Real-time DDoS Defense:

A collaborative Approach at Internet Scale

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

UNIVERSITEIT TWENTE.

CASED

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP
http://www.dasec.h-da.de/

Agenda

Problem & Goal

Insight

Overview

Challenges

Implementation

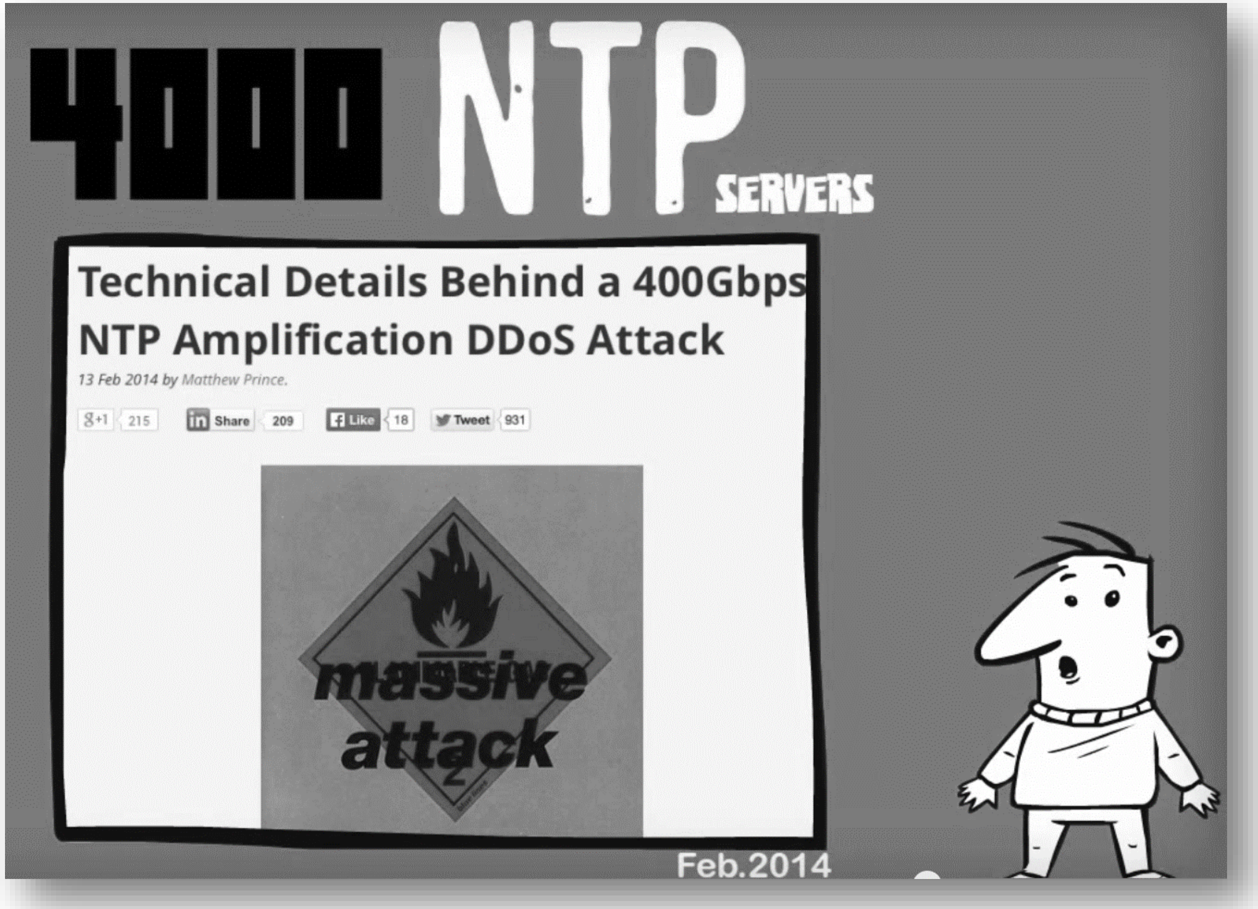
Evaluation

Conclusion

Discussion

Problem & Goal

Problem



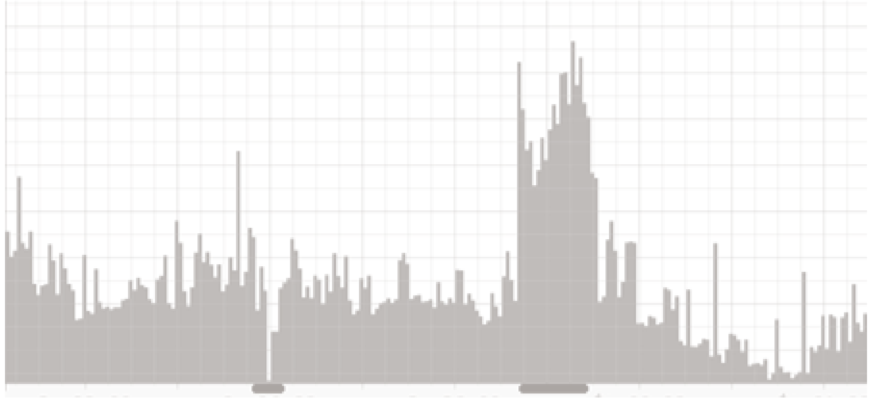
Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

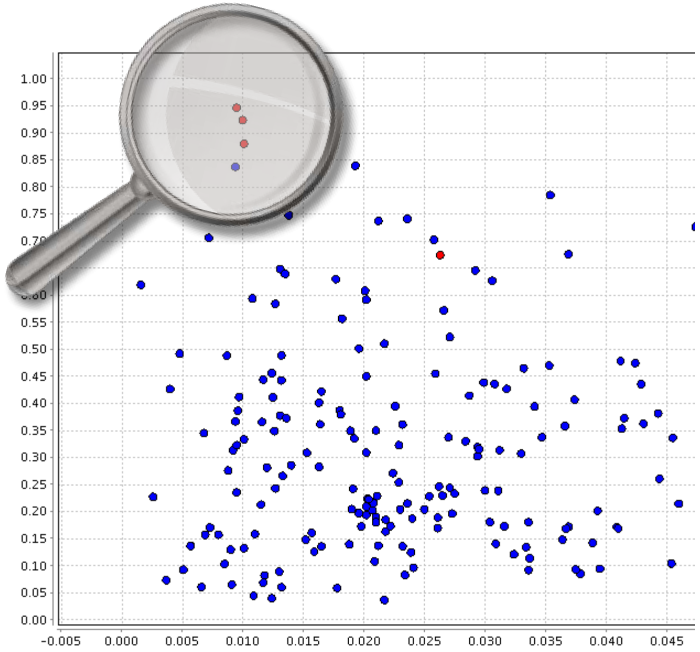
13 Feb 2014 by Matthew Prince.

Source: https://www.youtube.com/watch?v=kBBIqKeVdDo

Problem

network-traffic





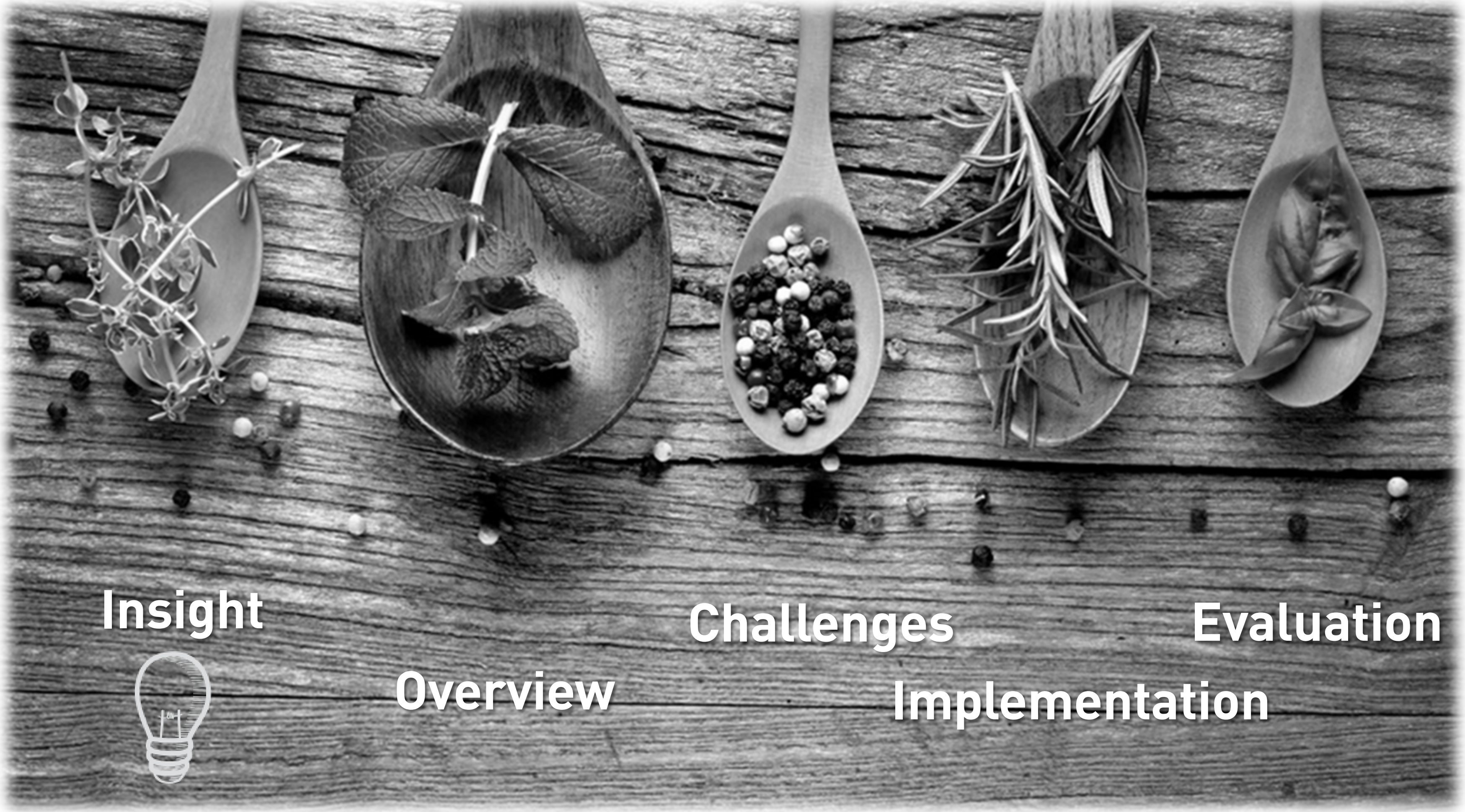
Problem

mitigation and reaction

Goal

Source: https://www.gallaudet.edu/rsia/world_deaf_information_resource.html

Ingredients



Source: http://www.mitnatur.com/wp-content/uploads//2013/11/Kochen.jpg

Insight

RQ1: Is real-time and automatic mitigation at ISP level performed and if yes, how?

Insight

Online

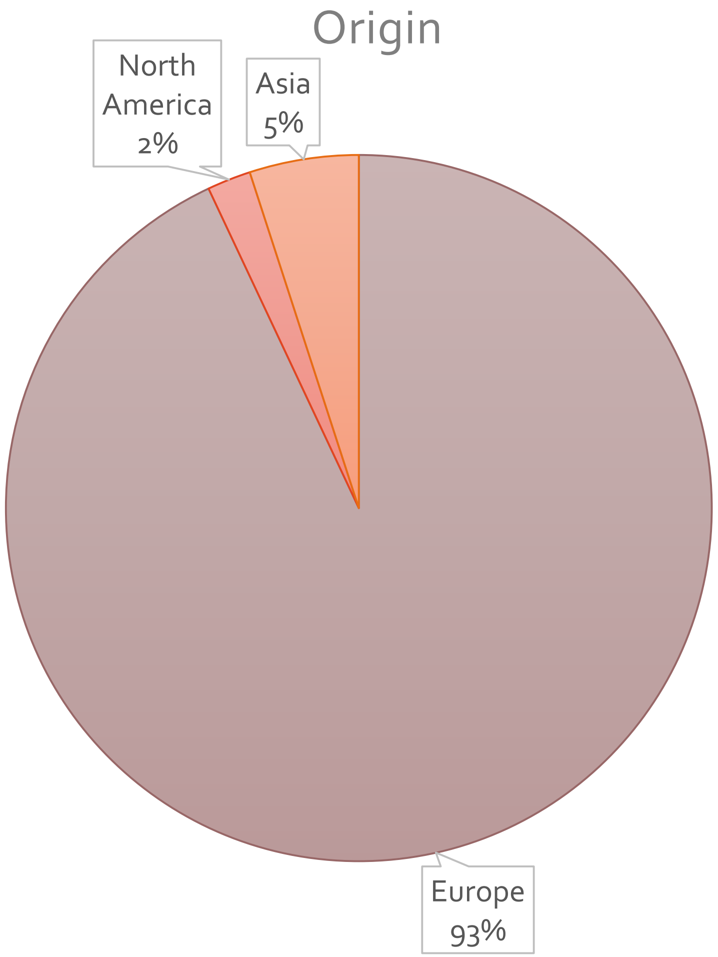
November – December 2012
May – July 2014

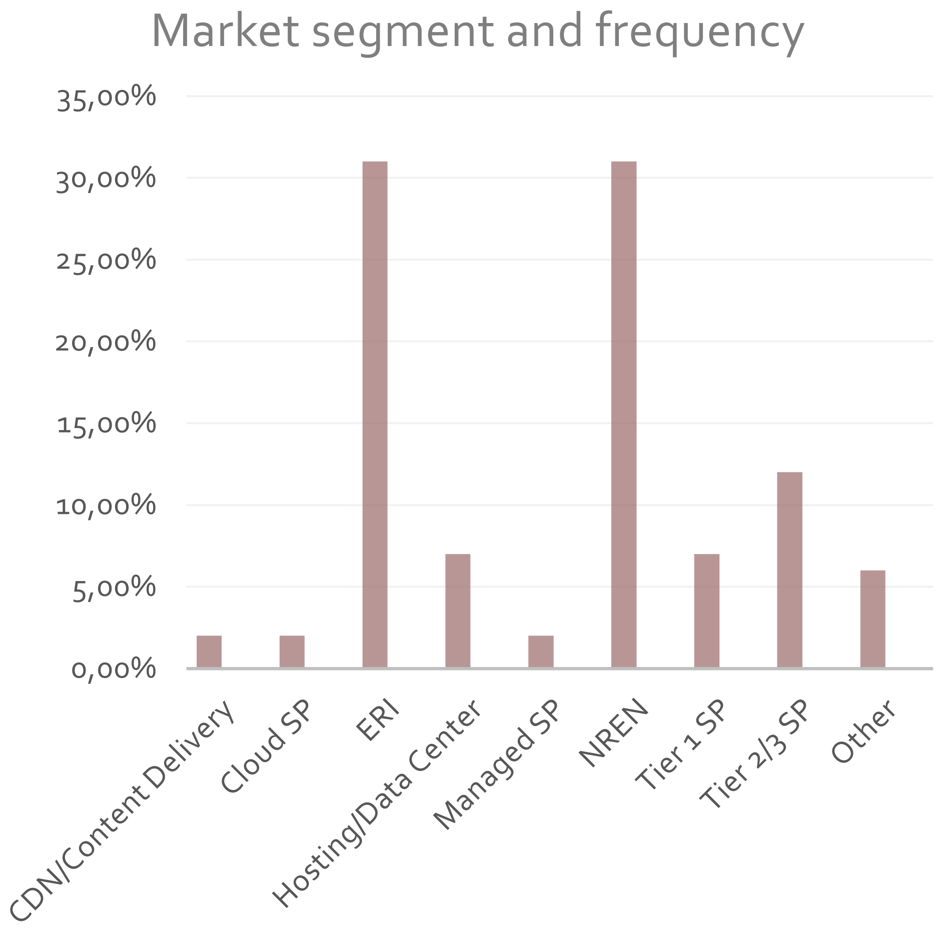
Source: http://www.pieuvre.ca/v2/wp-content/uploads/2010/01/survey.jpg

56
52

47
42

Real-time and automatic mitigation

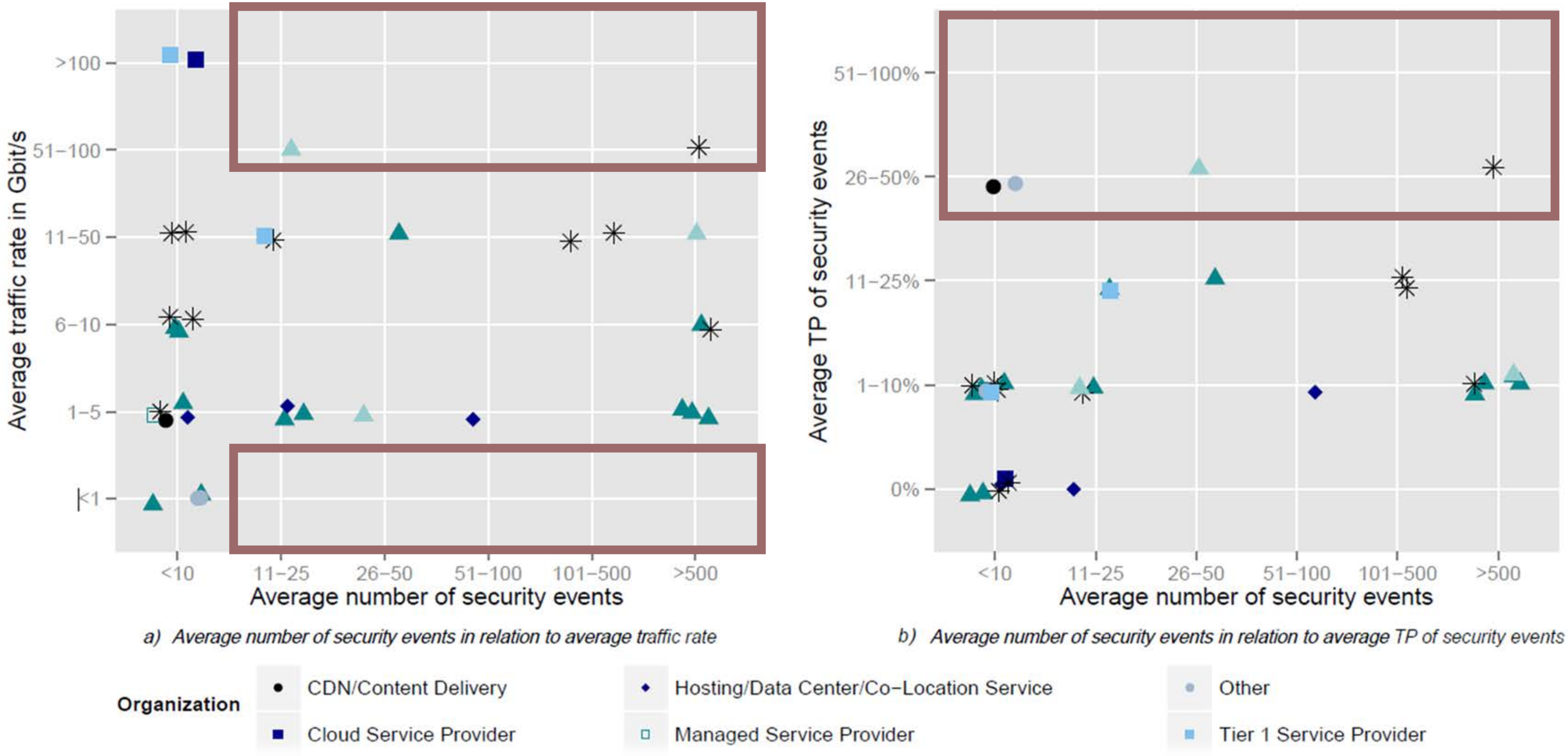




Real-time and automatic mitigation

- Process and involved third-parties
  - ISPs and CSIRTs
  - to aid NOC
  - by email or telephone

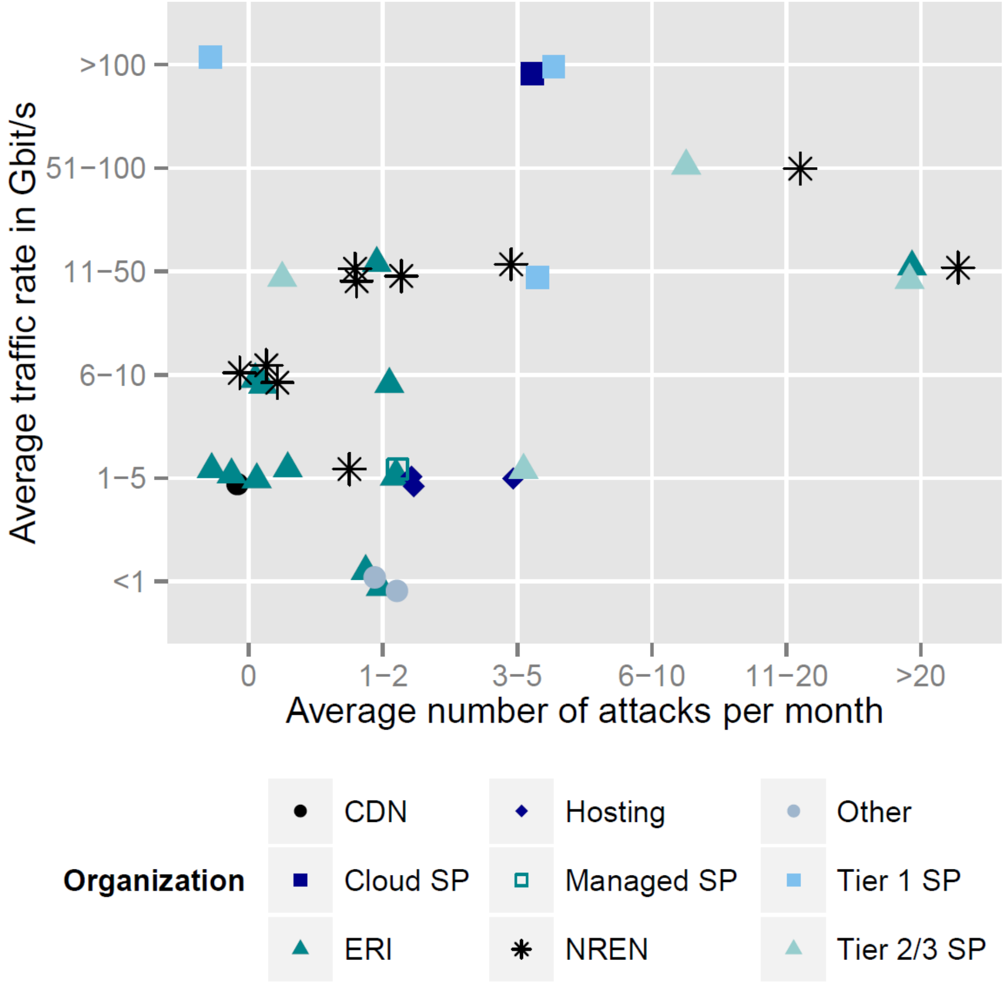
Real-time and automatic mitigation



a) Average number of security events in relation to average traffic rate

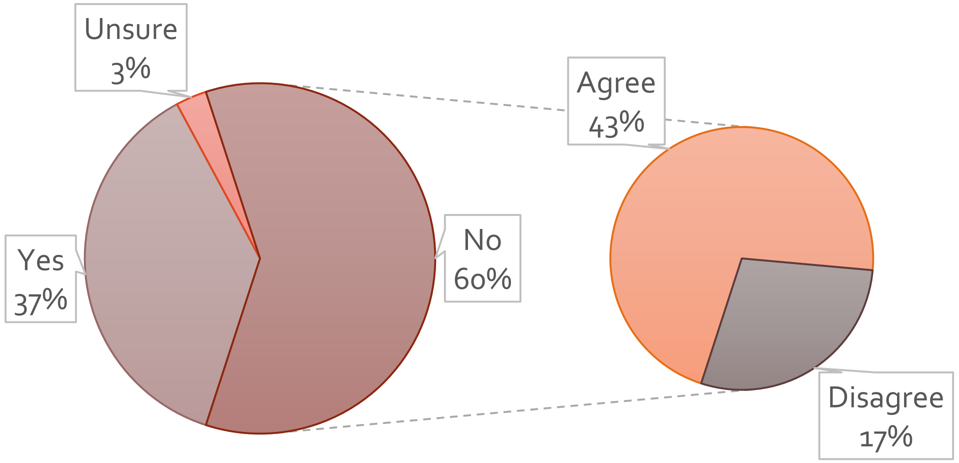
b) Average number of security events in relation to average TP of security events

Real-time and automatic mitigation

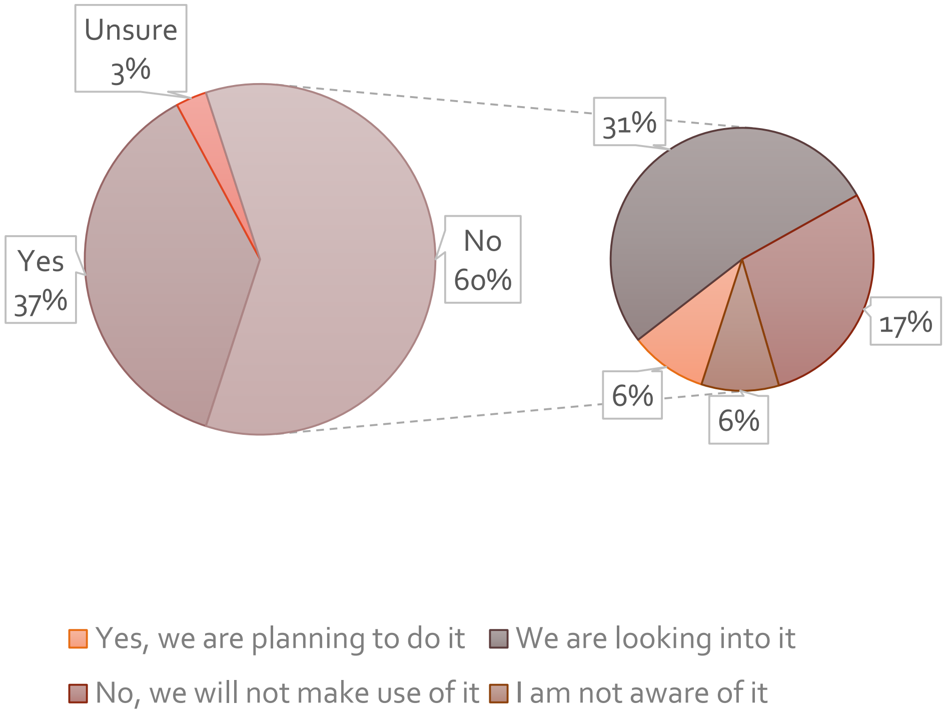


Real-time and automatic mitigation

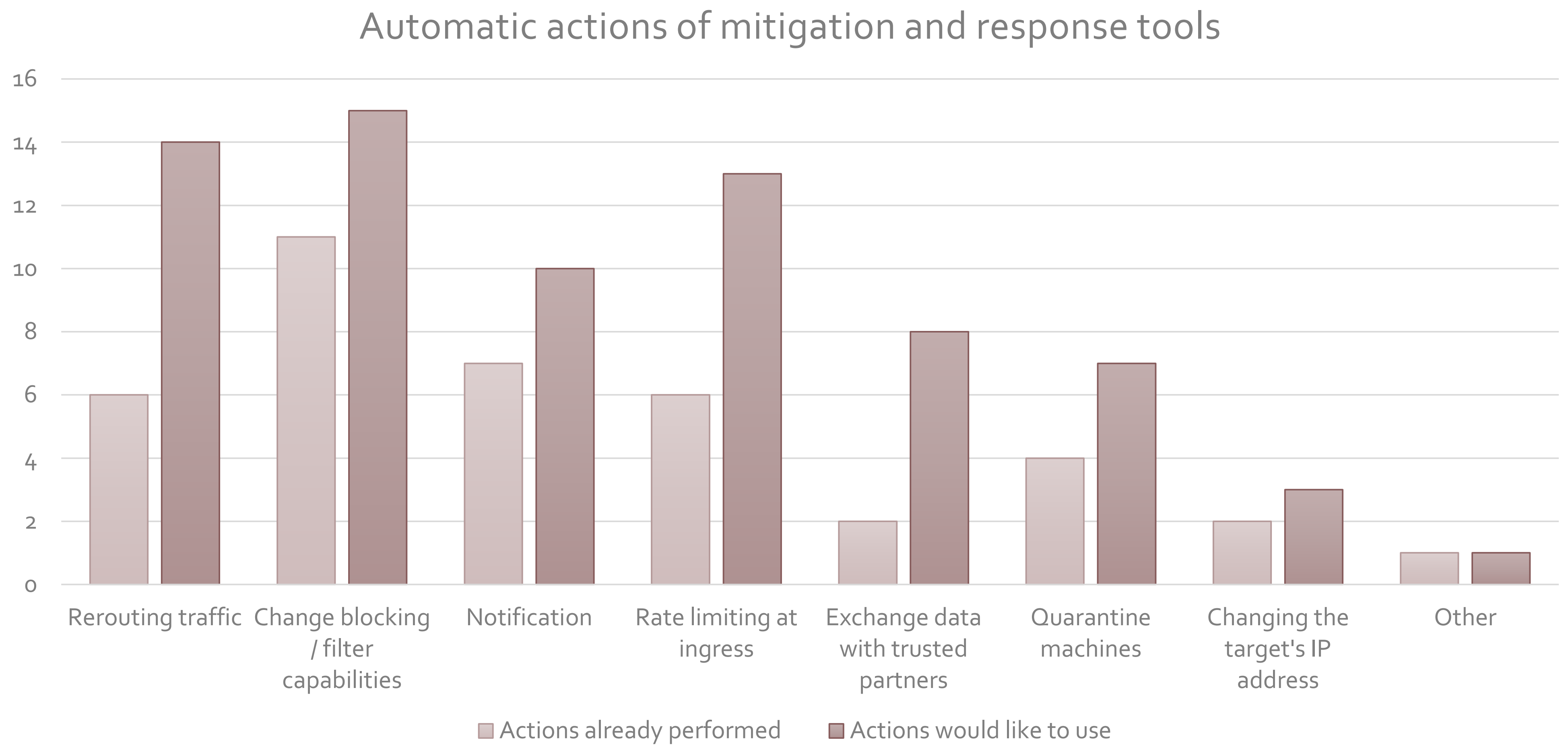
Use of automatic mitigation and response tools



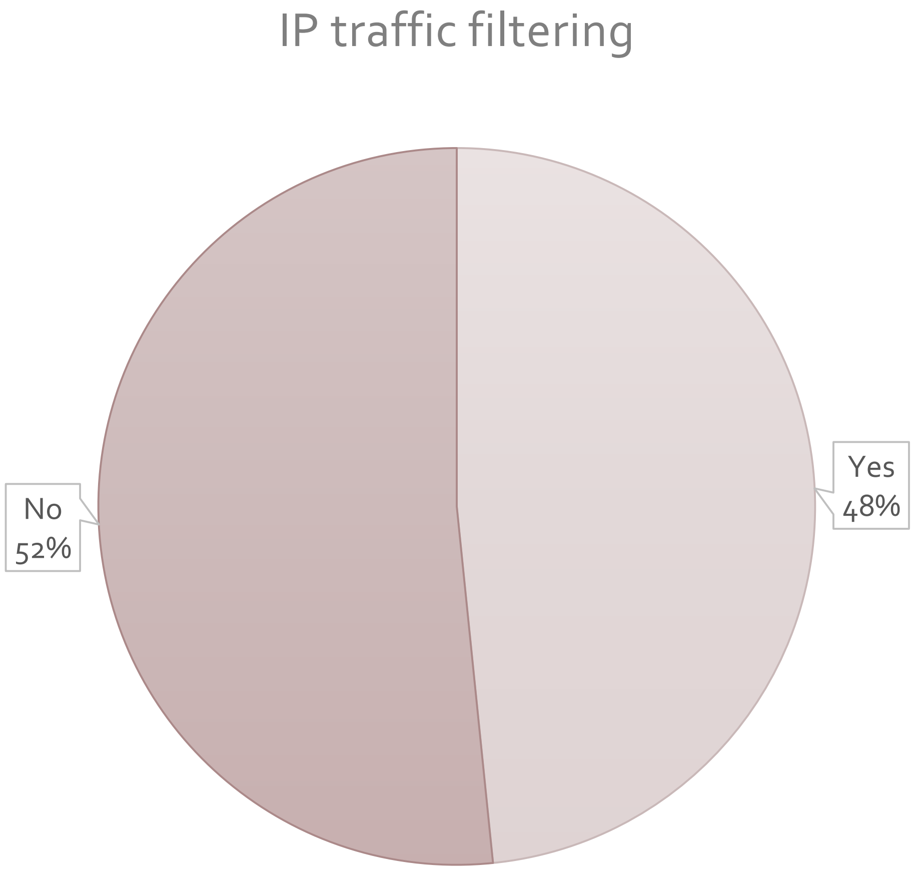
Plan of use of automatic mitigation and response tools

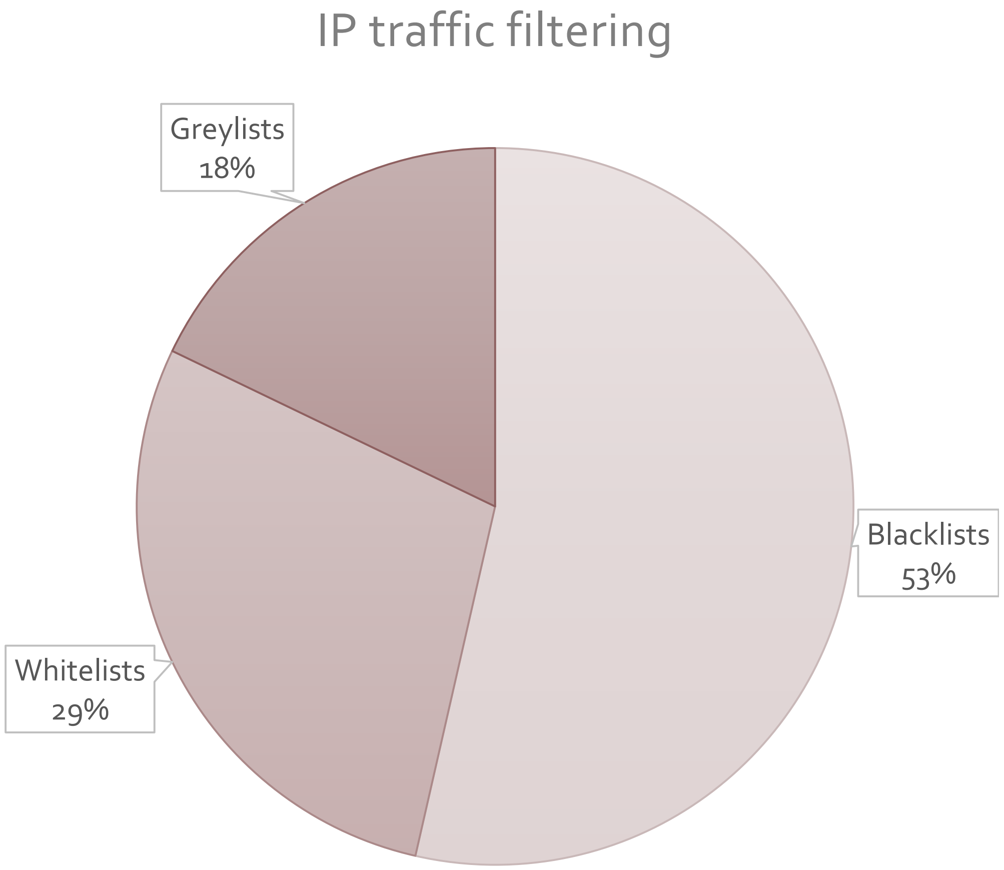


Real-time and automatic mitigation

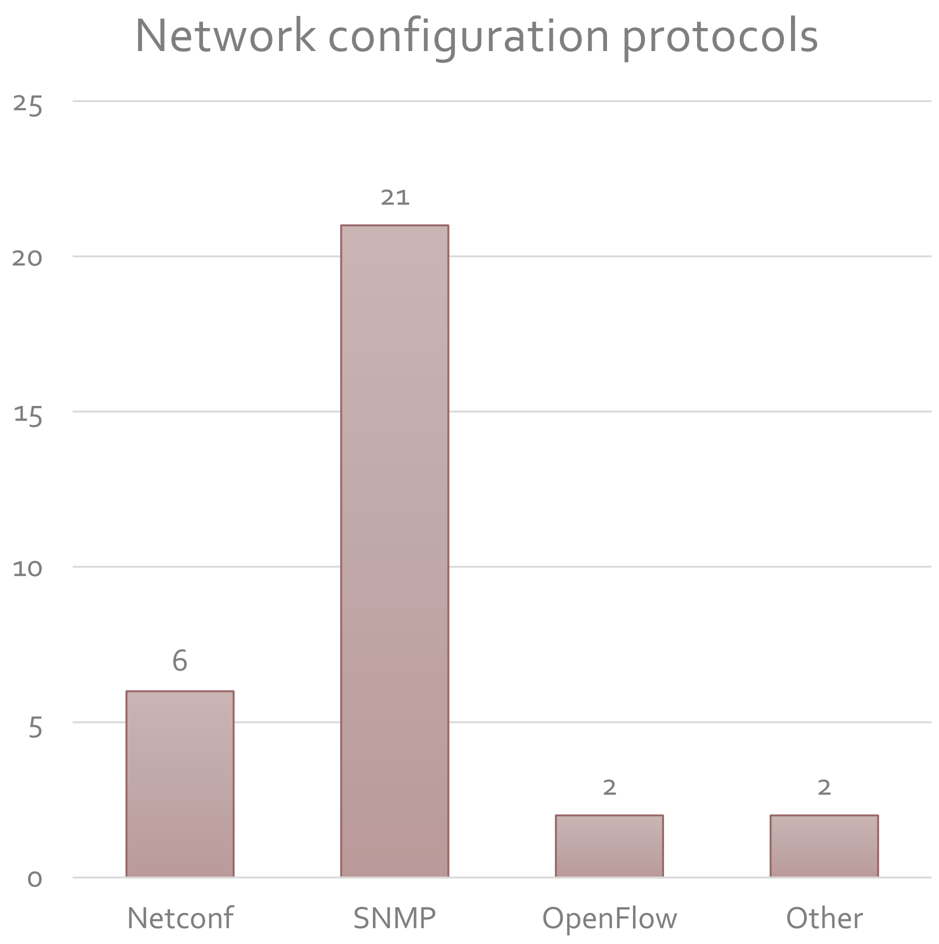


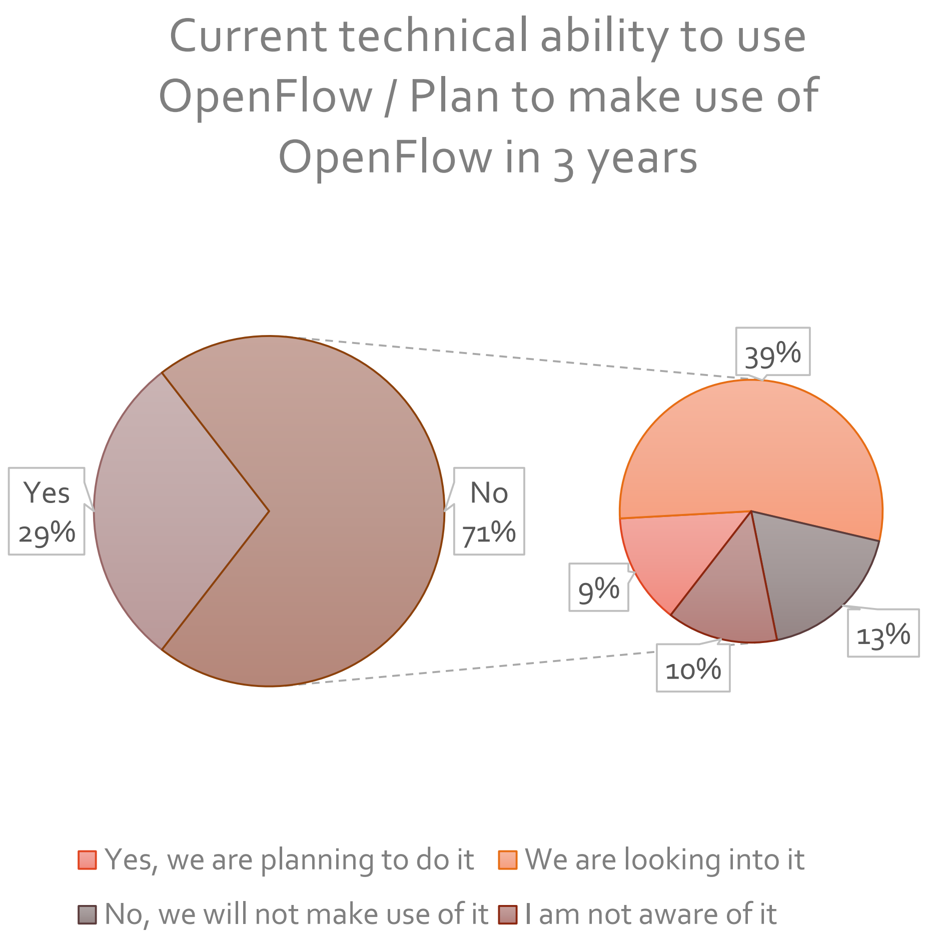
Real-time and automatic mitigation



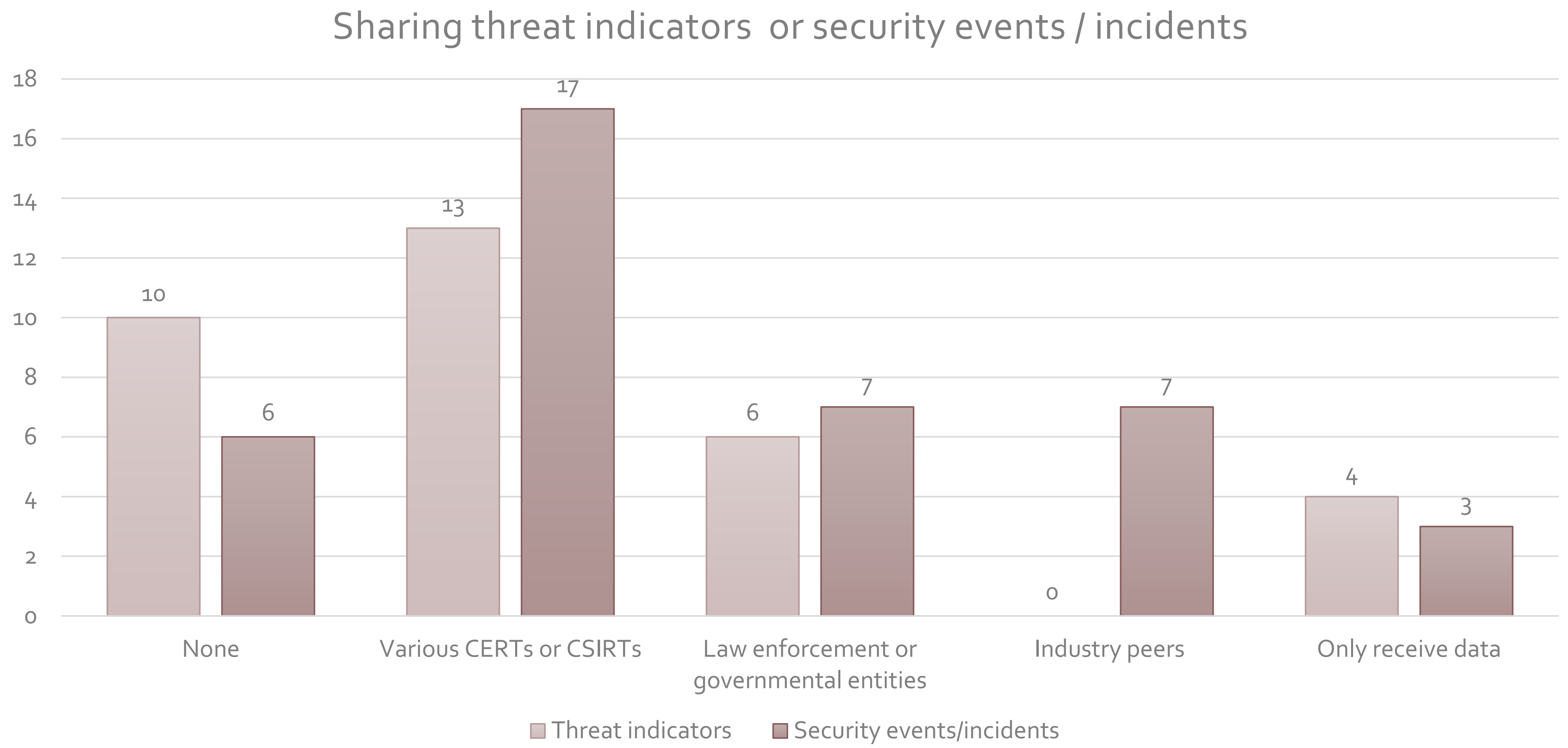


Real-time and automatic mitigation

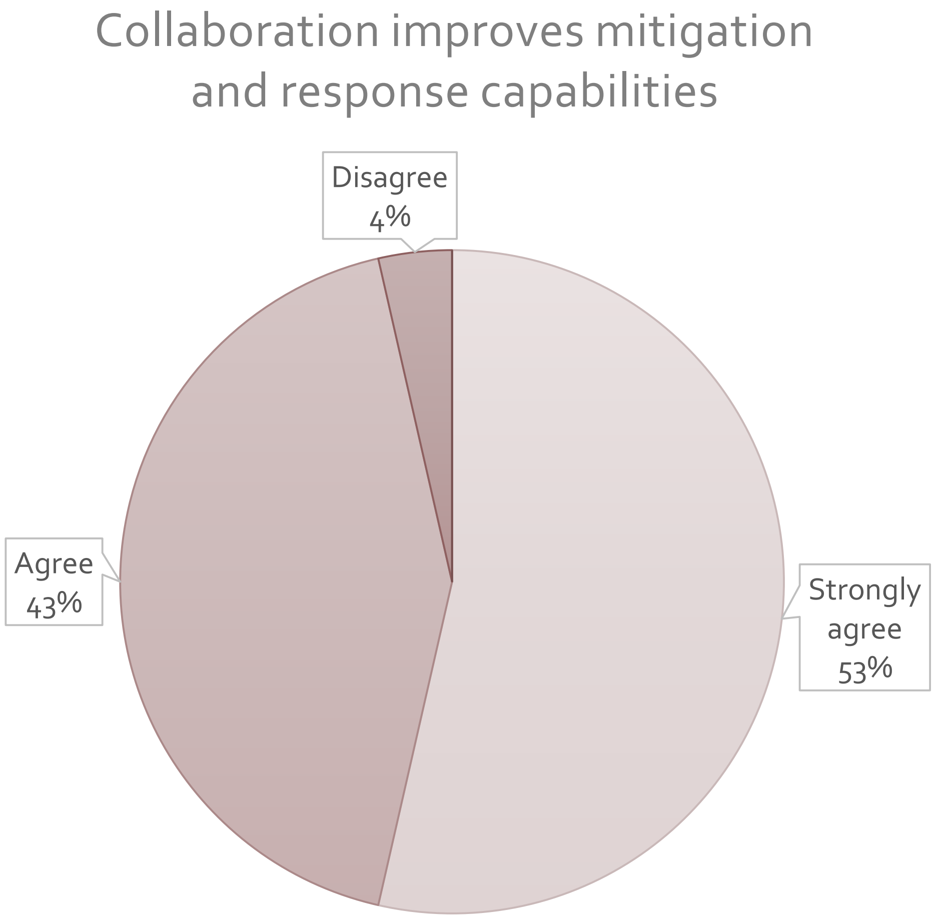

Network configuration protocols

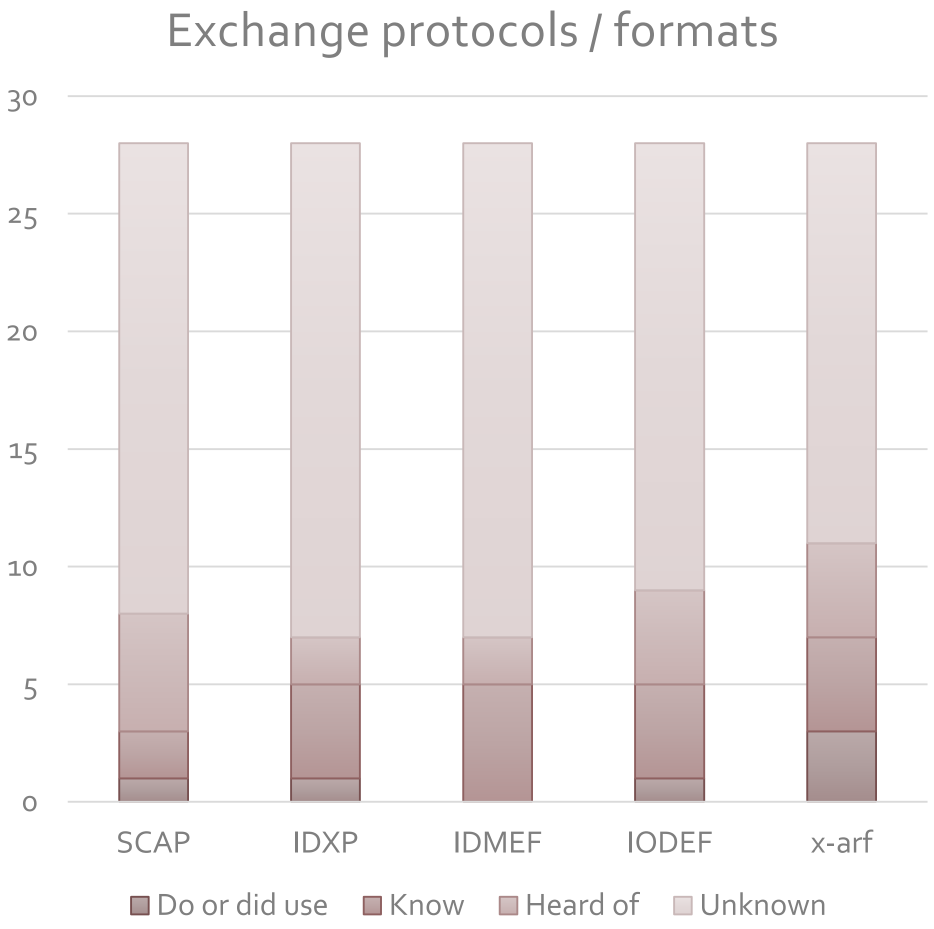

Current technical ability to use OpenFlow / Plan to make use of OpenFlow in 3 years

Real-time and automatic mitigation

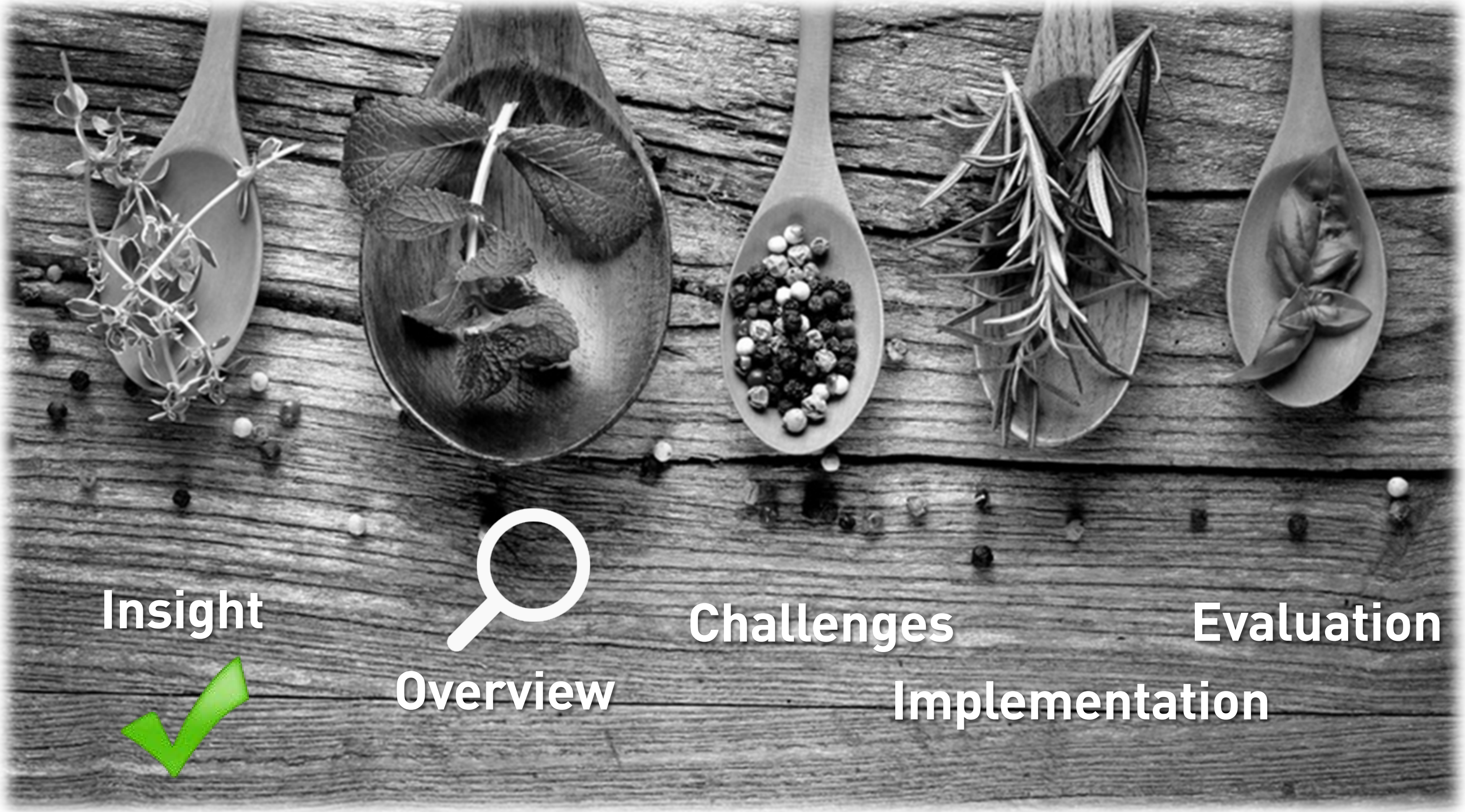


Real-time and automatic mitigation





Ingredients



Source: http://www.mitnatur.com/wp-content/uploads//2013/11/Kochen.jpg

Terminology

Format

vs.

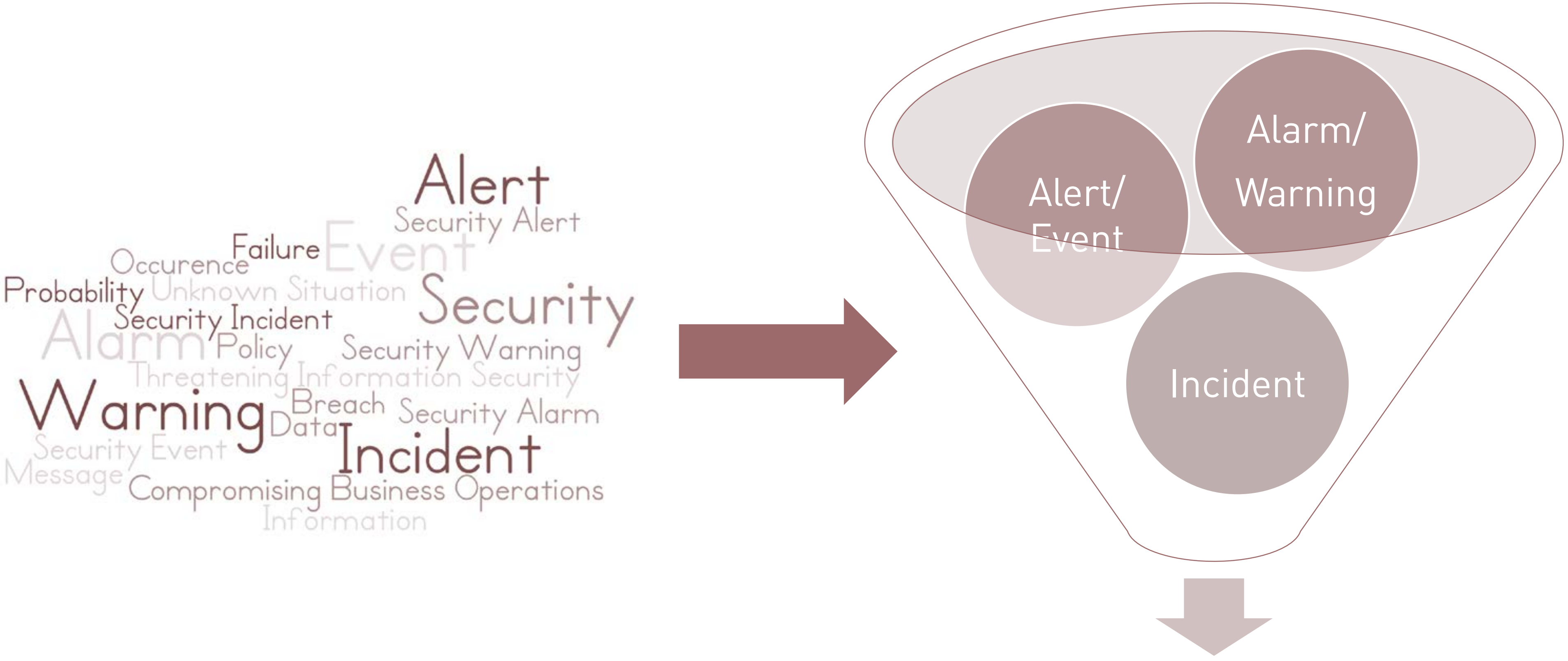
Protocol

Source: http://www.mifus.de/out/pictures/master/product/1/8000796013248_simba_sechs_sandformen.jpg
http://www.bluesource.at/2013/11/bluesource-enewsletter-november-2013/

Terminology

Alert
Security Alert
Failure
Event
Occurence
Probability
Unknown Situation
Security
Security Incident
Alarm
Policy
Security Warning
Threatening Information Security
Warning
Breach
Data
Security Alarm
Incident
Security Event
Message
Compromising Business Operations
Information

Terminology



Security Event/Incident

Terminology

Event

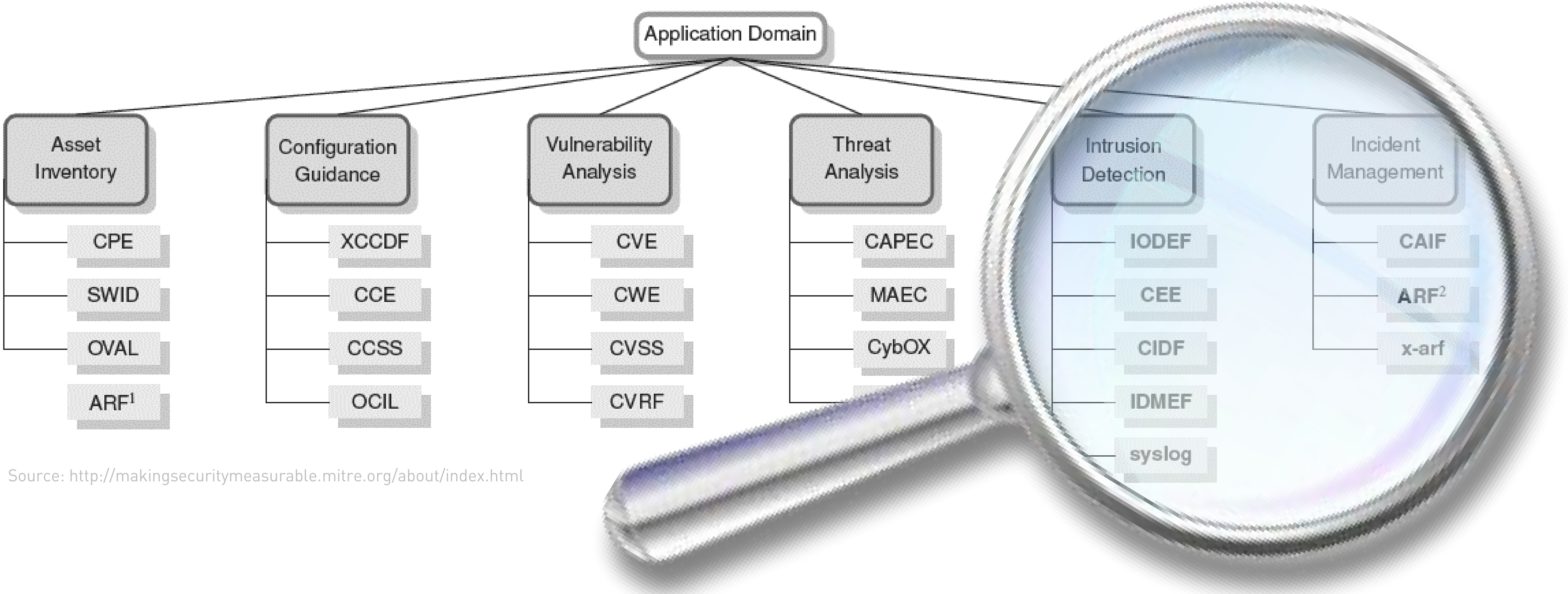
Source: http://www.hasbro.com/monopoly/de_DE/

vs.

Incident

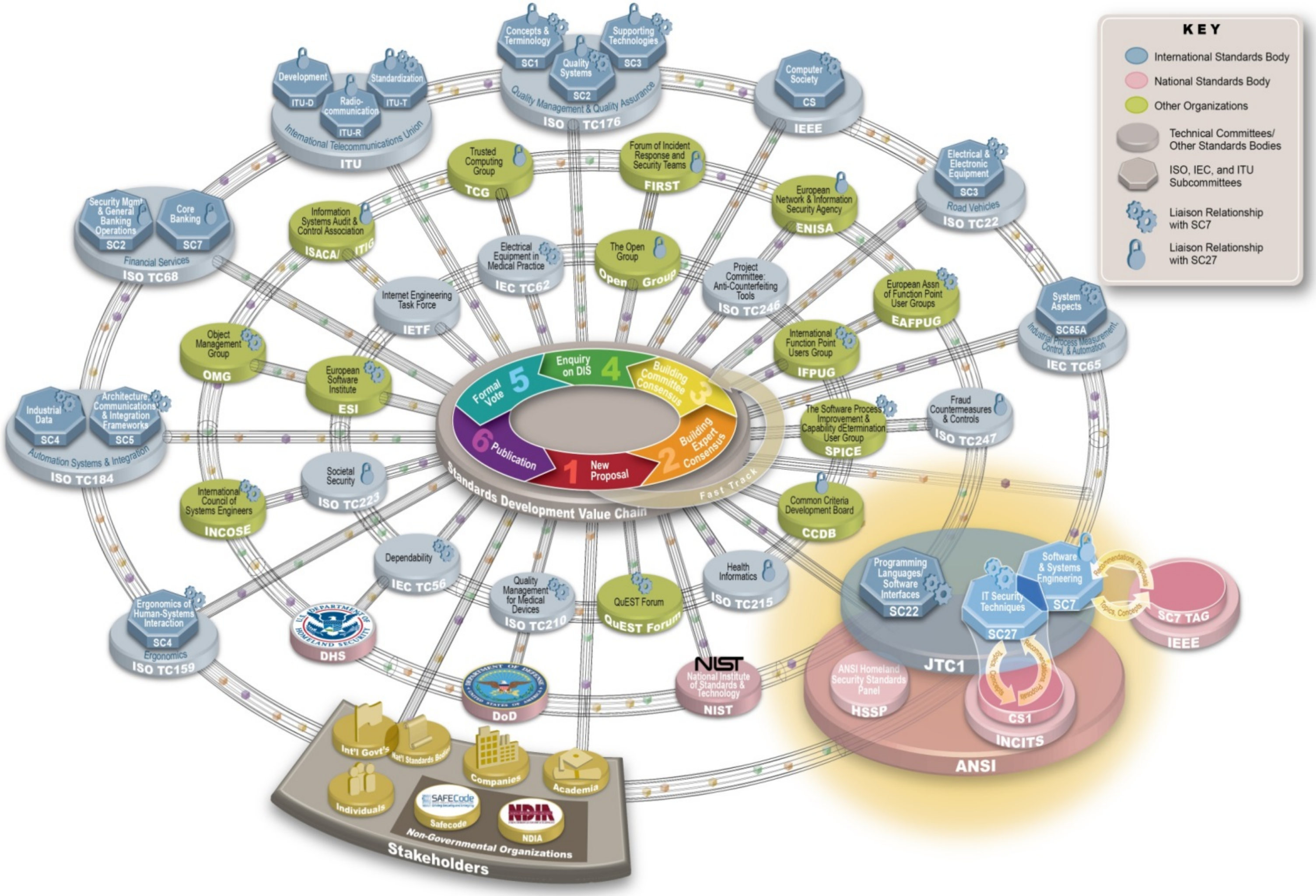
Source: http://www.bitstorm.org/journaal/2005-6/grolsch.jpg

Application Domain



Source: http://makingsecuritymeasurable.mitre.org/about/index.html

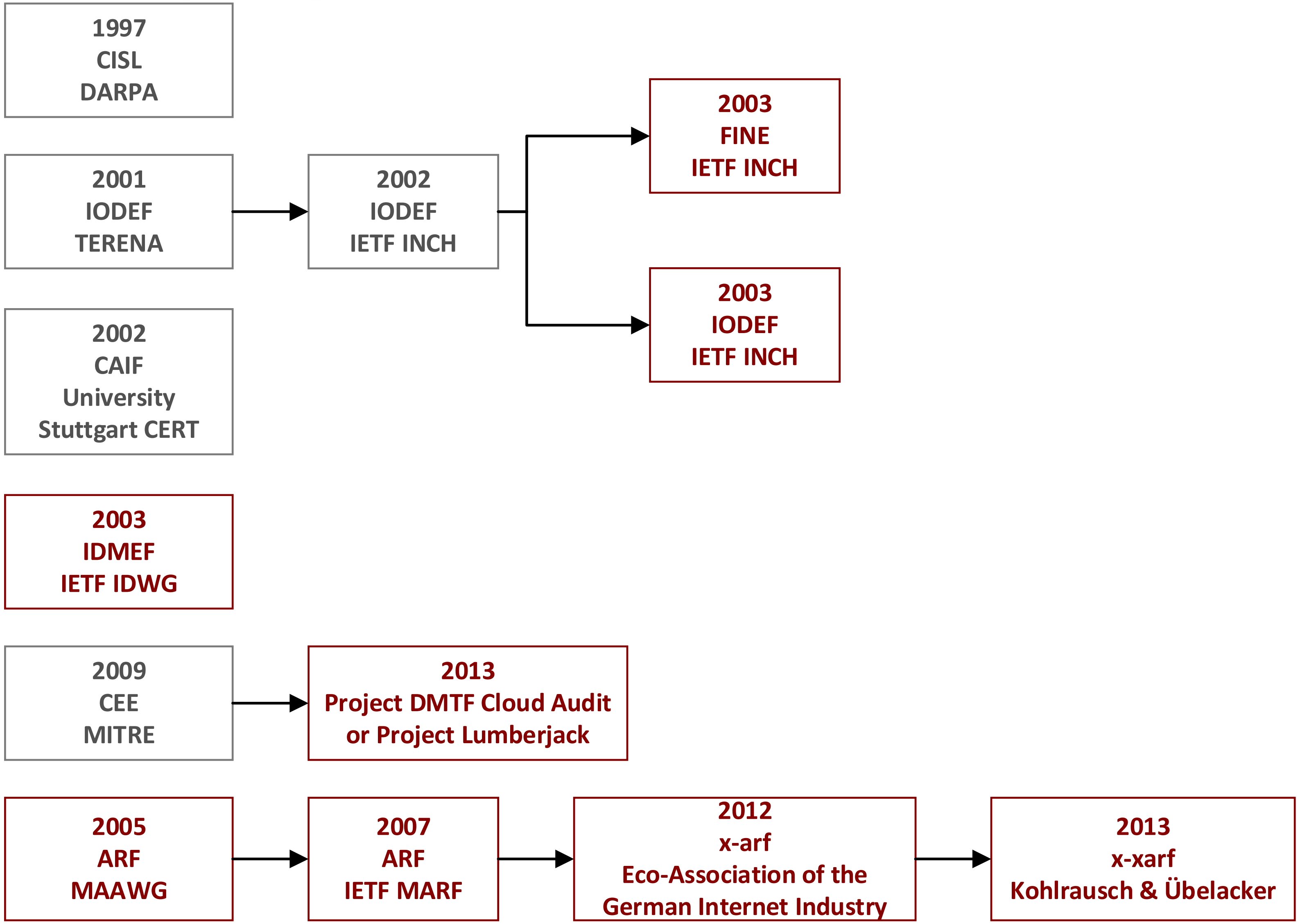
Who is involved ?


KEY
International Standards Body
National Standards Body
Other Organizations
Technical Committees/ Other Standards Bodies
ISO, IEC, and ITU Subcommittees
Liaison Relationship with SC7
Liaison Relationship with SC27
Concepts & Terminology
SC1
Quality Systems
SC2
Supporting Technologies
SC3
Quality Management & Quality Assurance
ISO TC176
Development
ITU-D
Radio-communication
ITU-R
Standardization
ITU-T
International Telecommunications Union
ITU
Computer Society
CS
IEEE
Electrical & Electronic Equipment
SC3
Road Vehicles
ISO TC22
Security Mgmt & General Banking Operations
SC2
Core Banking
SC7
Financial Services
ISO TC68
Trusted Computing Group
TCG
Forum of Incident Response and Security Teams
FIRST
European Network & Information Security Agency
ENISA
Information Systems Audit & Control Association
ISACA
ITIG
Electrical Equipment in Medical Practice
IEC TC62
The Open Group
Open Group
Project Committee: Anti-Counterfeiting Tools
ISO TC246
European Assn of Function Point User Groups
EAFPUG
System Aspects
SC65A
Industrial Process Measurement, Control, & Automation
IEC TC65
Internet Engineering Task Force
IETF
Object Management Group
OMG
European Software Institute
ESI
International Function Point Users Group
IFPUG
Industrial Data
SC4
Architecture, Communications & Integration Frameworks
SC5
Automation Systems & Integration
ISO TC184
Formal Vote
5
Enquiry on DIS
4
Building Committee Consensus
3
Building Expert Consensus
2
New Proposal
1
Publication
6
Standards Development Value Chain
Fast Track
The Software Process Improvement & Capability dEtermination User Group
SPICE
Fraud Countermeasures & Controls
ISO TC247
Societal Security
ISO TC223
International Council of Systems Engineers
INCOSE
Common Criteria Development Board
CCDB
Dependability
IEC TC56
Quality Management for Medical Devices
ISO TC210
QuEST Forum
QuEST Forum
Health Informatics
ISO TC215
Ergonomics of Human-Systems Interaction
SC4
Ergonomics
ISO TC159
DHS
DoD
NIST
National Institute of Standards & Technology
NIST
Programming Languages, Software Interfaces
SC22
IT Security Techniques
SC27
Software & Systems Engineering
SC7
SC7 TAG
IEEE
JTC1
ANSI Homeland Security Standards Panel
HSSP
CS1
INCITS
ANSI
Int'l Gov'ts
Nat'l Standards Bodies
Companies
Academia
Individuals
SAFECode
Safecode
NDIA
NDIA
Non-Governmental Organizations
Stakeholders

- US governments Defense Advance Research Projects Agency (DARPA)
- TERENA
- IETF Incident Handling
- Stuttgart University's CERT
- IETF IDWG
- MITRE
- IETF MARF
- Eco – Association of the German Internet Industry

Source: http://m.crosstalkonline.org/media/cache/54/c8/54c83f7398d4ee4bece7c84e899c8a64.jpg

Timeline



1997
CISL
DARPA

2001
IODEF
TERENA

2002
IODEF
IETF INCH

2003
FINE
IETF INCH

2003
IODEF
IETF INCH

2002
CAIF
University
Stuttgart CERT

2003
IDMEF
IETF IDWG

2009
CEE
MITRE

2013
Project DMTF Cloud Audit
or Project Lumberjack

2005
ARF
MAAWG

2007
ARF
IETF MARF

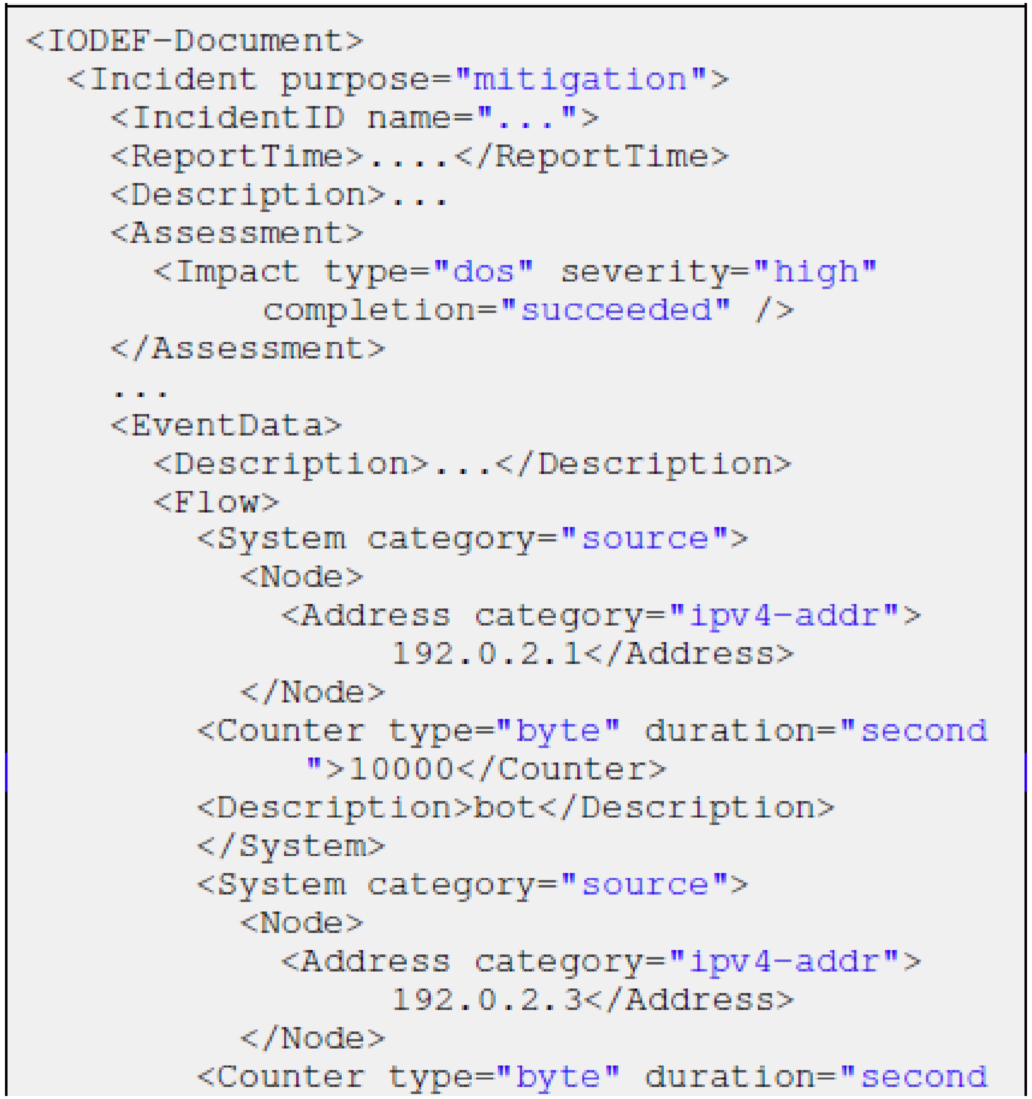
2012
x-arf
Eco-Association of the
German Internet Industry

2013
x-xarf
Kohlrausch & Übelacker

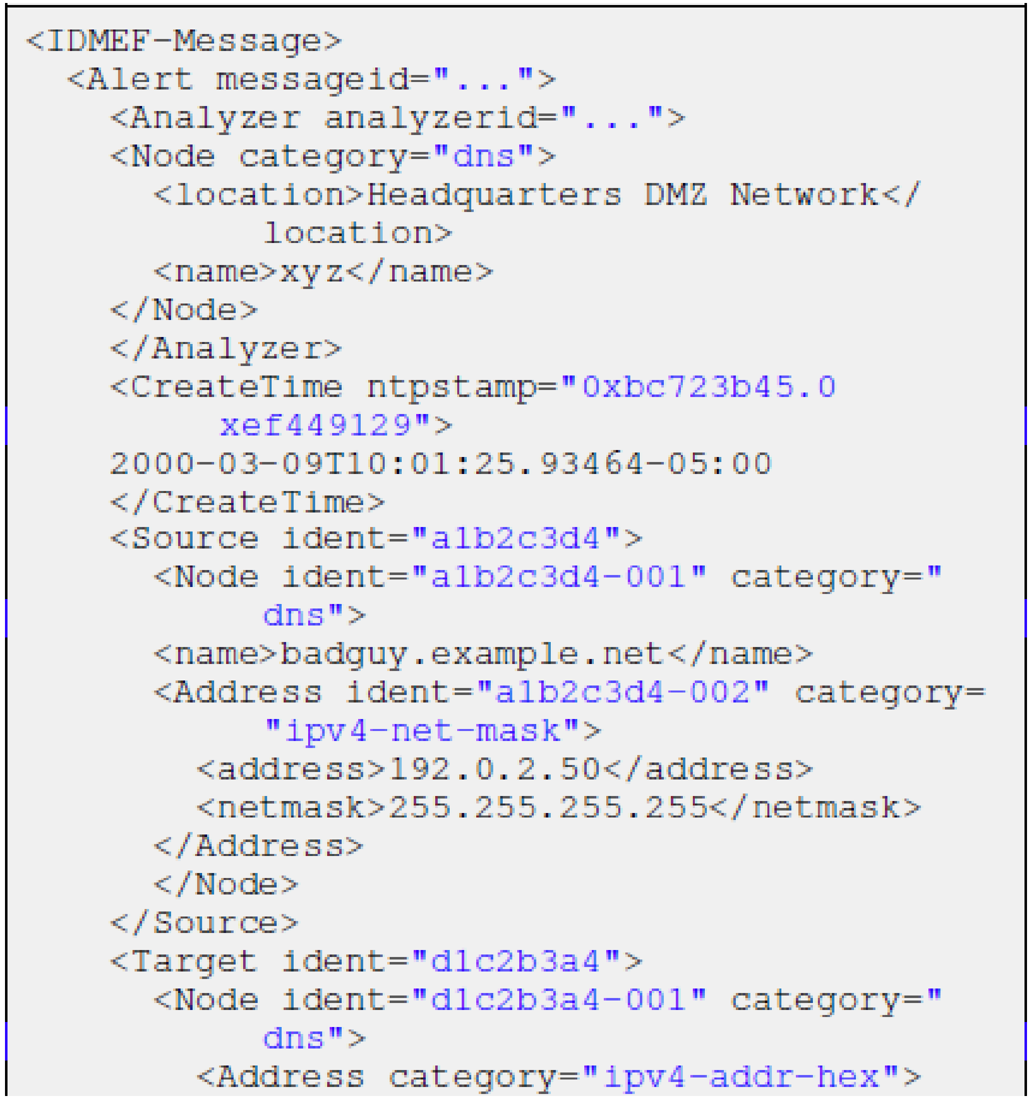
Exchange formats

	CISL	IODEF	CAIF	IDMEF	CEE	ARF	x-arf/x-xarf	syslog
Language	S-expressions	XML	XML	XML	XML, JSON	MIME	MIME	Text/XML
Content	Events, Attacks, Responses	Events, Incidents	Problem, Vulnerability, Exposure	Alerts, Alive messages	Events	Spam	Incidents, Attacks	Events
Producer	Machine	Human	Human	Machine	Machine	Machine	Machine	Machine
Consumer	Machine	Human	Human	Machine	Human	Machine/ Human	Machine/Human	Machine/ Human

IODEF vs. IDMEF

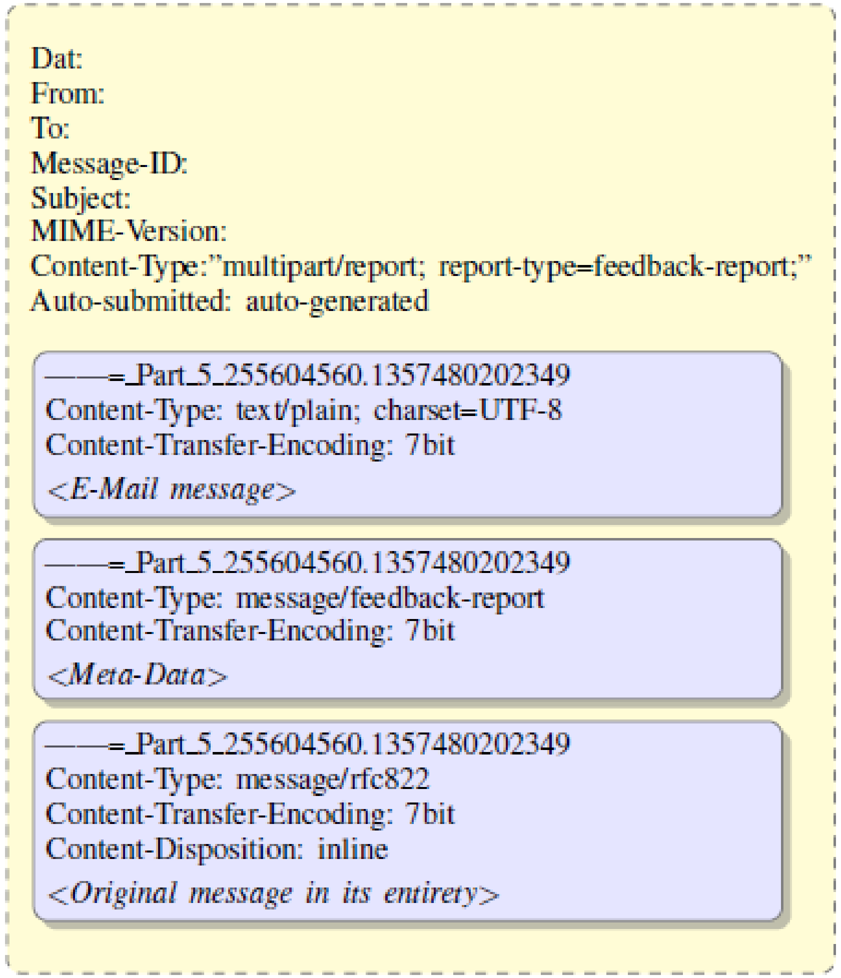


```
<IODEF-Document>
  <Incident purpose="mitigation">
    <IncidentID name="...">
    <ReportTime>....</ReportTime>
    <Description>...
    <Assessment>
      <Impact type="dos" severity="high"
           completion="succeeded" />
    </Assessment>
    ...
    <EventData>
      <Description>...</Description>
      <Flow>
        <System category="source">
          <Node>
            <Address category="ipv4-addr">
                 192.0.2.1</Address>
          </Node>
        <Counter type="byte" duration="second
             ">10000</Counter>
        <Description>bot</Description>
        </System>
        <System category="source">
          <Node>
            <Address category="ipv4-addr">
                 192.0.2.3</Address>
          </Node>
        <Counter type="byte" duration="second
```



```
<IDMEF-Message>
  <Alert messageid="...">
    <Analyzer analyzerid="...">
    <Node category="dns">
      <location>Headquarters DMZ Network</
           location>
      <name>xyz</name>
    </Node>
    </Analyzer>
    <CreateTime ntpstamp="0xbc723b45.0
         xef449129">
    2000-03-09T10:01:25.93464-05:00
    </CreateTime>
    <Source ident="a1b2c3d4">
      <Node ident="a1b2c3d4-001" category="
           dns">
      <name>badguy.example.net</name>
      <Address ident="a1b2c3d4-002" category=
           "ipv4-net-mask">
        <address>192.0.2.50</address>
        <netmask>255.255.255.255</netmask>
      </Address>
      </Node>
    </Source>
    <Target ident="d1c2b3a4">
      <Node ident="d1c2b3a4-001" category="
           dns">
        <Address category="ipv4-addr-hex">
```

ARF vs. x-xarf

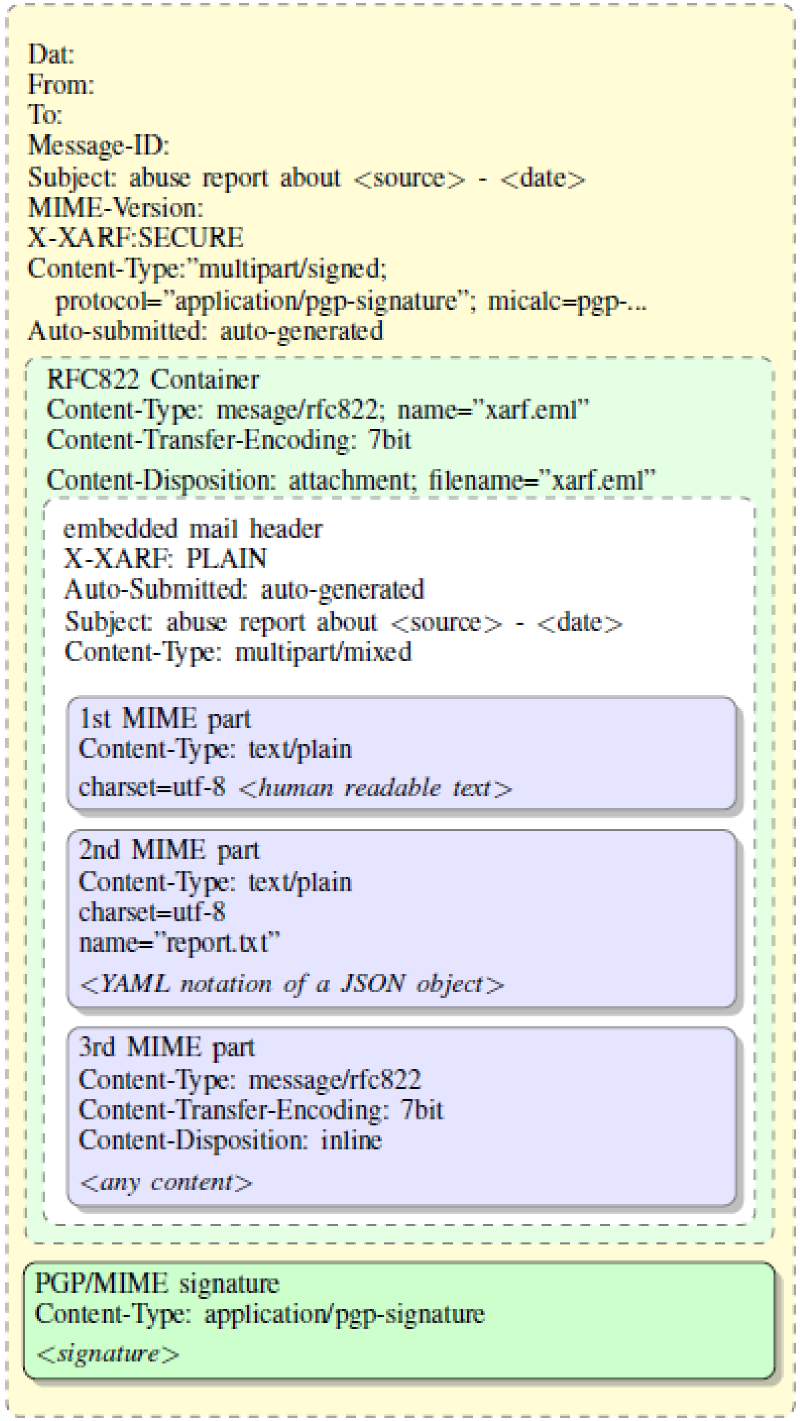


Dat:
From:
To:
Message-ID:
Subject:
MIME-Version:
Content-Type:"multipart/report; report-type=feedback-report;"
Auto-submitted: auto-generated

——=_Part_5_255604560.1357480202349
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit
<E-Mail message>

——=_Part_5_255604560.1357480202349
Content-Type: message/feedback-report
Content-Transfer-Encoding: 7bit
<Meta-Data>

——=_Part_5_255604560.1357480202349
Content-Type: message/rfc822
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
<Original message in its entirety>



Dat:
From:
To:
Message-ID:
Subject: abuse report about <source> - <date>
MIME-Version:
X-XARF:SECURE
Content-Type:"multipart/signed;
protocol="application/pgp-signature"; micalc=pgp-...
Auto-submitted: auto-generated

RFC822 Container
Content-Type: mesage/rfc822; name="xarf.eml"
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="xarf.eml"

embedded mail header
X-XARF: PLAIN
Auto-Submitted: auto-generated
Subject: abuse report about <source> - <date>
Content-Type: multipart/mixed

1st MIME part
Content-Type: text/plain
charset=utf-8 *<human readable text>*

2nd MIME part
Content-Type: text/plain
charset=utf-8
name="report.txt"
<YAML notation of a JSON object>

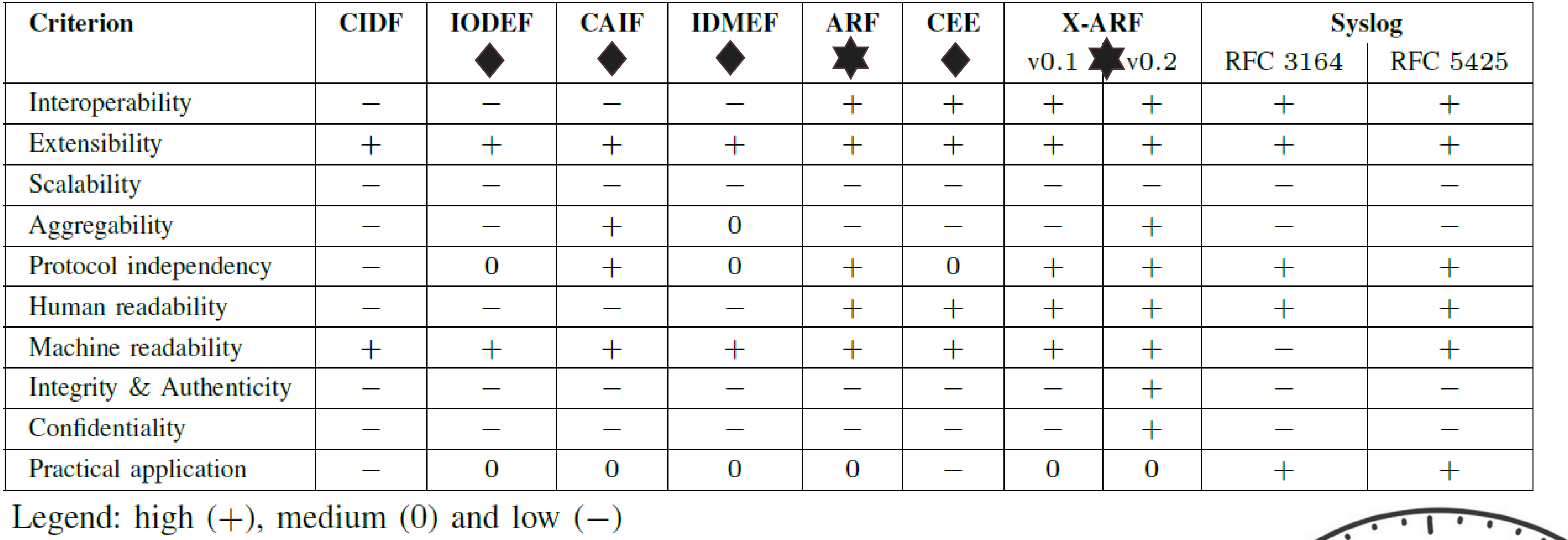
3rd MIME part
Content-Type: message/rfc822
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
<any content>

PGP/MIME signature
Content-Type: application/pgp-signature
<signature>

Exchange formats and protocols

Protocol	OSI layer	Format	Security
CIDF	Transport	CISL message	Symmetric Cryptography
RID	Application	IODEF	TLS
XEP-0268	Application	IODEF	TLS
IDXP	Application	IDMEF	TLS
CLT	Transport	CEE	Provided by syslog (RFC 5425)
SMTP	Application	CAIF ARF x-arf	None S/MIME Multipart/Signed Multipart/Encrypted
Syslog (RFC 3164)	Transport	Syslog (RFC 3164)	None
Syslog (RFC 5425)	Transport	Syslog (RFC 5424)	TLS

Evaluation results



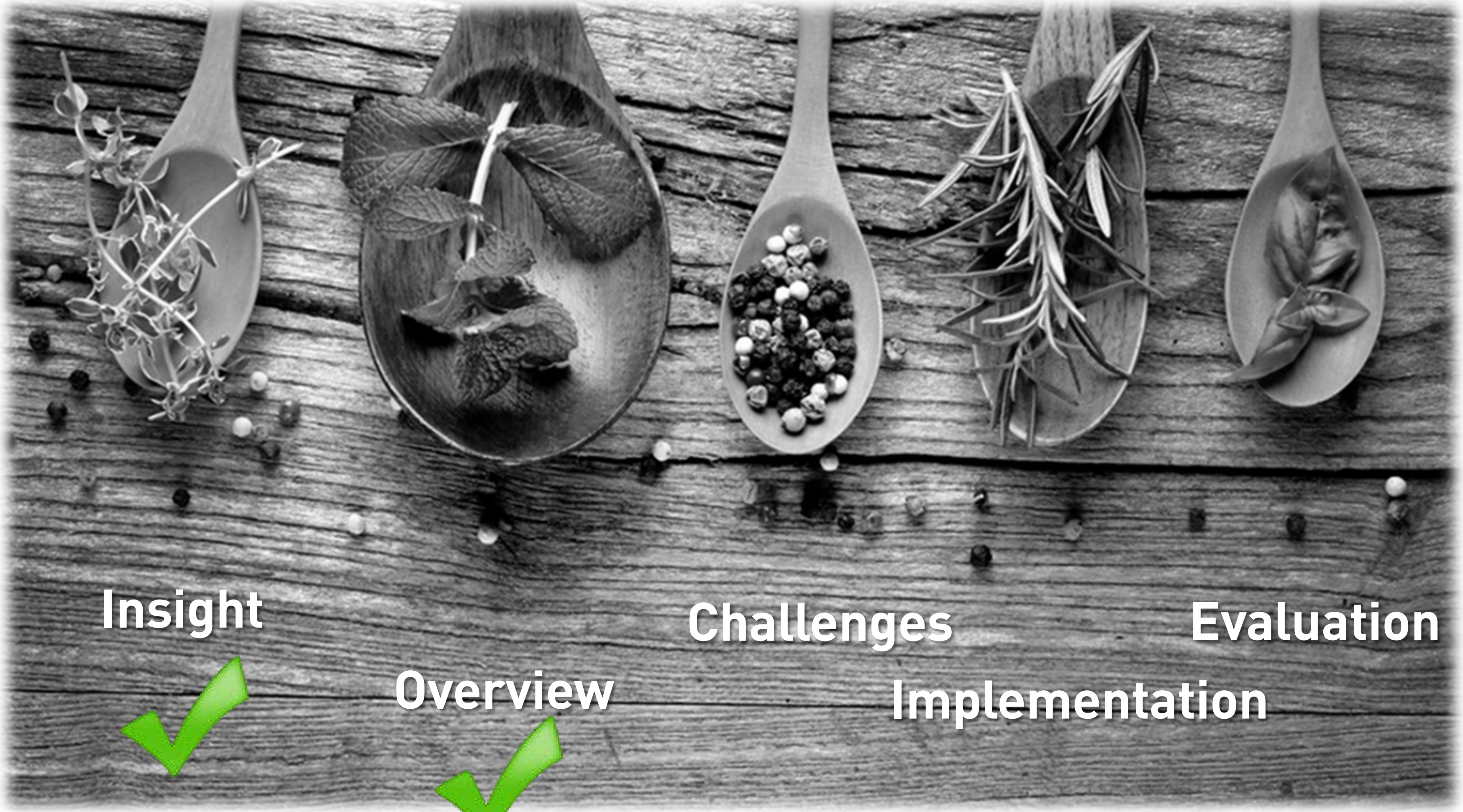
Criterion	CIDF	IODEF ◆	CAIF ◆	IDMEF ◆	ARF ✶	CEE ◆	X-ARF ✶		Syslog	
							v0.1	v0.2	RFC 3164	RFC 5425
Interoperability	–	–	–	–	+	+	+	+	+	+
Extensibility	+	+	+	+	+	+	+	+	+	+
Scalability	–	–	–	–	–	–	–	–	–	–
Aggregability	–	–	+	0	–	–	–	+	–	–
Protocol independency	–	0	+	0	+	0	+	+	+	+
Human readability	–	–	–	–	+	+	+	+	+	+
Machine readability	+	+	+	+	+	+	+	+	–	+
Integrity & Authenticity	–	–	–	–	–	–	–	+	–	–
Confidentiality	–	–	–	–	–	–	–	+	–	–
Practical application	–	0	0	0	0	–	0	0	+	+

Legend: high (+), medium (0) and low (–)

◆ XML

✶ MIME

Ingredients



Insight ✓

Overview ✓

Challenges

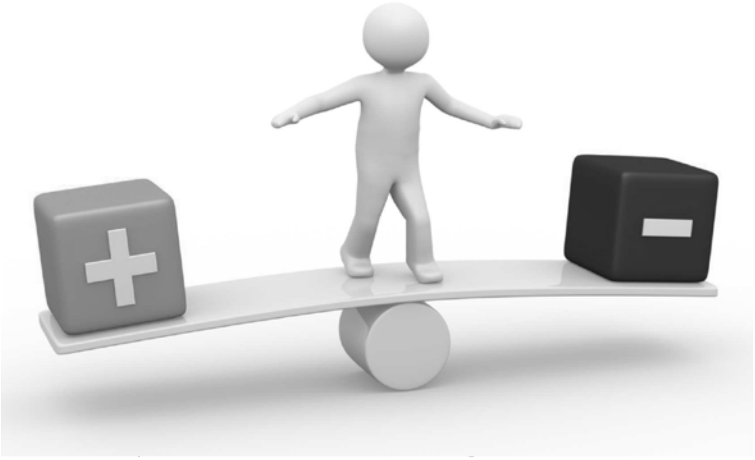
Implementation

Evaluation

Source: http://www.mitnatur.com/wp-content/uploads//2013/11/Kochen.jpg

Challenges

„rogue ISPs“



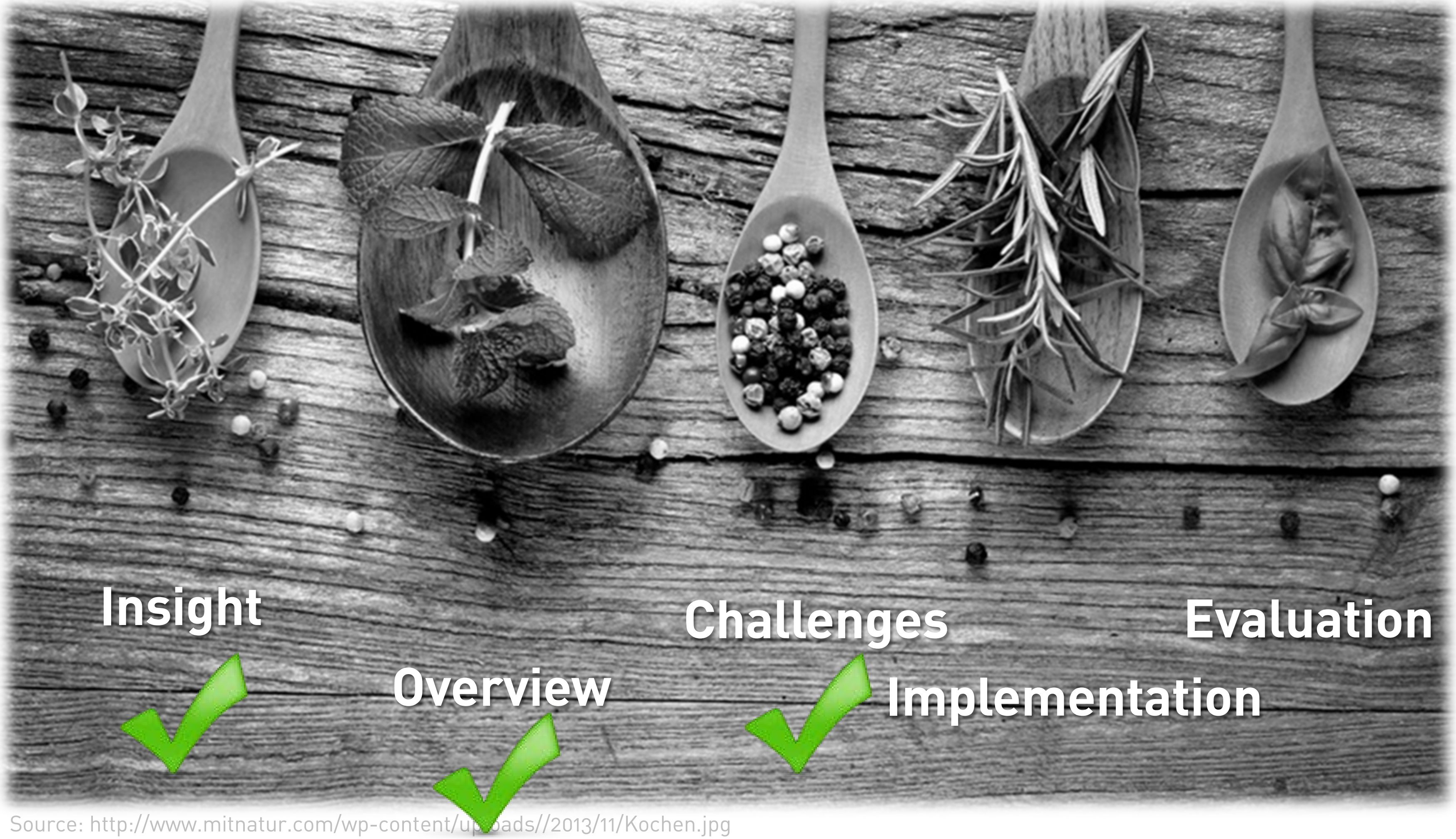
Quantifying cost/benefit

FP

Risk

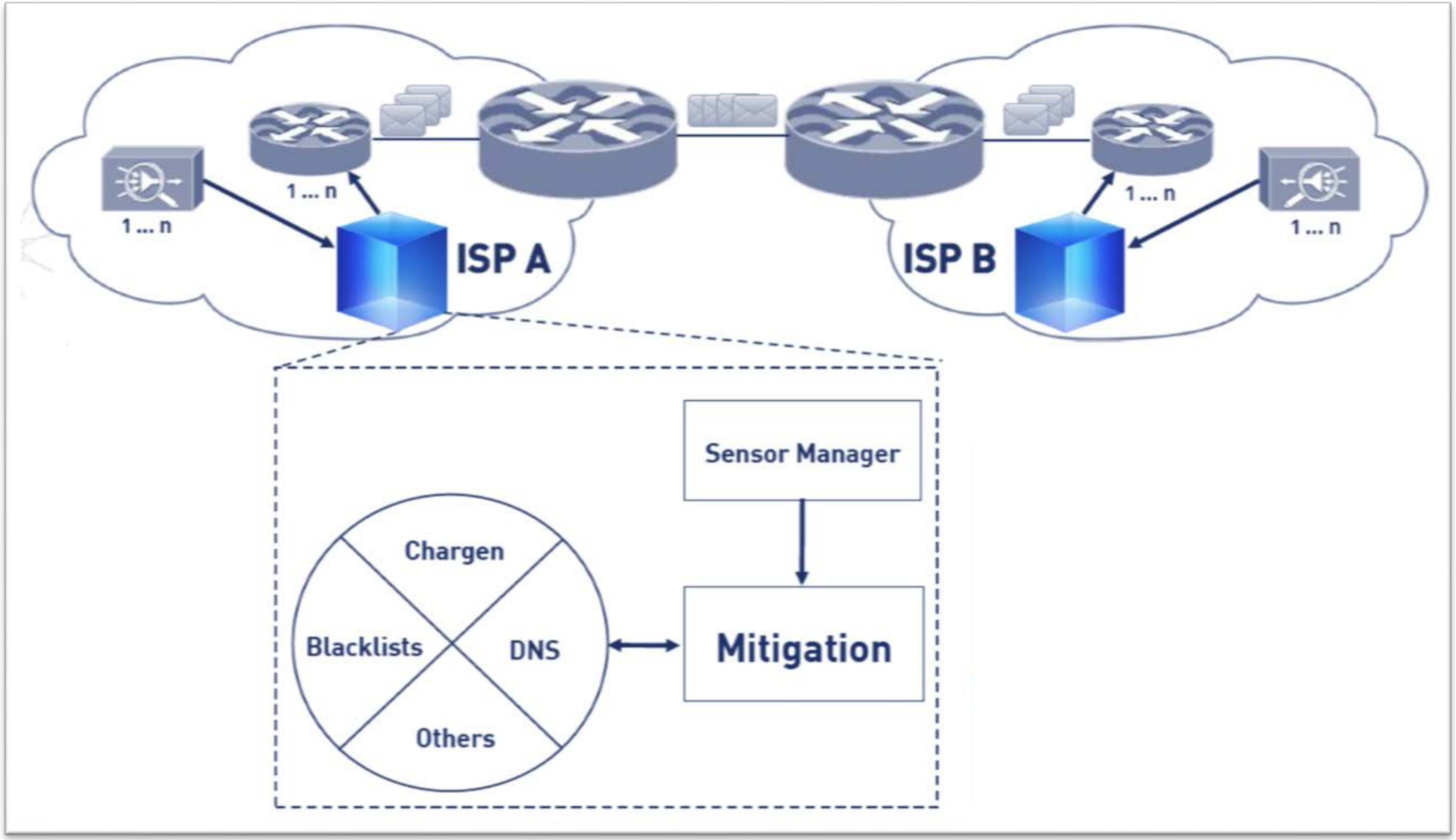
Source: http://whiteboard-ratgeber.de/wp-content/uploads/2013/04/digitales-whiteboard-vs-tafel.jpg

Ingredients

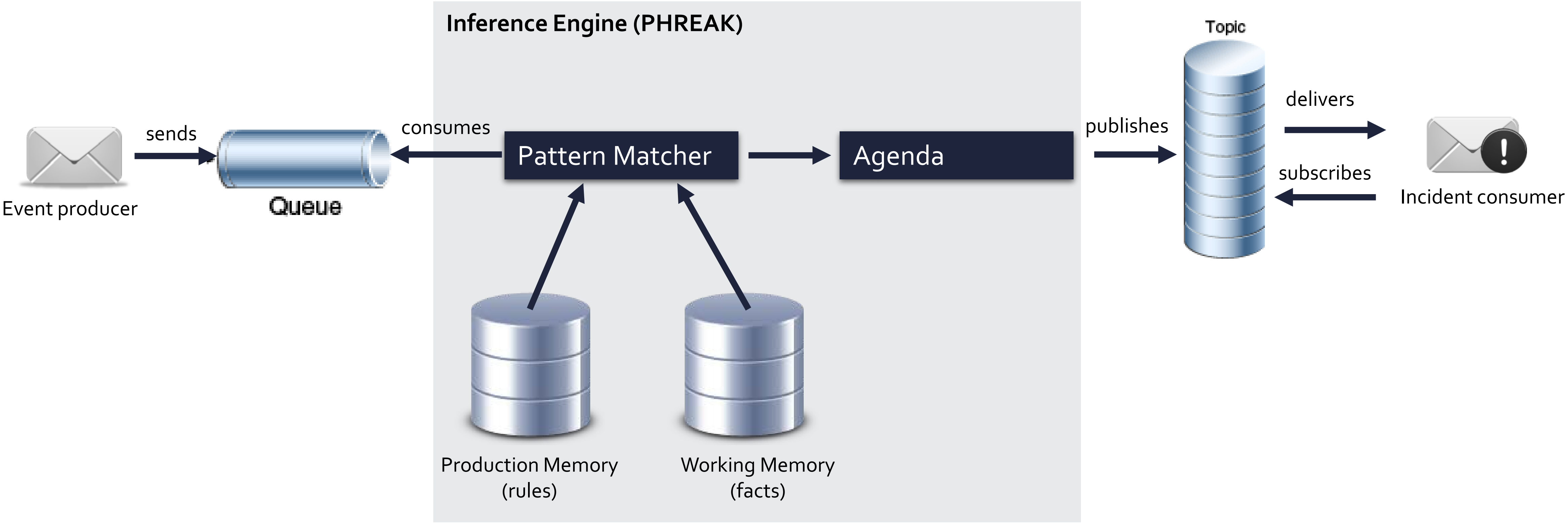


Source: http://www.mitnatur.com/wp-content/uploads//2013/11/Kochen.jpg

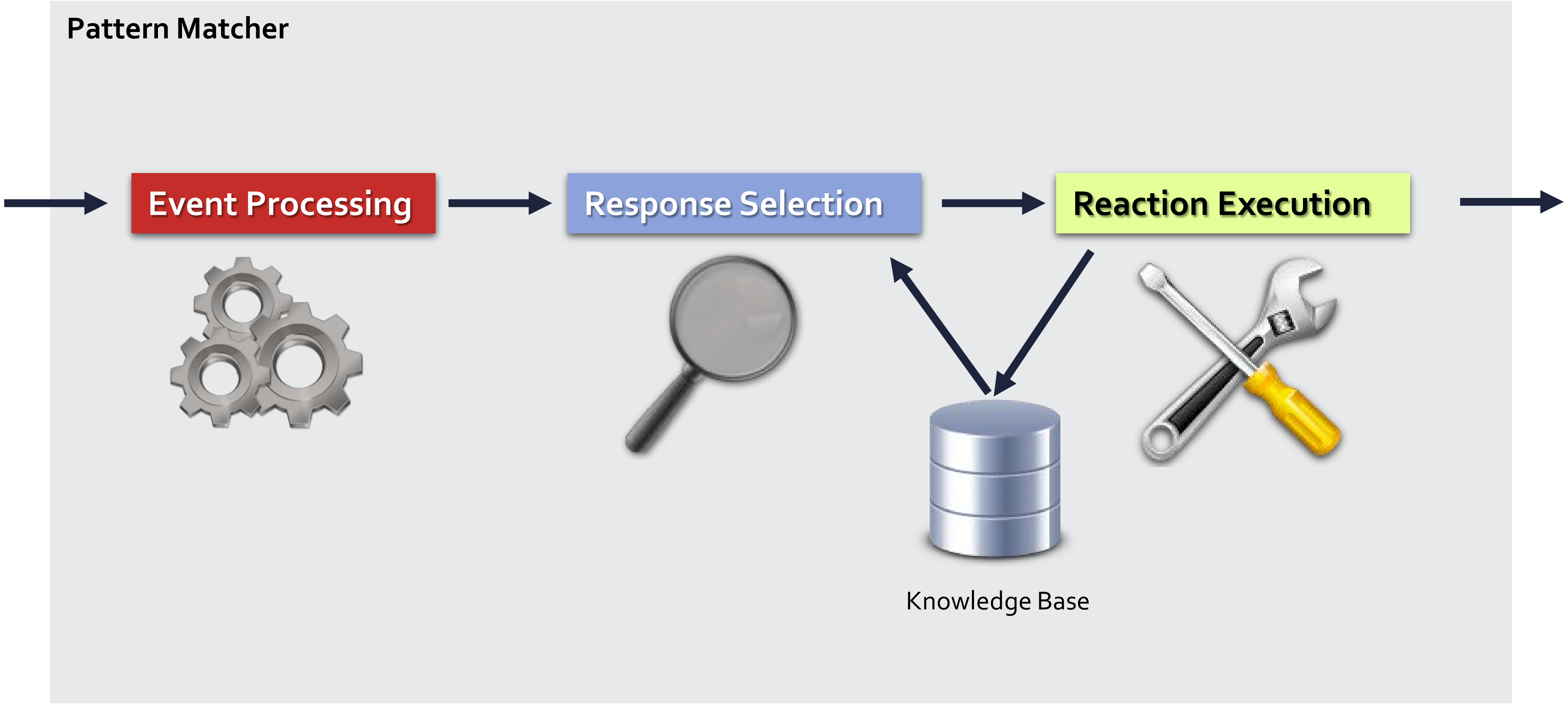
Framework


1 … n
1 … n
ISP A
1 … n
1 … n
ISP B
Sensor Manager
Chargen
Blacklists
DNS
Others
Mitigation

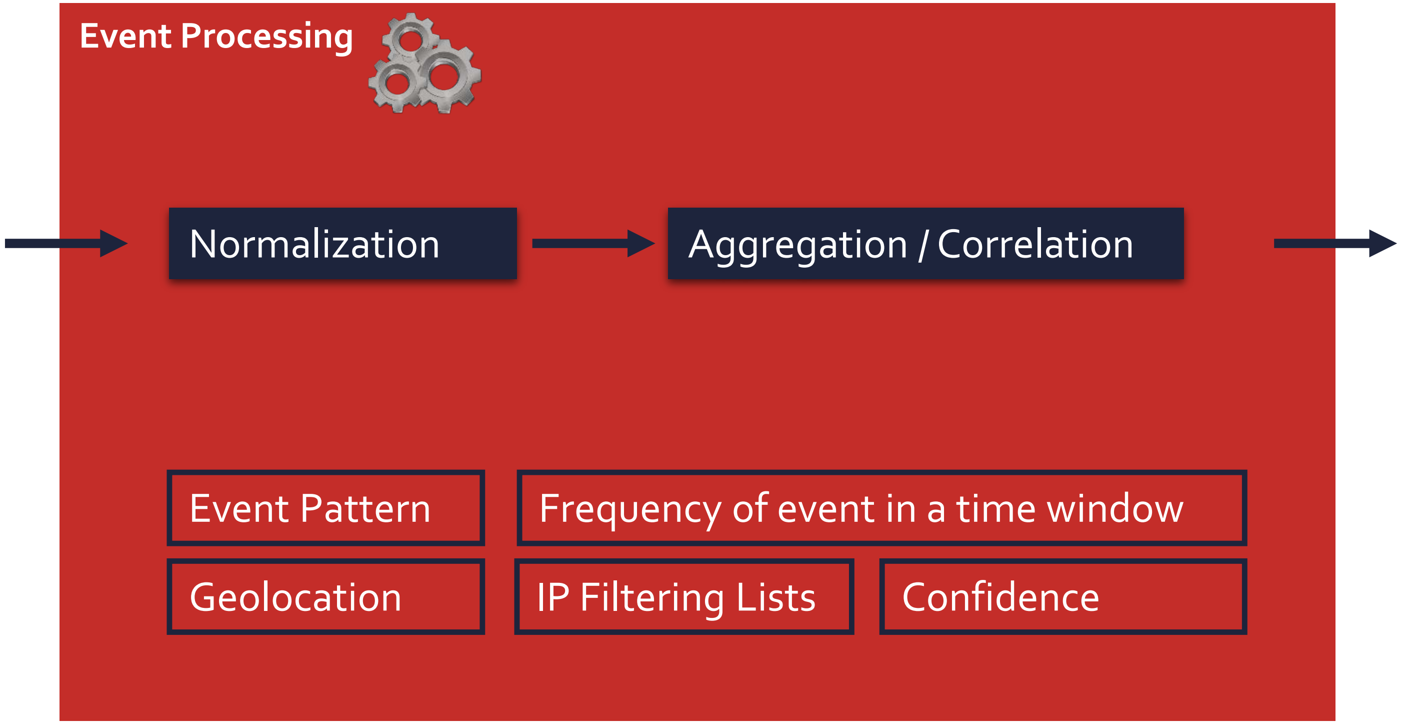
Mitigation and Response System



Mitigation and Response System



Mitigation and Response System



Event Processing

Normalization

Aggregation / Correlation

Event Pattern

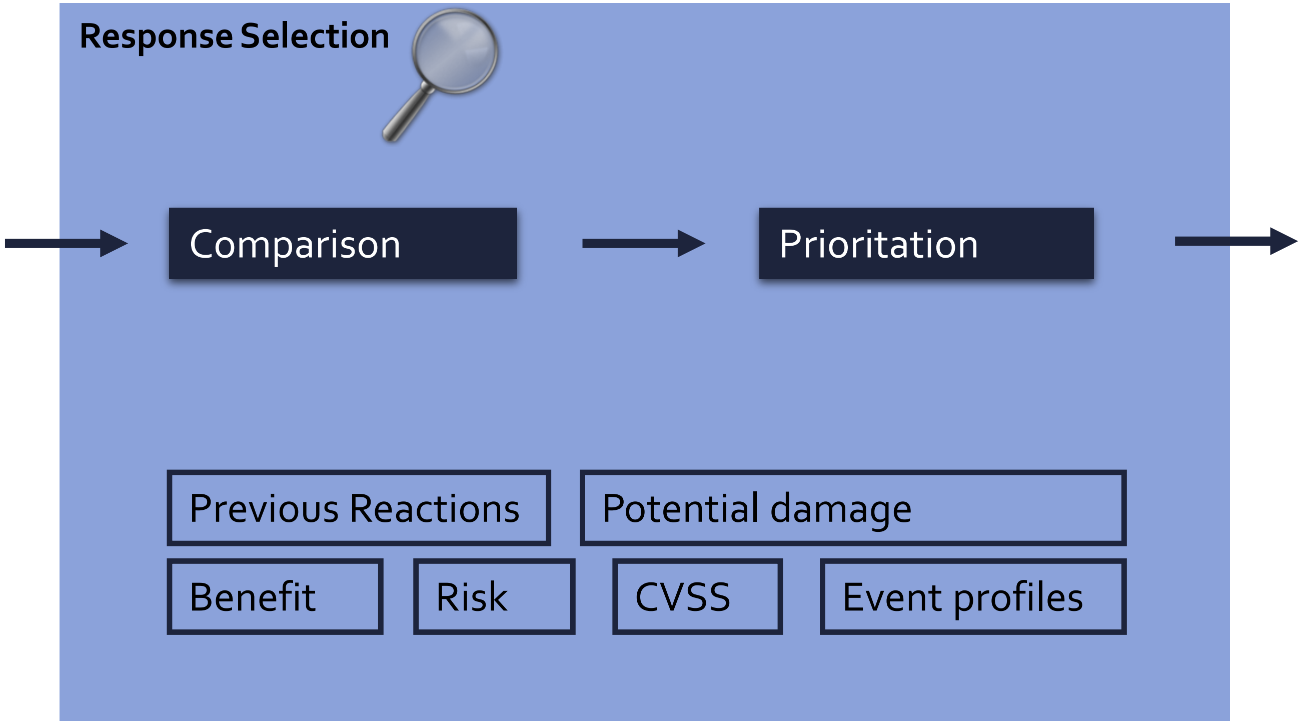
Frequency of event in a time window

Geolocation

IP Filtering Lists

Confidence

Mitigation and Response System



Response Selection

Comparison

Prioritation

Previous Reactions

Potential damage

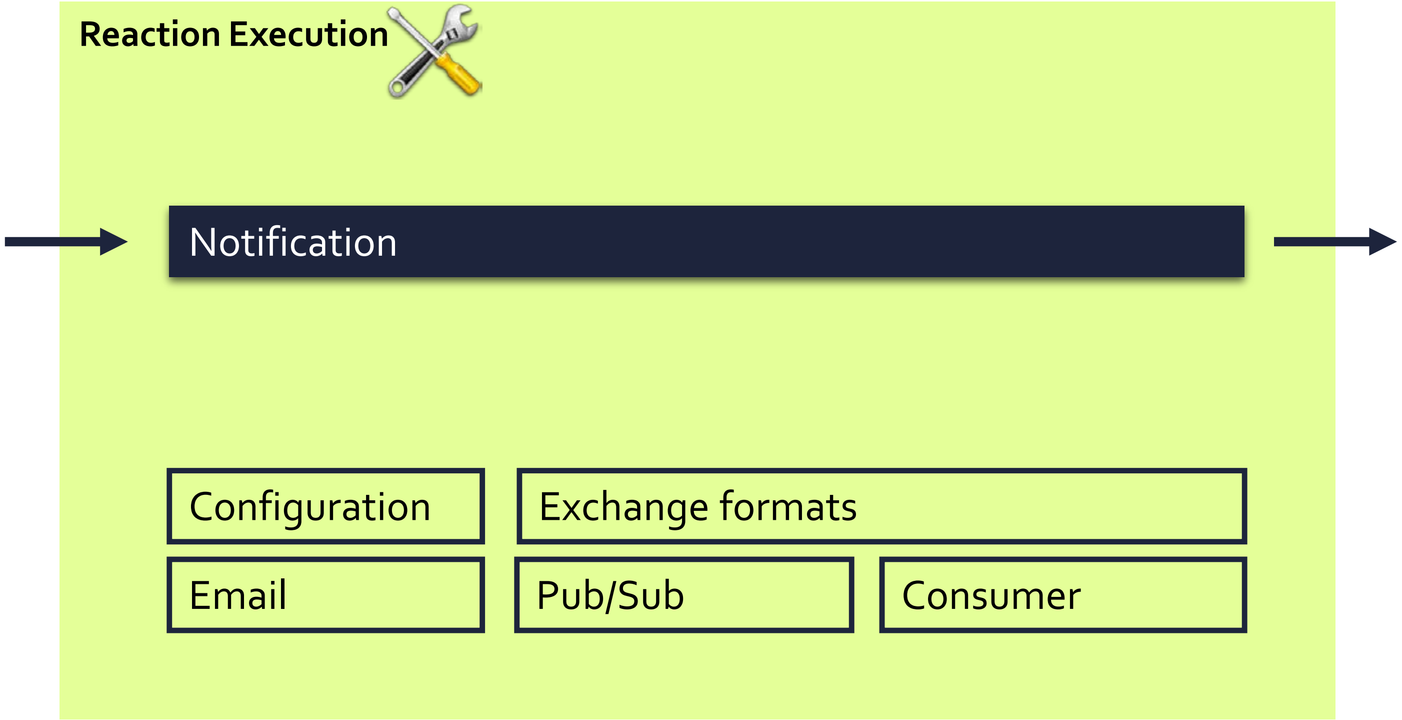
Benefit

Risk

CVSS

Event profiles

Mitigation and Response System



Reaction Execution

Notification

Configuration

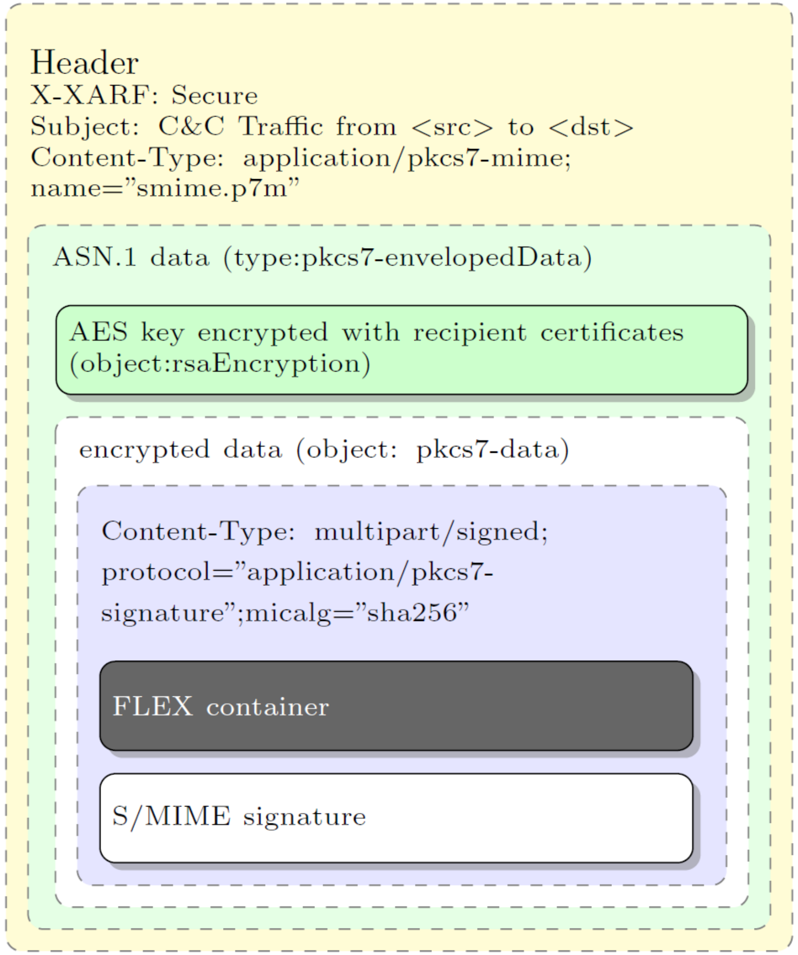
Exchange formats

Email

Pub/Sub

Consumer

Flow-based Event Exchange Format (FLEX)



Header
X-XARF: Secure
Subject: C&C Traffic from <src> to <dst>
Content-Type: application/pkcs7-mime;
name=”smime.p7m”

ASN.1 data (type:pkcs7-envelopedData)

AES key encrypted with recipient certificates (object:rsaEncryption)

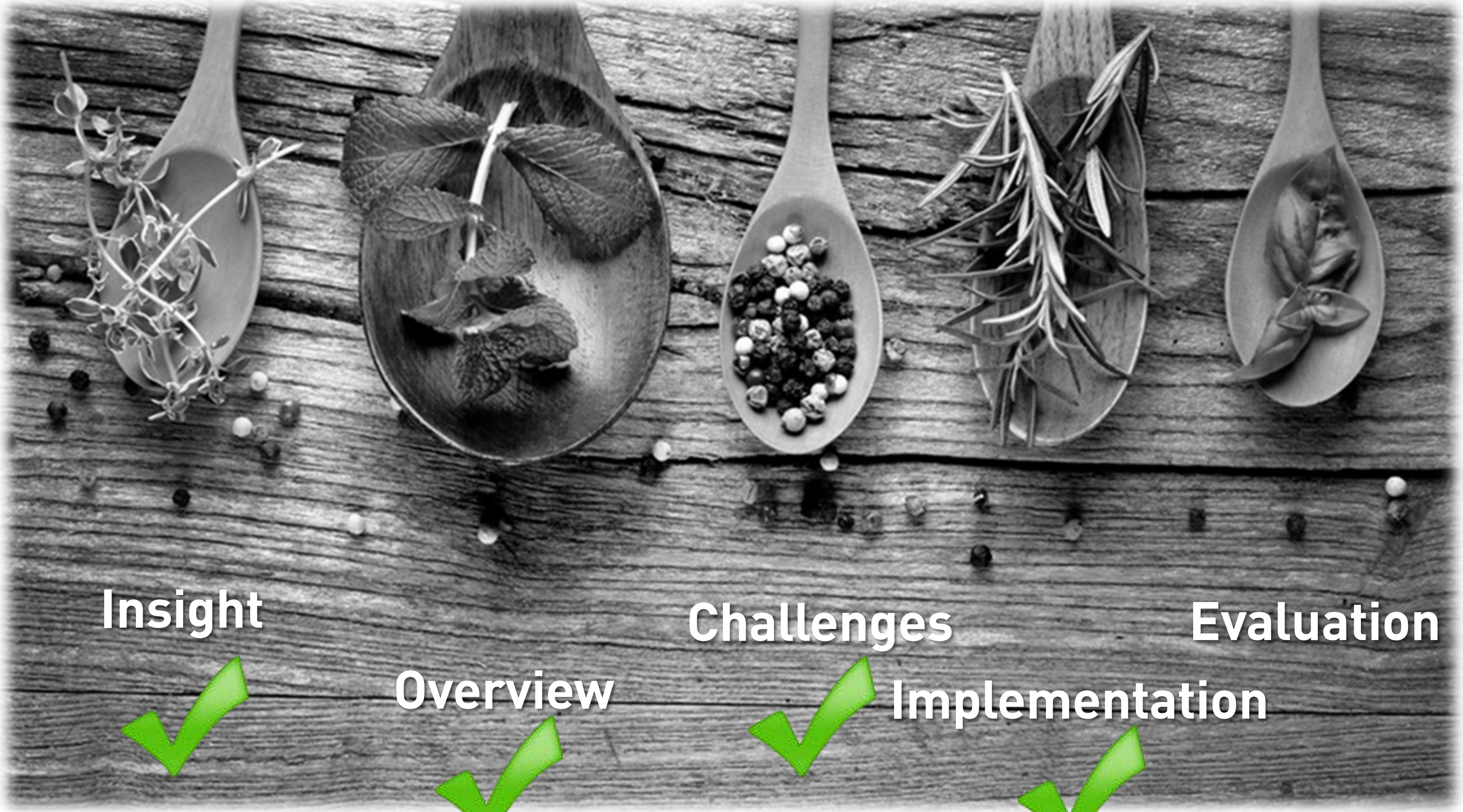
encrypted data (object: pkcs7-data)

Content-Type: multipart/signed; protocol=”application/pkcs7-signature”;micalg=”sha256”

FLEX container

S/MIME signature

Ingredients



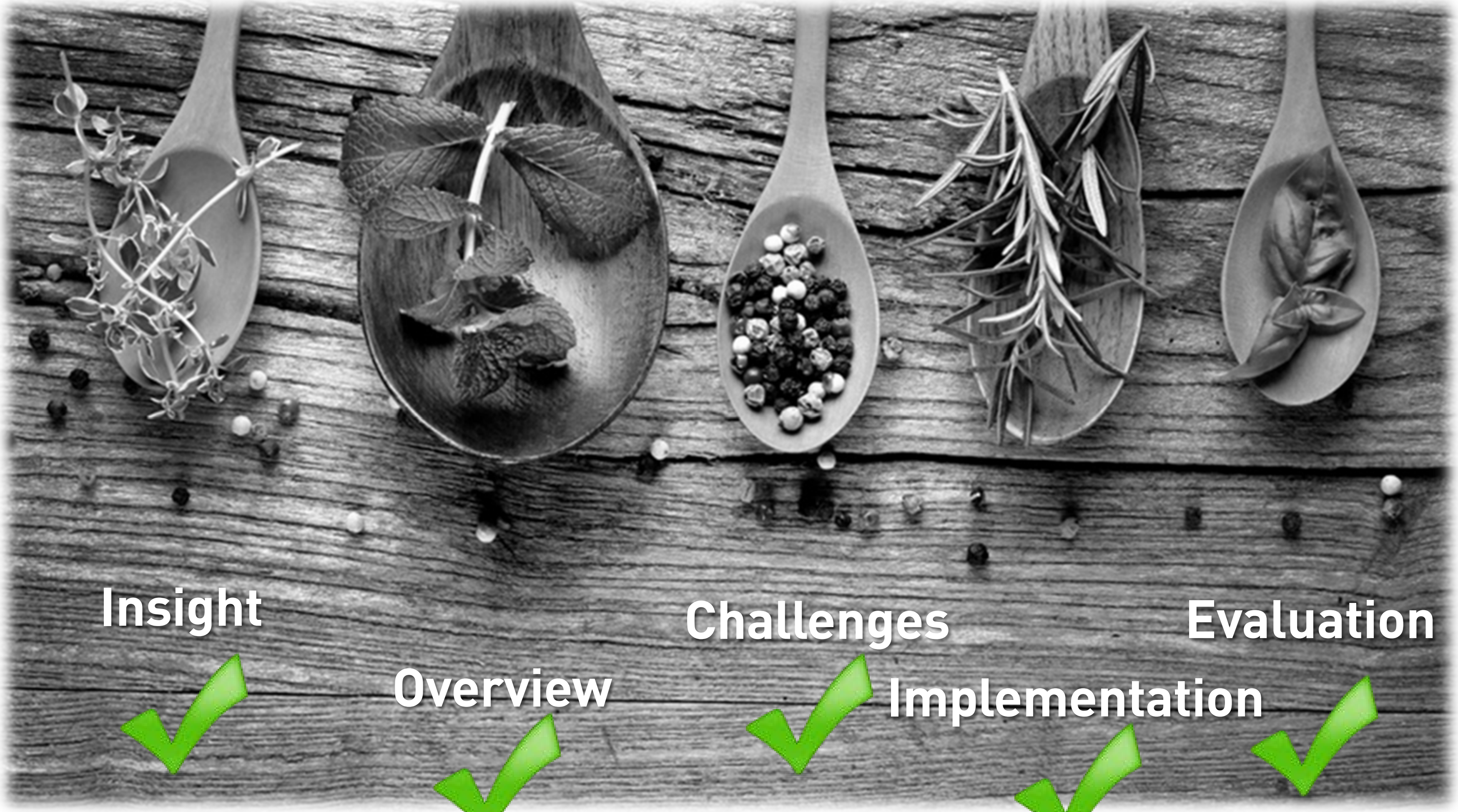
Source: http://www.mitnatur.com/wp-content/uploads//2013/11/Kochen.jpg

Evaluation Methodology

The **DETER** Project

Source: http://www.microgen.com/uk-en/products/microgen-aptitude/v4/microgen-aptitude-business-it-collaboration

Ingredients



Insight ✓

Overview ✓

Challenges ✓

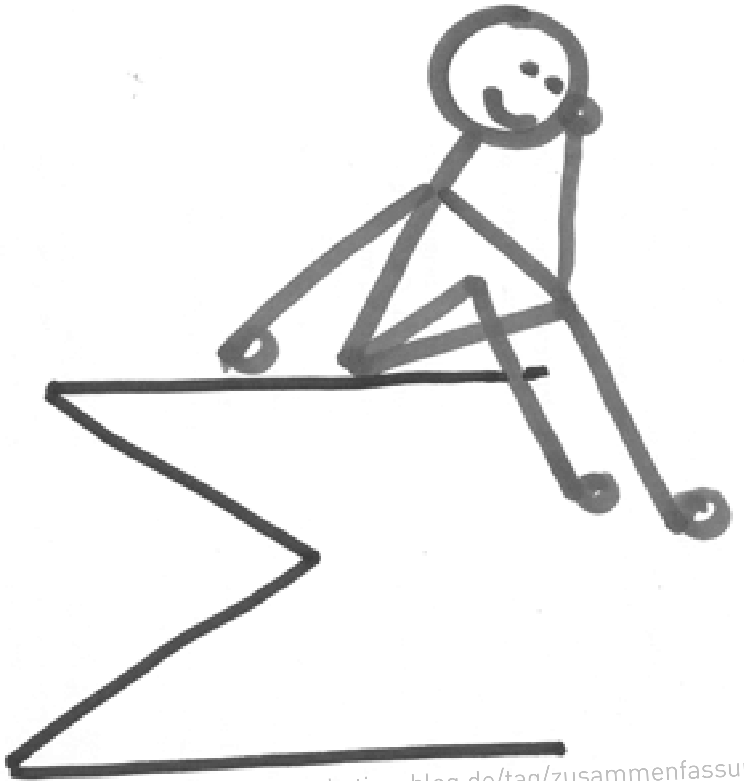
Implementation ✓

Evaluation ✓

Source: http://www.mitnatur.com/wp-content/uploads//2013/11/Kochen.jpg

Conclusion

- insight into processes, structures and capabilities
- a hands-on for network operators

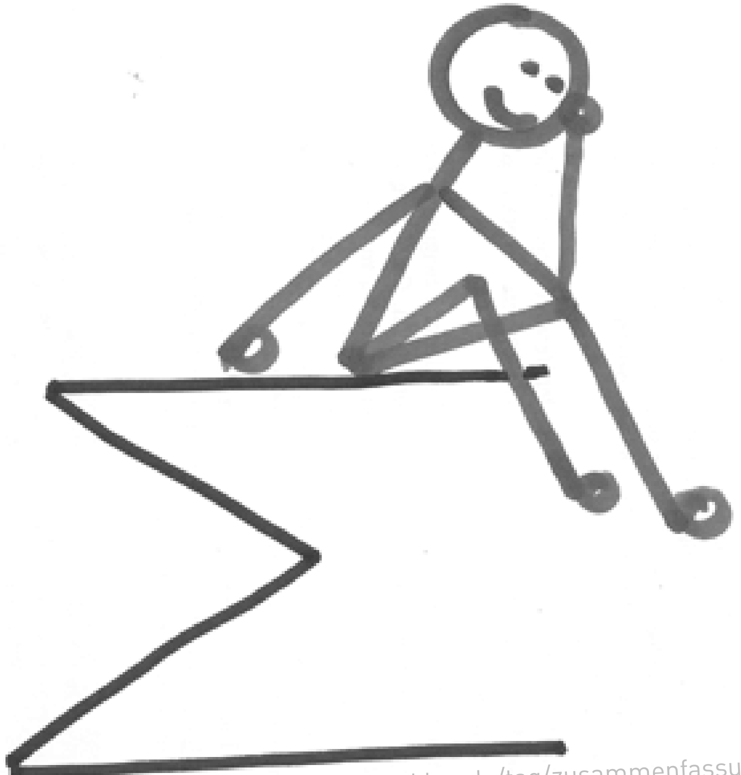


Source: http://bildungsmarketing-blog.de/tag/zusammenfassung/

Conclusion

- FLEX

- framework



Source: http://bildungsmarketing-blog.de/tag/zusammenfassung/

Discussion

Source: http://www.prosperitycometh.com/wp-content/uploads/2012/11/business_conference_1600_clr_3835.png