Cybersécurité: tout est sous contrôle?

Séminaire 2017

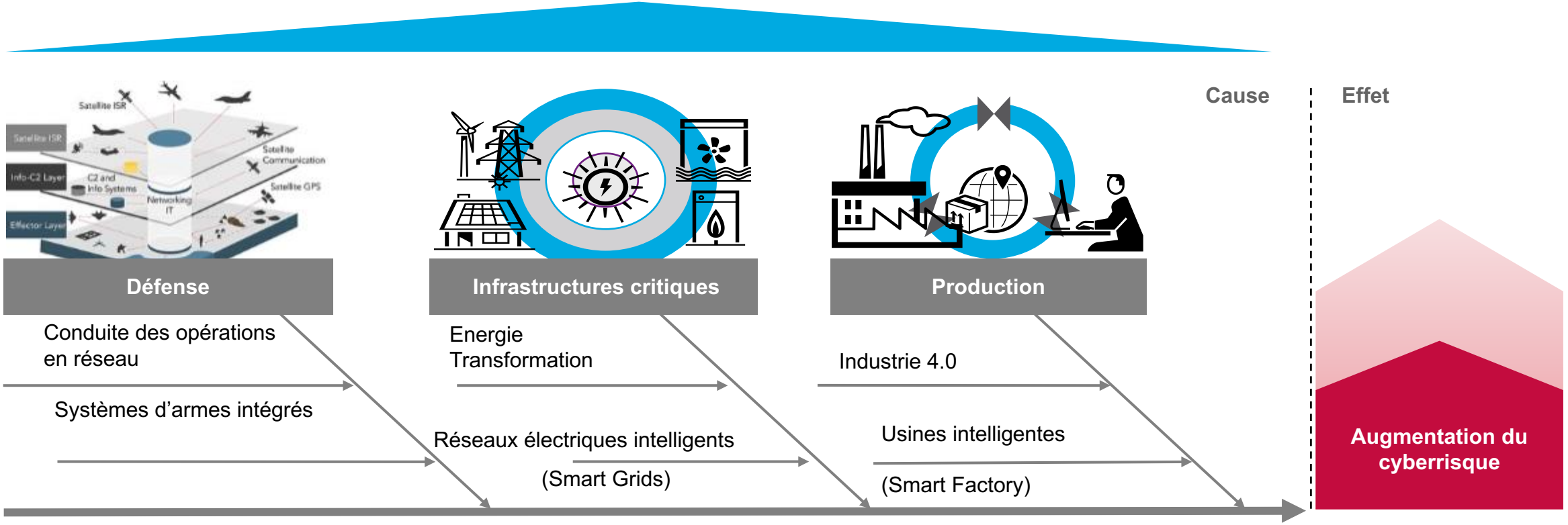
SZSV FSPC FSPC
Schweizerischer Zivilschutzverband
Fédération suisse de la protection civile
Federazione svizzera della protezione civile

René Bodmer
Director Sales Cyber Security
RUAG Defence
rene.bodmer@ruag.com

Together ahead. RUAG

Moteur du marché

La cybersécurité figure en première place des préoccupations des instances dirigeantes!



Together ahead. RUAG

Ein Blick zurück – Historie der Malware-Entwicklung

1994

1

EIN NEUES VIRUS
PRO STUNDE

2006

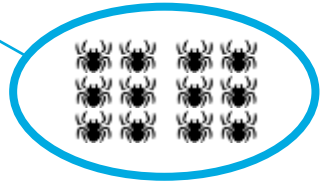
1

EIN NEUES VIRUS
PRO MINUTE

2011

1

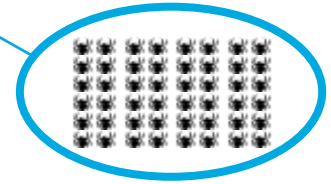
EIN NEUES VIRUS
PRO SEKUNDE



2016

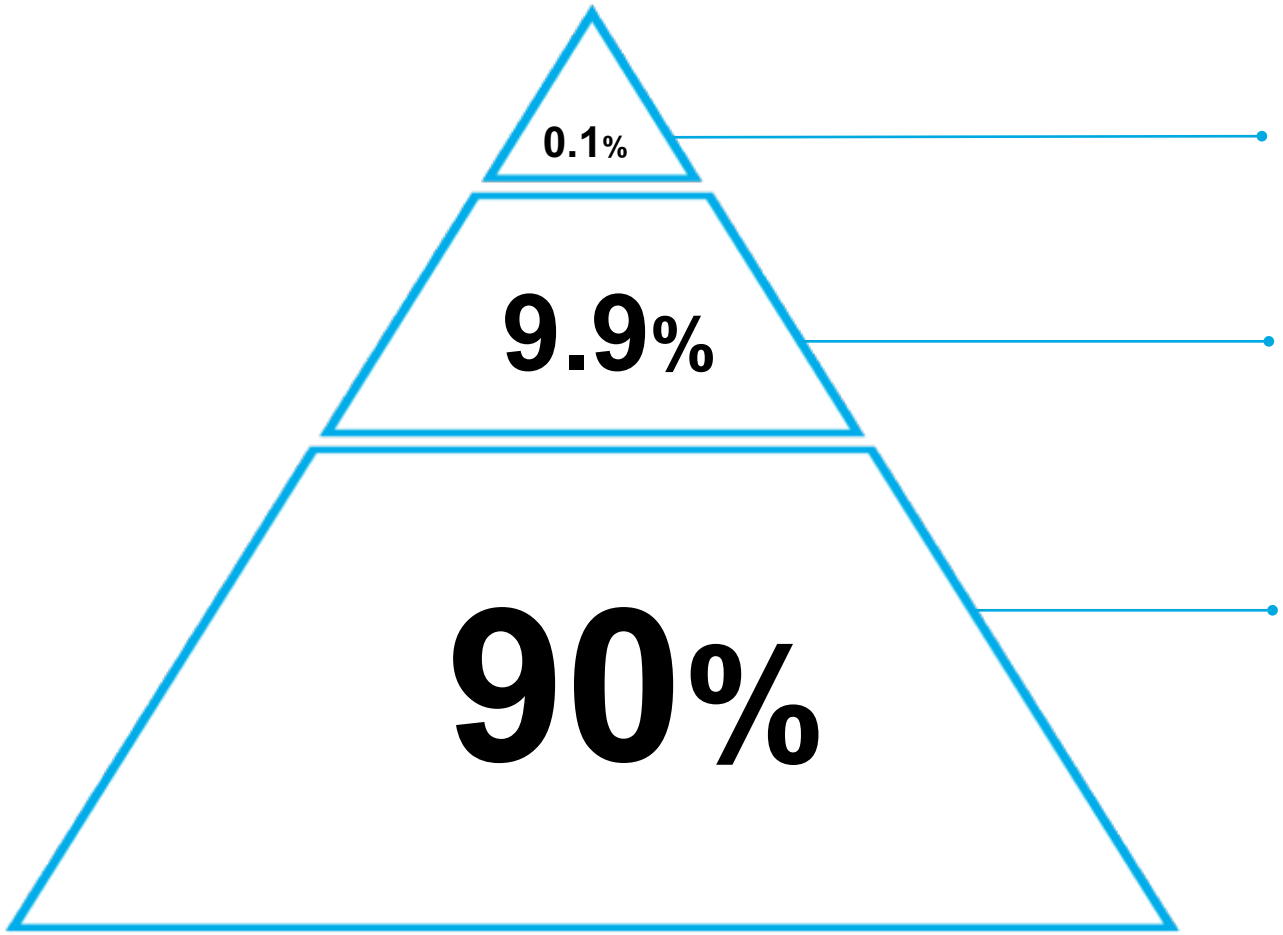
310’000

NEUE VARIANTEN
TÄGLICH



Together
ahead. RUAG

Maliciels aujourd’hui



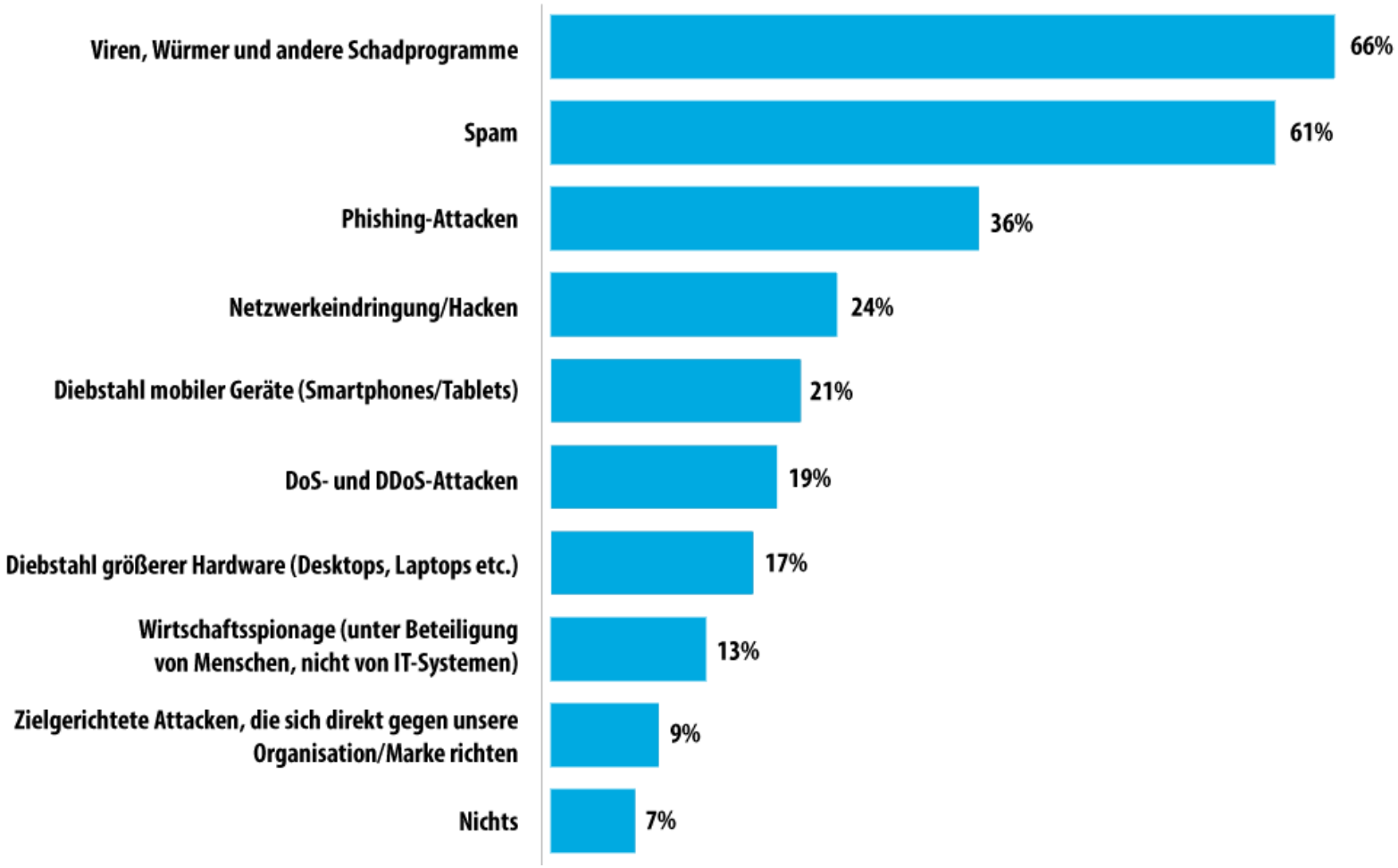
Véritables cyber-armes

Menaces ciblées contre des entreprises

Cybercriminalité courante

Together ahead. RUAG

Forme et ampleur de la menace pour les entreprises



Together ahead. RUAG

Voies de diffusion

Together ahead. RUAG

Motifs des attaques

- Vol de données
- Destruction et manipulation de données
- Vol d'argent
- Hacktivisme

Together ahead. RUAG

Planification de l'attaque

- Méthodes
- Maillon faible
- Ingénierie sociale (social engineering)
- Failles de sécurité

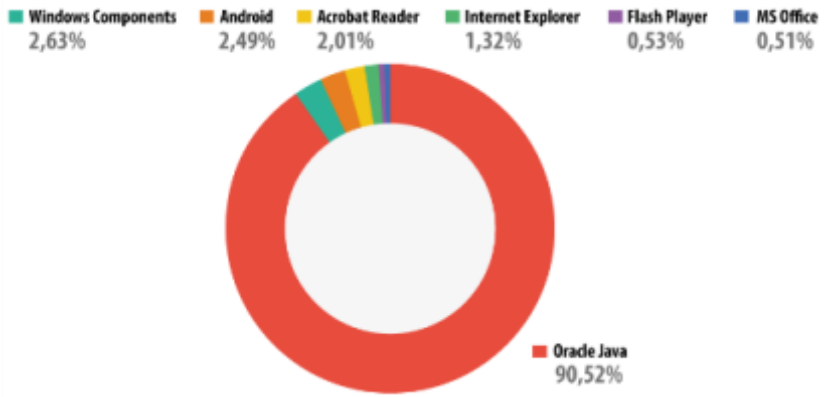
Together ahead. RUAG

Qui doit se protéger?

Together ahead. RUAG

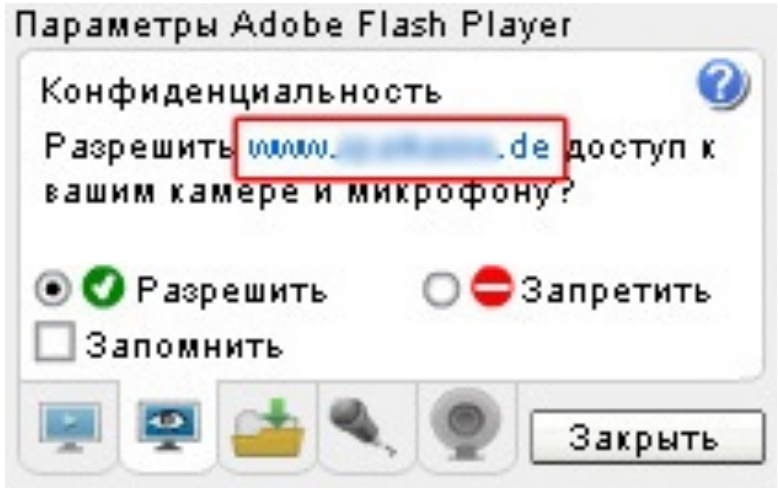
Technologies

- Vol de certificats
- Failles de sécurité
- Rançongiciels (Ransomware)
- Autres plates-formes

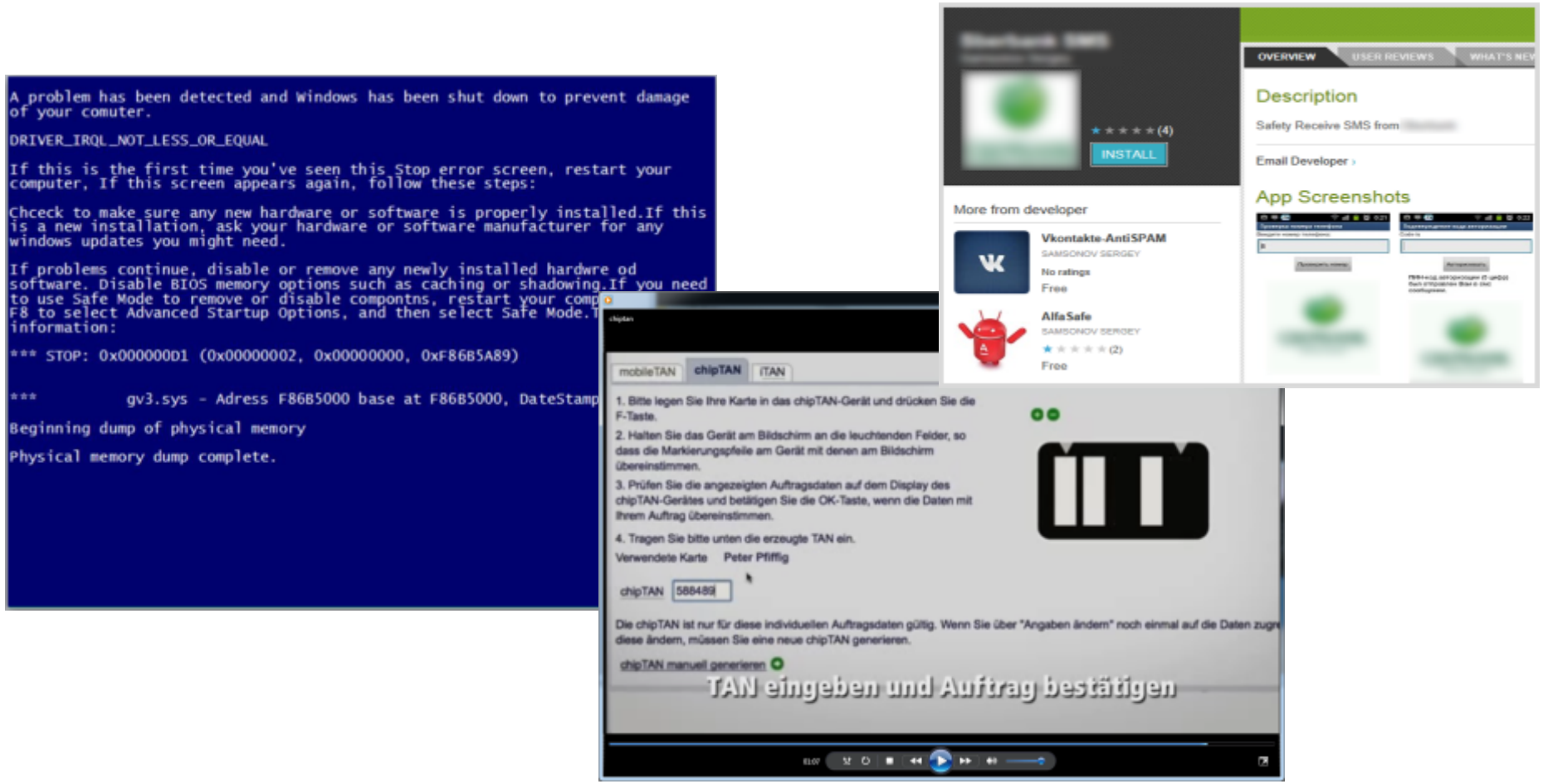


Together ahead. RUAG

Spyeye: espionnage via webcam



Opérations bancaires en ligne: sécurité encore garantie?



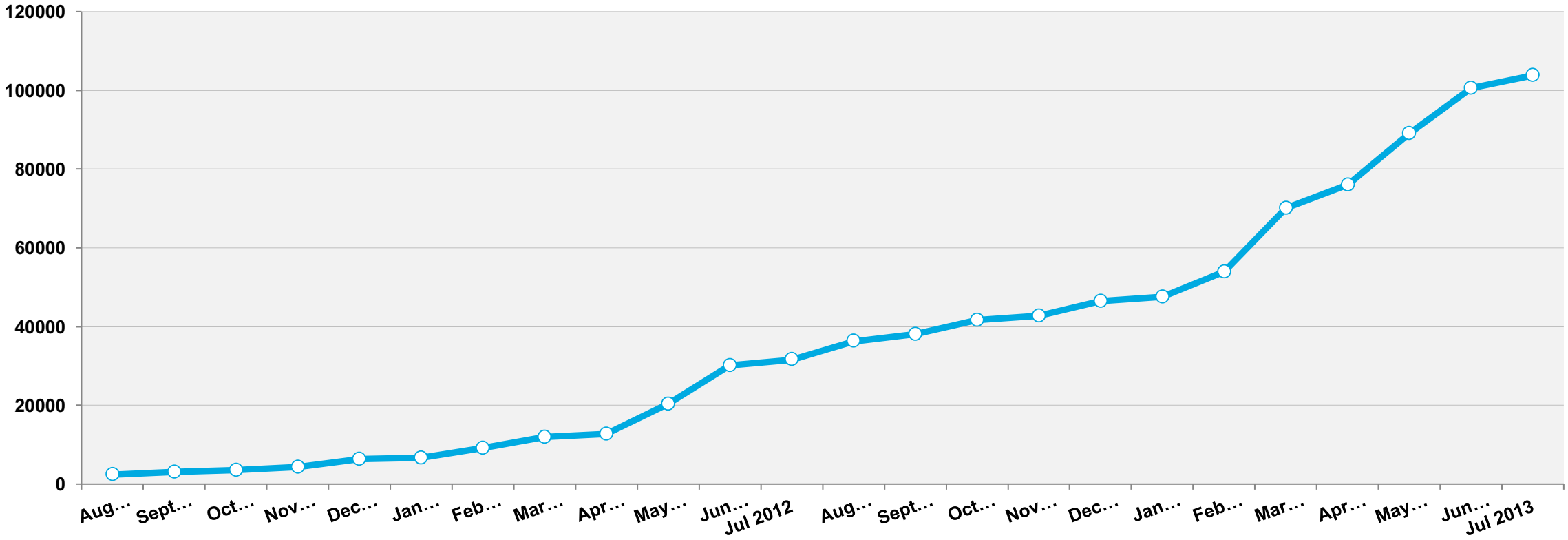
Together ahead. RUAG

Cible : les téléphones mobiles – pourquoi?

- Messages SMS sortants et entrants
- E-mails professionnels
- Contacts professionnels
- Photos personnelles
- Coordonnées GPS
- Données nécessaires au e-banking
- Calendrier
- Diverses applis installées

Nombres de variantes de maliciels pour les appareils mobiles

Nombre de variantes uniques



Together ahead. RUAG

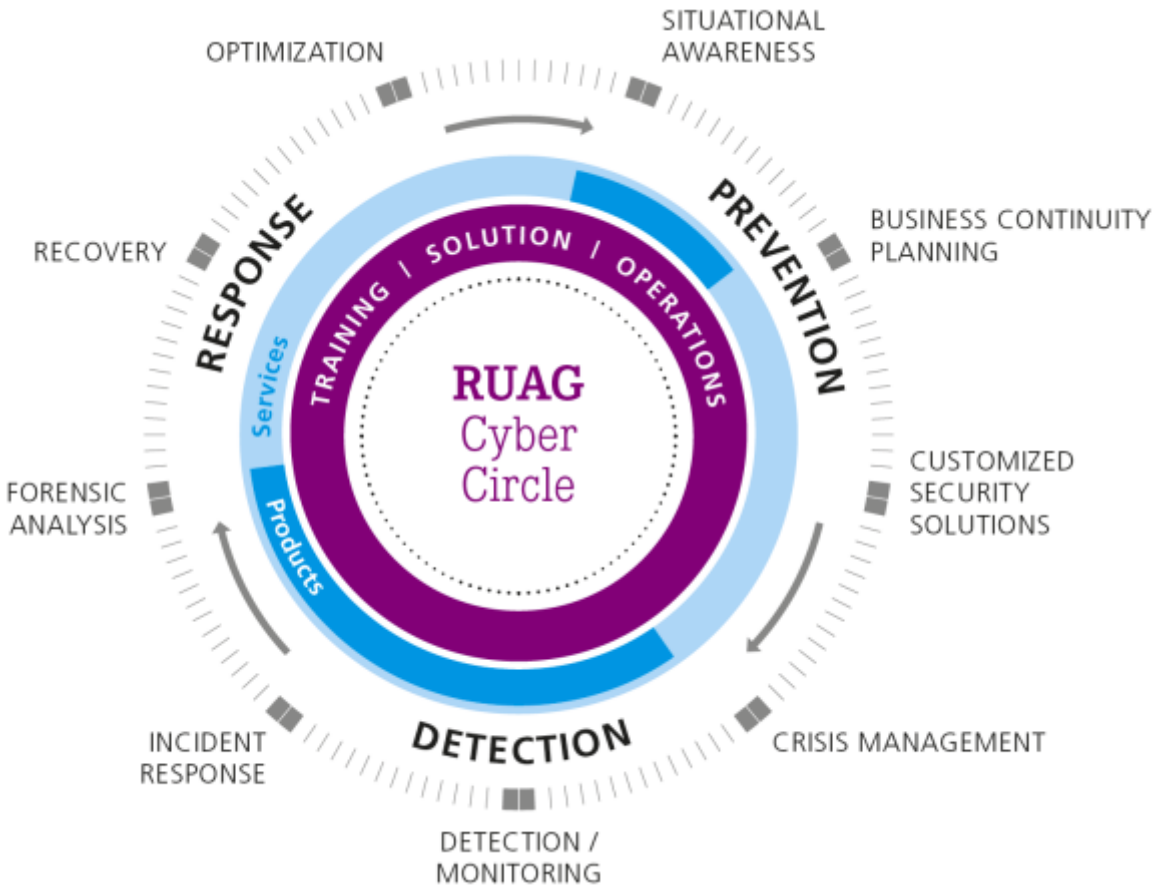
Pronotics

- Menaces mobiles
- Bitcoin
- Attaques portant sur les nuages permettant le stockage de données
- Cyber-mercenaires

Together ahead. RUAG

Consignes de survie dans le cyberespace

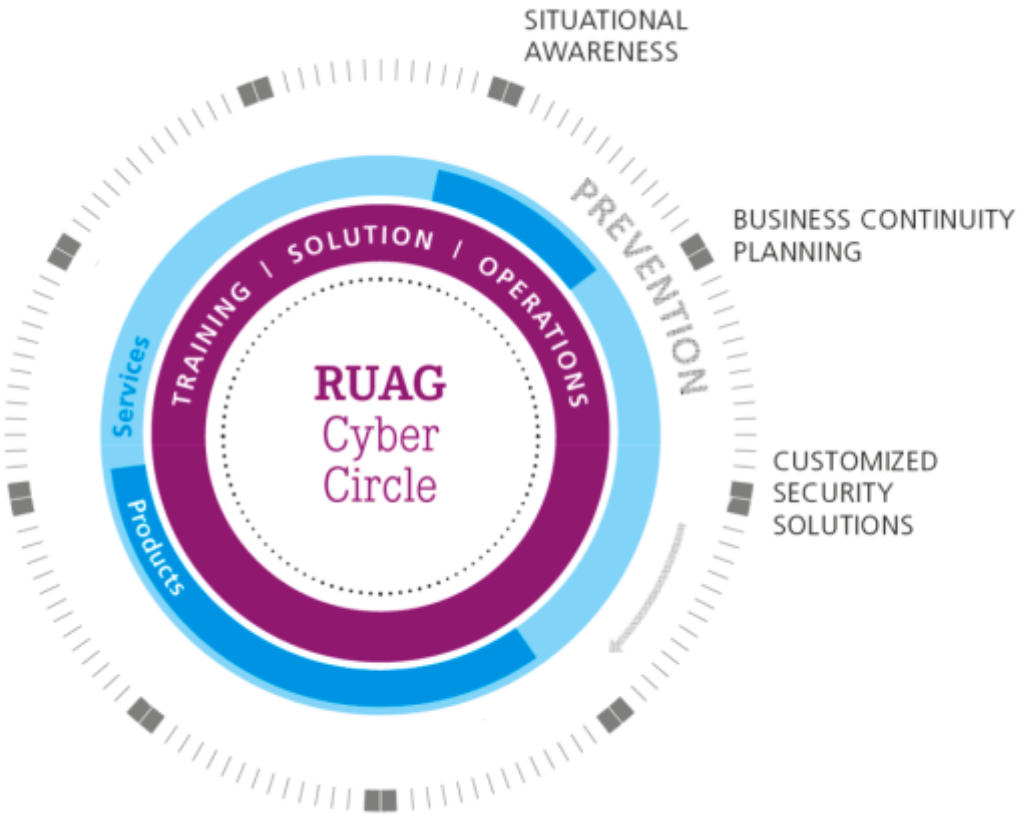
- **Avant l'attaque**
  - Bien connaître la situation
  - Définir la protection requise
  - Renforcer les systèmes
- **Durant l'attaque**
  - Détecter au plus tôt les attaques
  - Maintenir la capacité de résilience
  - Conduire pour traverser la crise
- **Après l'attaque**
  - Sauvegarder les preuves
  - Restaurer la productivité
  - Tirer les enseignements



Together ahead. RUAG

Contre-mesures – prévention

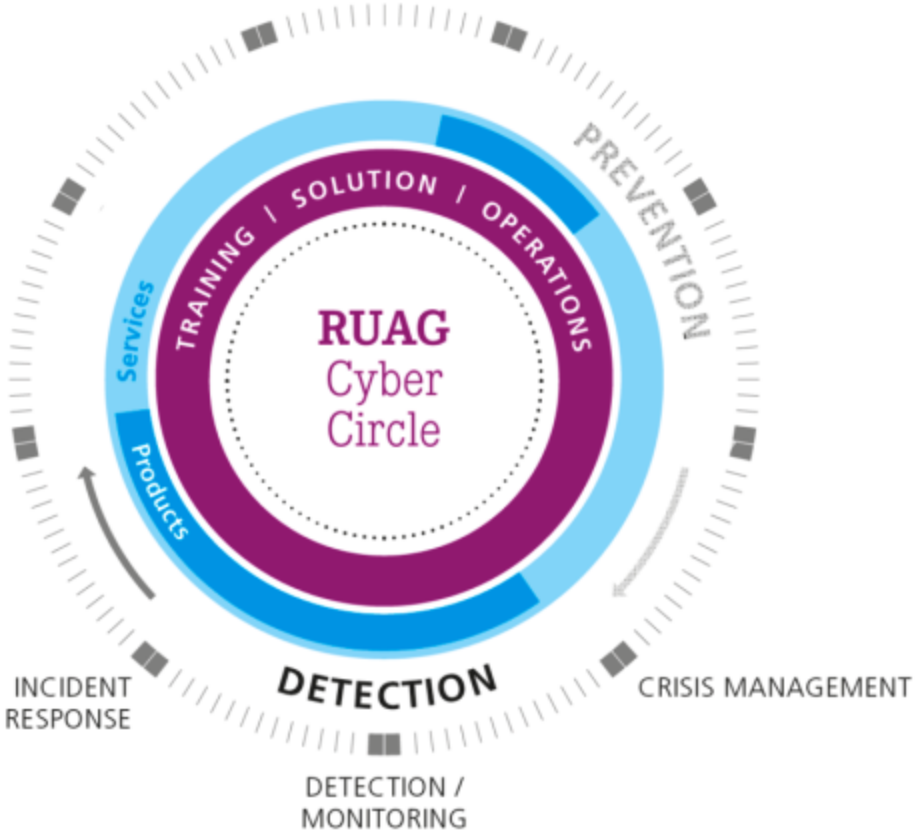
- Connaître les possibilités de l'attaquant
- Identifier les risques et les objets à protéger
- Renforcer les systèmes
- Eviter l'infection
- Sensibiliser les collaborateurs



Together ahead. RUAG

Contre-mesures – détection

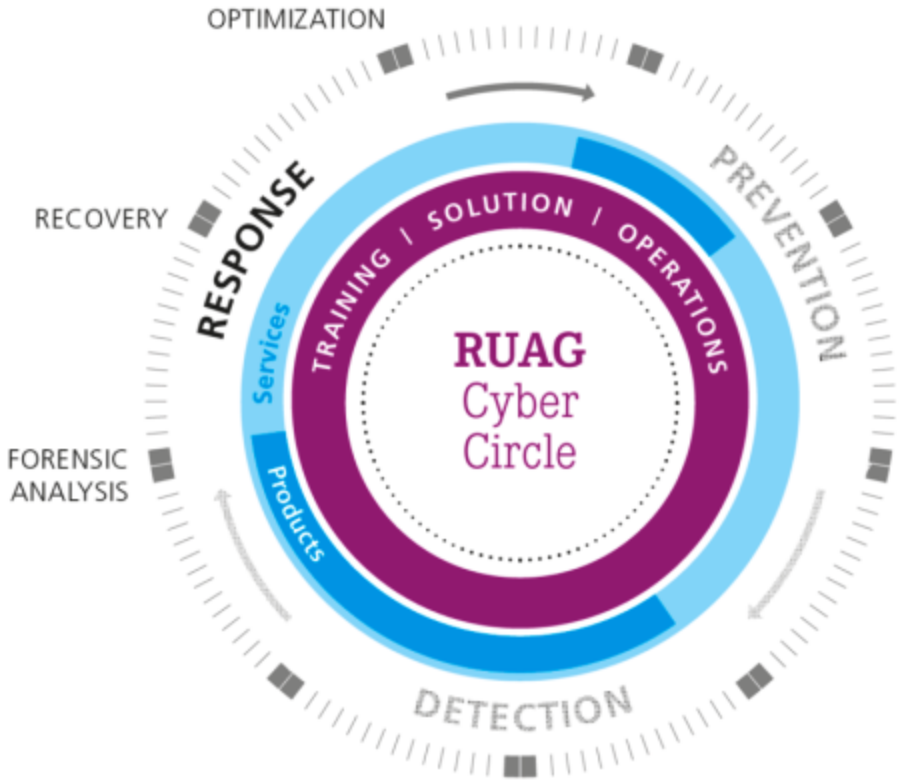
- Détecter les attaques au plus tôt
- Déterminer le type d'attaque
- Isoler les systèmes touchés
- Prendre des mesures d'urgence
- Conduire pour traverser la crise



Together ahead. RUAG

Contre-mesures – réponse

- Analyser les dégâts
- Sauvegarder les preuves
- Remettre en état les systèmes
- Combler les lacunes en matière de sécurité
- Tirer les enseignements



Together ahead. RUAG

Conclusions

- Les cyberattaques sont bien planifiées et bien conduites!
- Les attaques se déroulent par phases et sur une longue période.
- L'adversaire pense en termes d'effets.
- L'état-major de crise doit lui aussi adopter cette logique (vérifier en permanence les processus et la communication et les exercer).
- Ne pas se laisser perturber par la complexité technique.
- Assurer l'échange de savoir et le réseautage
  (p. ex. Swiss Cyber Experts, Security SIGS, Cyber Sicherheitsrat e.V. [Conseil de sécurité allemand en matière de cybermenace])

Je vous remercie de votre attention.

René Bodmer
Director Sales Cyber Security
RUAG Defence
rene.bodmer@ruag.com

Together ahead. RUAG