REDOWL

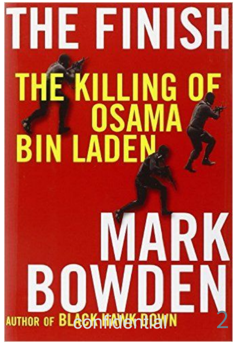
RedOwl Insider Threat Overview

February 22, 2017

RedOwl's Founding DNA

Guy Filippelli *RedOwl Founder and CEO*

- West Point graduate with graduate degree from Oxford
- Helped pioneer the use of big data in combat in Iraq and Afghanistan
  - Awarded National Intelligence Medallion
  - Featured in the book, The Killing of Osama Bin Laden, by Mark Bowden
- Lessons learned moving from the battlefield to the Boardroom
  - Context is king
  - People are part of the architecture



Company Overview

- **Technology**
  - Software platform to manage & mitigate insider risk
  - Consume multiple data sources; apply analytics to identify high-risk individuals
  - Primary customers are CISO’s (Insider Threat) and CCO/COO’s (Regulatory Surveillance)
- **Team/Location**
  - HQ in Baltimore; Offices in NY, SF, and London
  - ~70 employees -- strong mix of data science, intel/military & financial community
- **Market Focus**
  - Financial Services: Banks, HF’s, Asset Managers, PE
  - Energy: Utilities, Petro
  - Government: Federal Agencies, DOD
- **Business Success**
  - Customers: Banking, Energy, Government
  - Partners: Security companies (i.e. Forcepoint), large service providers (i.e. BT)
- **Investors**
  - Blackstone, Allegis Capital, ClearSky

RedOwl Mission

RedOwl's mission is to uncover individuals exhibiting specific patterns of risk, characterized by the actions they take and made relevant by the personal attributes that identify them.

This is driven by a deep understanding of:

- Who they are
- What we know about them
- What they say & do
- Whom & what they interact with
- How they do it
- When they do it
- What content is involved
- How this compares to themselves and their peers

RedOwl | *Solution Objectives*

Business

- Improve oversight of people
- Create a culture of security and compliance

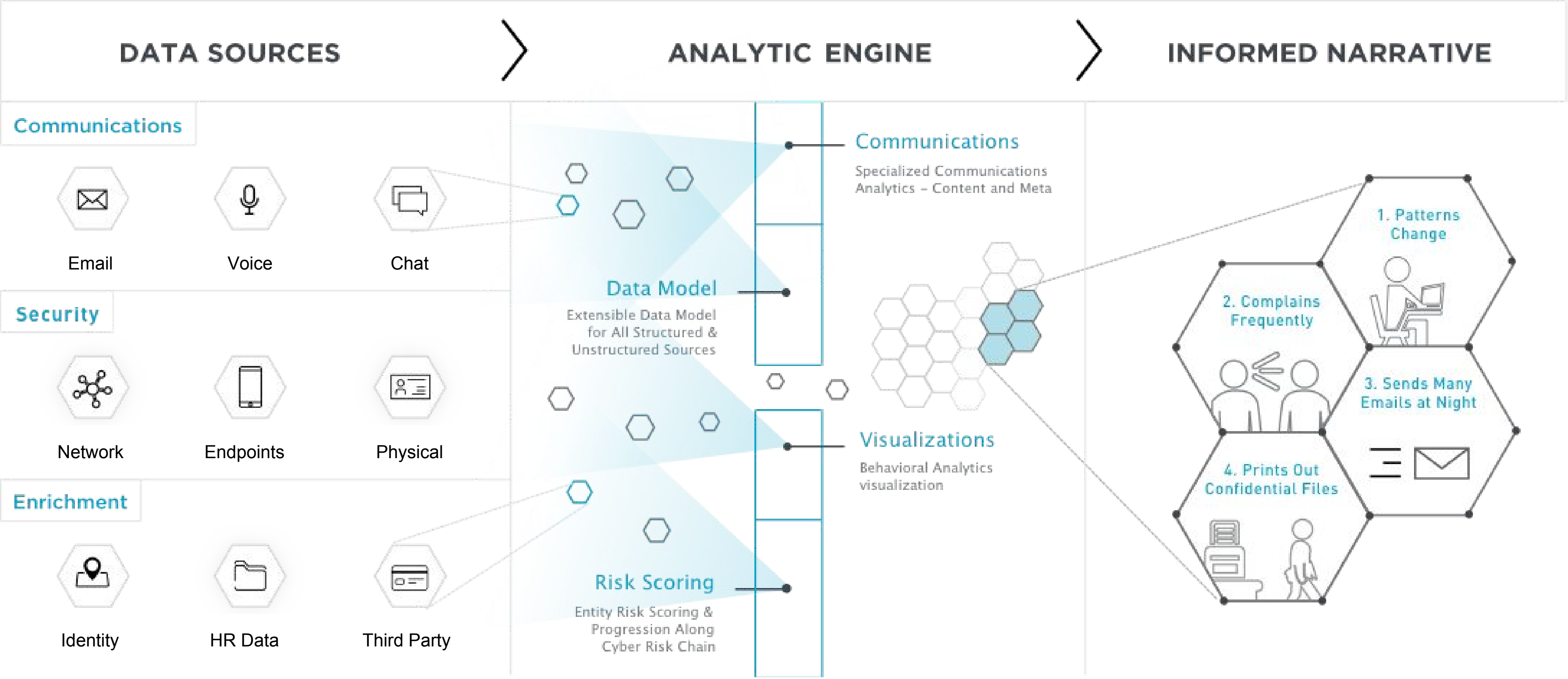
Analytic

- Close detection gaps
- Spot unwanted patterns activity
- Reduce noise (false positives)

Product

- Provide pre-configured insider risk models
- Improve data management TCO
- Facilitate collaborative workflow
- Enable analyst speed and efficiency (alert to investigation)

The Platform



DATA SOURCES

ANALYTIC ENGINE

INFORMED NARRATIVE

Communications

Email

Voice

Chat

Security

Network

Endpoints

Physical

Enrichment

Identity

HR Data

Third Party

Communications

Specialized Communications Analytics – Content and Meta

Data Model

Extensible Data Model for All Structured & Unstructured Sources

Visualizations

Behavioral Analytics visualization

Risk Scoring

Entity Risk Scoring & Progression Along Cyber Risk Chain

1. Patterns Change

2. Complains Frequently

3. Sends Many Emails at Night

4. Prints Out Confidential Files

Out-of-Box Use Cases | *RedOwl Baseline Analytics Model (RBAM)*

	Data Exfiltration	Malicious User	Compromised User Account	Negative Behavior	Illicit Behavior
Event Models	Internal Data Movement External Data Movement File Operations Data Reconnaissance Evasive Action	Network Reconnaissance Systems Administration Malicious Authentication Malicious Actions Research Baseline Configuration Deviation Physical Access Permissions Elevation Request	Malware Risk Compromised Authentication Phishing Risk Baseline Config Deviation Malware Resources	Sexual Harassment Workplace Violence Obscene Content Leaver Risk Decreased Productivity Corporate Disengagement Negative Sentiment	Organizational Conflict of Interests (OCI) Information Leakage Corporate Espionage Whistleblowing Risk Investigation Evasion Risk
Entity Models	Human Resources Risk	Human Resources Risk		Financial Distress Risk Human Resources Risk	Human Resources Risk
Data Sources	Web Proxy Windows Linux User Activity Monitoring Email Chat Network Flow Logs SharePoint Web Server Logs HR	Web Proxy Windows Linux User Activity Monitoring Email Chat Network Flow Logs VPN Badge Data Voice HR	Web Proxy Windows Linux User Activity Monitoring Email Chat Network Flow Logs VPN Firewall Anti-Virus HR Voice	Web Proxy Email Chat Network Flow Logs HR Voice	Web Proxy Email Chat Firewall HR Voice DLP

REDOWL

Baltimore | New York | San Francisco | London