RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK TREND AND AGGREGATES

This module is an introduction to some analytics used in risk monitoring

- Trend Analysis
- Aggregation Analysis

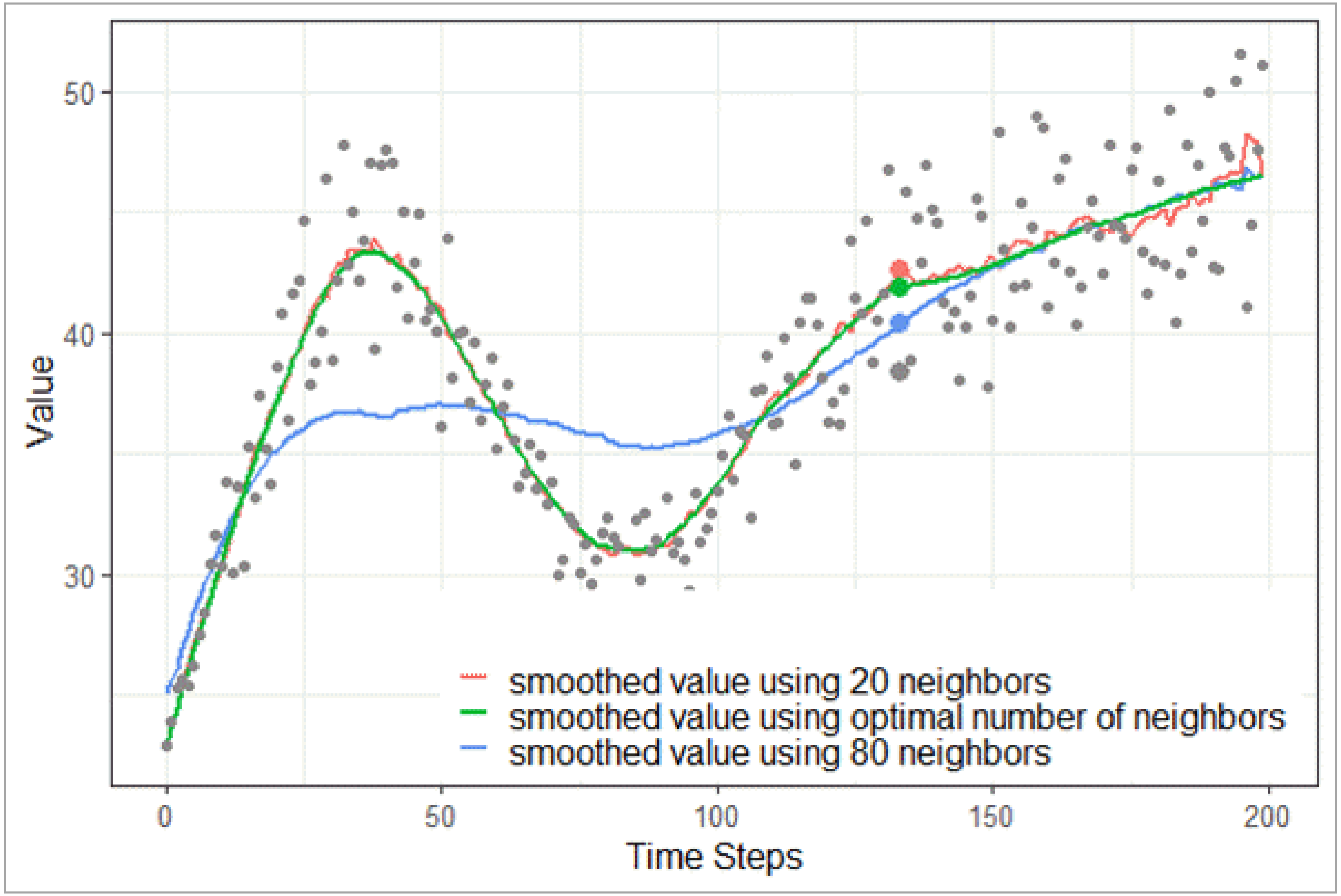
TIME SERIES/AGGREGATE ANALYSIS

- Monitoring longitudinal behavior, not just point-in-time metrics
  - Time-series approaches detect patterns, anomalies, and accumulative risks that indicate systemic vulnerabilities
  - Why time-series analysis matters
    - Identifies slow-moving, chronic failures (e.g., growing patch backlog).
    - Reveals seasonality or cyclical patterns (e.g., transaction spikes causing stress).
    - Highlights drift in performance or control effectiveness.
    - Provides early warnings when multiple KRIs deteriorate simultaneously.
  - Mature organizations aggregate metrics across:
    - Business units (e.g., rising access exceptions across departments)
    - Systems (e.g., API latency trends across microservices)
    - Geographies (e.g., region-wide authentication failures)
    - Control families (e.g., decline in detective control success rates)

ADVANCED ANALYTICAL TECHNIQUES

- Moving averages /exponential smoothing
  - Purpose
    - Smooth noisy data to expose underlying trends and direction.
  - Example in risk monitoring
    - KRI: Failed login attempts per hour (indicator of brute-force attack or credential abuse)
    - Raw failed login counts are highly volatile
    - Using a 7-day moving average, a rising trend becomes visible even if daily values fluctuate
    - Exponential smoothing assigns higher weight to recent values, making emerging attacks easier to spot
  - Outcome
    - The SOC detects an upward directional trend in authentication anomalies
    - This triggers proactive controls like throttling, geo-blocking, or requiring MFA challenges

SMOOTHING

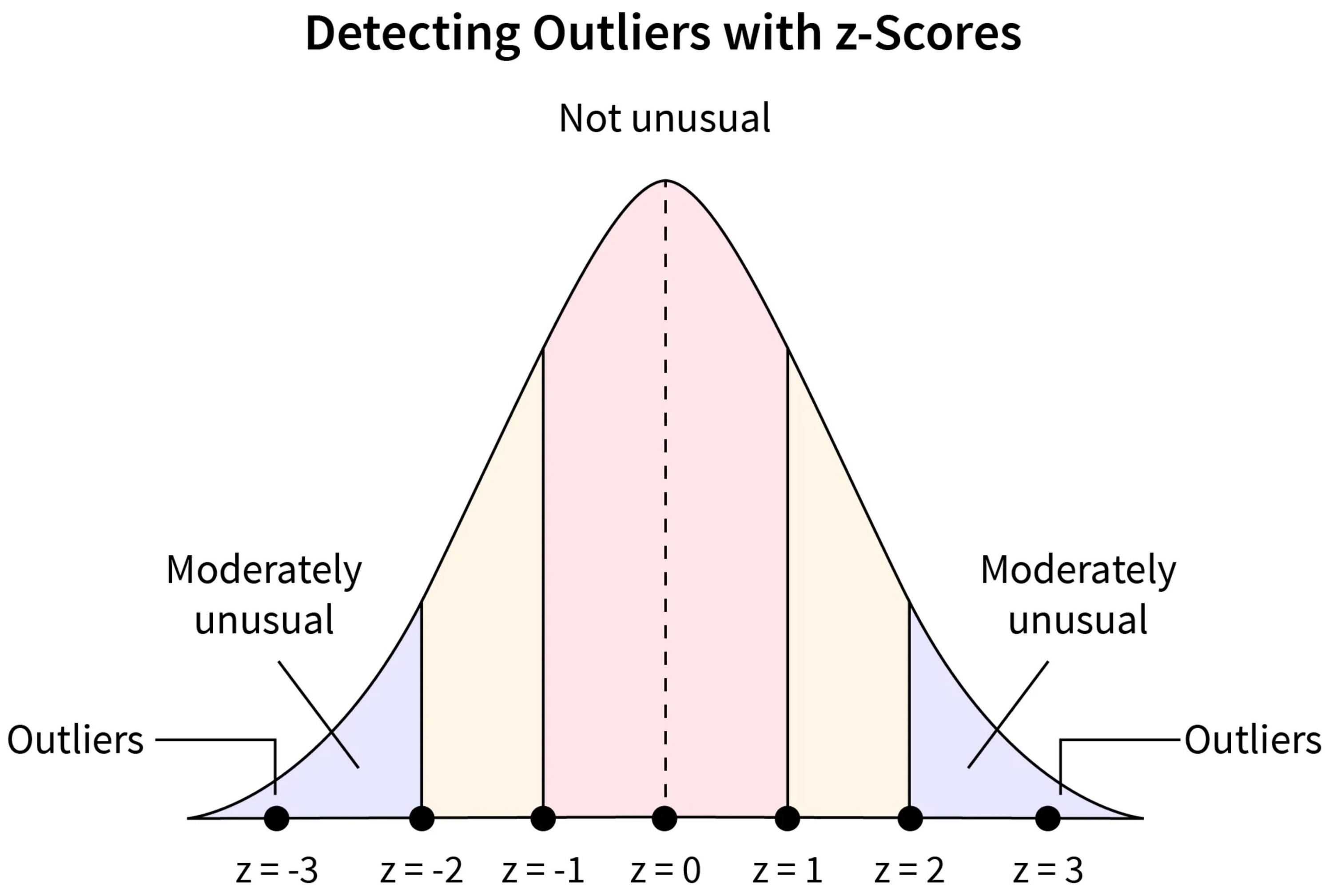


Value
50
40
30
Time Steps
0
50
100
150
200
smoothed value using 20 neighbors
smoothed value using optimal number of neighbors
smoothed value using 80 neighbors

ADVANCED ANALYTICAL TECHNIQUES

- Z-Score Normalization / outlier detection
  - Purpose
    - Identify values that deviate significantly from normal behavior
  - Example in risk monitoring
    - KRI: Outbound data transfer volume from a sensitive database
    - The system computes a Z-score for each hour’s outbound traffic
    - Z-score > 3 (three standard deviations above the mean) triggers a security alert for potential data exfiltration
    - Even if the transfer size is below an absolute threshold, statistical deviation flags the anomaly
  - Outcome
    - An insider threat or compromised account can be detected before significant data is lost, based solely on abnormal behavior relative to historical patterns

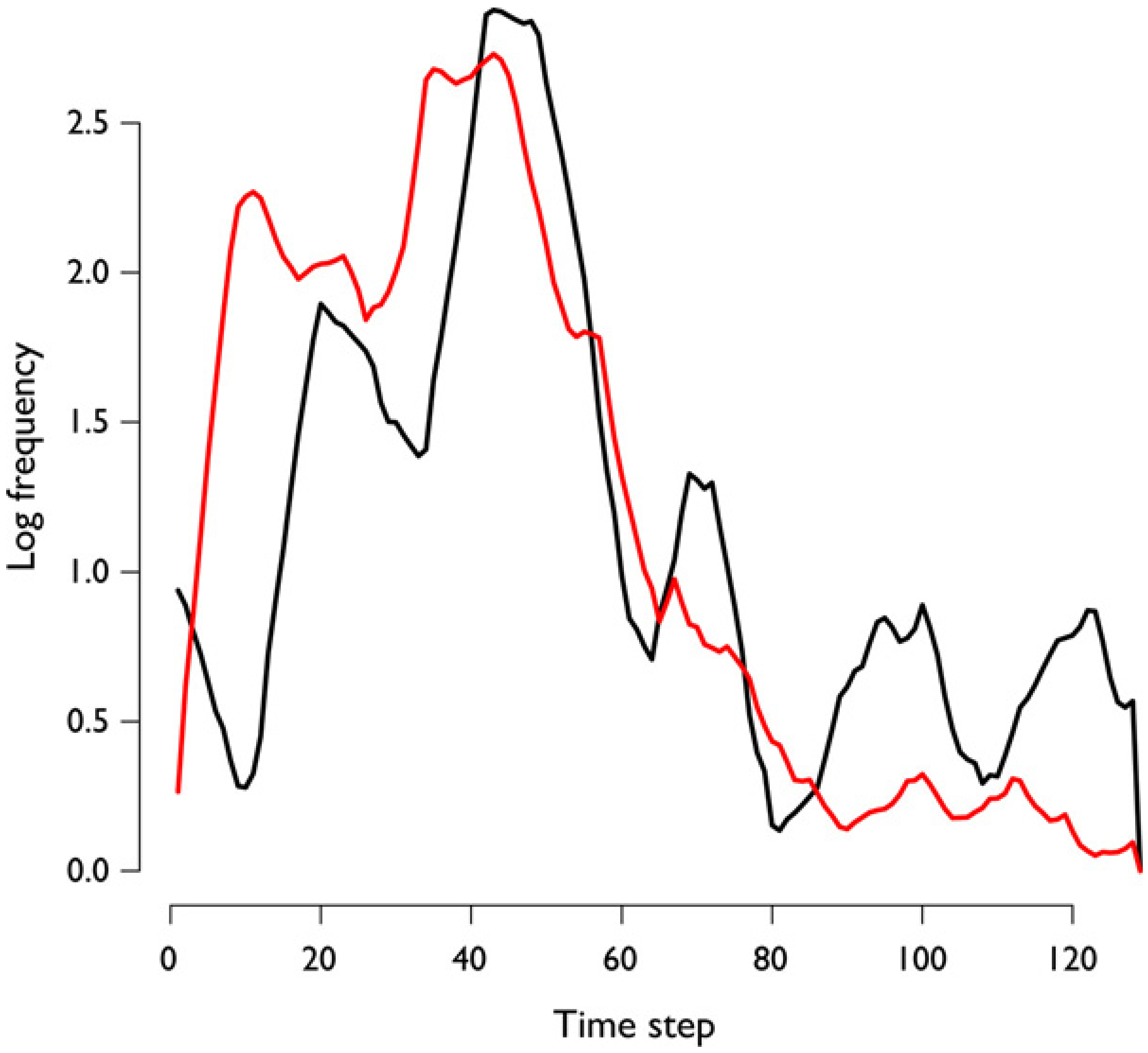
Z-SCORE


Detecting Outliers with z-Scores
Not unusual
Moderately unusual
Moderately unusual
Outliers
Outliers
z = -3
z = -2
z = -1
z = 0
z = 1
z = 2
z = 3

ADVANCED ANALYTICAL TECHNIQUES

- Lag analysis
  - Purpose
    - Measure whether changes in one metric precede changes in another metric
  - Example in risk monitoring
    - KPI: Patch completion rate vs KRI: Count of critical vulnerabilities
    - Lag-7 analysis reveals
    - A decrease in patch completion today correlates with
    - An increase in critical vulnerabilities seven days later
  - Outcome
    - Risk teams can demonstrate a causal or predictive relationship between a KIR and heightened vulnerability exposure which strengthens the case for resource allocation or process redesign

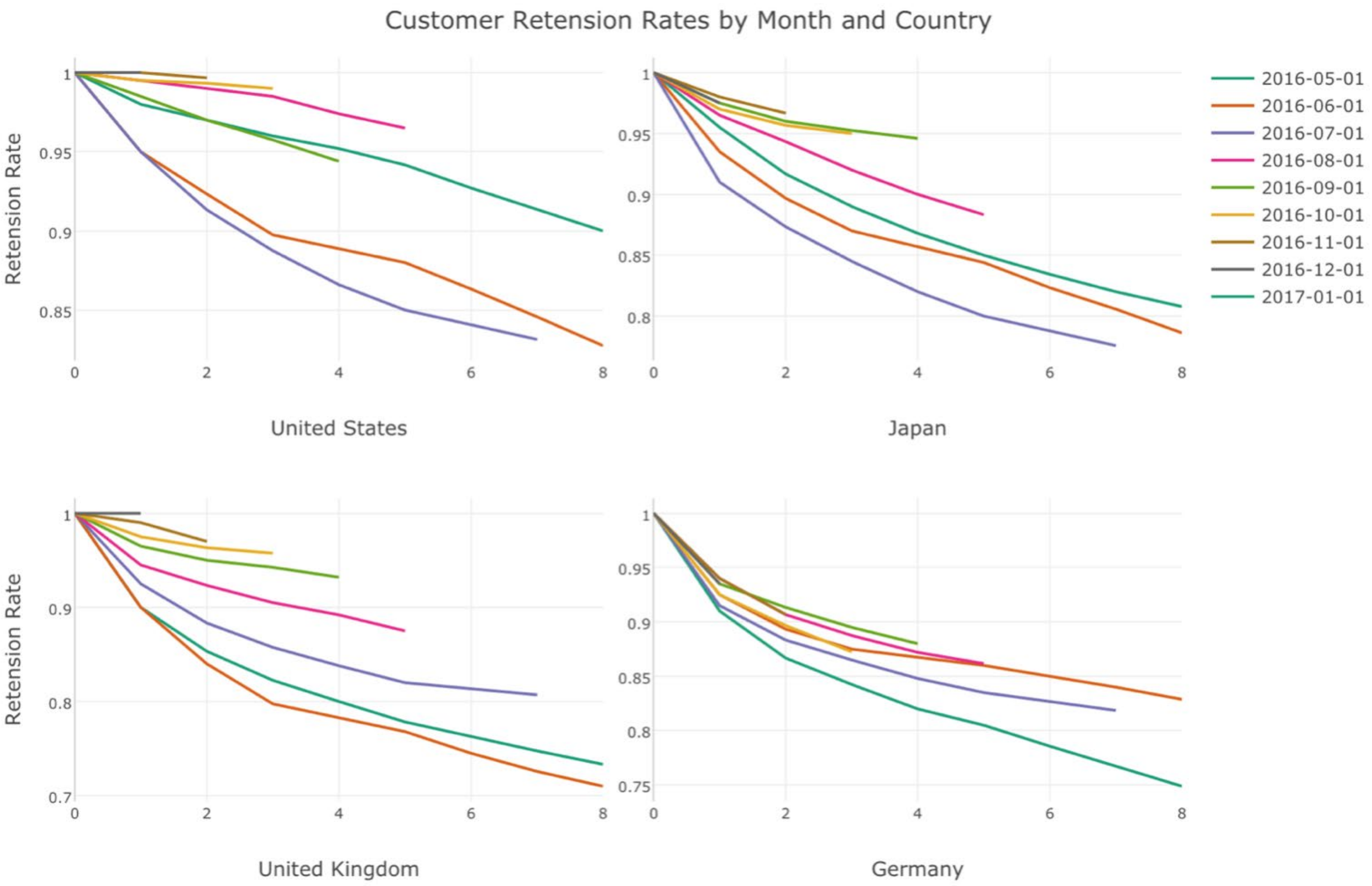
LAG ANALYSIS



ADVANCED ANALYTICAL TECHNIQUES

- Cohort trend analysis
  - Purpose
    - Compare similar groups (cohorts) to find patterns or outliers within a category
  - Example in risk monitoring, cohorts are created by
    - Application type (web apps vs. batch apps)
    - Technology stack (Java vs. Node vs. Python)
    - Environment (production vs. staging)
    - Ownership (Team A vs. Team B)
  - A cohort analysis reveals
    - Systems owned by Team B show a 3× higher growth rate of high-severity vulnerabilities compared to similar systems owned by other teams.
  - Outcome
    - This reveals a team-specific process breakdown rather than a global security weakness suggests targeted training, staffing, or process intervention can be deployed

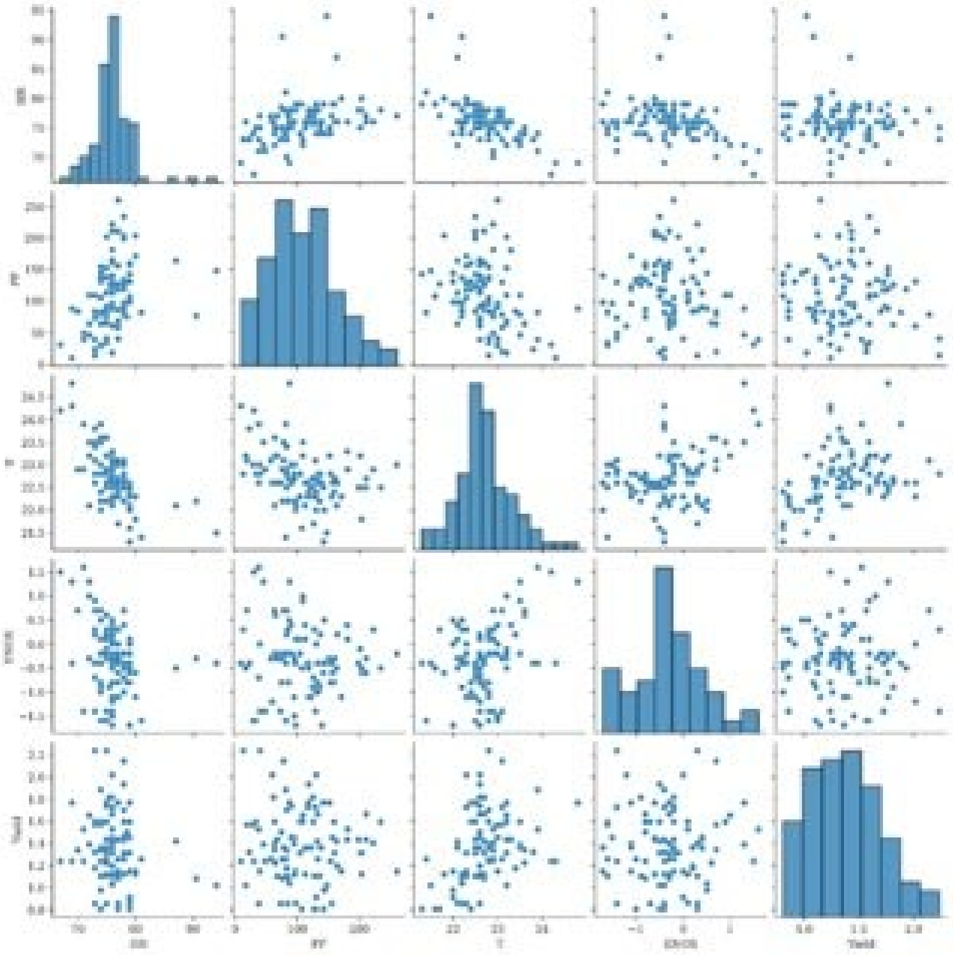
COHORT ANALYSIS



ADVANCED ANALYTICAL TECHNIQUES

- Cross-correlation matrices
  - Purpose
    - Identify how metrics influence each other across time.
  - Metrics include
    - KPI: Mean Time to Recover (MTTR) for incidents
    - KRI: Incident frequency
    - KPI: Change success rate
    - KRI: Number of repeated near misses
  - Cross-correlation shows
    - When change success rate decreases
    - Incident frequency increases with a correlation coefficient of 0.82
    - Additionally, higher MTTR correlates with a rise in repeated near misses, suggesting control inefficiency
  - Outcome
    - The correlation matrix grounds the argument that unstable change processes are the root cause of operational risk increases which should trigger major change-control reforms

CROSS-CORRELATION MATRICES



ADVANCED ANALYTICAL TECHNIQUES

- Composite KRI Index
  - Purpose
    - Combine disparate KRIs into a single normalized risk score that can be tracked over time
  - Combine KRIs such as
    - Number of critical vulnerabilities (weighted 30%)
    - Privileged access exceptions (20%)
    - Failed login anomalies (20%)
    - Backup integrity failures (15%)
    - End-of-life infrastructure ratio (15%)
  - Outcome
    - The correlation matrix grounds the argument that unstable change processes are the root cause of operational risk increases which should trigger major change-control reforms

ADVANCED ANALYTICAL TECHNIQUES

- Composite KRI Index
  - Using normalized values and weights produces a Composite KRI Index (0–100).
  - Example trend
    - Q1: 42
    - Q2: 49
    - Q3: 63
    - Q4: 71
  - Even without a major incident, the index shows a clear erosion of risk posture, prompting leadership to invest in remediation before conditions worsen
  - Composite indices provide:
    - Board-friendly reporting
    - Cohesive trend visibility
    - A single metric that captures complex, multidimensional risk exposure
    - This enables strategic prioritization and budget planning

Q&A AND OPEN DISCUSSION