CITD

Corporate Insider Threat Detection

SMi Oil and Gas Cyber Security Conference
June 2014

Dr. Philip A. Legg
phil.legg@cs.ox.ac.uk
Cyber Security Centre, University of Oxford, UK.

Insider Threat

- What do we mean when we talk of *insider threat*?

- An abuse of privaledged access:
  - – Destruction / sabotage (e.g. information, physical).
  - – Theft (e.g. information, financial, physical).
  - – Theft for distribution (e.g. IP).

- Unlike a typical attack, the insider is entitled to act within the organisation, to fulfill their job role.
  - – How can we assess when entitled behaviour becomes malicious behaviour?

UNIVERSITY OF OXFORD

CYBER SECURITY CENTRE

The CITD Project

- Sponsored by the Centre for the Protection of National Infrastructure (CPNI).
- Collaboration between University of Oxford (Cyber Security, e-Research and Business School), University of Leicester and Cardiff University.
    - Psychology and behavioural analysis led by Leicester.
    - Criminology analysis led by Cardiff.
    - Cyber Security Centre focus on the detection algorithms.
    - e-Research Centre focus on the visual analytics development.
    - Business school focus on the education and awareness.

CPNI
Centre for the Protection
of National Infrastructure

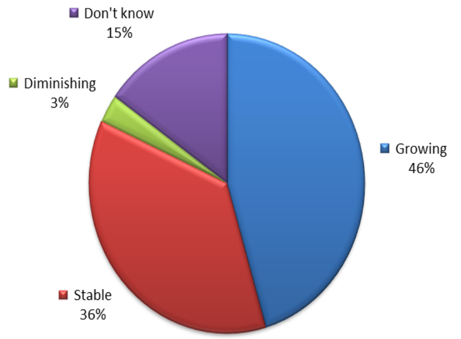
INSIDERTHREAT

UNIVERSITY OF OXFORD

CYBER SECURITY CENTRE

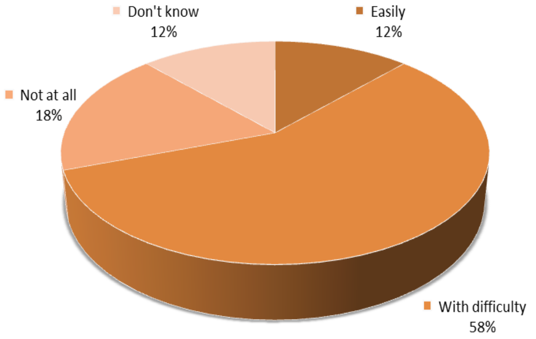
Highlights from Web-based Survey

Do you think that the threat from insiders is growing or diminishing?



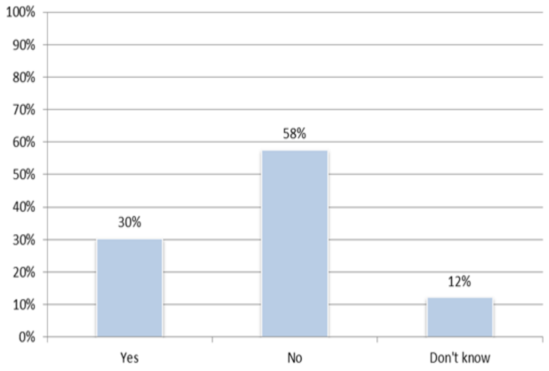
Almost half of the respondents felt that the threat from insiders was growing.

Please describe the extent to which you can predict insider threats before they conduct attacks.



This is an important question that validates the aim of the overall project. 76% of managers said that they were only able to predict an insider attack with difficulty or not at all.

Is insider-threat detection an important part of your organisation's culture?



A strong majority say that insider threat detection was not part of the culture. This suggests that there may be cultural challenges in changing both attitudes and behaviour on the topic.

INSIDERTHREAT

Conceptual Modeling

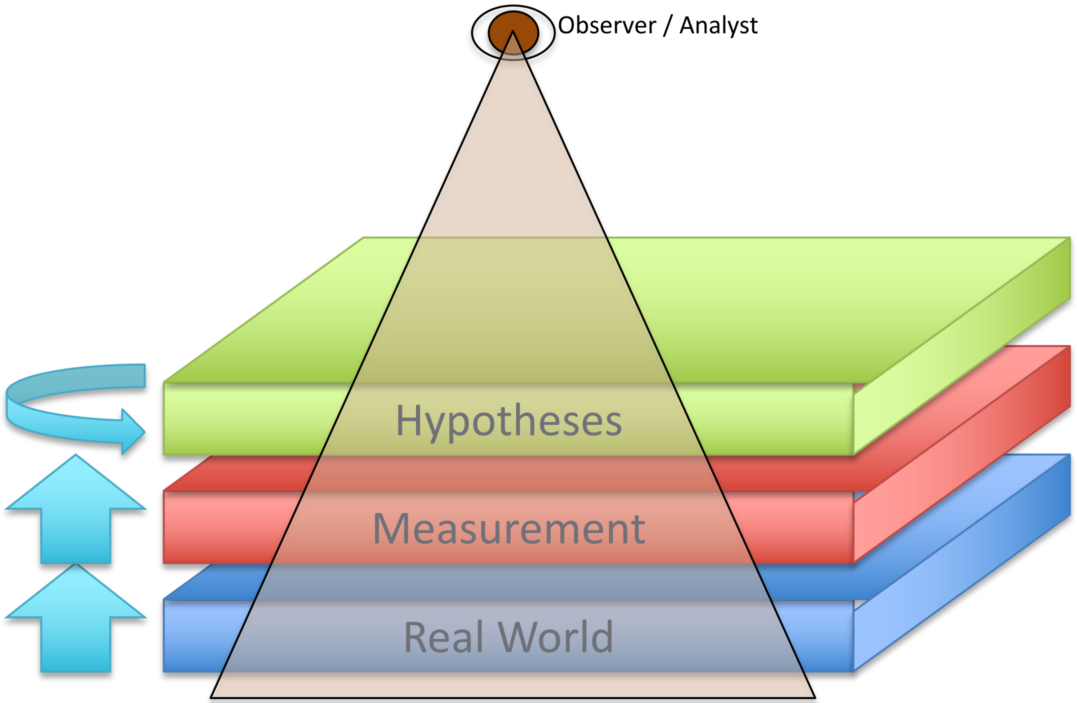
Conceptual Model

- Identifying the problem space, and the related elements that exist within this space.

- Insider Threat is not only a cyber issue – therefore, we need to understand the full scope of the problem.

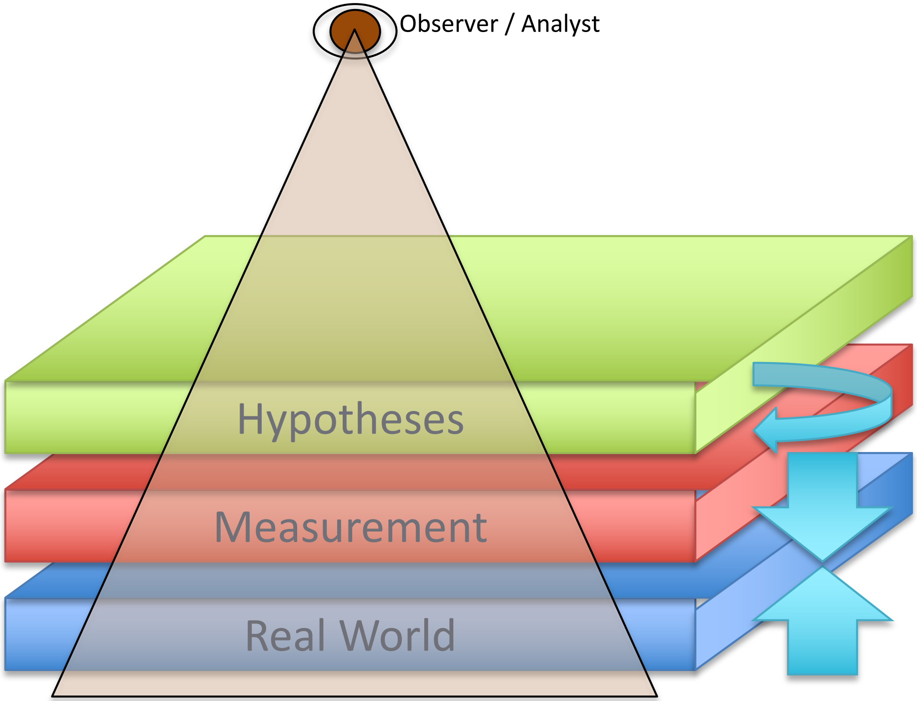
- The conceptual model can help to inform aspects that should be considered in the implementation of a detection system.

Conceptual Model



Hypotheses made regarding the observed insider.
What do we think of their intent based upon the measured data?

Conceptual Model



The measured representation of the real world enables the analyst to explore the data with regards to their initial hypothesis.

Conceptual Model

- Bottom-up reasoning:
  - The data is used to identify suspicious behaviour which in turn alerts the analyst to draw a particular hypothesis.
  - Machine learning and data mining concepts.
  - Anomaly detection.
- Top-down reasoning:
  - The analyst has their own hypothesis for which they would like to verify, in which case the data is utilized in order to support this.
  - Visual analytics and visualization concepts.
  - Data exploration.

Elements of the Model

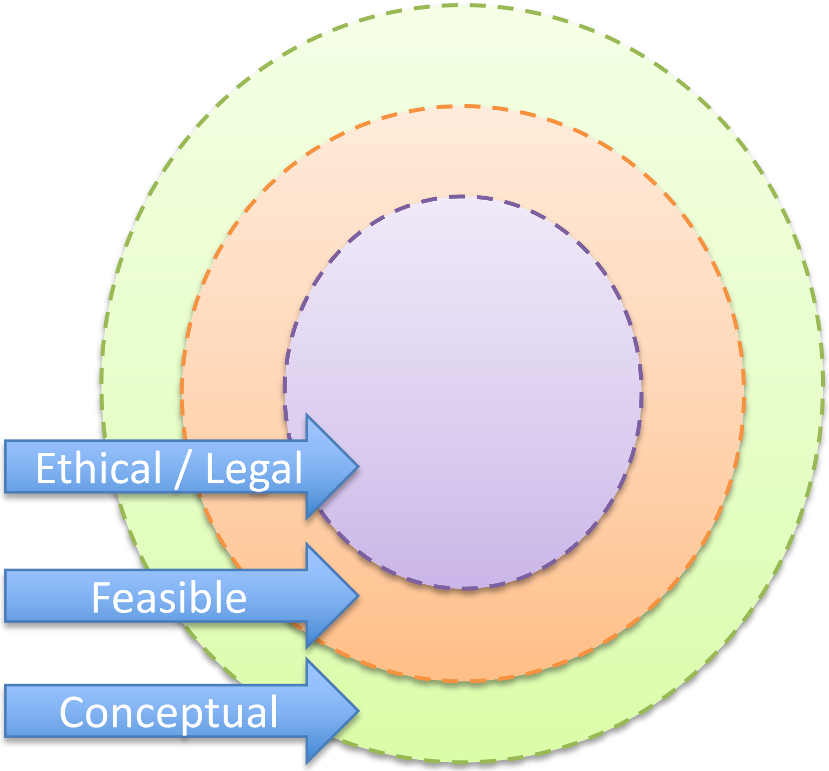
- At the core of the conceptual model are the elements that exist within the problem space of insider-threat.

- All elements would be present within the real world level of the conceptual model.

- The elements would all be measureable (to some extent) to propagate upwards through the model.

Modeling Approach

- Conceptual
  - What is the scope of information that could possibly be collected?
- Feasible
  - What is actually feasible to collect?
  - E.g., How would one quantify employee mentality or disgruntlement?
- Ethical / Legal
  - What is ethically feasible to collect?
  - E.g., Social media monitoring may be a breach of privacy.

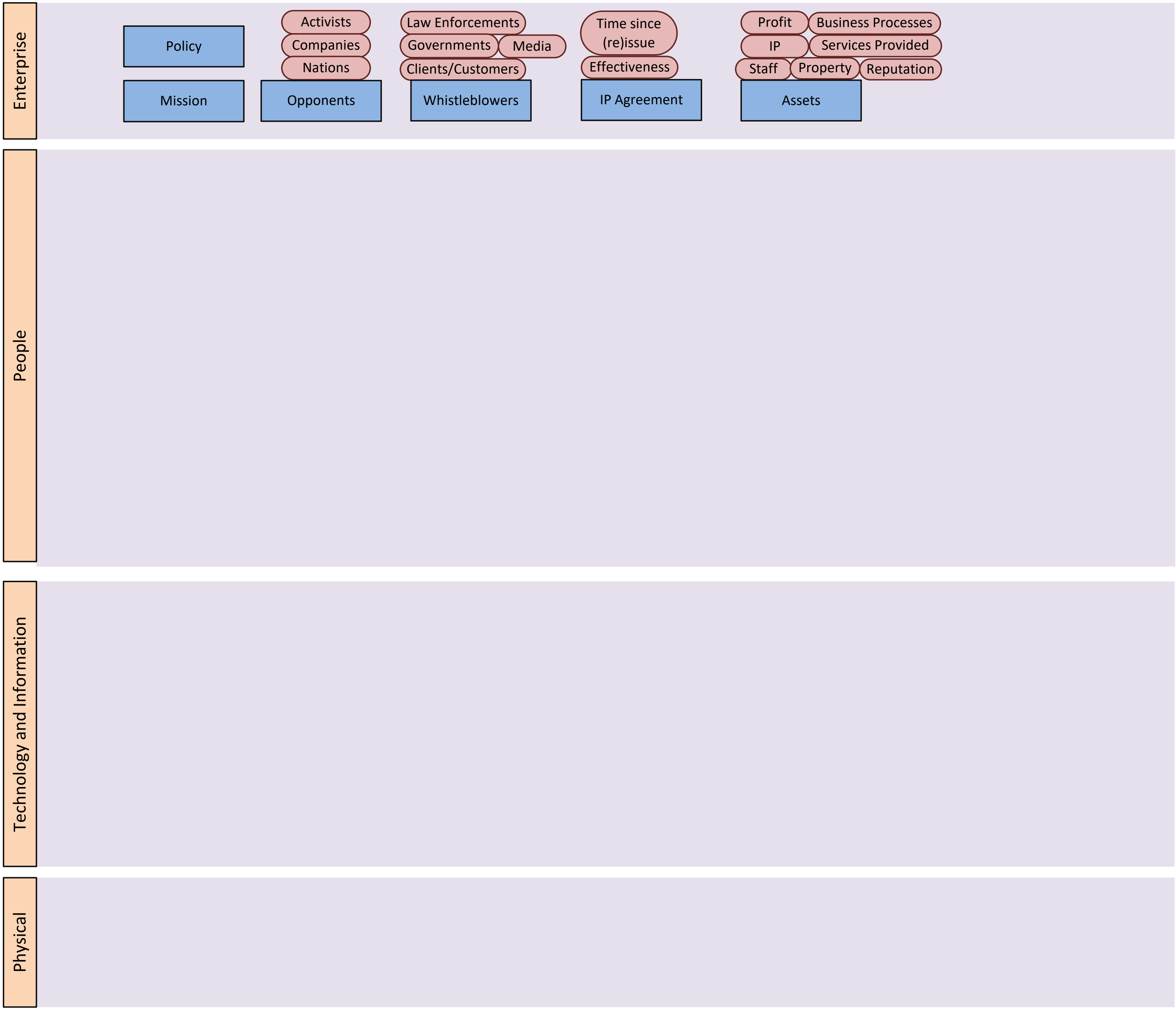


Enterprise

People

Technology and Information

Physical



Enterprise

Policy

Mission

Activists

Companies

Nations

Opponents

Law Enforcements

Governments

Media

Clients/Customers

Whistleblowers

Time since (re)issue

Effectiveness

IP Agreement

Profit

Business Processes

IP

Services Provided

Staff

Property

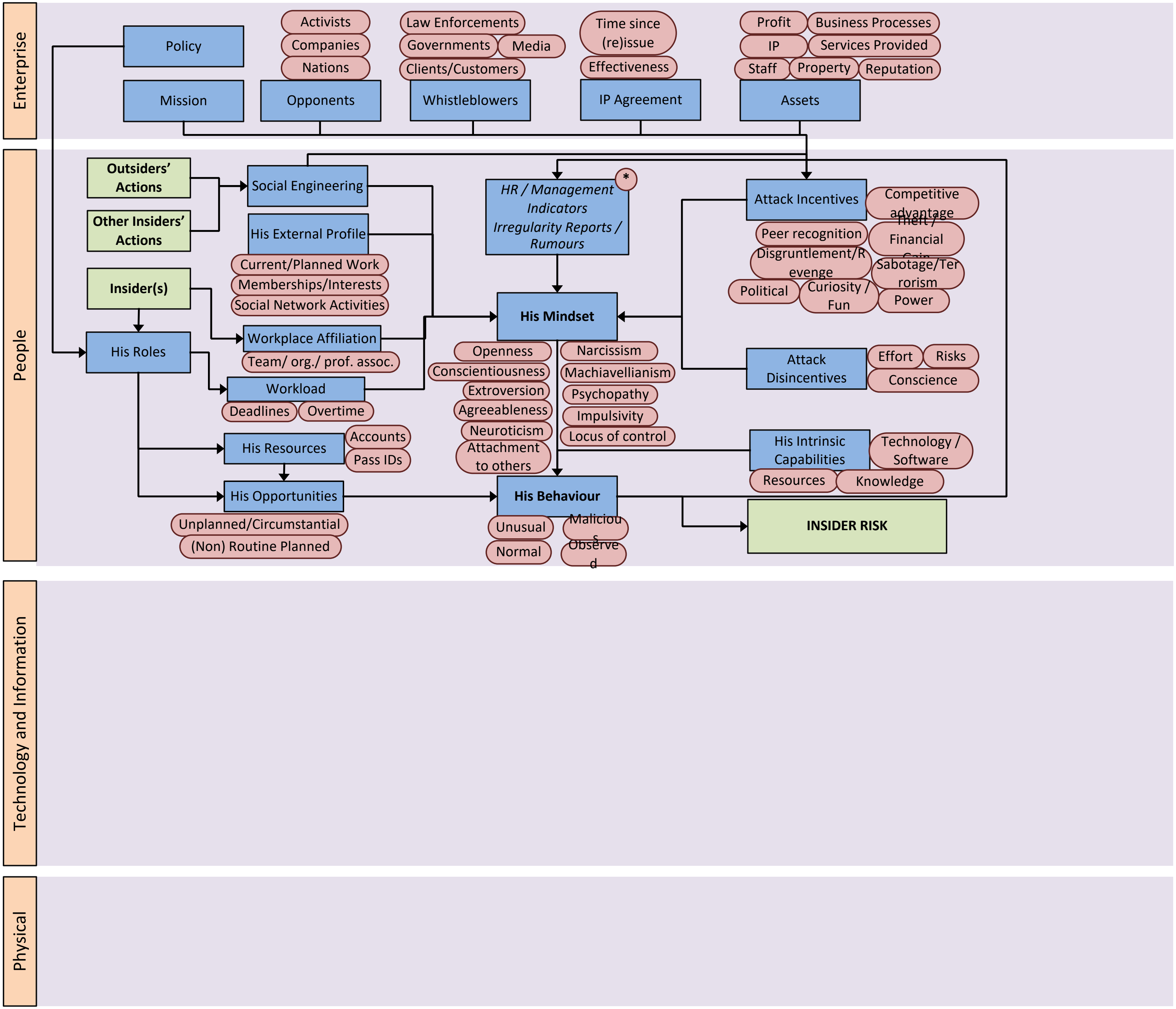
Reputation

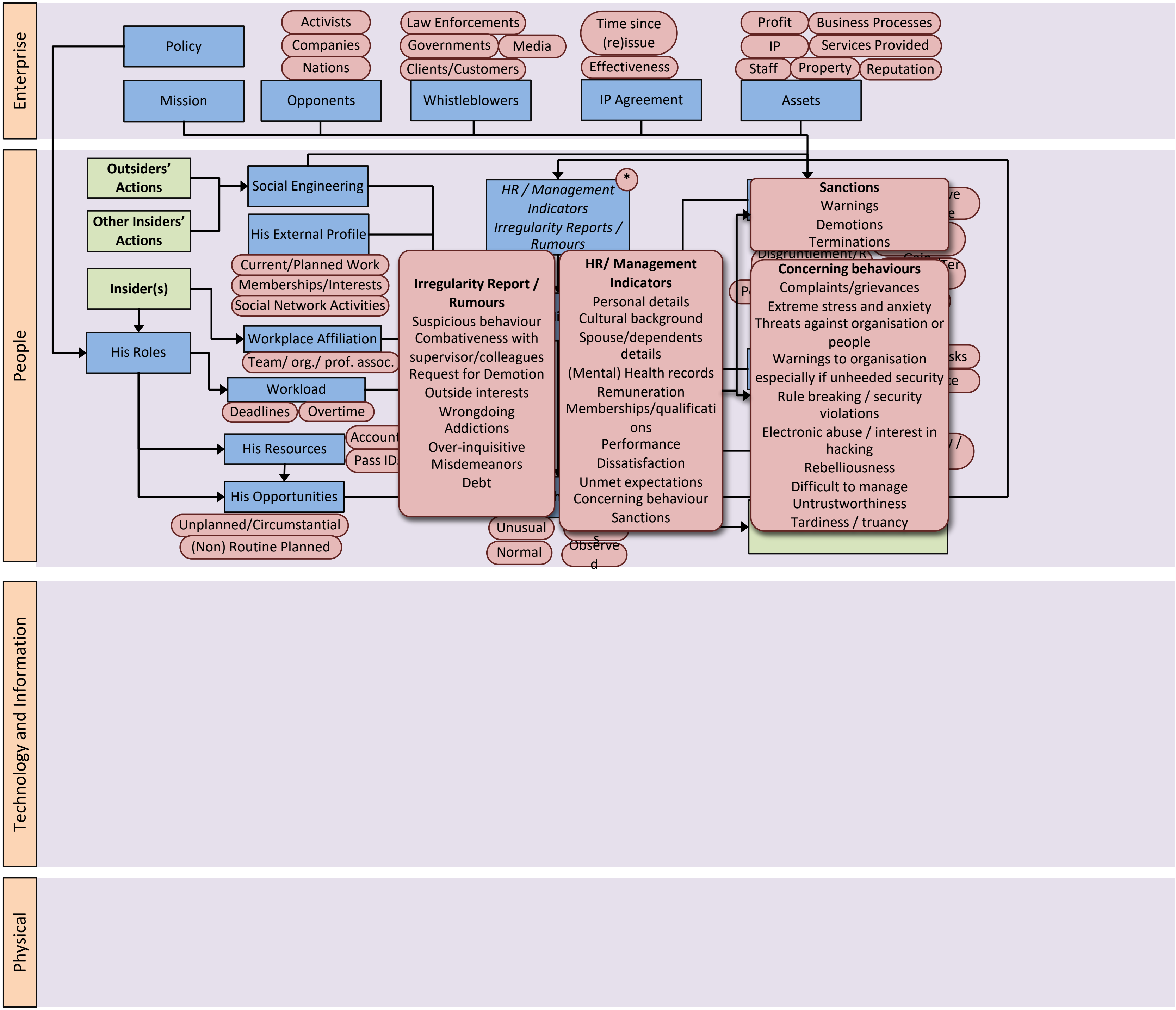
Assets

People

Technology and Information

Physical


Enterprise
People
Technology and Information
Physical
Policy
Mission
Activists
Companies
Nations
Opponents
Law Enforcements
Governments
Media
Clients/Customers
Whistleblowers
Time since (re)issue
Effectiveness
IP Agreement
Profit
Business Processes
IP
Services Provided
Staff
Property
Reputation
Assets
Outsiders' Actions
Other Insiders' Actions
Social Engineering
His External Profile
Current/Planned Work
Memberships/Interests
Social Network Activities
Insider(s)
His Roles
Workplace Affiliation
Team/ org./ prof. assoc.
Workload
Deadlines
Overtime
His Resources
Accounts
Pass IDs
His Opportunities
Unplanned/Circumstantial
(Non) Routine Planned
HR / Management Indicators Irregularity Reports / Rumours
*
His Mindset
Openness
Conscientiousness
Extroversion
Agreeableness
Neuroticism
Attachment to others
Narcissism
Machiavellianism
Psychopathy
Impulsivity
Locus of control
His Behaviour
Unusual
Normal
Maliciou s
Observe d
Attack Incentives
Competitive advantage
Peer recognition
Theft / Financial Gain
Disgruntlement/R evenge
Sabotage/Ter rorism
Political
Curiosity / Fun
Power
Attack Disincentives
Effort
Risks
Conscience
His Intrinsic Capabilities
Technology / Software
Resources
Knowledge
INSIDER RISK

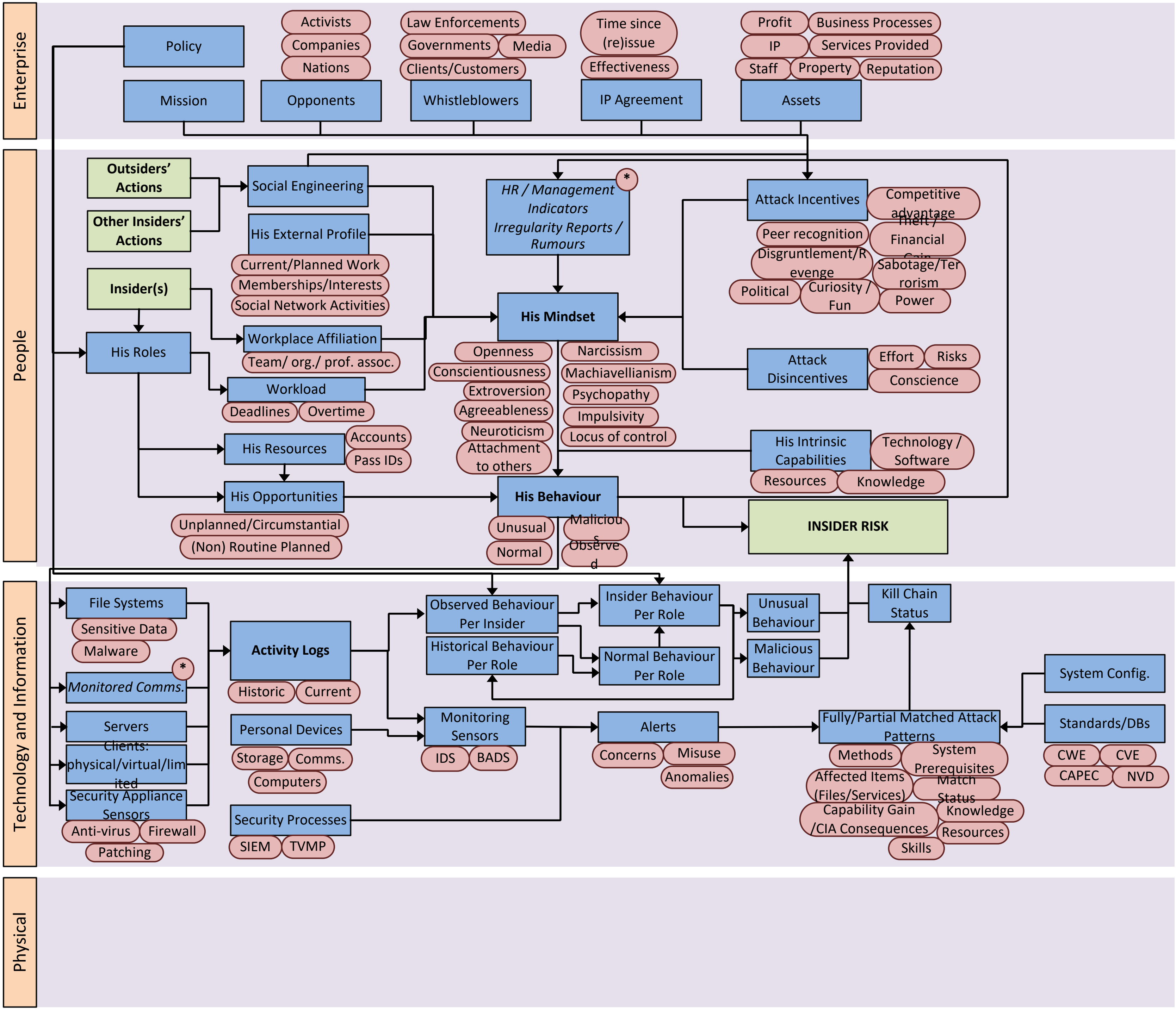


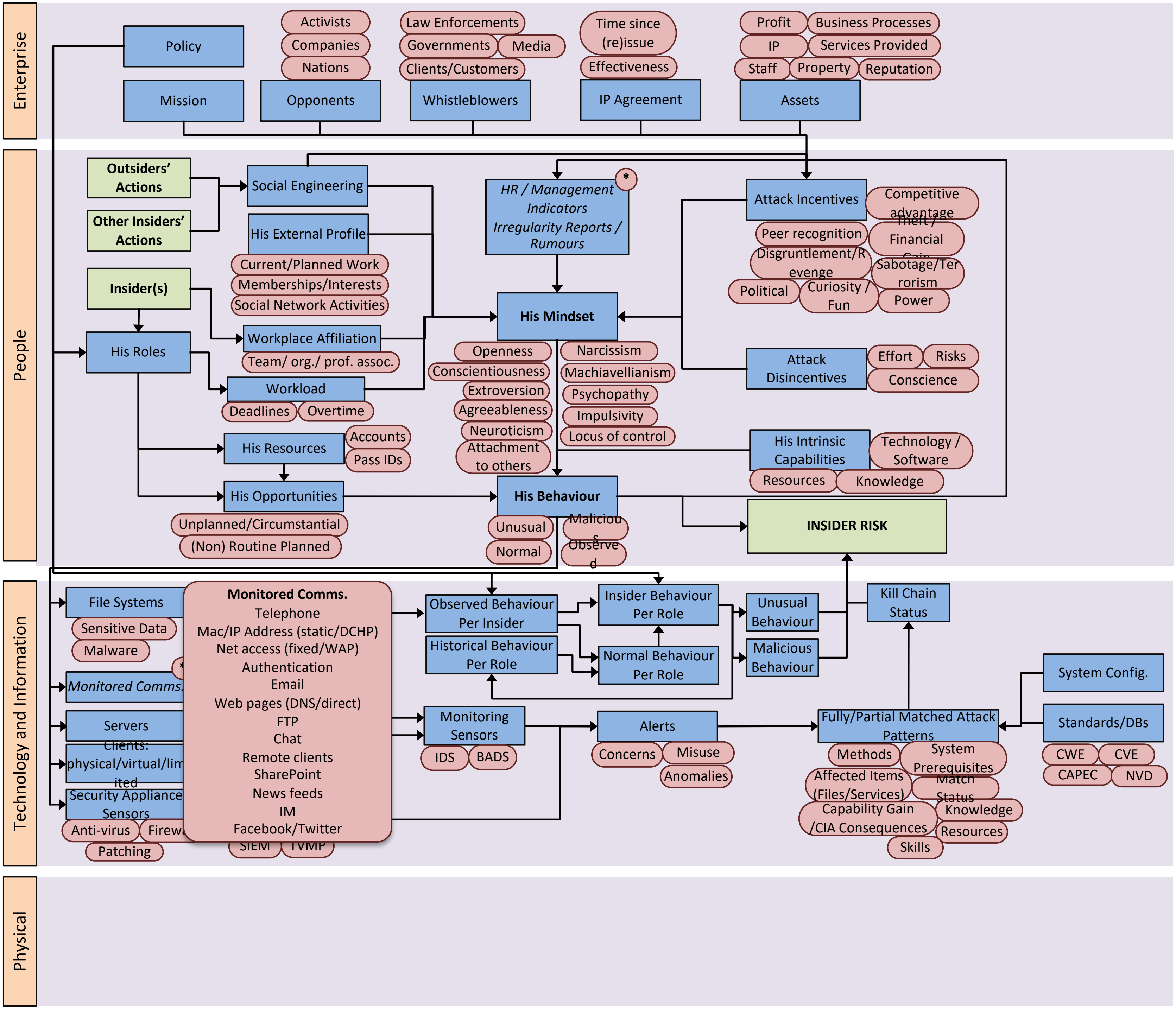
Irregularity Report / Rumours
Suspicious behaviour
Combativeness with supervisor/colleagues
Request for Demotion
Outside interests
Wrongdoing
Addictions
Over-inquisitive
Misdemeanors
Debt

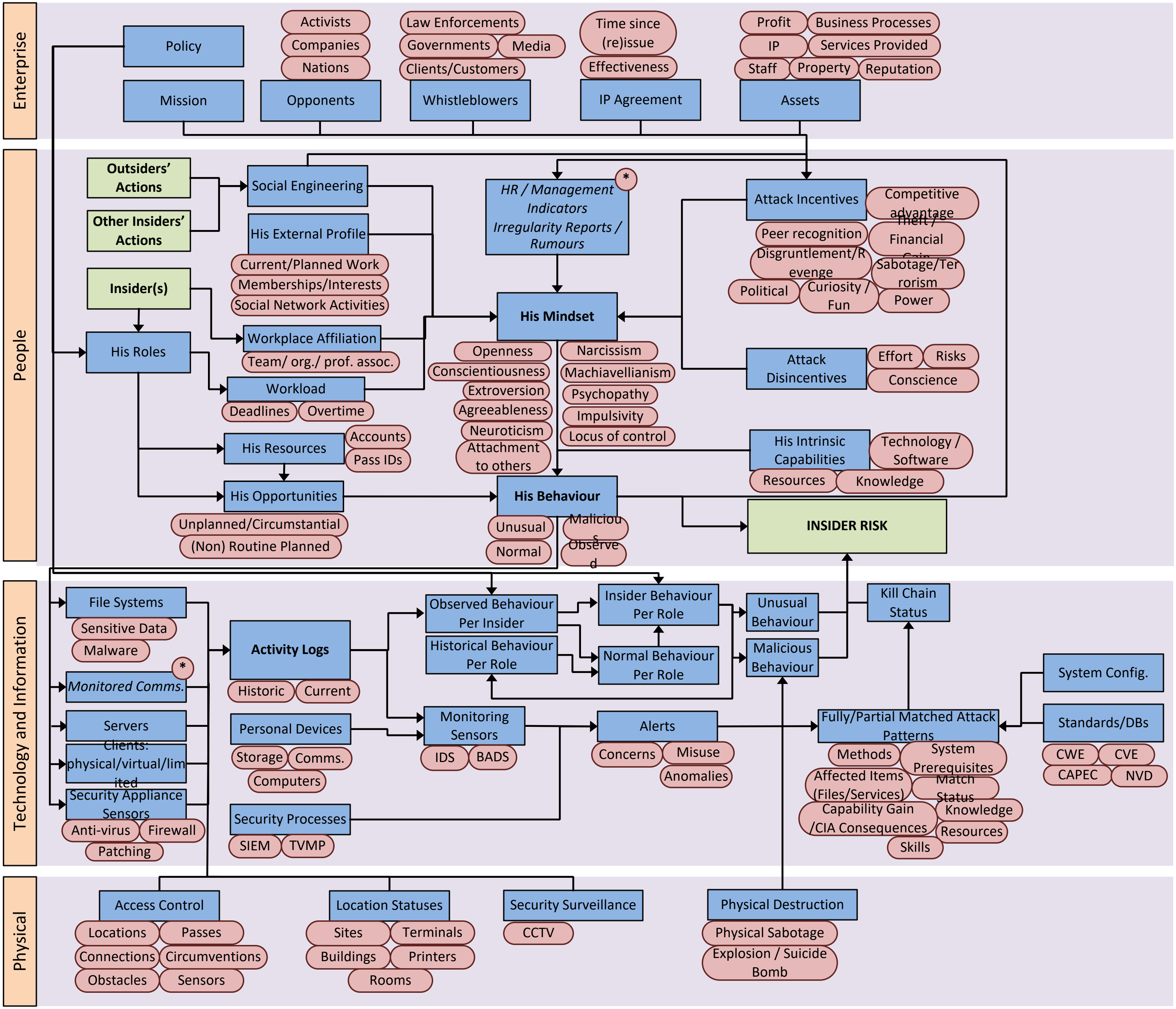
HR/ Management Indicators
Personal details
Cultural background
Spouse/dependents details
(Mental) Health records
Remuneration
Memberships/qualifications
Performance
Dissatisfaction
Unmet expectations
Concerning behaviour
Sanctions

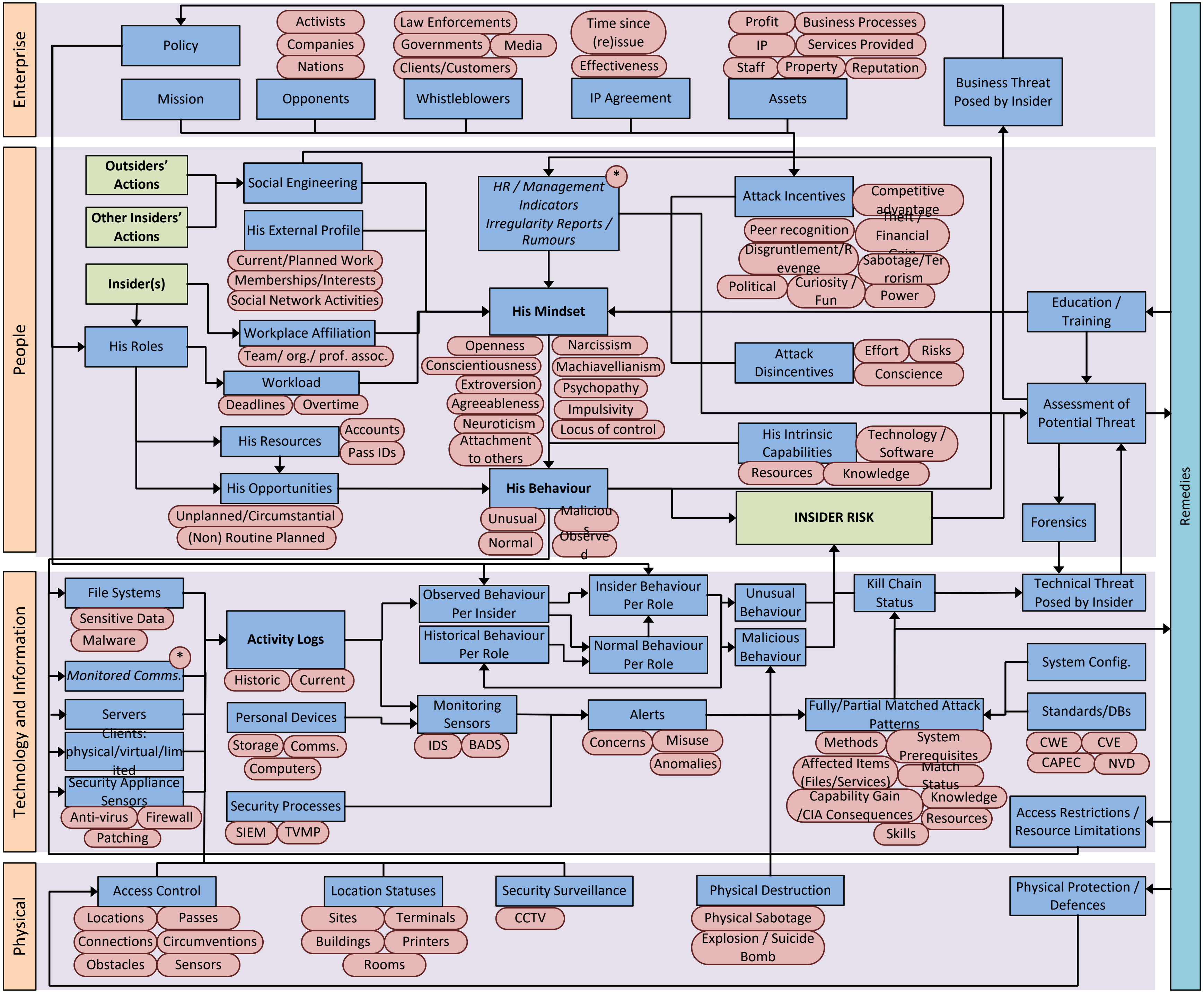
Sanctions
Warnings
Demotions
Terminations

Concerning behaviours
Complaints/grievances
Extreme stress and anxiety
Threats against organisation or people
Warnings to organisation especially if unheeded security
Rule breaking / security violations
Electronic abuse / interest in hacking
Rebelliousness
Difficult to manage
Untrustworthiness
Tardiness / truancy


Enterprise
Policy
Mission
Activists
Companies
Nations
Opponents
Law Enforcements
Governments
Media
Clients/Customers
Whistleblowers
Time since (re)issue
Effectiveness
IP Agreement
Profit
Business Processes
IP
Services Provided
Staff
Property
Reputation
Assets
People
Outsiders' Actions
Other Insiders' Actions
Insider(s)
His Roles
Social Engineering
His External Profile
Current/Planned Work
Memberships/Interests
Social Network Activities
Workplace Affiliation
Team/ org./ prof. assoc.
Workload
Deadlines
Overtime
His Resources
Accounts
Pass IDs
His Opportunities
Unplanned/Circumstantial
(Non) Routine Planned
HR / Management Indicators Irregularity Reports / Rumours
*
His Mindset
Openness
Conscientiousness
Extroversion
Agreeableness
Neuroticism
Attachment to others
Narcissism
Machiavellianism
Psychopathy
Impulsivity
Locus of control
His Behaviour
Unusual
Normal
Malicious
Observed
Attack Incentives
Competitive advantage
Peer recognition
Theft / Financial Gain
Disgruntlement/Revenge
Sabotage/Terrorism
Political
Curiosity / Fun
Power
Attack Disincentives
Effort
Risks
Conscience
His Intrinsic Capabilities
Technology / Software
Resources
Knowledge
INSIDER RISK
Technology and Information
File Systems
Sensitive Data
Malware
Monitored Comms.
*
Servers
Clients: physical/virtual/limited
Security Appliance Sensors
Anti-virus
Firewall
Patching
Activity Logs
Historic
Current
Personal Devices
Storage
Comms.
Computers
Security Processes
SIEM
TVMP
Observed Behaviour Per Insider
Historical Behaviour Per Role
Insider Behaviour Per Role
Normal Behaviour Per Role
Unusual Behaviour
Malicious Behaviour
Kill Chain Status
Monitoring Sensors
IDS
BADS
Alerts
Concerns
Misuse
Anomalies
Fully/Partial Matched Attack Patterns
Methods
System Prerequisites
Affected Items (Files/Services)
Match Status
Capability Gain /CIA Consequences
Knowledge
Resources
Skills
System Config.
Standards/DBs
CWE
CVE
CAPEC
NVD
Physical


Enterprise
Policy
Mission
Activists
Companies
Nations
Opponents
Law Enforcements
Governments
Media
Clients/Customers
Whistleblowers
Time since (re)issue
Effectiveness
IP Agreement
Profit
Business Processes
IP
Services Provided
Staff
Property
Reputation
Assets
People
Outsiders' Actions
Other Insiders' Actions
Insider(s)
Social Engineering
His External Profile
Current/Planned Work
Memberships/Interests
Social Network Activities
Workplace Affiliation
Team/ org./ prof. assoc.
His Roles
Workload
Deadlines
Overtime
His Resources
Accounts
Pass IDs
His Opportunities
Unplanned/Circumstantial
(Non) Routine Planned
HR / Management Indicators Irregularity Reports / Rumours
*
His Mindset
Openness
Conscientiousness
Extroversion
Agreeableness
Neuroticism
Attachment to others
Narcissism
Machiavellianism
Psychopathy
Impulsivity
Locus of control
His Behaviour
Unusual
Normal
Malicious
Observed
Attack Incentives
Competitive advantage
Peer recognition
Theft / Financial Gain
Disgruntlement/Revenge
Sabotage/Terrorism
Political
Curiosity / Fun
Power
Attack Disincentives
Effort
Risks
Conscience
His Intrinsic Capabilities
Technology / Software
Resources
Knowledge
INSIDER RISK
Technology and Information
File Systems
Sensitive Data
Malware
Monitored Comms.
*
Servers
Clients: physical/virtual/limited
Security Appliance Sensors
Anti-virus
Firewall
Patching
SIEM
TVMP
Monitored Comms.
Telephone
Mac/IP Address (static/DCHP)
Net access (fixed/WAP)
Authentication
Email
Web pages (DNS/direct)
FTP
Chat
Remote clients
SharePoint
News feeds
IM
Facebook/Twitter
Observed Behaviour Per Insider
Historical Behaviour Per Role
Insider Behaviour Per Role
Normal Behaviour Per Role
Unusual Behaviour
Malicious Behaviour
Kill Chain Status
Monitoring Sensors
IDS
BADS
Alerts
Concerns
Misuse
Anomalies
Fully/Partial Matched Attack Patterns
Methods
System Prerequisites
Affected Items (Files/Services)
Match Status
Capability Gain /CIA Consequences
Knowledge
Resources
Skills
System Config.
Standards/DBs
CWE
CVE
CAPEC
NVD
Physical


Enterprise
Policy
Mission
Activists
Companies
Nations
Opponents
Law Enforcements
Governments
Media
Clients/Customers
Whistleblowers
Time since (re)issue
Effectiveness
IP Agreement
Profit
Business Processes
IP
Services Provided
Staff
Property
Reputation
Assets
People
Outsiders' Actions
Other Insiders' Actions
Insider(s)
His Roles
Social Engineering
His External Profile
Current/Planned Work
Memberships/Interests
Social Network Activities
Workplace Affiliation
Team/ org./ prof. assoc.
Workload
Deadlines
Overtime
His Resources
Accounts
Pass IDs
His Opportunities
Unplanned/Circumstantial
(Non) Routine Planned
*
HR / Management Indicators Irregularity Reports / Rumours
His Mindset
Openness
Conscientiousness
Extroversion
Agreeableness
Neuroticism
Attachment to others
Narcissism
Machiavellianism
Psychopathy
Impulsivity
Locus of control
His Behaviour
Unusual
Normal
Malicious
Observed
Attack Incentives
Competitive advantage
Peer recognition
Theft / Financial Gain
Disgruntlement/Revenge
Sabotage/Terrorism
Political
Curiosity / Fun
Power
Attack Disincentives
Effort
Risks
Conscience
His Intrinsic Capabilities
Technology / Software
Resources
Knowledge
INSIDER RISK
Technology and Information
File Systems
Sensitive Data
Malware
*
Monitored Comms.
Servers
Clients: physical/virtual/limited
Security Appliance Sensors
Anti-virus
Firewall
Patching
Activity Logs
Historic
Current
Personal Devices
Storage
Comms.
Computers
Security Processes
SIEM
TVMP
Observed Behaviour Per Insider
Historical Behaviour Per Role
Insider Behaviour Per Role
Normal Behaviour Per Role
Monitoring Sensors
IDS
BADS
Alerts
Concerns
Misuse
Anomalies
Unusual Behaviour
Malicious Behaviour
Kill Chain Status
Fully/Partial Matched Attack Patterns
Methods
System Prerequisites
Affected Items (Files/Services)
Match Status
Capability Gain /CIA Consequences
Knowledge
Resources
Skills
System Config.
Standards/DBs
CWE
CVE
CAPEC
NVD
Physical
Access Control
Locations
Passes
Connections
Circumventions
Obstacles
Sensors
Location Statuses
Sites
Terminals
Buildings
Printers
Rooms
Security Surveillance
CCTV
Physical Destruction
Physical Sabotage
Explosion / Suicide Bomb


Enterprise
Policy
Mission
Activists
Companies
Nations
Opponents
Law Enforcements
Governments
Media
Clients/Customers
Whistleblowers
Time since (re)issue
Effectiveness
IP Agreement
Profit
Business Processes
IP
Services Provided
Staff
Property
Reputation
Assets
Business Threat Posed by Insider
People
Outsiders' Actions
Other Insiders' Actions
Insider(s)
His Roles
Social Engineering
His External Profile
Current/Planned Work
Memberships/Interests
Social Network Activities
Workplace Affiliation
Team/ org./ prof. assoc.
Workload
Deadlines
Overtime
His Resources
Accounts
Pass IDs
His Opportunities
Unplanned/Circumstantial
(Non) Routine Planned
*
HR / Management Indicators
Irregularity Reports / Rumours
His Mindset
Openness
Conscientiousness
Extroversion
Agreeableness
Neuroticism
Attachment to others
Narcissism
Machiavellianism
Psychopathy
Impulsivity
Locus of control
His Behaviour
Unusual
Normal
Malicious
Observed
Attack Incentives
Competitive advantage
Peer recognition
Theft / Financial Gain
Disgruntlement/Revenge
Sabotage/Terrorism
Political
Curiosity / Fun
Power
Attack Disincentives
Effort
Risks
Conscience
His Intrinsic Capabilities
Technology / Software
Resources
Knowledge
INSIDER RISK
Education / Training
Assessment of Potential Threat
Forensics
Technology and Information
File Systems
Sensitive Data
Malware
*
Monitored Comms.
Servers
Clients: physical/virtual/limited
Security Appliance Sensors
Anti-virus
Firewall
Patching
Activity Logs
Historic
Current
Personal Devices
Storage
Comms.
Computers
Security Processes
SIEM
TVMP
Observed Behaviour Per Insider
Historical Behaviour Per Role
Insider Behaviour Per Role
Normal Behaviour Per Role
Monitoring Sensors
IDS
BADS
Alerts
Concerns
Misuse
Anomalies
Unusual Behaviour
Malicious Behaviour
Kill Chain Status
Technical Threat Posed by Insider
Fully/Partial Matched Attack Patterns
Methods
System Prerequisites
Affected Items (Files/Services)
Match Status
Capability Gain /CIA Consequences
Knowledge
Resources
Skills
System Config.
Standards/DBs
CWE
CVE
CAPEC
NVD
Access Restrictions / Resource Limitations
Physical
Access Control
Locations
Passes
Connections
Circumventions
Obstacles
Sensors
Location Statuses
Sites
Terminals
Buildings
Printers
Rooms
Security Surveillance
CCTV
Physical Destruction
Physical Sabotage
Explosion / Suicide Bomb
Physical Protection / Defences
Remedies

UNIVERSITY OF OXFORD

CYBER SECURITY CENTRE

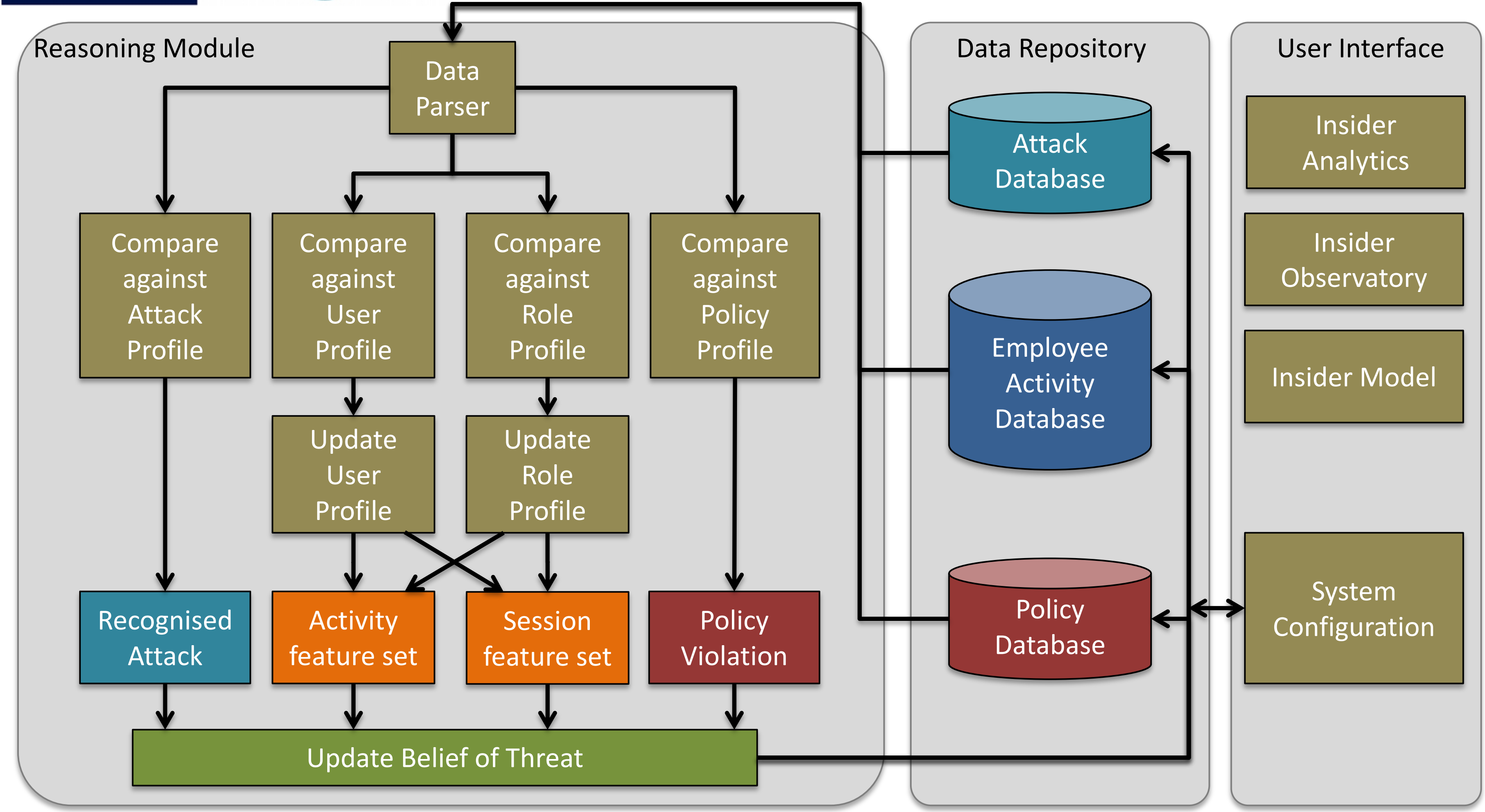
Construction of the Detection Prototype

INSIDERTHREAT

Construction of the Detection Prototype

- IDS-inspired architecture: sensors/monitors, databases, data mining and attack correlation, visual analytics.
- Alert for both anomaly detection and misuse: learning algorithms to understand normal behaviour combined with data mining to find events (single and chained) in large datasets.
- Connection between detection algorithms and visual analytics interface to support semi-supervised learning.
- Exploration of performance for subsets of data, attack sensor sources and system configrations.
- Validation via experimentation.

Current Architecture

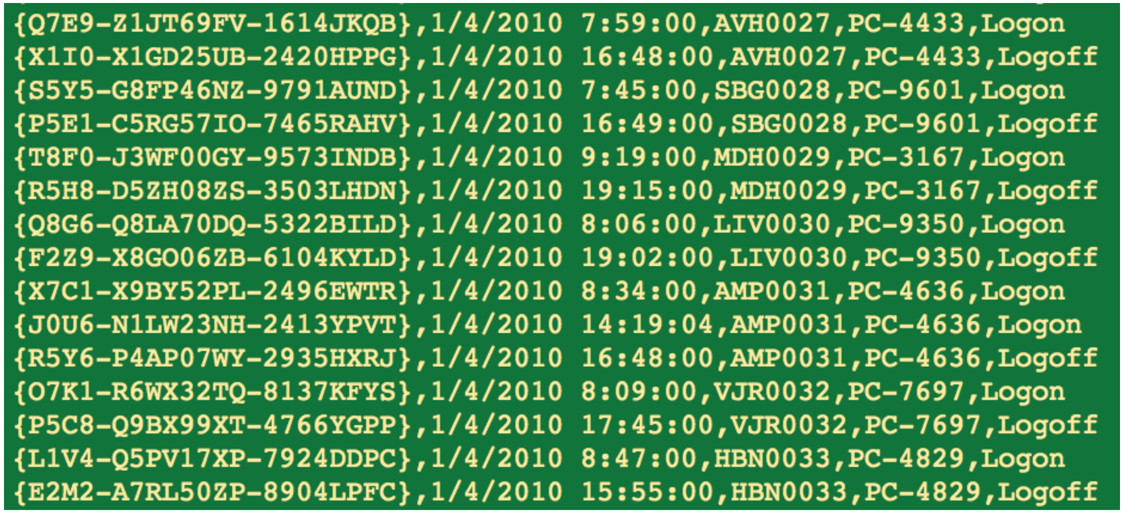


Our approach

- A probabilistic, generative model of user behaviour.
  - Models the activities that the user performs, the associated attributes with these activities, the time activities are performed and how frenquent these activities are performed.

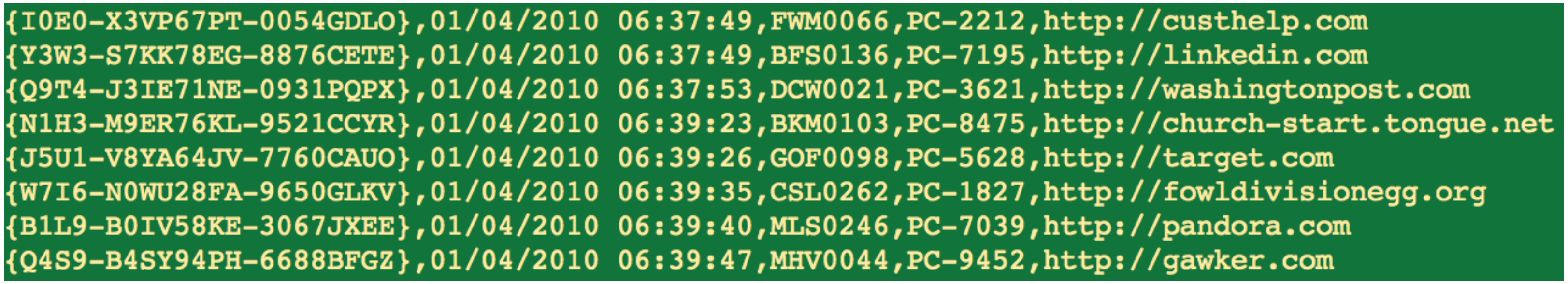
- Unsupervised – we do not assume in advance what defines anomaly behaviour, or threatening behaviour.
- Online – the system learns the user profile in real-time as new data is observed.

Test Data

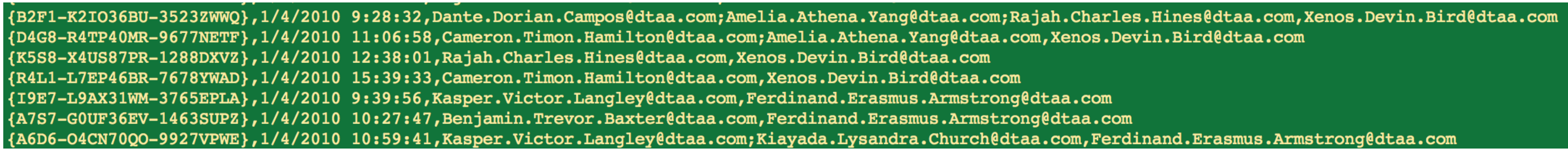


```
{Q7E9-Z1JT69FV-1614JKQB},1/4/2010 7:59:00,AVH0027,PC-4433,Logon
{X1I0-X1GD25UB-2420HPPG},1/4/2010 16:48:00,AVH0027,PC-4433,Logoff
{S5Y5-G8FP46NZ-9791AUND},1/4/2010 7:45:00,SBG0028,PC-9601,Logon
{P5E1-C5RG57IO-7465RAHV},1/4/2010 16:49:00,SBG0028,PC-9601,Logoff
{T8F0-J3WF00GY-9573INDB},1/4/2010 9:19:00,MDH0029,PC-3167,Logon
{R5H8-D5ZH08ZS-3503LHDN},1/4/2010 19:15:00,MDH0029,PC-3167,Logoff
{Q8G6-Q8LA70DQ-5322BILD},1/4/2010 8:06:00,LIV0030,PC-9350,Logon
{F2Z9-X8GO06ZB-6104KYLD},1/4/2010 19:02:00,LIV0030,PC-9350,Logoff
{X7C1-X9BY52PL-2496EWTR},1/4/2010 8:34:00,AMP0031,PC-4636,Logon
{J0U6-N1LW23NH-2413YPVT},1/4/2010 14:19:04,AMP0031,PC-4636,Logon
{R5Y6-P4AP07WY-2935HXRJ},1/4/2010 16:48:00,AMP0031,PC-4636,Logoff
{O7K1-R6WX32TQ-8137KFYS},1/4/2010 8:09:00,VJR0032,PC-7697,Logon
{P5C8-Q9BX99XT-4766YGPP},1/4/2010 17:45:00,VJR0032,PC-7697,Logoff
{L1V4-Q5PV17XP-7924DDPC},1/4/2010 8:47:00,HBN0033,PC-4829,Logon
{E2M2-A7RL50ZP-8904LPFC},1/4/2010 15:55:00,HBN0033,PC-4829,Logoff
```

- Logon, USB Device, E-mail, Web, File activity logs.
- Could also introduce additional logs (physical access, ftp, ssh, application usage).



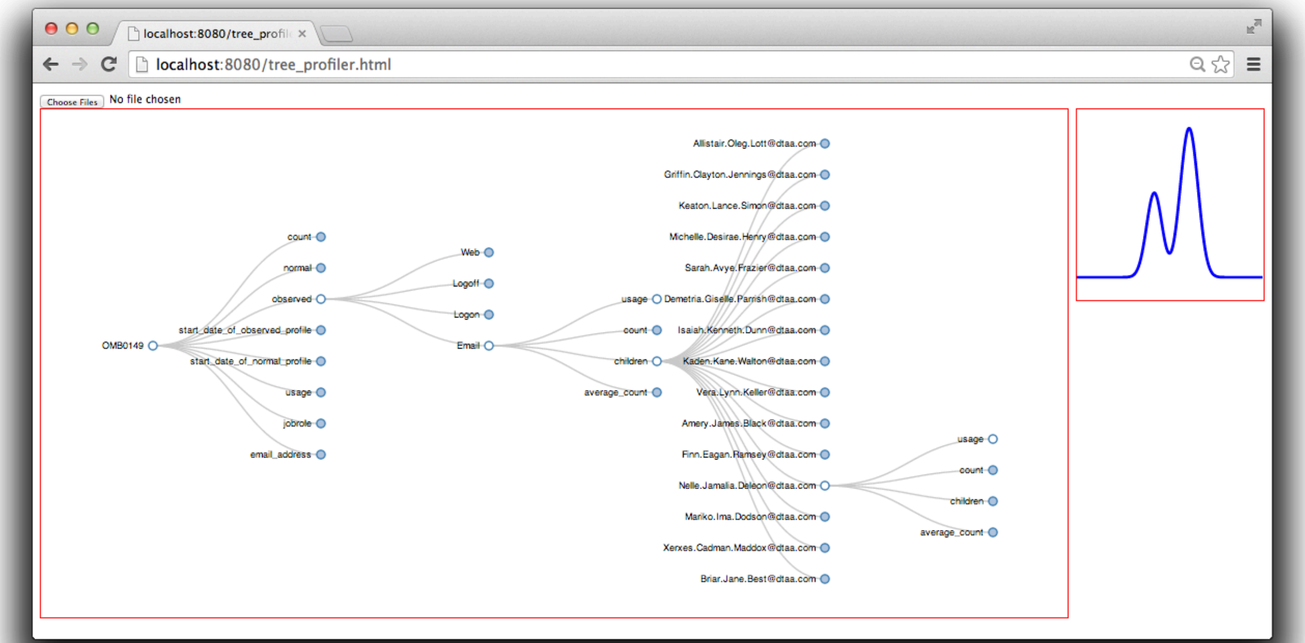
```
{I0E0-X3VP67PT-0054GDLO},01/04/2010 06:37:49,FWM0066,PC-2212,http://custhelp.com
{Y3W3-S7KK78EG-8876CETE},01/04/2010 06:37:49,BFS0136,PC-7195,http://linkedin.com
{Q9T4-J3IE71NE-0931PQPX},01/04/2010 06:37:53,DCW0021,PC-3621,http://washingtonpost.com
{N1H3-M9ER76KL-9521CCYR},01/04/2010 06:39:23,BKM0103,PC-8475,http://church-start.tongue.net
{J5U1-V8YA64JV-7760CAUO},01/04/2010 06:39:26,GOF0098,PC-5628,http://target.com
{W7I6-N0WU28FA-9650GLKV},01/04/2010 06:39:35,CSL0262,PC-1827,http://fowldivisionegg.org
{B1L9-B0IV58KE-3067JXEE},01/04/2010 06:39:40,MLS0246,PC-7039,http://pandora.com
{Q4S9-B4SY94PH-6688BFGZ},01/04/2010 06:39:47,MHV0044,PC-9452,http://gawker.com
```



```
{B2F1-K2IO36BU-3523ZWWQ},1/4/2010 9:28:32,Dante.Dorian.Campos@dtaa.com;Amelia.Athena.Yang@dtaa.com;Rajah.Charles.Hines@dtaa.com,Xenos.Devin.Bird@dtaa.com
{D4G8-R4TP40MR-9677NETF},1/4/2010 11:06:58,Cameron.Timon.Hamilton@dtaa.com;Amelia.Athena.Yang@dtaa.com,Xenos.Devin.Bird@dtaa.com
{K5S8-X4US87PR-1288DXVZ},1/4/2010 12:38:01,Rajah.Charles.Hines@dtaa.com,Xenos.Devin.Bird@dtaa.com
{R4L1-L7EP46BR-7678YWAD},1/4/2010 15:39:33,Cameron.Timon.Hamilton@dtaa.com,Xenos.Devin.Bird@dtaa.com
{I9E7-L9AX31WM-3765EPLA},1/4/2010 9:39:56,Kasper.Victor.Langley@dtaa.com,Ferdinand.Erasmus.Armstrong@dtaa.com
{A7S7-G0UF36EV-1463SUPZ},1/4/2010 10:27:47,Benjamin.Trevor.Baxter@dtaa.com,Ferdinand.Erasmus.Armstrong@dtaa.com
{A6D6-O4CN70QO-9927VPWE},1/4/2010 10:59:41,Kasper.Victor.Langley@dtaa.com;Kiayada.Lysandra.Church@dtaa.com,Ferdinand.Erasmus.Armstrong@dtaa.com
```

Statistical Profiling

- Statistical profiling of employee behaviour.
  - Normal vs current
  - Individual, role, organisation
- Measure deviation from typical/normal usage.
  - Unusual logins, increase in emails/web browsing, new contacts, access of new server files… etc.

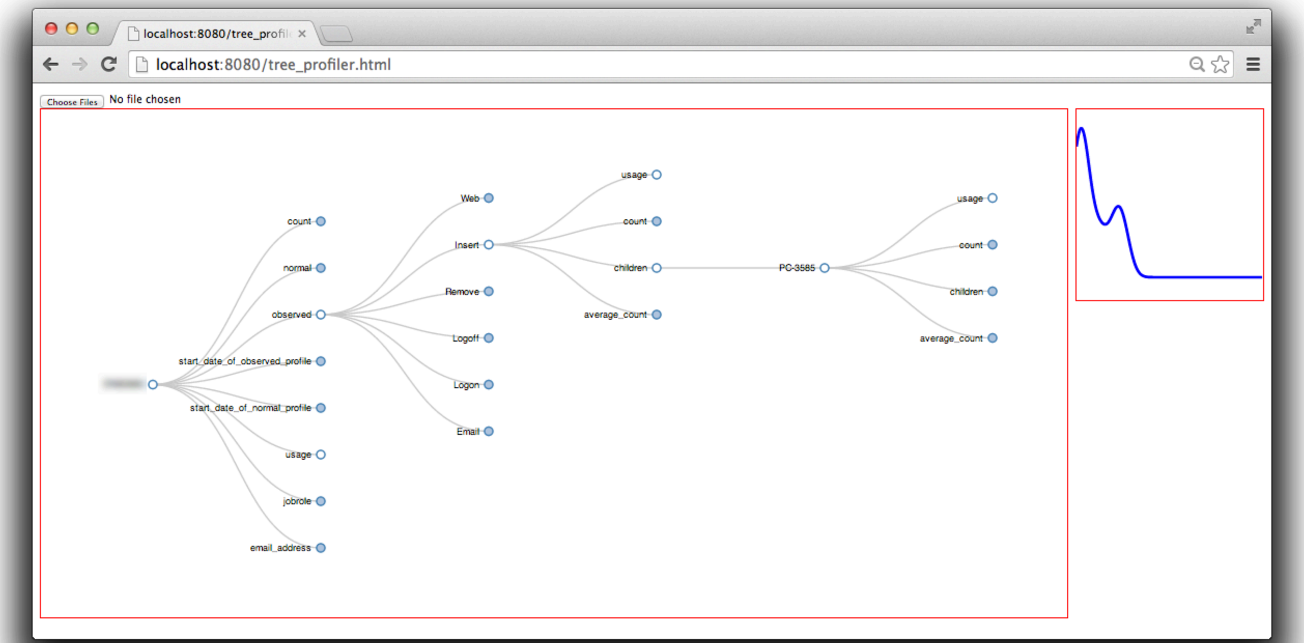

localhost:8080/tree_profil
localhost:8080/tree_profiler.html
Choose Files
No file chosen
OMB0149
count
normal
observed
start_date_of_observed_profile
start_date_of_normal_profile
usage
jobrole
email_address
Web
Logoff
Logon
Email
usage
count
children
average_count
Allistair.Oleg.Lott@dtaa.com
Griffin.Clayton.Jennings@dtaa.com
Keaton.Lance.Simon@dtaa.com
Michelle.Desirae.Henry@dtaa.com
Sarah.Avye.Frazier@dtaa.com
Demetria.Giselle.Parrish@dtaa.com
Isaiah.Kenneth.Dunn@dtaa.com
Kaden.Kane.Walton@dtaa.com
Vera.Lynn.Keller@dtaa.com
Amery.James.Black@dtaa.com
Finn.Eagan.Ramsey@dtaa.com
Nelle.Jamalia.Deleon@dtaa.com
Mariko.Ima.Dodson@dtaa.com
Xerxes.Cadman.Maddox@dtaa.com
Briar.Jane.Best@dtaa.com
usage
count
children
average_count

Employee monitoring that does not show deviating behaviour

Statistical Profiling

- Statistical profiling of employee behaviour.
  - Normal vs current
  - Individual, role, organisation

- Measure deviation from typical/normal usage.
  - Unusual logins, increase in emails/web browsing, new contacts, access of new server files… etc.



Employee monitoring that shows suspicious device usage

Digging deep in data

- Some activities will also carry *content* that should be incorporated into an employee profile.
  - *Email message, web site content, file content.*

- Whilst not essential for the system, this information would provide greater context to an employee's mindset.
  - What do web browsing habits suggest about an employee?
  - If a file has been modified, what *exactly* has been modified?
  - What does the sentiment of their e-mails suggest about an employee?

- Opens up issues surrounding employee privacy – organisation to decide on level of desired monitoring.

Profile Metrics

Technical metrics:

#logins
login duration
#unique_logins
earliest_login
latest_login

#usb_insertions
#unique_usb_insertions
#usb_upload_MB
#usb_download_MB

#emails_received
#unique_senders
#new_senders

#emails_sent
#unique_recipients
#new_recipients
earliest_email_sent
latest_email_sent

#files_created
#files_accessed
#unique_files_accessed
#new_files_accessed
#files_modified
#unique_files_modified
#new_files_modified
#files_deleted

email_bag_of_words
files_bag_of_words
website_bag_of_words
email_sentiment

keyboard_biometrics
mouse_biometrics

#websites_visited
#unique_websites
#new_websites
browsing_duration

cpu_usage
memory_usage
network_upload
network_download
processes_running

Physical metrics:

#swipe_card_entries
earliest_swipe_entry
latest_swipe_entry
#keypad_entries
#keyfob_entries

CCTV monitoring

Workstation location
IP address

Activity metrics:

user_new_activity
user_new_attribute
user_time_activity
user_time_attribute
user_count_activity
user_count_attribute
role_new_activity
role_new_attribute
role_time_activity
role_time_attribute
role_count_activity
role_count_attribute

Behavioural metrics:

Openness
Conscientiousness
Extroversion
Agreeableness
Neuroticism

Narcissism
Machiavellianism
Psychopathy

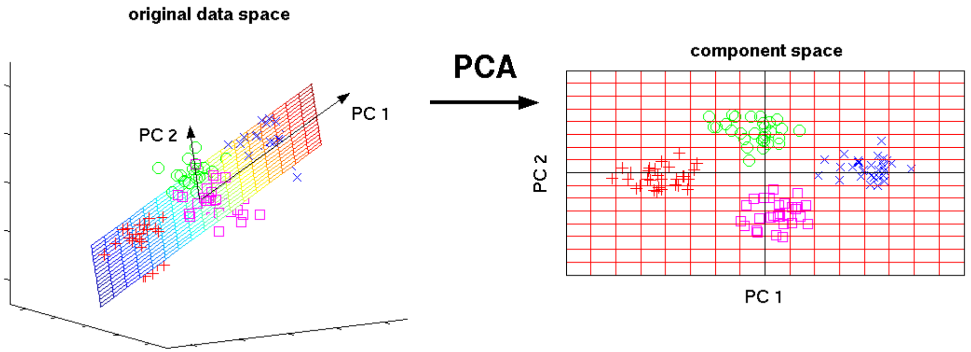
Workplace Affliation
Locus of Control
Attachment to others
Impulsivity

Disgruntlement
Not accepting feedback
Anger management issues
Disengagement
Disregard for Authority
Performance
Stress
Confrontational
Personal Issues
Self-Centeredness
Lack of Depandability
Absenteeism
(Greitzer et al. 2012)

...more to be established with Leicester

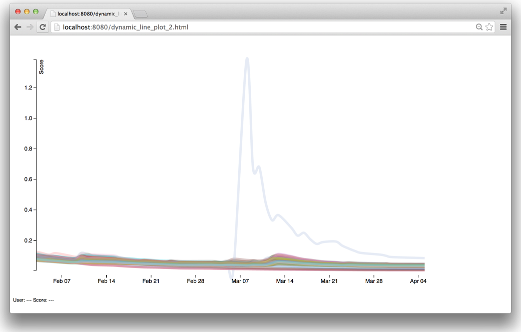
- Two forms of metric to consider:
  - Daily-based metrics
  - Activity-based metrics

Anomaly Detection

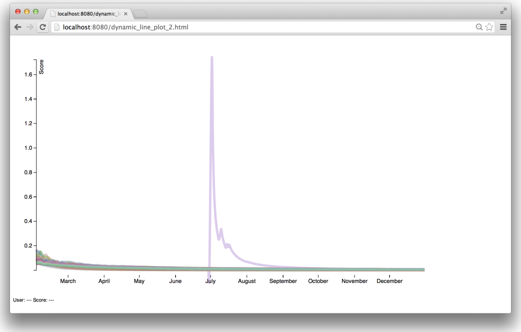


- Principal Component Analysis
  - Reduces n-D features to $< \boldsymbol{n}$ components based on variance.
  - A user with a suddenly-large variance could indicate an anomaly.
- Requires a consistent n-D feature set for comparison
  - e.g., login count, USB count, email count, file count.
  - Can include time-based features (e.g., mean, earliest, latest…)
  - Can also include ‘new’ accesses from user profile.
  - Suitable for daily- or session-based profiling.

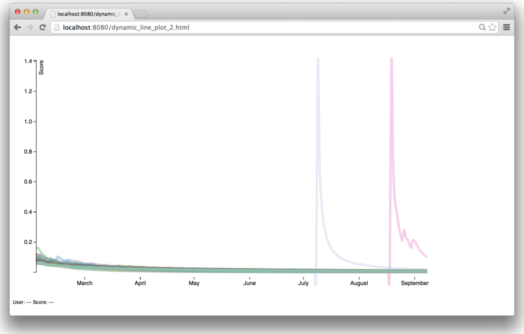
Anomaly Detection



User: --- Score: ---



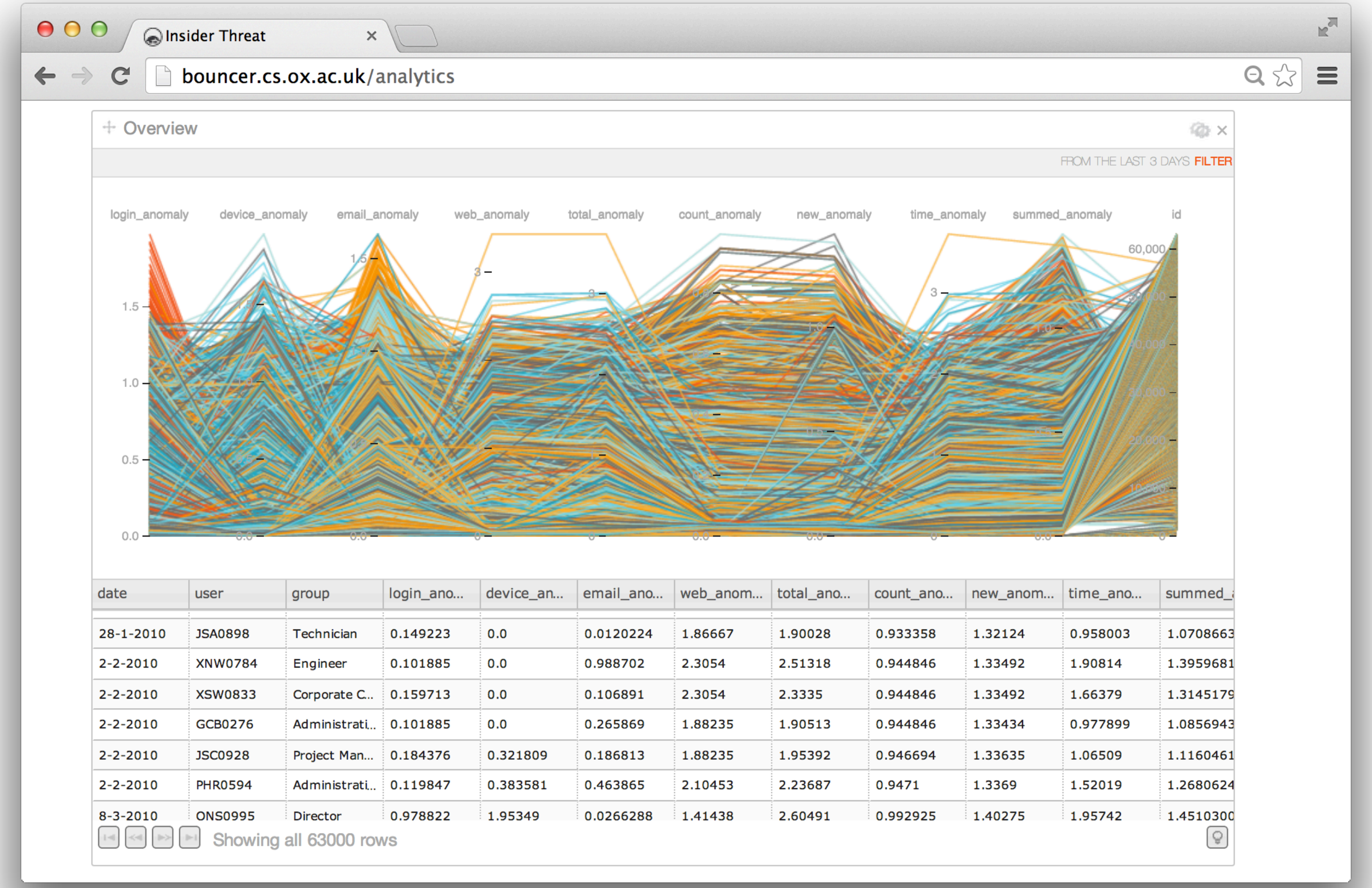
User: --- Score: ---



User: --- Score: ---

- Measurements are gathered from the employee profile data.
- Suspicious behaviour is likely to provoke an anomaly on one or more measurement.
- These provide a means to reason about the threat posed by a particular individual.

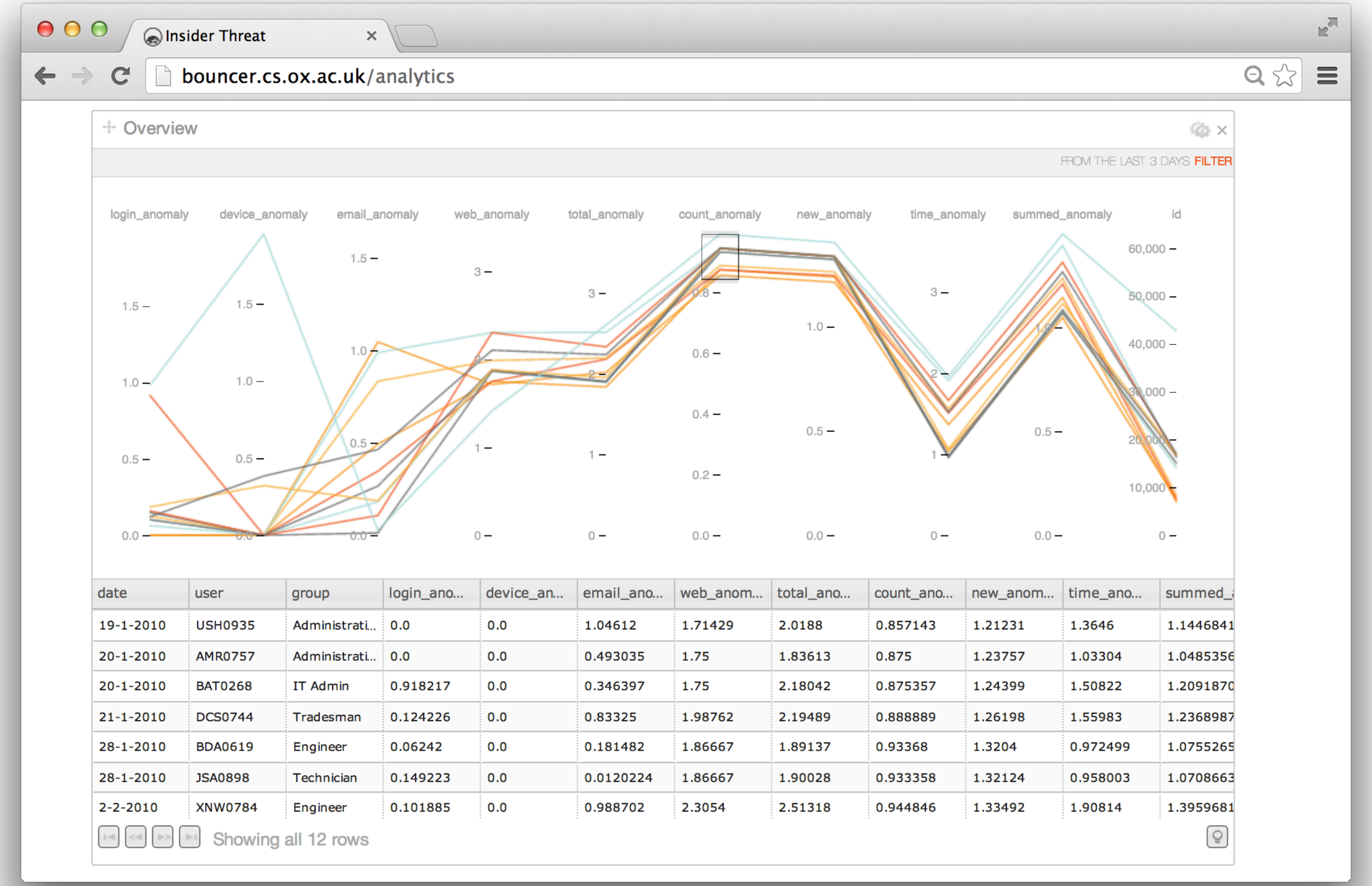
Analysis of Detection Results



date	user	group	login_ano...	device_an...	email_ano...	web_anom...	total_ano...	count_ano...	new_anom...	time_ano...	summed_
28-1-2010	JSA0898	Technician	0.149223	0.0	0.0120224	1.86667	1.90028	0.933358	1.32124	0.958003	1.0708663
2-2-2010	XNW0784	Engineer	0.101885	0.0	0.988702	2.3054	2.51318	0.944846	1.33492	1.90814	1.3959681
2-2-2010	XSW0833	Corporate C...	0.159713	0.0	0.106891	2.3054	2.3335	0.944846	1.33492	1.66379	1.3145179
2-2-2010	GCB0276	Administrati...	0.101885	0.0	0.265869	1.88235	1.90513	0.944846	1.33434	0.977899	1.0856943
2-2-2010	JSC0928	Project Man...	0.184376	0.321809	0.186813	1.88235	1.95392	0.946694	1.33635	1.06509	1.1160461
2-2-2010	PHR0594	Administrati...	0.119847	0.383581	0.463865	2.10453	2.23687	0.9471	1.3369	1.52019	1.2680624
8-3-2010	ONS0995	Director	0.978822	1.95349	0.0266288	1.41438	2.60491	0.992925	1.40275	1.95742	1.4510300

Showing all 63000 rows

Analysis of Detection Results



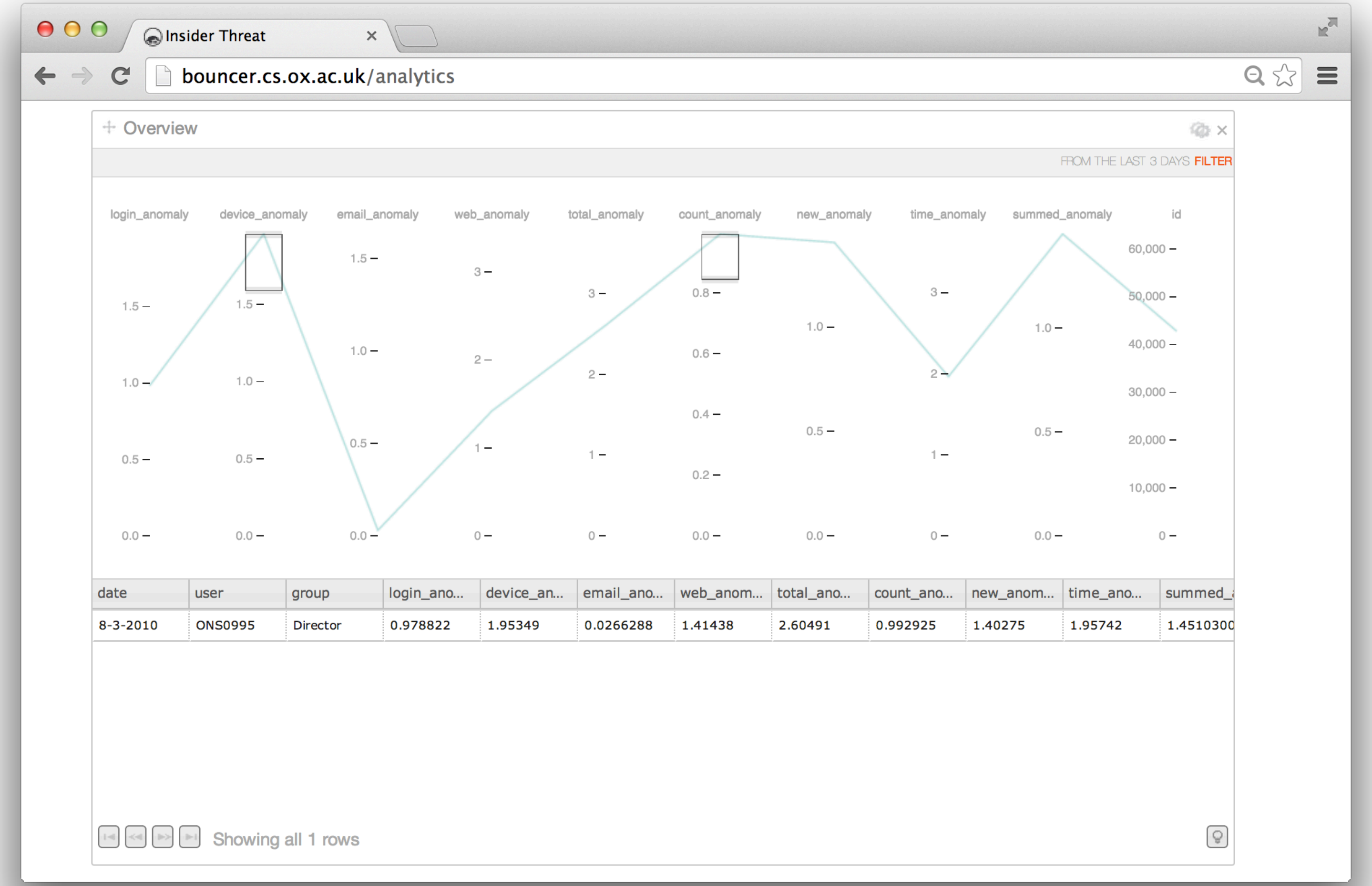
date	user	group	login_ano...	device_an...	email_ano...	web_anom...	total_ano...	count_ano...	new_anom...	time_ano...	summed_
19-1-2010	USH0935	Administrati...	0.0	0.0	1.04612	1.71429	2.0188	0.857143	1.21231	1.3646	1.1446841
20-1-2010	AMR0757	Administrati...	0.0	0.0	0.493035	1.75	1.83613	0.875	1.23757	1.03304	1.0485356
20-1-2010	BAT0268	IT Admin	0.918217	0.0	0.346397	1.75	2.18042	0.875357	1.24399	1.50822	1.2091870
21-1-2010	DCS0744	Tradesman	0.124226	0.0	0.83325	1.98762	2.19489	0.888889	1.26198	1.55983	1.2368987
28-1-2010	BDA0619	Engineer	0.06242	0.0	0.181482	1.86667	1.89137	0.93368	1.3204	0.972499	1.0755265
28-1-2010	JSA0898	Technician	0.149223	0.0	0.0120224	1.86667	1.90028	0.933358	1.32124	0.958003	1.0708663
2-2-2010	XNW0784	Engineer	0.101885	0.0	0.988702	2.3054	2.51318	0.944846	1.33492	1.90814	1.3959681

Showing all 12 rows

UNIVERSITY OF OXFORD

CYBER SECURITY CENTRE

Analysis of Detection Results



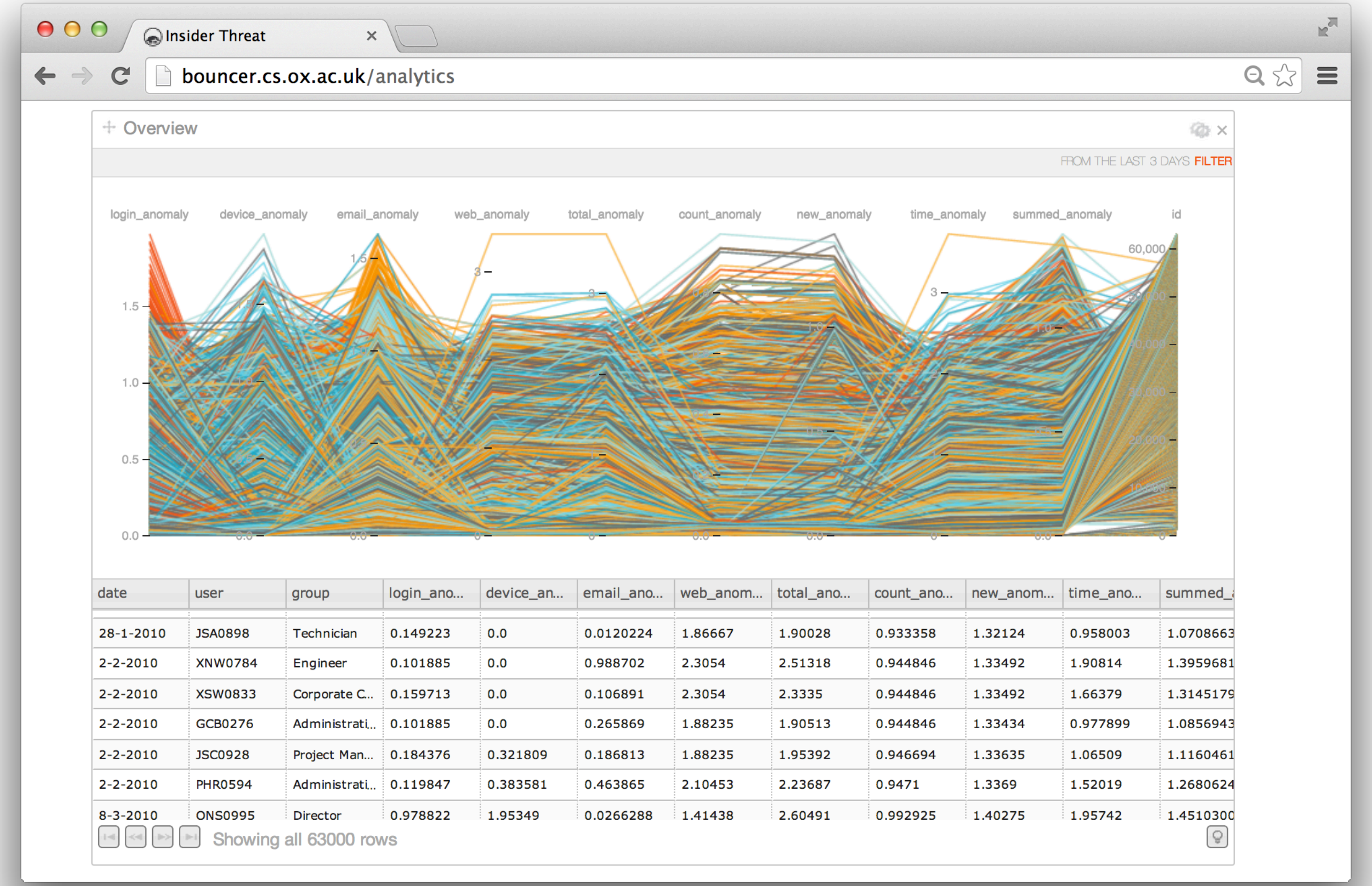
date	user	group	login_ano...	device_an...	email_ano...	web_anom...	total_ano...	count_ano...	new_anom...	time_ano...	summed_
8-3-2010	ONS0995	Director	0.978822	1.95349	0.0266288	1.41438	2.60491	0.992925	1.40275	1.95742	1.4510300

INSIDERTHREAT

UNIVERSITY OF OXFORD

CYBER SECURITY CENTRE

Analysis of Detection Results

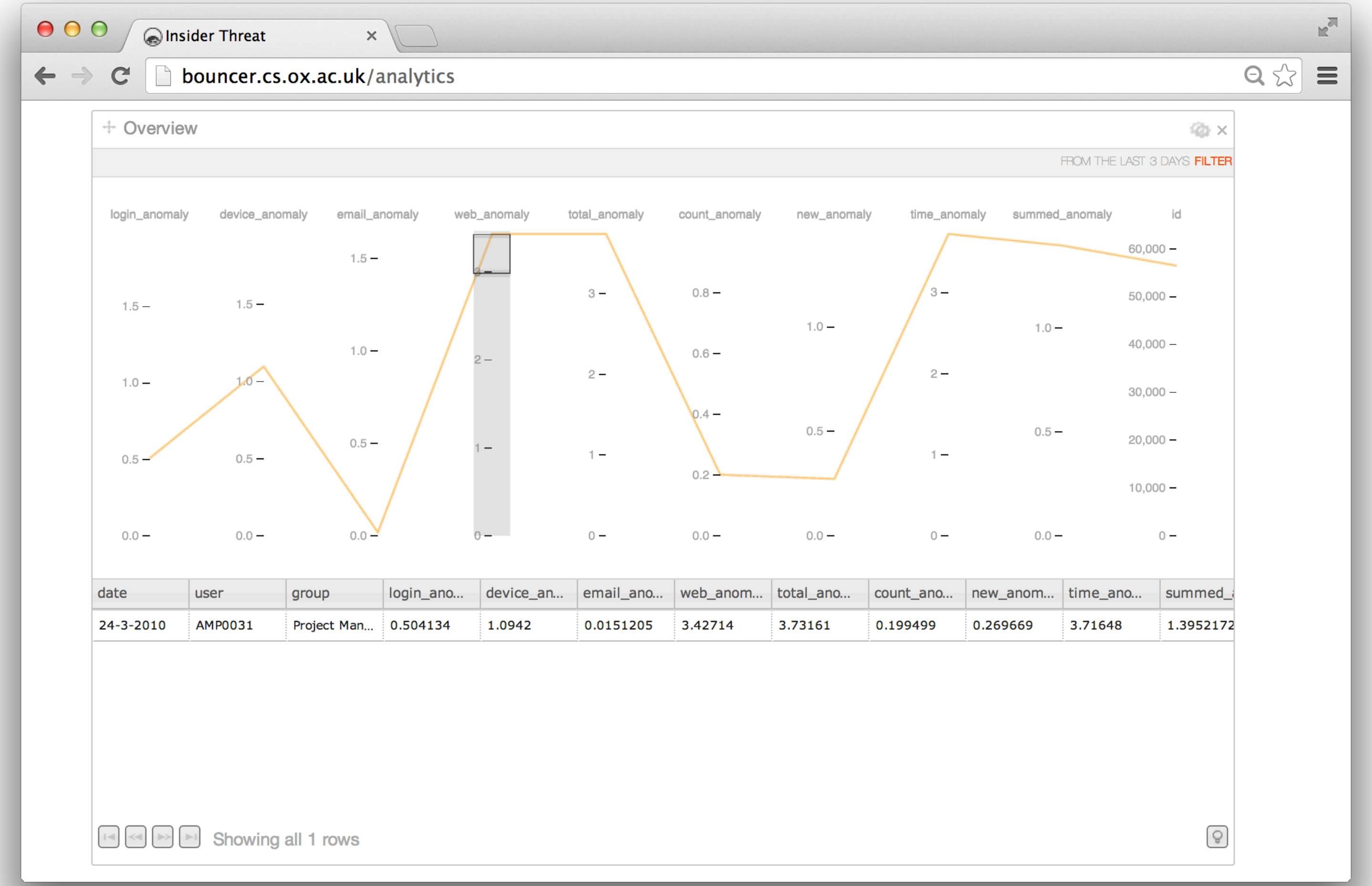


date	user	group	login_ano...	device_an...	email_ano...	web_anom...	total_ano...	count_ano...	new_anom...	time_ano...	summed_
28-1-2010	JSA0898	Technician	0.149223	0.0	0.0120224	1.86667	1.90028	0.933358	1.32124	0.958003	1.0708663
2-2-2010	XNW0784	Engineer	0.101885	0.0	0.988702	2.3054	2.51318	0.944846	1.33492	1.90814	1.3959681
2-2-2010	XSW0833	Corporate C...	0.159713	0.0	0.106891	2.3054	2.3335	0.944846	1.33492	1.66379	1.3145179
2-2-2010	GCB0276	Administrati...	0.101885	0.0	0.265869	1.88235	1.90513	0.944846	1.33434	0.977899	1.0856943
2-2-2010	JSC0928	Project Man...	0.184376	0.321809	0.186813	1.88235	1.95392	0.946694	1.33635	1.06509	1.1160461
2-2-2010	PHR0594	Administrati...	0.119847	0.383581	0.463865	2.10453	2.23687	0.9471	1.3369	1.52019	1.2680624
8-3-2010	ONS0995	Director	0.978822	1.95349	0.0266288	1.41438	2.60491	0.992925	1.40275	1.95742	1.4510300

Showing all 63000 rows

INSIDERTHREAT

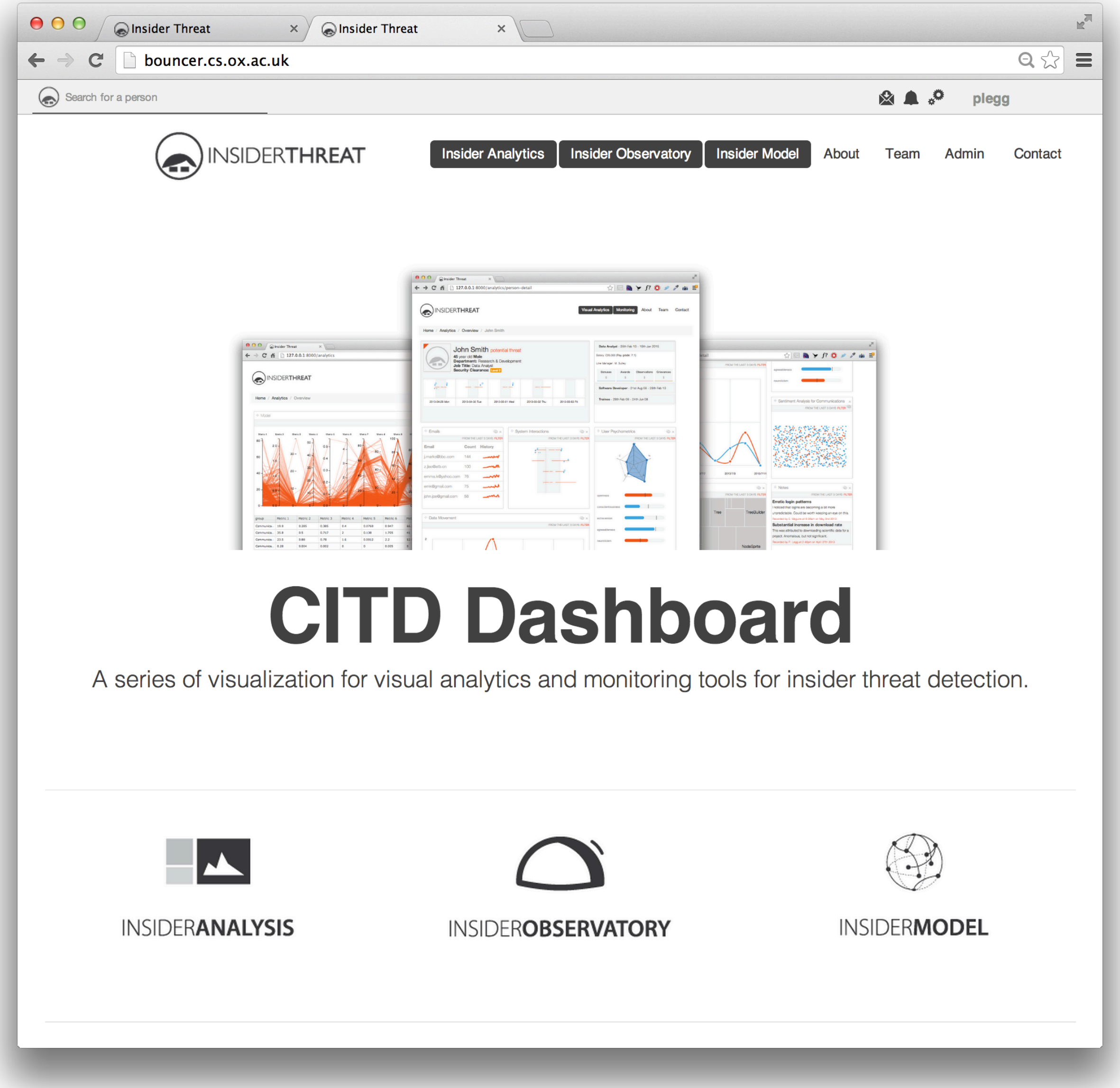
Analysis of Detection Results



date	user	group	login_ano...	device_an...	email_ano...	web_anom...	total_ano...	count_ano...	new_anom...	time_ano...	summed_
24-3-2010	AMP0031	Project Man...	0.504134	1.0942	0.0151205	3.42714	3.73161	0.199499	0.269669	3.71648	1.3952172

INSIDERTHREAT

Visual Analytics



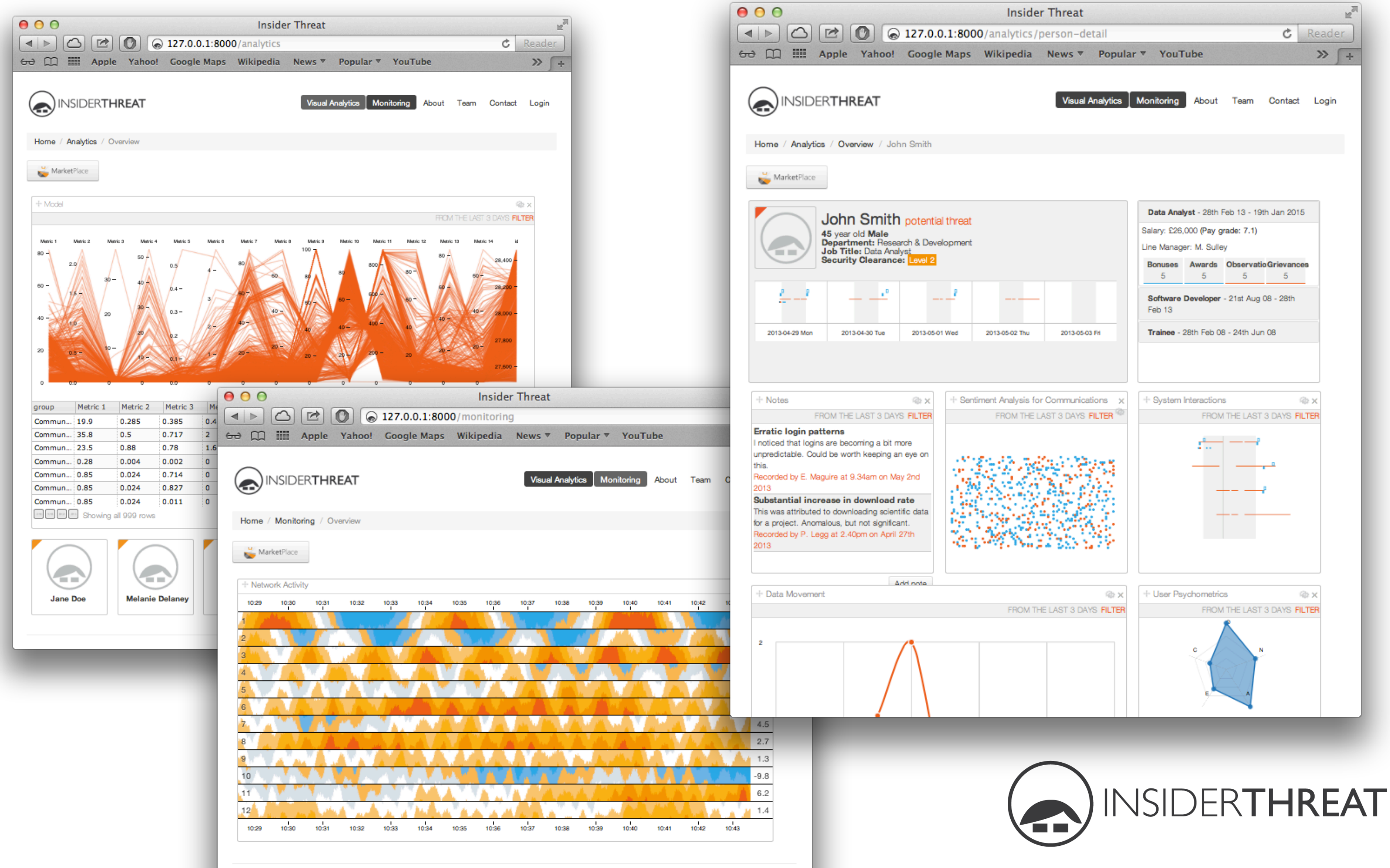
CITD Dashboard

A series of visualization for visual analytics and monitoring tools for insider threat detection.

UNIVERSITY OF OXFORD

CYBER SECURITY CENTRE

Visual Analytics



Insider Threat
127.0.0.1:8000/analytics
Apple Yahoo! Google Maps Wikipedia News Popular YouTube
INSIDERTHREAT
Visual Analytics Monitoring About Team Contact Login
Home / Analytics / Overview
MarketPlace
Model
FROM THE LAST 3 DAYS FILTER
Metric 1 Metric 2 Metric 3 Metric 4 Metric 5 Metric 6 Metric 7 Metric 8 Metric 9 Metric 10 Metric 11 Metric 12 Metric 13 Metric 14 id

group	Metric 1	Metric 2	Metric 3	Me
Commun...	19.9	0.285	0.385	0.4
Commun...	35.8	0.5	0.717	2
Commun...	23.5	0.88	0.78	1.6
Commun...	0.28	0.004	0.002	0
Commun...	0.85	0.024	0.714	0
Commun...	0.85	0.024	0.827	0
Commun...	0.85	0.024	0.011	0

Showing all 999 rows

Jane Doe
Melanie Delaney
Insider Threat
127.0.0.1:8000/monitoring
Apple Yahoo! Google Maps Wikipedia News Popular YouTube
INSIDERTHREAT
Visual Analytics Monitoring About Team
Home / Monitoring / Overview
MarketPlace
Network Activity
10:29 10:30 10:31 10:32 10:33 10:34 10:35 10:36 10:37 10:38 10:39 10:40 10:41 10:42 10:43
1 2 3 4 5 6 7 8 9 10 11 12
4.5 2.7 1.3 -9.8 6.2 1.4
Insider Threat
127.0.0.1:8000/analytics/person-detail
Apple Yahoo! Google Maps Wikipedia News Popular YouTube
INSIDERTHREAT
Visual Analytics Monitoring About Team Contact Login
Home / Analytics / Overview / John Smith
MarketPlace

John Smith potential threat
45 year old **Male**
Department: Research & Development
Job Title: Data Analyst
Security Clearance: Level 2

2013-04-29 Mon
2013-04-30 Tue
2013-05-01 Wed
2013-05-02 Thu
2013-05-03 Fri

Data Analyst - 28th Feb 13 - 19th Jan 2015
Salary: £26,000 (Pay grade: 7.1)
Line Manager: M. Sulley

Bonuses	Awards	Observatio	Grievances
5	5	5	5

Software Developer - 21st Aug 08 - 28th Feb 13

Trainee - 28th Feb 08 - 24th Jun 08

Notes
FROM THE LAST 3 DAYS FILTER

Erratic login patterns
I noticed that logins are becoming a bit more unpredictable. Could be worth keeping an eye on this.
Recorded by E. Maguire at 9.34am on May 2nd 2013

Substantial increase in download rate
This was attributed to downloading scientific data for a project. Anomalous, but not significant.
Recorded by P. Legg at 2.40pm on April 27th 2013

Add note
Sentiment Analysis for Communications
FROM THE LAST 3 DAYS FILTER
System Interactions
FROM THE LAST 3 DAYS FILTER
Data Movement
FROM THE LAST 3 DAYS FILTER
2
User Psychometrics
FROM THE LAST 3 DAYS FILTER
C N E A

INSIDERTHREAT

Outcomes

- Conceptual model developed to identify the key elements that contribute towards insider threat.
  - Human element is core to the model.
  - Understanding the human aspect is clearly important to detect and prevent such attacks.

- Detection system developed that adopts a reasoning-based approach for insider threat detection.
  - Incorporates individual- and role-based profiling.
  - Activity- and session-based profiling.
  - Belief-based reasoning that constantly updates to observed data based on prior knowledge (e.g., logged activity, or human-observable).
  - Initial results are encouraging – currently undergoing further experimentation.

UNIVERSITY OF OXFORD

CYBER SECURITY CENTRE

Moving forward

- We have developed a detection prototype that proves effective for our initial testing on available data sets.
- We need to ensure that our system is widely applicable, and can cope with varied scenarios and different organisational data structures in order to be effective.
- Currently developing different data scenarios to experiment on – we also welcome those with real world scenarios who can share anomalized data or experiences to test against.

INSIDERTHREAT

Thank you for listening.

Dr. Philip A. Legg
phil.legg@cs.ox.ac.uk
Cyber Security Centre, University of Oxford, UK.