SECURITY SIMPLIFIED:
Decoding Data Forensics into Enforceable Evidence

Lisa S. O’Leary, Ph.D. – V.P., Product and Service Management
Corina M. Owens, Ph.D. – Manager, Client Solutions
& Senior Psychometricians

MORE

Technology in our Measurement
Measurement in our Technology

VALIDITY

Alpine Testing Solutions
Technology-Enabled, People-Powered, Validity-Centered

Test Development & Psychometric Solutions
Customized, technology-enhanced assessment development and consulting services

CertMetrics – Candidate, Credentialing, & Exam Data Management
Integrated credential logic, exam data, and candidate management platform

Security Simplified - Exam & Program Security
Comprehensible prevention, mitigation, detection, and enforcement outcomes

Development Platform & Test Delivery Solutions
Unified ecosystem inclusive of item banking, publication, and delivery options
Systematic Security

Prevention
Mitigation
Detection
Enforcement
• defining what preventative actions can be taken to deter anomalous testing behavior,
• defining what data forensic and statistical analyses could be run to address your testing programs unique needs (and how to interpret those findings in a useful way),
• providing guidance on defensible enforcement actions, and
• recommending mitigation strategies to implement at the exam and program level to decrease security issues in the future.
Prevention

• Rapid and robust content development
  • Deep item banks
• Publication strategy and cadence that matches your exam audience and security concerns
• Alignment of policies across your program
• Delivery modality and selection of delivery providers
• SME and system protocols
• Verified credentials
<table>
<thead>
<tr>
<th>Retake Policy Rules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failing Outcome Waiting Period</td>
<td>Flags when a candidate violates retake policy for attempt AFTER FAIL within x number of days</td>
</tr>
<tr>
<td>Passing Outcome Waiting Period</td>
<td>Flags when a candidate violates retake policy for retake attempt AFTER PASS within x number of days (RECERTIFICATION POLICY)</td>
</tr>
<tr>
<td>Pass in Perpetuity</td>
<td>Flags when a candidate violates retake policy for any attempt AFTER PASS (EXAM STATUS FOR LIFE)</td>
</tr>
<tr>
<td>Total Attempts in Time Limit</td>
<td>Flags when a candidate violates retake policy for total number of attempts exceeds x within z timeframe</td>
</tr>
</tbody>
</table>
Mitigation

• Active monitoring of item, form, and candidate performance trends throughout the life cycle of exams and programs
  • Same exam across time
    • Review longitudinal data to determine exam specific next steps
  • Same program across exams
    • Review aggregate data to discuss programmatic patterns
Mitigation: Web Crawling

• Aides in the monitoring of stolen exam content that is available on the web
  • Availability and amount of exam content available on the web is clear and obvious evidence that content has been exposed
• May be used in conjunction with forensic analyses or used independently
Mitigation

- Warning lights activated, now what?
  - Conduct targeted data forensics based on security concern
  - Revisit prevention strategies to take exam specific action
    - Content development
    - Form publication
    - Exam delivery
- Adjust and communicate
  - Candidate policies
  - Delivery provider agreements
  - Test design details
Data Forensics: CertMetrics Security Scripts – Piracy and Access to Content

<table>
<thead>
<tr>
<th>Exam Time Rules</th>
<th>Item Skipped or Answered Too Quickly</th>
<th>x% of items skipped or answered in less than y seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exam Passed Too Quickly</td>
<td>Scoring more than x% in less than y minutes</td>
<td></td>
</tr>
<tr>
<td>Exam Taken Too Quickly</td>
<td>Less than y minutes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exam Form Rules</th>
<th>Exam retake score increase too high</th>
<th>x% score increase in y days</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Item Performance Comparison Rules</th>
<th>Item Subset Differential</th>
<th>x% or more for Subset 1 &amp; y% or less for Subset 2</th>
</tr>
</thead>
</table>
Data Forensics – Piracy and Access to Content

- Identification of Candidates’ Pre-Knowledge
  - Differential Person Functioning (DPF)
  - Bivariate Score by Time (BST)
- Identification of Exposed Content
  - Differential Item Functioning (DIF)
  - Drift
  - Unscored-Only Analysis
Data Forensics – Candidate Conduct

• Collusion among test takers
  • Response Similarity Index (RSI) Analyses
  • Score Similarity Index (SSI) Analyses
  • Cluster Analyses

• Proxy Test Taking
  • Flags from delivery provider
  • Behavior analyses
  • Proctoring information
  • Collusion analyses
## Data Forensics – Candidate Conduct

<table>
<thead>
<tr>
<th>Item Performance Comparison Rules</th>
<th>Approximation Score Similarity Index (SSI)</th>
<th>Z-score threshold + # of matches</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Approximation Response Similarity Index (RSI)</td>
<td>Z-score threshold + # of matches</td>
</tr>
</tbody>
</table>
## Similarity Indices with Clustering

<table>
<thead>
<tr>
<th>Form</th>
<th>Total No. of Candidate Records</th>
<th>Total No. of Pairs Analyzed</th>
<th>No. of Flagged Pairs</th>
<th>Percent Flagged Candidate Pairs</th>
<th>No. of Unique Candidate Records Flagged</th>
<th>Percent Flagged Candidate Records</th>
<th>No. of Clusters</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>4,883</td>
<td>11,919,403</td>
<td>536</td>
<td>0.004%</td>
<td>281</td>
<td>5.75%</td>
<td>97</td>
</tr>
<tr>
<td>B</td>
<td>4,828</td>
<td>11,652,378</td>
<td>323</td>
<td>0.003%</td>
<td>247</td>
<td>5.12%</td>
<td>94</td>
</tr>
</tbody>
</table>

![Observed Matches vs. Expected Matches](image1)

![Observed Matches vs. Expected Matches](image2)
## Criteria for Describing Likelihood of Involvement in Other Suspicious Activity

### Extreme
- Extreme RSI/SSI p-values <1.0E-07, 3+ BST Flags (HS/LT)
- Extreme RSI/SSI p-values

### Very High
- RSI and BST (HS/LT) flag
- Extreme SSI p-value
- Extreme SSI p-value and RSI flag

### High
- RSI and BST (HS/LT) flag
- 3+ <20 Sec and BST Flags, 5+ SSI Flags
- 10+ SSI flags, min SSI p-value <1.0E-05
- 10+ SSI flags, RSI Flag
- 10+ SSI flags, BST or <20 Sec flag
- 5+ SSI flags, min SSI p-value <1.0E-05, RSI Flag
- 5+ SSI flags, min SSI p-value <1.0E-05, and BST/<20 sec flag
- Multiple RSI Flags

### Moderate
- 3+ BST Flags (HS/LT)
- 3+ <20 Sec and BST Flags
- 10+ SSI flags
- 5+ SSI flags, min SSI p-value <1.0E-05

### Written

<table>
<thead>
<tr>
<th>Level of Suspicion</th>
<th>Date</th>
<th>Testing Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0) Moderate</td>
<td>8/11/2021</td>
<td>xz0x</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>5/1/2021</td>
<td>5</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>10/24/2021</td>
<td>z6</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>11/8/2021</td>
<td>5xz6</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>10/16/2021</td>
<td>6x</td>
</tr>
<tr>
<td>(1) High</td>
<td>3/3/2021</td>
<td>9y02</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>3/8/2021</td>
<td>9y02</td>
</tr>
<tr>
<td>(2) Very High</td>
<td>5/4/2021</td>
<td>x6x8</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>Extreme RSI/SSI p-values</td>
<td>(3) Extreme</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>5+ SSI flags, min SSI p-value &lt;1.0E-05, RSI Flag</td>
<td>(1) High</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>10+ SSI flags, min SSI p-value &lt;1.0E-05</td>
<td>(1) High</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>10+ SSI flags, min SSI p-value &lt;1.0E-05</td>
<td>(1) High</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>10+ SSI flags</td>
<td>(0) Moderate</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>10+ SSI flags</td>
<td>(0) Moderate</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>10+ SSI flags</td>
<td>(0) Moderate</td>
</tr>
<tr>
<td>(0) Moderate</td>
<td>6/20/2021</td>
<td>9y06</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Written</th>
<th>Decimal Notation</th>
<th>Scientific Notation</th>
<th>Excel Scientific Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 in 10</td>
<td>0.1</td>
<td>10⁻¹</td>
<td>1.0E-01</td>
</tr>
<tr>
<td>1 in 100</td>
<td>0.01</td>
<td>10⁻²</td>
<td>1.0E-02</td>
</tr>
<tr>
<td>1 in 1,000</td>
<td>0.001</td>
<td>10⁻³</td>
<td>1.0E-03</td>
</tr>
<tr>
<td>1 in 10,000</td>
<td>0.0001</td>
<td>10⁻⁴</td>
<td>1.0E-04</td>
</tr>
<tr>
<td>1 in 100,000</td>
<td>0.00001</td>
<td>10⁻⁵</td>
<td>1.0E-05</td>
</tr>
<tr>
<td>1 in 1,000,000</td>
<td>0.000001</td>
<td>10⁻⁶</td>
<td>1.0E-06</td>
</tr>
<tr>
<td>1 in 10,000,000</td>
<td>0.0000001</td>
<td>10⁻⁷</td>
<td>1.0E-07</td>
</tr>
<tr>
<td>1 in 100,000,000</td>
<td>0.00000001</td>
<td>10⁻⁸</td>
<td>1.0E-08</td>
</tr>
<tr>
<td>1 in 1,000,000,000</td>
<td>0.000000001</td>
<td>10⁻⁹</td>
<td>1.0E-09</td>
</tr>
</tbody>
</table>
Enforcement

• Consult with legal
• Establish written security policy
• Require candidate agreements
• Establish candidate appeals process
• Conduct comprehensive data forensics
• Triangulate multiple sources evidence of anomalous behavior prior to taking action
## Enforcement with CertMetrics

<table>
<thead>
<tr>
<th>Candidate Access Rules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watch List Test Taker</td>
<td>Flags at the time of import when a candidate that is on an established Watch List takes an exam (administration date)</td>
</tr>
<tr>
<td>Banned Candidate Test Taker</td>
<td>Flags at the time of import when a candidate that is on an established Banned List takes an exam (administration date)</td>
</tr>
<tr>
<td>Prohibited Country Test Taker</td>
<td>Flags at the time of import when a candidate, with a home address in a client-specified prohibited country (by ISO verified country)</td>
</tr>
</tbody>
</table>
Enforcement Actions

- Warning email
- Require review prior to exam/certification results being available
- Restriction on future registration
- Exam status change
- Credential status change
- Add to watch list
- Add to banned list
• Document security prevention, mitigation, detection, and enforcement policies
• Consult with your legal team/advisors on planned security policies and prior to taking any actions against candidates, test centers based on data forensic results
• Be transparent at a high-level with candidates regarding security policies
• Align candidate agreements with documented policies and processes
• Provide candidates the opportunity and means to challenge resulting actions
• Triangulate multiple sources of evidence of anomalous behavior
• Treat all candidates equally (e.g., do not target data forensic techniques at a particular subset of candidates)
• Continually evaluate of exam and program to assess appropriate actions
Questions? Please reach out as questions arise.
We would love to discuss all things security!
corina.owens@alpinetesting.com
lisa.oleary@alpinetesting.com