Advanced Analytics in Cyber Security

Michael McFadden
Fraud, Security & Compliance
August 1, 2017
Topics for Today’s Session

Streaming analytics to detect and stop cyber threats

Empirical analytics to assess cyber security posture
Streaming analytics to detect and stop threats
New Entry Points Bring New Risk

1994
Online Banking

2001
1 Million online users

2005
FFIEC announces regulation for online banking

2007
Apple launches iPhone and banking by phone launches

2011
Online Banking is now mainstream

2012
20%+ of all smartphone users use a mobile banking app

2013
One in three Americans state they stay with their bank because their mobile banking services make it convenient

2014
US m-commerce makes up 29% of web sales

2015
57% of US smartphone owners have used their devices for online banking

2016
Smartphone users will account for 96% of total mobile banking

© 2017 Fair Isaac Corporation.
Over 6 BILLION records exposed in first half of 2017*

There has been an alarming trend in the TARGETING OF TAX DATA. The number of confirmed successful attacks increased by 25%.

Current “State of the Art” in Cyber Security

- **Pattern-matching**
  - Technical analysis (unpacking or detonating malware) to define signatures
- **Cyber Criminals know the rules well enough to break them and avoid detection**
- **Exploit the Interoperability and demands for convenience**
- **Use Social Media for Phishing**
The gap between breach and discovery

When a breach occurs, the majority of sensitive data is stolen within minutes increasing this challenge.

### In 60% of breaches, data is stolen within hours

- **Seconds**
  - ATTACK TO COMPROMISE: 10%
  - COMPROMISE TO DATA LOSS: 8%
- **Minutes**
  - ATTACK TO COMPROMISE: 75%
  - COMPROMISE TO DATA LOSS: 38%
- **Hours**
  - ATTACK TO COMPROMISE: 12%
  - COMPROMISE TO DATA LOSS: 14%

### 54% of breaches are not discovered for months

- **Days**
  - ATTACK TO COMPROMISE: 2%
  - COMPROMISE TO DATA LOSS: 25%
  - TIME TO DISCOVERY: 13%
  - DISCOVERY TO REMEDIATION: 32%
- **Weeks**
  - ATTACK TO COMPROMISE: 0%
  - COMPROMISE TO DATA LOSS: 8%
  - TIME TO DISCOVERY: 29%
  - DISCOVERY TO REMEDIATION: 38%
- **Months**
  - ATTACK TO COMPROMISE: 1%
  - COMPROMISE TO DATA LOSS: 8%
  - TIME TO DISCOVERY: 54%
  - DISCOVERY TO REMEDIATION: 17%
- **Years**
  - ATTACK TO COMPROMISE: 1%
  - COMPROMISE TO DATA LOSS: 0%
  - TIME TO DISCOVERY: 2%
  - DISCOVERY TO REMEDIATION: 4%

Source: Verizon 2013 Data Breach Investigations Report
Shortcomings of the current "state-of-the-art" detection

MOST OF TODAY’S SECURITY SOLUTIONS HAVE FUNDAMENTAL FLAWS:

- Based on what happened yesterday (or last week or last year)
- Require human interpretation of events
- Lack the means to adapt and self-correct
- No effective method to differentiate alerts
- Threats have become dynamic, making rule-based approaches less effective
- Devices, access points, and use cases have grown exponentially
- Network complexity has evolved beyond expert capacity to understand

TOO MANY UNDIFFERENTIATED ALERTS

TOO MANY NEW / MORPHING / EVOLVING THREATS SLIPPING THROUGH

TOO FEW QUALIFIED RESOURCES TO INVESTIGATE AND RESOLVE CYBER THREATS
Machine Learning Analytics are the New Imperative in Cyber
Cybersecurity Analytics

Streaming data analysis

- Real-time threat detection
- Enables automated containment and faster remediation
- Scalable distributed processing

Self-learning UEBA

- Emerging threat detection
- Layered analytics model - Not limited to heuristics or peer group comparisons
- Responsive to analyst feedback through global consortium
- Continuous adaptation reduces false positives

Continuous entity scoring

- Entity profiling – devices, users, etc.
- Precise risk ranking with score range
- Simple results - score with detailed reasons to guide triage and response
Cyber Security Analytics – Key Highlights

Addresses Major Security Gaps

- Reduces threat dwell time through real-time detection
- Reduces false positives – precise detection using self-learning analytical model
- Improves efficiency of security professionals
  - Prioritizes threat risks through granular scoring
  - Simple Results – Score plus detailed reasons to guide analyst in investigation

Adaptable

- Self-learning AI technology
- Flexible model - Accommodates new data sources and entity types (IoT)
- Scalable - Doesn’t require large data store, fast streaming engine
- Modular design - Integrates with existing security eco-system solutions

Proven Technology

- Analytic Models have been used across industries to detect and stop fraud
- Numerous threat behaviors detected such as:
  - Reconnaissance activity
  - Command and Control (C&C) communication
  - Data Exfiltration
Empirical analysis to assess cyber security posture
Can your vendors and partners be trusted with your data?

- Customer records for at least **14 million subscribers**, including phone numbers and account PINs, were exposed.

- Records were found on an unprotected Amazon S3 storage server controlled by an employee of Nice Systems, a **vendor of Verizon**

- **Over a week** before the data was eventually secured.
Key challenges in cyber risk quantification

• The space is nascent, and commercial solutions are just coming on the scene.

• Available metrics are expert-driven, lacking an empirical, quantitative connection between conditions, behaviors, and outcomes.

• Typical scores or ratings are backwards-looking assessments, or focus on current state rather than future outcomes - which is what is actually needed to drive business decision making.

• As good metrics evolve, transparency will be key in allowing market forces to increase our collective security posture.

• The state of the art in cyber breach insurance is pre-actuarial, and currently more art than science. A large proportion of cyber risk remain un-quantified and un-covered, or are “silent cyber” risks, not expressly excluded from other E&O policies.
Parallel Paths – a Historical Perspective

1990s Consumer Credit Scoring

Opportunity
• Apply predictive analytics to drive efficiency and scale in consumer credit underwriting and portfolio management

Solution
• Consumer Credit Scoring
• Rank-order consumers based on likelihood of paying their credit obligations

Result
• Adoption of Credit Scoring now ubiquitous in credit decisions
• Greatly expanded access to consumer credit

2017 Enterprise Security Scoring

Opportunity
• Apply predictive analytics to drive efficiency and scale in active vendor management and executive-level security oversight

Solution
• Enterprise Security Scoring
• Rank-order organizations based on likelihood of suffering a material data breach

Result
• Empirically-derived assessment of risk
• Trusted metric for active vendor management
• Consistent breach insurance underwriting and portfolio monitoring
Enterprise Security Scoring

- Predictive score based on supervised, empirical analysis of continuously updated data collected at internet scale.
- Score or Grade encapsulates the future likelihood of a significant breach event.
- Compares external network observations to previously breached networks.
- Combines condition and behavior signals.
- Reason codes detail primary risk vectors – enabling contextual explanation of results.
- Accessed “on-demand”
Security Scoring – The Data

- Data elements continually monitored at internet scale, reflecting:
  - Policy effectiveness
  - Management behaviors

- Data richness that supports empirical analysis, not judgment-based grades

- Data utilized reflects historical risk indicators from global organizations
  - Machine learning used to evaluate historical risk indicators to understand correlated pre breach behaviors
  - Risk indicators are then used in the predictive model as labels
Different Views of your Risk Posture

Internal Self Assessment
- Enable CISOs to demonstrate security performance over time
- Provides detailed threat info across all evaluated network assets
- Supports drill-down to primary threat vectors
- Strengthens defenses with actionable information
- Supports investment decisions and resource allocation

Third Party/Vendor Risk Assessment
- Supports CROs and CISOs in active vendor management
- Vet the risk of potential partners
- Monitor the risk of your entire partner portfolio
- Benchmark across categories or segments of partners
- Supports breach insurance underwriting
Enterprise Security Scoring – Key Highlights

**Empirical**
- Leverages an extensive array of **analytic techniques**
- **Supervised** modeling approach correlates signals with real outcomes
- Evaluates both **condition and inferred behavior**
- An **empirically-derived** benchmark of cyber risk, rather than an opinion-based ranking

**Predictive**
- Predictive model focuses on **future outcomes** rather than transient threats
- Visibility into enterprise security behaviors to **mitigate future potential failures**
- Aligns to **forward-looking** business objectives and outcomes

**Actionable**
- **User controls** scope of analysis and definition of enterprise
- Enables **sharing and collaboration**
- Integrates with ticketing and workflow systems for systematic **remediation**
- NIST controls cross-reference supports **compliance** initiatives

**Inform, Predict Odds of Breach, Remediate, Repeat**
# FICO Overview

| Profile | The leader in advanced analytics and decision management  
| | Founded: 1956  
| | • NYSE: FICO / $881M revenue FY2016  
| | • Analytics and decision management systems  
| | • Reducing the time from insight to action  
| Products and Services | • FICO Scores – used for 96% of US credit underwriting  
| | • Predictive analytics for risk management  
| | • AI systems for security threat and fraud detection  
| | • Advanced analytics for cyber risk quantification  
| | • Tools for analytics authoring and decision management  
| Clients and Markets | 10,000+ clients in 90+ countries  
| | Industry focus: Banking, government, insurance, logistics  
| Offices | 20+ offices worldwide, HQ in San Jose, California  
| | 3,100 employees  
| | Regional Hubs: San Rafael and San Diego (CA), New York, London, Birmingham (UK), Johannesburg, Milan, Moscow, Bensheim, Munich, Madrid, Istanbul, Sao Paulo, Bangalore, Beijing, Singapore |
Thank You

Michael McFadden
Fraud, Security & Compliance
michaelmcfadden@fico.com
(858) 369-8425