UNIVERSITETET I AGDER

Chronic Workload Problems in Computer Security Incident Response Teams

Johannes Wiik, Jose J. Gonzalez
University of Agder, Norway

Pål I. Davidsen
University of Bergen, Norway

Klaus-Peter Kossakowski
SEI Europe, Carnegie Mellon University, Germany

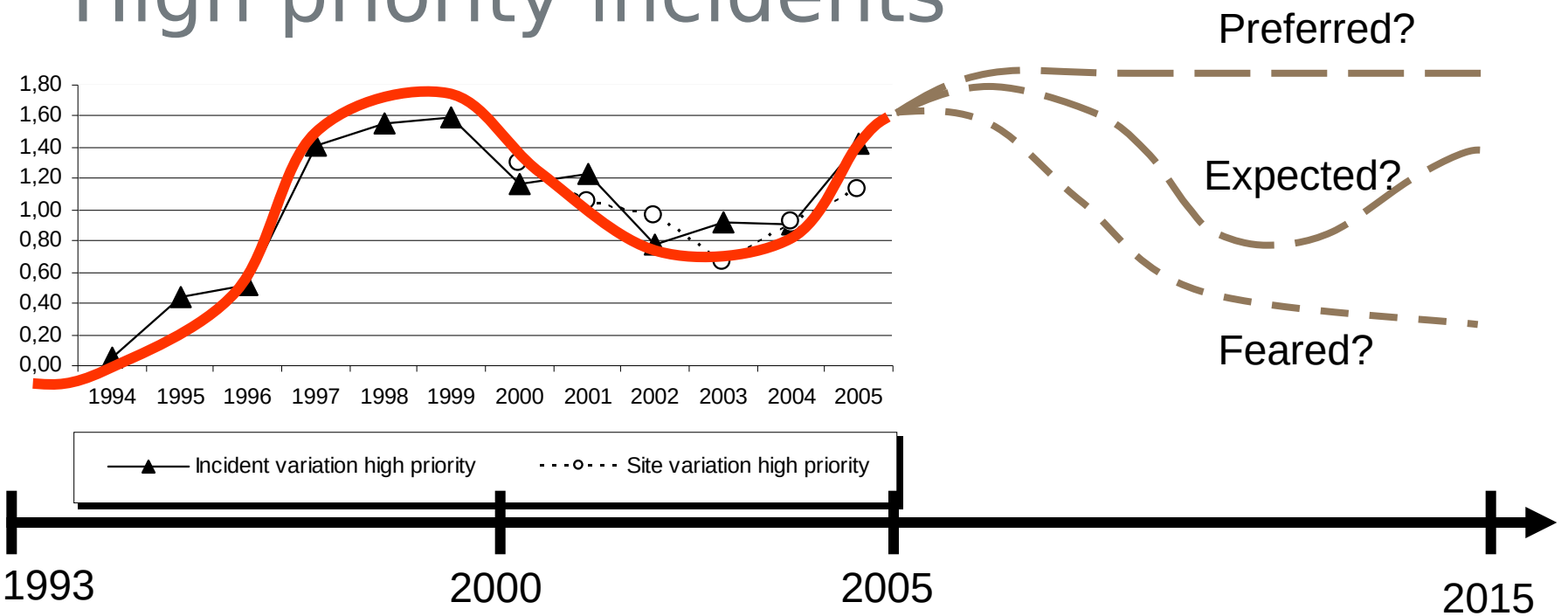
Computer security incidents

- Low-priority incidents
  - Such as port scans, spam, fake email, and other nuisances
  - Nevertheless, a significant challenge owing to their large volume
  - Dynamics: quite accurately described as exponentially growing
  - Essential point: Cannot be matched by staff increase and CSIRT-funding
- High-priority incidents
  - Such as attacks on net infrastructure, serious new worms, viruses, botnets, sniffers, account compromisers, etc
  - Low volume, but very serious
  - Dynamics: basically oscillatory

CSIRTs

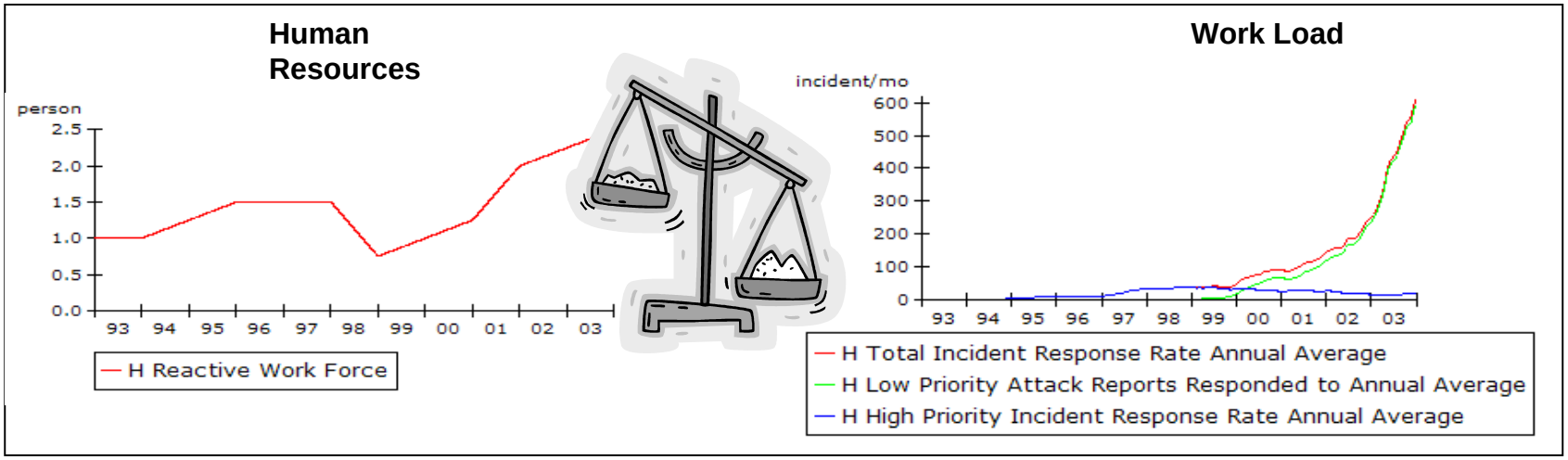
- Computer Security Incidence Response Teams (CSIRTs/CERTs) provide one or more services:
  - incident analysis
  - incident response on site, support & coordination
  - nowadays increasing emphasis on proactive services
- Chronic situation for CSIRTs since their inception in 1988
  - CSIRTs are underfunded, understaffed
  - CSIRT staff is overworked
- Worsening situation for CSIRTs in recent years
  - Increasing volume of (mainly low-priority) incidents, automation and speed of new attack tools give CSIRT staff less and less time to react
  - Instabilities in high-priority security incident reports from the constituency (internal sites) and affected external sites

High priority incidents



- Instabilities in incident reports ➔ instabilities in workload ➔ inefficient use of resources
- Problems to retain the CSIRT constituency (➔ funding problems)
- See posters # 1193 and 1212

Low-priority incidents

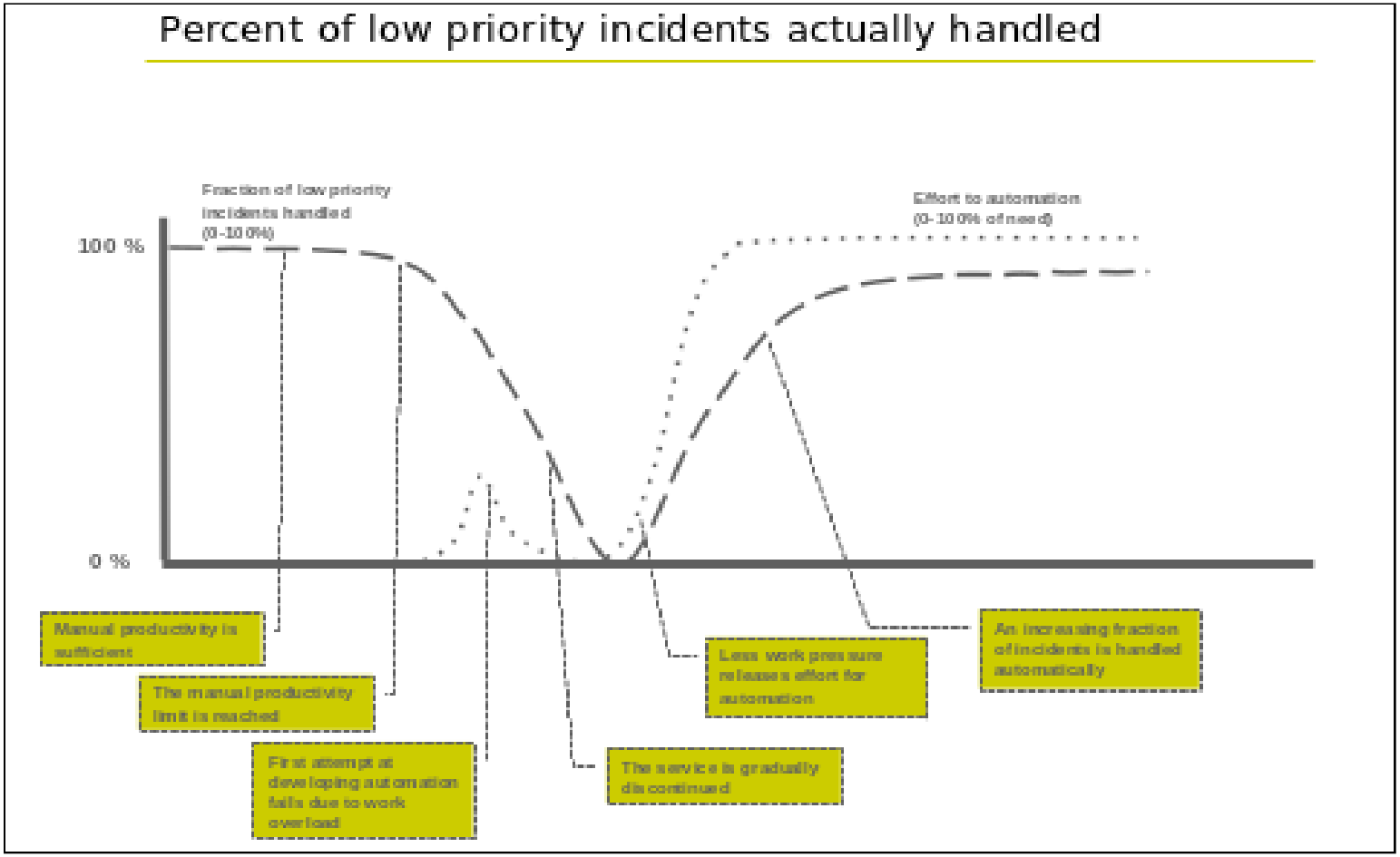


- Overwhelming increase in the rate of low-priority incidents
  - The workload increases accordingly
  - Human resources cannot keep pace

Modeling process

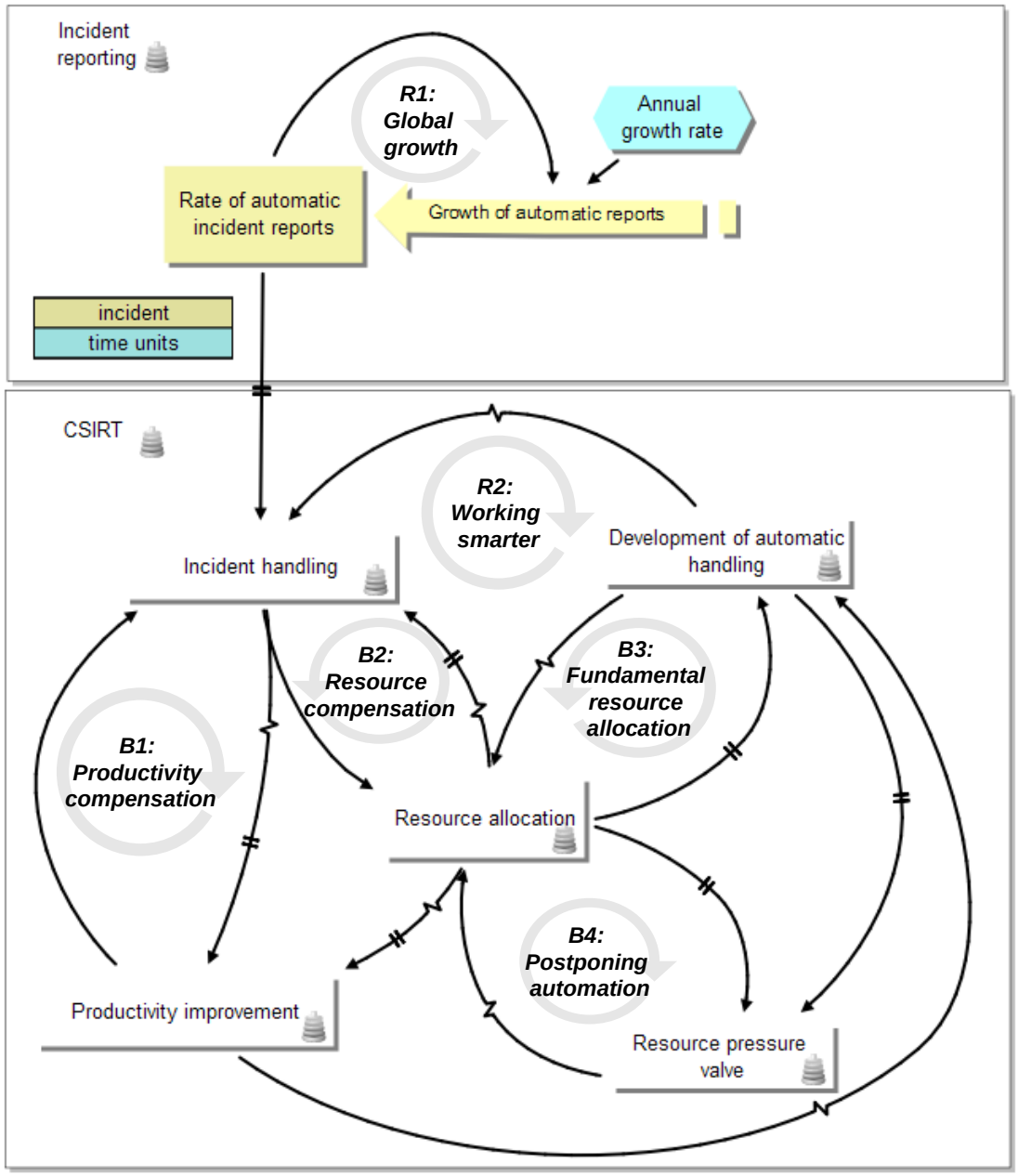
- Close collaboration with one of the oldest and largest “coordinating” CSIRTs
- Initial research questions
  - What factors limit the effectiveness of the incident response service in the CSIRT
  - What policies can improve the effectiveness of the incident response service in the CSIRT?
  - What constitutes effective incident response in the CSIRT?
- The management and staff of the CSIRT participated in 5 face-to-face working sessions of 1 – 4 days over a 1 ½ year period:
  - Eliciting of mental, written and numerical information, incl. reference behavior modes
  - Review of model structure
  - Model verification, validation & policy testing

Reference behavior modes

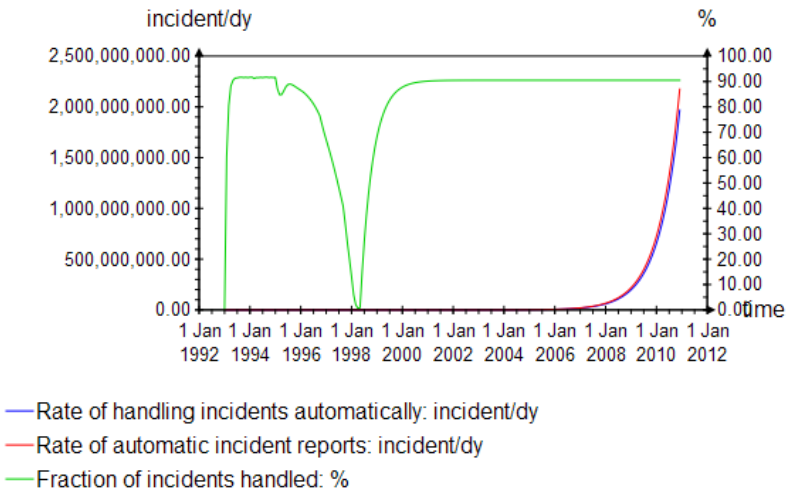


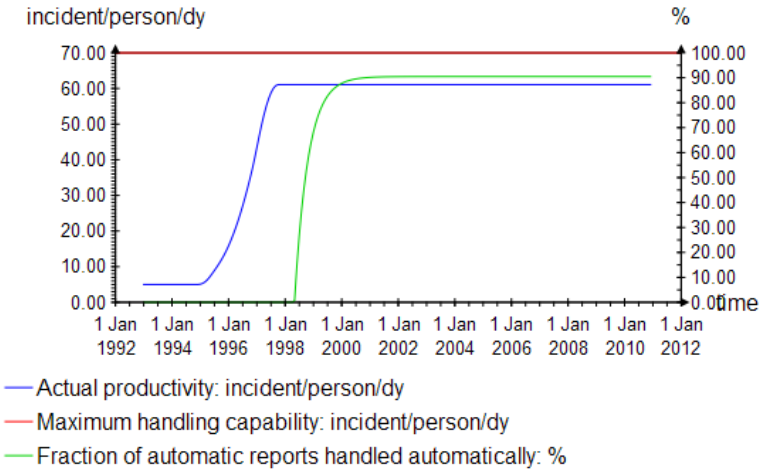
Idealized reference behavior derived from time series data and from interviews with CSIRT management and staff

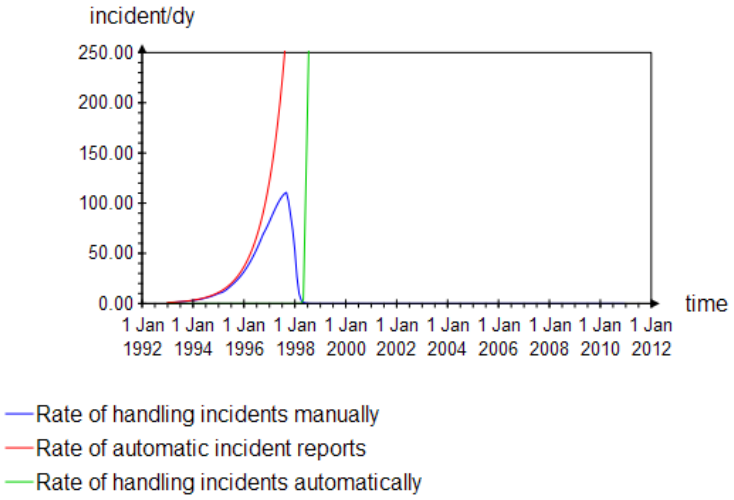
Policy structure diagram

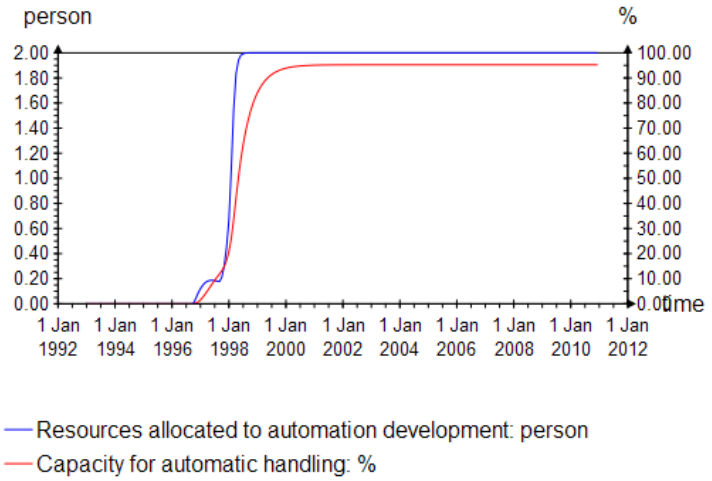


Base run


incident/dy
%
2,500,000,000.00
2,000,000,000.00
1,500,000,000.00
1,000,000,000.00
500,000,000.00
0.00
100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
time
1 Jan 1992
1 Jan 1994
1 Jan 1996
1 Jan 1998
1 Jan 2000
1 Jan 2002
1 Jan 2004
1 Jan 2006
1 Jan 2008
1 Jan 2010
1 Jan 2012
Rate of handling incidents automatically: incident/dy
Rate of automatic incident reports: incident/dy
Fraction of incidents handled: %


incident/person/dy
%
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
time
1 Jan 1992
1 Jan 1994
1 Jan 1996
1 Jan 1998
1 Jan 2000
1 Jan 2002
1 Jan 2004
1 Jan 2006
1 Jan 2008
1 Jan 2010
1 Jan 2012
Actual productivity: incident/person/dy
Maximum handling capability: incident/person/dy
Fraction of automatic reports handled automatically: %

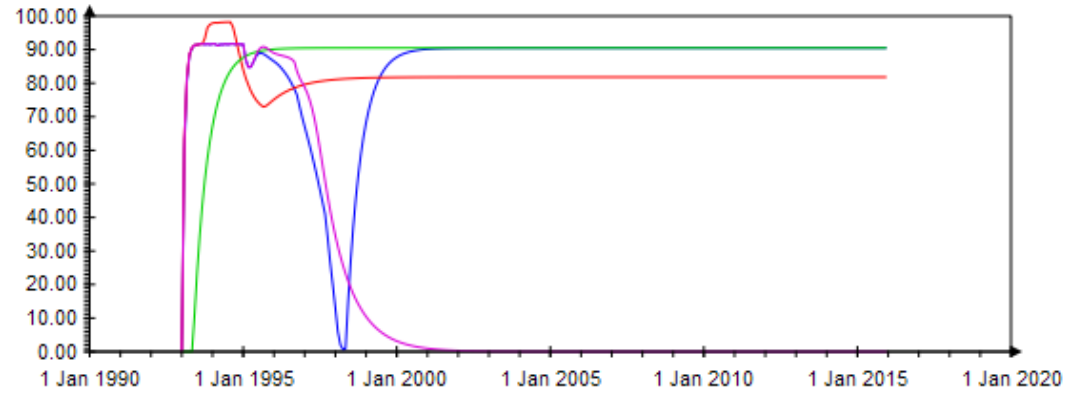

incident/dy
250.00
200.00
150.00
100.00
50.00
0.00
time
1 Jan 1992
1 Jan 1994
1 Jan 1996
1 Jan 1998
1 Jan 2000
1 Jan 2002
1 Jan 2004
1 Jan 2006
1 Jan 2008
1 Jan 2010
1 Jan 2012
Rate of handling incidents manually
Rate of automatic incident reports
Rate of handling incidents automatically

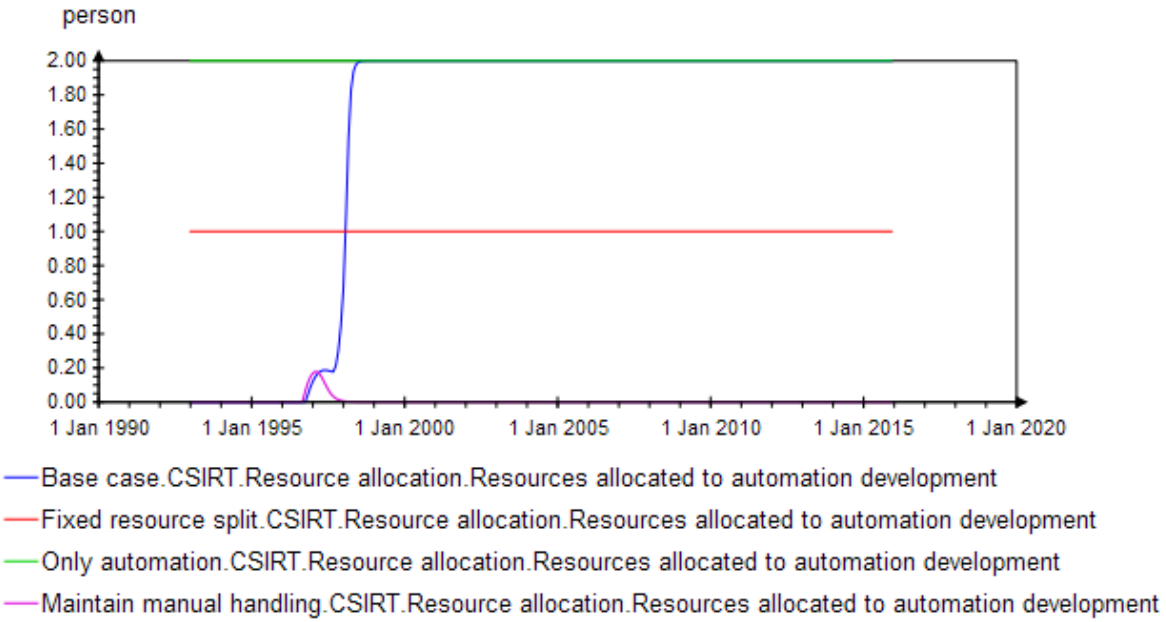

person
%
2.00
1.80
1.60
1.40
1.20
1.00
0.80
0.60
0.40
0.20
0.00
100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
time
1 Jan 1992
1 Jan 1994
1 Jan 1996
1 Jan 1998
1 Jan 2000
1 Jan 2002
1 Jan 2004
1 Jan 2006
1 Jan 2008
1 Jan 2010
1 Jan 2012
Resources allocated to automation development: person
Capacity for automatic handling: %

Policy analysis scenarios

- **Fixed resource split**: The CSIRT separates the workforce into two fixed workgroups instead of using it as a shared resource between tool development and incident response
- **Only automation**: The CSIRT only offers automatic response
- **Maintain manual handling**: The CSIRT refuses to change the service scope and only provides manual handling

Policy runs


100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
1 Jan 1990
1 Jan 1995
1 Jan 2000
1 Jan 2005
1 Jan 2010
1 Jan 2015
1 Jan 2020
Base case.CSIRT.Incident Handling.Fraction of incidents handled
Fixed resource split.CSIRT.Incident Handling.Fraction of incidents handled
Only automation.CSIRT.Incident Handling.Fraction of incidents handled
Maintain manual handling.CSIRT.Incident Handling.Fraction of incidents handled


person
2.00
1.80
1.60
1.40
1.20
1.00
0.80
0.60
0.40
0.20
0.00
1 Jan 1990
1 Jan 1995
1 Jan 2000
1 Jan 2005
1 Jan 2010
1 Jan 2015
1 Jan 2020
Base case.CSIRT.Resource allocation.Resources allocated to automation development
Fixed resource split.CSIRT.Resource allocation.Resources allocated to automation development
Only automation.CSIRT.Resource allocation.Resources allocated to automation development
Maintain manual handling.CSIRT.Resource allocation.Resources allocated to automation development

Thank you!