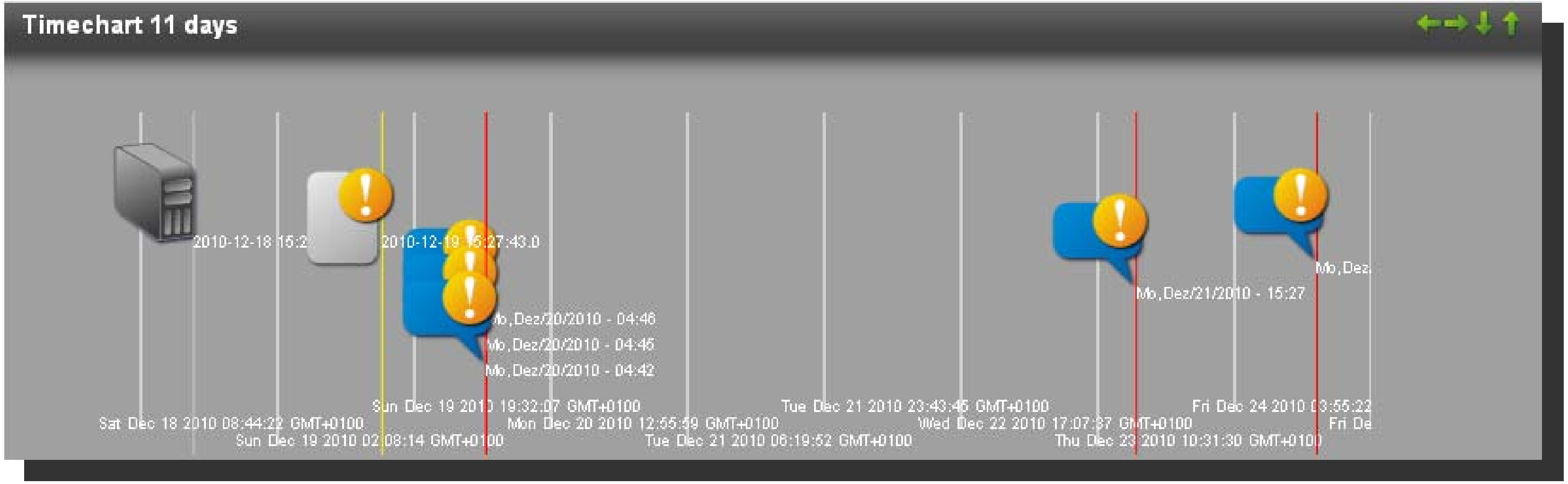
Computational Documentation of IT Incidents as Support for Forensic Operations

Sebastian Kurowski, Sandra Frings

Dept. of Information Management

Fraunhofer IAO, Stuttgart


Timechart 11 days
2010-12-18 15:2
2010-12-19 15:27:43.0
Mo,Dez/20/2010 - 04:46
Mo,Dez/20/2010 - 04:45
Mo,Dez/20/2010 - 04:42
Mo,Dez/21/2010 - 15:27
Mo,Dez
Sat Dec 18 2010 08:44:22 GMT+0100
Sun Dec 19 2010 02:08:14 GMT+0100
Sun Dec 19 2010 19:32:07 GMT+0100
Mon Dec 20 2010 12:55:59 GMT+0100
Tue Dec 21 2010 06:19:52 GMT+0100
Tue Dec 21 2010 23:43:45 GMT+0100
Wed Dec 22 2010 17:07:37 GMT+0100
Thu Dec 23 2010 10:31:30 GMT+0100
Fri Dec 24 2010 03:55:22
Fri De

Contents

1. Scope of the project
2. Definition of documentation
3. Assumptions
4. State-of-the-art systems
5. Contents of documentation
6. Documentation along with ITIL
7. Computational support and automation workflow
8. Implementation

Scope of the project

- Bachelor thesis as part of doctor thesis
- Focuses on large and distributed IT service and infrastructure providers
- Development of an „automated“ documentation system
  - **Define** documentation for computational processing
  - **Analyse** flow of information and knowledge
  - **Design** a documentation process
  - **Develop** computational automation and assistance algorithms
  - **Implement** algorithms as prototype
- For IT Incidents

Definition of documentation

- „…tool for information transmission and communication…“
- „...depend on the nature of the organizations‘ products and processes…“
- „provision of eveidence that what was planned, has actually been done.“
- „disseminate and preserve…experiences“

Source: ISO 9001:2008

- Tool of Information Security Management Systems
  - Assessment
  - Handling
  - Learning
  - Detecting
  - Avoiding

Source: ISO 27001:2009

Assumptions for further analysis and design

Organisational assumptions

- Structural assumptions
  - Organizations‘ structure is distributed
  - Centralized management (top) vs. multiple computing centres (bottom)
- Human resources
  - No communication between generations of employees
- Knowledge in IT security
  - Is further developed along the generations
  - Knowledge must be gathered and learned in each generation
  - Implicated knowledge is abstract due to lack of communication between generations

Assumptions for further analysis and design

Technical assumptions

- Existing datasources
  - Configuration management databases
  - Ticketing system
  - RSS feeds on vulnerabilities
- All communication wrt. incident through ticketing system

Assumptions for further analysis and design

Incident Response

- Employee loses information partially/completely after resolvement
- During resolvement the employee is completely focused on the Incident
  - No focus on documentation

→ Documentation might not fully comply to the requirements

- wrt. its structure
- wrt. its contents

State-of-the-art systems

- GSTool
  - Configuration Management
  - Risk assessment
  - Documentation of actions & next steps

  → But: No correlation with IT incidents

Source: German Federal Office for Information Security

State-of-the-art systems

- Helpdesk systems

  - Documentation of
    - Configuration
    - Costs
    - Involved Employees

  - Monitoring of costs & types of incidents

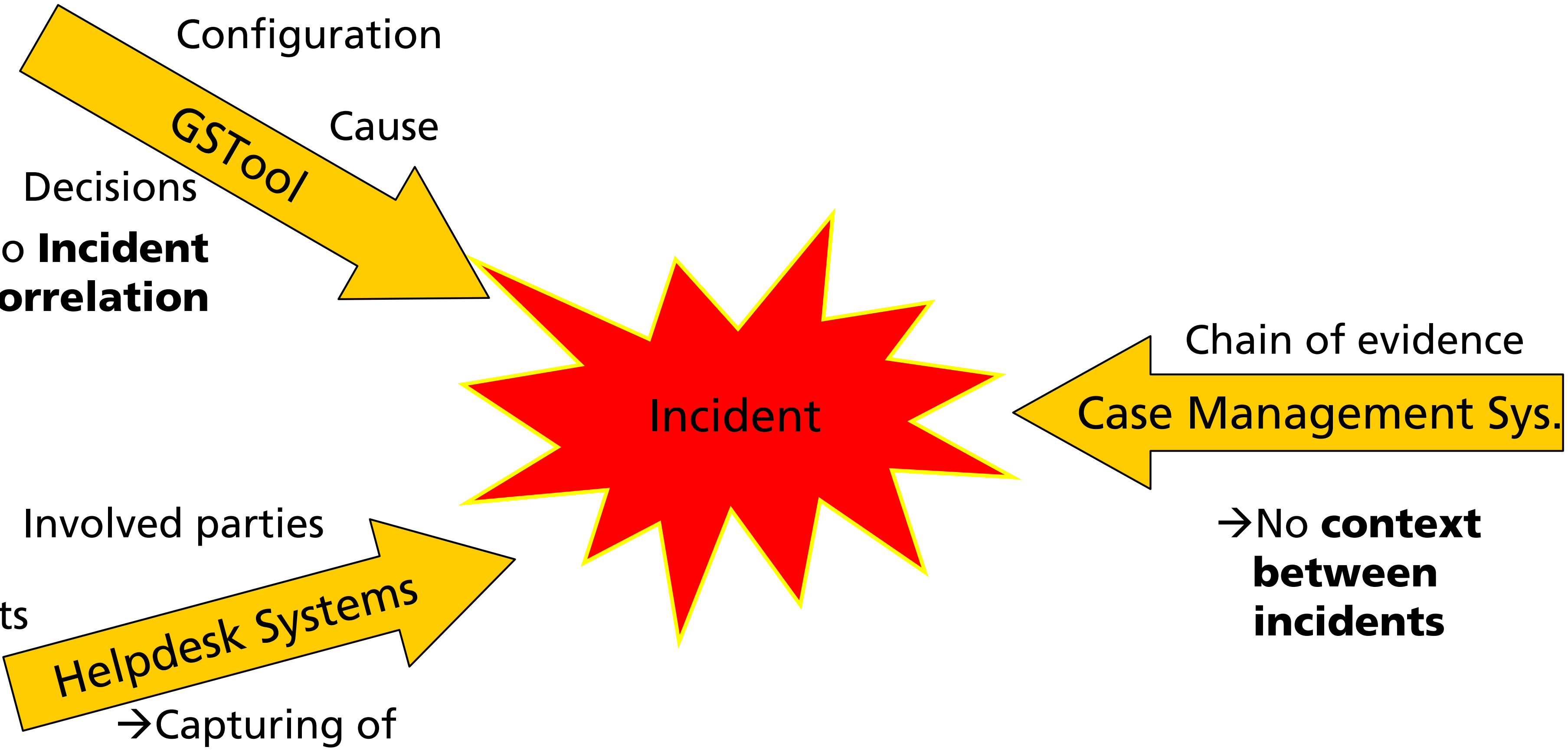
  - Main focus: Communication with customer during incident resolving

  → Often no preservation of knowledge (except for special CBR modules)

State-of-the-art systems

- Case management systems (i.e. Encase)
  - Used in IT forensics
  - Organization of forensic assets
  - Provide most necessary forensic functions (i.e. search)
  - Do not capture
    - Management decisions
    - Contexts between incidents

State of the art systems



GSTool

Configuration

Cause

Decisions

→No **Incident Correlation**

Incident

Chain of evidence

Case Management Sys.

→No **context between incidents**

Involved parties

Costs

CBR

Helpdesk Systems

→Capturing of **technical knowledge**?

Contents of documentation
Focus of requirements analysis

- Captured through analysis of standards and best practices

- Identified through survey
  - Throughout persons involved in IT security
    - Information security managers
    - IT administrators, etc.

  - 2 large and distributed research organisations

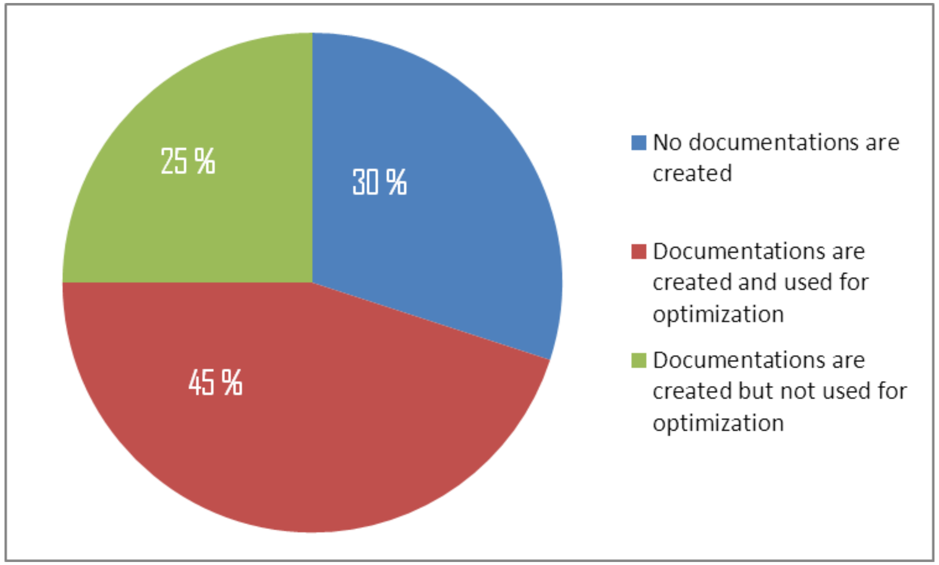
  - Answer time 4 weeks
  - 17% Answer rate
    - Not representative as single outcome
    - By combination with research of standards and best practices
      - Validation of requirements

Contents of documentation

Results from survey

- Are IT incidents documented?
- Documentation as input for optimization?
- 30% do not document IT incidents
- 25% do not use the documentation

→ Loss of valuable knowledge



Contents of documentation
Results from survey

- Other questions
  - Required information assets for incident response / security status optimization
  - Used systems for deposit / retrieval / analysis of documentation
  - Used helpdesk system
  - Media for communication of IT incidents

Contents of documentation

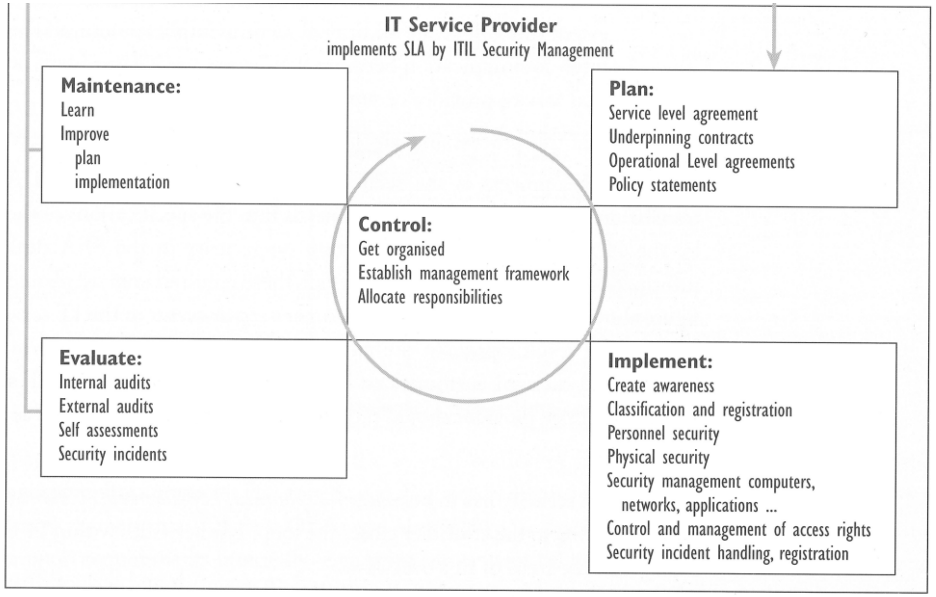
- Outcome: Definition of documentation

- Container document of information regarding
  - Configuration
  - Vulnerabilities & Risks
  - Communication data
  - Affected configuration
  - Risk assessments
  - Used procedure for resolvment
  - Proposal of future changes / Lessons Learned

Documentation along ITIL

- ITIL Best Practices on Security Management
  - Framework for maintaining and managing all aspects of IT security
  - Mostly implemented along IT infrastructure providers
  - Documentation along ITIL

    → Easier implementation of documentation process



IT Service Provider
implements SLA by ITIL Security Management

Maintenance:
Learn
Improve
plan
implementation

Plan:
Service level agreement
Underpinning contracts
Operational Level agreements
Policy statements

Control:
Get organised
Establish management framework
Allocate responsibilities

Evaluate:
Internal audits
External audits
Self assessments
Security incidents

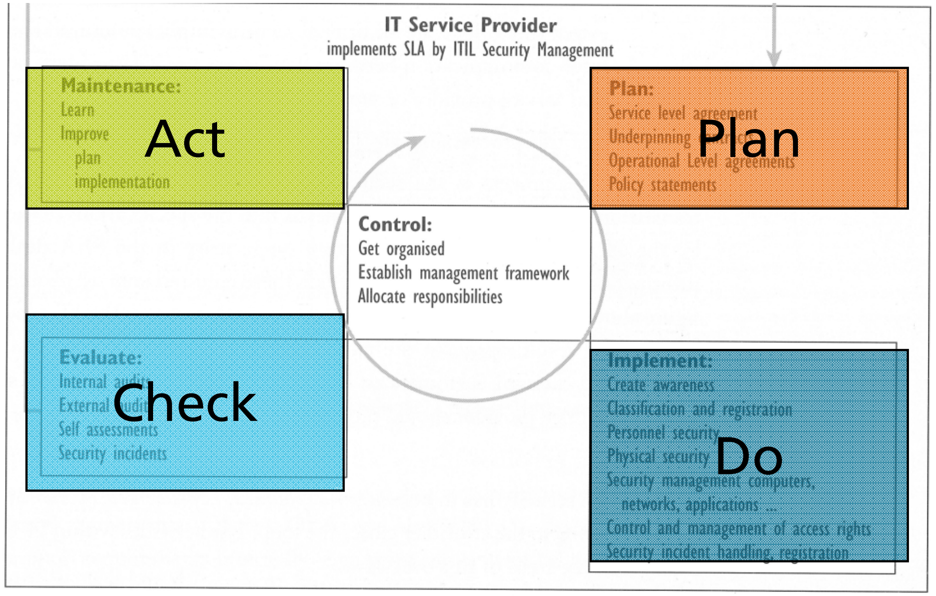
Implement:
Create awareness
Classification and registration
Personnel security
Physical security
Security management computers, networks, applications ...
Control and management of access rights
Security incident handling, registration

Source: ITIL Best Practices on Security Management

Documentation along ITIL

- Implied PDCA Cycle
  - ITIL & ISO 27000 define a PDCA (Plan – Do – Check – Act) Cycle
  - Cycle for maintaining common ground during operations
  - Infinite PDCA Cycle offers knowledge preservation capabilities

→ Isolation of information providers along the PDCA Cycle


IT Service Provider
implements SLA by ITIL Security Management
Maintenance:
Learn
Improve
plan
implementation
Act
Plan:
Service level agreement
Underpinning
Operational Level agreements
Policy statements
Plan
Control:
Get organised
Establish management framework
Allocate responsibilities
Evaluate:
Internal audits
External audits
Self assessments
Security incidents
Check
Implement:
Create awareness
Classification and registration
Personnel security
Physical security
Security management computers, networks, applications ...
Control and management of access rights
Security incident handling, registration
Do

Documentation along ITIL

- PDCA loop
  - „Act“ Phase as next iteration of information asset creation

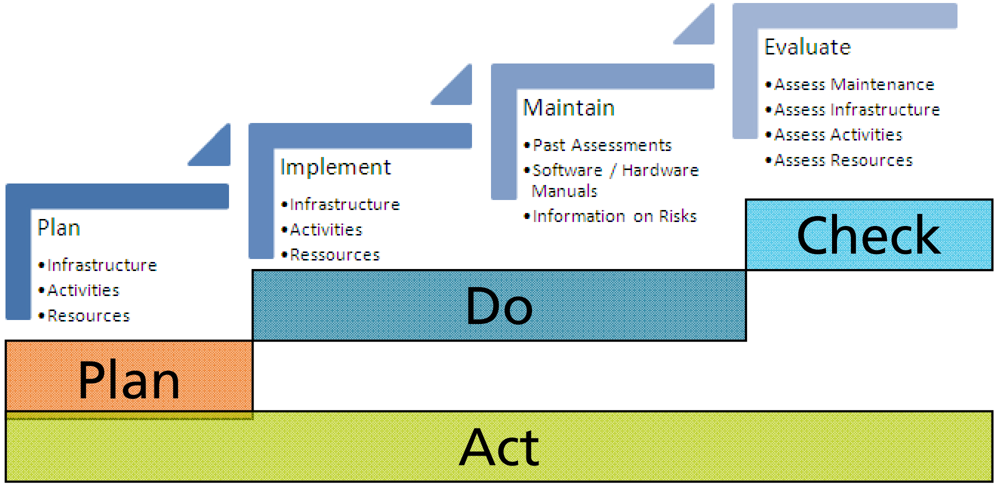
→ Information retrieval during

- Planning
- Implementing
- Maintaining

- IT Security actions

→ Creation of documentation

- By creating context to IT incident
- During evaluation

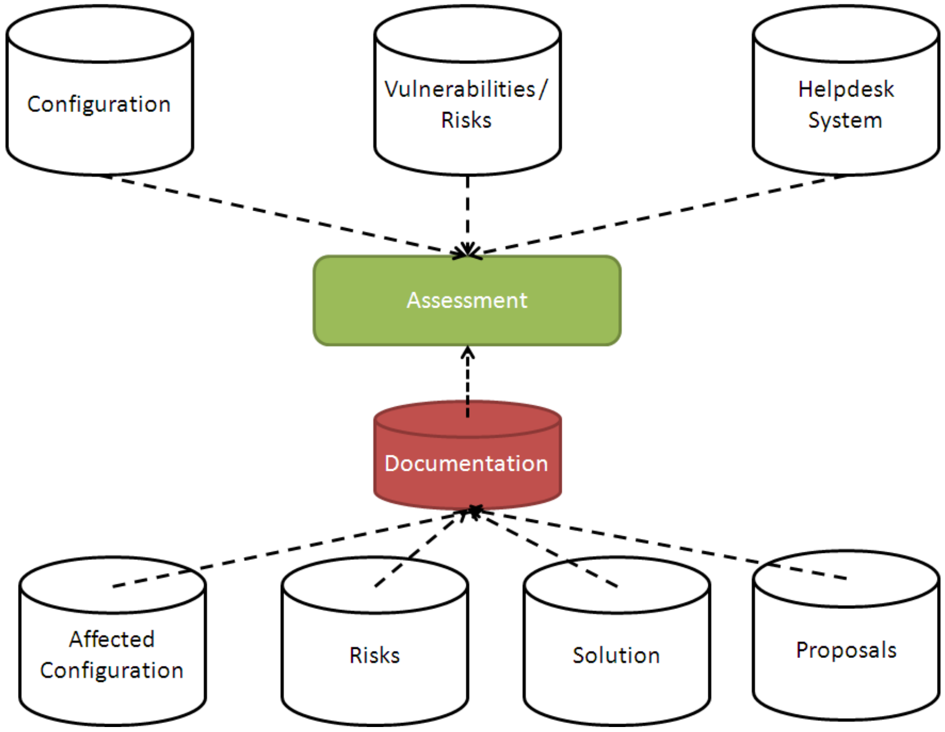


Documentation along ITIL

- Documentation as information container
- Knowledge capturing due to assessment
  - Of information wrt. IT incident

→ 2 Phases of documentation creation

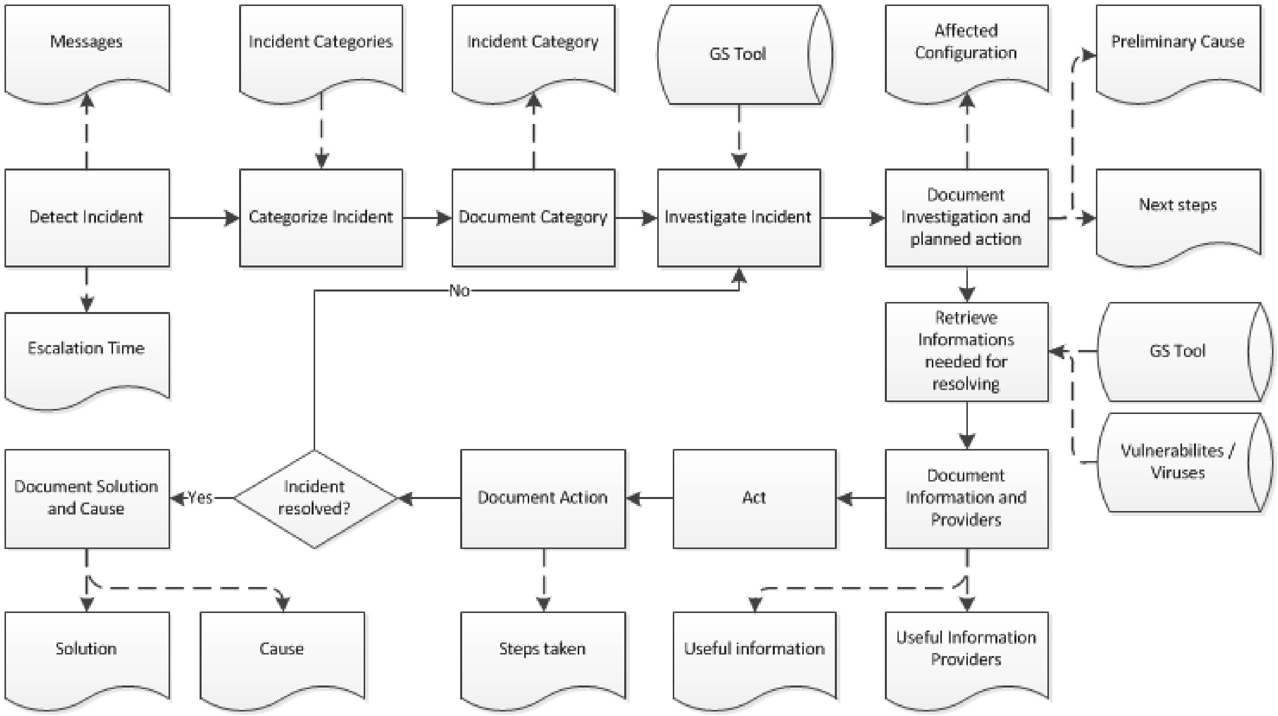
  - Information retrieval (Plan, Do)
  - Evaluation of information (Check)



Documentation along ITIL

- Information retrieval phase
  - During incident resolvement
  - Conflict with focus on IT incident

  → Automation needed

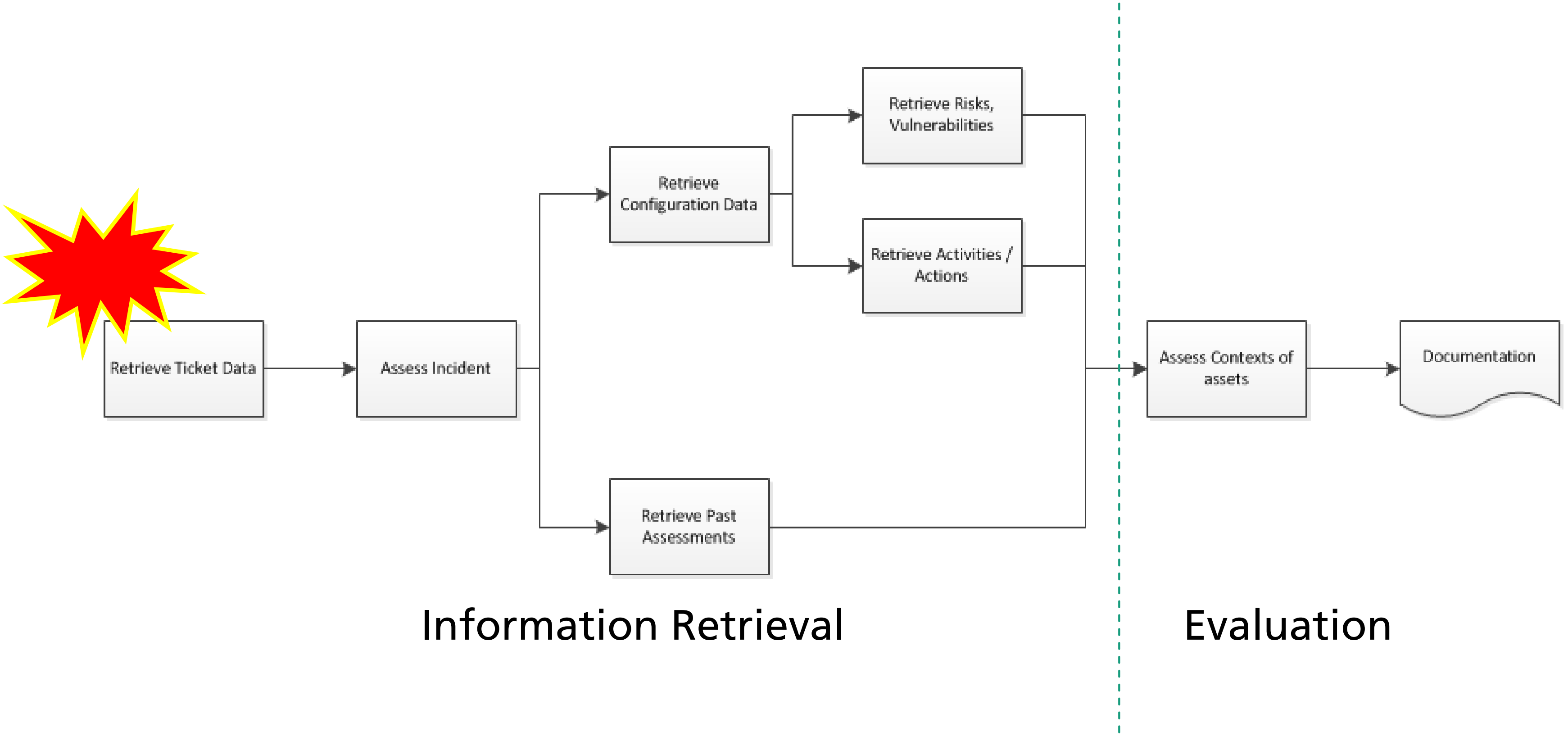


Documentation along ITIL

- Evaluation of information captured
  - Done after incident
  - Presentation of information
  - Computational assistance for improving evaluation process.

Computational support and automation workflow

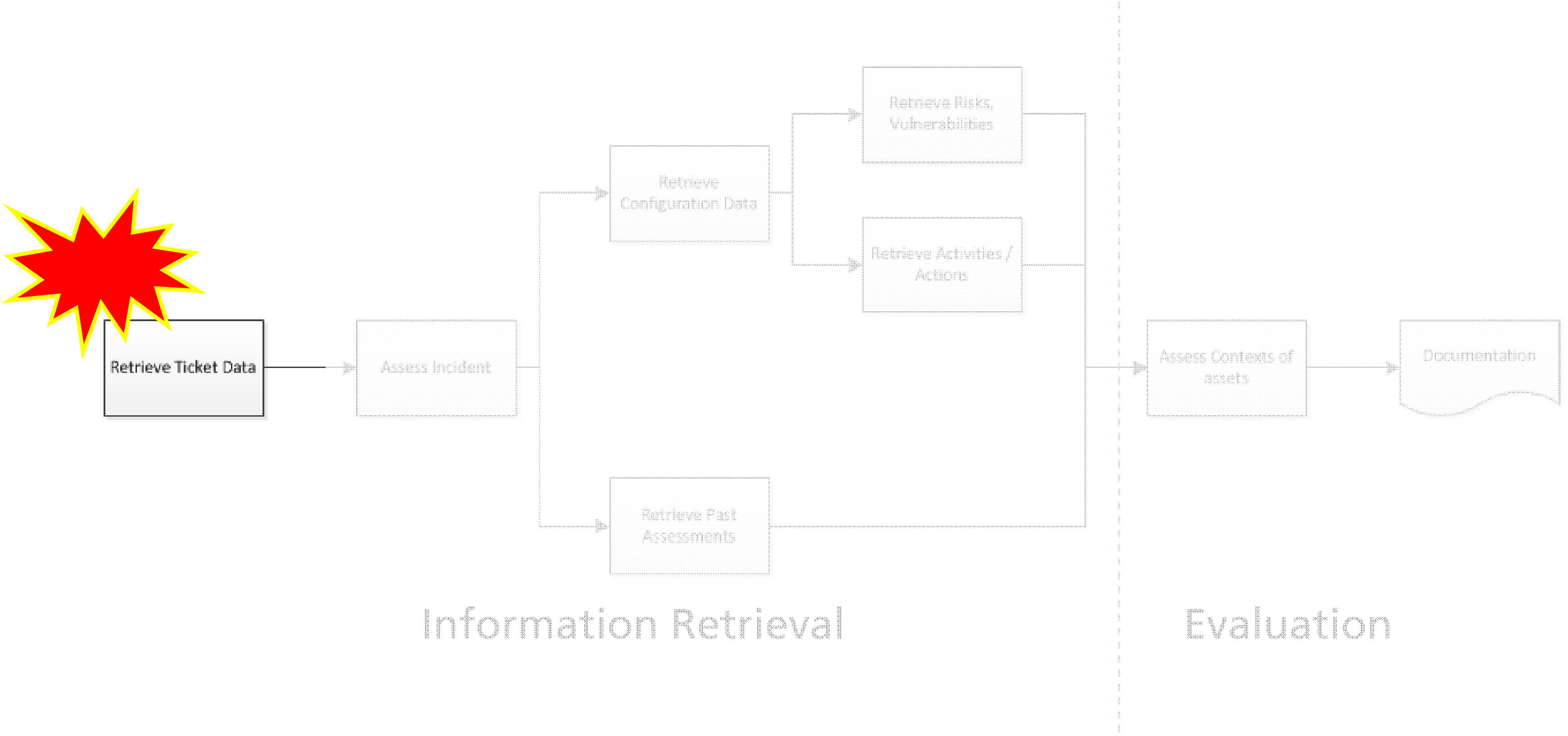
Technical abstract of documentation process


Retrieve Ticket Data
Assess Incident
Retrieve Configuration Data
Retrieve Risks, Vulnerabilities
Retrieve Activities / Actions
Retrieve Past Assessments
Assess Contexts of assets
Documentation
Information Retrieval
Evaluation

- Automation and support of processes involved in documentation

Computational support and automation workflow

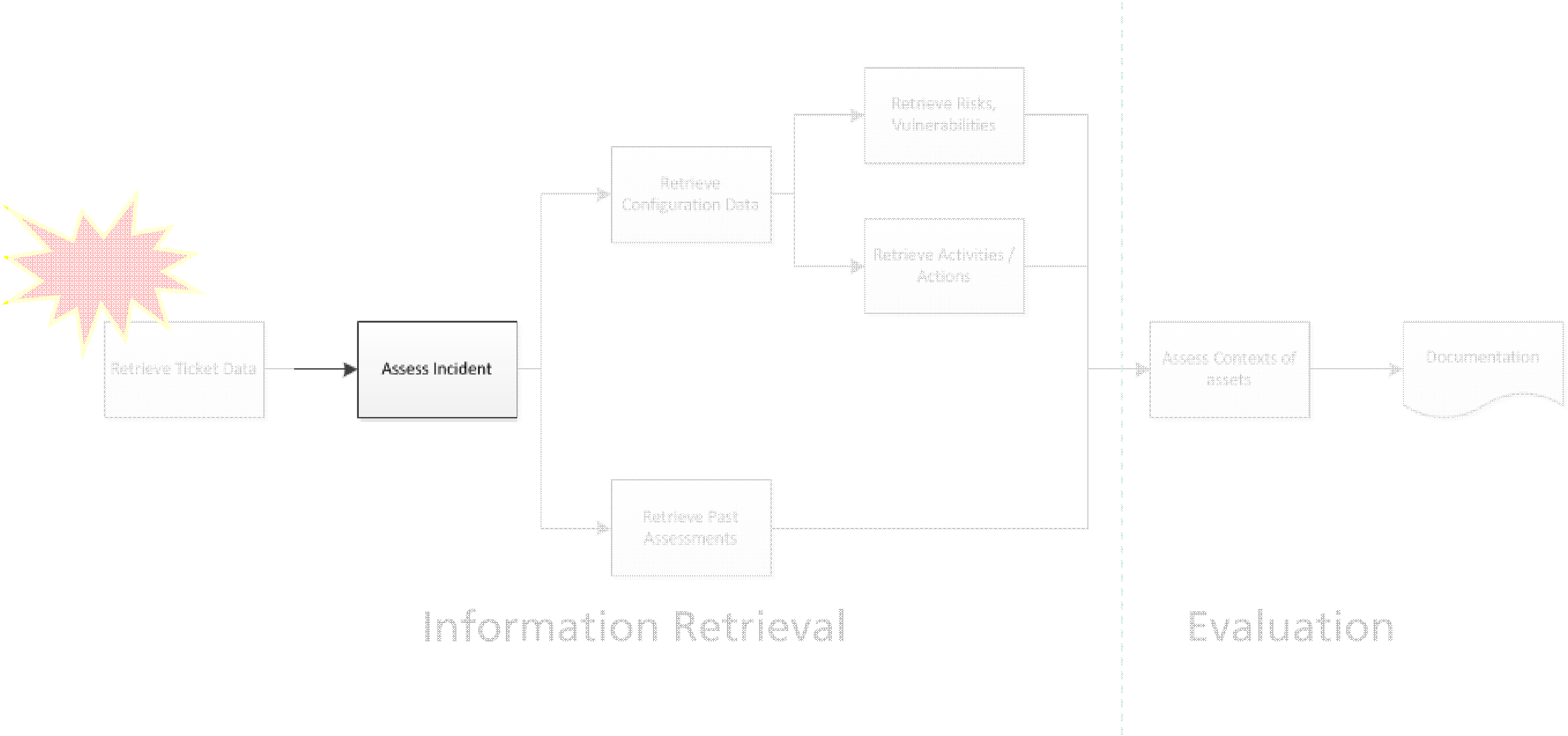
Technical abstract of documentation process


Retrieve Ticket Data
Assess Incident
Retrieve Configuration Data
Retrieve Risks, Vulnerabilities
Retrieve Activities / Actions
Retrieve Past Assessments
Assess Contexts of assets
Documentation
Information Retrieval
Evaluation

- Content of Ticket as basis for further processing

Computational support and automation workflow

Technical abstract of documentation process

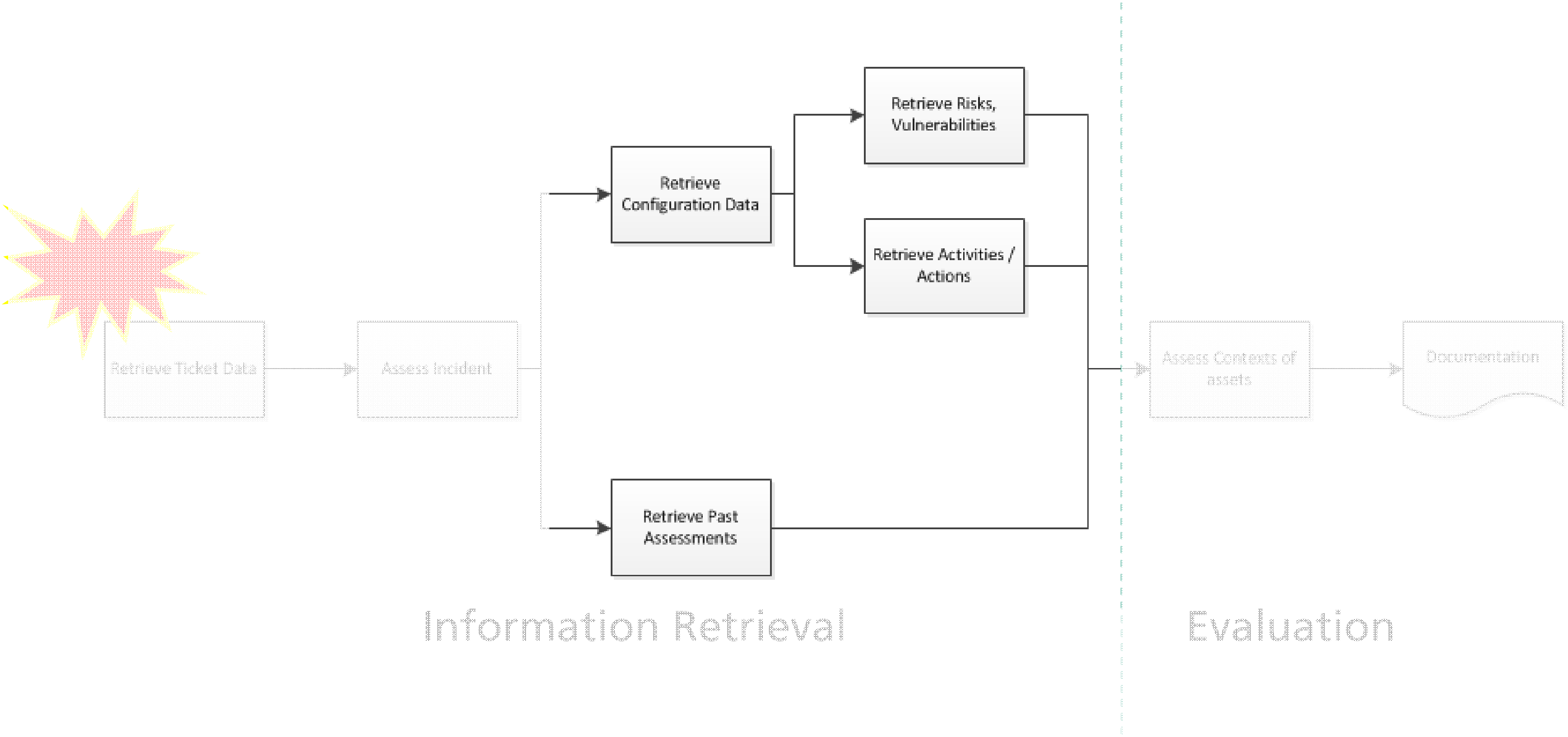

Retrieve Ticket Data
Assess Incident
Retrieve Configuration Data
Retrieve Risks, Vulnerabilities
Retrieve Activities / Actions
Retrieve Past Assessments
Assess Contexts of assets
Documentation
Information Retrieval
Evaluation

- Extract Keywords
- Categorize Incident

→ Information for further querying of information providers

Computational support and automation workflow

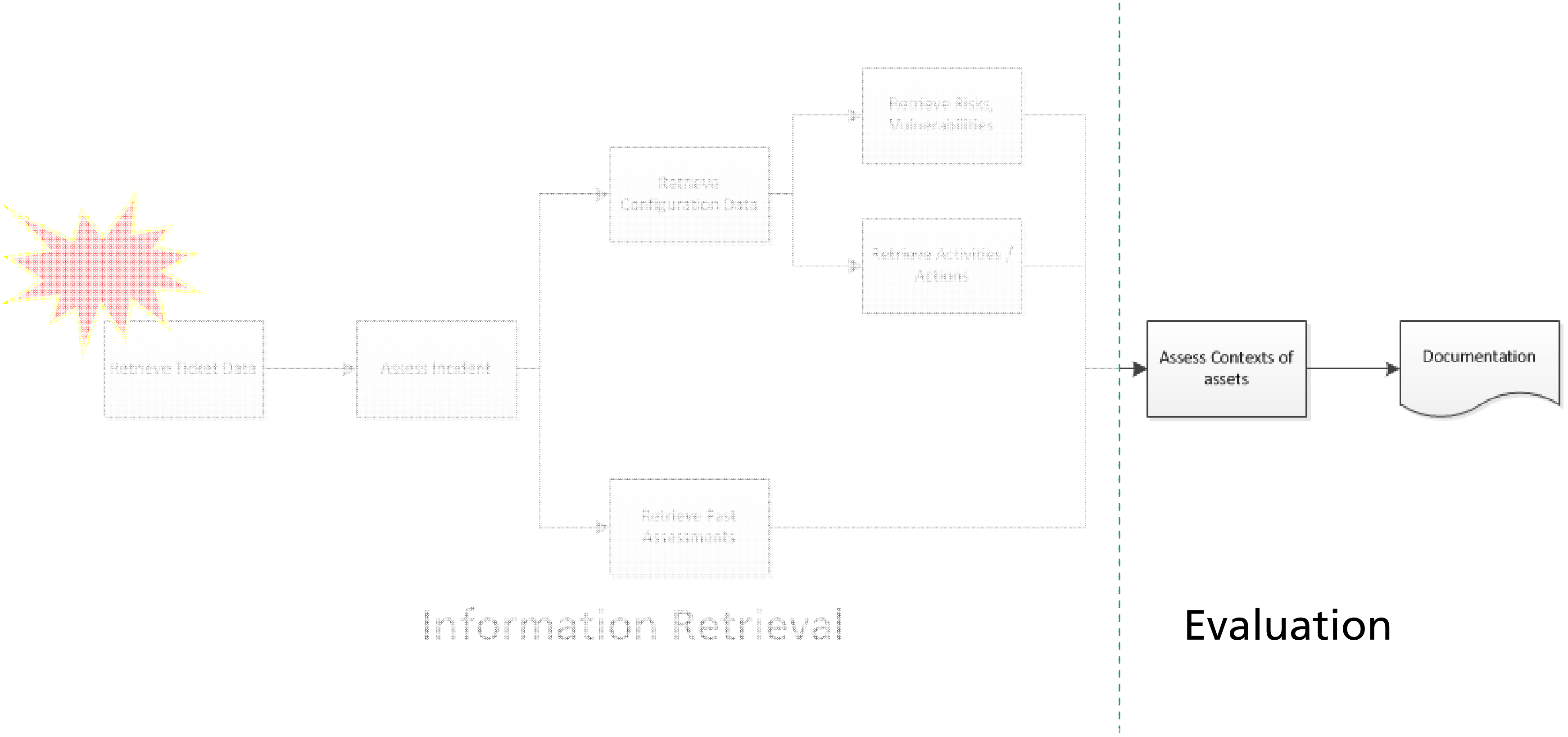
Technical abstract of documentation process


Retrieve Risks, Vulnerabilities
Retrieve Configuration Data
Retrieve Activities / Actions
Retrieve Ticket Data
Assess Incident
Assess Contexts of assets
Documentation
Retrieve Past Assessments
Information Retrieval
Evaluation

- Retrieve Information using extracted keywords and category

Computational support and automation workflow

Technical abstract of documentation process

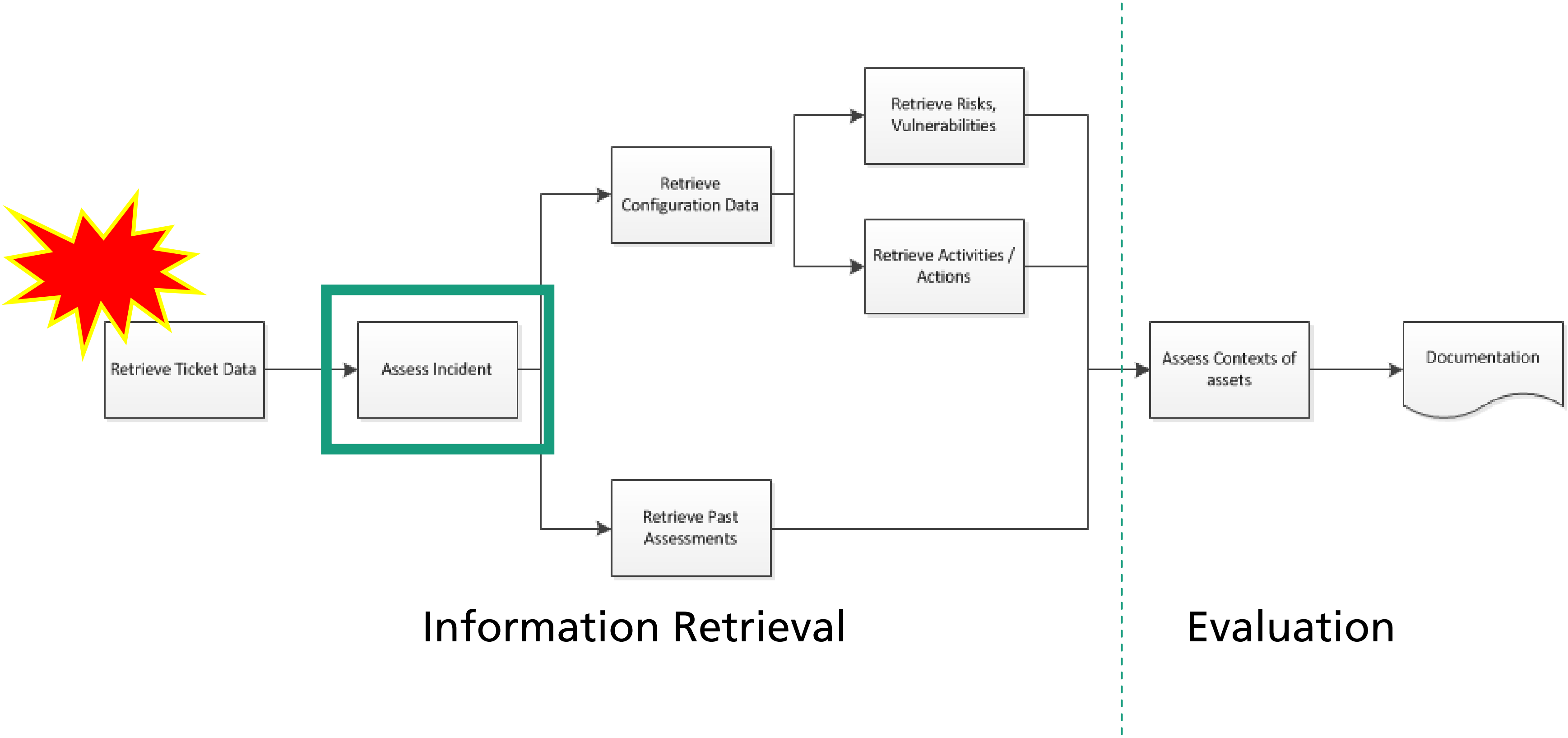


Retrieve Ticket Data
Assess Incident
Retrieve Configuration Data
Retrieve Risks, Vulnerabilities
Retrieve Activities / Actions
Retrieve Past Assessments
Assess Contexts of assets
Documentation
Information Retrieval
Evaluation

- Generate a lessons learned survey and create documentation

Computational support and automation workflow

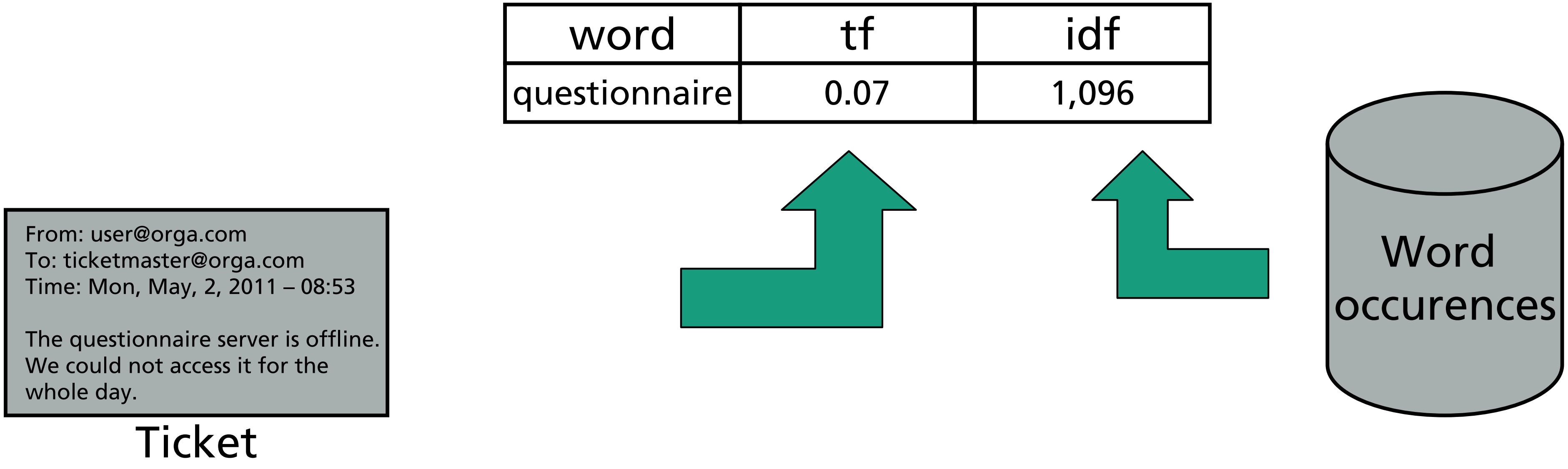
Technical abstract of documentation process


Retrieve Ticket Data
Assess Incident
Retrieve Configuration Data
Retrieve Risks, Vulnerabilities
Retrieve Activities / Actions
Retrieve Past Assessments
Assess Contexts of assets
Documentation
Information Retrieval
Evaluation

- Assessment and asset proposing algorithms

Computational support and automation workflow

Extraction of query information



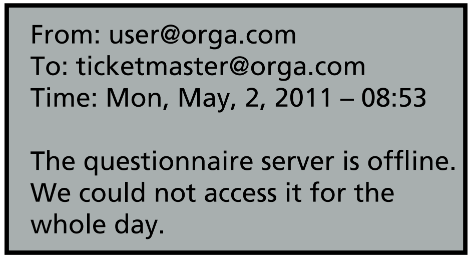
word	tf	idf
questionnaire	0.07	1,096

From: user@orga.com
To: ticketmaster@orga.com
Time: Mon, May, 2, 2011 – 08:53

The questionnaire server is offline. We could not access it for the whole day.

Computational support and automation workflow

Extraction of query information - keywords

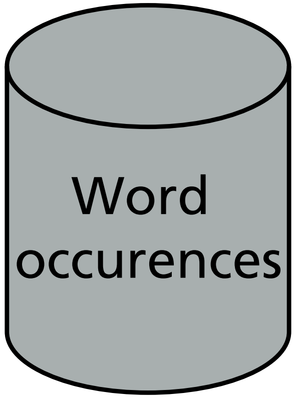


From: user@orga.com
To: ticketmaster@orga.com
Time: Mon, May, 2, 2011 – 08:53

The questionnaire server is offline. We could not access it for the whole day.

Ticket

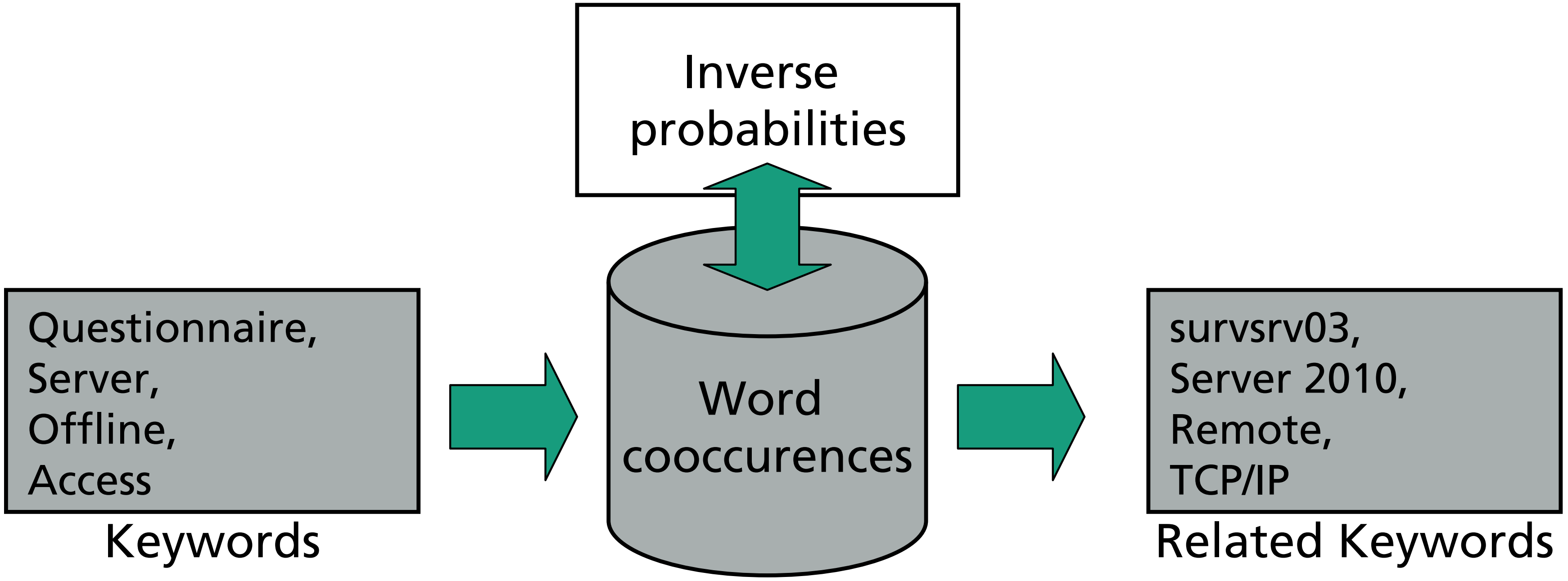
word	tf	idf
questionnaire	0.07	1,096
server	0.07	0,187
offline	0.07	0,48
access	0.07	0,34
…	…	…
the	0.14	0,022



- Keywords for querying the information providers
- Questionnaire, server, offline, access

Computational support and automation workflow

Extraction of query information - keywords



Inverse probabilities

Questionnaire,
Server,
Offline,
Access

Keywords

Word cooccurences

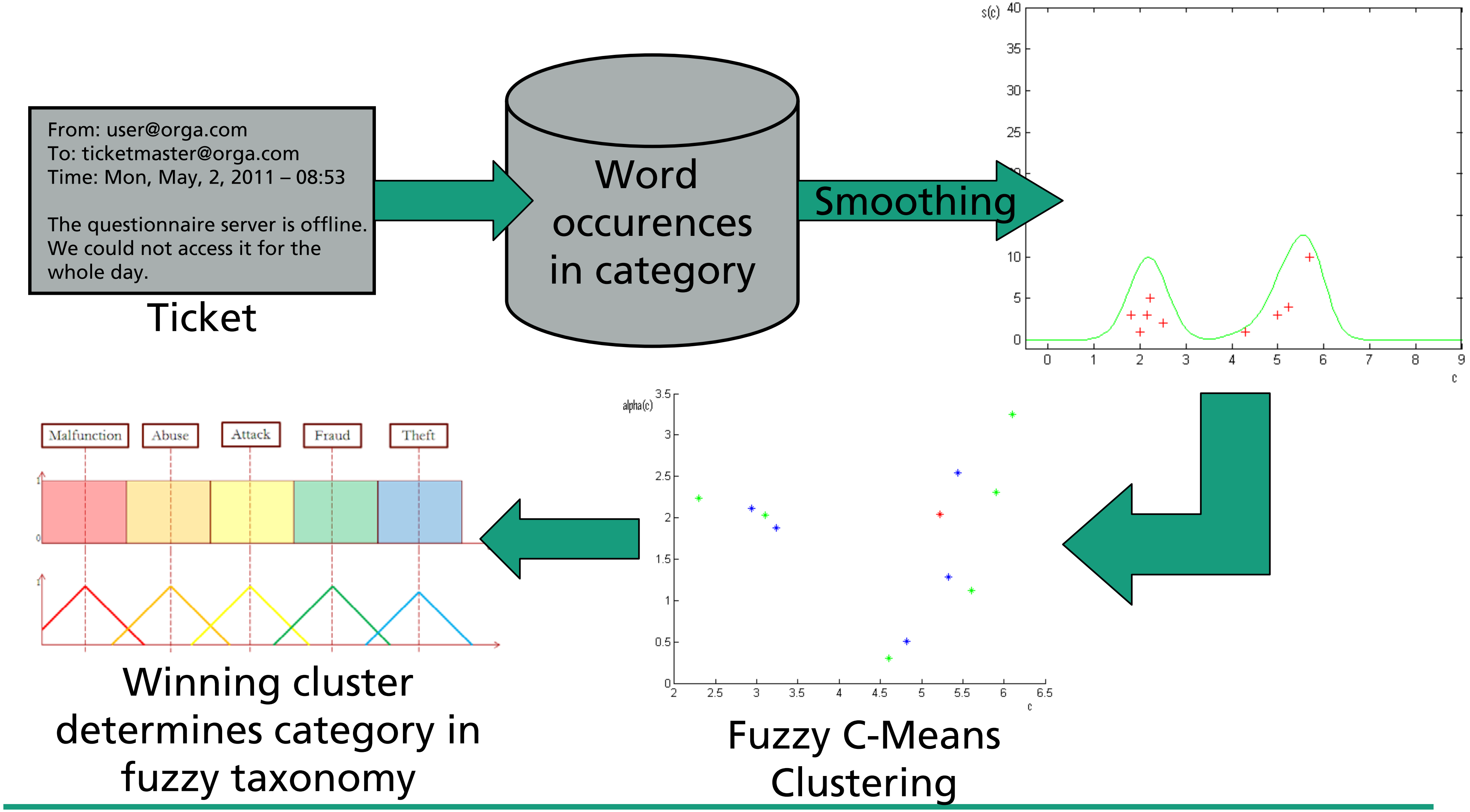
survsrv03,
Server 2010,
Remote,
TCP/IP

Related Keywords

- Extraction of related keywords
- Domain specific language vs. natural language

Computational support and automation workflow

System overview – Categorization algorithm



From: user@orga.com
To: ticketmaster@orga.com
Time: Mon, May, 2, 2011 – 08:53

The questionnaire server is offline.
We could not access it for the
whole day.

Ticket

Word occurences in category

Smoothing

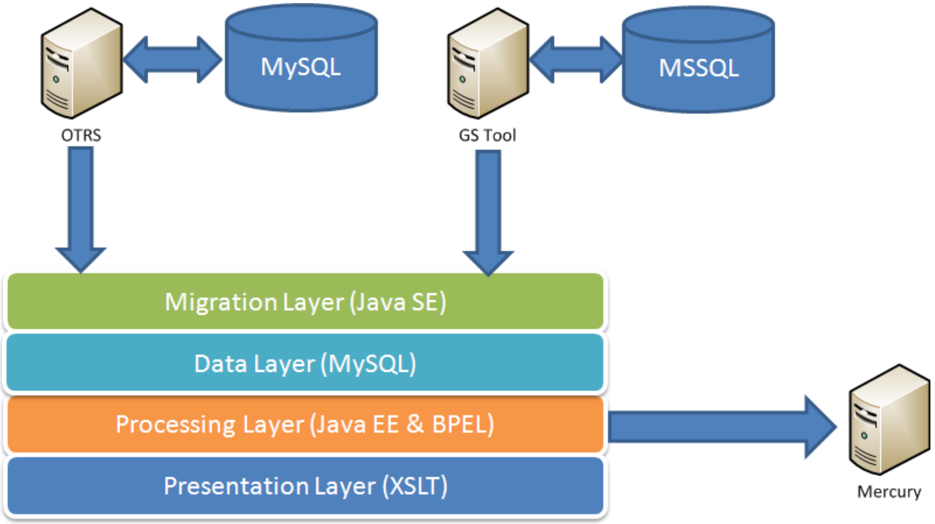
Fuzzy C-Means Clustering

Winning cluster determines category in fuzzy taxonomy

Implementation

Prototype overview

- Distributed system
  - Easier integration of information providers
  - Orchestration process external
    - Easier maintenance
  - → More flexibility and adaption to corporative structures


MySQL
OTRS
MSSQL
GS Tool
Migration Layer (Java SE)
Data Layer (MySQL)
Processing Layer (Java EE & BPEL)
Presentation Layer (XSLT)
Mercury

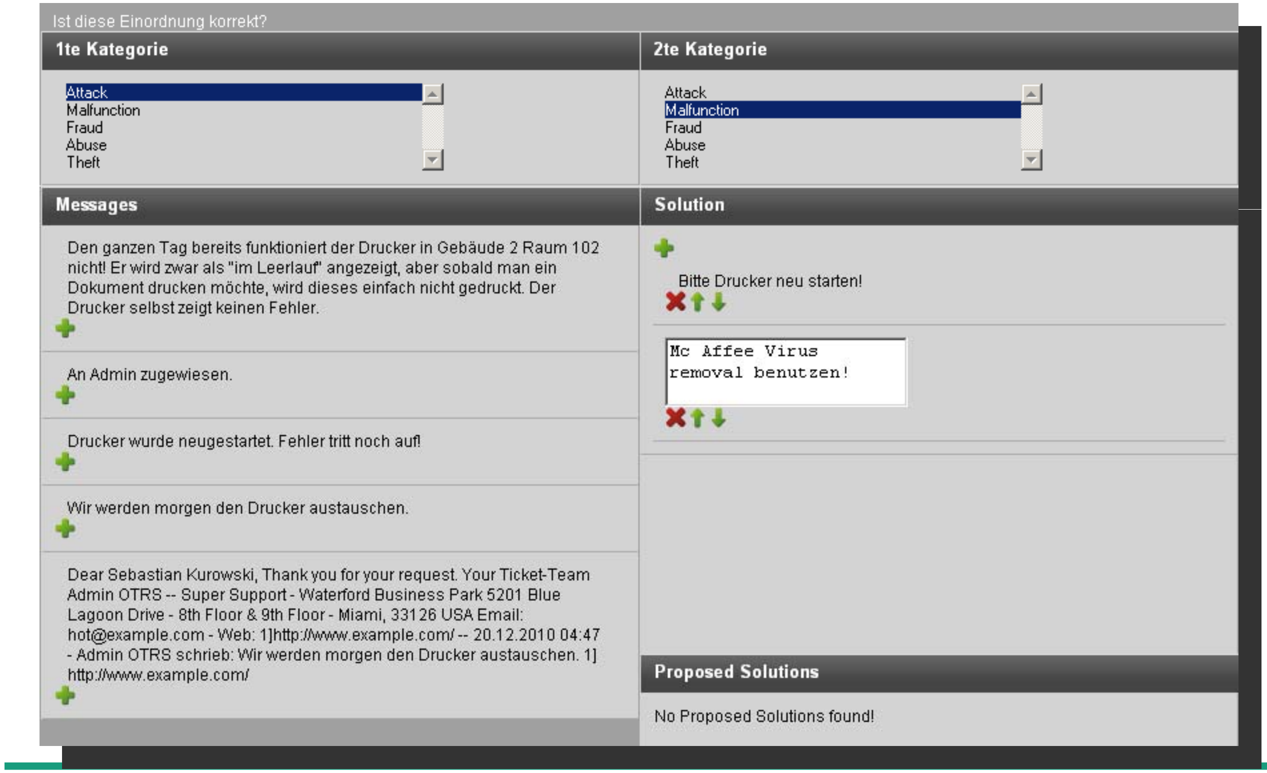
- Presentation through XSL Transformation
  - Easier integration in existing systems
  - Currently XML → XHTML
  - XML → IODEF* also possible

* Source: http://xml.coverpages.org/iodef.html

Implementation

Lessons learned survey during evaluation

- Assessment of retrieved information
- Capturing of solution & proposals for future changes
- Documentation is created after assessment through survey



Ist diese Einordnung korrekt?

1te Kategorie

Attack (selected)
Malfunction
Fraud
Abuse
Theft

2te Kategorie

Attack
Malfunction (selected)
Fraud
Abuse
Theft

Messages

Den ganzen Tag bereits funktioniert der Drucker in Gebäude 2 Raum 102 nicht! Er wird zwar als "im Leerlauf" angezeigt, aber sobald man ein Dokument drucken möchte, wird dieses einfach nicht gedruckt. Der Drucker selbst zeigt keinen Fehler.

An Admin zugewiesen.

Drucker wurde neugestartet. Fehler tritt noch auf!

Wir werden morgen den Drucker austauschen.

Dear Sebastian Kurowski, Thank you for your request. Your Ticket-Team Admin OTRS -- Super Support - Waterford Business Park 5201 Blue Lagoon Drive - 8th Floor & 9th Floor - Miami, 33126 USA Email: hot@example.com - Web: 1]http://www.example.com/ -- 20.12.2010 04:47 - Admin OTRS schrieb: Wir werden morgen den Drucker austauschen. 1] http://www.example.com/

Solution

Bitte Drucker neu starten!

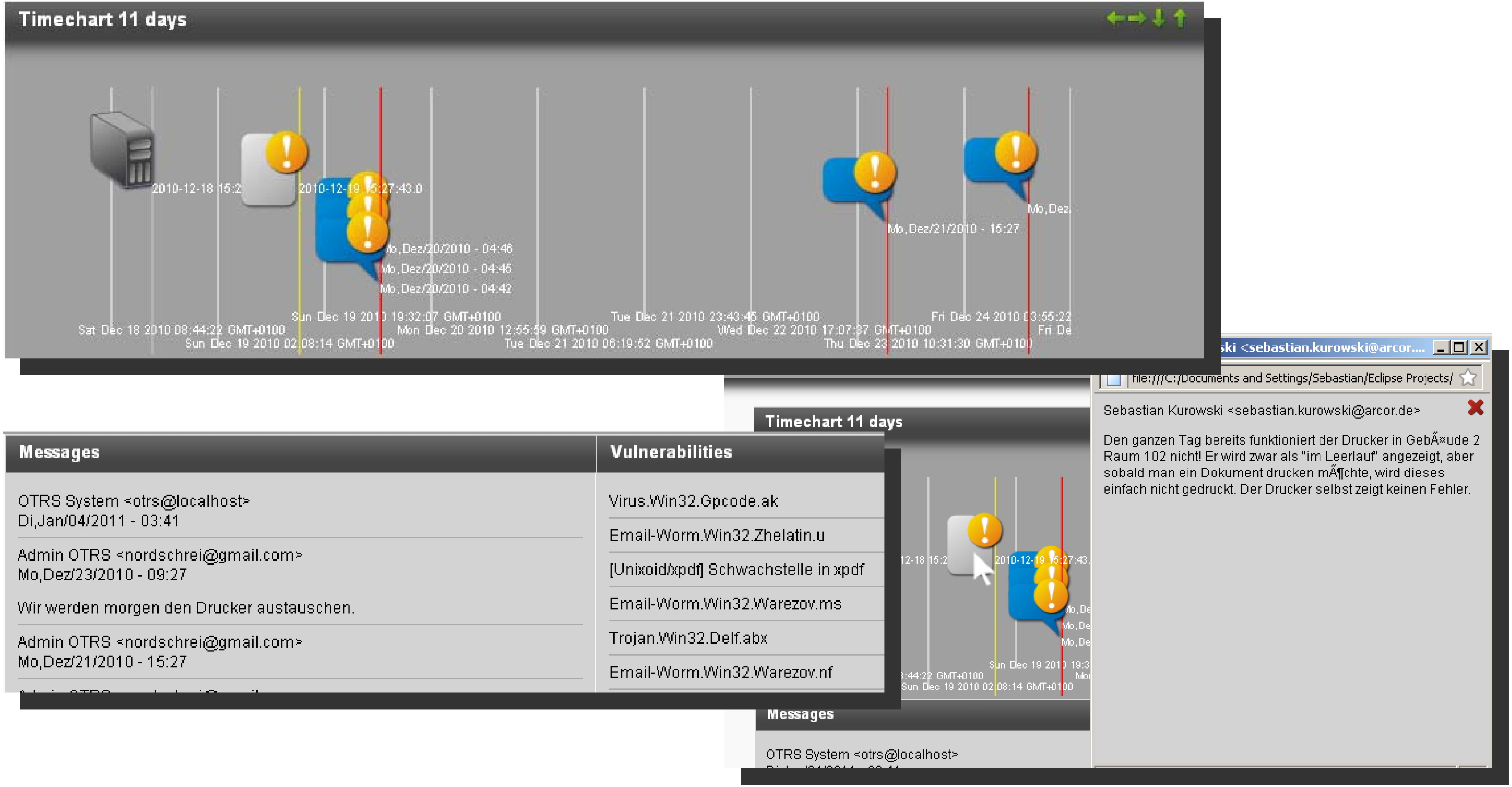
Mc Affee Virus removal benutzen!

Proposed Solutions

No Proposed Solutions found!

Implementation

Presentation of documentation (XHTML)



Timechart 11 days
2010-12-18 15:2
2010-12-19 15:27:43.0
Mo,Dez/20/2010 - 04:46
Mo,Dez/20/2010 - 04:45
Mo,Dez/20/2010 - 04:42
Mo,Dez/21/2010 - 15:27
Mo,Dez
Sat Dec 18 2010 08:44:22 GMT+0100
Sun Dec 19 2010 02:08:14 GMT+0100
Sun Dec 19 2010 19:32:07 GMT+0100
Mon Dec 20 2010 12:55:59 GMT+0100
Tue Dec 21 2010 06:19:52 GMT+0100
Tue Dec 21 2010 23:43:45 GMT+0100
Wed Dec 22 2010 17:07:37 GMT+0100
Thu Dec 23 2010 10:31:30 GMT+0100
Fri Dec 24 2010 03:55:22
Fri De

Messages	Vulnerabilities
OTRS System <otrs@localhost> Di,Jan/04/2011 - 03:41	Virus.Win32.Gpcode.ak
Admin OTRS <nordschrei@gmail.com> Mo,Dez/23/2010 - 09:27	Email-Worm.Win32.Zhelatin.u
Wir werden morgen den Drucker austauschen.	[Unixoid/xpdf] Schwachstelle in xpdf
Admin OTRS <nordschrei@gmail.com> Mo,Dez/21/2010 - 15:27	Email-Worm.Win32.Warezov.ms
	Trojan.Win32.Delf.abx
	Email-Worm.Win32.Warezov.nf

ski <sebastian.kurowski@arcor....
file:///C:/Documents and Settings/Sebastian/Eclipse Projects/
Timechart 11 days
12-18 15:2
2010-12-19 15:27:43.
Sun Dec 19 2010 19:3
:44:22 GMT+0100
Sun Dec 19 2010 02:08:14 GMT+0100
Messages
OTRS System <otrs@localhost>

Sebastian Kurowski <sebastian.kurowski@arcor.de>

Den ganzen Tag bereits funktioniert der Drucker in GebÃ¤ude 2 Raum 102 nicht! Er wird zwar als "im Leerlauf" angezeigt, aber sobald man ein Dokument drucken mÃ¶chte, wird dieses einfach nicht gedruckt. Der Drucker selbst zeigt keinen Fehler.

Conclusions
Organisational

- Capturing of knowledge
  - Assessment of retrieved information
  - Information providers adaptable
  - Less effort for the expert

- Documentation
  - As knowledge provider
    - Risk assessment
    - Incident response

  - As evidence provider

Conclusions
Technical

- Prototype as distributed system
  - External orchestration processes
  - Respects corporative structures and processes
- Adaptable output
  - XML + XSLT
  - Transformation to any output format possible
  - IODEF*
- Keyword extraction & categorisation of incidents
  - Adaption by using feedback from lessons learned survey
  - Problems of overfitting

* Source: http://xml.coverpages.org/iodef.html

Computational Documentation of IT Incidents as Support for Forensic Operations

Thank you. Questions?