Fraud Detection and Advanced AI for Cyber Threats

Scott M. Zoldi, Ph.D
Chief Analytics Officer
FICO

@ScottZoldi

Simon Eappariello
SVP Product & Engineering
IBOSS

Schematic of a Better Approach

Real-time streaming approach

- Reducing mean time to discovery
- Enabling automated response/remediation

Unsupervised, self-learning entity behavior analytics

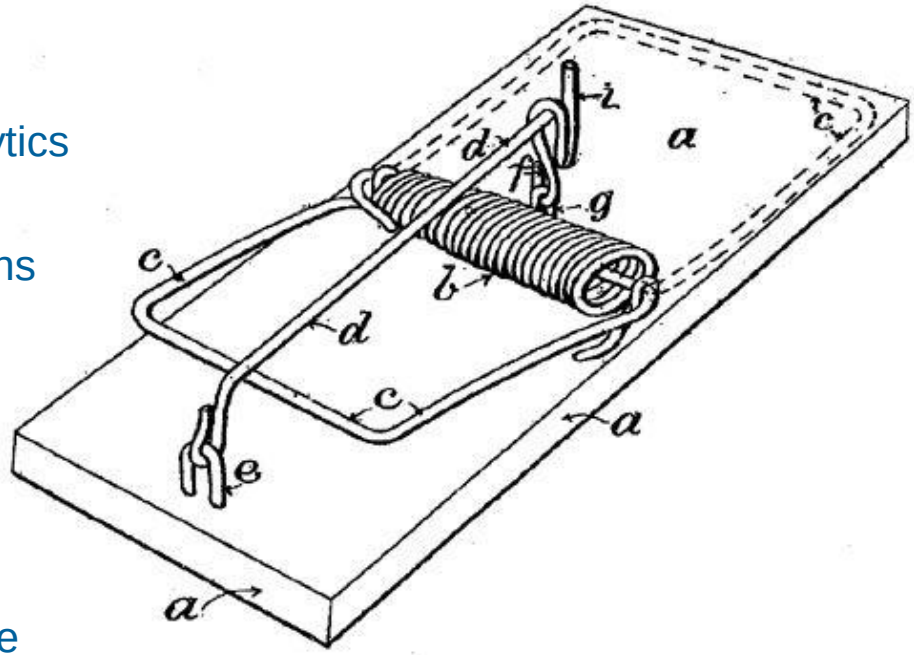
- Enabling zero-day detection
- Not limited to heuristics or peer comparisons

Adaptive analytics

- Responsive to analyst feedback
- Reducing false positives

Continuous outcome scoring

- Enabling more precise risk ranking
- Reason codes to guide triage and response



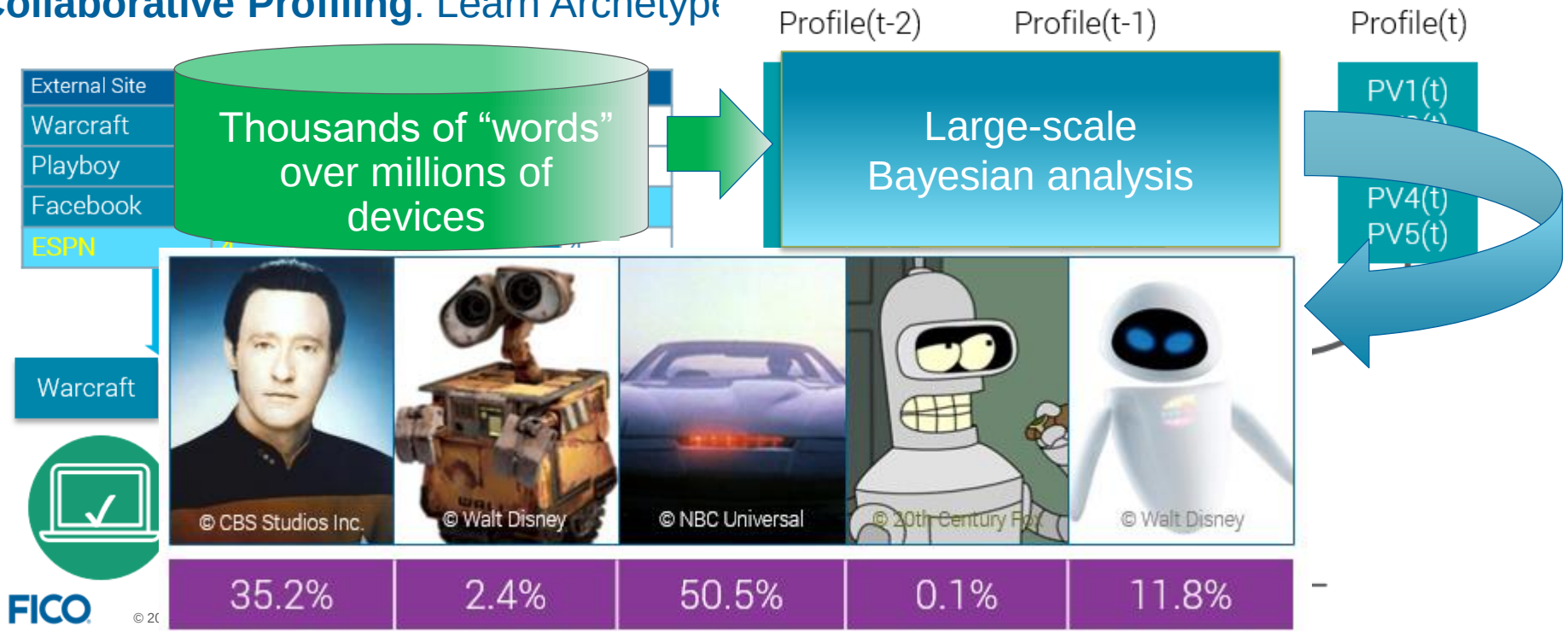
A better mousetrap for detecting and defeating emerging and evolving threats

Real-Time Streaming Analytics – Feature Creation

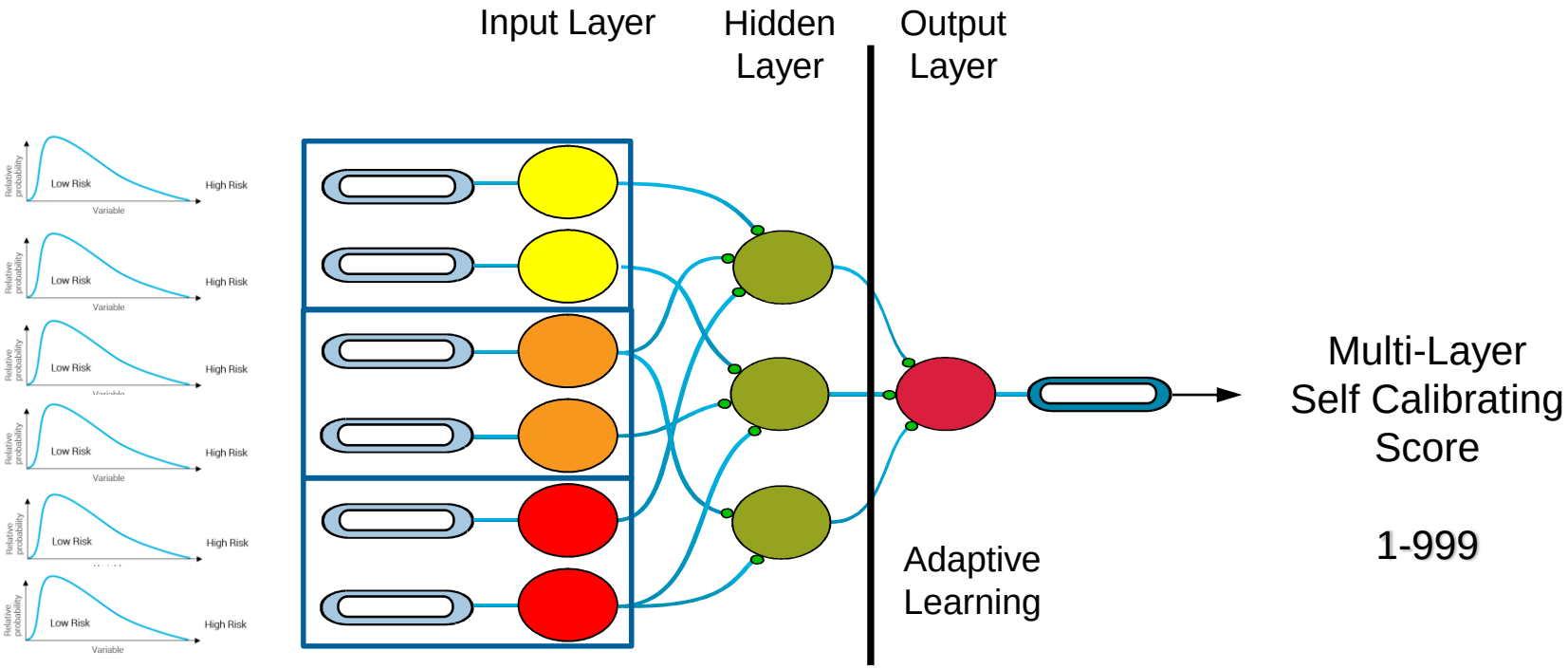
Transaction Profiles: Recursively updated variables track behavior of relevant entities

Behavior-Sorted Lists: Reduce false positives for “normal”, even in high-risk categories

Collaborative Profiling: Learn Archetype



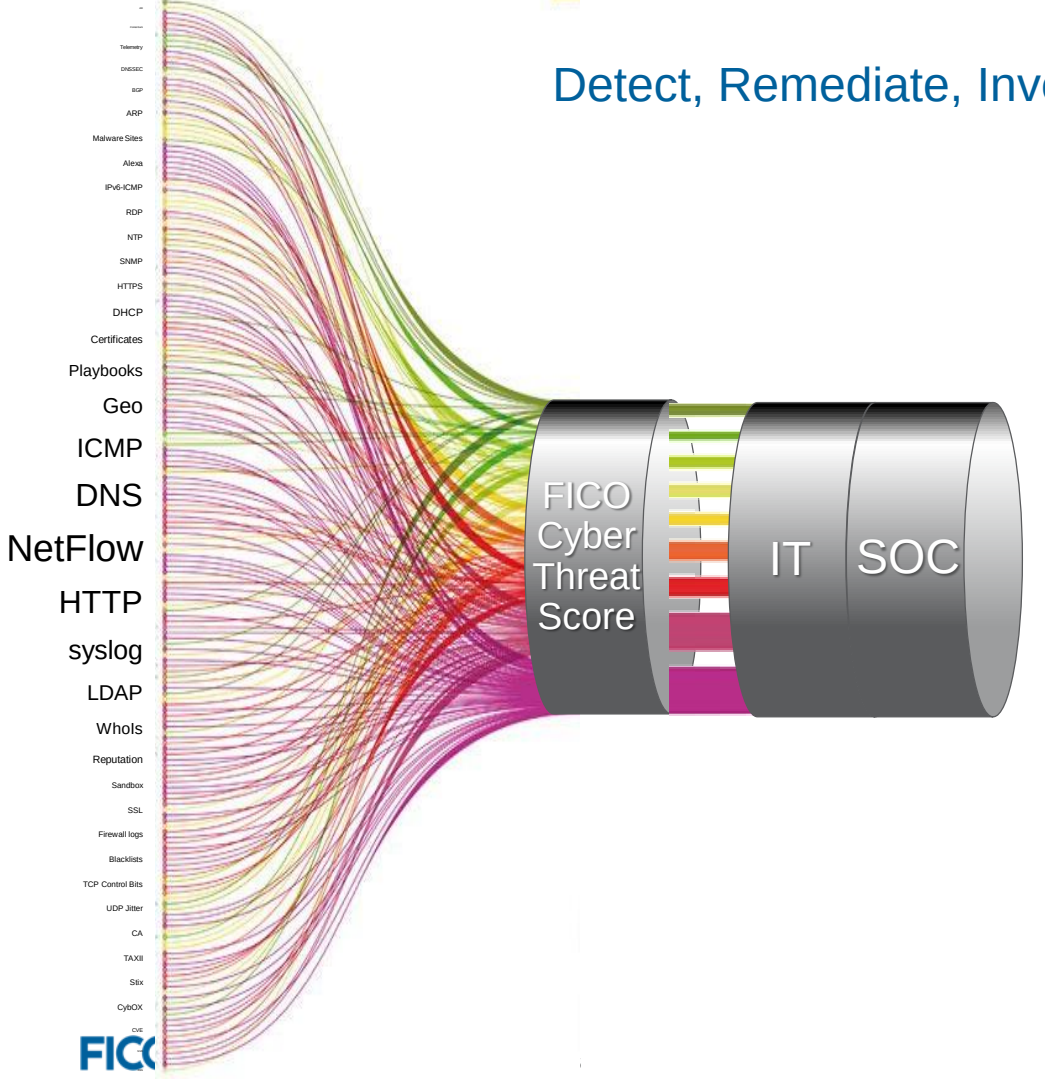
Real-time Streaming AI: Multi-Layered Self-Calibrating Analytics



3,000 research-years on Artificial Intelligence

US Patent 8,027,439; 8,041,597; 13/367,344

Detect, Remediate, Investigate



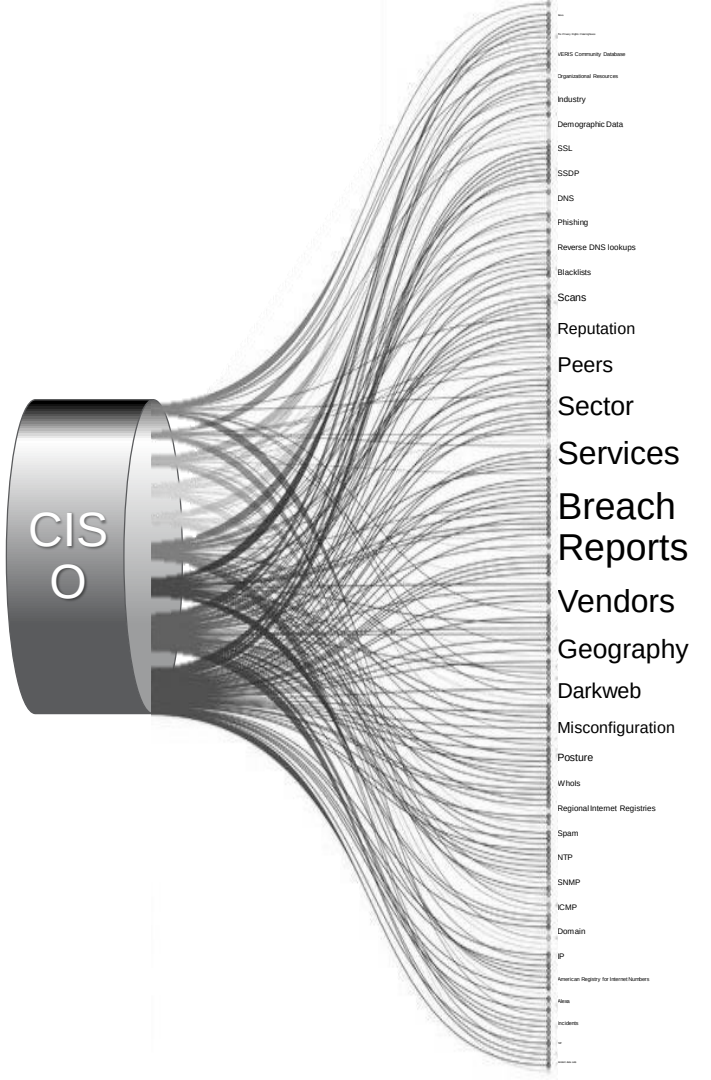
But not the complete picture

Driving IT/SOC Priorities

Reporting to C's and Board

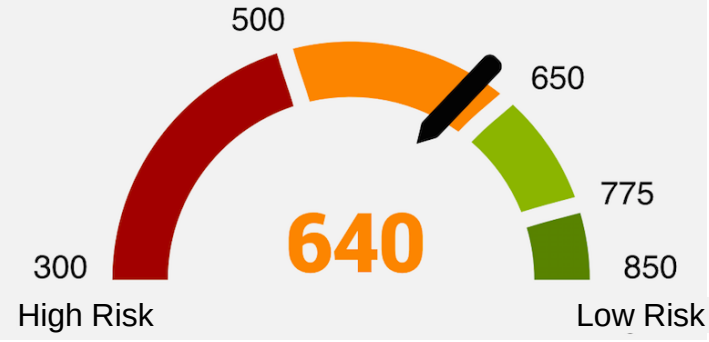
Cyber Insurance Underwriting

Vendor Management



Cyber Risk – Leveraging a Credit Risk Playbook

FICO® SCORE | 25 YEARS



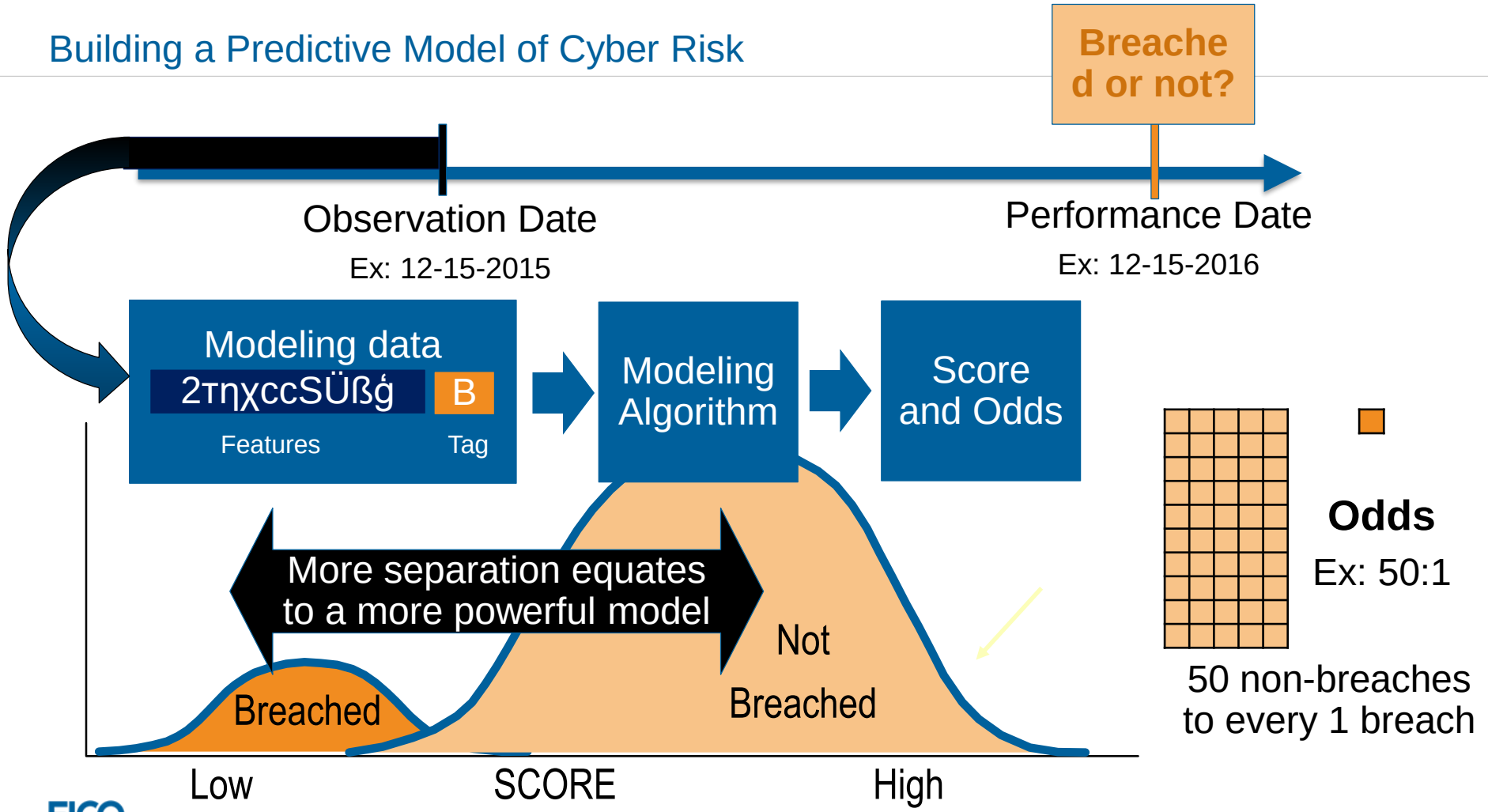
90% Top lenders using FICO® Scores when making lending decisions

10B FICO Scores purchased in US annually

70K Businesses that rely on the FICO Score

20 Countries where the FICO Score is deployed

Building a Predictive Model of Cyber Risk



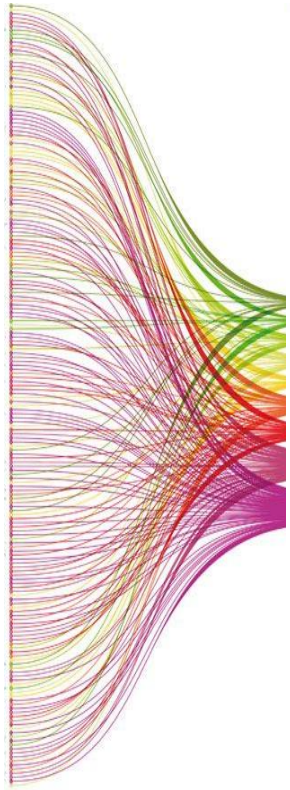
Data Collected; Operationalized via Score and Reason Codes

Three categories of monitored issues with corresponding reason codes

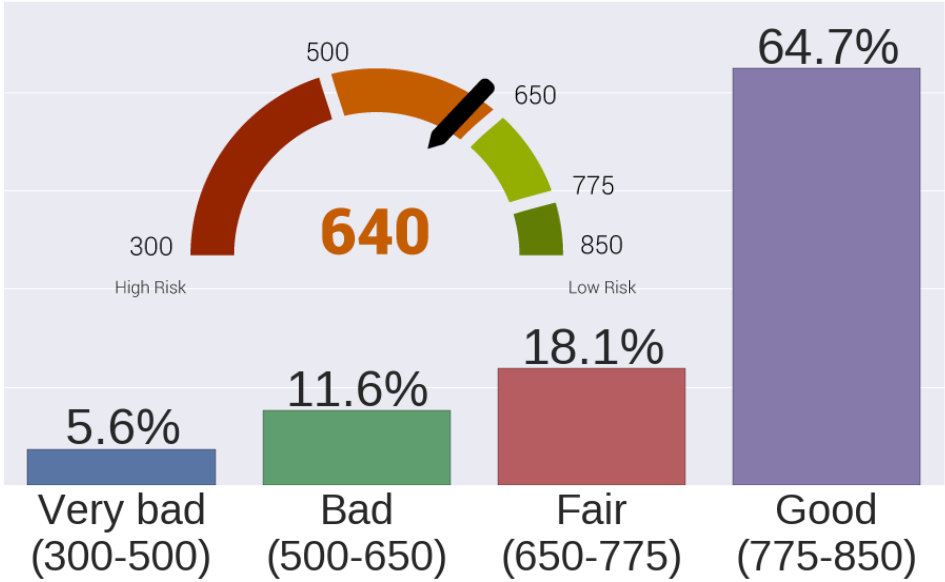
Endpoint Security
Malware/Spam/Phishing

Infrastructure Security
NTP/DNS/SNMP/SSDP

Services & Software
Certificates/Configurations



Organization Score



Unifying both Real-time Threat and Odds of Breach

Active Threat Scores inform the Enterprise Score

Telemetry
DNSSEC
BGP
ARP
Malware Sites
Alexa
IPv6-ICMP
RDP
NTP
SNMP
HTTPS
DHCP
Certificates
Playbooks
Geo
ICMP
DNS
NetFlow
HTTP
syslog
LDAP
WhoIs
Reputation
Sandbox
SSL
Firewall logs
Blacklists
TCP Control Bits
UDP Jitter
CA
TAXII
Stix
CybOX
CVE

vERIS Community Database
Organizational Resources
Industry
Demographic Data
SSL
SSDP
DNS
Phishing
Reverse DNS lookups
Blacklists
Scans
Reputation
Peers
Sector
Services
Breach Reports
Vendors
Geography
Darkweb
Misconfiguration
Posture
WhoIs
Regional Internet Registries
Spam
NTP
SNMP
ICMP
Domain
IP
American Registry for Internet Numbers
Alexa
Incidents

iboss™

The platform is built on the concept of nodes.

Gateway

Malware Defense

Reporting

FICO Cyber Risk Scoring

Cyber Risk Scoring Node Powered By FICO

Cyber Risk Scoring Node

Core Responsibilities

Generate FICO behavioral cyber risk scores for devices and users on a network

Delivers Features

- **Define and deploy FICO Analytics against Protected Networks and Assets**
- **Create Risk Score Thresholds for Protected Objects**
- **Alert or Block based on set score thresholds**
- **Prioritize Incident Response for Most Critical Issues**

Advantages

- **FICO's patented behavioral analytics** identifies anomalous activity and scores suspicious "behavior" of devices, users or servers, similar to the way FICO's leading card fraud solution instantly scores billions of credit card transaction around the world daily.
- **Through the cyber threat scores**, FICO and iboss clients are able to more accurately quantify their cyber threats and remediate in real time to stop catastrophic infections and data loss before they occur.
- **FICO and iboss combined technologies** can quickly spot breaches other systems miss, including attacks that mask communications using TOR software, such as Zeus64 malware Trojan and Locky ransomware.
- **Elastic node-based cloud architecture** means that FICO technology can be deployed in distributed organizations quickly and easily, or choose a physical node deployment and keep your data on-premises.

FICO Decisions

Fraud Detection and Advanced AI for Cyber Threats

Thank You!

@ScottZoldi