AMRES
Serbian Academic Network

BELGRADE SECURITY WORKSHOP 2015

Creating a University CERT:
CERT OSIRIS

Jean BENOIT & Guilhem BORGHESI,
University of Strasbourg /
RENATER Campus Best Practice

UNIVERSITÉ DE STRASBOURG

RENATER
CONNECTEUR DE SAVOIRS

GÉANT

Summary

- University of Strasbourg
- CERT OSIRIS : how it all started
- Services currently operated
- Tools
- Key achievements
- What's next ?
- Conclusion

University of Strasbourg

- 4 centuries of existence (founded 1621)
- 45 000 students
- 6 000 professors, researchers and technical staff
- 38 faculties, 77 research groups and 3 active Nobel Price recipients
- IT staff : over 100 people

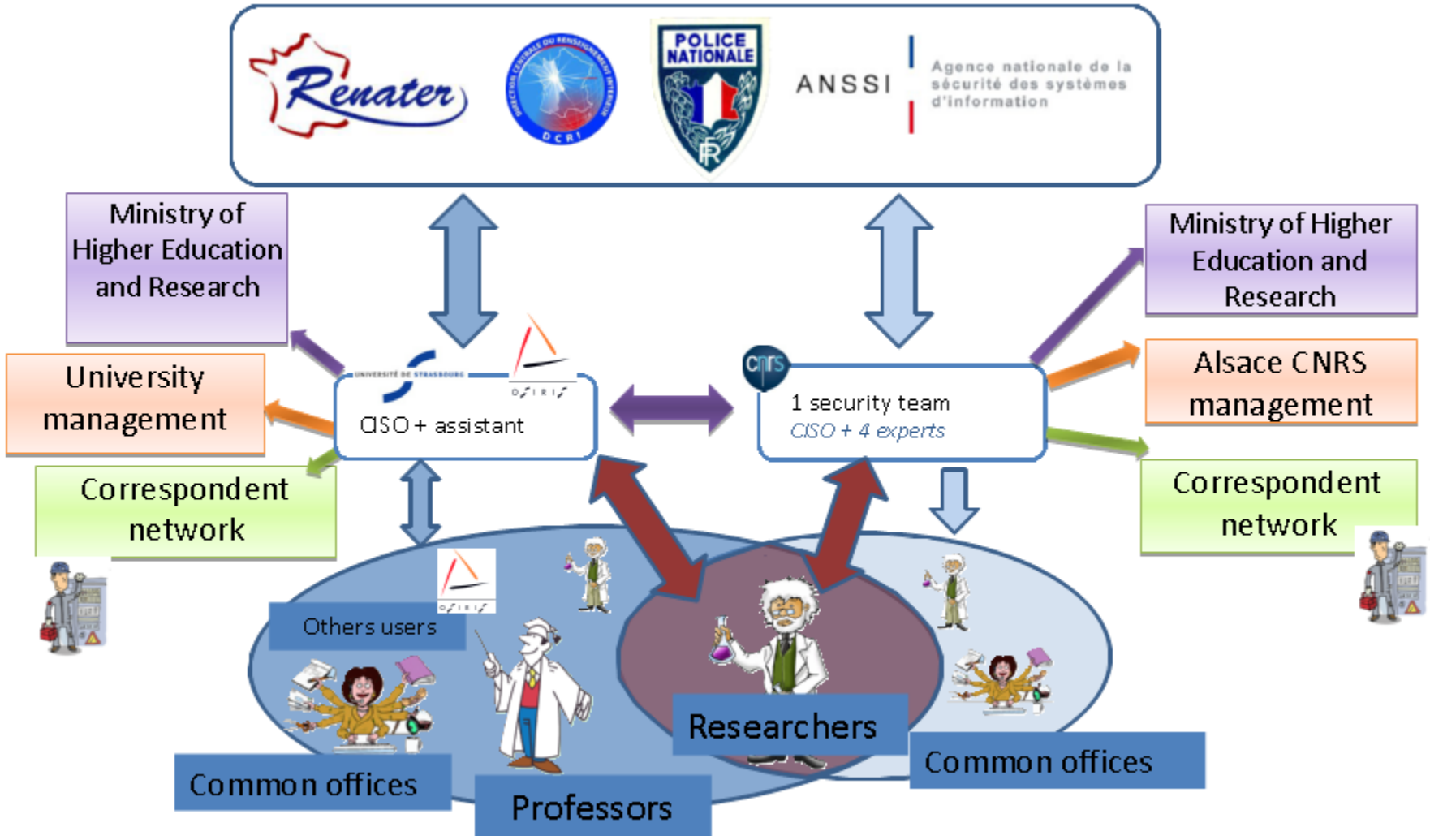
CERT OSIRIS : how it all started

- Why a CERT ?
- Context: organizational complexity
  - Different structures (faculty, labs etc..) intertwined
  - Each structure is controlled and financed by at least 2 actors:
    - University for the teaching part
    - A research agency (CNRS, INSERM etc.) for the research part
- Each structure appoints a security contact, often the same person
- Merging of 3 universities (2009)
- Most labs make heavy use of the services provided by the university IT department (network access, email, applications etc.)
- A willingness to work together:
  - Security expertise is a scarce resource
  - Co-ordinated effort → efficient use of these resources
  - Goal : increase the global level of IT security

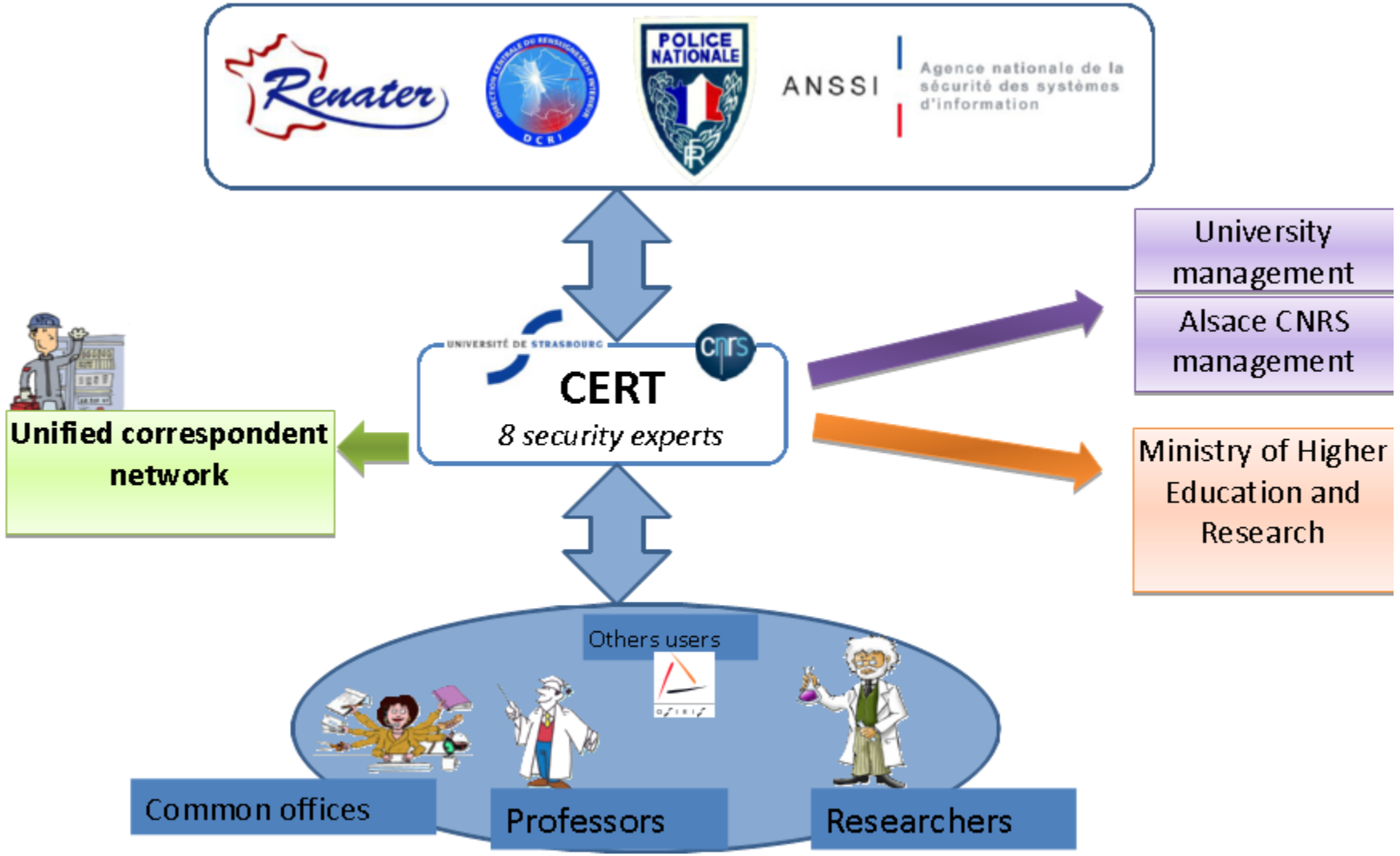
CERT OSIRIS: how it all started

- Project start: 2011/02
  - Approved by management and partners
  - First deployment of tools (incident handling, mailing lists etc.)
- Official start: 2012/01/01
- Organization selected
  - Informal structure of 8 security experts
  - Co-lead by the CISOs of CNRS and University

Before the CERT OSIRIS...



… and NOW


Renater
POLICE NATIONALE
ANSSI
Agence nationale de la sécurité des systèmes d'information
University management
Alsace CNRS management
Ministry of Higher Education and Research
UNIVERSITÉ DE STRASBOURG
cnrs
CERT
8 security experts
Unified correspondent network
Others users
Common offices
Professors
Researchers

CERT Services

- Security incident handling
  - Network monitoring, intrusion detection
  - Incident handed over to the local security correspondent
  - Blocking to prevent further impacts : address filtering on the backbone, account locking
  - Incident tracking, providing help to the security correspondent
  - Coordination between partners (police, justice, security chain)
- Training
  - Training programs for users and administrators
  - Awareness programs

CERT Services

- Providing security information
  - Relaying security vulnerability and alerts (issued by national CERTs)
  - Monitoring legal developments
- Supporting Information Security Management Systems deployment
  - Upon request by any lab or faculty
- Forensics
  - Proof collection
  - Log analysis

Tools (1/2)

- Unified network of security correspondent
- Incident tracking (Request Tracker)
  - Common tool also used IT department
  - Better coordination
- Communication
  - Single contact : cert-osiris@unistra.fr
  - Website : http://cert-osiris.unistra.fr
  - Phone: through IT Department support line

Tools (2/2)

- Compromised account monitoring
  - fixed rate of sent e-mails per hour per login
- Automation
  - Tool-chain to create security incident including all relevant informations: network, contact etc.
  - Reminders (when correspondent won't answer)
- Blocking
  - IP address
  - User login
  - Domain names (RPZ)

Host compromission

Compromised account

Phishings URL

Missing tools

- Netflow: project starting in april
- Browser tests
- Network scanner: provided by RENATER

Key achievements

- Building anew the security correspondent network
- Formalization of the security incidents handling process
- Poor user passwords finding
  - Password same as login (350)
  - Password too short (160)
  - Password too simple (14.000 accounts which makes 12 %)
- Training and awareness programs
  - Training « Internet without scare» (100)
  - Awareness campaign for security correspondents (700)

What's next ?

- Extend the CERT to include other Higher-Education institutions in the Alsace region
- More training programs
  - Webdoc to raise security awarness amongs students
- Improve tools

Conclusion

- Increased security posture and awareness
  - our users, our management, our partners and our correspondents
- A clearer and more consistent message
  - to CNRS and University users alike
- Few financial/human resources needed through a more efficient use of them
- Just a informal structure of people willing work together on IT Security !
- Campus Best Practice document: « creating a university CERT » to be released soon in english

BELGRADE SECURITY WORKSHOP 2015