Analysis and Tools for Auditing Insider Accesses

DANIEL FABBRI, VANDERBILT UNIVERSITY

Cybersecurity Research Acceleration Workshop and Showcase, Indianapolis, IN
October 11, 2017

Cybersecurity Research Acceleration Workshop and Showcase

October 11, 2017 | Indianapolis, IN

Analysis and Tools for Auditing Insider Accesses

Quad Chart for:

Challenge:

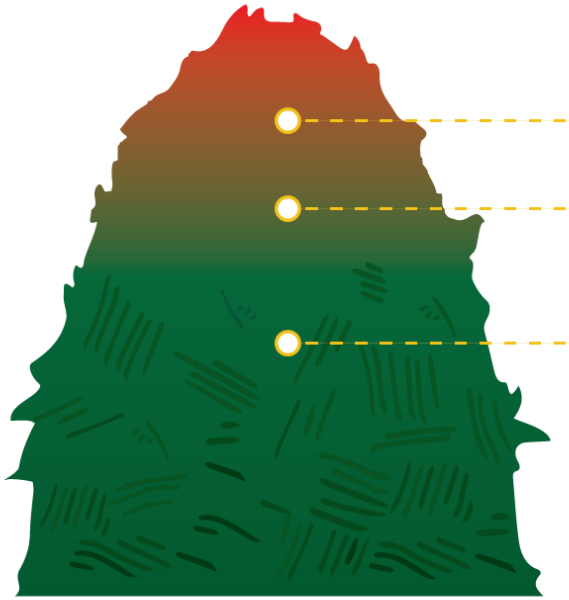
Identifying inappropriate access to electronic medical records

Solution:

- Graph-based machine learning
- Identify reason for each access
- Fill-in missing facts for analysis (enhanced explanations)
- Rank accesses by suspiciousness

Delivery System:

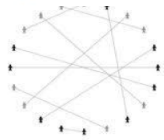
- Integrate with EMR systems
- Deploy as VM locally or in cloud



Ranking 1%

Enhanced explanations 97-99%

Filtered by explanations 95-97%



MAIZE ANALYTICS

Value proposition:

- Filtering 95-99% of accesses
- Reduce time to complete audits
- Focus auditors on suspicious behavior

Results:

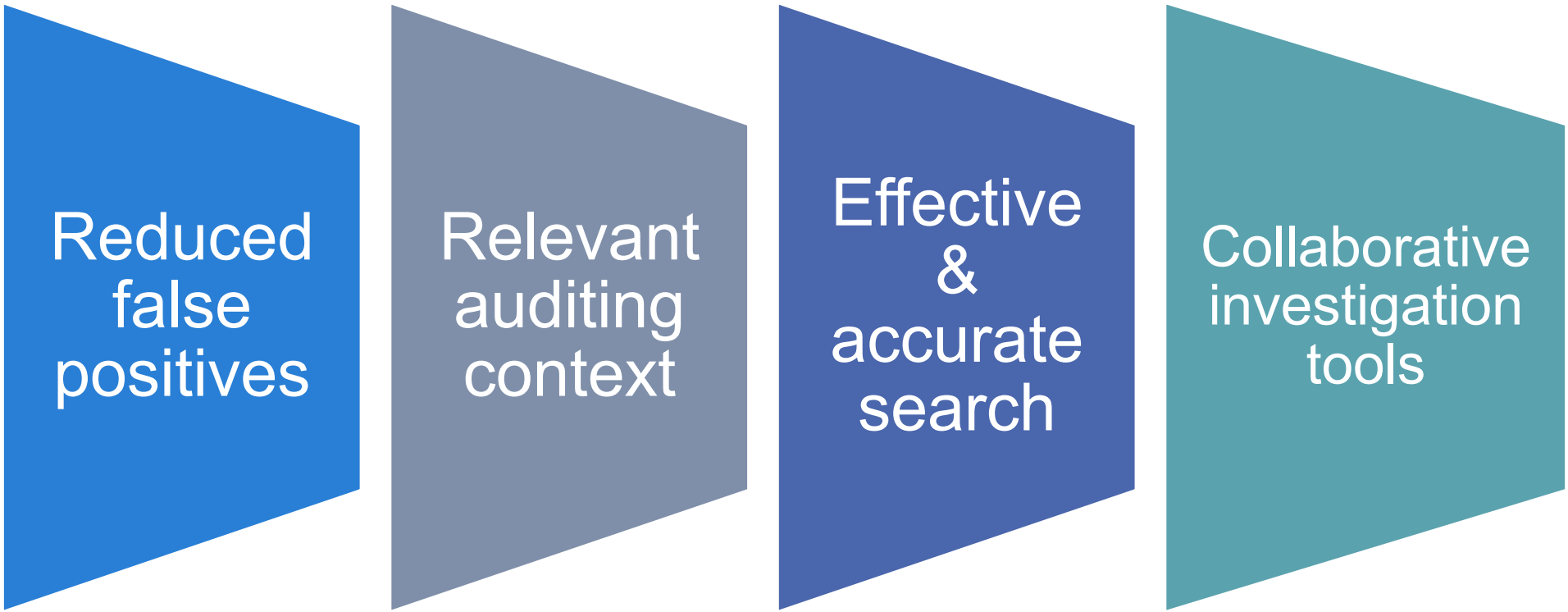
- NSF ICorps Completed: 2013
- Company created: Maize Analytics
- Growing user base (nearly profitable)

Contact us

- Daniel.fabbri@vanderbilt.edu

What Privacy Officers Ask For

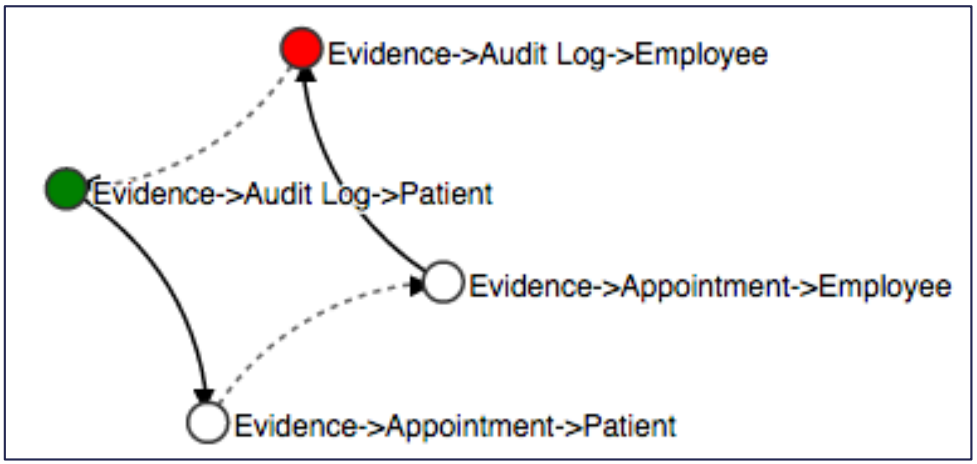
Problem: Monitoring for inappropriate access to patient data

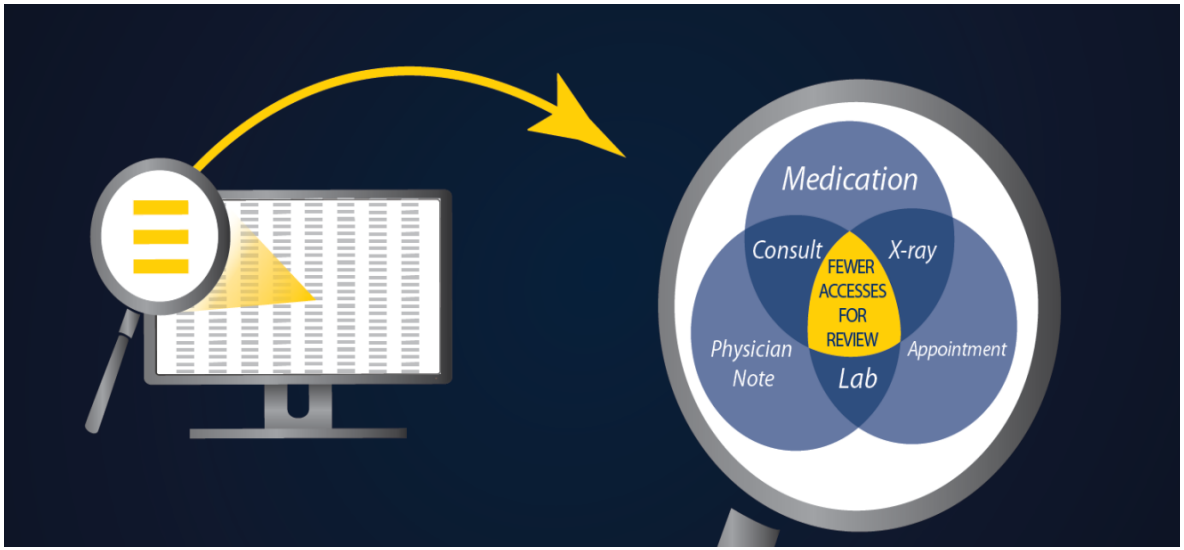


Efficient Search for Inappropriate Access

Find connections between patients and employees

Accesses with connections deemed to be appropriate





Automatically filter **95-98%** of accesses

Rank Suspicious Accesses

Challenges

Integration with EMR Systems

Cerner GE Healthcare Epic Allscripts…

Deployment (local vs cloud)

Hospital Sales:

- Need for reference
- Long time to close

Trajectory

NSF ICorps 2013

Started Company: Maize Analytics

Growing Team

Realization we needed non-tech skills (training, ops)

300+ Hospitals and Health facilities actively using Maize

Need to support each organization and specific needs