SAS® FINANCIAL CRIMES EXECUTIVE FORUM
Toronto, 2018

Conduct Risk Analytics:

Suspect Behavior Detection through Communication Surveillance & Deep Sentiment Analysis

Constantine T. Boyadjiev
Accenture Digital – Applied Intelligence
NA Fraud & Risk Analytics Practice Lead

Copyright © SAS Institute Inc. All rights reserved.

THE POWER TO KNOW®

Why Focus on Surveillance and What Makes it Challenging?

- ***Financial Crime and Rogue Conduct poses significant risks / costs*** to firms, including monetary losses, regulatory repercussions, and adverse reputational impacts
- Recent organized crime, as well as individual and collusive market manipulation events have caused ***regulators to impose severe fines, increase scrutiny, and tighten supervision***
- Given malicious behavior is complex and dynamic in nature, ***identifying and effectively monitoring is difficult***
- Adding to the complexity, ***multiple data sources*** (structured / unstructured) are required to proactively detect / prevent evolving fraudulent behaviors and illicit activity
- Though some technology is available to combat the problem, generally ***no holistic 'silver bullet' solution exists***

Financial Crime, Unauthorized Trading & Market Abuse is a top concern for Banks, Exchanges, Regulators, and other market participants across industries

- High priority – yet hard to timely detect and very expensive
- Regulators cracking down with no end in sight
- Relatively new market and few viable end-to-end analytic solutions exist

Illustrative Subset of Regulatory Fines:

Unauthorised Trading / Market Abuse / Fin Crime

UBS	JPMorgan	HSBC	Rabobank
$2.3B related to index futures trades	**$5.8B related to credit derivs index trades**	**$1.9B related to money laundering violations**	**$1B related to LIBOR manipulation**

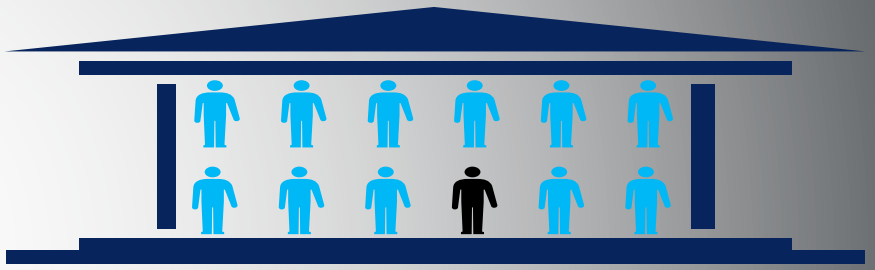
Copyright © 2017 Accenture. All rights reserved.

Surveillance & Monitoring of Misconduct

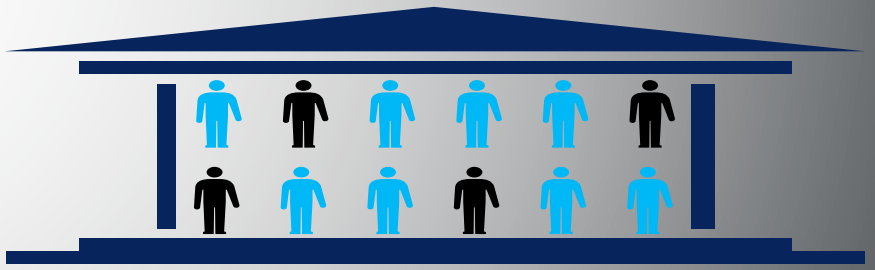
Through Surveillance Analytics institutions can detect and prevent various forms of Misconduct, such as Rogue Trading, Market Abuse, and Fin Crime / Money Laundering

Main Focus Areas:

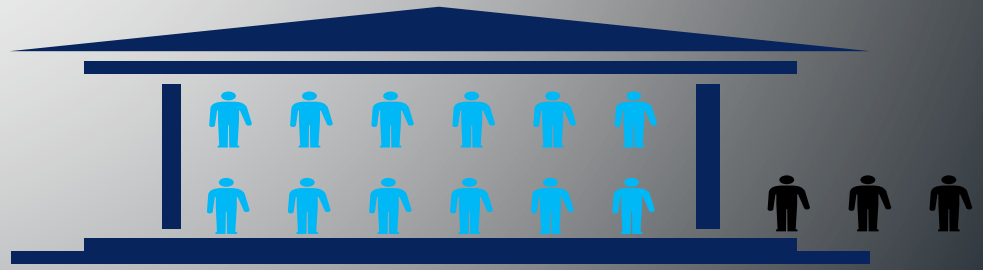
- **Unauthorized Trading – individual traders that find mechanisms to go around systems, processes, and controls to distort / hide actual risk exposure and true trading profits / losses**



- **Market Manipulation & Abuse – dealers that engage in collusion with external counterparts of other institutions, with the intent to move a benchmark rate / index (e.g. LIBOR) in order to obtain financial gain**



- **Money Laundering – client's concealment of the true origin of illegally obtained moneys, typically through placement, layering, and integration into the financial system**



Movement Towards “Holistic Surveillance” Approach

The industry is moving towards Surveillance & Monitoring being part of a broad holistic approach, reflecting dependencies between use cases, in mitigating risk and complying with regulations

Trade Surveillance

- Wash Trading
- Mark the Close
- Best Execution
- Cancellations and Re-bookings
- Cross Trades
- Fair Allocation
- Front Running
- Insider Trading
- Mark Up – Down
- Market Manipulation
- Off-Market Transactions
- Parking
- Spoofing / Layering
- Side By Side
- Suitability
- Trades with Affiliated Broker Dealers
- Warehouse Accounts

Control Room

- Outside Business Interests
- Licenses and Registrations – Fit and Pro Attestations, Continuing Ed
- Large Holdings
- Conflicts Clearance / Control Room
- Personal Account Trading

Fin Crime Compliance

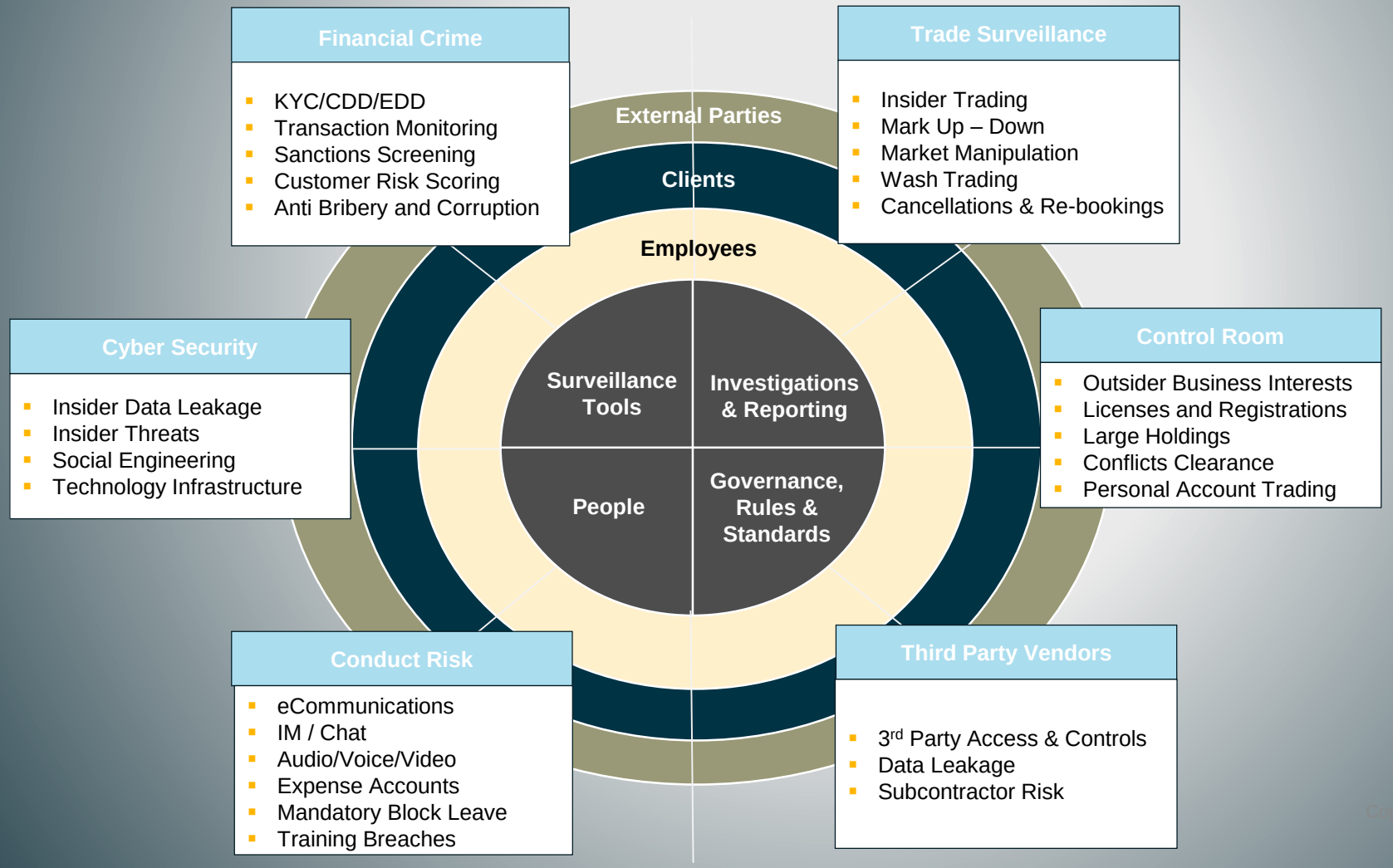
- Customer Sanctions
- Terrorist Financing
- Payment Sanctions
- Transaction Surveillance
- KYC/ CDD /EDD
- PEPs
- Bribery and Corruption

Other

- eCommunications
- IM / Chat
- Voice
- Political Contributions
- Badge swipes
- Mandatory Block Leave
- Expense Accounts
- Travel Habits
- Web Browsing & Print History
- Training Breaches

Surveillance capabilities are evolving to develop a broader integrated framework

Bringing capabilities to life through an understanding of how surveillance fits within the business



The evolving surveillance landscape focuses on analyzing disparate data points and gathering insight through their integration

Copyright © 2017 Accenture. All rights reserved.

AML / KYC / Conduct Surveillance: Representative suspicious behaviors & red flags

Most banks leverage multiple technologies as part of their AML Monitoring and Conduct Surveillance control activities. Leading practices require an enterprise view with close evaluation of behaviors to maintain appropriate visibility into activity across the institution.

Conduct Red Flags

Price Manipulation

- Abusive short selling
- Abusive squeeze
- Creation of artificial price level
- Cross product / venue manipulation
- Naked short selling

Dissemination of False & Misleading Market Information

- Dissemination of false or misleading market info
- Concealing ownership / parking

Misuse of Insider Info

- Inside information misuse including insider dealing
- Front running

AML & Conduct Red Flags

Insufficient or Suspicious Information

- Suspicious identification documents
- Efforts to avoid reporting or recordkeeping requirements
- Unusual funds transfer patterns
- Unusual or illegal requests for currencies not available for trading
- Cross boarder payments not consistent with business
- Third party loans and payments
- Multiple transfers of funds under regulatory reporting thresholds
- Unusual trading requests - e.g. sanctioned currencies

AML Red Flags

Unusual Transactions

- Large and rounded dollar amounts
- Business & personal account inter transfers
- Transactions in High risk jurisdictions
- Multiple jurisdictions and beneficiaries
- Structured deposits through multiple branches

Abnormal Client Behavior

- Misrepresentation of nature of business
- Frequent changes in Financial Advisors
- Complex Organization structure with multiple layers of trusts, beneficial owners etc.
- Borrowing against life insurance

Copyright © 2017 Accenture. All rights reserved.

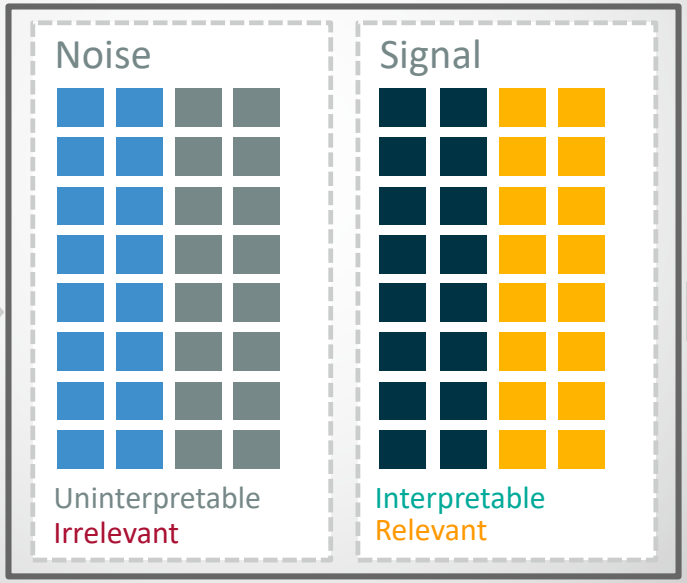
Big Data Discovery will Uncover Malicious Behavior Insights

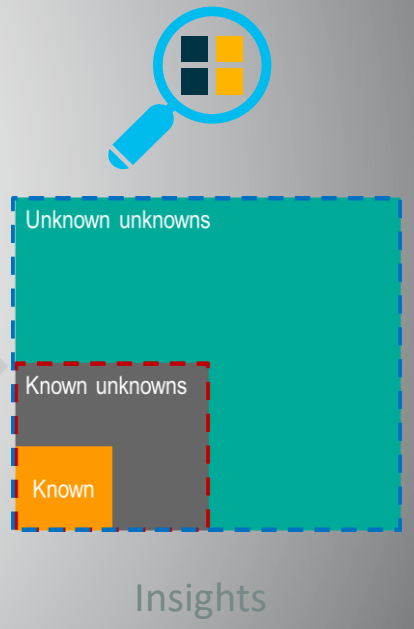
Surveillance is a Big Data Behavioral Problem - separating the signal from the noise is challenging

1. BIG DATA
2. INFORMATION
3. INSIGHTS

Data's 3 V's:

- ***Volume***
- ***Variety***
- ***Velocity***





Interpretable
Uninterpretable
Relevant
Irrelevant

- **What is the hidden value?**
- **What can I know now what I couldn't before?**
- **How do I do all this in a constrained environment?**

Copyright © 2014 Accenture All rights reserved.

Copyright © 2017 Accenture. All rights reserved.

7

Developing a Holistic Surveillance Analytics Solution

Integrated Surveillance & Monitoring Requires Analysis of Disparate Data Sources:

Real-Time Transactional Analysis

Financial Performance

Has PnL / Exposure changed dramatically?

Transactions Performance

How many cancel and corrected trades?

Market Benchmarking

How does trader performance compare to the market?

Transactions Screening and Monitoring

Who are your customers dealing with?

Communications Analysis

Email

Focus of this phrase & sentiment

Documents

Are they sharing confidential info?

Social Media

What do they say on Social Media ?

Chat

Who do they talk to?

Voice

What are they sharing?

SMS

What are they exchanging?

Behavioral Analysis

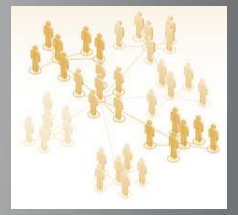
Banker Behavioral Data

Which systems they accessed? Log-on times?

HR Data

How many hours of professional training?

Social Network



Who are they connected to?

Sentiment Analysis

Compare historical sentiment dynamics

Customer Behavioral Data

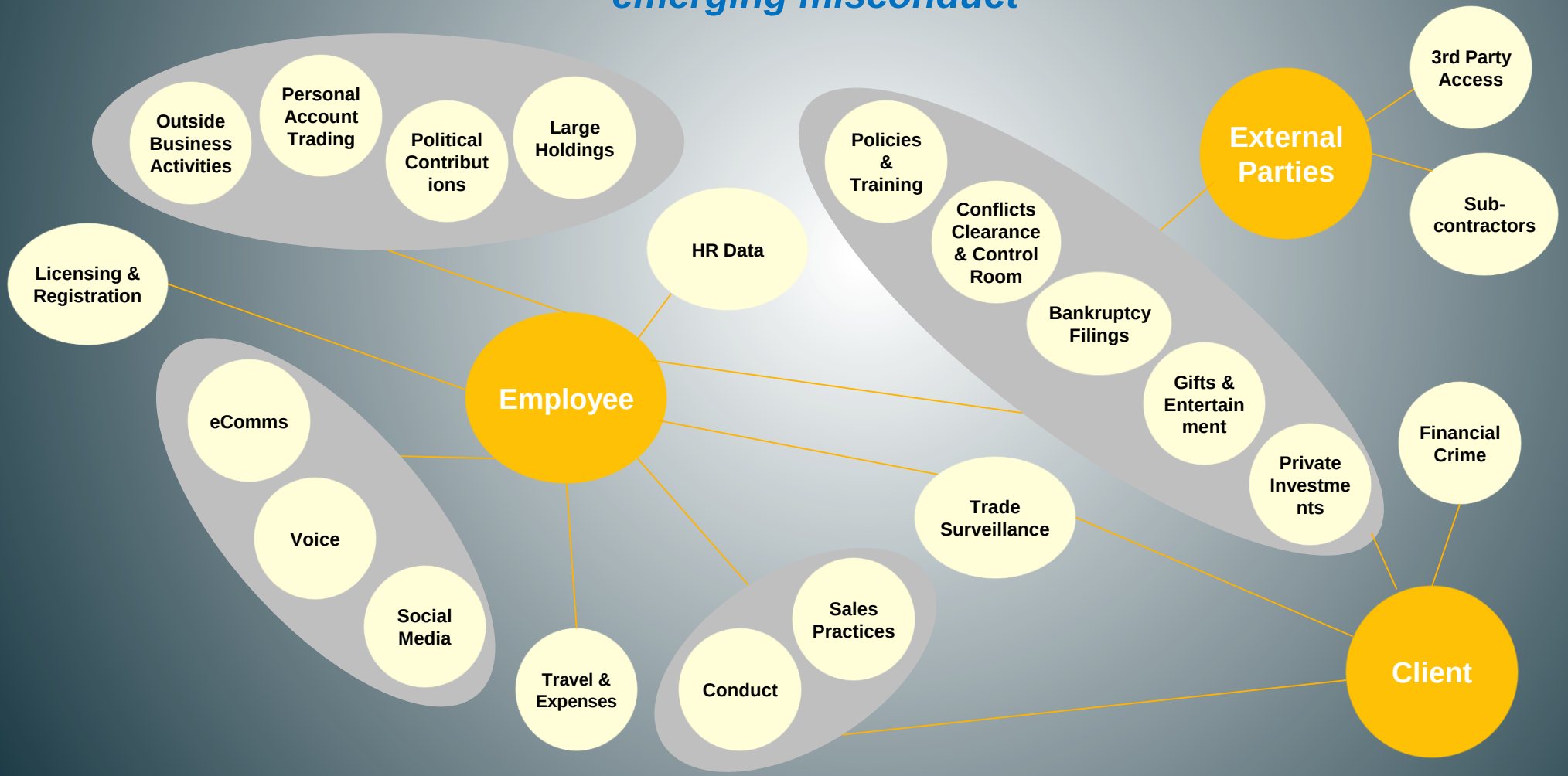
Compare historical behaviors vs recent

Peer Groups analysis

Compare transactional behavior against peers

Integrated Surveillance: “Joining the Dots”

Connecting data points is key to enable surveillance to proactively monitor and identify emerging misconduct

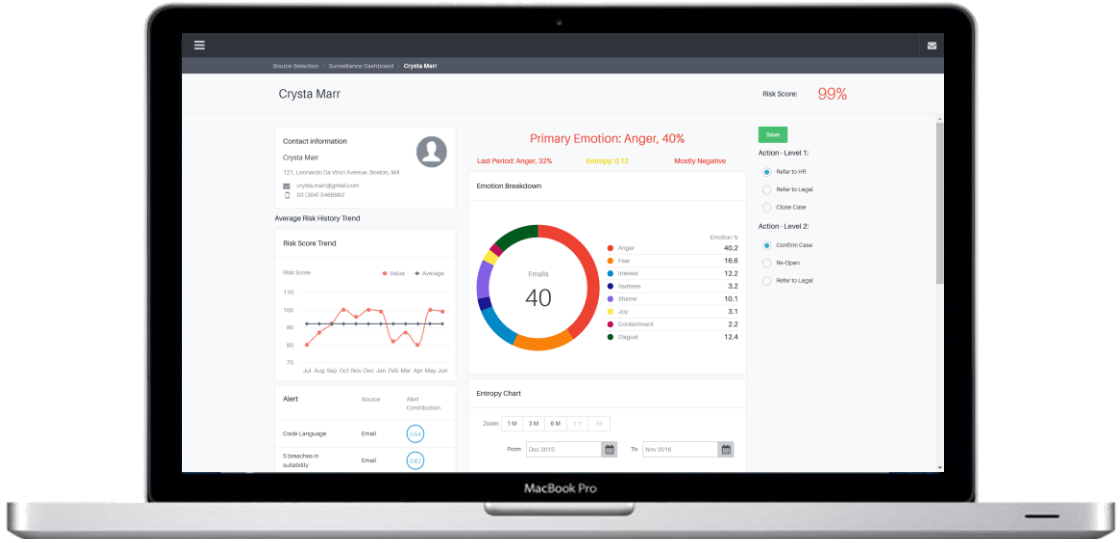


The Accenture-SAS Surveillance Analytics Solution

- Utilizing both linguistic analysis (NLP) & stochastic modeling, goal was to find both **content-based sensitive information and *unusual behavioral patterns in communications*** (detection of illicit / suspect / coded information, oddity & substitution in languages, habitual abnormality in emails).
- ***Deployed additional advanced analytics techniques & algorithms***, such as text mining / forensics, Principle Component Analysis, Multi-Dimensional Scaling, K-means Clustering, Deep Machine Learning, etc. to ***develop Communication & Social Network Analysis, Emotion / Sentiment Analytics, and Detection of Problematic / Deceptive Behavior***.
- ***Analyzed diverse datasets*** including Enron, Hillary Clinton, US Election, & Social Media data.
- Built **"Suspect Behavior Detector"** Advanced Analytics App **on SAS Visual Investigator**.
- Current work focusing on using / integrating ***Deep Machine Learning for Voice Analytics*** (e.g. ***extraction of Audio/Acoustic signatures, detection of spoofing, synthetic impersonation, emotional sentiment***), moving swiftly to a ***"Holistic End-to-End Surveillance" capability.***
- Formal ***Intellectual Property Rights Trademarked / Patents Pending***.

Suspect Behavior Detector Surveillance App

“Suspect Behavior Detector” Surveillance Analytics Application



SAS Visual Investigator

Core Capabilities

Integration	Integrate multiple data sources to produce a holistic surveillance view
Analytics	Obtain insight into illicit behavior thru communication surveillance and sentiment extraction
Tracking / Case Mgmt	Track risk and surveillance actions, converting insight into prudent risk decisioning
Thought Leadership	Embedded Accenture-Stevens co-developed advanced analytics AI assets and SAS accelerators

High performance. Delivered.

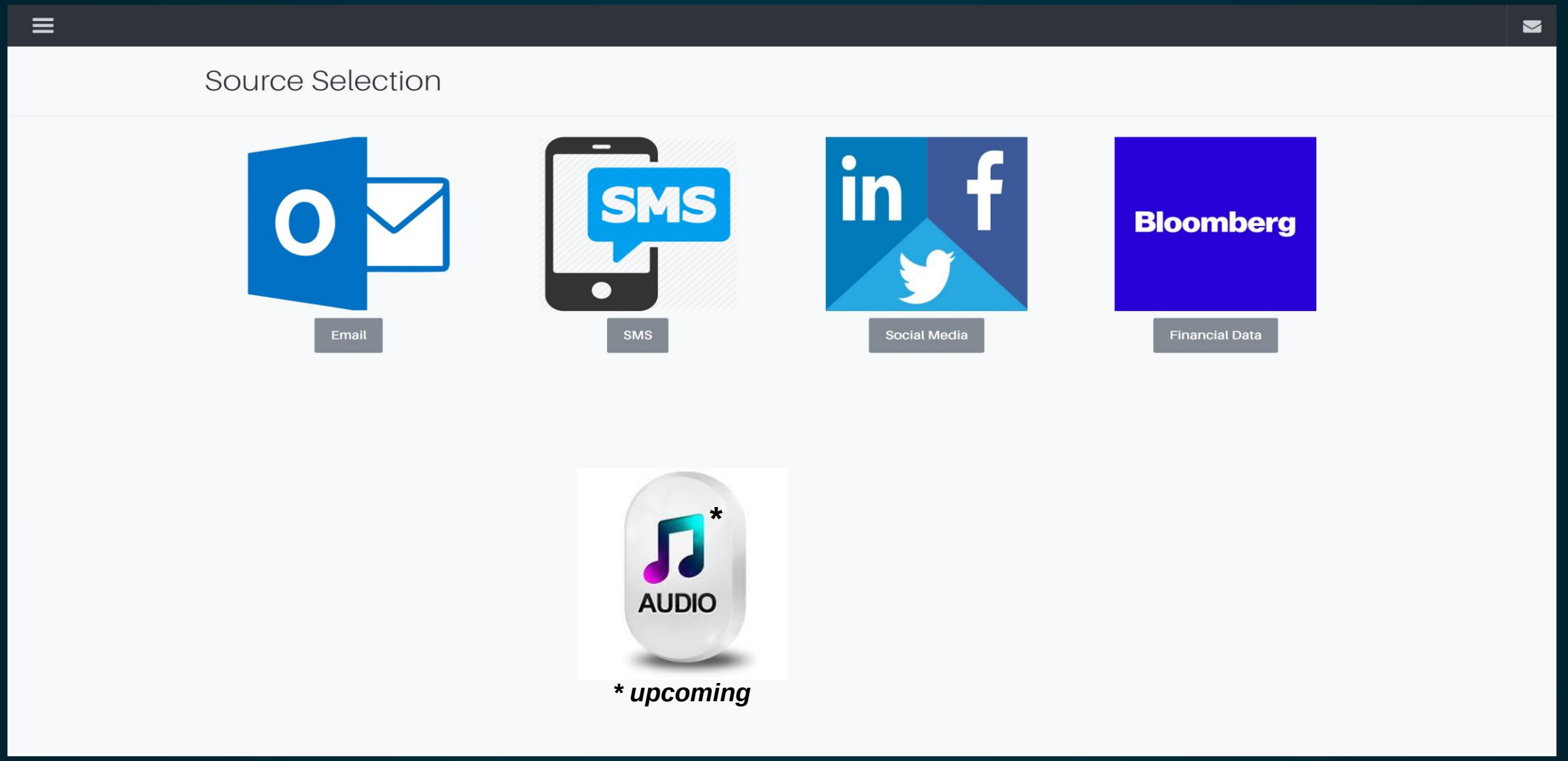
Intelligent Surveillance Demo (SAS Visual Investigator):

"Suspect Behavior Detector"

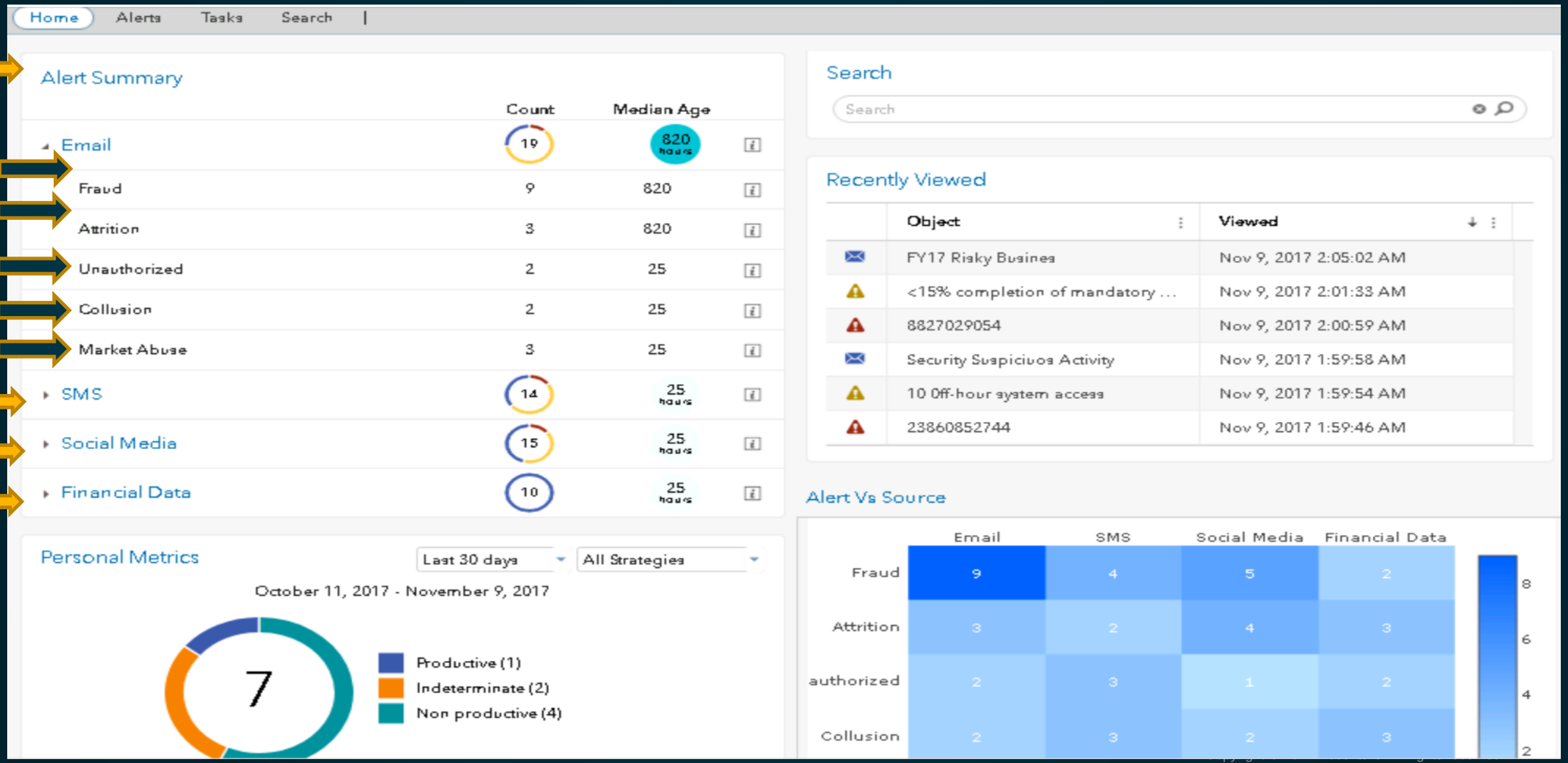
SAS VI Screenshots (Surveillance Investigator + Manager Views)

Copyright © 2015 Accenture All Rights Reserved.

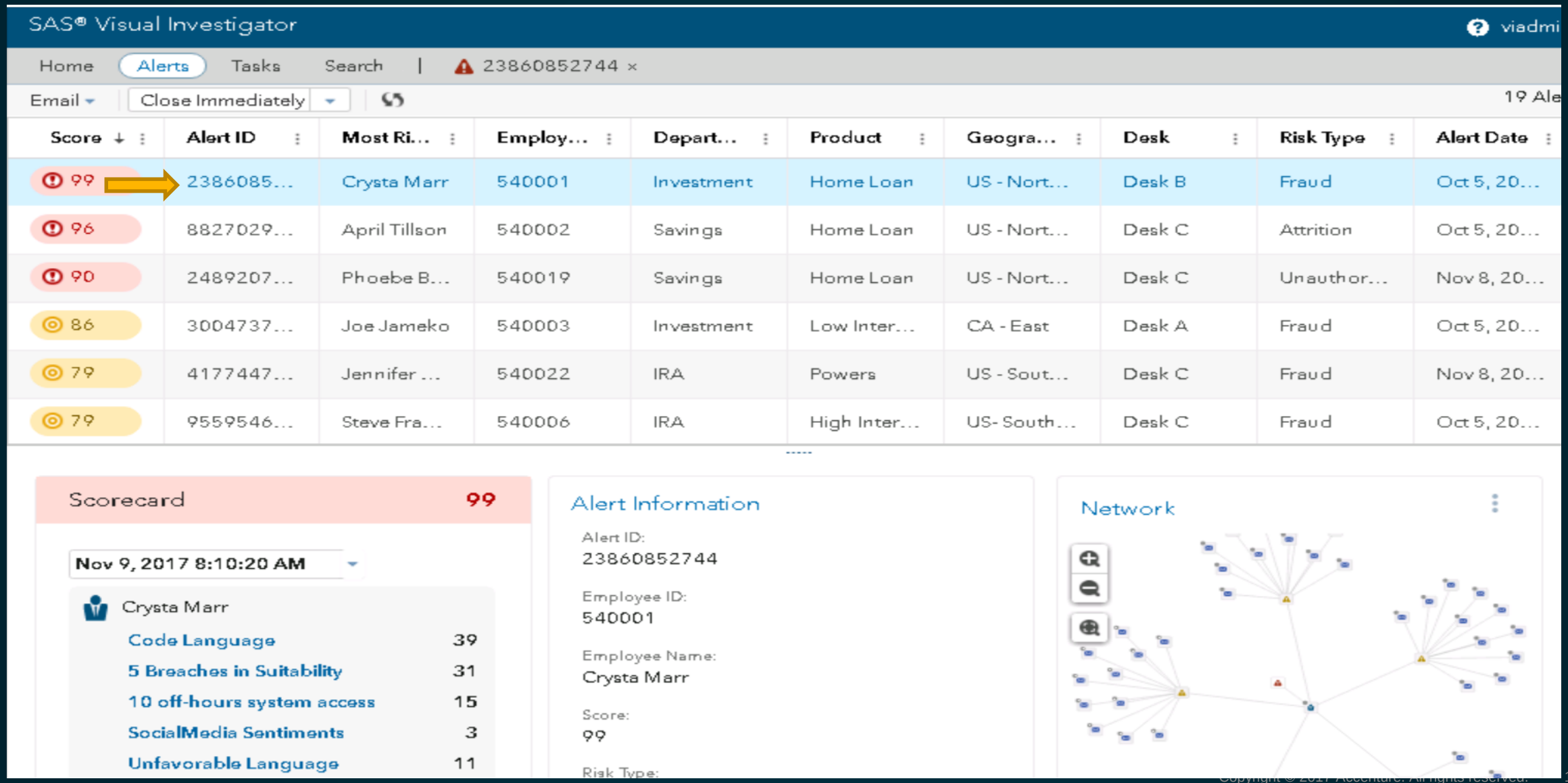
User Can Select The Surveillance Source(s)



User Can Select The Surveillance Source(s) and Risk Type(s)

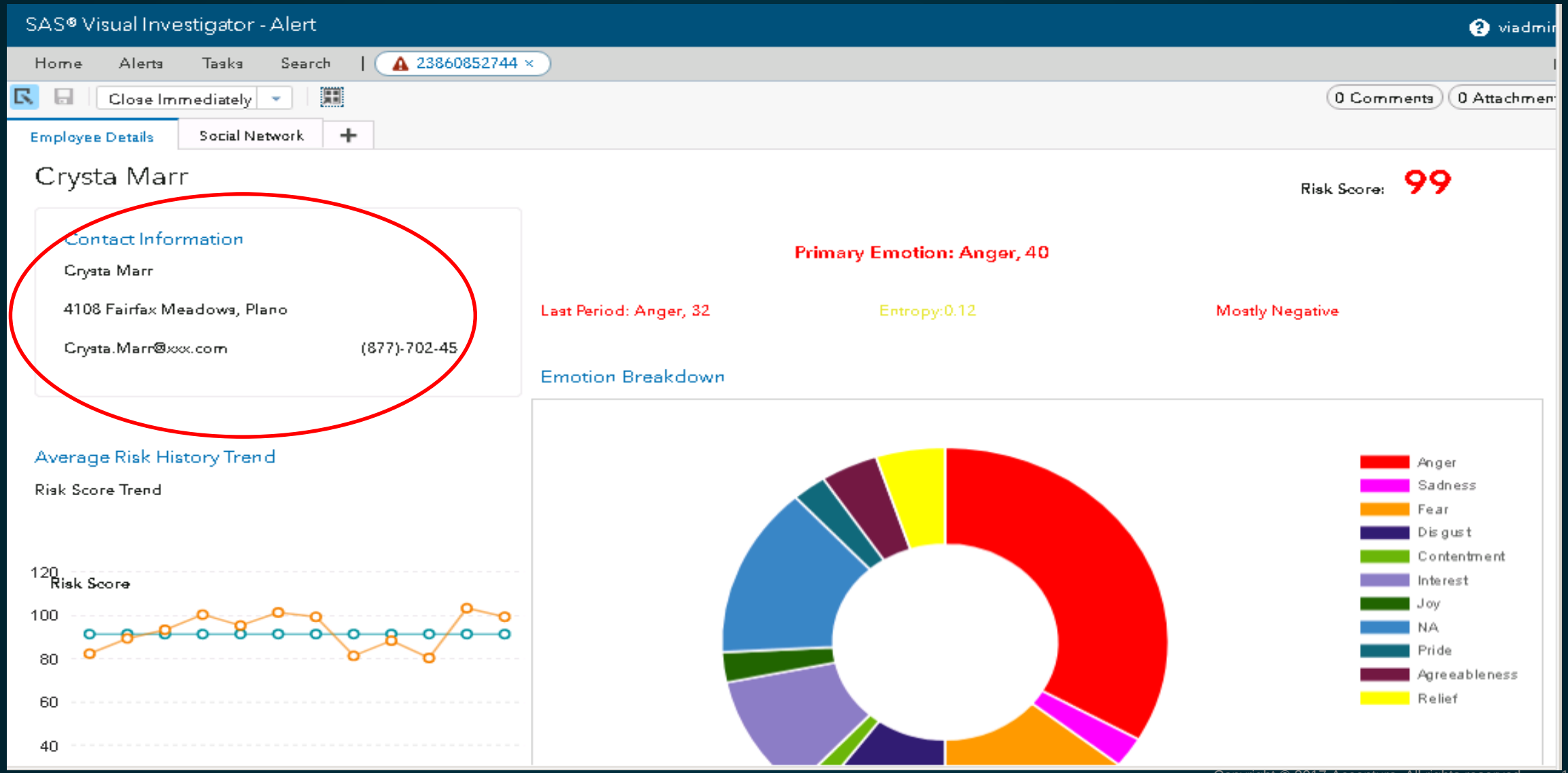


Investigator dashboard of all alerts from a chosen source(s)



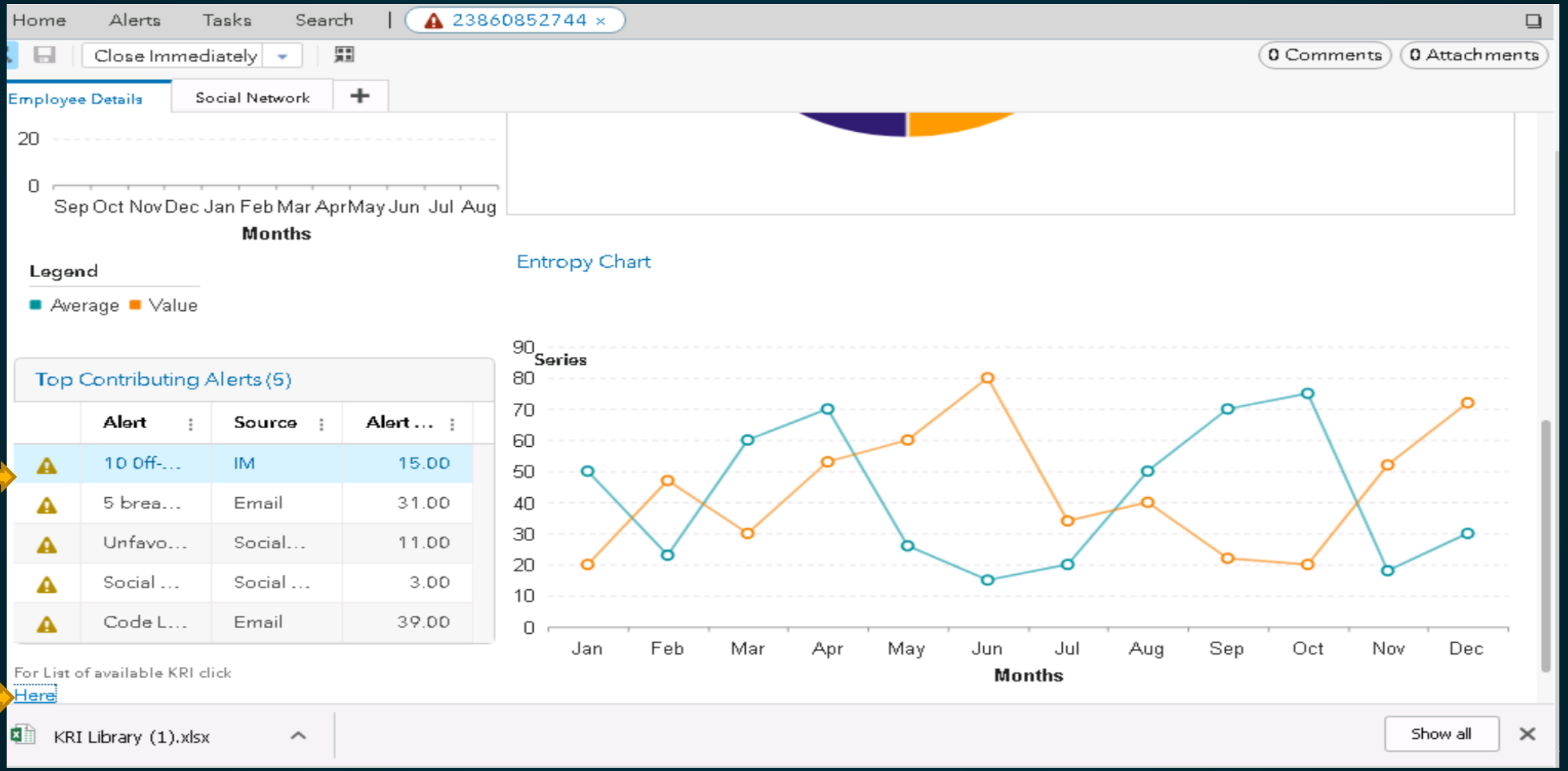
Copyright © 2017 Accenture. All rights reserved.

User can drill down into alerts for a specific employee

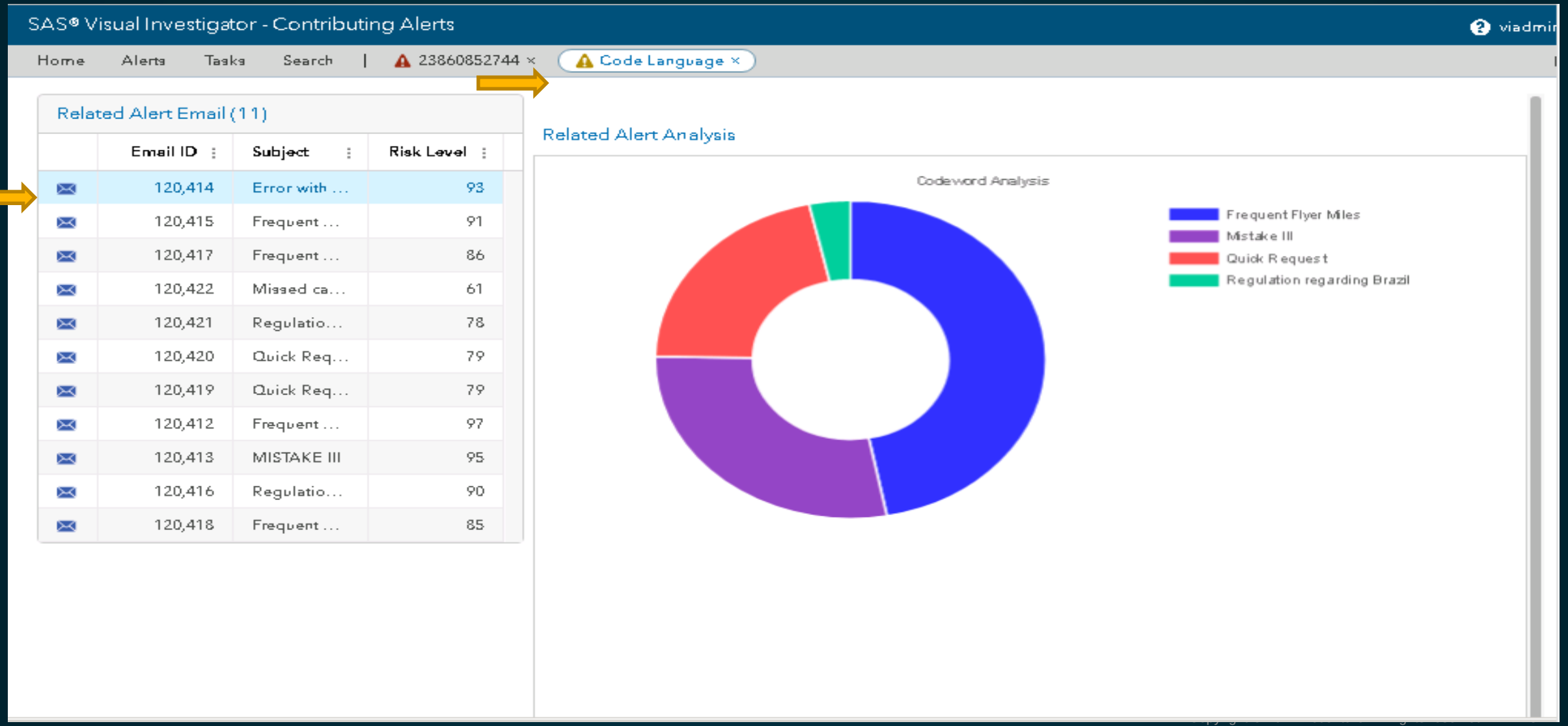


Copyright © 2017 Accenture. All rights reserved.

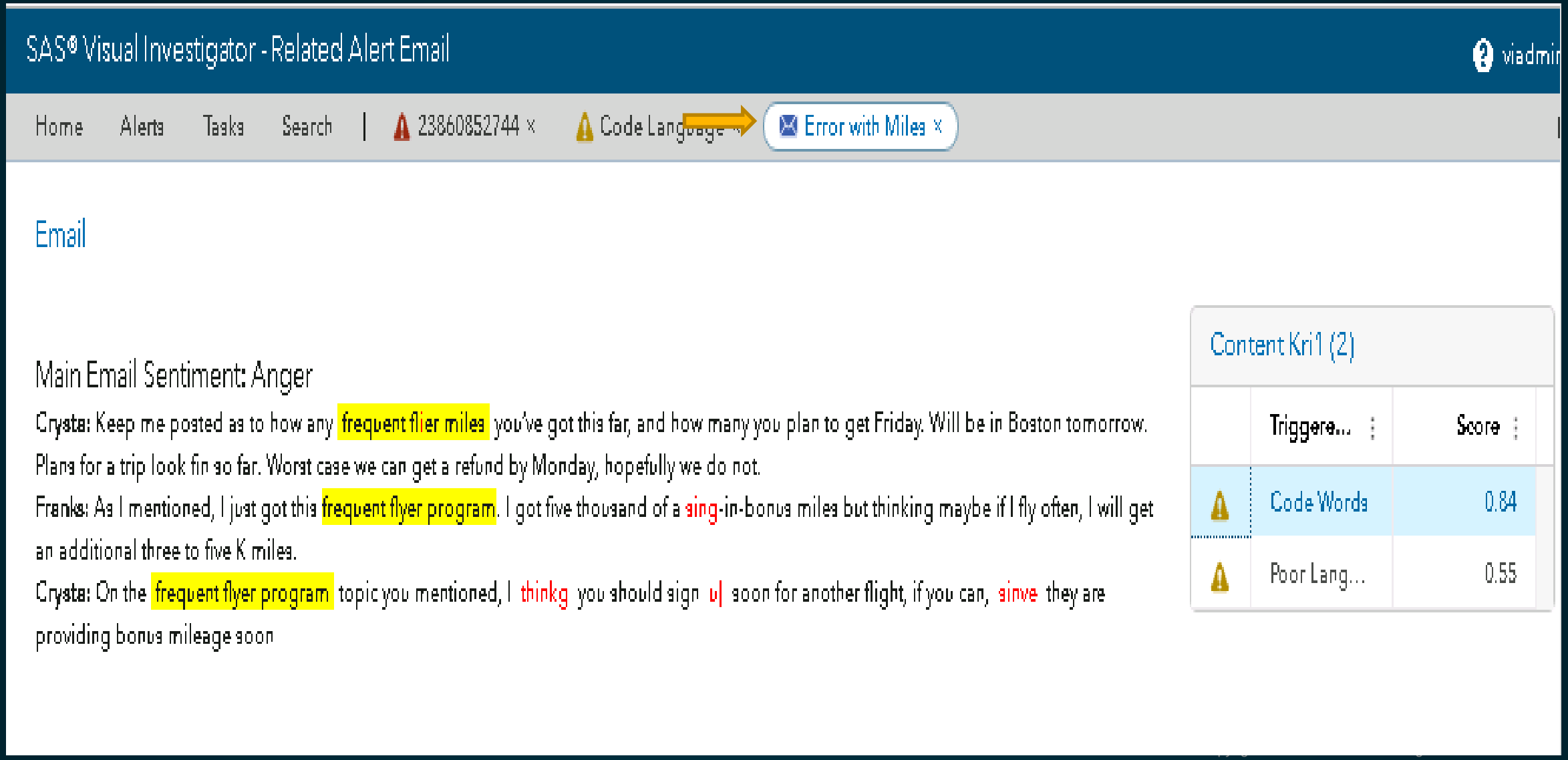
User can examine top Key Risk Indicators triggered per employee



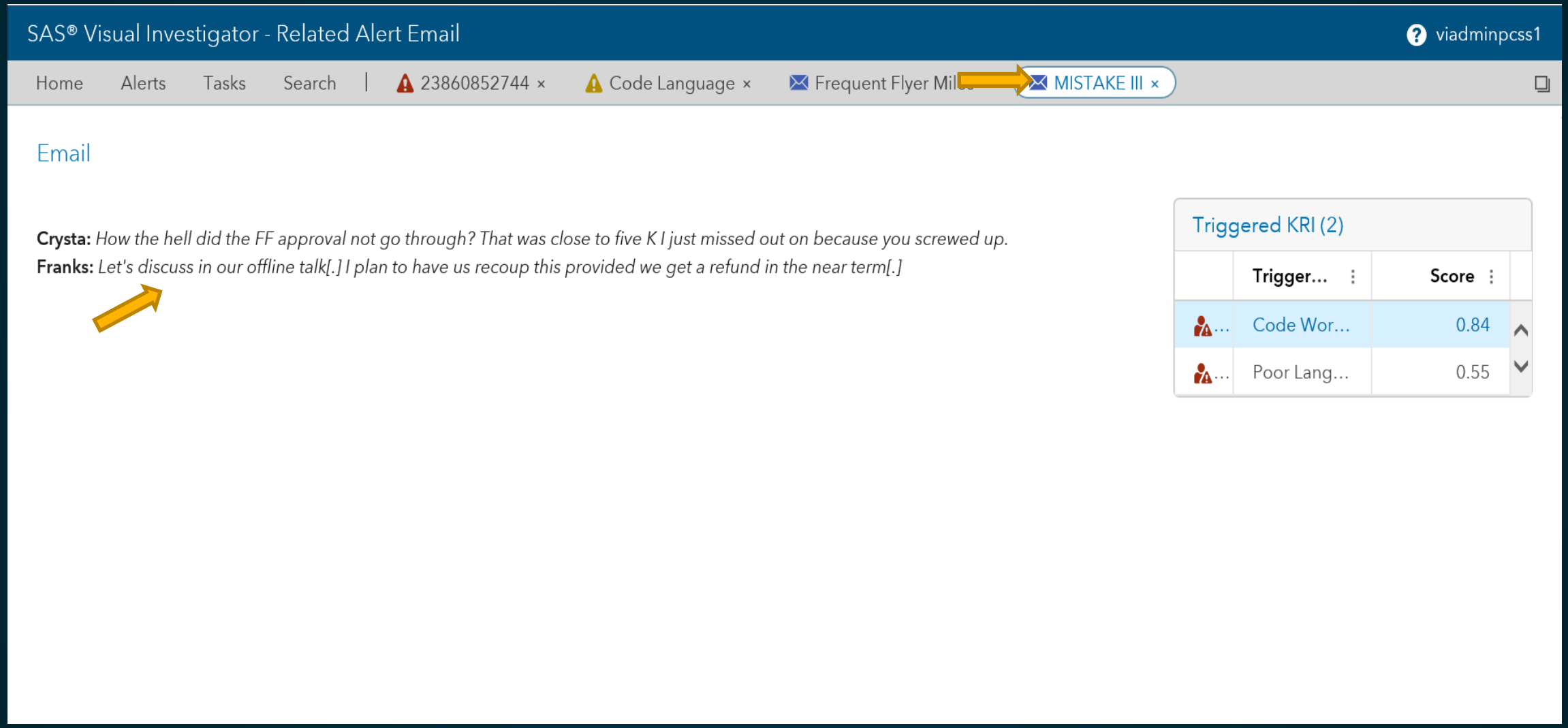
User can look further into a specific type of alert for that employee



User can drill down to specific email triggering the alert

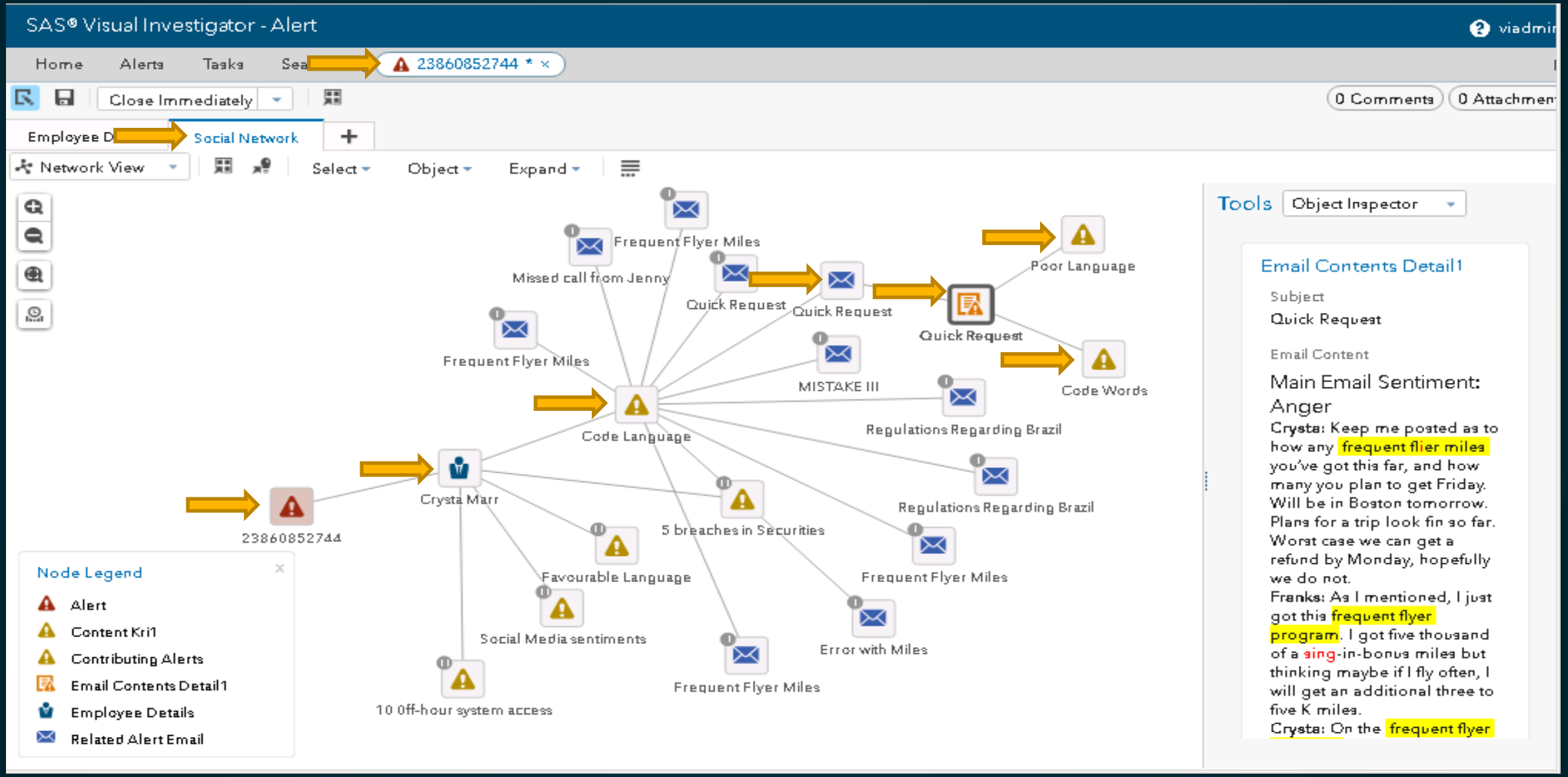


User can drill down to specific email triggering alert

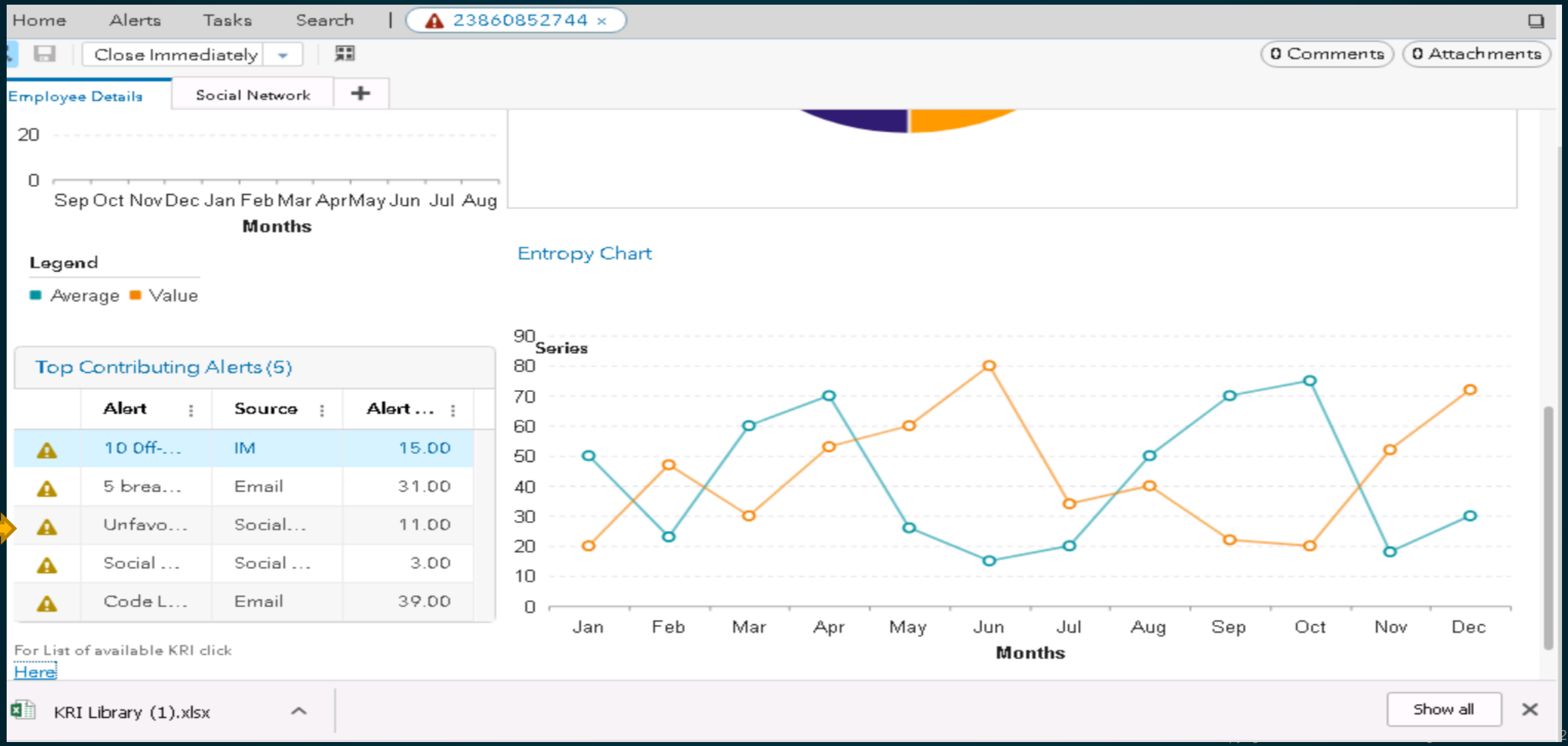


Copyright © 2017 Accenture. All rights reserved.

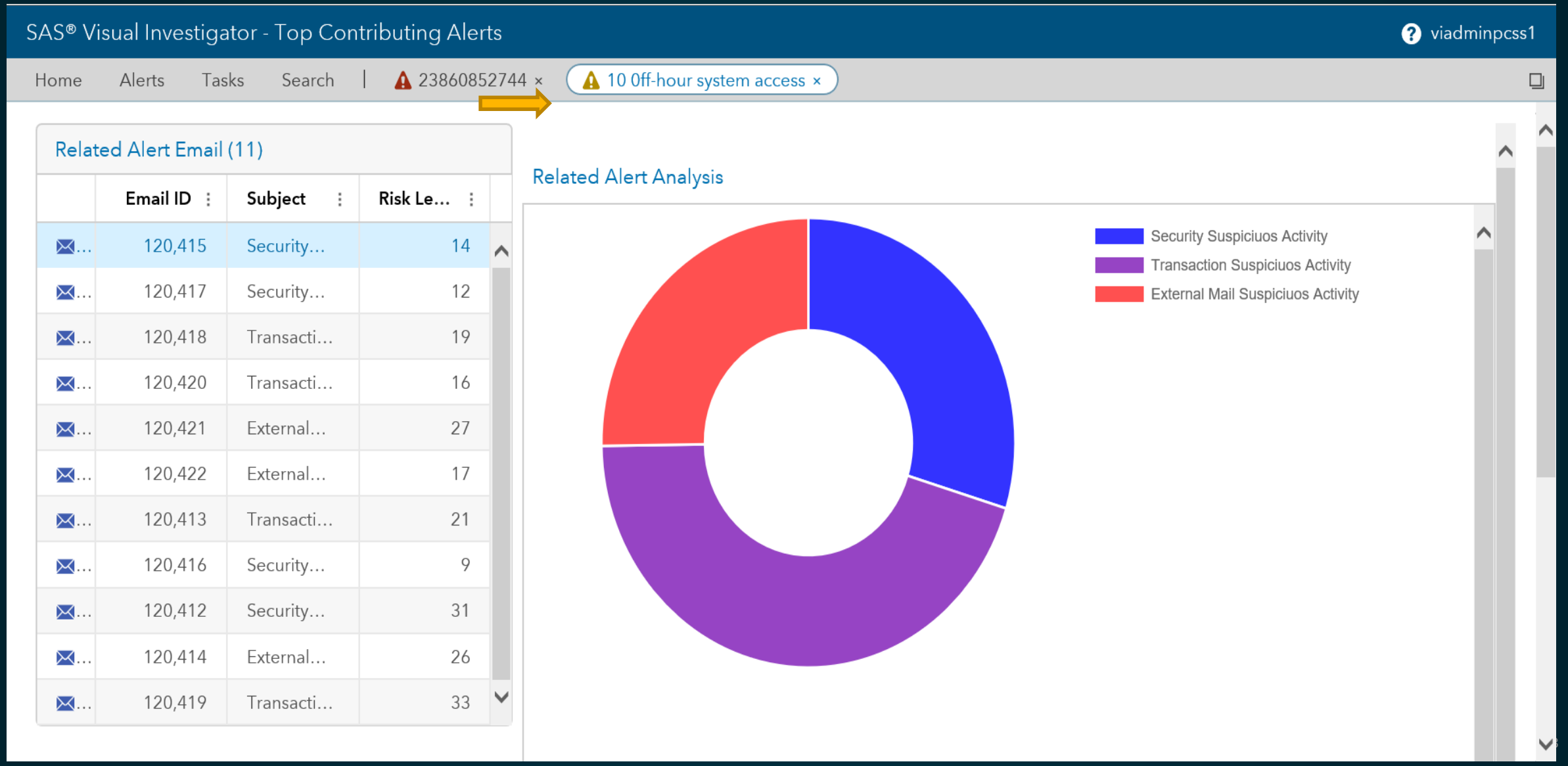
User can view interrelation from Social Network Analytics perspective



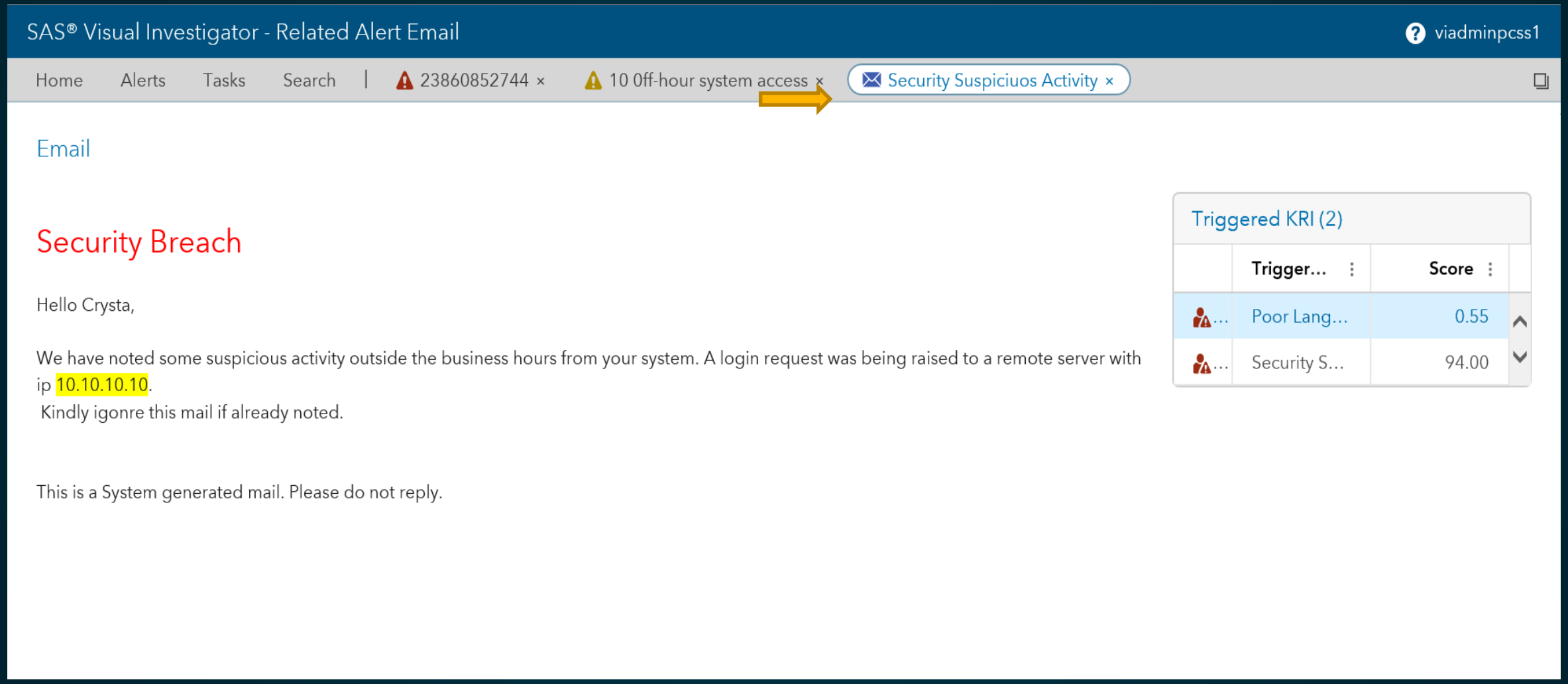
User can examine top Key Risk Indicators triggered per employee



User can look further into a specific type of alert for that employee

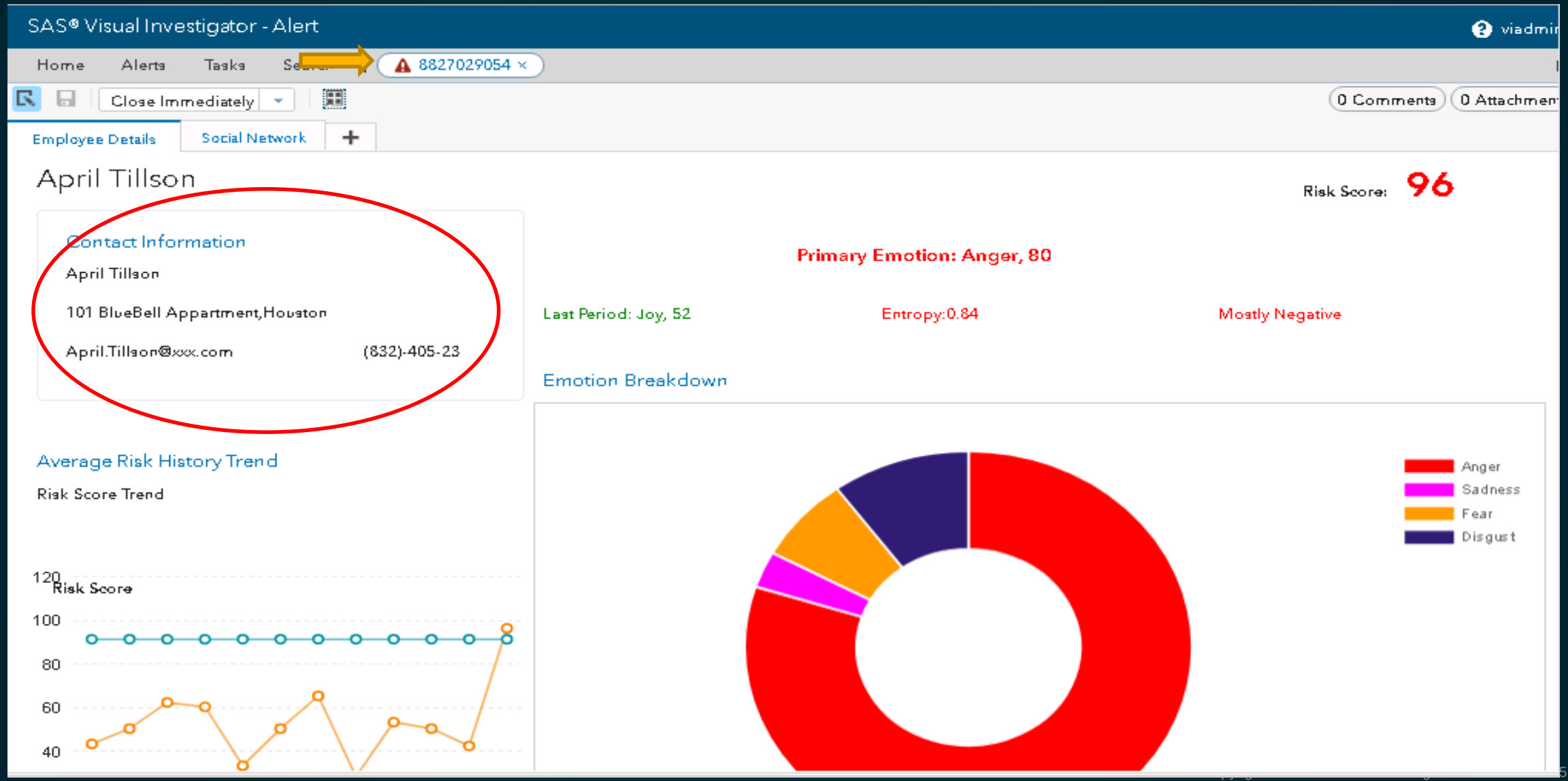


User can drill down to specific email triggering alert

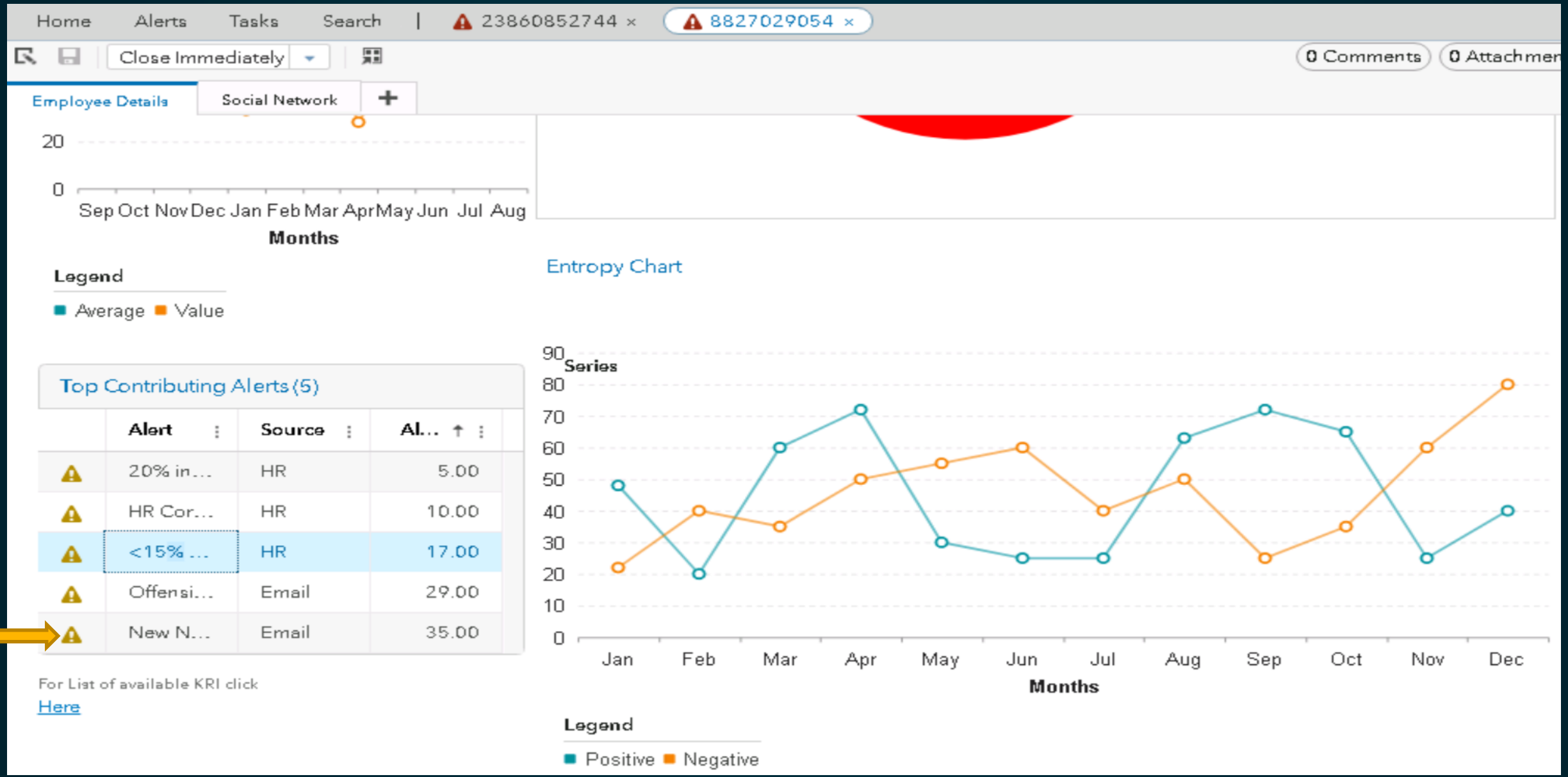


Copyright © 2017 Accenture. All rights reserved.

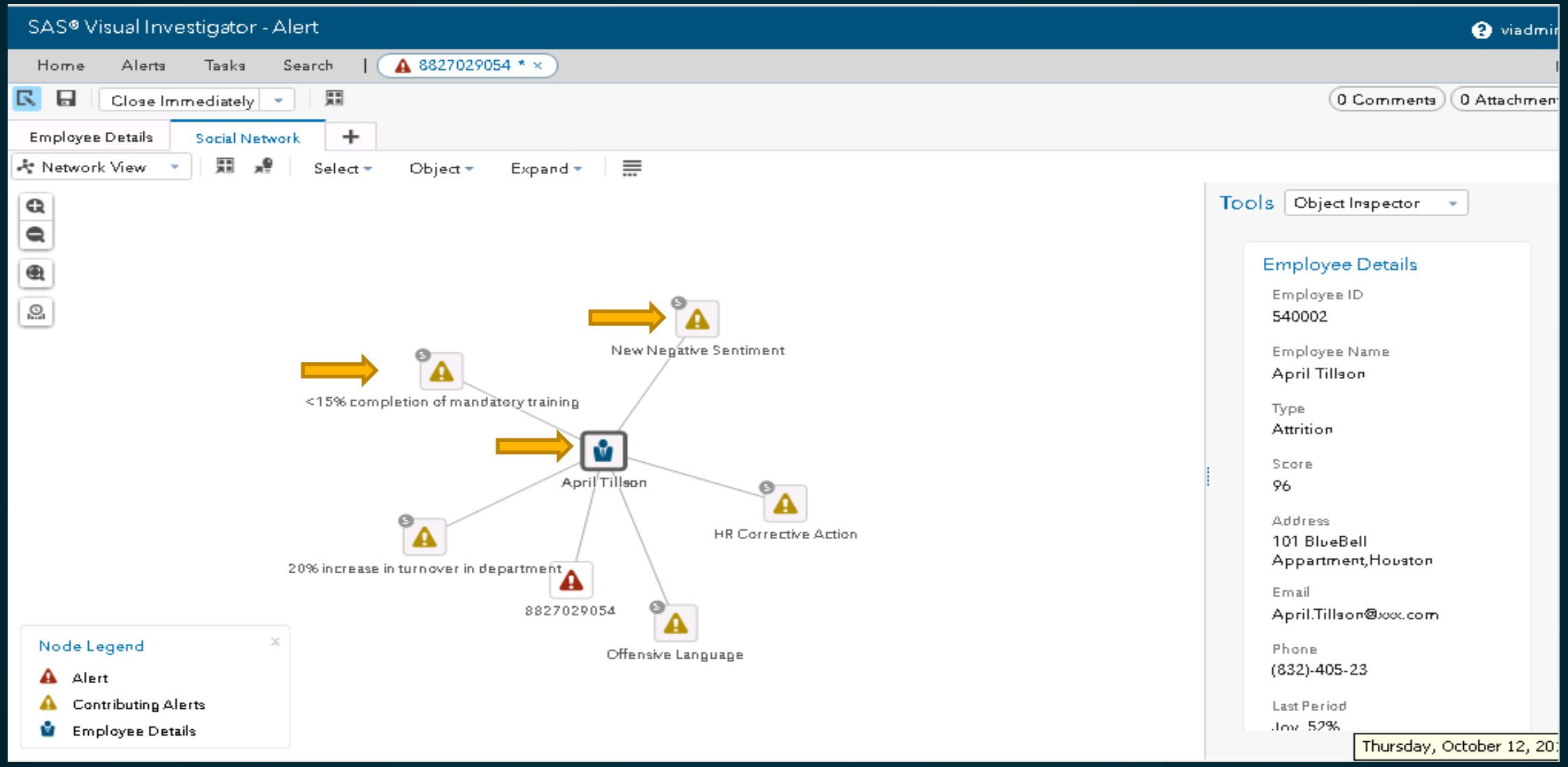
User can drill down into alerts for a specific employee



User can examine top Key Risk Indicators triggered per employee

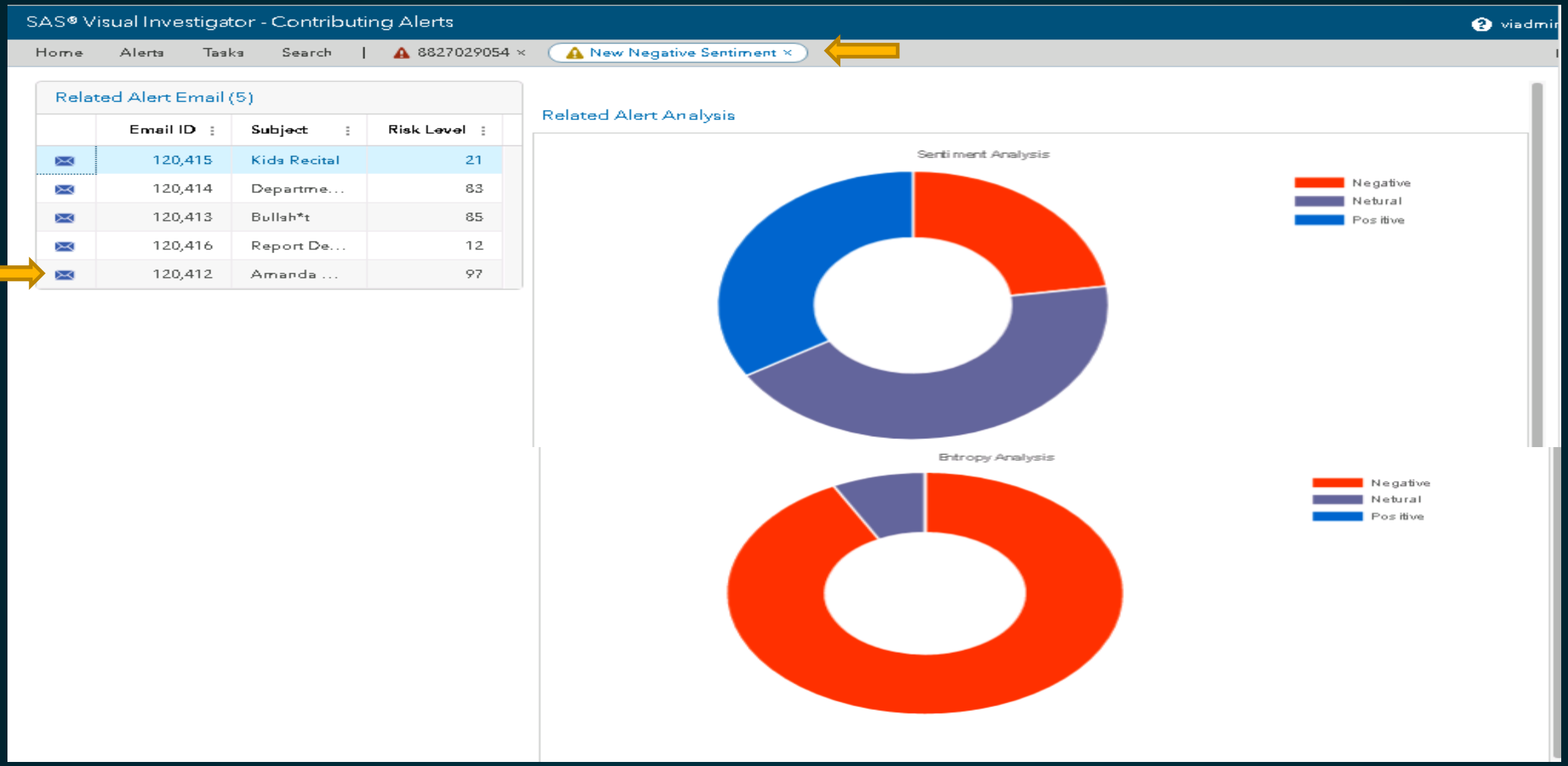


User can view interrelation from Social Network Analytics perspective



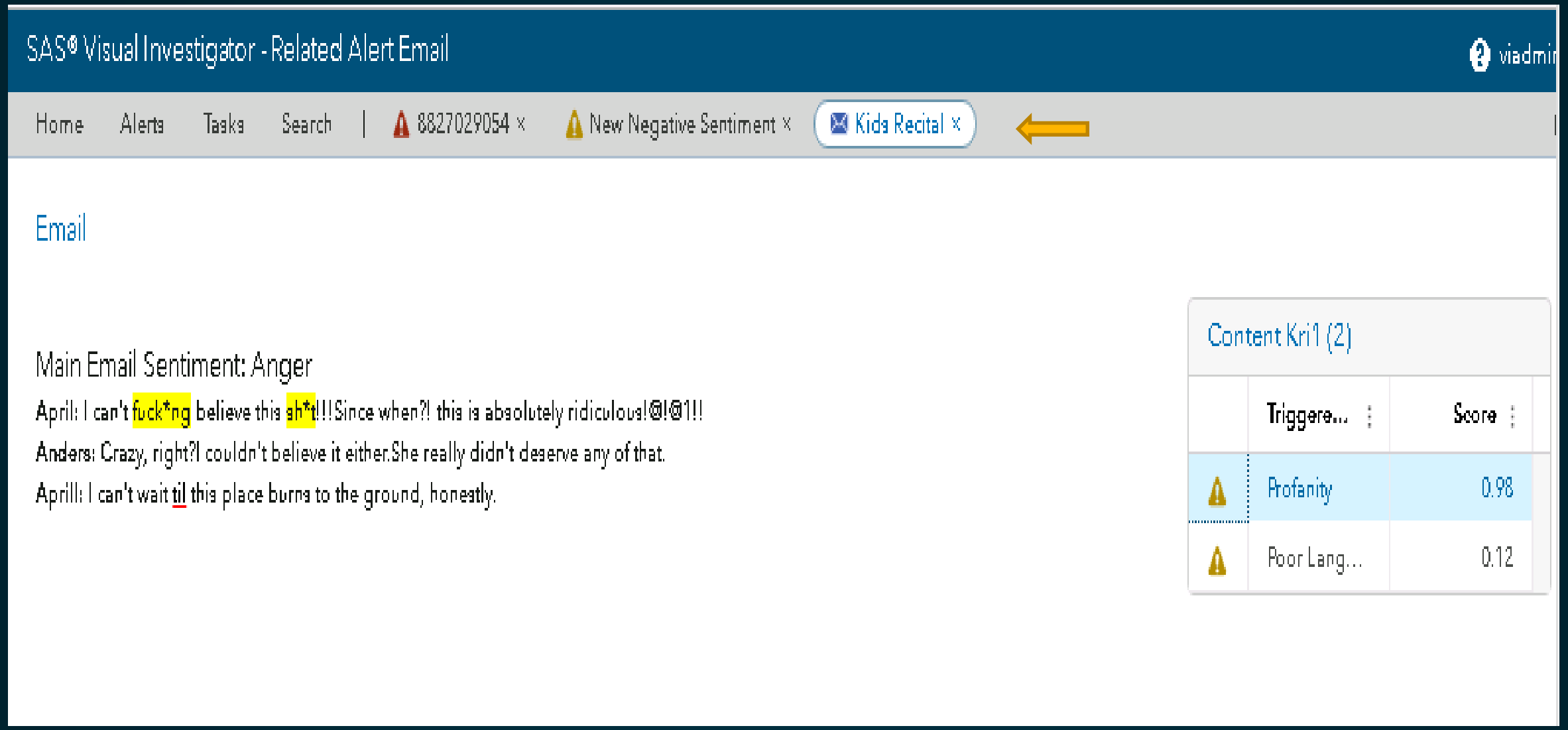
Copyright © 2017 Accenture. All rights reserved.

User can look further into a specific type of alert for that employee



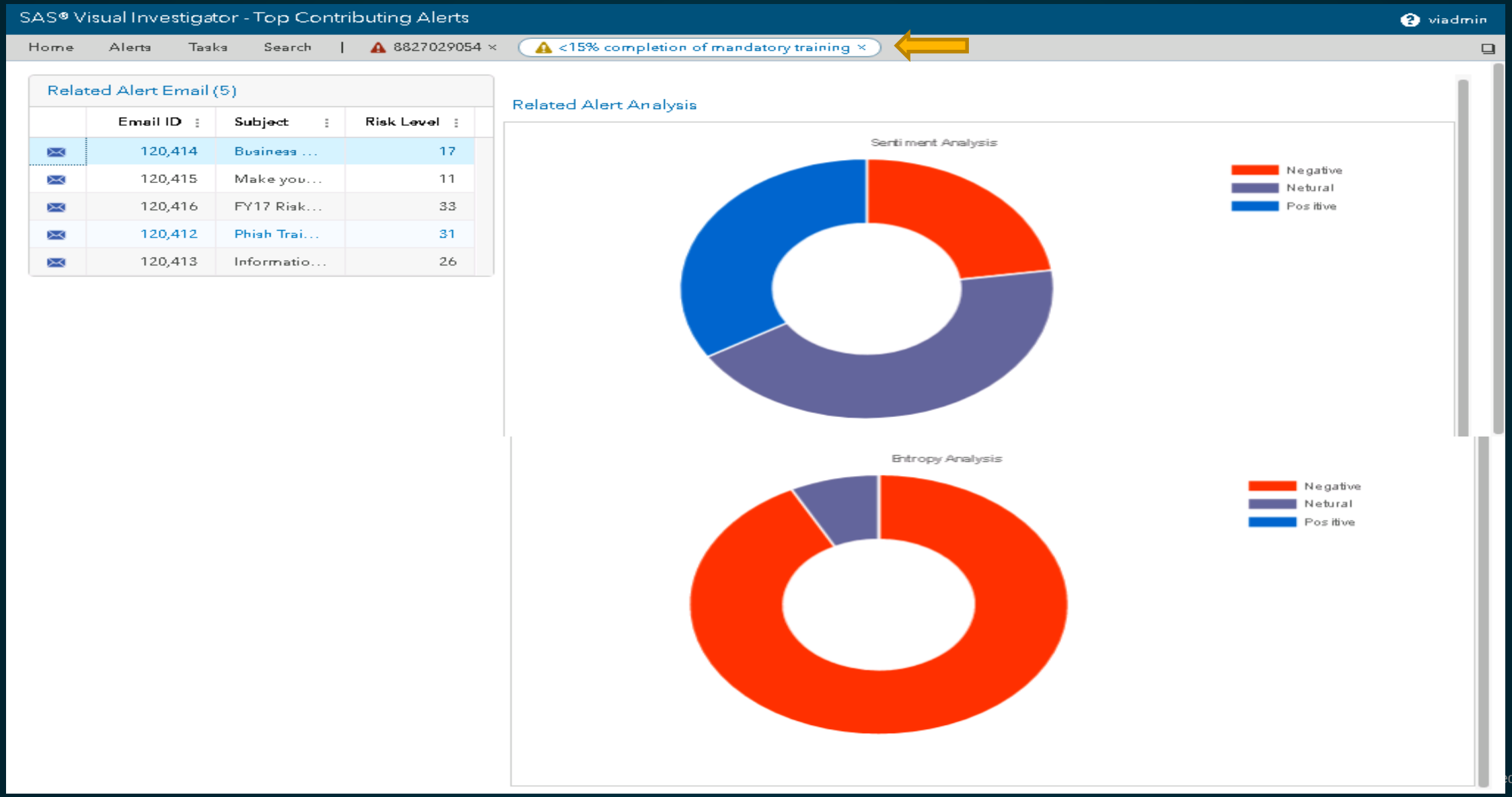
Copyright © 2017 Accenture. All rights reserved.

User can drill down to specific email triggering the alert

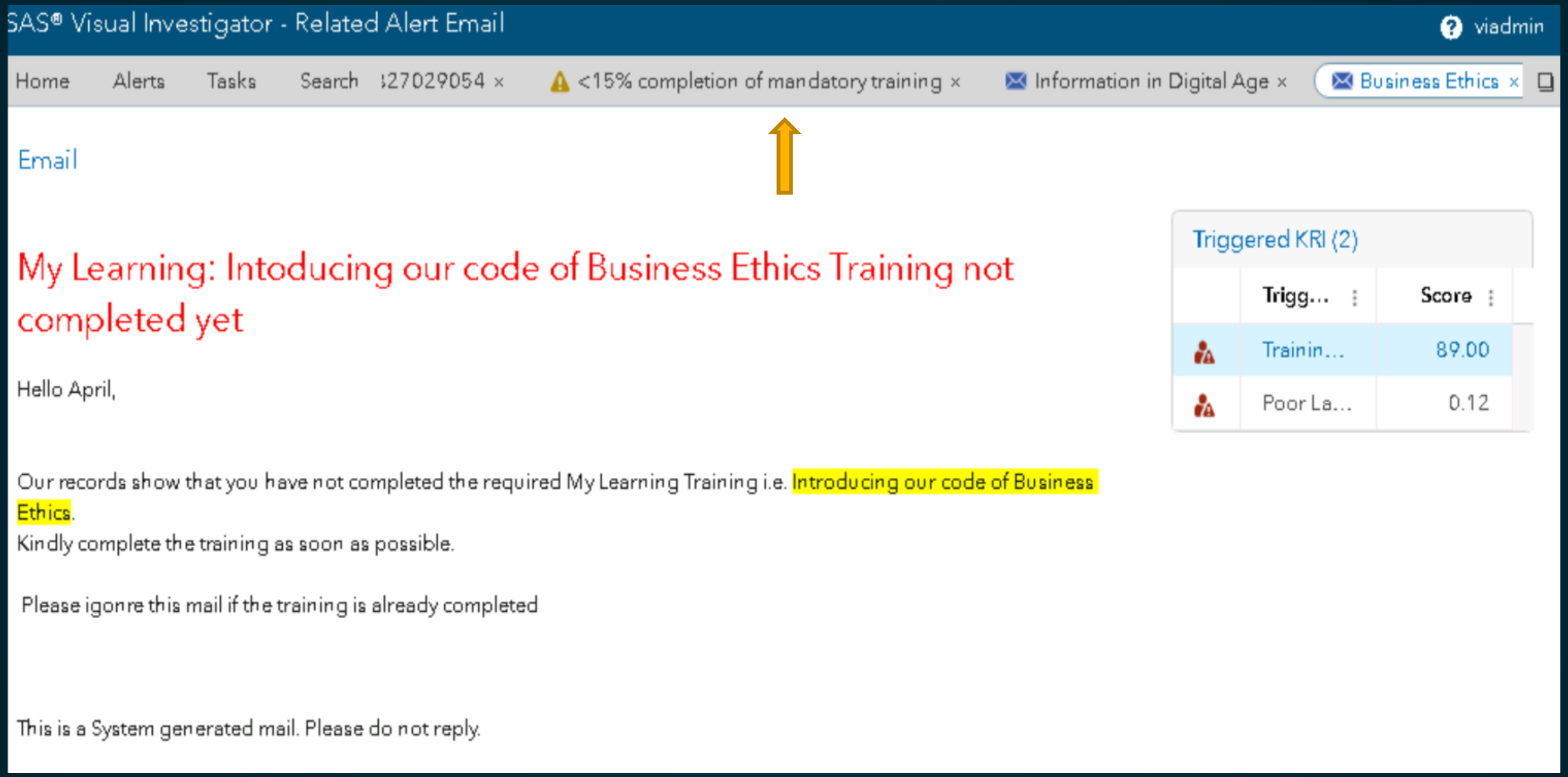


Copyright © 2017 Accenture. All rights reserved.

User can look further into a specific type of alert for that employee

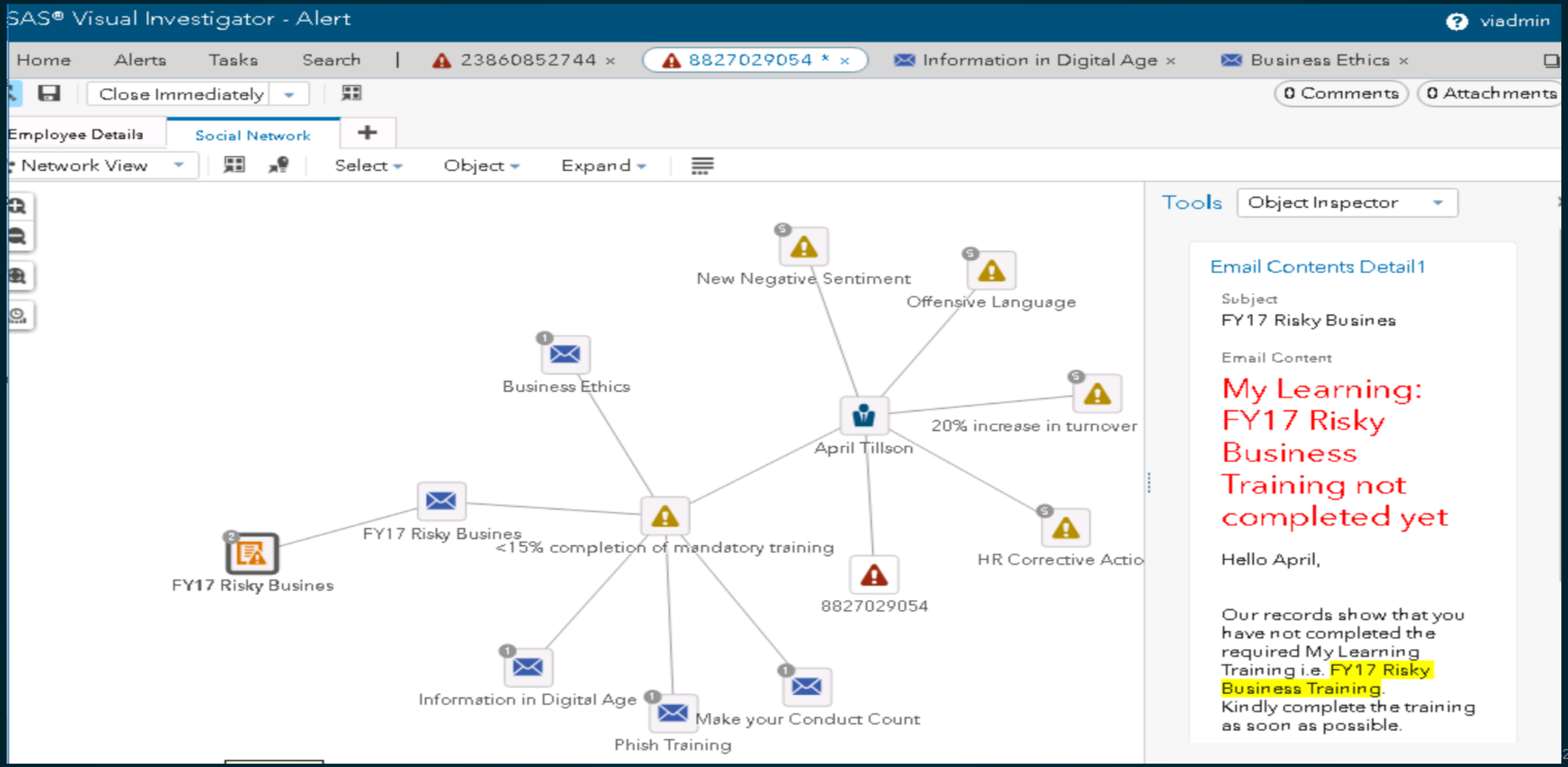


User can drill down to specific email triggering alert

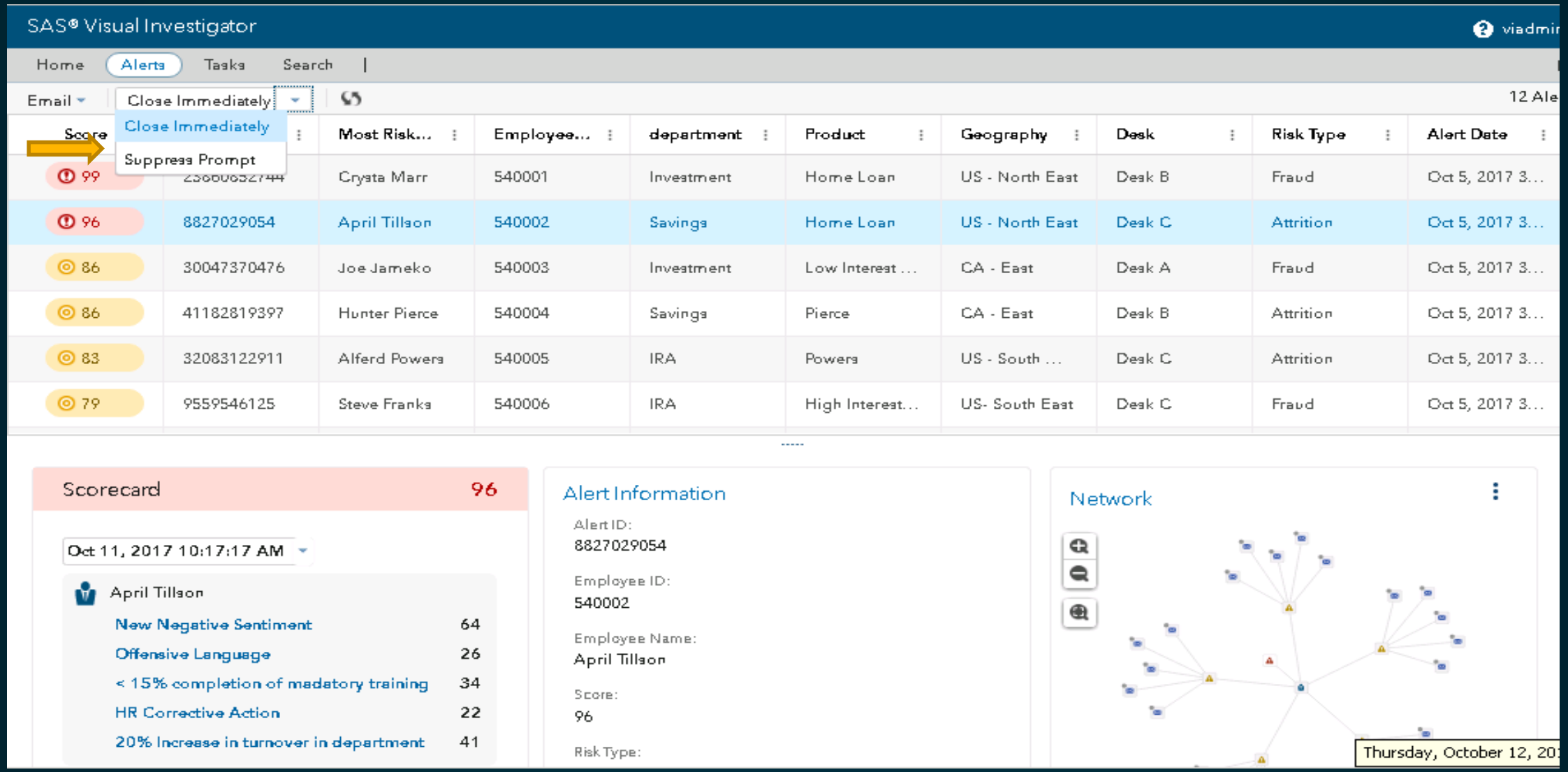


Copyright © 2017 Accenture. All rights reserved.

User can view interrelation from Social Network Analytics perspective



User can take case management action per investigated alert



Copyright © 2017 Accenture. All rights reserved.

High performance. Delivered.

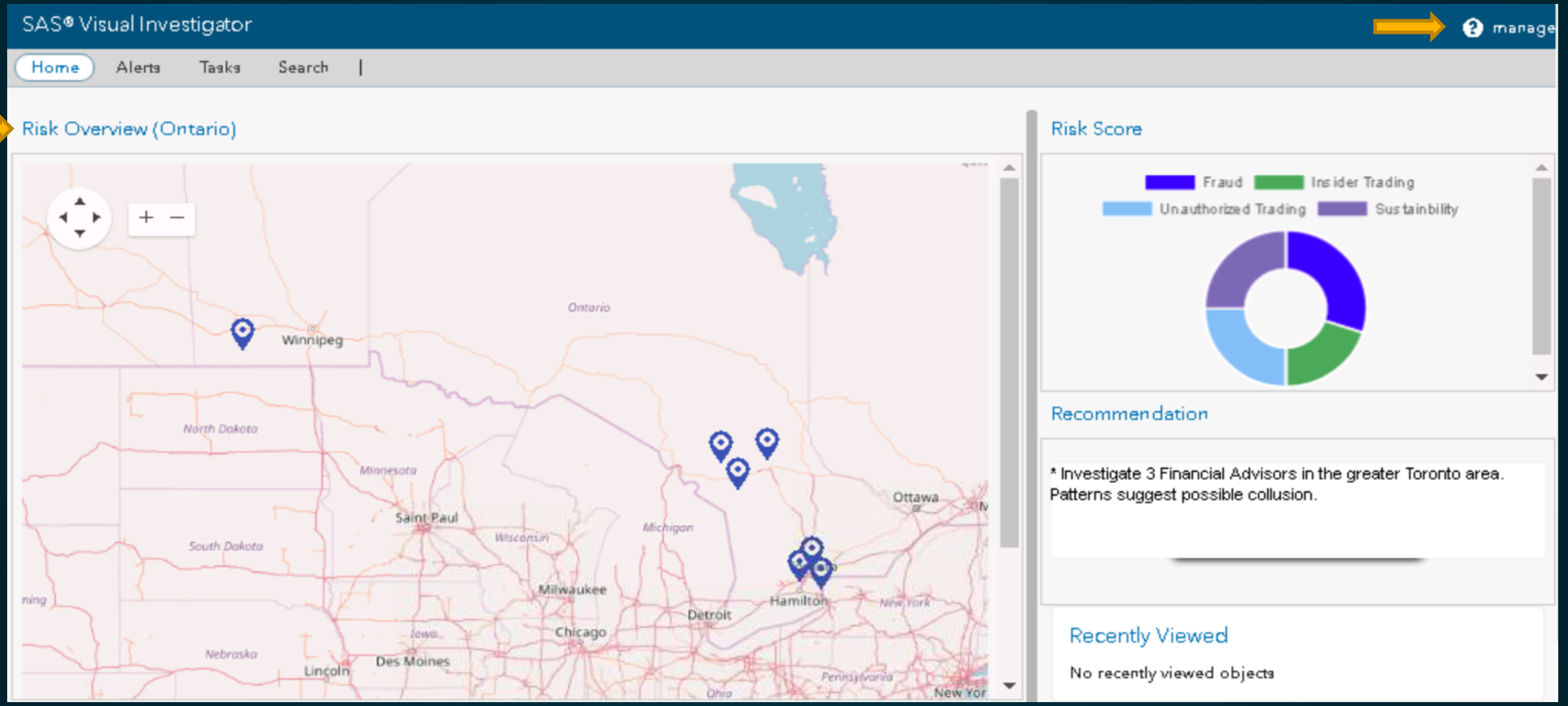
Intelligent Surveillance Demo (SAS Visual Investigator):

"Suspect Behavior Detector"

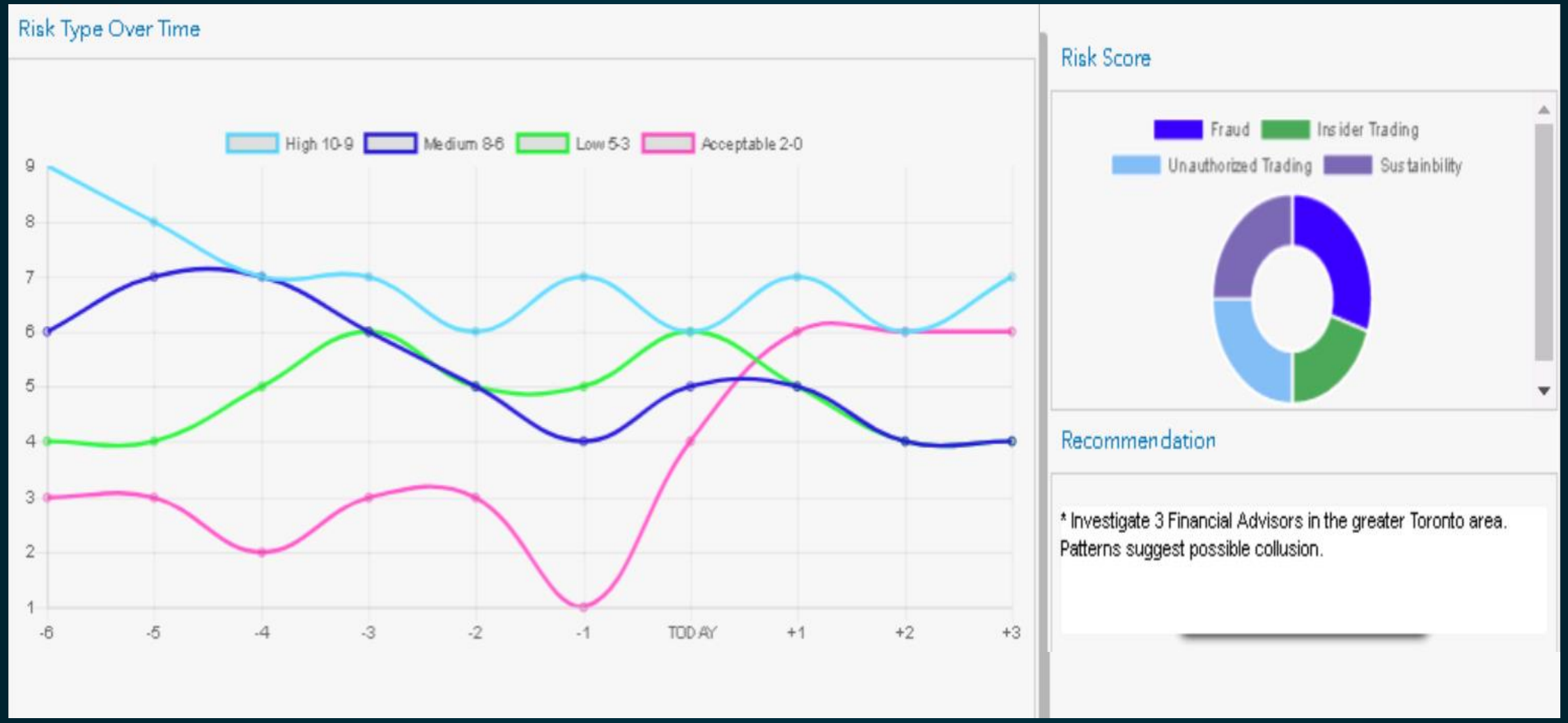
Surveillance Manager View

Copyright © 2015 Accenture All Rights Reserved.

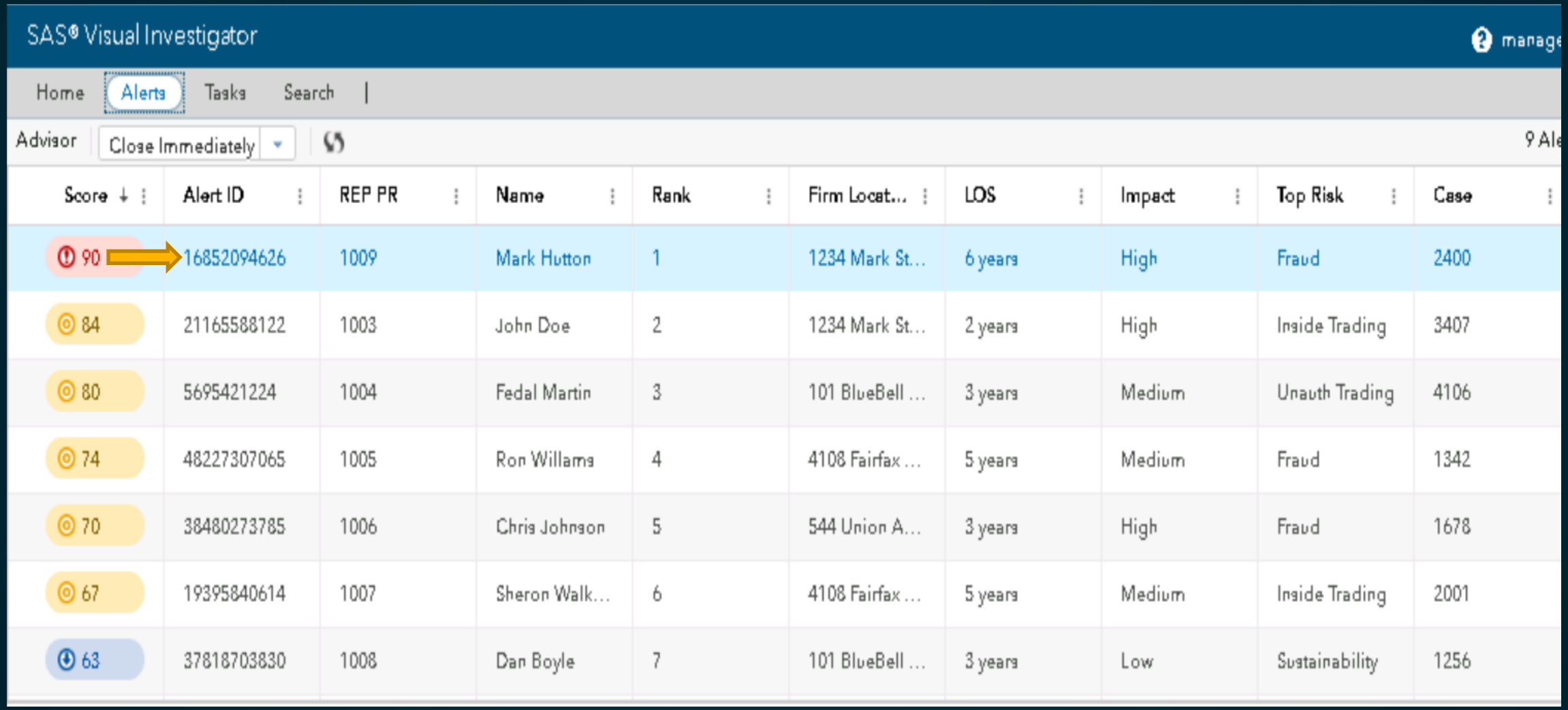
Surveillance/Compliance Manager can examine alerts geospatially



Surveillance/Compliance Manager can examine historical trending of risk typologies

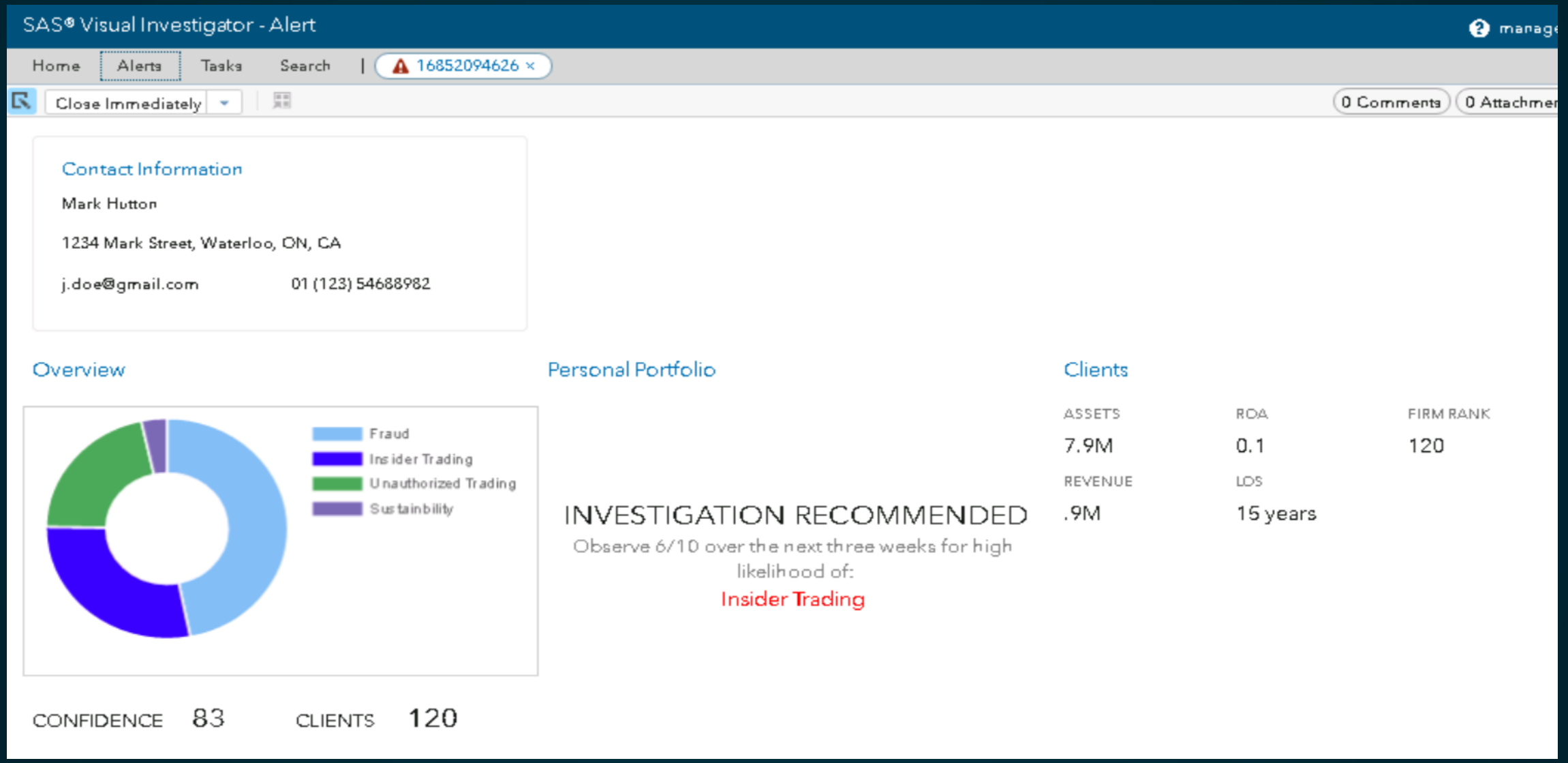


Surveillance/Compliance Manager can examine/investigate individual cases



Score	Alert ID	REP PR	Name	Rank	Firm Locat...	LOS	Impact	Top Risk	Case
90	16852094626	1009	Mark Hutton	1	1234 Mark St...	6 years	High	Fraud	2400
84	21165588122	1003	John Doe	2	1234 Mark St...	2 years	High	Inside Trading	3407
80	5695421224	1004	Fedal Martin	3	101 BlueBell ...	3 years	Medium	Unauth Trading	4106
74	48227307065	1005	Ron Williams	4	4108 Fairfax ...	5 years	Medium	Fraud	1342
70	38480273785	1006	Chris Johnson	5	544 Union A...	3 years	High	Fraud	1678
67	19395840614	1007	Sheron Walk...	6	4108 Fairfax ...	5 years	Medium	Inside Trading	2001
63	37818703830	1008	Dan Boyle	7	101 BlueBell ...	3 years	Low	Sustainability	1256

Surveillance/Compliance Manager can make actionable decisions



accenturedigital

COMMUNICATION SURVEILLANCE & SENTIMENT ANALYSIS

Suspect Behavior Detection

SURVEILLANCE- CHALLENGES & USE CASES

WHY SURVEILLANCE ?

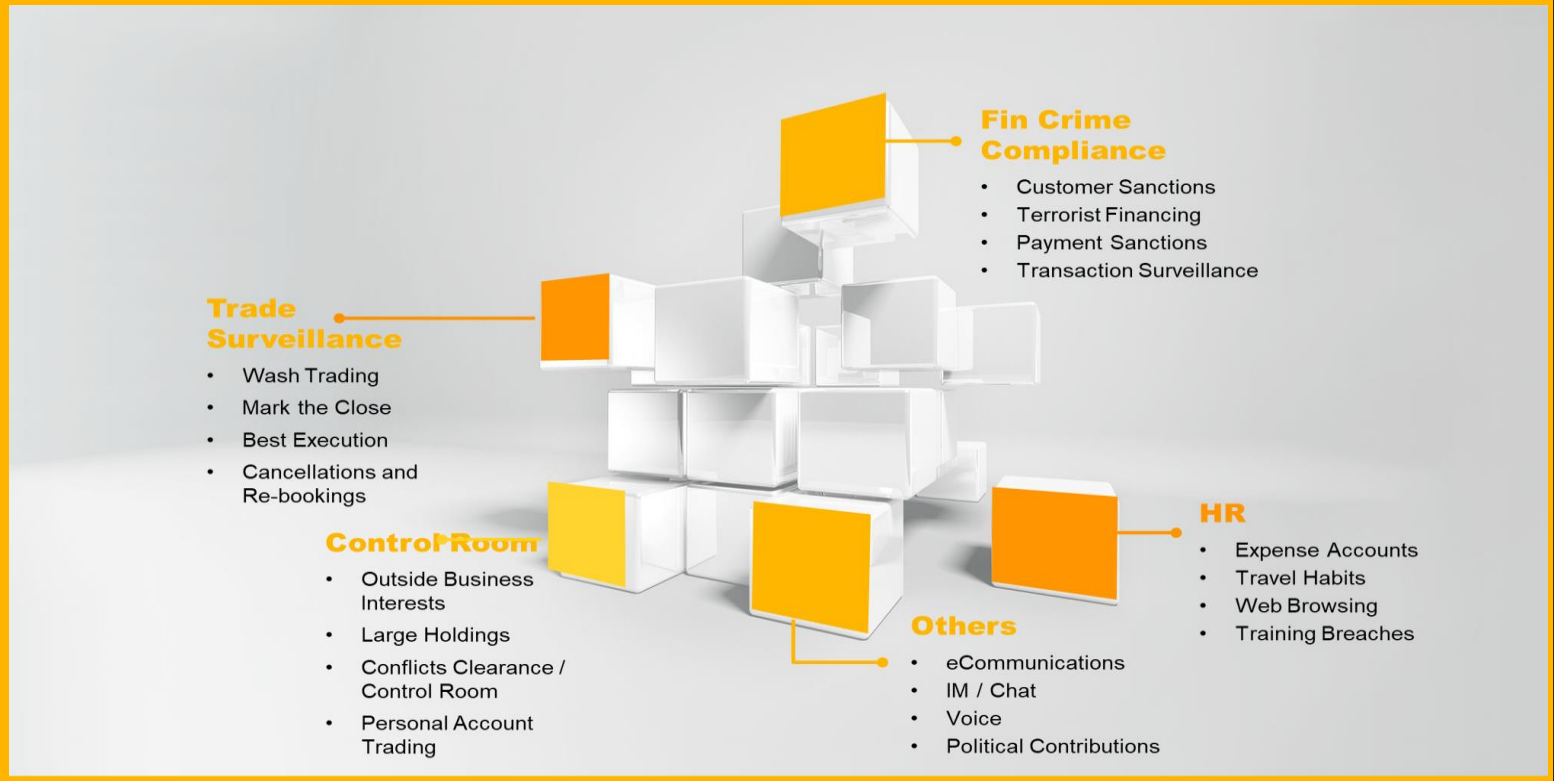
- **Unauthorized Trading** – individual traders that find mechanisms to go around systems, processes, and controls to distort / hide actual risk exposure and true trading profits / losses.
- **Market Manipulation & Abuse** – traders that engage in collusion with external counterparts of other institutions, with the intent to move a benchmark rate / index (e.g. LIBOR) in order to obtain financial gain.
- **Rogue Trading** - Rogue trading poses significant risks / costs to firms, including monetary losses, regulatory repercussions, and adverse reputational impacts.

WHAT MAKES THE LANDSCAPE CHALLENGING ?

- Given malicious behaviour is complex and dynamic in nature, identifying and effectively monitoring is difficult.
- Adding to the complexity, multiple data sources (structured / unstructured) are required to proactively detect / prevent evolving fraudulent behaviours.
- Though some technology is available to combat the problem (e.g. Big Data), generally no holistic 'silver bullet' solution exists.
- Separating the signal from the noise is challenging.
- Relatively new market and few viable end-to-end analytic solutions exist.

Accenture is uniquely positioned to integrate leading academic research, IP led innovations in advanced analytics and operations within complex & demanding business environments.

The industry is moving towards surveillance being part of a broader holistic approach, reflecting dependencies between various use cases, in mitigating risk and complying with regulations.



Copyright © 2018 Accenture. All rights reserved.

SURVEILLANCE- SOLUTION & IP LED ASSETS

POTENTIAL DATA SOURCES

Real Time Transactions/ Trading activity
- Financial Performance - Exposure changed dramatically?
- Transaction Performance - Cancel and corrected trades?
- Market Benchmarking - Performance against market?

Communication
- Email - Focus of this phrase & sentiment
- Documents - Are they sharing confidential info?
- Social Media - What do they say on Social Media ?
- Chat - Who do they talk to?

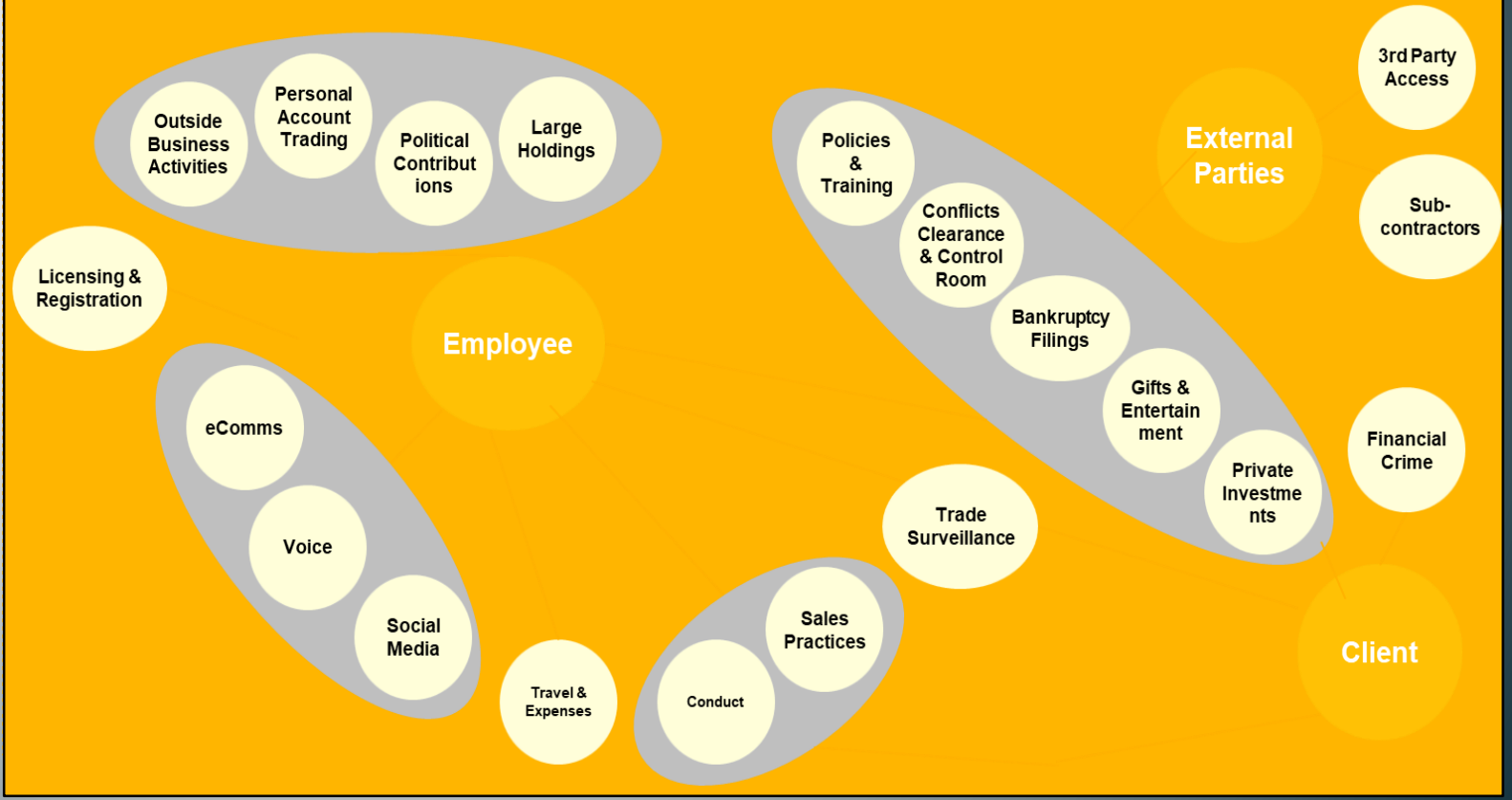
Behavior
- Behavior data - Systems accessed /Log-on times?
- HR data - How many hours of professional training?

ACCELERATORS AND DIFFERENTIATORS

- Deployed additional advanced analytics techniques & algorithms, such as text mining, PCA, Multi-dimensional Scaling, K-means Clustering, Machine Learning etc.
- Analysed diverse datasets including Enron, Hillary Clinton, US Election, & Social Media data.
- Built "Suspect Behaviour Detector" Advanced Analytics App on the Accenture Insights Platform (AIP), also running on SAS VI (Visual Investigator).
- Current development focus on adding audio/voice analytics in the tool to determine synthetic voice etc. to enhance the tool capability to encompass wholistic behavioral modelling.

Integrated Surveillance requires analysis of disparate data sources and both linguistic analysis (e.g. NLP) & stochastic modeling. The goal is to find both content-based sensitive information and unusual behavioral patterns.

Connecting data points from multiple entities is key to enable surveillance to proactively identify emerging misconduct.



Copyright © 2018 Accenture. All rights reserved.