Incident handling in the Norwegian academic sector

12. June 2018

TNC 2018

Rune Sydskjør, team leader Uninett CERT

UNINETT

Uninett ties Norwegian research- and educational institutions together

Visa says service returning to normal

1 June 2018

Share

A Sainsbury's store in Vauxhall, London, is not taking card payments

Visa says its service is "close to normal" again following a system failure which left customers across Europe unable to make some purchases.

The company apologised and said it had no reason to believe the hardware failure was down to "any unauthorised access or malicious event".

Visa says service returning to normal

1 June 2018

Share

A Sainsbury's store in Vauxhall, London, is not taking card payments

Visa says its service is "close to normal" again following a system failure which left customers across Europe unable to make some purchases.

The company apologised and said it had no reason to believe the hardware failure was down to "any unauthorised access or malicious event".

Uninett CERT and certification

- Uninett CERT (Computer Emergency Response Team), since 1995
  - Coordination, Communication (advisories, reports, recommendations) and basic analysis and forensics
- Uninett CERT is a certified team from 2014 (by Trusted Introducer)
  - All information we are handling is done in a safe and consistent way.
  - We have access to a lot of information sources which in turn will help the whole sector

The role as a sectorial CERT

- The Norwegian National Security Authority (NSM) – Annual security report 2017 - «The ability to discover serious cyber incidents must be strenghted on the national level, through sectorial teams and in the business/companies.»
- SektorCERT = Sektorvist Responsmiljø (SRM) - standardized term in Norway since 2016
- Uninett CERT is the ”sectorCERT” for the academic sector and for the customers of Uninett
- Main focus of a sectorCERT is to coordinate incidents in a sector and be a link to the authorities and other teams.

CERT - Web of trust

- Cyber security is a global problem. No one has the full overview and maybe not all the necessary capabilities.
- Trusted partners and safe communication is crucial.
- Close cooperation with other teams is necessary.
- Uninett CERT is a member of several national and international networks where we receive information, tools and methods which will benefit our sector.

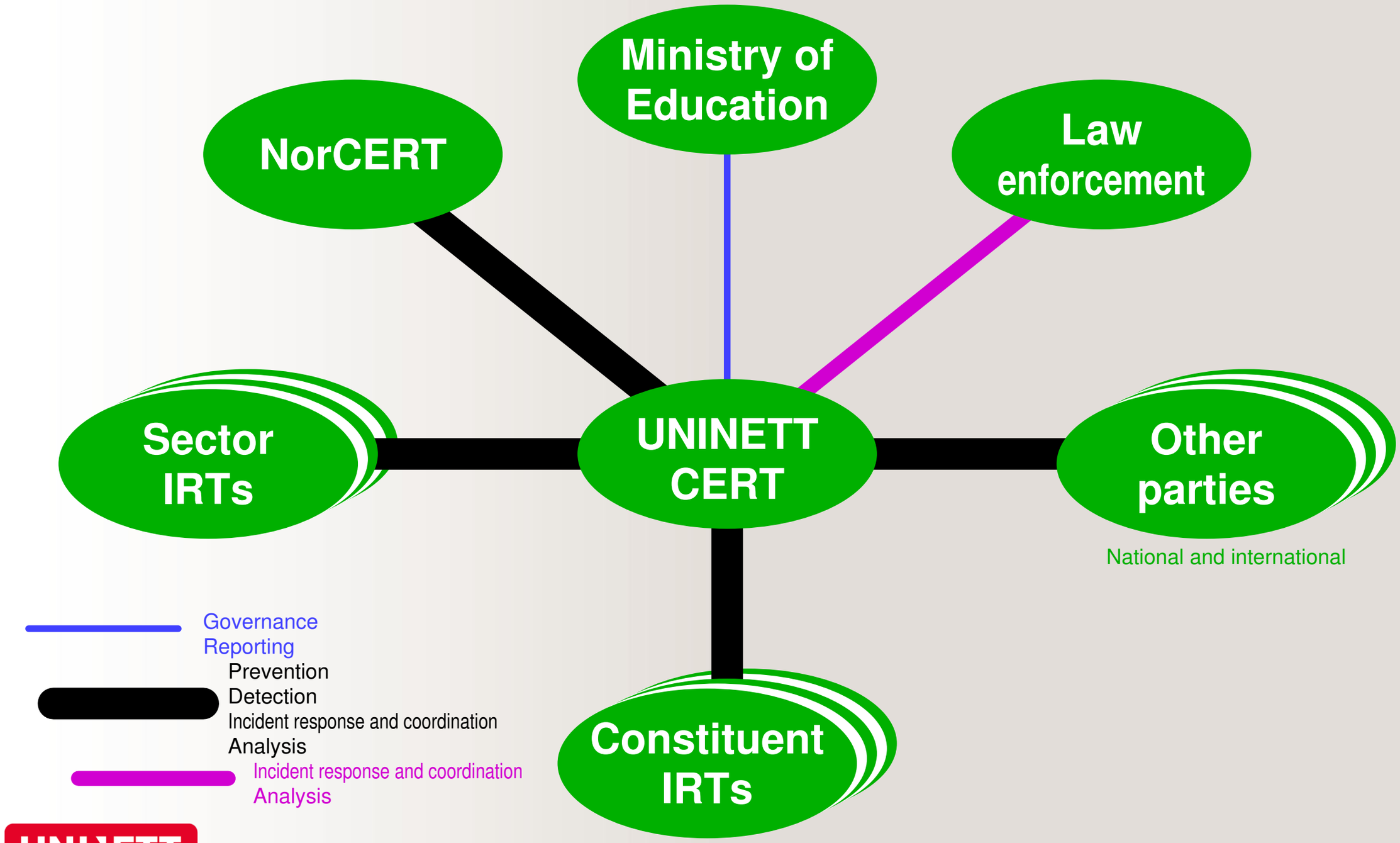
TF-CSIRT Trusted Introducer

FIRST Improving Security Together

UNINETT

Communications map – National level

Uninett centric



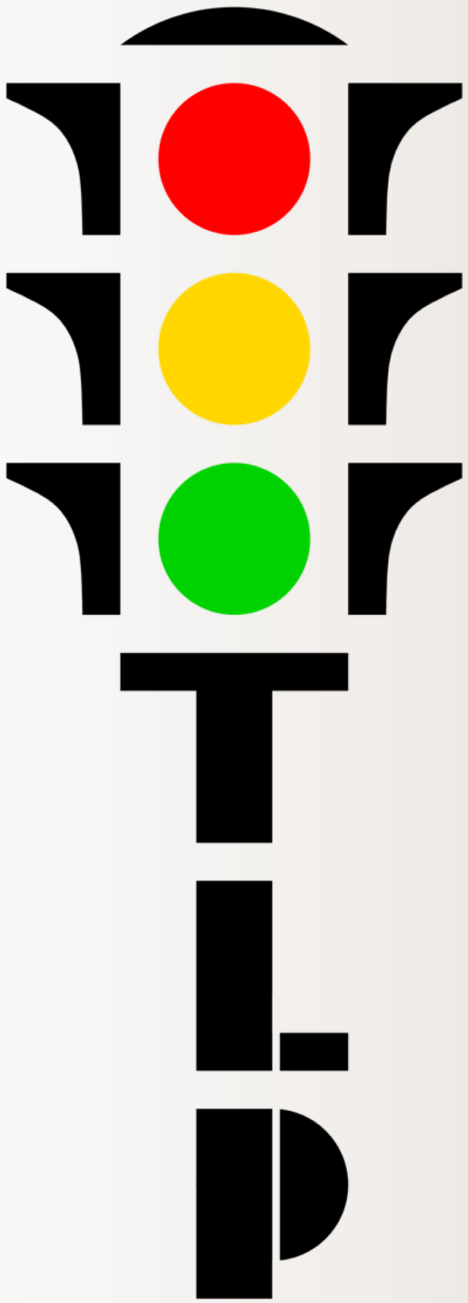
UNINETT

Cooperation in Norway

- Meetings with National Security Authority´s CERT - NorCERT and other sectorial CERTs.
  - Weekly video meetings. Share status in each sector.
  - Monthly physical meetings
- The last months we have also had a test period with secondment/sit in to NorCERT every Wednesday from all sectorial CERTs. Currently under evaluation and will probably continue.
- IRC chat with a lot of communication. Especially during serious incidents. Easy way to get in touch with other teams!

Handle information - experience from incidents and exercises

TLP – Traffic light protocol



TLP: RØD

Kan ikke deles med noen
uten godkjenning fra kilden

TLP: GUL

Kan kun deles internt
med relevante personer

TLP: GRØNN

Kan deles med andre
aktører i sikkerhetsmiljøet

TLP: HVIT

Kan og bør publiseres
til offentligheten

UNINETT

So.. Whats been the challenge/problem?

- We are serving 21 (recently merged) universities and university colleges
- Plus ca 120 other r&d institutions connected to our network
- Lack of clear and responsive security contact points in our constituency.
- When we wanted to share sensitive and time critical information with our constituency
  - Lack of Traffic Light Protocol Agreements between UNINETT CERT and the institutions
  - Lack of encryption keys to all contact points

UNINETT

IRTs on all institions?

- Experiences we got from IKT-16, a national cyber crisis excersise, led to discussions with our owner, the ministry of education

  They thought our idea of IRT at all institutions was splendid ☺

- Management´s ownership is essential

  The ”Secretariat for information security”, (now hosted at the newly created directorate Unit), made phone calls to management and CSOs at all institutions (univ. and college univ.)

  Emphasize the link between IRT and ISMS

UNINETT

IRTs on all institions? (cont.)

- We updated and translated our course material (based on the TRANSITs course)
- We arranged a training course in conjunction with a Uninett technical workshop, 2 May 2017
- Invitation letter from Uninett sent to top management, copy to ICT department
- Letter from the ministry to top management at all institutions

  Strongly recommended to attend

  Strongly recommendation to create a team

  Linking ISMS and IRT

UNINETT

Formalizing teams in our sector:

- A team may exist, but not be formalized
- A formalized team should have:

  Clear contact points

  A team leader

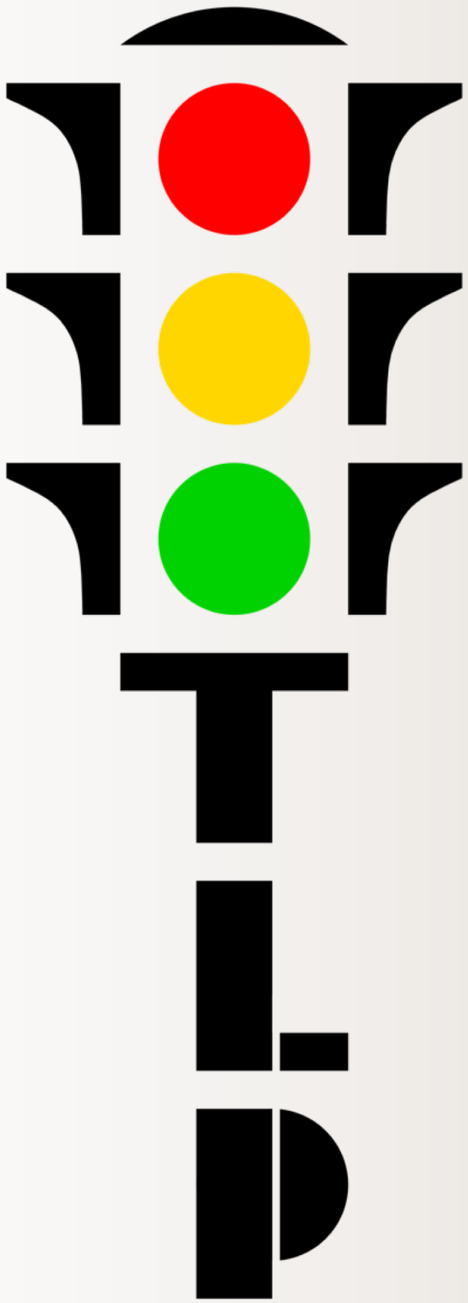
  A well defined team of trusted people

  Beeing listed by the sectorCERT

  Have signed a Traffic Light Protocol Agreement with the sectorCERT

UNINETT

TLP – Traffic light protocol



TLP: RØD

Kan ikke deles med noen
uten godkjenning fra kilden

TLP: GUL

Kan kun deles internt
med relevante personer

TLP: GRØNN

Kan deles med andre
aktører i sikkerhetsmiljøet

TLP: HVIT

Kan og bør publiseres
til offentligheten

UNINETT

Formalizing teams in our sector:

- A team may exist, but not be formalized
- A formalized team should have:

  Clear contact points

  A team leader

  A well defined team of trusted people

  Beeing listed by the sectorCERT

  Have signed a Traffic Light Protocol Agreement with the sectorCERT

  Their cryptography keys (pgp) should be signed by the sectorCERT, by minimum

  Should have been through basic training and have technical skills

  Should be an integral part of the institutions ISMS.

  Should commit them self participating in a sector wise web-of-trust

  - Minimum yearly gatherings etc.

UNINETT

35 IRT's in our sector

Workshop 2 may 2017:

Handelshøyskolen BI (cert@bi.no)
Universitetet i Oslo (cert@uio.no
Høgskolen i Oslo og Akershus (csirt@hioa.no)
Høgskulen på Vestlandet (csirt@hvl.no)
NMBU (csirt@nmbu.no)
Universitetet i Agder (csirt@uia.no)
UiT Norges arktiske universitet (csirt@uit.no)
Norges musikkhøgskole (hendelsesresponsteam@nmh.no)
Nord universitet (irt.nord@nord.no)
Arkitektur- og designhøgskolen i Oslo (irt@aho.no)
Fagskolen Innlandet (irt@fagskolen-innlandet.no)
Høgskolen i Molde (irt@himolde.no)
Høgskolen i Østfold (irt@hiof.no)
Høgskulen i Volda (irt@hivolda.no)
Høgskolen I Innlandet (irt@inn.no)
Kunsthøgskolen i Oslo (irt@khio.no)
Norges Handelshøyskole (irt@nhh.no)
Norges forskningsråd (irt@rcn.no)
Sámi allaskuvla (irt@samiskhs.no)
Universitetet i Bergen (irt@uib.no)
Universitetet i Stavanger (irt@uis.no)
UNIS (irt@unis.no)
NTNU (soc@ntnu.no)
Høgskolen i Sørøst-Norge (usn-irt@usn.no)
Norges idrettshøgskole (irt@nih.no)
Høgskolen i Innlandet (irt@inn.no)

Workshop 9 november 2017:

Utdanningsdirektoratet (irt@udir.no)
Kompetanse Norge (csirt@kompetansenorge.no)
Chr. Michelsen Institutt (irt@cmi.no)
Fagskolen i Ålesund (fials_irt@fials.no)
Nasjonalbiblioteket (irt@nb.no)
UNINETT Sigma2 (csirt@sigma2.no)
Det teknologiske menighetsfakultet (irt@mf.no)
Norsk regnesentral (irt@nr.no)

Uninett CERT (cert@uninett.no)

UNINETT

So, 25 IRTs was formalized the 2nd of May.

The week after;

- ”WannaCry” and ”Leakage from Bing”
- Uninett CERT could now easily forward received TLP Amber and Green tagged information (sent from NorCERT) to the teams.
- Our ministry was also alarmed by Norway’s national security agency. Now they had a secure communication path to all teams at the universities and colleges.

  We got payback ☺. And applause ☺.

UNINETT

Way forward

- More training and gatherings
- Need a communication platform for the sector (chat)
- You need to know your contacts when the incident occurs.
- Our constituency wants more help with detection and analysis capability
- Looking at a possibility to cooperate closer with some of the “stronger” teams in the sector. Some services can be run from the sector -> Virtual teams.
- We have asked for 60M NOK in funding in a 3 year program to ramp up our services. -> “Analysis center”

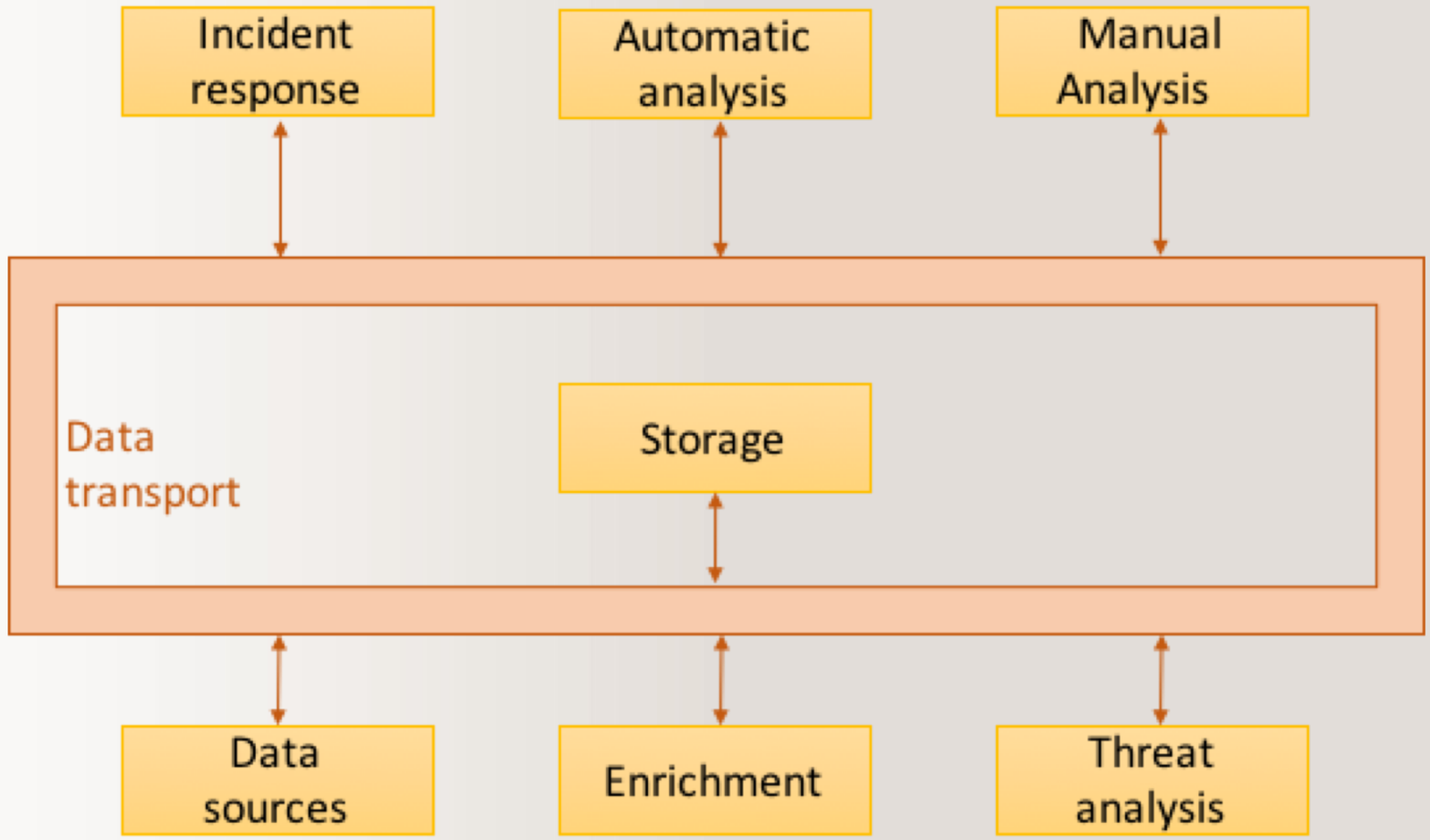
“We are drowning in information but starved for knowledge.”

John Naisbitt

New architecture for analysis platform

- We need more data/log
- We need to correlate more data
- We need to enrich our data (e.g MISP)
- -> SIEM (Security Incident and Event Management system)
- Our data need to be secure!!

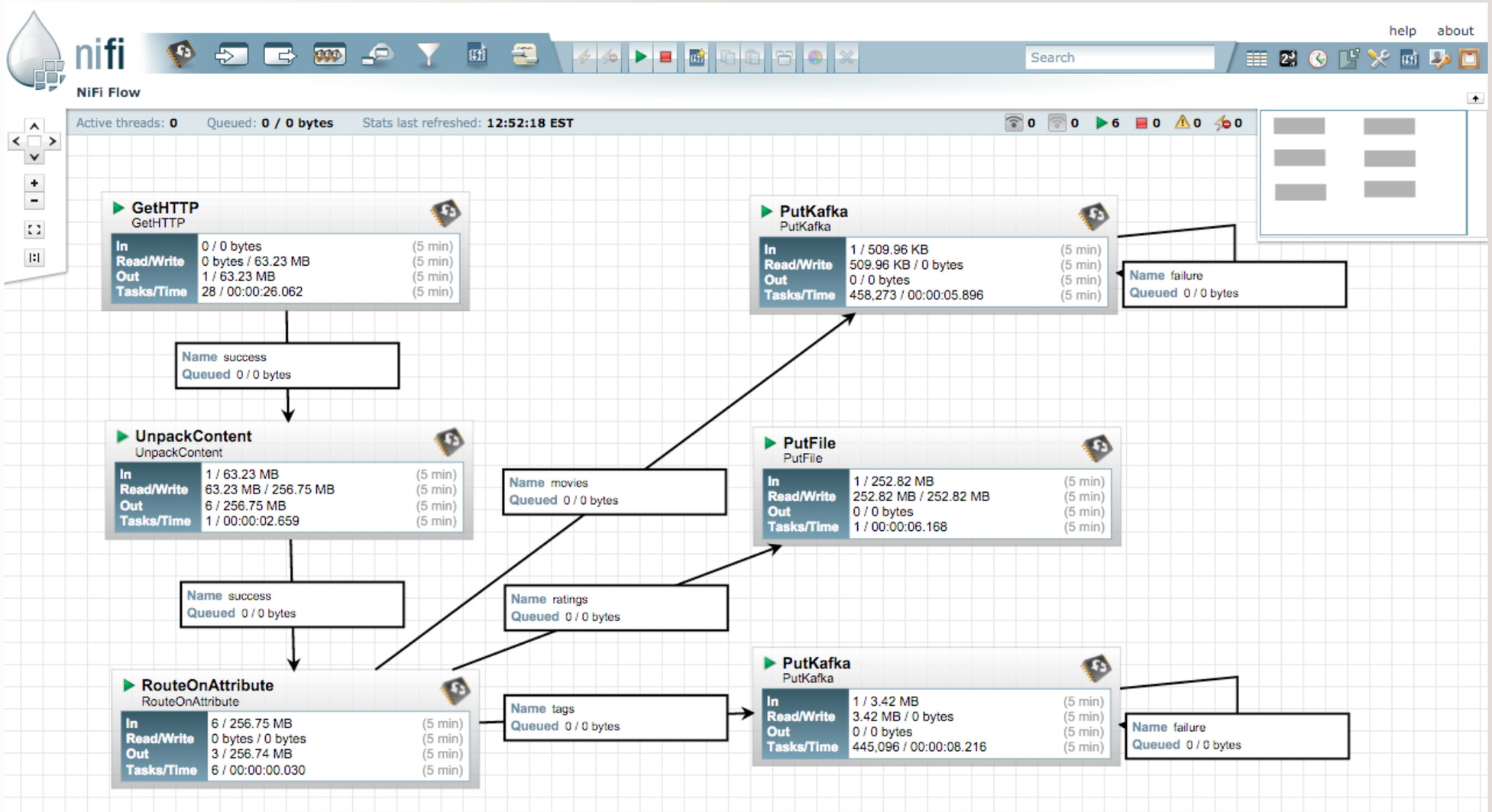
High level architecture



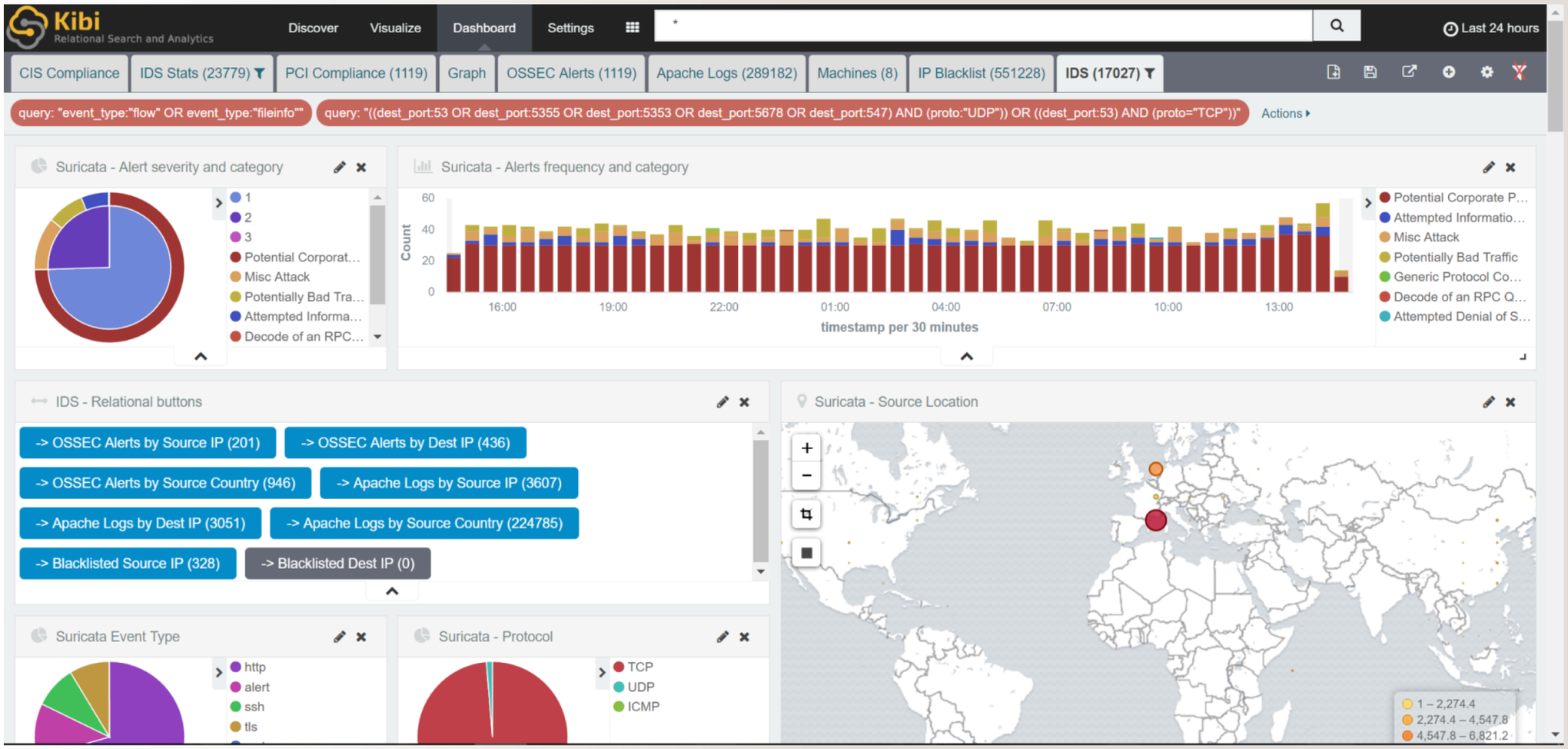
New architecture – new tools

- Apache NiFi – data transport
- Elasticsearch og Siren platform – Storage
- Kibi/Siren investigate – Analysis (Based on Kibana)
- MISP – Threat analysis and sharing
- Wazuh – Securing the infrastructure

Data transport: Apache NiFi



Analysis: Kibi/Siren investigate



Summed up

- Anchoring/Backing/Commitment is a key success factor
  - Both on a governmental level and on the insitutional level
  - Incorporate IRT into the ISMS!
- The National Team (NorCERT) and the SectorCERTs is vital for handling a national cyber crisis;
  - Someone has to be a central point, the driving force
  - Coordination between sectors
  - Controlled information flow to the institutions
  - Coordination towards other national and international parties
- It´s important to follow up the IRTs
  - With regular information (This will also somethimes test their respons)
  - Minimum yearly gatherings - for information, develop competence, web-of-trust
- We assume solid payback when we have situations
  - And we will have situations!

UNINETT

Questions?

- Rune Sydskjør
- rune.sydskjor@uninett.no
- cert@uninett.no
- cert-info@uninett.no