CYBER SECURITY DAYS

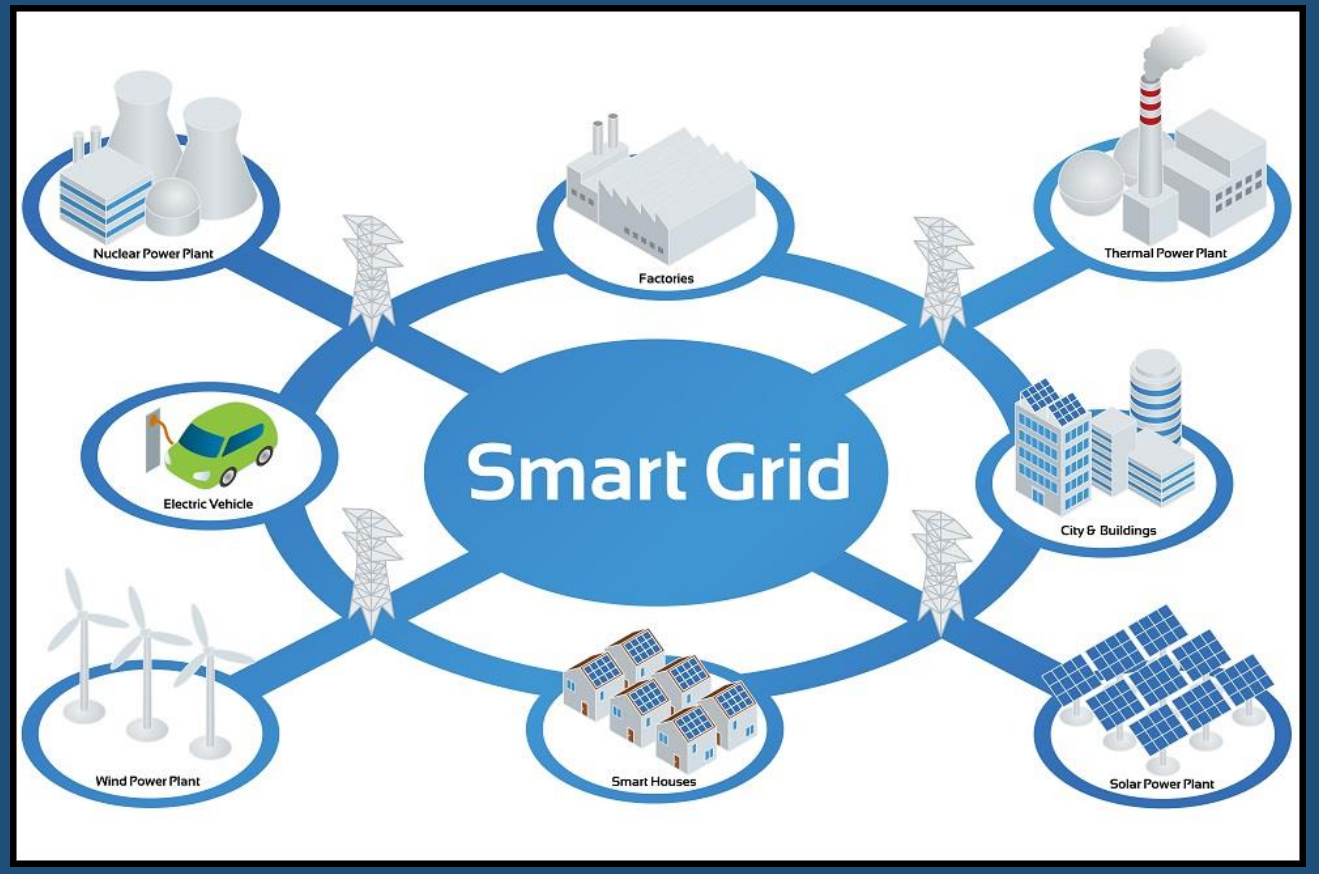
8ème ÉDITION 2018

La Cybersécurité dans le secteur de l'énergie : enjeux et solutions

Haythem EL MIR

Haythem.elmir@keystone.tn

Le secteur de l'énergie a un impact considérable sur la société.



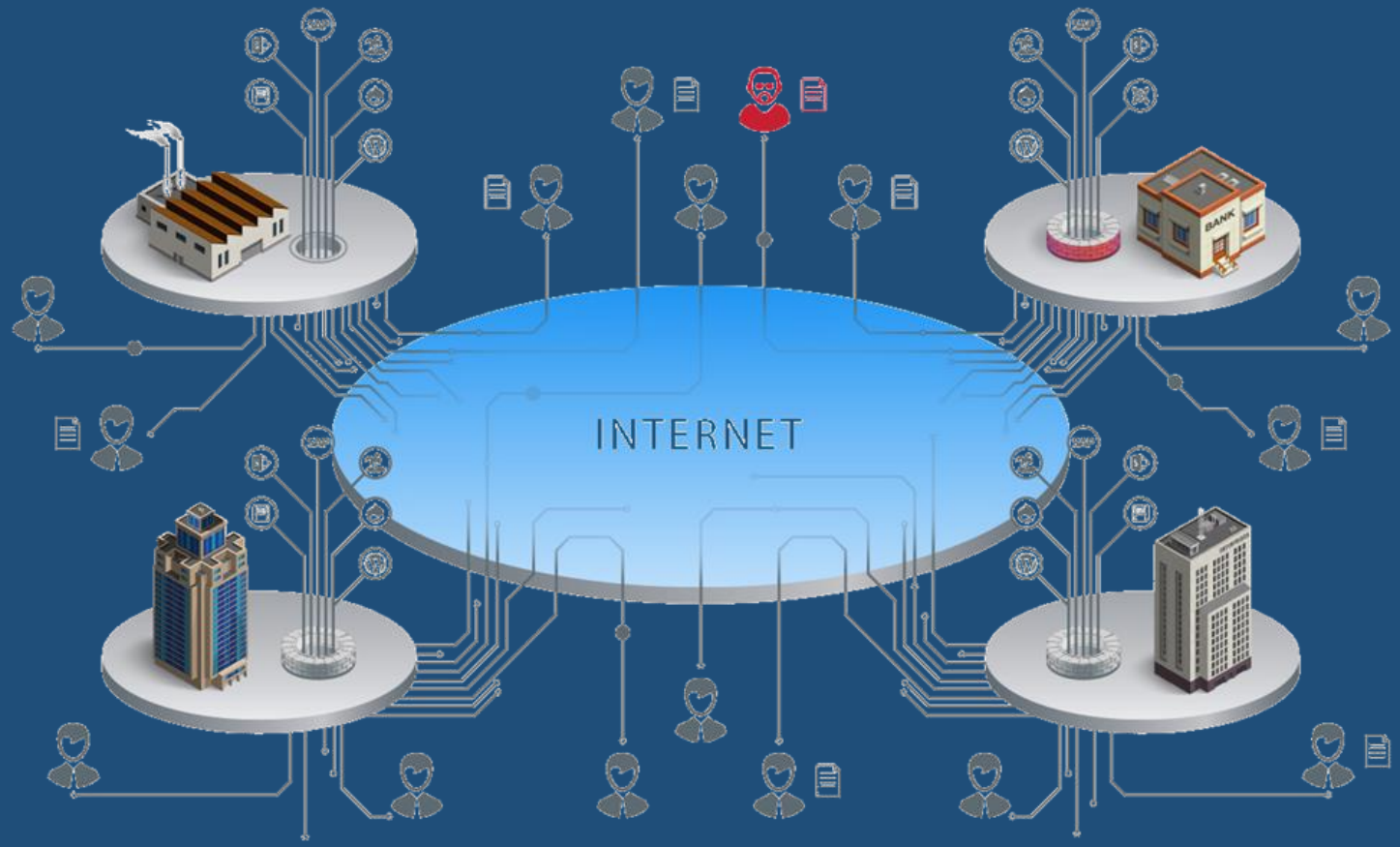
Cas de l’Ukraine en 2015 et 2016

Aujourd'hui: Une totale convergence

La convergence accrue entre les systèmes informatiques et les systèmes technologiques opérationnels offre des opportunités de transformation pour les organisations industrielles.

OT moderne:

- ICS/SCADA
- Télécom
- Transport
- IoT



Digitalisation

=

Exposition

=

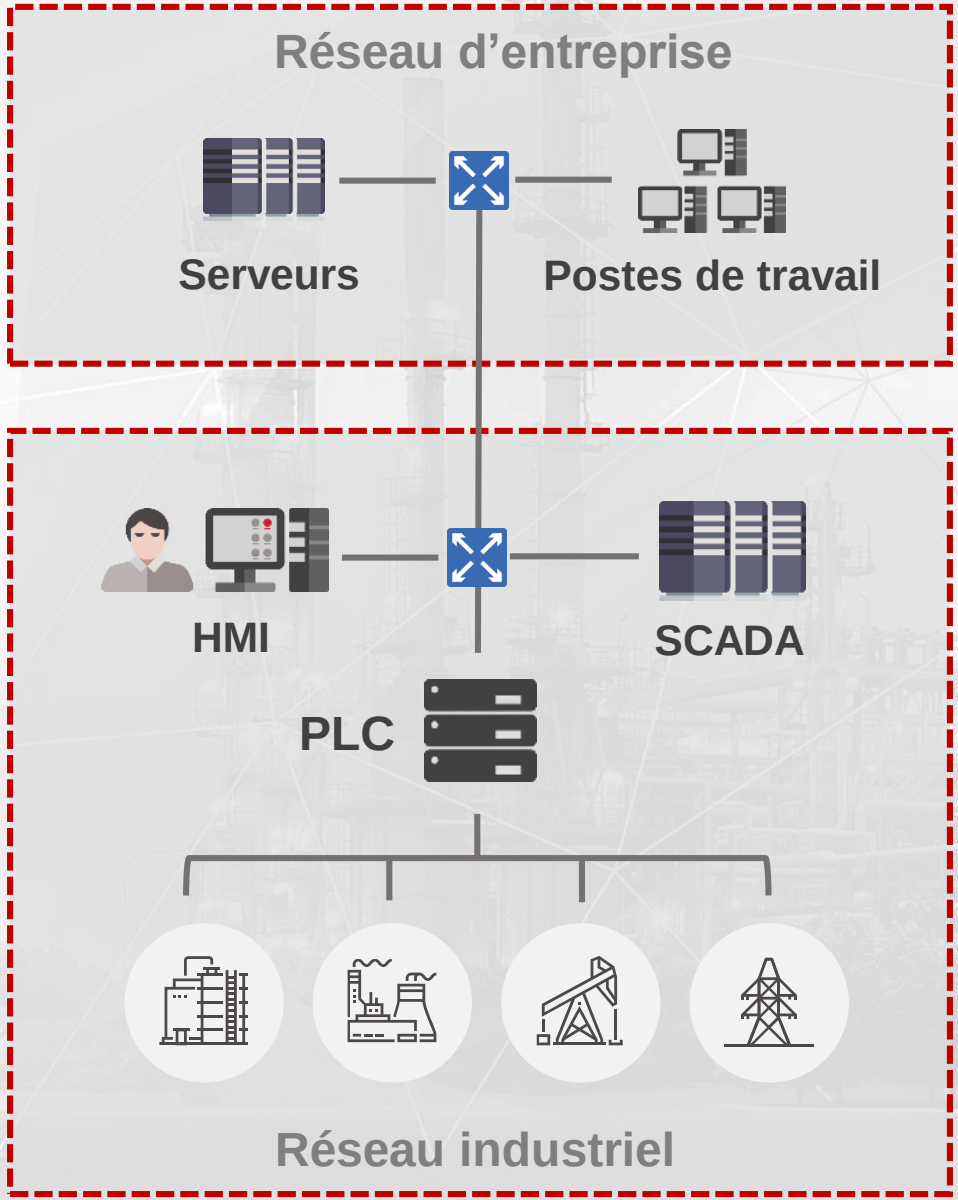
Menaces

La cybersécurité dans le secteur de l’énergie n’est pas une option.

Les risques sont trop importants.

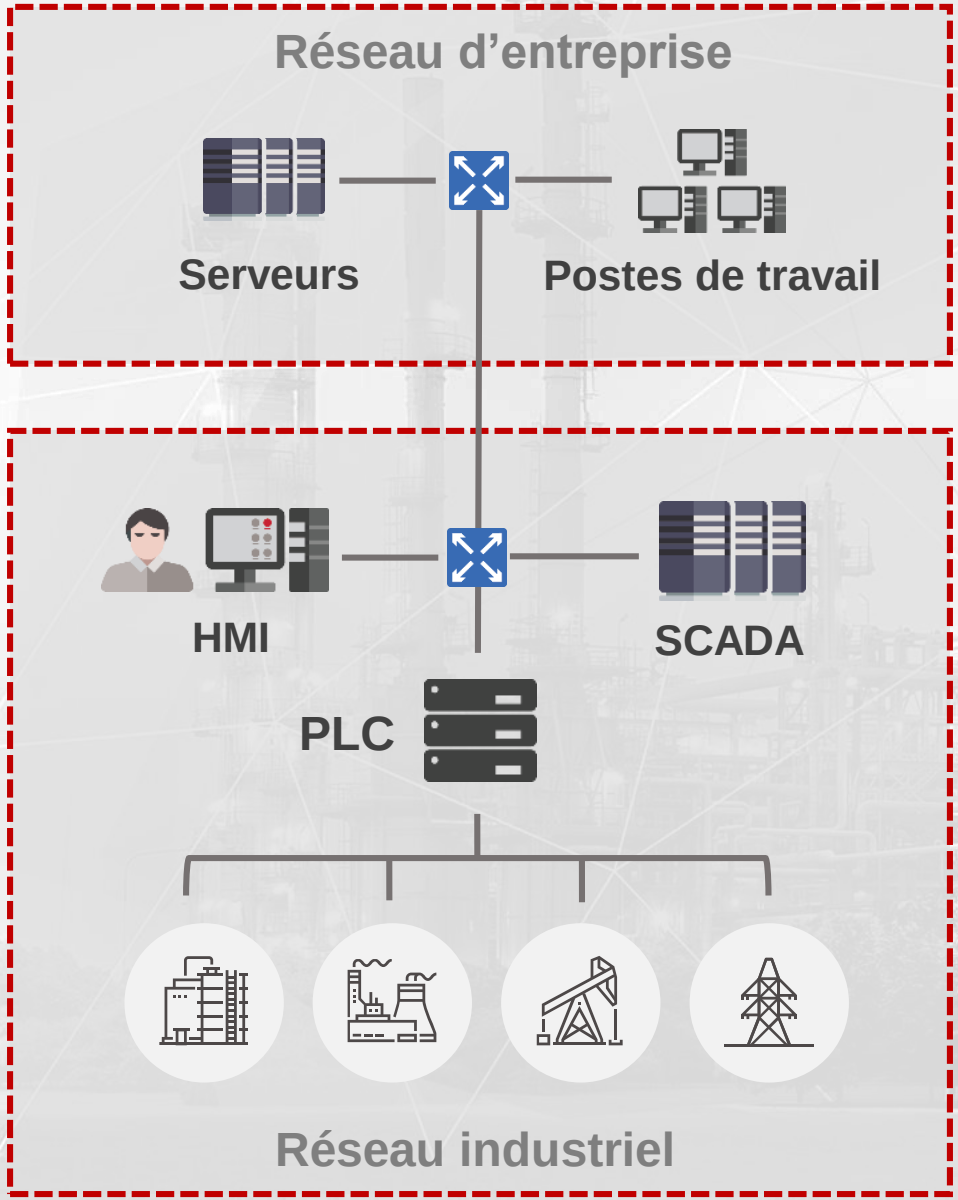
Que sait-on de la cybersécurité ICS?

- Grande surface d'attaque
- Adoption lente des pratiques de sécurité
- Augmentation du nombre d'incidents



Cybersecurité des réseaux industriels

- **Les cyberattaques sont de plus en plus variées et complexes,**
- **Le secteur de l'énergie devient de plus en plus digitalisé,**
- **La nécessité de faire évoluer les pratiques en matière de cybersécurité devient une priorité,**
- **Les réseaux industriels sont mal sécurisés contre les attaques des systèmes d'information d'entreprise,**
- **La plupart des attaques sont faciles à mettre en œuvre.**



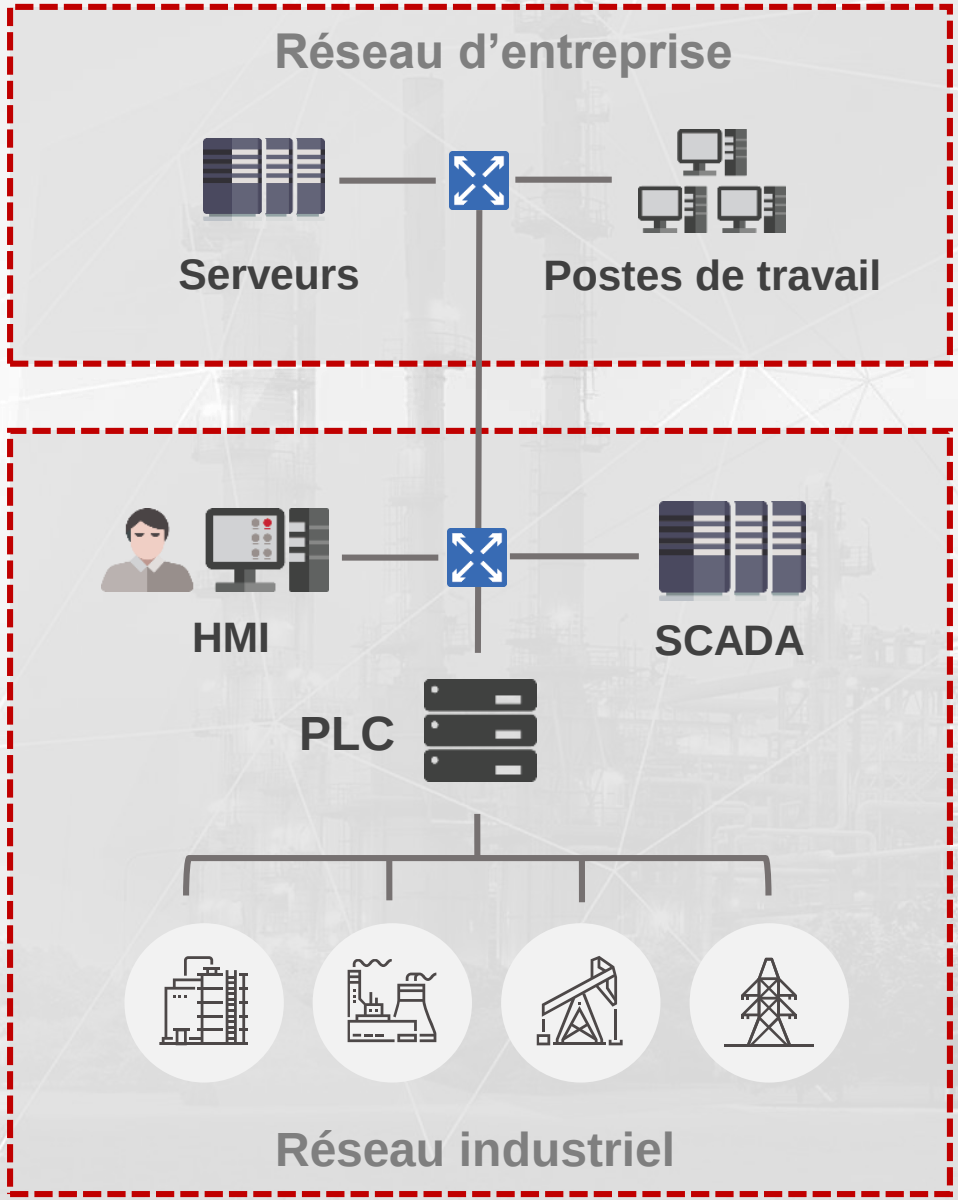
On est bien conscient, mais!

Lente adoption des pratiques de sécurité

Mesures de protection classiques?

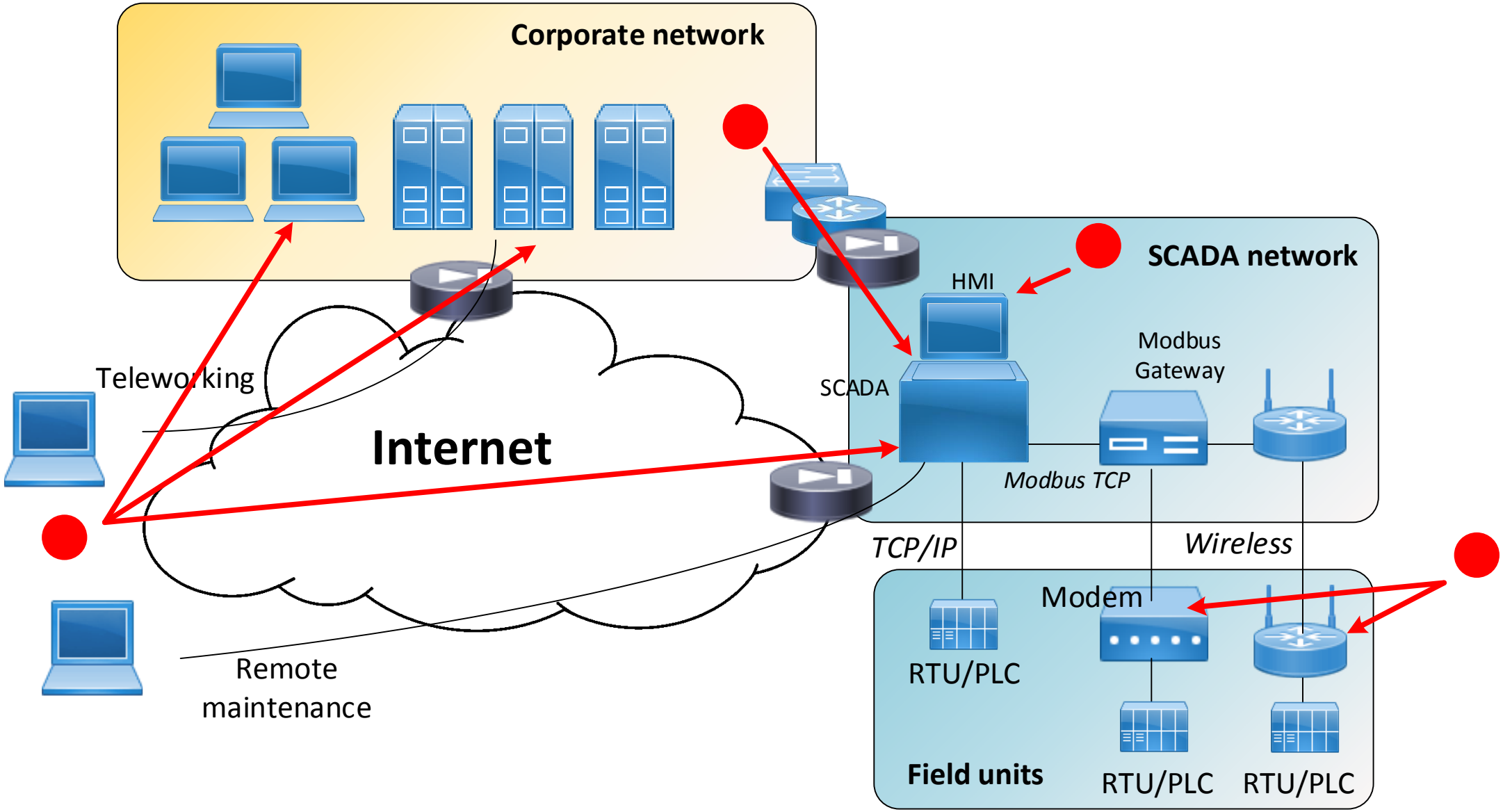
Oui, nous en avons, mais

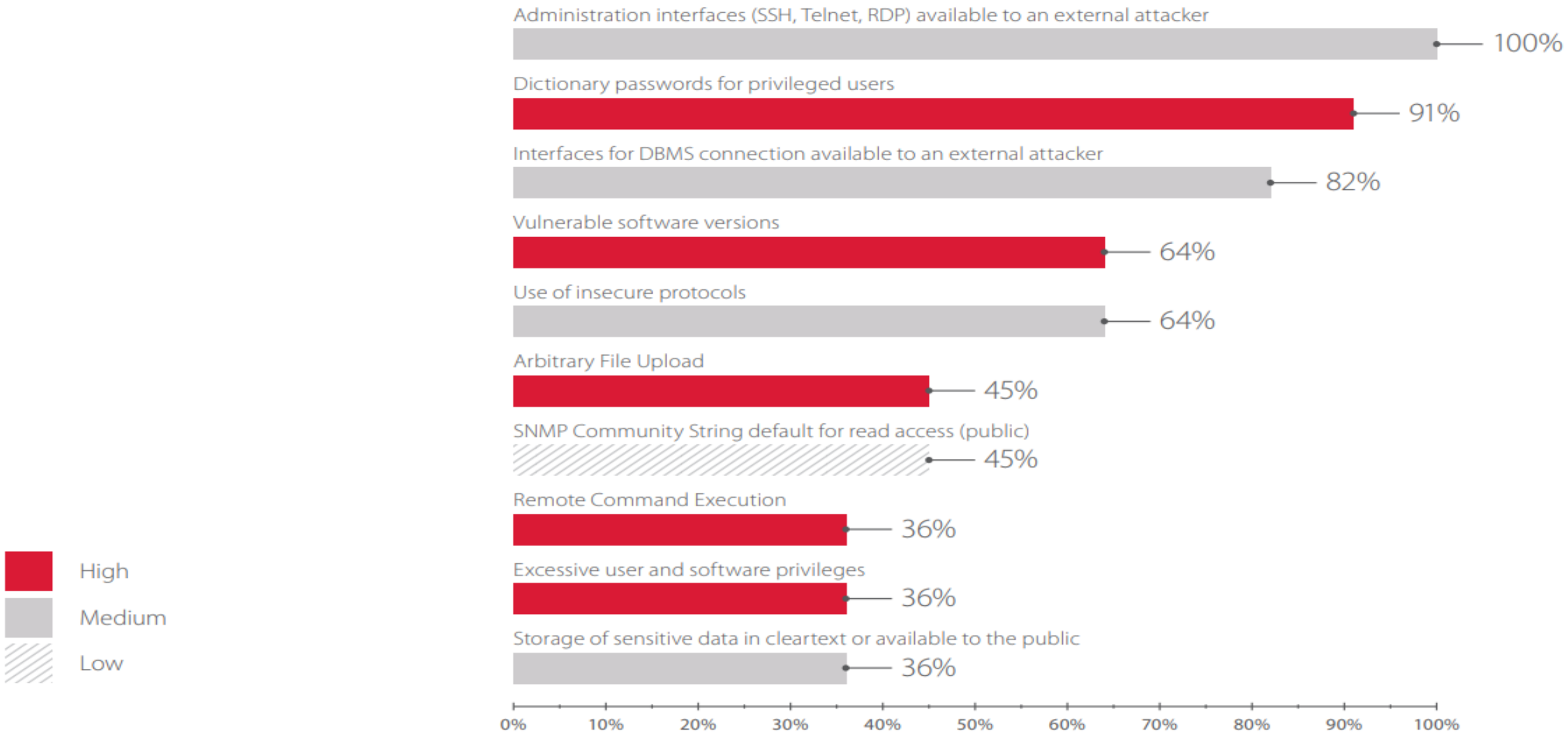
- Logiciel en conflit
- Les faux positifs ne sont pas permis
- Patching n'est pas le cas
- Pas de support pour les composants industriels
- Pas de support de la logique métier
- Etc …



Un problème de compréhension du problème

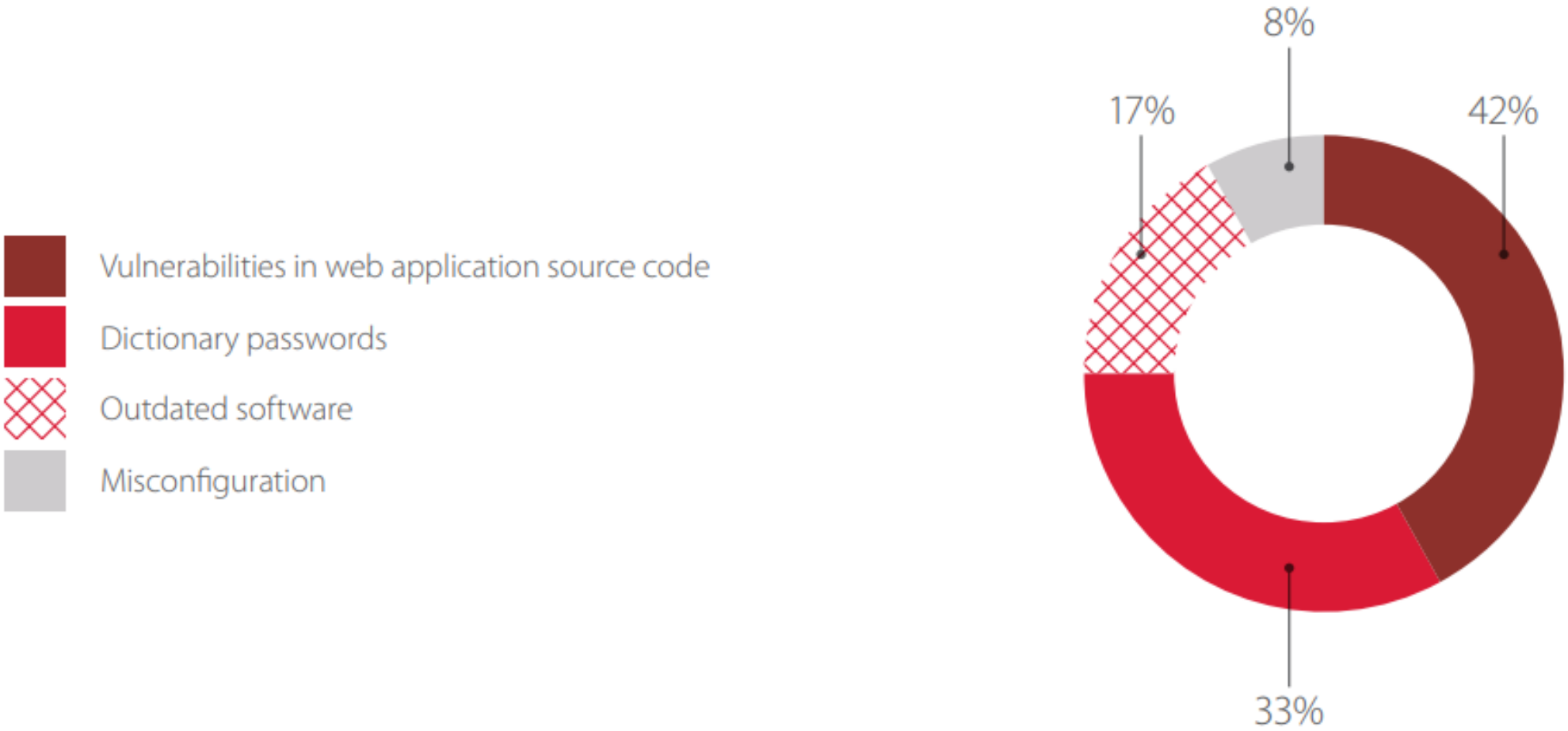
Revenons au problème





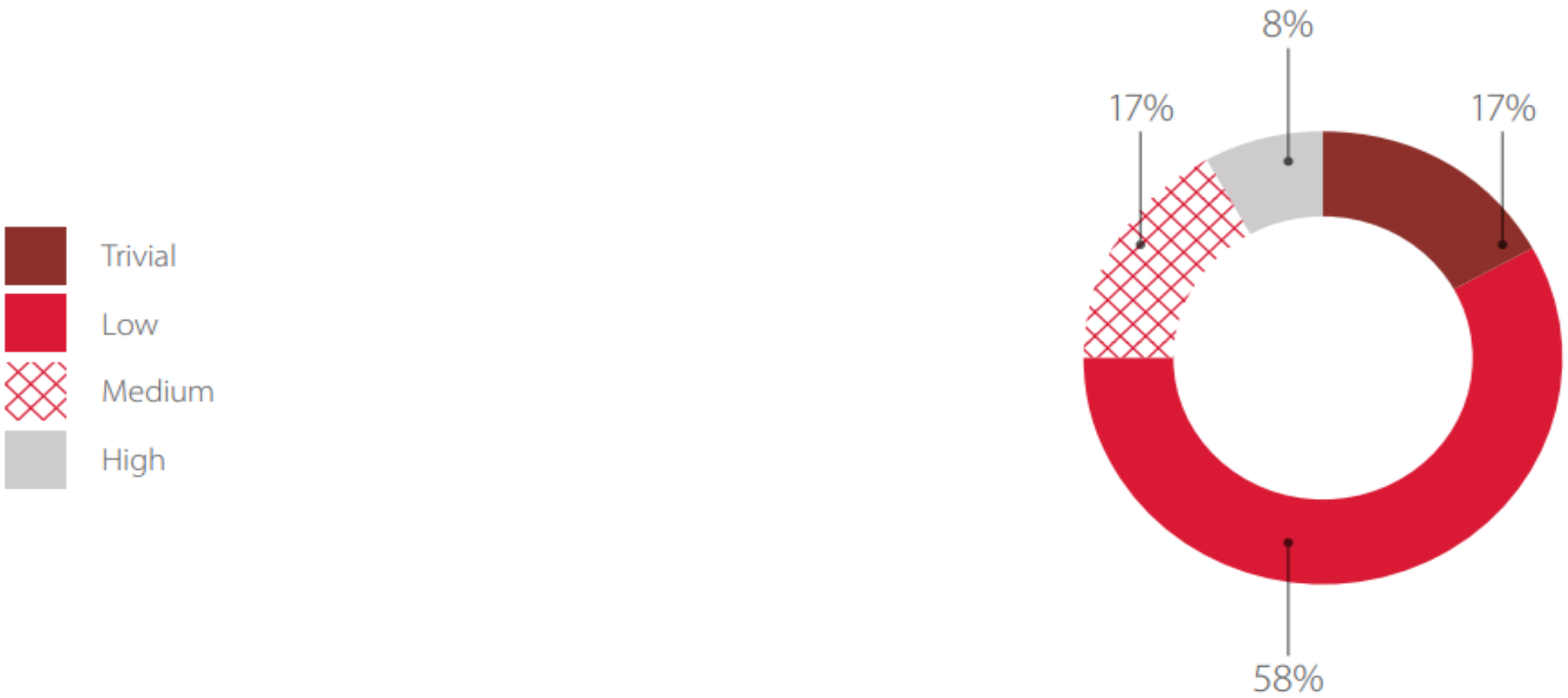
Top 10 vulnerabilities on the corporate information system perimeter of industrial companies (percentage of client companies, by severity level)

Rapport PTsecurity



Vulnerabilities used for penetration of the corporate information system from the Internet
(percentage of attack vectors)

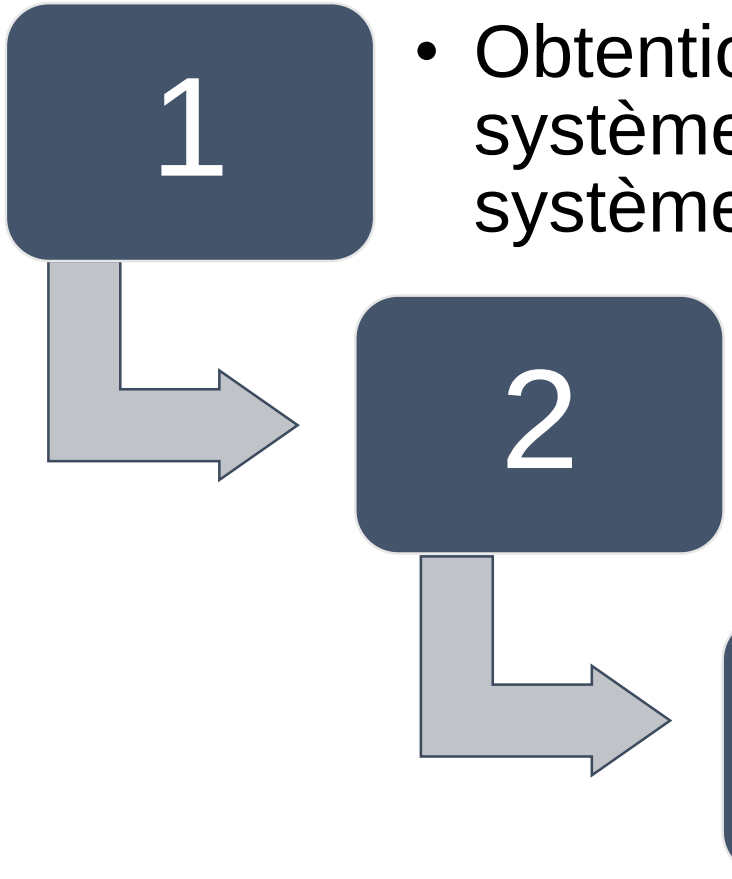
Rapport PTsecurity



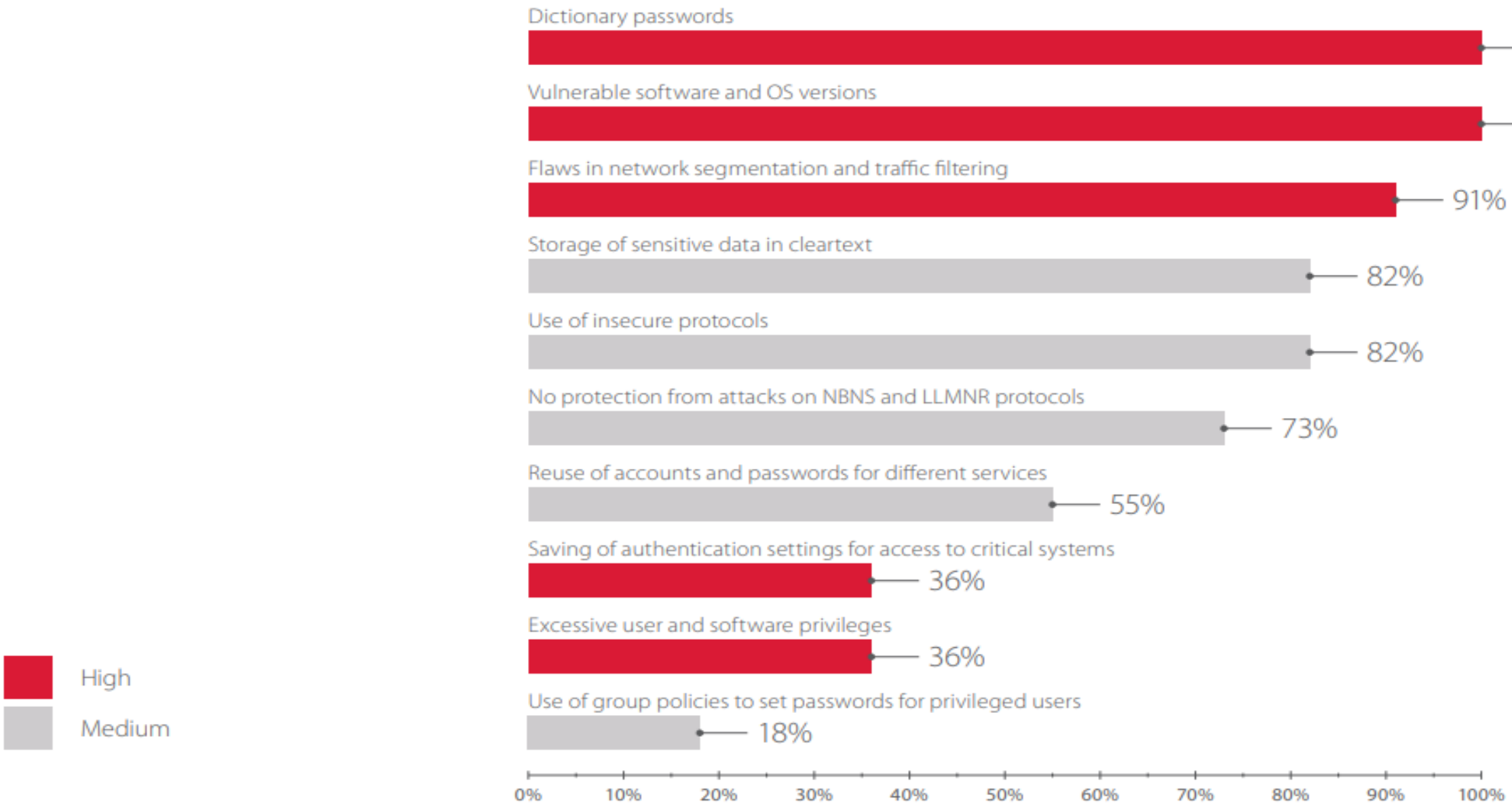
Difficulty of vectors for penetration of the corporate information system from the Internet
(percentage of attack vectors)

Rapport PTsecurity

Schéma typique d‘une attaque



- Obtention et escalade des privilèges de système d'exploitation sur les hôtes de système d'information d'entreprise
- Poursuivre une attaque pour s'implanter dans le système d'information de l'entreprise
- Accéder aux systèmes critiques et attaquer le réseau industriel



Top 10 vulnerabilities in corporate LAN of industrial companies
(percentage of client companies, by severity level)

Rapport PTsecurity


Votre système SCADA est-il en sécurité?
Oui,
Bien évidement


Mais, pourquoi vous en êtes si sûre?
On l’a physiquement isolé


Etes-vous sûre?
Puisque je vous le dit.


Avez-vous vérifié?
Si je vous prouve le contraire?
Non ... C’est impossible


La séparation physique n’est pas une solution durable
On n’est pas concerné aujourd'hui

Comprendre le problème, c’est 50% de la solution

OT vs IT vs Sécurité // Complexité environnementale
Absence d’expertise // Absence de vision et de stratégie


Tester et auditer
Conformité
Une stratégie et une vision
Développer l’expertise (former)
Une gouvernance
Gestion des vulnérabilités
Approche inclusive (OT, IT, Business, etc.)
Proactivité – préparation de la réponse
Disposer d’une visibilité (Monitoring continue)
Protéger et prévenir

Stratégie de protection des infrastructures critiques du secteur de l’énergie.

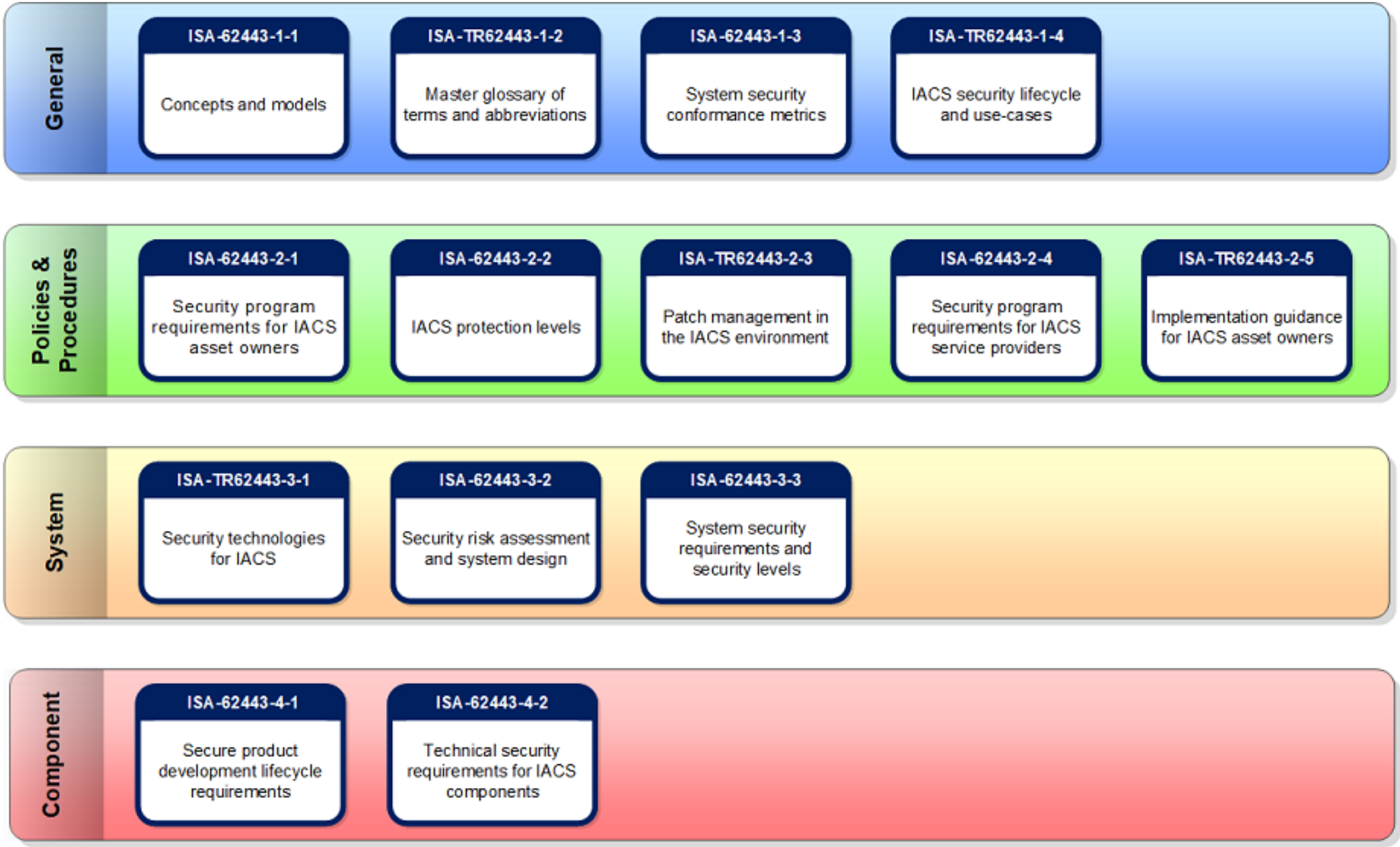
Nationale – Sectorielle – Entreprise.

Adopter les standards

NERC-CIP

- CIP-002-1: Identification des cyber actifs critiques
- CIP-003-1: Contrôles du management de la sécurité
- CIP-004-1: Personnel et formation
- CIP-005-1: périmètre de sécurité électronique
- CIP-006-1: Sécurité physique des cyber actifs électroniques
- CIP-007-1: Gestion de la sécurité des systèmes
- CIP-008-1: Déclaration d'incident et planification de l'intervention
- CIP-009-1: Plans de reprise pour les cyber actifs critiques

ISA99


General
ISA-62443-1-1
Concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security conformance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-cases
Policies & Procedures
ISA-62443-2-1
Security program requirements for IACS asset owners
ISA-62443-2-2
IACS protection levels
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Security program requirements for IACS service providers
ISA-TR62443-2-5
Implementation guidance for IACS asset owners
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security risk assessment and system design
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Secure product development lifecycle requirements
ISA-62443-4-2
Technical security requirements for IACS components

SCADA SECURITY POLICY FRAMEWORK

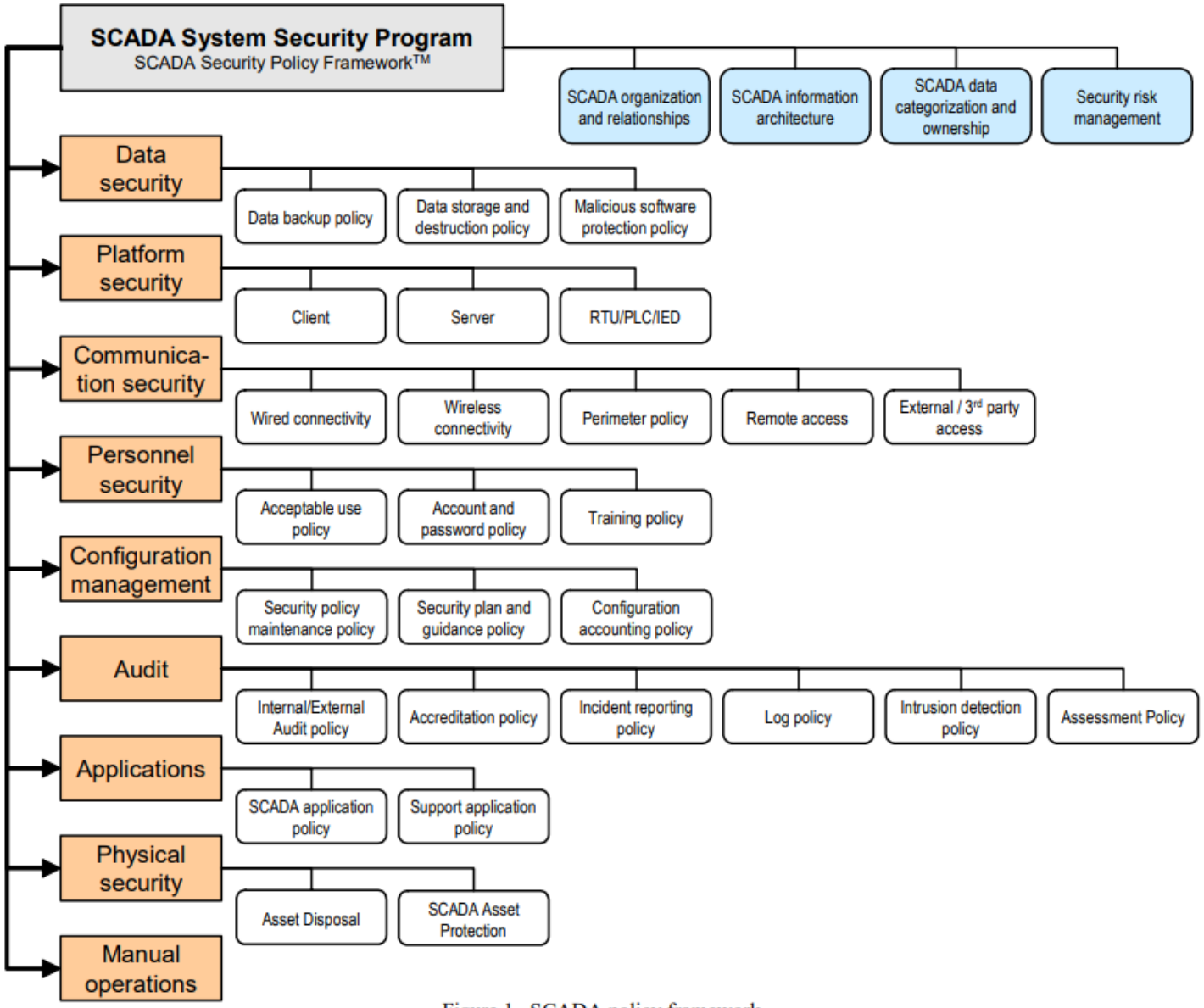


Figure 1. SCADA policy framework.

CYBER SECURITY DAYS
8ème ÉDITION 2018

Merci pour votre attention.

Haythem EL MIR
Haythem.elmir@keystone.tn