EV ŞARJ İSTASYONU LOG ANOMALİSİ ANALİZİ

Log Pattern Tespiti ve Anomali Analizi

Hazırlayan: Eren Can Utku
Fırat Üniversitesi, Yazılım Mühendisliği

Analiz Tarihi: 05.11.2025

LOG ANOMALİSİ RAPOR GEREKSİNİMLERİ

- SWOT analizi dosyası (log anomali odaklı)
- Test script'i + log çıktısı (pattern analizi)
- Veri analizi (log anomali metrikleri)
- Savunma önerisi (log güvenliği)

1. LOG ANOMALİSİ SWOT ANALİZİ

LOG ANOMALİ TESPİT SİSTEMİ - SWOT	
GÜÇLÜ YÖNLER: • Regex tabanlı log pattern analizi • Gerçek zamanlı log işleme • Çoklu anomali kalıp türü tespiti • Düşük false positive oranı • Büyük log dosyaları işleme • Otomatik log ayrıştırma • JSON sonuç formatı	ZAYIF YÖNLER: • Log format değişikliklerine duyarlılık • Yeni anomali pattern manuel ekleme • Çok büyük dosyalarda bellek kullanımı • Zaman damgası format varyasyonları • Çok satırlı log entry sınırı • Encoding sorunları (UTF-8 dışı) • Log rotation sırasında veri kaybı
FIRSATLAR: • Machine Learning pattern öğrenme • Elasticsearch/ELK Stack entegrasyon • Streaming log analizi (Kafka) • Distributed processing (Spark) • SIEM sistemleri entegrasyonu • Cloud-native log servisleri • Log data mining & visualization	TEHDİTLER: • Log obfuscation teknikleri • Anti-forensics yöntemleri • Log tampering ve manipulation • Encrypted log kayıtları • NoSQL ve yapısız log formatları • Log flooding saldırıları • Binary log formatları

2. TEST SCRİPT + LOG PATTERN ANALİZİ

2.1 Log Anomali Tespit Script'i:
• Dosya: evcs_attack_analyzer.py
• Fonksiyon: Log satır bazında anomali arama
• Method: Regex pattern matching
• Input: evcs_system_detailed.log

2.2 Log Pattern Tespiti:
• İşlenen log satırı: 500
• Anomali tespit edilen: 39
• Anomali yoğunluğu: 7.8%

2.3 Tespit Edilen Log Anomali Pattern'leri:
CREDENTIAL_LEAK Pattern:
  auth token=([A-Za-z0-9]{8,}) Maskelenmemiş token

COMMAND_INJECTION Pattern:
  (rm\s+-rf|;\s*reboot|shutdown) Şüpheli komutlar

PRICE_MANIPULATION Pattern:
  set_price.*price=(\d+) Anormal fiyat değerleri

DOS_ATTACK Pattern:
  connection_flood|rate_limit_exceeded Trafik anomalisi

2.4 Log Analiz Başarı Metrikleri:
 Tüm log satırları ayrıştırıldı
 Anomali pattern'leri tespit edildi
 Satır numarası eşleştirmesi yapıldı
 JSON format sonuç üretildi

3. LOG VERİ ANALİZİ

3.1 Log İstatistiksel Özet:
• İşlenen toplam log: 500 satır
• Anomali tespit edilen: 39 adet
• Log anomali oranı: 7.80%

3.2 Log Anomali Türü Dağılımı:
• COMMAND_INJECTION: 9 adet (23.1%)
• PRICE_MANIPULATION: 10 adet (25.6%)
• CREDENTIAL_LEAK: 8 adet (20.5%)
• UNAUTHORIZED_ACCESS: 8 adet (20.5%)
• DOS_ATTACK: 4 adet (10.3%)

3.3 Log Pattern Risk Değerlendirmesi:
• Genel anomali seviyesi: CRITICAL
• Kritik log pattern'leri: COMMAND_INJECTION, UNAUTHORIZED_ACCESS
• Orta risk log pattern'leri: CREDENTIAL_LEAK, PRICE_MANIPULATION

3.4 Log Anomali Trend Analizi:
• Log anomali yoğunluğu: Yüksek (her 13 log'da 1 anomali)
• En yaygın log anomalisi: Komut enjeksiyonu pattern'i
• Log güvenlik açığı: Hassas veri maskeleme eksikliği

3.5 Log Format Analizi:
• Zaman damgası formatı: ISO 8601 (YYYY-MM-DDTHH:MM:SS)
• Log seviye dağılımı: INFO, WARN, ALERT, CRITICAL
• Ortalama log satır uzunluğu: ~100 karakter
• Log encoding: UTF-8

4. LOG GÜVENLİĞİ ÖNERİLERİ

4.1 Log Veri Güvenliği:

• Hassas Veri Maskeleme:
  - Token/şifre otomatik maskeleme
  - PII (Personally Identifiable Information) koruma
  - Credit card/finansal veri redaksiyonu

• Log Encryption:
  - Transit şifreleme (TLS 1.3)
  - Rest şifreleme (AES-256)
  - Log integrity checksums

• Access Control:
  - Role-based log erişimi
  - Log viewer authentication
  - Audit trail for log access

4.2 Log Anomali Monitoring:

• Real-time Log Analysis:
  - Stream processing ile anomali tespiti
  - Machine learning anomaly detection
  - Behavior-based pattern analysis

• Log Aggregation & Correlation:
  - Merkezi log toplama (ELK Stack)
  - Cross-system log correlation
  - Timeline analysis

4.3 Log Retention & Compliance:

• Log Retention Policy:
  - Operational logs: 90 gün
  - Security logs: 1 yıl
  - Compliance logs: 7 yıl

• Data Protection:
  - GDPR Article 32 uyumluluğu
  - Log anonymization teknikleri
  - Right to be forgotten compliance

4.4 Log Infrastructure Security:

• Log Server Security:
  - Hardened log servers
  - Network segmentation
  - Intrusion detection

• Backup & Recovery:
  - Automated log backups
  - Geographic distribution
  - Disaster recovery procedures

5. LOG ANOMALİ MATEMATİK ANALİZLERİ

5.1 Log Anomali İstatistik Formülleri:

• Log Anomali Tespit Oranı (LADR):
LADR = (Tespit Edilen Anomali / Toplam Log Satırı) × 100
LADR = (39 / 500) × 100 = 7.80%

• Log Pattern Entropy Hesaplama:
H(X) = -Σ P(xi) × log2(P(xi))
Yüksek entropy = Normal log patterns
Düşük entropy = Anomali patterns

5.2 Log İşleme Algoritma Karmaşıklığı:

• Log Parsing Döngüsü:

```
for line in log_file:              # O(n)
    for pattern in anomaly_patterns: # O(m)
        if regex.match(pattern, line): # O(k)
            detect_anomaly()
```

Toplam Karmaşıklık: O(n × m × k)
n = 500 (log satırları)
m = 10 (anomali pattern'leri)
k = 50 (ortalama regex karmaşıklığı)
Toplam işlem: 250,000 operasyon

5.3 Log Anomali Pattern Frequency Analysis:

• Pattern Frequency Distribution:
f(pattern) = count(pattern) / total_anomalies
Most frequent pattern = COMMAND_INJECTION
Least frequent pattern = REPLAY_ATTACK

• Log Anomali Clustering:
K-means clustering için optimal k:
k = √(n/2) where n = anomaly_count
Optimal k = √(39/2) ≈ 4

5.4 Log Performance Metrikleri:

• Log Processing Throughput:
Throughput = 500 lines / processing_time
Target: > 1000 lines/second

• Memory Usage Estimation:
Log size: 50000 bytes (avg 100 char/line)
Pattern storage: 10 × 50 bytes = 500 bytes
Result storage: 39 × 200 bytes

• Log Anomali Confidence Interval (95%):
CI = detection_rate ± (1.96 × √(p(1-p)/n))
p = anomali_rate, n = sample_size
95% CI: 0.078 ± 0.021