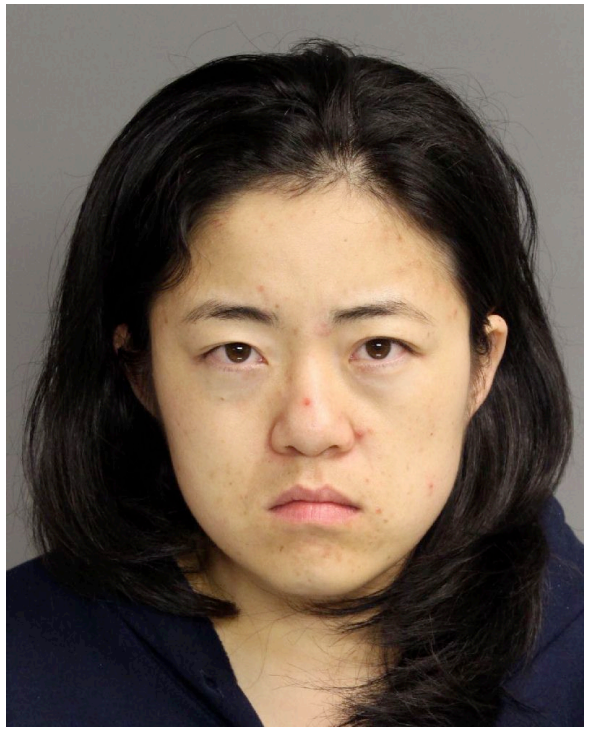
The Human Side of Insider Threats

Doug Sampson, Founder & CEO at Soteritech

Soteritech

Context



- Yuan Li

SANOFI

Context

- Edward Snowden

Booz | Allen | Hamilton

CENTRAL INTELLIGENCE AGENCY

Context

- Lt. Cmdr. Edward C. Lin

Context

- Kun Shan “Joey” Chun

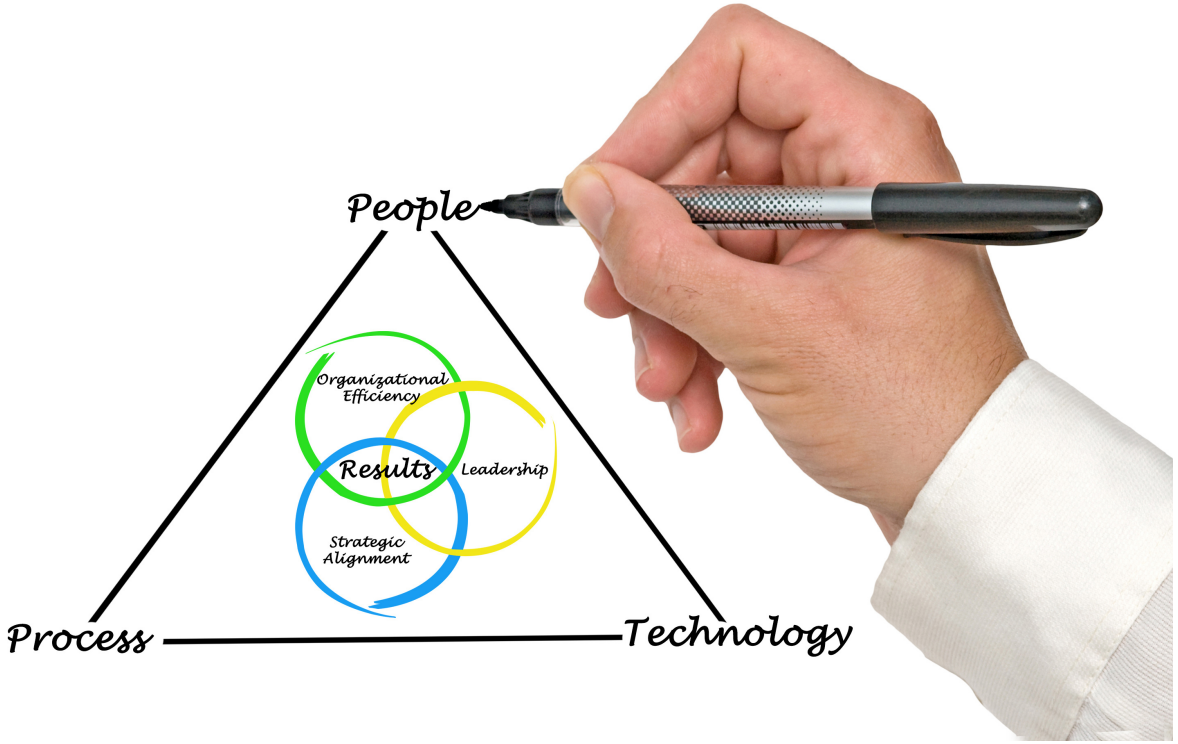
Context

- IMPACT?

Insider Threat Program

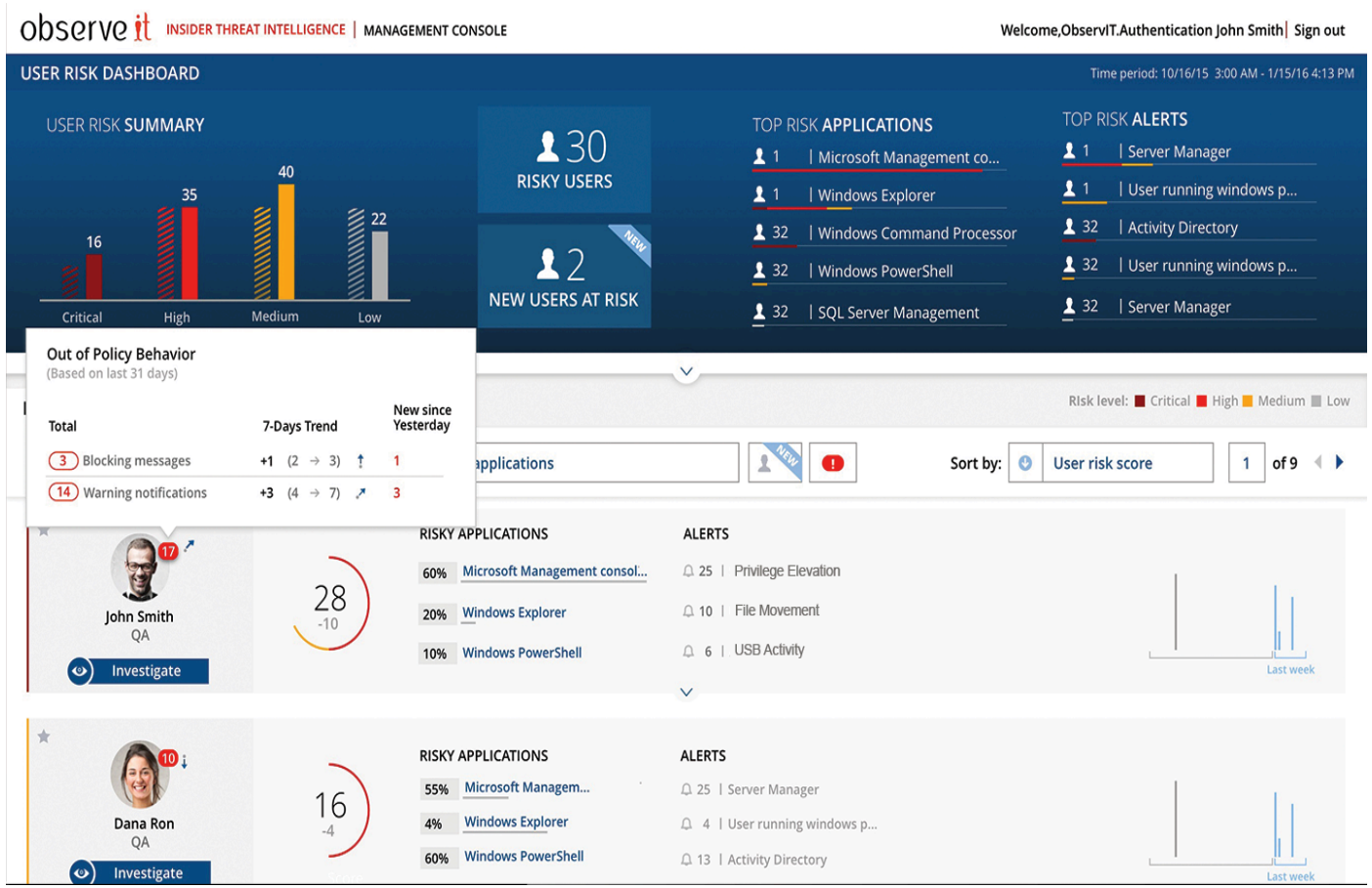
- Definition
- Why it’s important

Insider Threat Program



- People
- Process
- Technology

Technologies

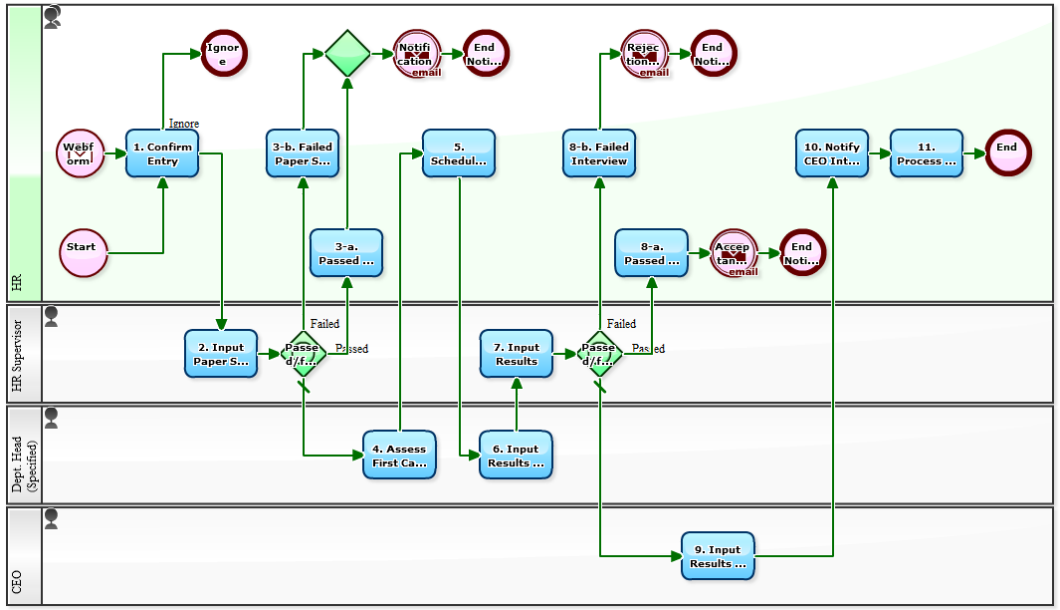


- ObserveIT
- Fortinet
- Forcepoint
- Vormetric
- Identrix
- Lancope

People

- Executives
- Management
- Working Group/HUB
- Employees

Process



- Policy & employment agreement changes
- Enterprise risk assessments
- HUB and employee training
- Proactively managing employee issues
- Comprehensive termination procedures

Monitoring Process

Inputs →

- Network monitors
- Ins Threat tools
- Anonymous tip line
- Other employees
- Perf appraisals
- HR activity
- Outside monitors

Collection

Activity →

Evaluate, Communicate, Rate

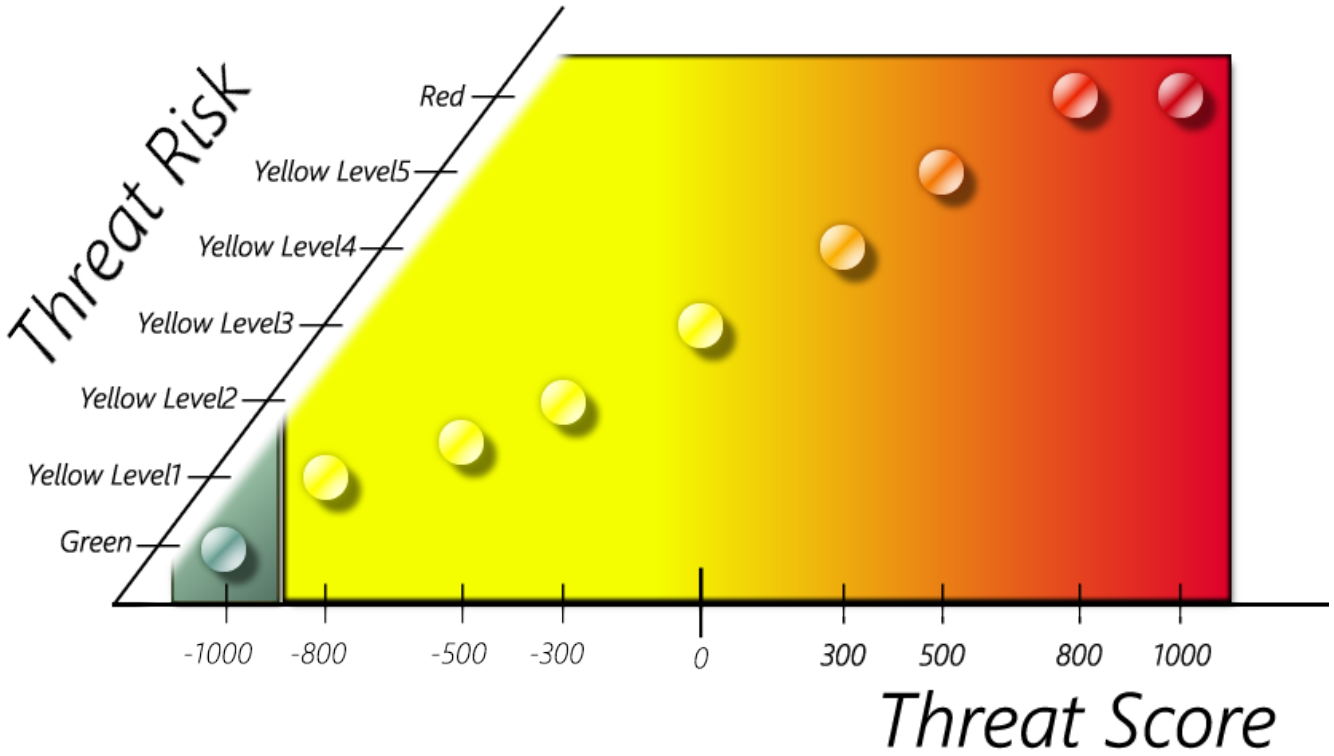
Outputs

Comms Plan, Communicate, React

HUB

- Purpose
- Participants
- Prearranged agreements
- Activities

Indicators



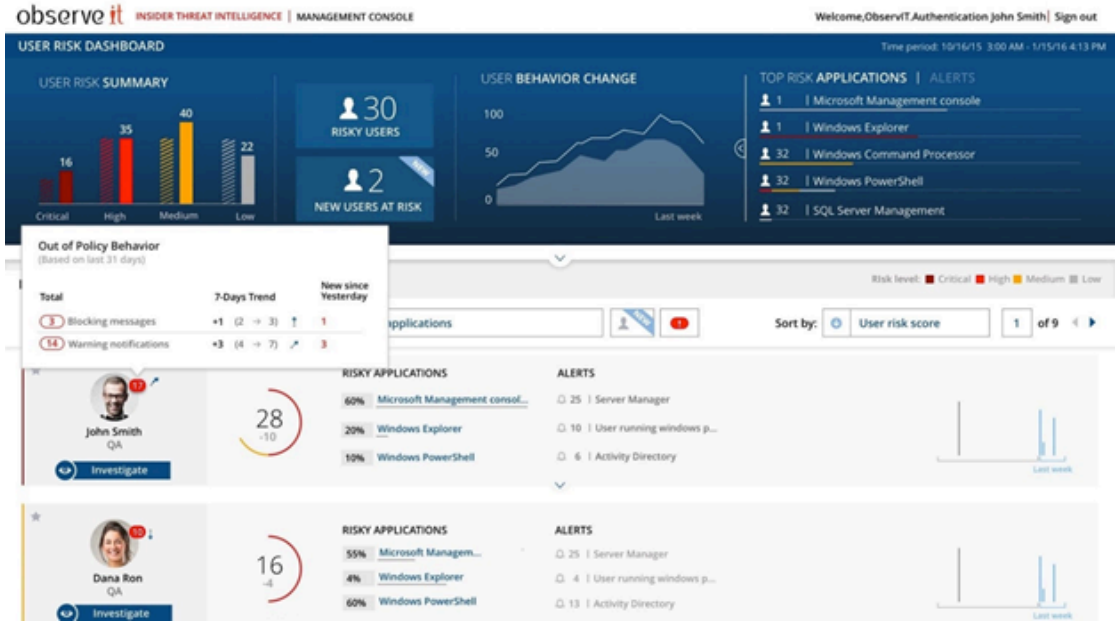
- Classified info handling
- Criminal activity
- Finances
- Interpersonal
- Leave of absence
- Loyalty
- Mental health
- Substance abuse
- Technical activity

Evaluations

- Notification comes in
- Triage within 10 minutes
- Initial level assigned
  - Green (low risk potential, no further investigation needed)
  - Yellow (unsure risk potential, needs immediate initial investigation)
  - Red (sure risk, needs immediate investigation and action)

Green

- Person’s behavior is deemed normal for his or her job function and responsibility level
- Examples



Yellow

- Questionable behavior that deserves further investigation.
- Widest reporting of incidents
- Could be broken down further
- Broad range of
  - Communication
  - Collection
  - Consequence
- Examples

Red

- Behavior unacceptable and against company policy
- Significant information gathering (proof)
- Severe consequences
- Examples

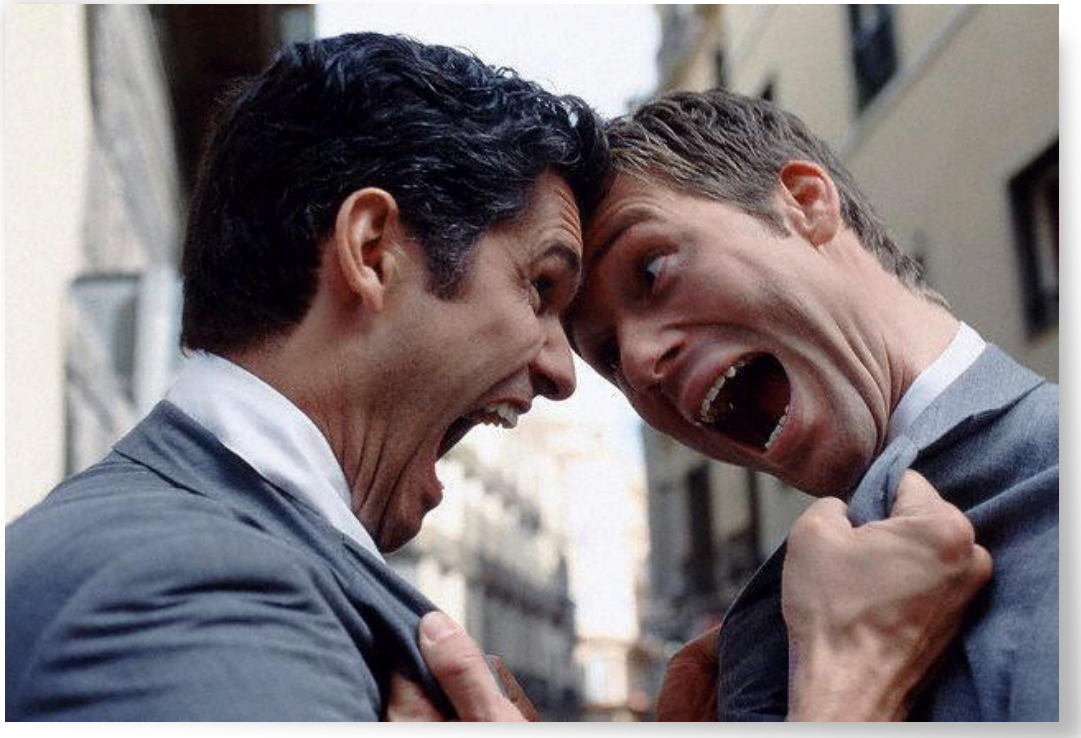
Hub Communication

Communicate with certain groups based on severity scale

- Green – maintain internal log
- Yellow – involve HR, IT, Security Office, Legal and Exec (possibly Govt - COTR) depending on level
- Red – involve HR, IT, Legal, Security Office, Exec, COTR (if applicable) and Authorities

Confrontation

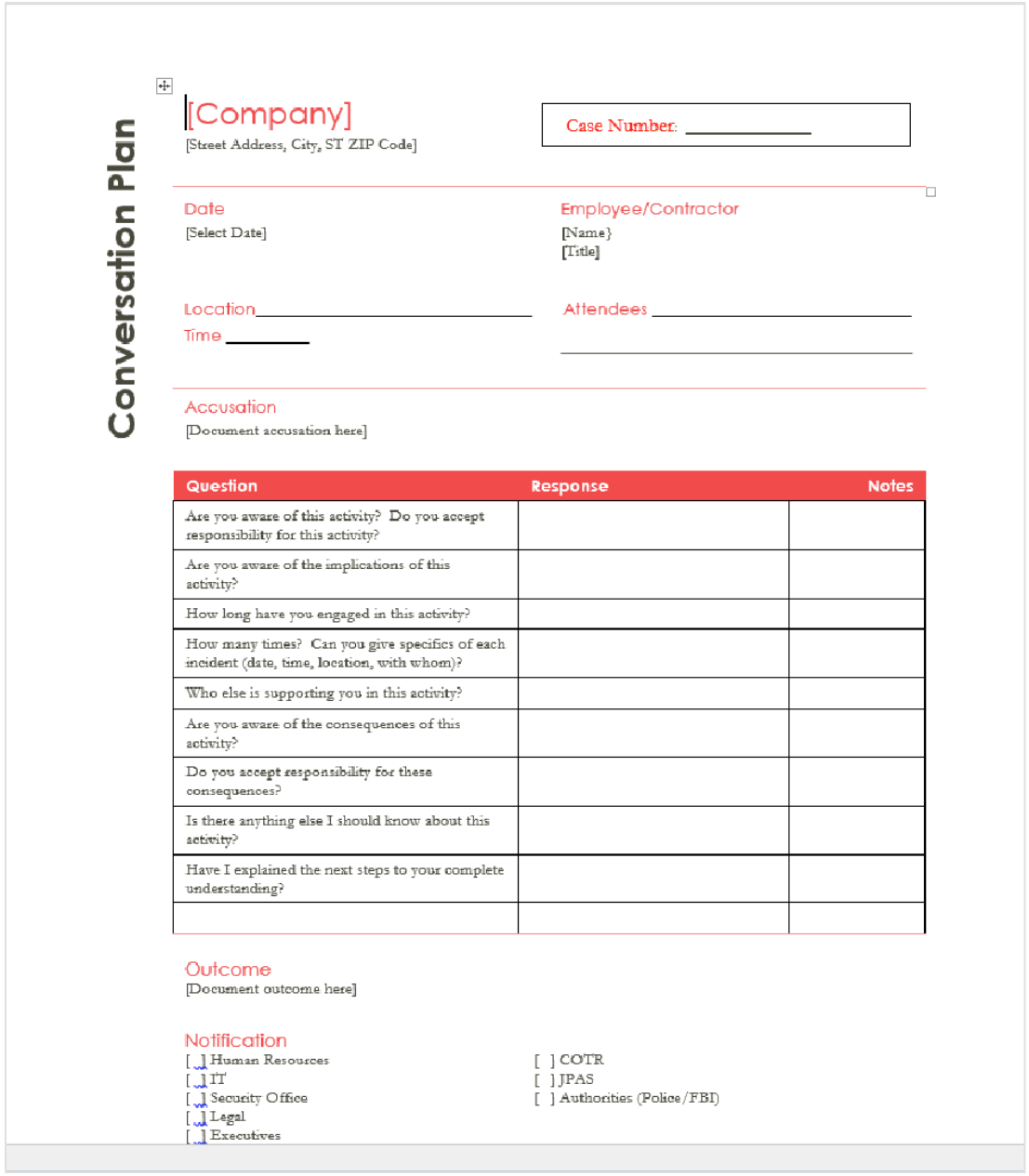
- Green – none
- Yellow – mild to moderate/intense
- Red – intense/severe



Conversations

- Logistics
- Who to have involved?
- How to prepare?
- What if they go sour?
- What to do?

Conversation Plan



Conversation Plan

[Company]
[Street Address, City, ST ZIP Code]

Case Number: _____

Date
[Select Date]

Employee/Contractor
[Name]
[Title]

Location_____
Time _____

Attendees _____

Accusation
[Document accusation here]

Question	Response	Notes
Are you aware of this activity? Do you accept responsibility for this activity?		
Are you aware of the implications of this activity?		
How long have you engaged in this activity?		
How many times? Can you give specifics of each incident (date, time, location, with whom)?		
Who else is supporting you in this activity?		
Are you aware of the consequences of this activity?		
Do you accept responsibility for these consequences?		
Is there anything else I should know about this activity?		
Have I explained the next steps to your complete understanding?		

Outcome
[Document outcome here]

Notification
[ ] Human Resources
[ ] IT
[ ] Security Office
[ ] Legal
[ ] Executives
[ ] COTR
[ ] JPAS
[ ] Authorities (Police/FBI)

Yellow

Scenario: Employee overhead talking about the new rocket guidance kit to a fellow employee at a local restaurant

- Pre-discussion preparations
- Situational awareness
- Discussion Part 1: Accusation
- Discussion Part 2: Consequences
- Successful outcomes
- Un-successful outcomes
- Monitoring

Red

Scenario: Leaving the premises with prototype radar sensors

- HUB communications
- Pre-discussion preparations
- Situational awareness
- Discussion Parts 1&2
- Successful outcomes
- Un-successful outcomes

How to Get Better at the Conversation

- Simulation/Role Play
- Repetition
- Culture of Security

Questions

Doug Sampson
doug.Sampson@soteritech.com
Soteritech, LLC (@soteritech)
571-393-3801