ANOMALOUS LOGIN DETECTION USING ELK(P06)

Mustafa Hussain

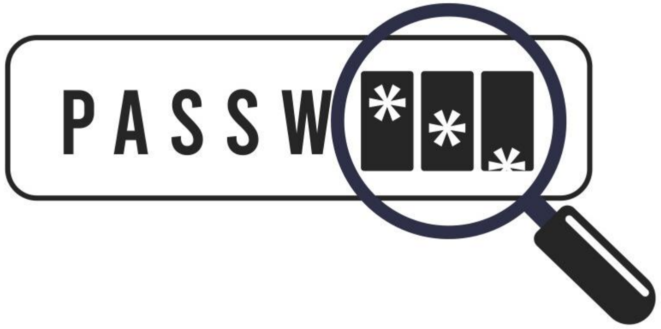
Affan Khan Niazi

Muhammad Mustafa

Shehroz faryad

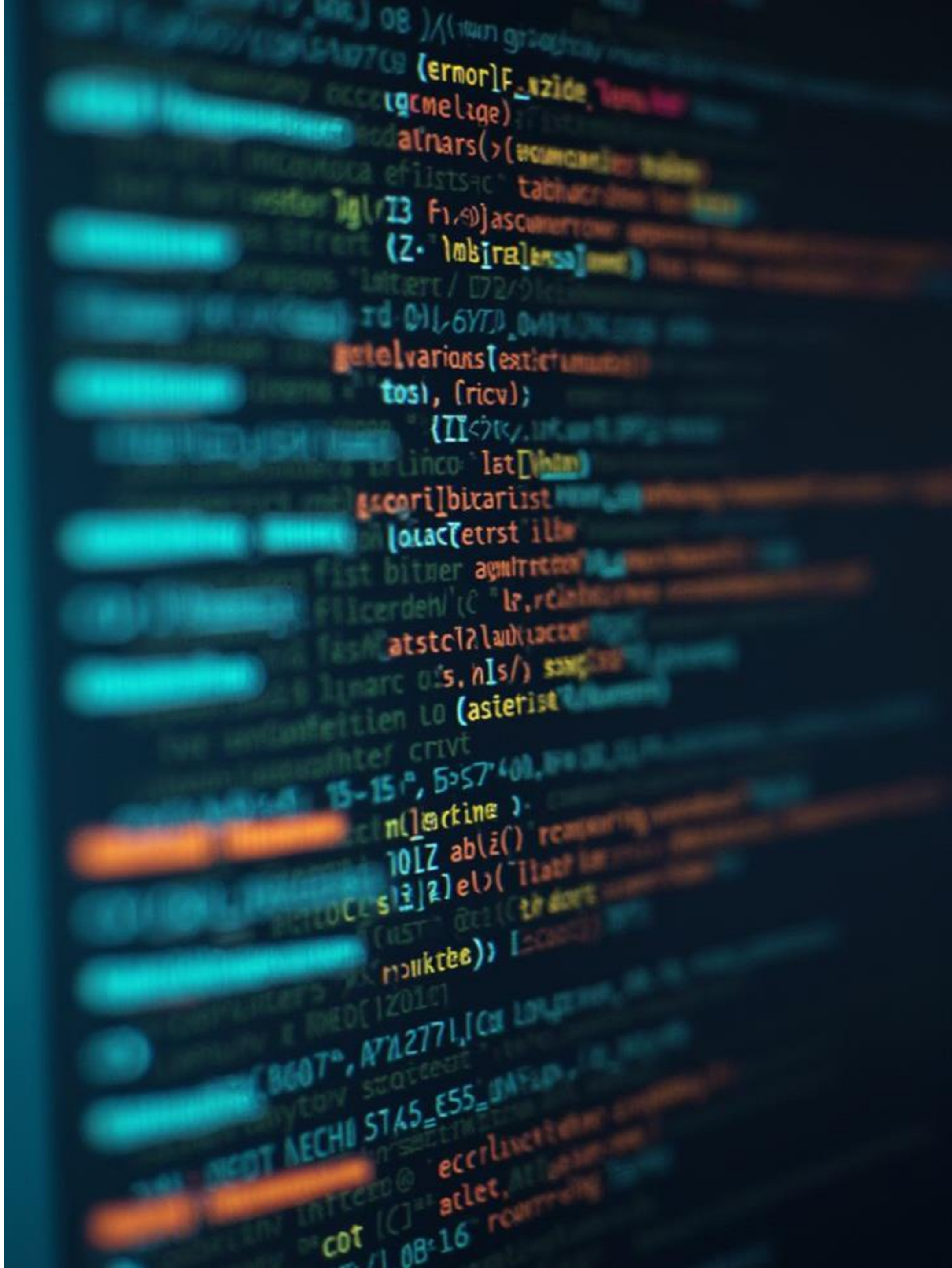
INTRODUCTION

- Detect suspicious login behavior in real-time
- Tools: **ELK Stack (Elasticsearch, Logstash, Kibana) + Wazuh SIEM**
- **Anomalies we detect**:
- Multiple failed login attempts (brute force)
- Login from unusual geo-location
- Impossible travel (different countries in minutes)
- Login at odd hours
- Privilege escalation (user → admin)
- New/unknown device login



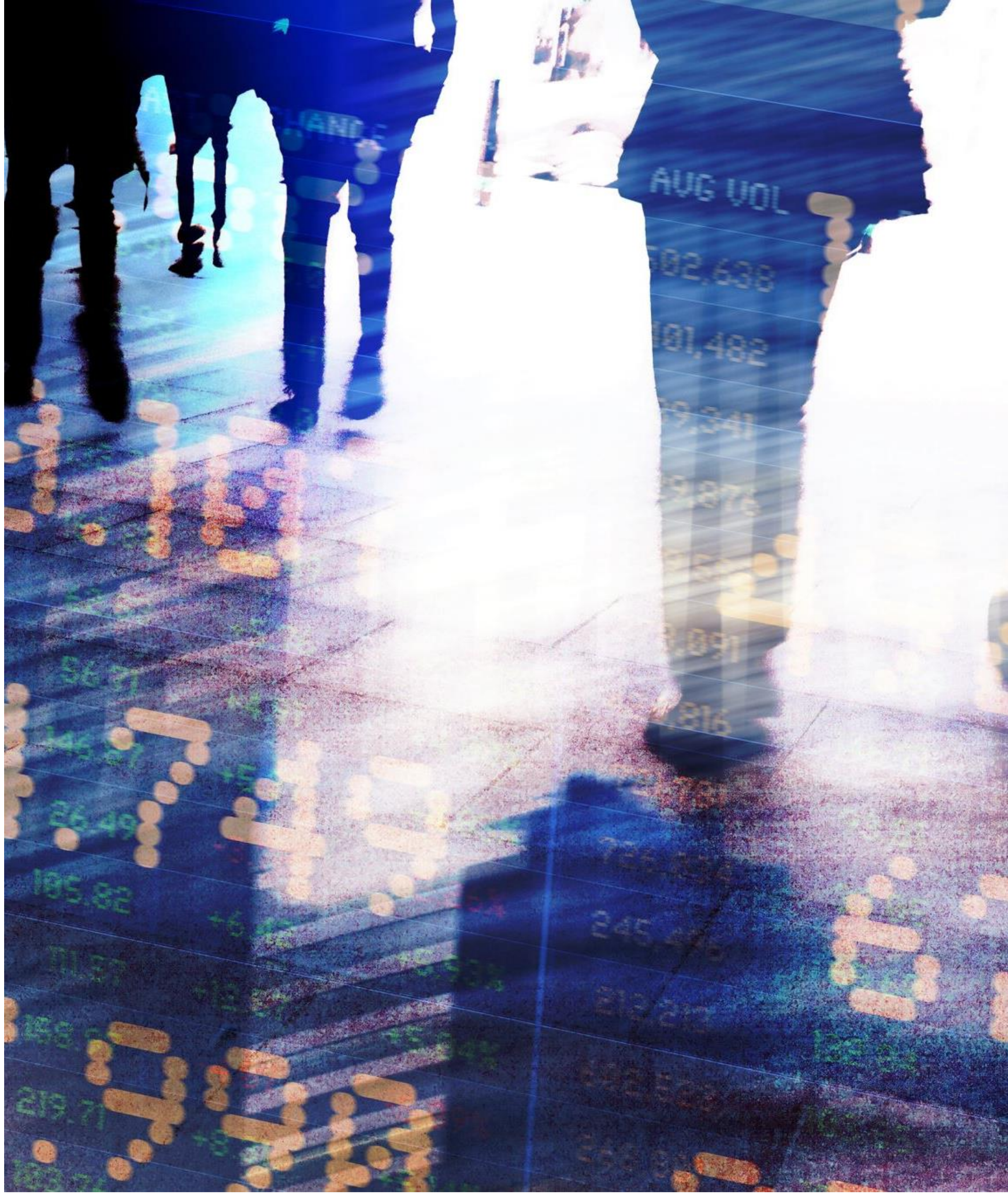
MAJOR REQUIREMENTS

- **Log Collection**
    - Authentication logs (Windows/Linux)
    - *Ebryx providing real-world data support*
- **Parsing & Storage**
    - Logstash for parsing, Elasticsearch for indexing
- **Detection Rules**
    - Multiple failed logins
    - Unusual geo-locations
    - Impossible travel (country switches in minutes)
    - Odd hour logins
    - Privilege escalation
    - New/unknown devices
- **Dashboards & Alerts**
    - Kibana dashboards
    - Wazuh alerting
- **Performance Goals**
    - ≥ 10,000 logs/sec



IMPACT ON USERS

- **System Administrators**
- Real-time dashboard for suspicious logins
- Faster response to incidents
- **Organizations**
- Reduced risk of breaches & account compromise
- Improved compliance & security posture
- **End Users**
- Better protection from unauthorized access
- Increased trust in system security
- **Industry Benefit**
- *Ebryx & similar companies* can use solution with real-world data



FUTURE EXTENSIONS

- **Machine Learning Integration**
- Adaptive anomaly detection with user behavior patterns
- **User Behavior Analytics (UBA)**
- Detect deviations from normal login habits
- **Cloud Integration**
- Support AWS, Azure, and GCP environments
- **Automated Incident Response**
- Block suspicious IPs, notify admins instantly
- **Enterprise-Grade Solution**
- Deploy as a security service for organizations (e.g., Ebryx, SOC teams)