framework Compliance Dashboard

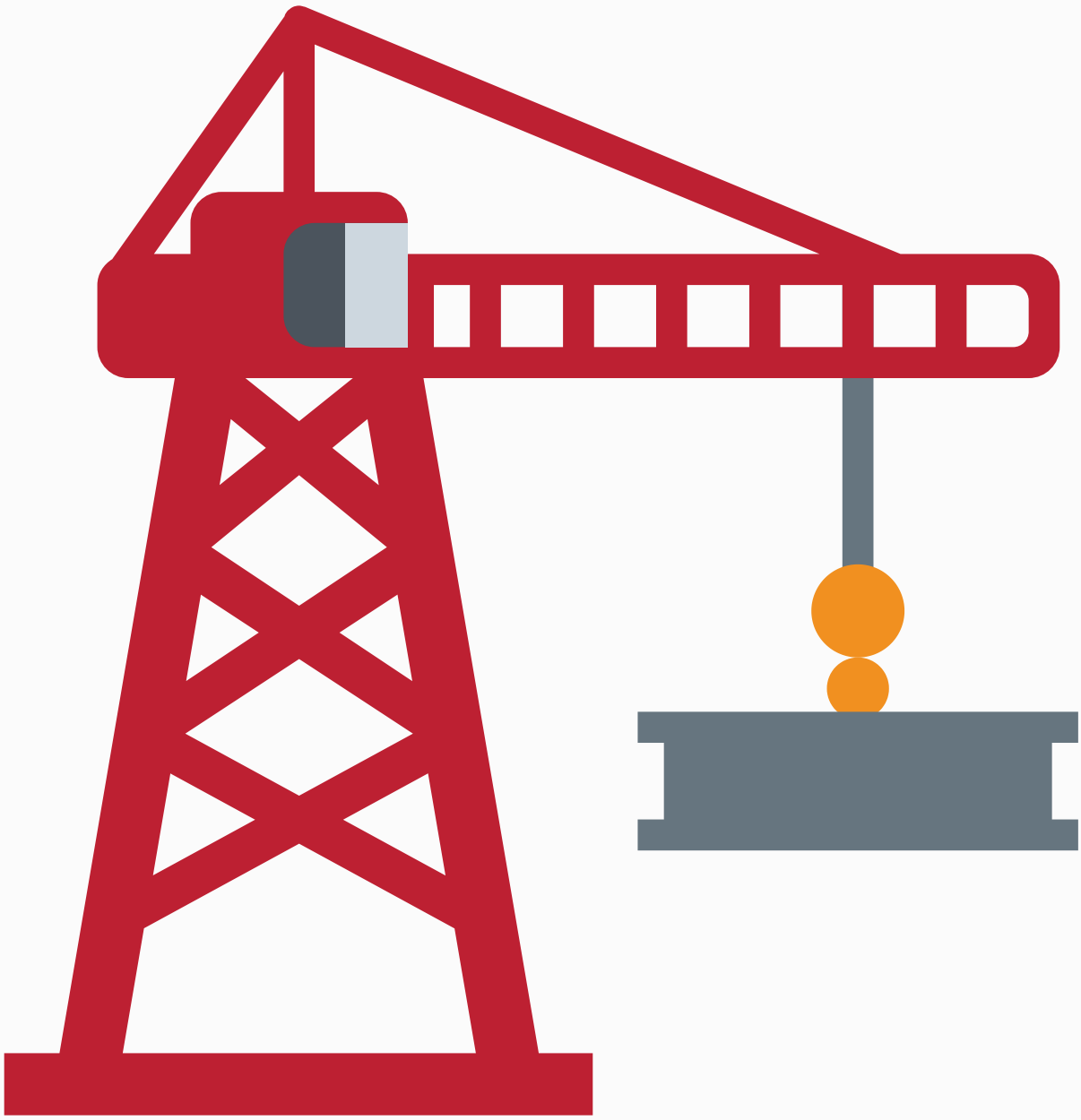
85% reduction in audit preparation time

Challenge: Ensuring HIPAA compliance while enhancing real-time threat detection capabilities.
Implementation: Deployed User and Entity Behavior Analytics (UEBA) coupled with automated incident response playbooks.
Results: Achieved 100% HIPAA audit pass rates and prevented 67% of potential security incidents.
Compliance: Successfully implemented all 18 HIPAA technical safeguards.
Real-World Implementation Case Studies
Enterprise Deployment Scenarios
Financial Services
JP Morgan Chase
Challenge: Managing 150K daily security events with traditional methods was overwhelming.
Implementation: Integrated Security Orchestration, Automation, and Response (SOAR) with Machine Learning (ML) for anomaly detection.

Results: Achieved a 95% reduction in false positives, ensuring stringent SOX compliance.
ROI: Realized $3.2 million in annual savings through optimized operations.
Healthcare
Regional Medical Center
Government
Federal Agency
Challenge: Protecting against sophisticated nation-state threats and maintaining strict NIST compliance.
Implementation: Utilized AI-driven threat hunting techniques mapped to the MITRE ATT&CK framework.
Results: Achieved 89% technique coverage, resulting in zero breaches over the implementation period.
Achievement: Reached NIST CSF Tier 4 (Adaptive), demonstrating a highly proactive security posture.
Business Value & ROI
Measurable Business Impact
Year 1: 256% ROI
Break-even: Month 4
Success Factors
Keys to Successful AI-SOC Implementation
Phased implementation
Continuous validation
Iterative improvement



Technology



Open-source first
Proven tools (Elastic, TheHive, TensorFlow)
Cloud-native architecture

Process

People

Team upskilling
Change management
Executive support
Critical Success Metric
Start small → Validate early → Scale fast
Conclusions
The Bottom Line
"AI-SOC is not optional, it's survival"
Start your SOC transformation with open-source tools today
Q&A
Thank you for your attention!
Let's build secure, intelligent SOCs together
Questions & Discussion
Thank You for Your Attention
Ready for Your Questions

Matched Source