Data-centric security in software-defined networks

Dr.-Ing. Konrad Wrona

Lecture 5: Introduction to data-centric security

Briefing Purpose and Content

Purpose

- Motivate the effort on Data Centric Security
- Communicate where we are
- Prepare you for future communications

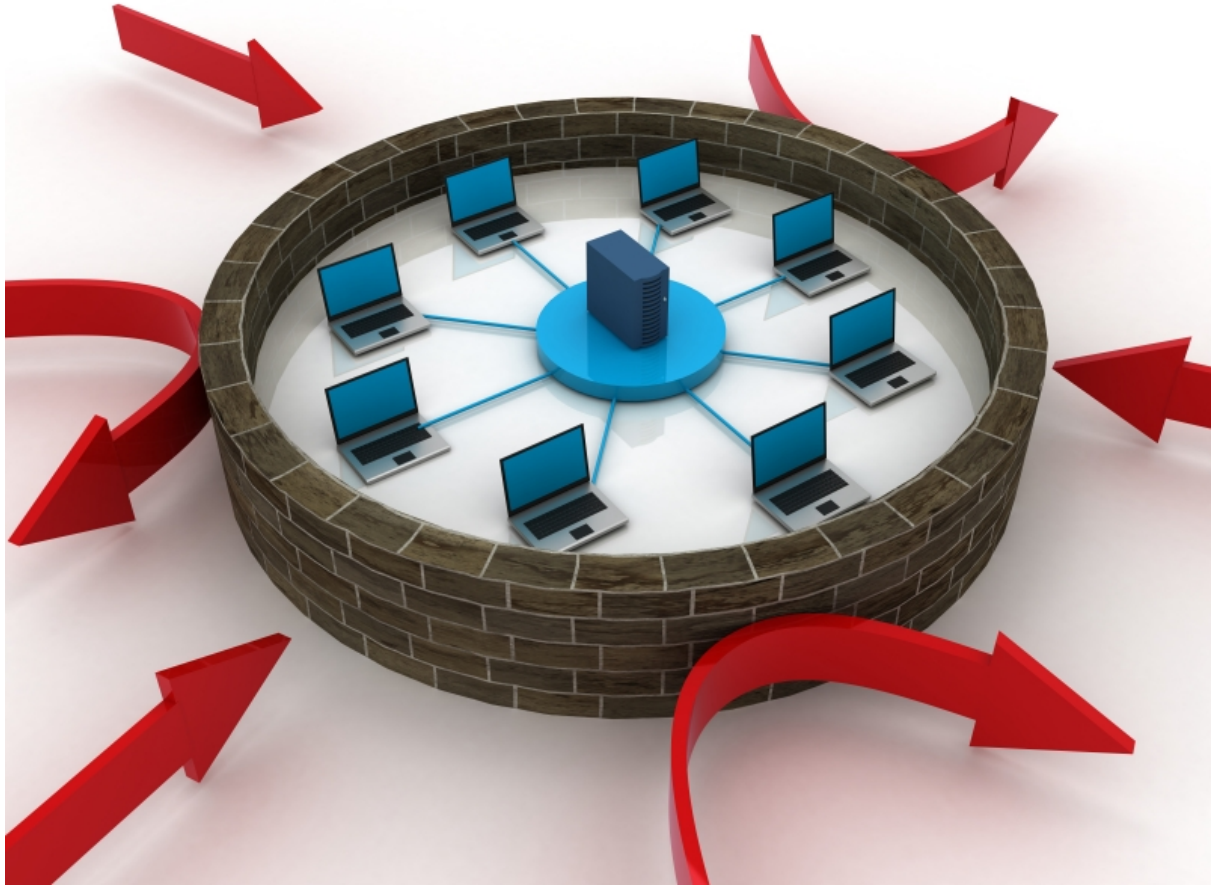
Content

(provide background information)

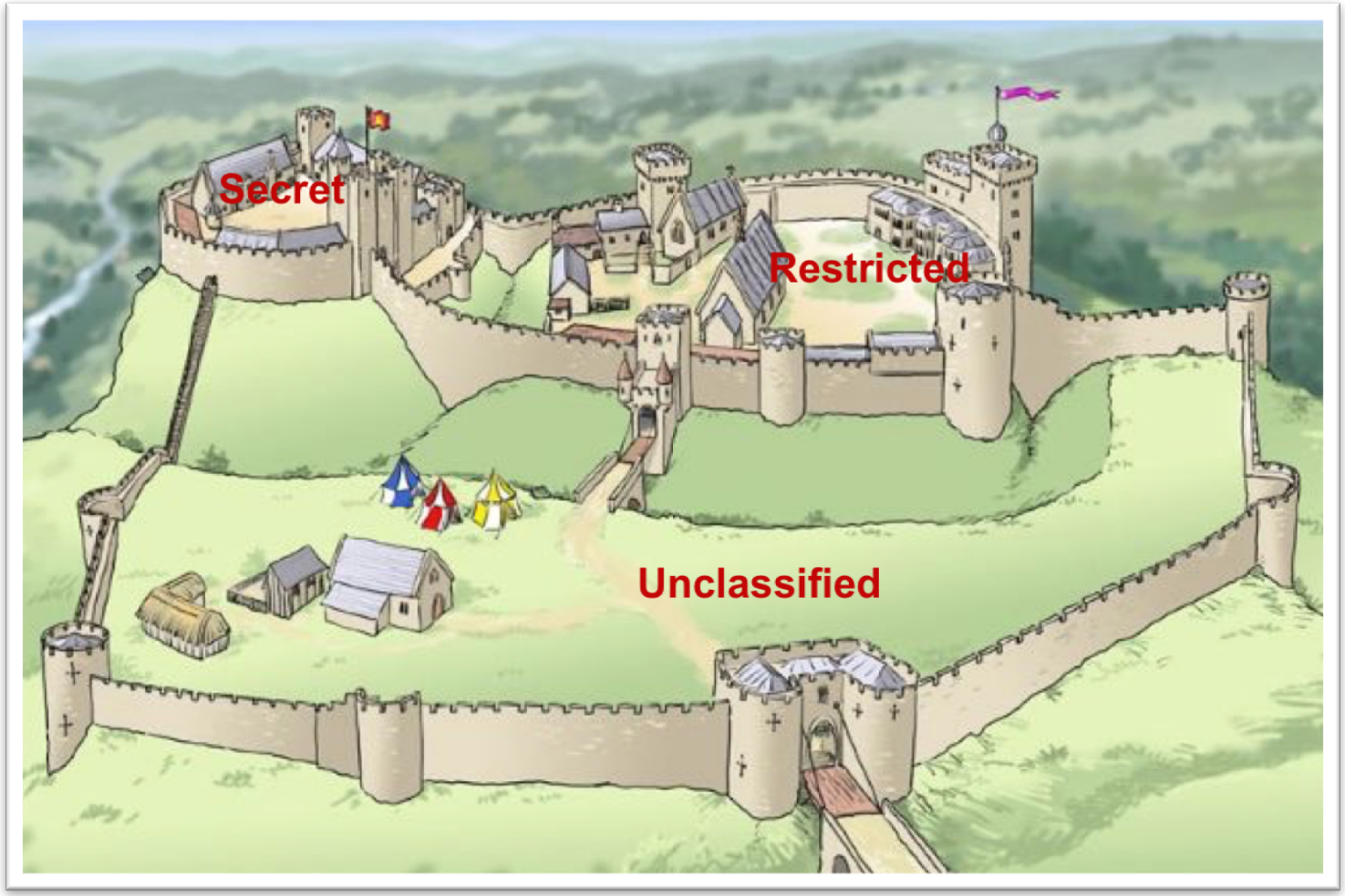
- What are the current pain points
- Related environment changes / triggers
- How can DCS address these challenges
- Work already done on DCS

Historically data security in military focused on communication channels …

… and network perimeter protection



… leading to a lot of perimeters

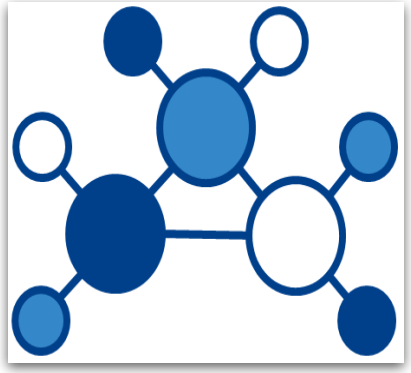


Current pain points

Trust model and spectacular failures

Information sharing

Environment Changes



Federated operations

Cloud solutions and outsourced services

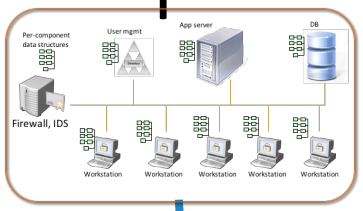
What is Data Centric Security (DCS)

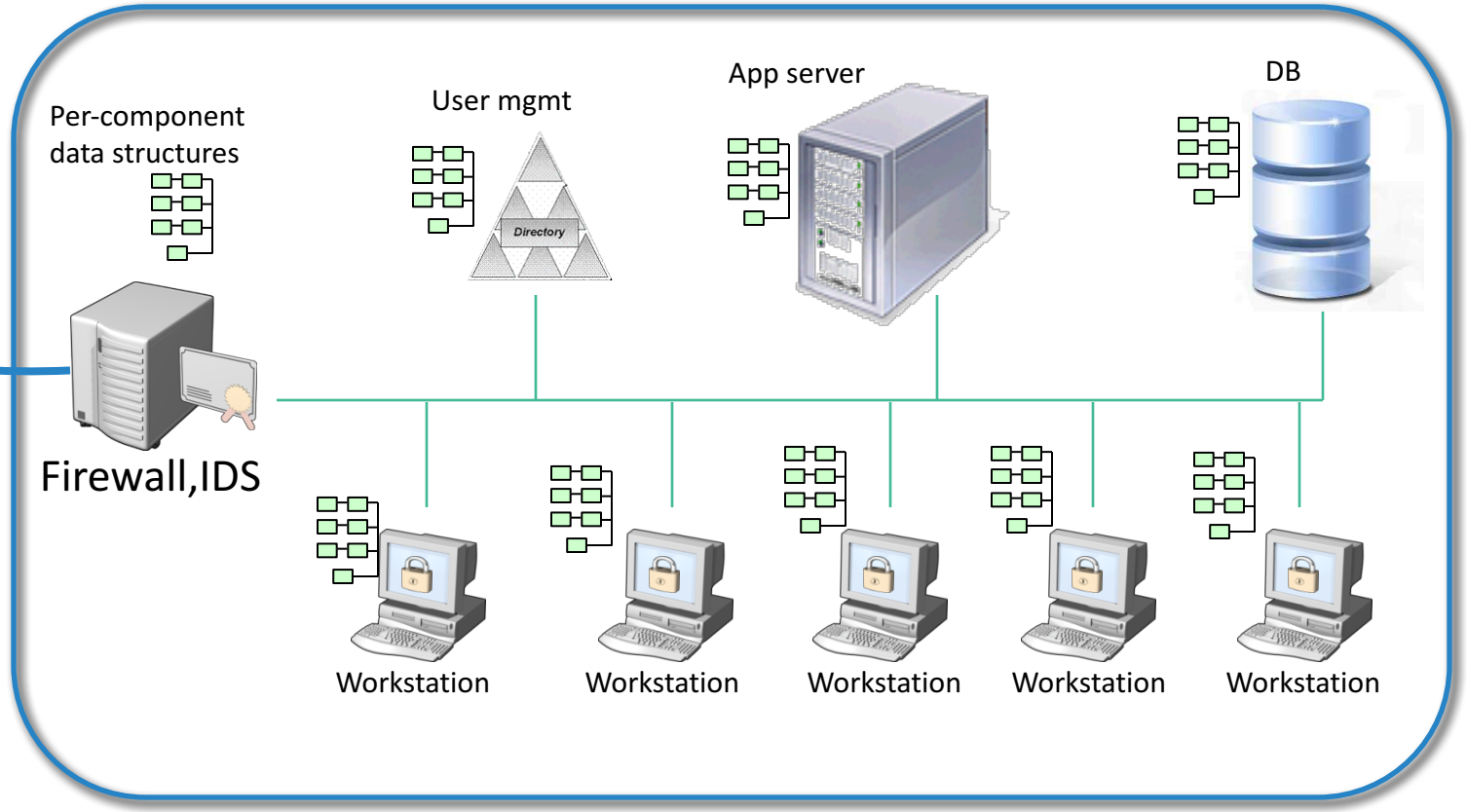
Data Centric Security

Characterized by

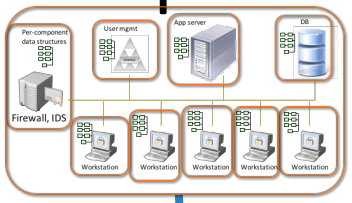
- Focus on protecting data objects rather than domains
- Meta-data to facilitate protection
- Protection includes any combination of Confidentiality, Integrity, Availability
- Facilitates various solutions for access management at the object level

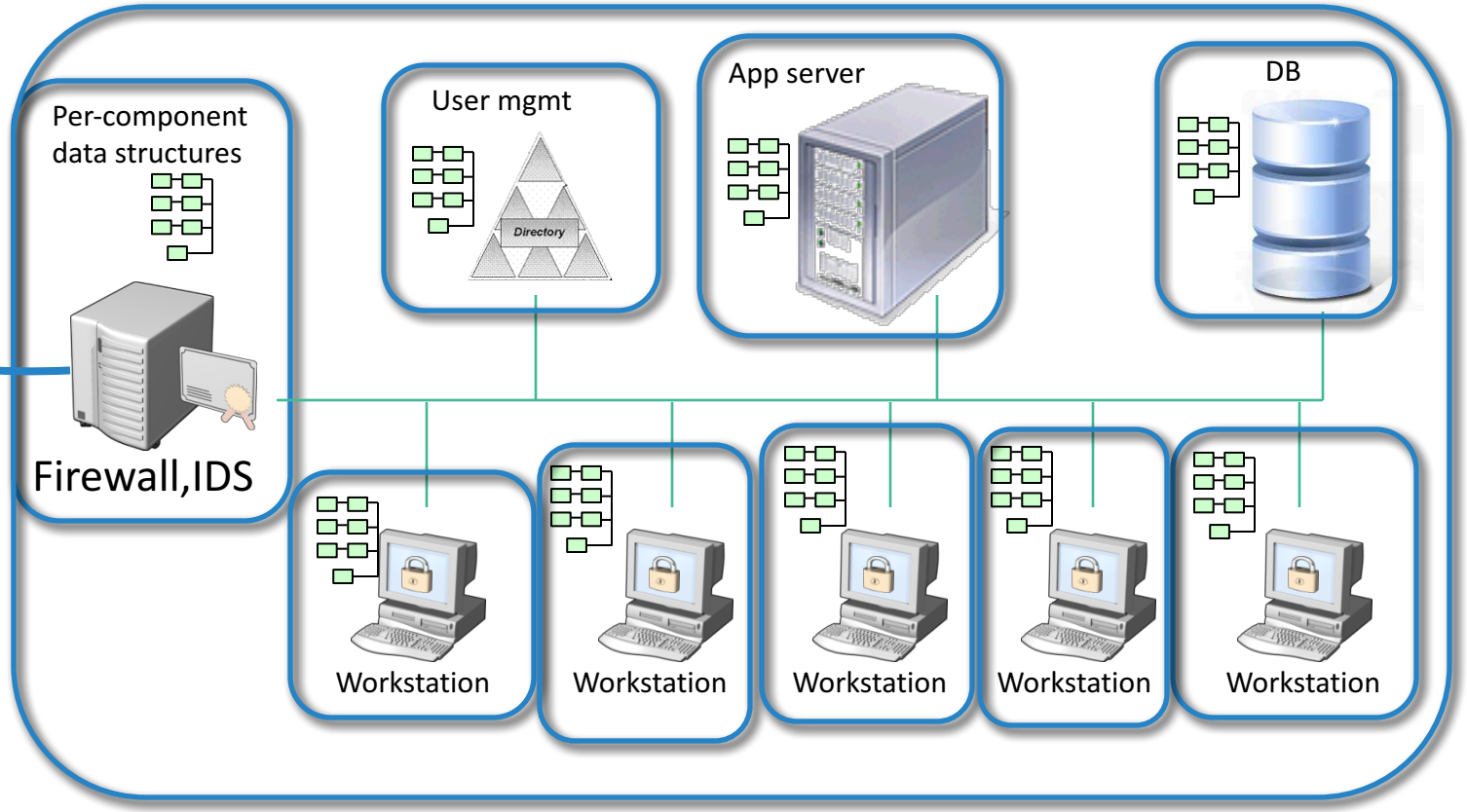
DCS: From perimeter to object level protection



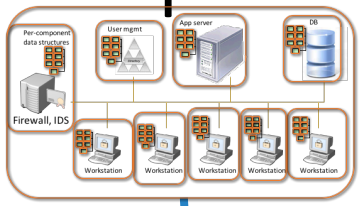


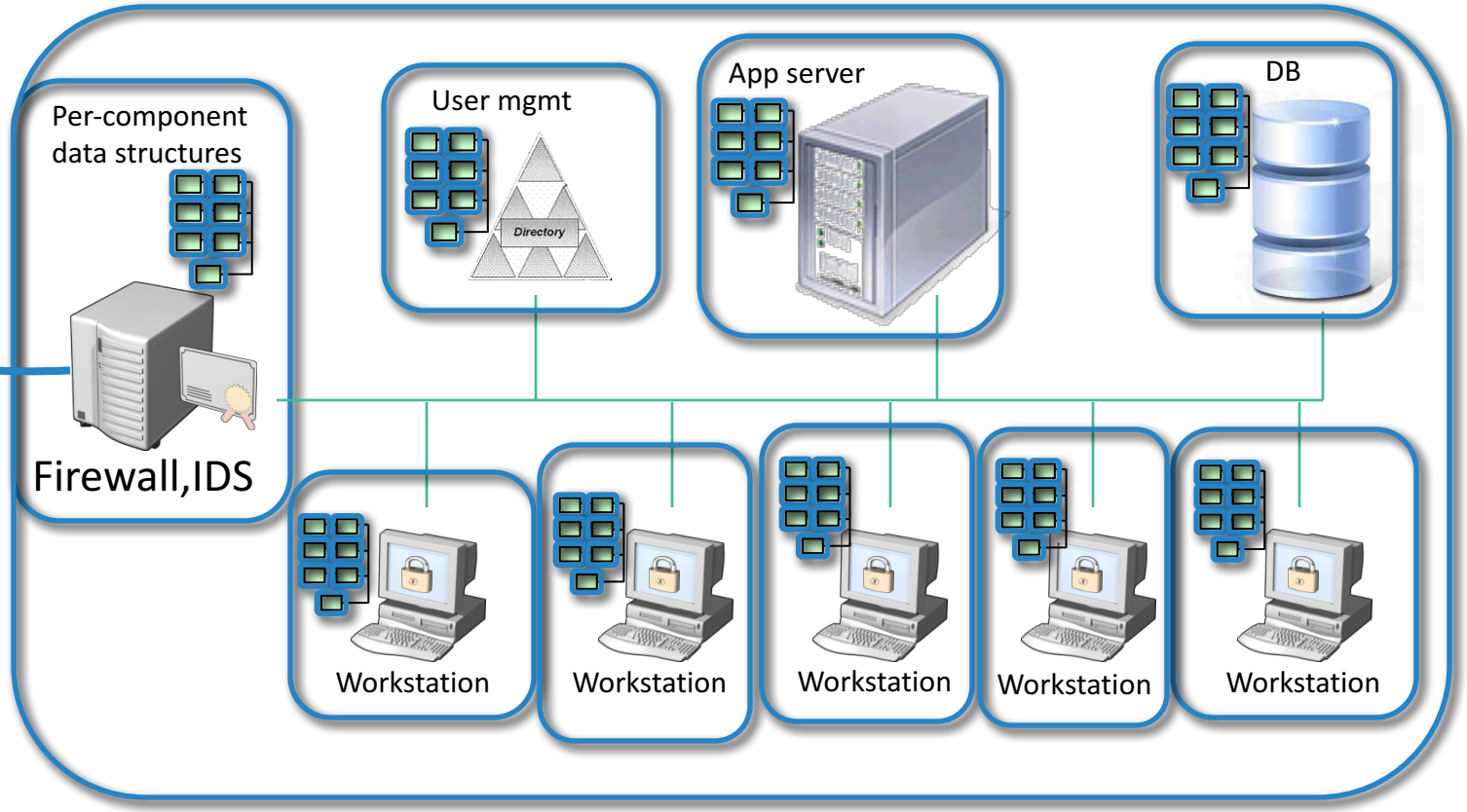
DCS: From perimeter to object level protection



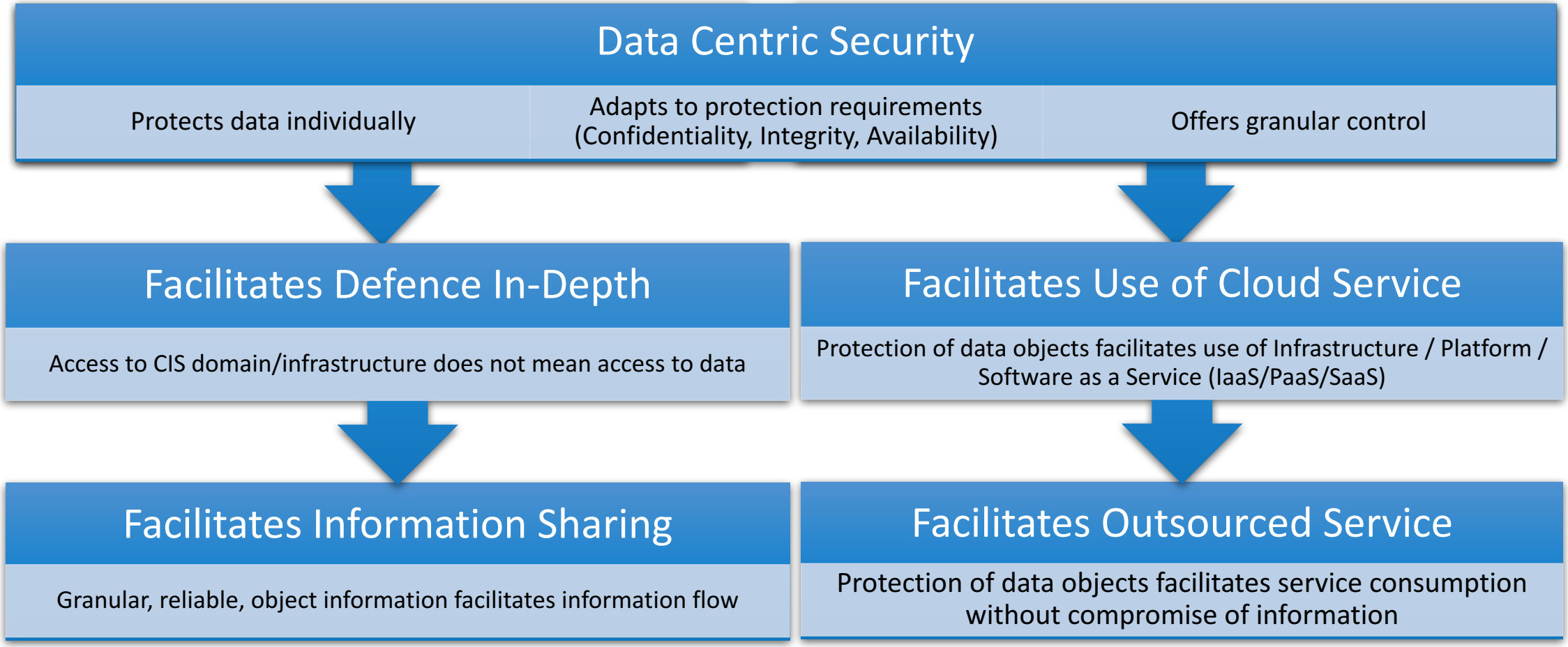


DCS: From perimeter to object level protection



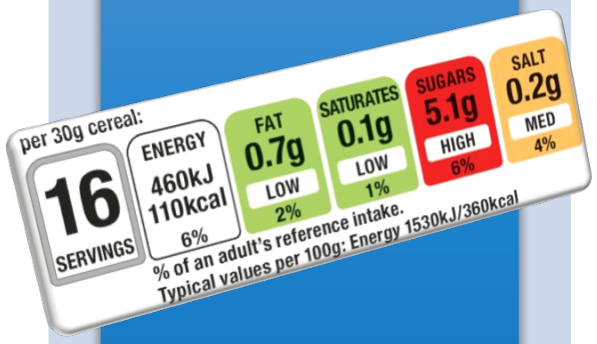


How can DCS address the pain points and triggers



Existing/ongoing work on DCS

Labelling (STANAG 4774)



Binding (STANAG 4778)

Guards

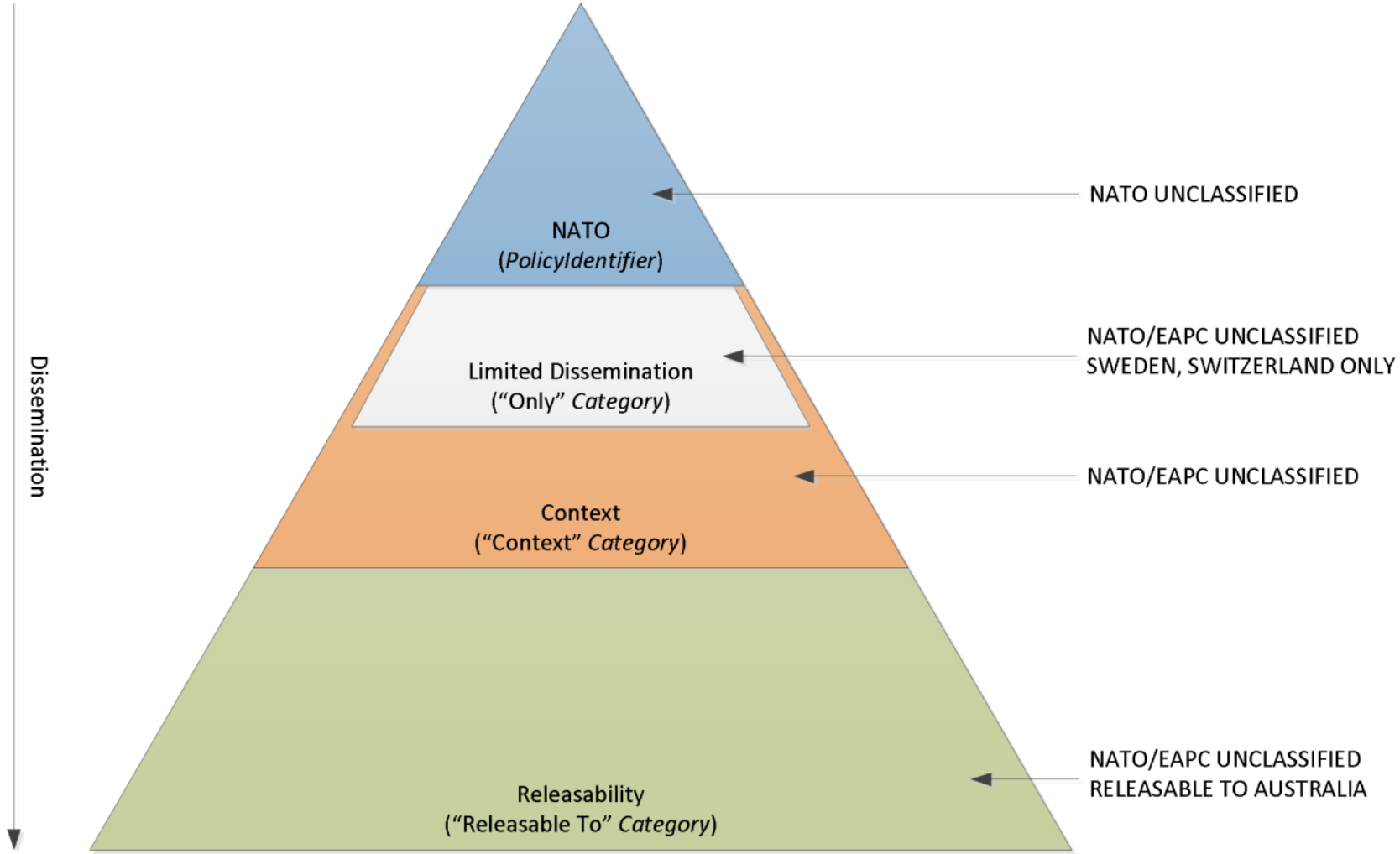
Existing NCI Agency studies & development

- Object Level Protection (OLP)
- Cryptographic Access Control
- Content Protection and Release (CPR)

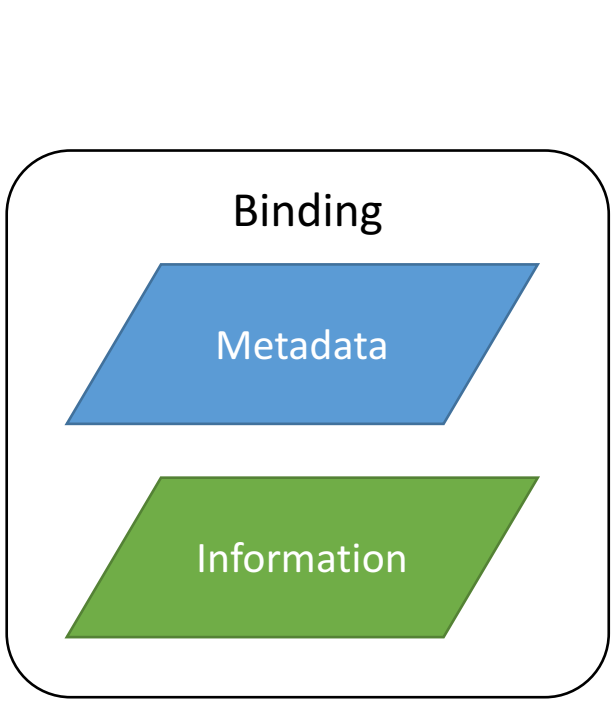
Challenge 1: Labelling

- All data needs to be labelled → STANAG 4774 and 4778
- Complex metadata
  - Cumbersome to assign
  - Large base of pre-existing documents → Assisted labelling based on semantic analysis and machine learning
  - Difficult to interpret by human → Bridge predicates for translation of content properties to sensitivity markings
- Backwards compatibility → Bridge predicates for translation of content properties to sensitivity markings

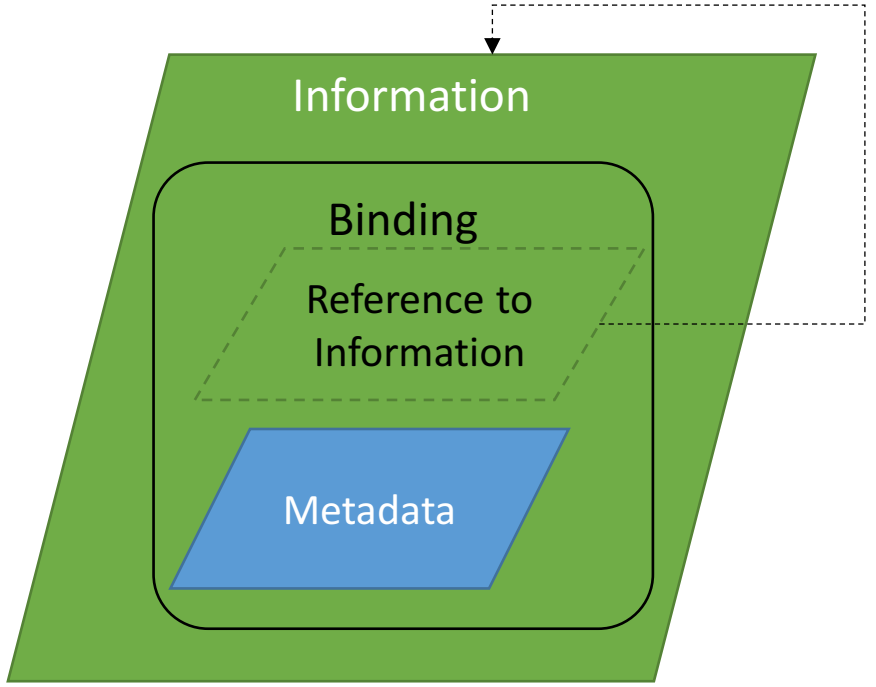
Labelling of data: STANAG 4774



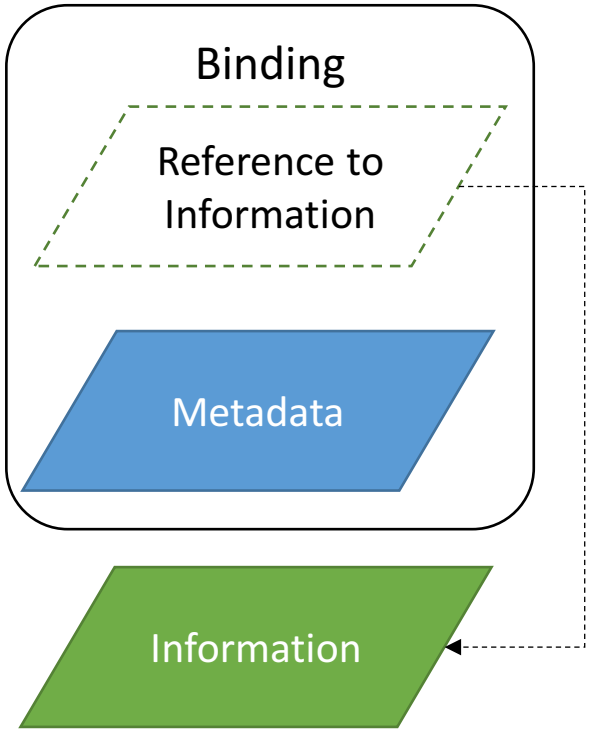
Labelling of data: STANAG 4778



encapsulating



embedded

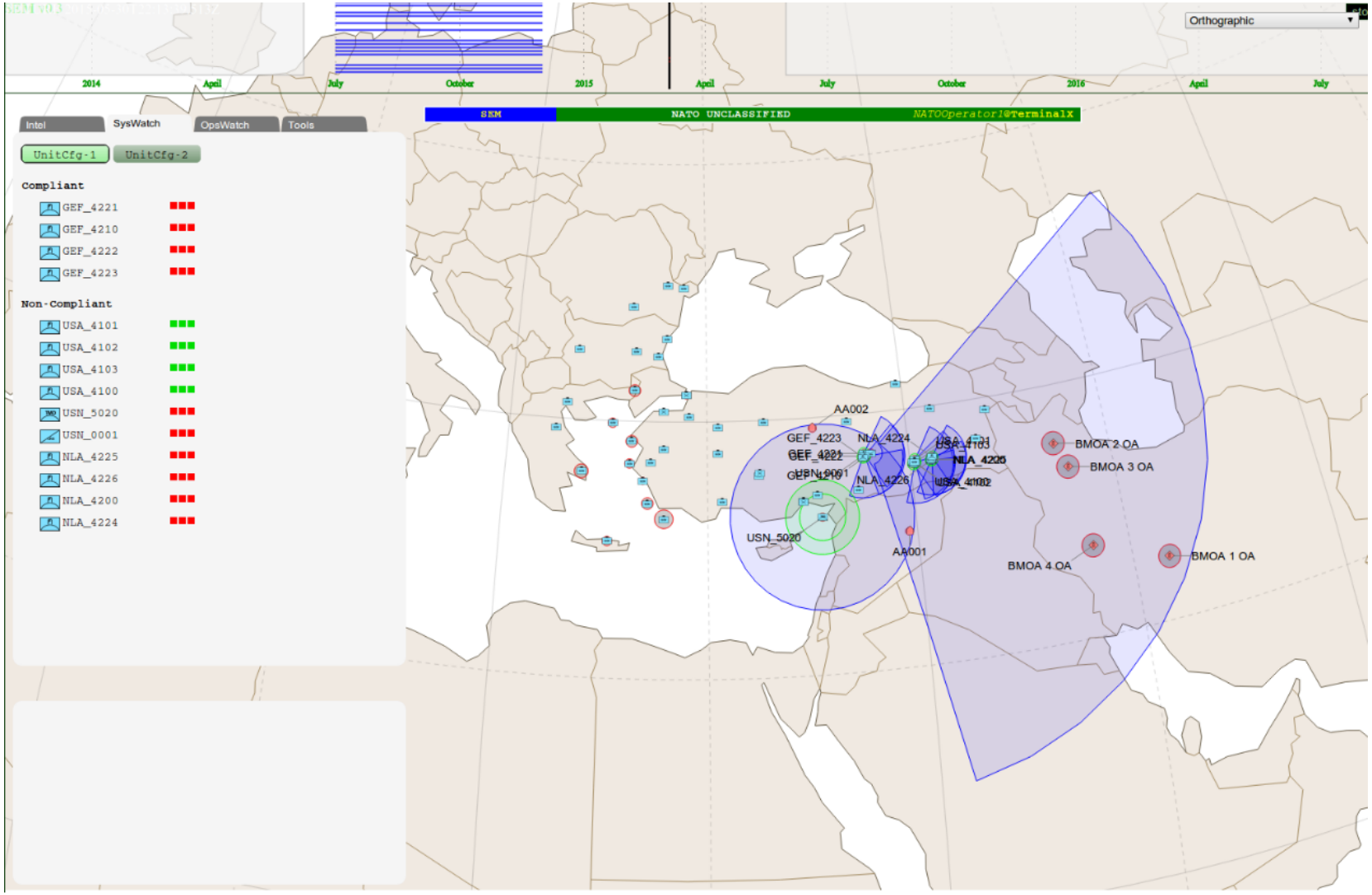


detached

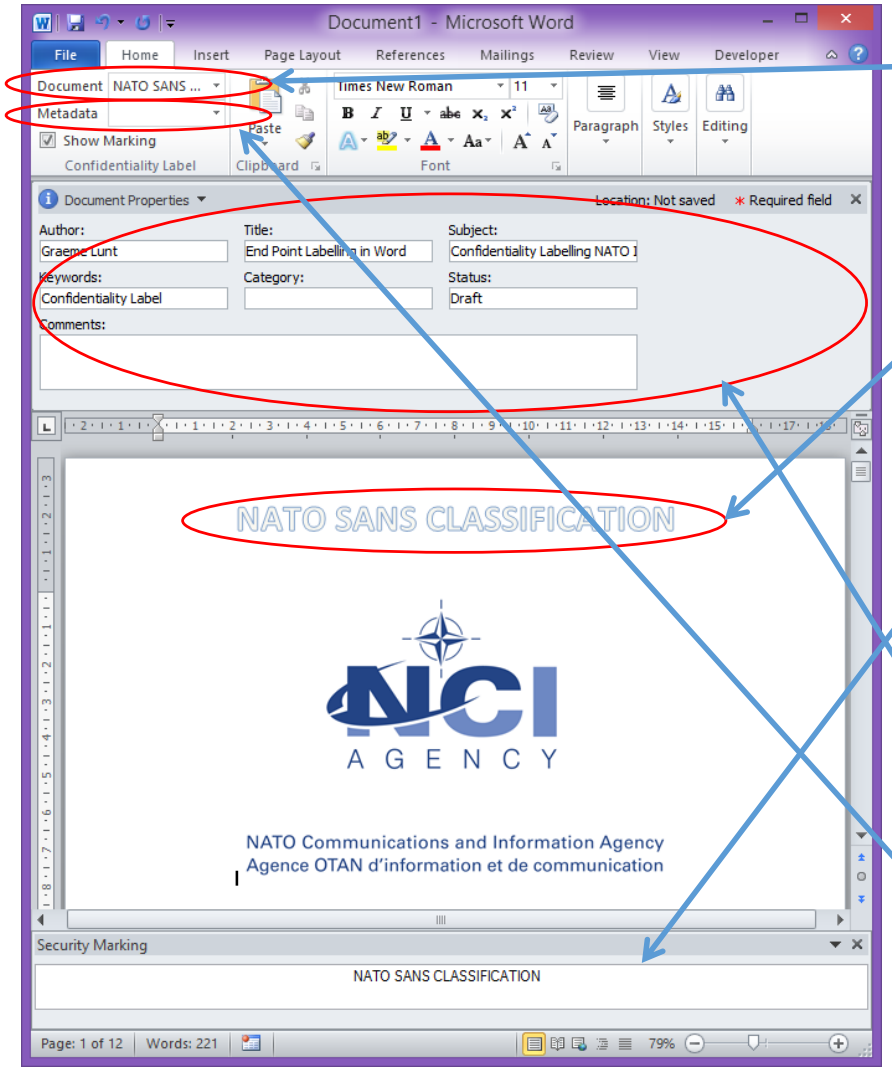
Compatibility with legacy systems and human processing

- Many existing systems support only sensitivity markings
- Content properties can be complex and confusing to the human users
  - Handling of physical representation of information (e.g. print out, computer display)
- Bridge predicates enable mapping from attributes to sensitivity markings
  - Or any other markings (e.g. availability, integrity)

Bridge predicate example: display markings

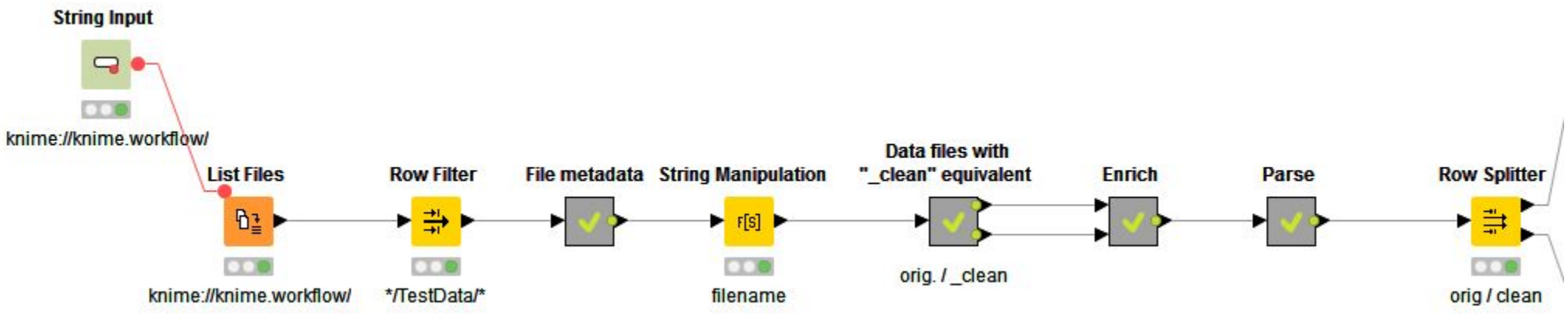


Assisted labelling during creation



- Originator Confidentiality Label for whole document
- Corresponding security marking embedded within document.
- Security marking also shown in footer
- Document Properties mapped to NCMS
- Metadata Confidentiality Label

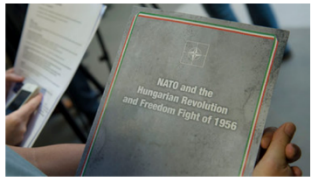
Assisted classification of existing data



e-Library › NATO Archives

Last updated: 26 Jun. 2015 12:51

NATO ARCHIVES
Files on-line



The NATO Archives revisits the Hungarian Revolution on its 60th anniversary

24 Oct. 2016

At the request of the Hungarian Delegation to NATO, the NATO Archives published a softbound collection of publicly disclosed NATO documents to help support the commemoration ceremony for the Hungarian Revolution of 1956 held today at NATO HQ. The publication, titled "NATO and the Hungarian Revolution and Freedom Fight of 1956", showcases documents dating from 1956-1959 to present the story of NATO's reactions and responses to the dramatic events that were unfolding in Hungary.

more

The NATO Archives revisits the Alliance's international arts heritage

01 Jun. 2016

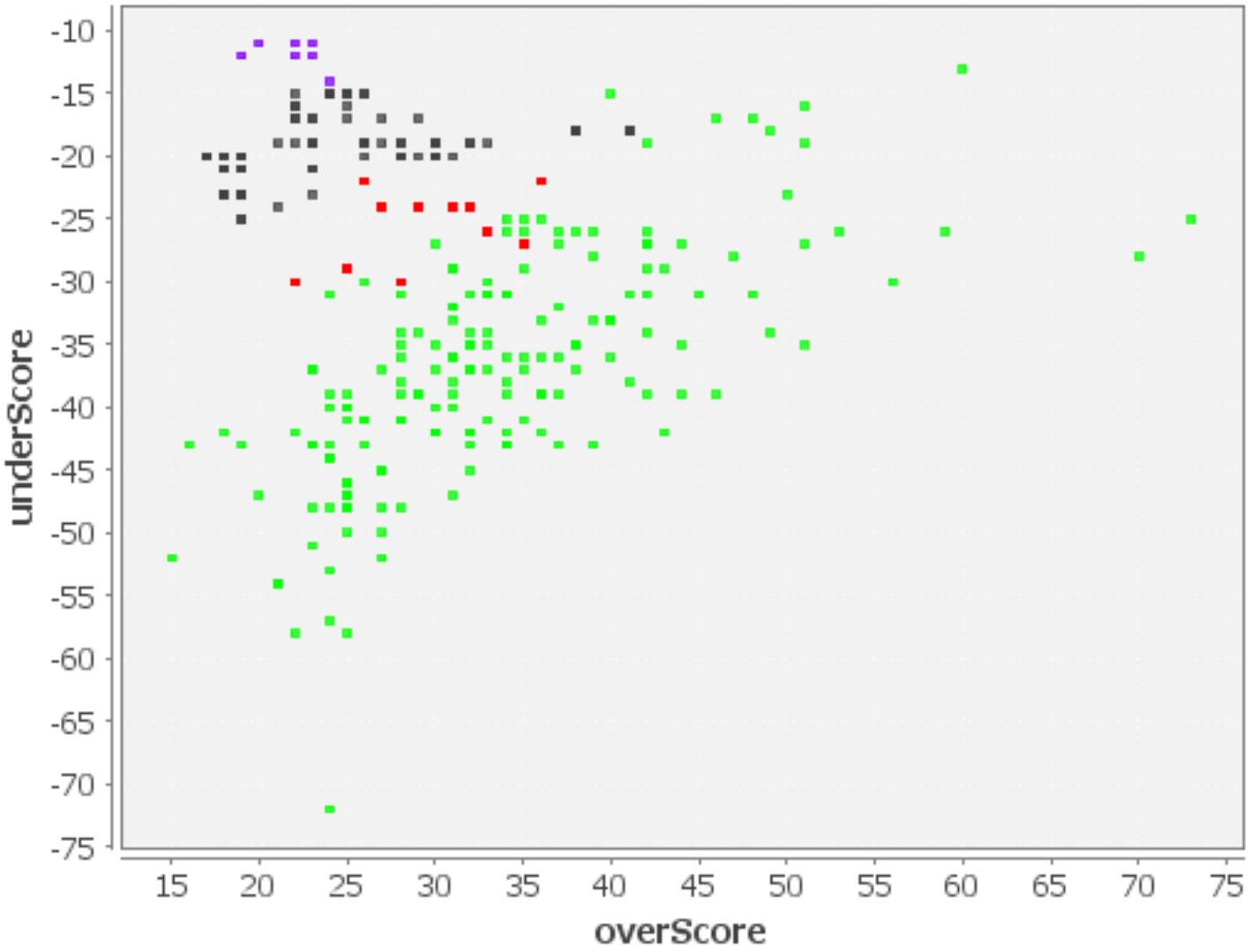
ALSO AVAILABLE IN:

- English
- French

NATO ARCHIVES ONLINE

Visit NATO Archives Online, our web-based research tool that provides access to thousands of declassified and publicly disclosed NATO documents.

Accuracy of automated classification



	top secret	secret	confidential
top secret	± 0	$+1$	$+2$
secret	-1	± 0	$+1$
confidential	-2	-1	± 0

$$R = CD^T$$

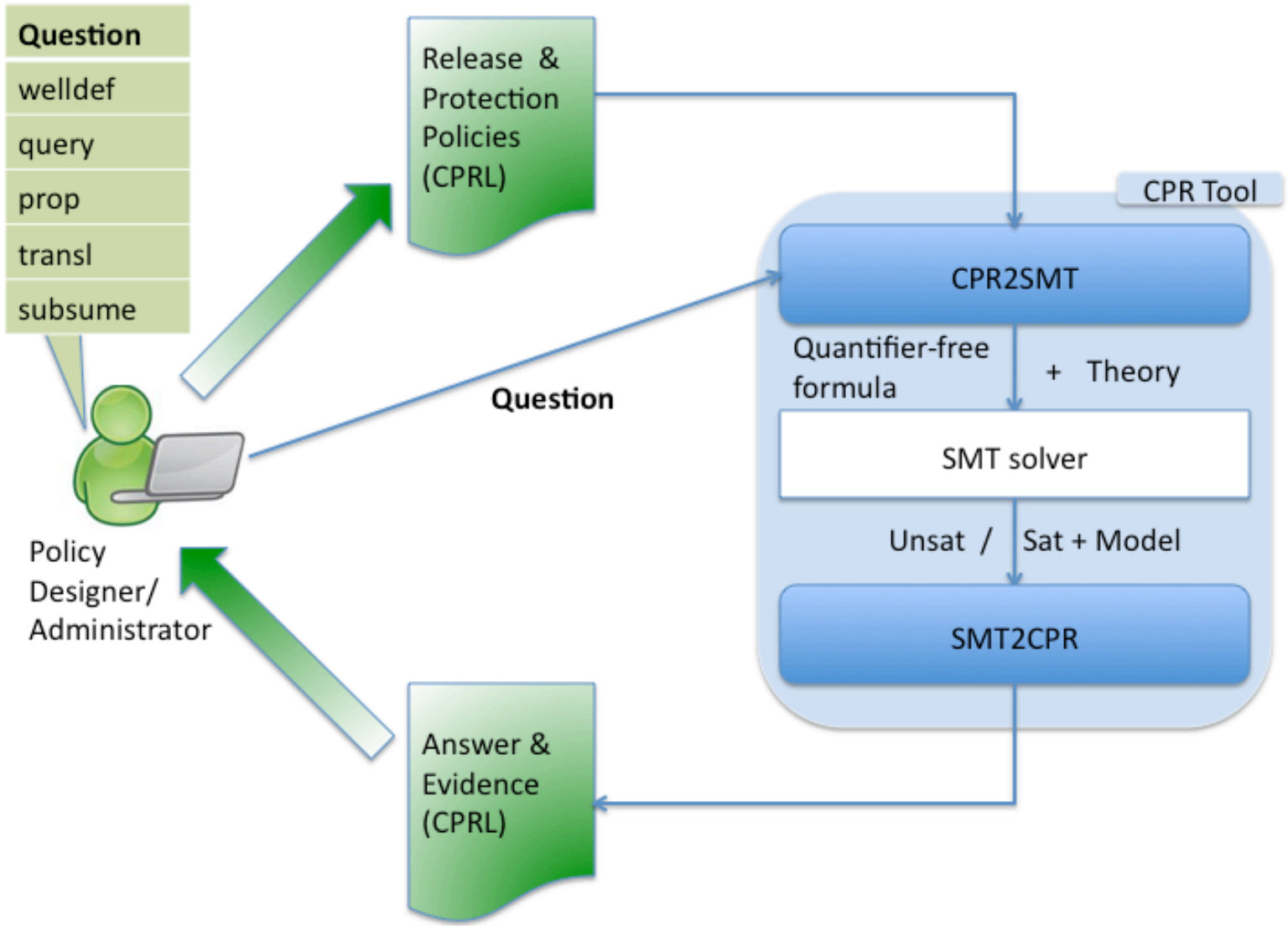
Challenge 2: Complex security policies

```
type Clearances = { None, Unclassified, Restricted, Confidential, Secret };
type Confidentialities = { NoInfo, Basic, Standard, Enhanced, High };
type Categories = { PublicInformation, ScenarioDescriptions, COIMetrics };
type Topics = { HighValuesAssetsOrLists, ThreatOperatingAreas,
                ThreatAndInterceptorTrajectoryDetails,
                GeneralHazardAreaLocation, SubmunitionAreaLocation };
type Organizations = { NATO_Org, Red_Cross };
entity User = [ clearance : Clearances, organization : Organizations ];
entity Resource = [ category : Categories, topic : Topics ];
entity Terminal = [ confidentiality : Confidentialities,
    mgauthority : Organizations ];
```

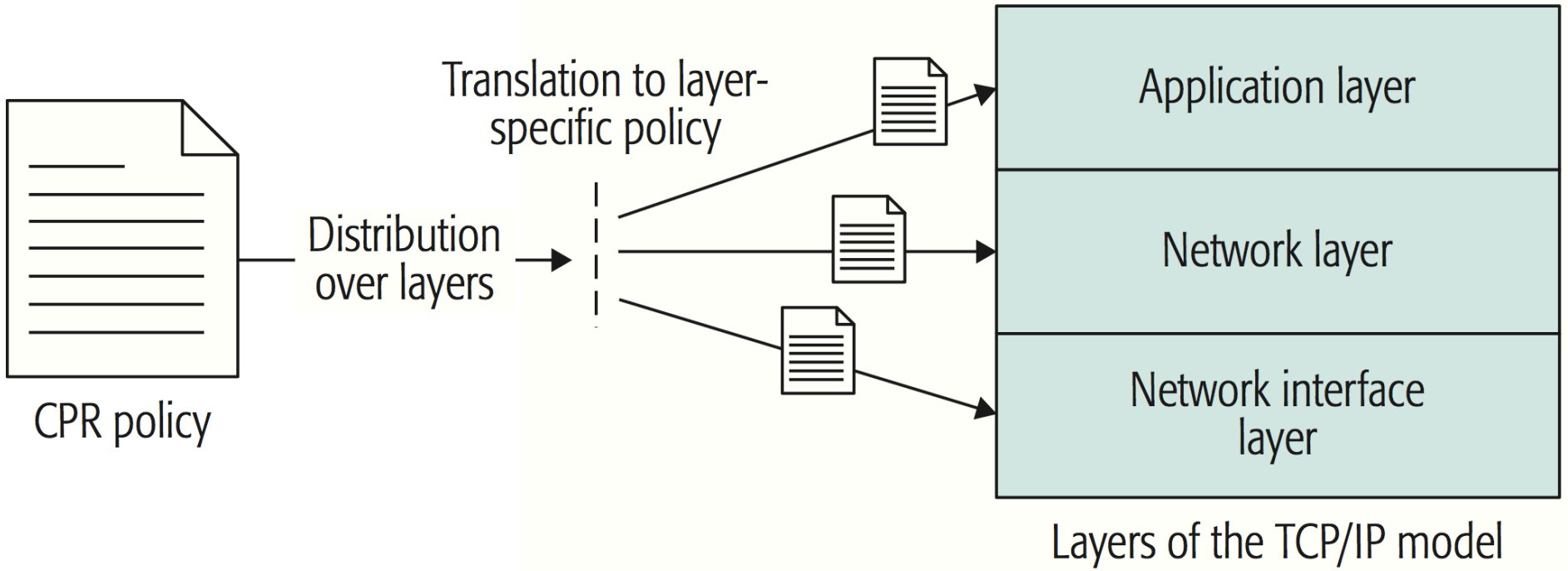
```
release rP1 = (resource.category = PublicInformation);
release rP2 = (user.clearance = Secret) &
    (user.organization = NATO_Org) &
    (resource.category = ScenarioDescriptions) &
    ((resource.topic = HighValuesAssetsOrLists) |
        (resource.topic = ThreatOperatingAreas) |
        (resource.topic = ThreatAndInterceptorTrajectoryDetails));
release rP3 = (user.organization = NATO_Org) &
    (resource.category = COIMetrics) &
    (resource.topic = GeneralHazardAreaLocation);
release rP4 = (user.organization = NATO_Org) &
    (resource.category = COIMetrics) &
    (resource.topic = SubmunitionAreaLocation) &
    ((user.clearance = Secret)       |
    (user.clearance = Confidential) |
    (user.clearance = Restricted)    );
```

```
protection pP1 = (resource.category = PublicInformation);
protection pP2 = (resource.category = ScenarioDescriptions) &
    (terminal.mgauthority = NATO_Org) &
    ((resource.topic = HighValuesAssetsOrLists) |
        (resource.topic = ThreatOperatingAreas) |
        (resource.topic = ThreatAndInterceptorTrajectoryDetails)) &
    ((terminal.confidentiality = High) |
        (terminal.confidentiality = Enhanced));
protection pP3 = (resource.category = COIMetrics) &
    (resource.topic = GeneralHazardAreaLocation) &
    ((terminal.confidentiality = High)       |
        (terminal.confidentiality = Enhanced) |
        (terminal.confidentiality = Standard) |
        (terminal.confidentiality = Basic)    |
        (terminal.confidentiality = NoInfo)) &
    (terminal.mgauthority = NATO_Org);
protection pP4 = (resource.category = COIMetrics) &
    (resource.topic = SubmunitionAreaLocation) &
    !(terminal.confidentiality = NoInfo) &
    (terminal.mgauthority = NATO_Org);
```

Complex security policies



Challenge 3: How and where to enforce it?



Applying data-centric security to IoT