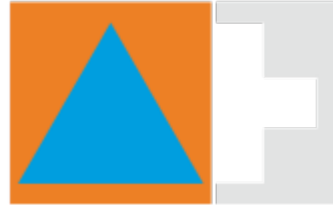


Cybersécurité: tout est sous contrôle?

Séminaire 2017



SZSV
FSPC
FSPC

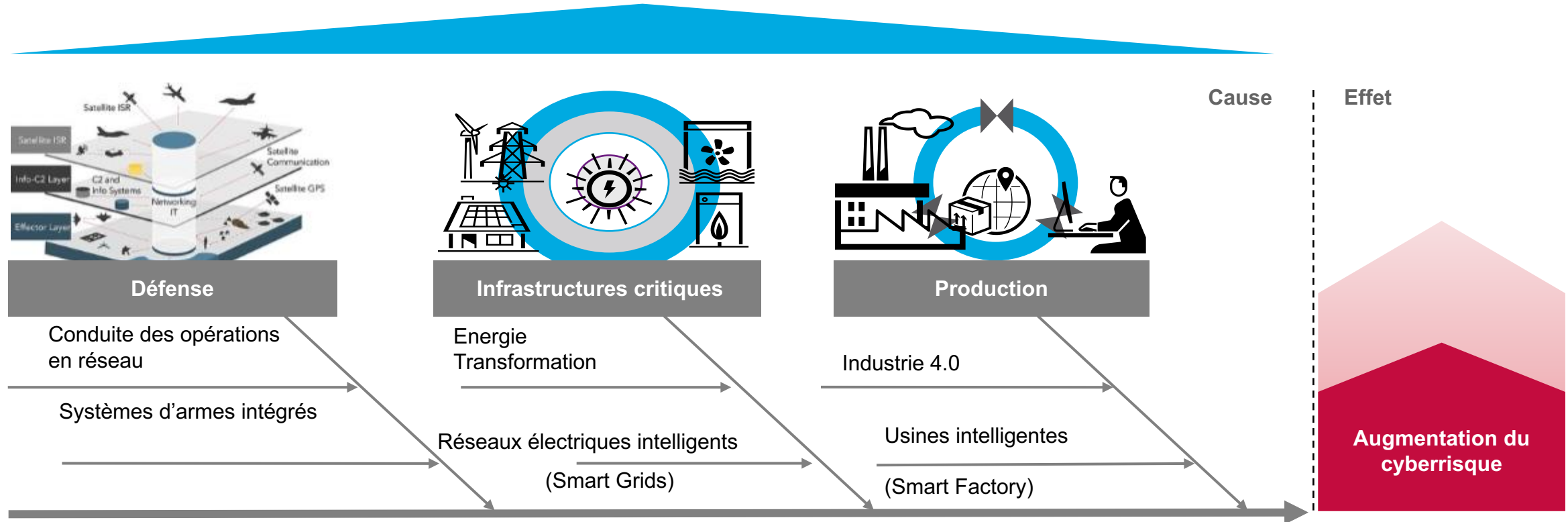
Schweizerischer Zivilschutzverband
Fédération suisse de la protection civile
Federazione svizzera della protezione civile

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

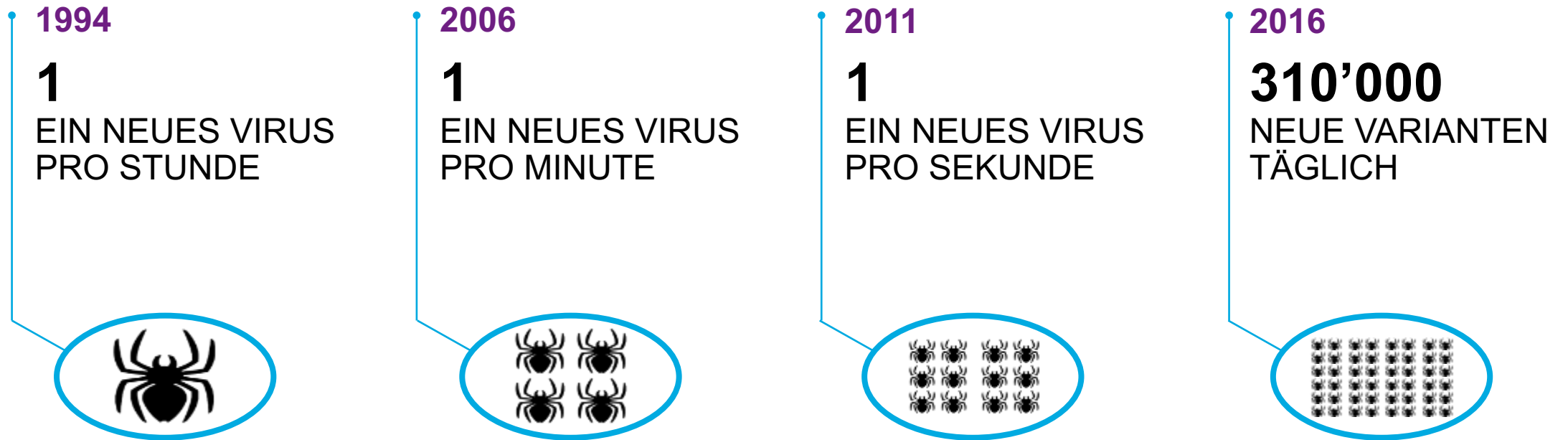
Together
ahead. **RUAG**

Moteur du marché

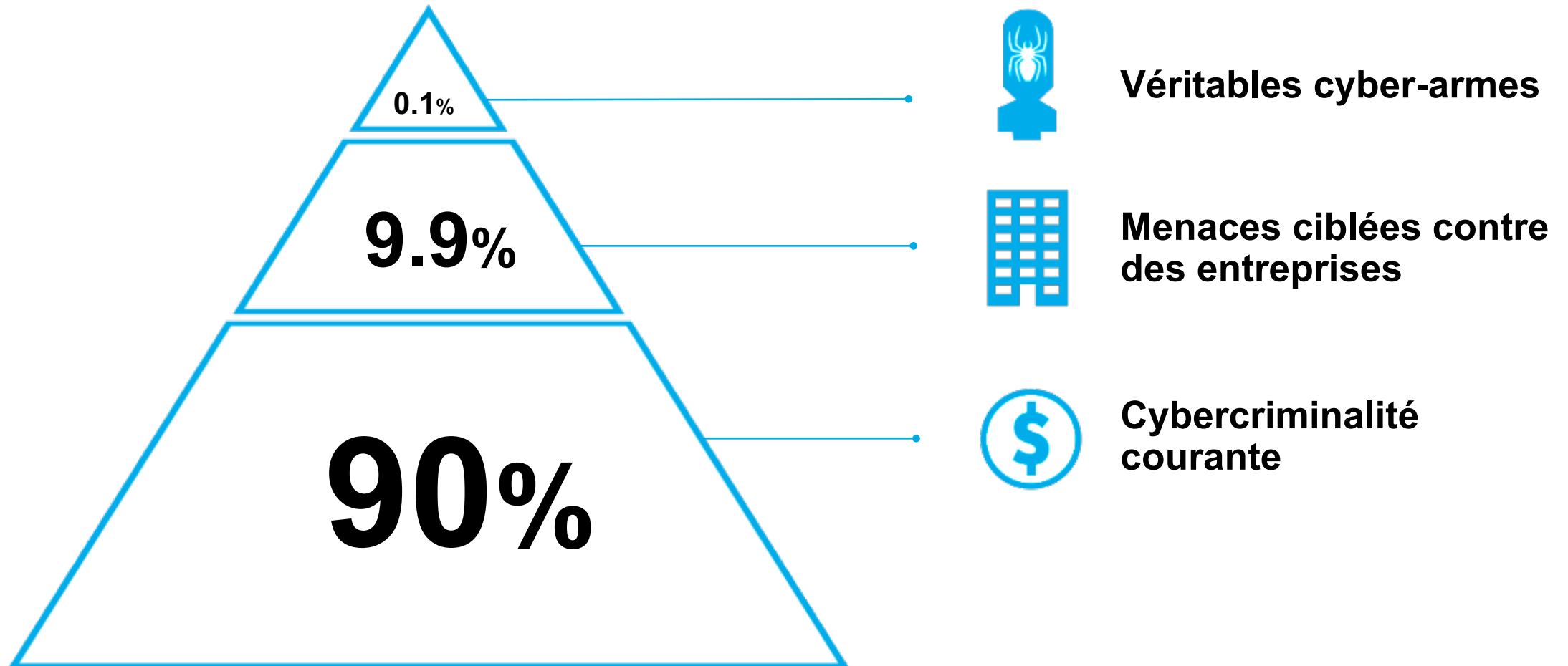
La cybersécurité figure en première place des préoccupations des instances dirigeantes!



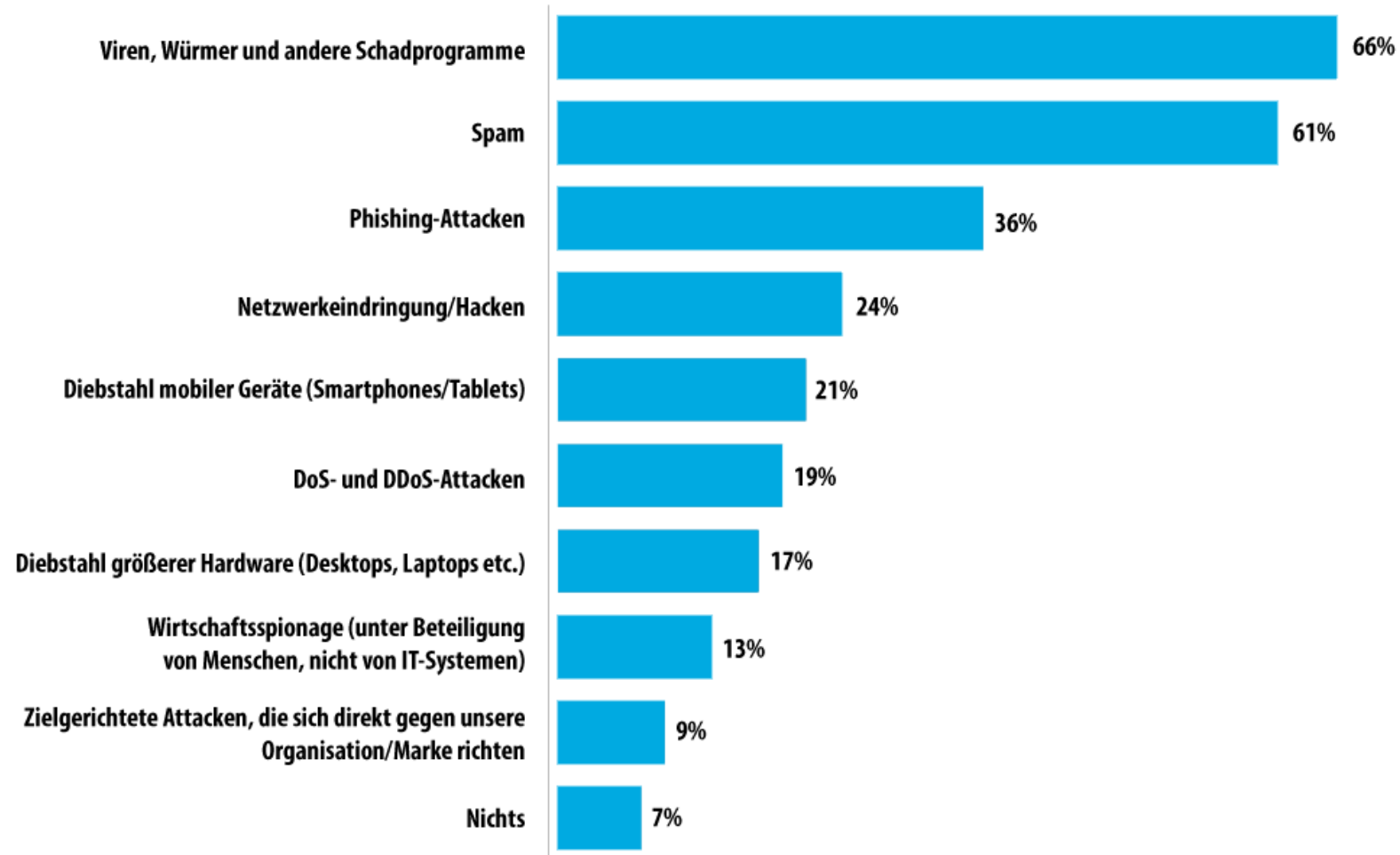
Ein Blick zurück – Historie der Malware-Entwicklung



Maliciels aujourd'hui



Forme et ampleur de la menace pour les entreprises

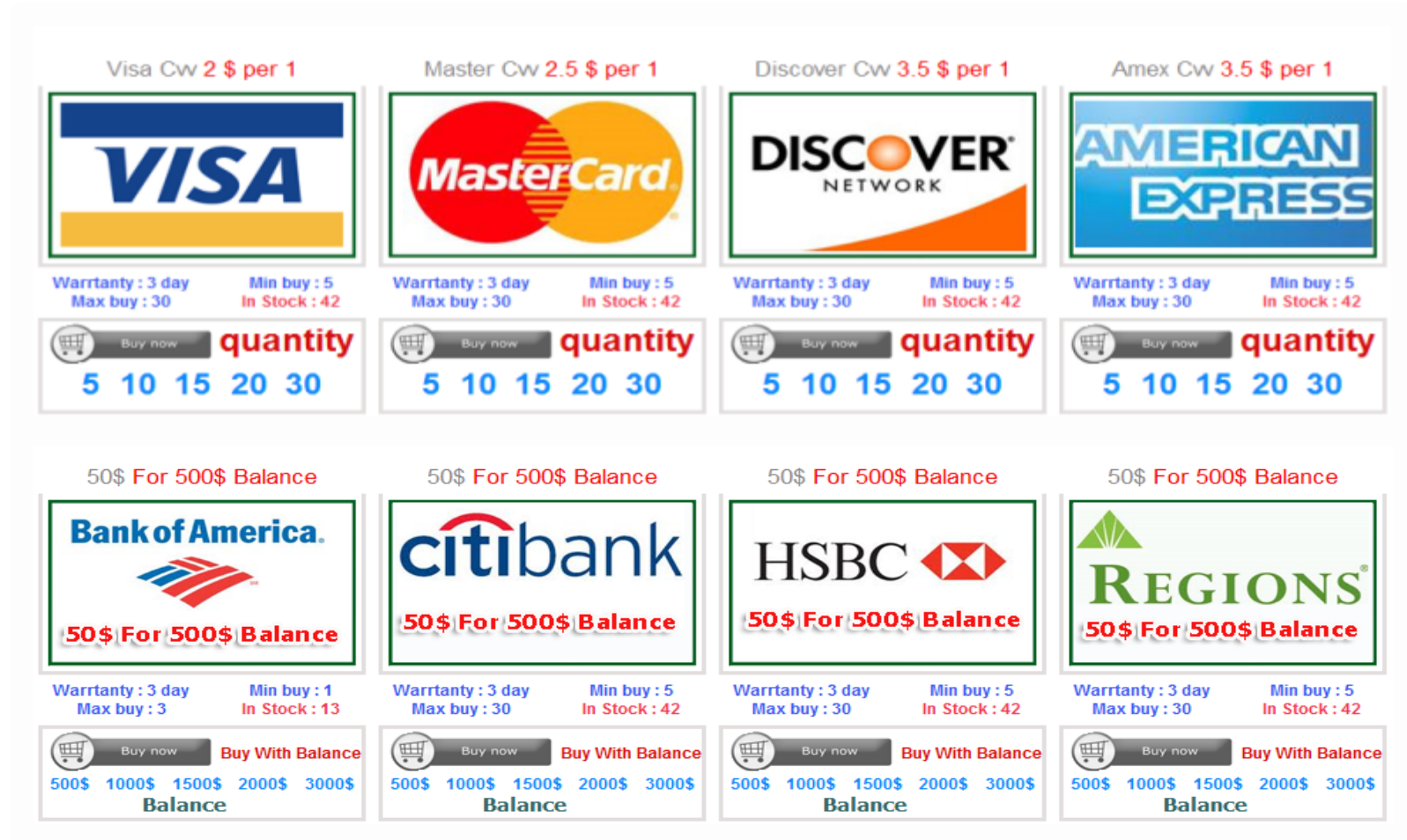


Voies de diffusion



Motifs des attaques

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



The image displays a grid of eight product cards, each representing a different financial institution or network. Each card includes a logo, a price per unit, a warranty, a minimum buy quantity, a maximum buy quantity, and an in-stock quantity. Below each card is a 'Buy now' button and a quantity selector.

Product	Price per Unit	Warranty	Min Buy	Max Buy	In Stock
Visa Cw	2 \$	3 day	5	30	42
Master Cw	2.5 \$	3 day	5	30	42
Discover Cw	3.5 \$	3 day	5	30	42
Amex Cw	3.5 \$	3 day	5	30	42
Bank of America	50\$ For 500\$ Balance	3 day	1	3	13
Citibank	50\$ For 500\$ Balance	3 day	5	30	42
HSBC	50\$ For 500\$ Balance	3 day	5	30	42
Regions	50\$ For 500\$ Balance	3 day	5	30	42



Together
ahead. **RUAG**

Planification de l'attaque

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



Qui doit se protéger?



Adressen

Adressen-Datenblatt

Adress-Kennzeichen: PS negativ

Adr-Nr.	7	Kunden-Nr.		Geburtsdatum		Datum letzter Besuch	04.02.2013
Anrede	Familie	Titel		Geburtsjahr		Bezugnahme durch	
Name/Firma	Mustermann			Telefon		Notfall Ansprechpartner	
Vorname	Max			Mobil-Telefon		Name	
Zusatzname				Fax		Telefon	
PLZ Ort	01234	Dresden		E-Mail Eingabe			
Straße				Anwendung		l.g.schmidt@t-online.de	
Anmerkungen							

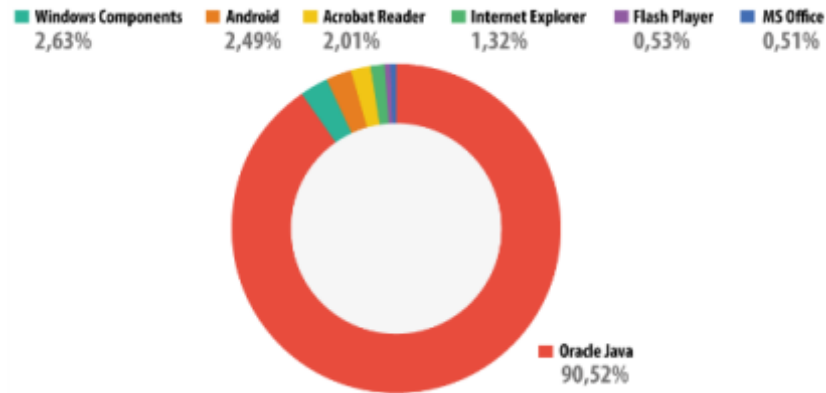
Tiere Rabatt 0% alle Tiere zur Adr.: Otto Bello

TierNr.	9	Merkmale	
Tierart	Katze	Auswahl	
Tiername	Otto	Krankheiten	
Rasse	Perserkatze	Medikamente	
Mischung		Auswahl	
Geburtsdatum		Fütterung	
Geburtsjahr		keine Besonderheiten	
Größenkl.	Tagesgebühr	Auswahl	
kastriert	unverträglich	Bilddatei	
Übernahme		C:\Users\Schmidt\Pictures\Bilder\Morli.JPG	
Chip/Tatow		Vorbesitzer	Tierarzt wählen
Anmerkungen		Versicherung	Verbleib Ableben



Technologies

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



Die offizielle Mitteilung der Bundeskriminalamt

BUNDESPOLIZEI Bundeskriminalamt

Ukash dedede OK

Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse).

Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

Tankstellen - jetzt auch erhältlich bei folgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.

epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

Achtung!

Ein Vorgang illegaler Aktivitäten wurde erkannt.

Das Betriebssystem wurde im Zusammenhang mit Verstößen gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet "82.254.165.159" mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornographie, Sadomie und Gewalt gegen Kinder aufgerufen.

Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!

Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperrung des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.

Ihre Daten:

IP: 82.254.165.159
Browser: Internet Explorer 7.0
OS: Windows XP
Das Land: FRANCE
City: Paris
ISP: Orange France

Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von 100 Euro zu zahlen. Die Zahlung ist innerhalb von 24 Stunden zu leisten. Sollte der Eingang der Zahlung in der vorgegebenen Zeit nicht erfolgen, so wird Ihre Festplatte unwiderruflich formatiert/ gelöscht.

Die Bezahlung erfolgt durch einen Ukash Coupon-Code in Höhe von 100 Euro.

Um die Bezahlung durchzuführen, geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschließend auf OK).

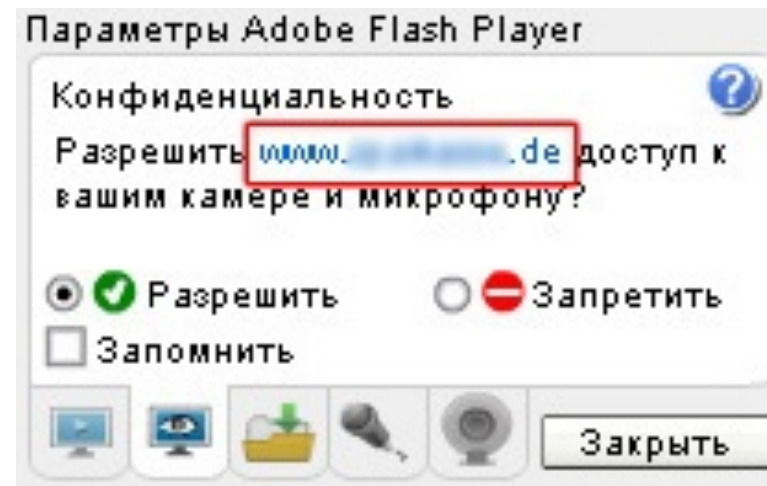
Sollte das System Fehler melden, so müssen Sie den Code per Email (XXXXXXXXXXXX@yaho.com) versenden.

Nach Eingang der Zahlung wird Ihr Computer innerhalb von 24 Stunden wieder freigestellt.

2010 - 2011 © Der Service des Dienstes des Internet der Sicherheit ist mit der Unterstützung der Gesellschaften entwickelt.

McAfee symantec Kaspersky Microsoft

Spyeye: espionage via webcam



Opérations bancaires en ligne: sécurité encore garantie?

```
A problem has been detected and windows has been shut down to prevent damage of your computer.  
DRIVER_IRQL_NOT_LESS_OR_EQUAL  
If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:  
Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.  
If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode. For more information:  
*** STOP: 0x000000D1 (0x00000002, 0x00000000, 0xF86B5A89)  
***      gv3.sys - Address F86B5000 base at F86B5000, DateStamp 00000000  
Beginning dump of physical memory  
Physical memory dump complete.
```

AlfaSafe
SAMSONOV SERGEY
★ ★ ★ ★ (4)
INSTALL

More from developer

- Vkontakte-AntiSPAM
SAMSONOV SERGEY
No ratings
Free
- AlfaSafe
SAMSONOV SERGEY
★ ★ ★ ★ (2)
Free

OVERVIEW USER REVIEWS WHAT'S NEW

Description
Safety Receive SMS from [redacted]

Email Developer [redacted]

App Screenshots

mobileTAN chipTAN iTAN

- Bitte legen Sie Ihre Karte in das chipTAN-Gerät und drücken Sie die F-Taste.
- Halten Sie das Gerät am Bildschirm an die leuchtenden Felder, so dass die Markierungspfeile am Gerät mit denen am Bildschirm übereinstimmen.
- Prüfen Sie die angezeigten Auftragsdaten auf dem Display des chipTAN-Gerätes und betätigen Sie die OK-Taste, wenn die Daten mit Ihrem Auftrag übereinstimmen.
- Tragen Sie bitte unten die erzeugte TAN ein.

Verwendete Karte Peter Pfiffig

chipTAN 588489

Die chipTAN ist nur für diese individuellen Auftragsdaten gültig. Wenn Sie über "Angaben ändern" noch einmal auf die Daten zugreifen, müssen Sie diese ändern, müssen Sie eine neue chipTAN generieren.

chipTAN manuell generieren

TAN eingeben und Auftrag bestätigen

Cible : les téléphones mobiles – pourquoi?



Messages SMS sortants
et entrants



E-mails professionnels



Contacts professionnels



Photos personnelles



Coordonnées GPS



Données nécessaires au
e-banking



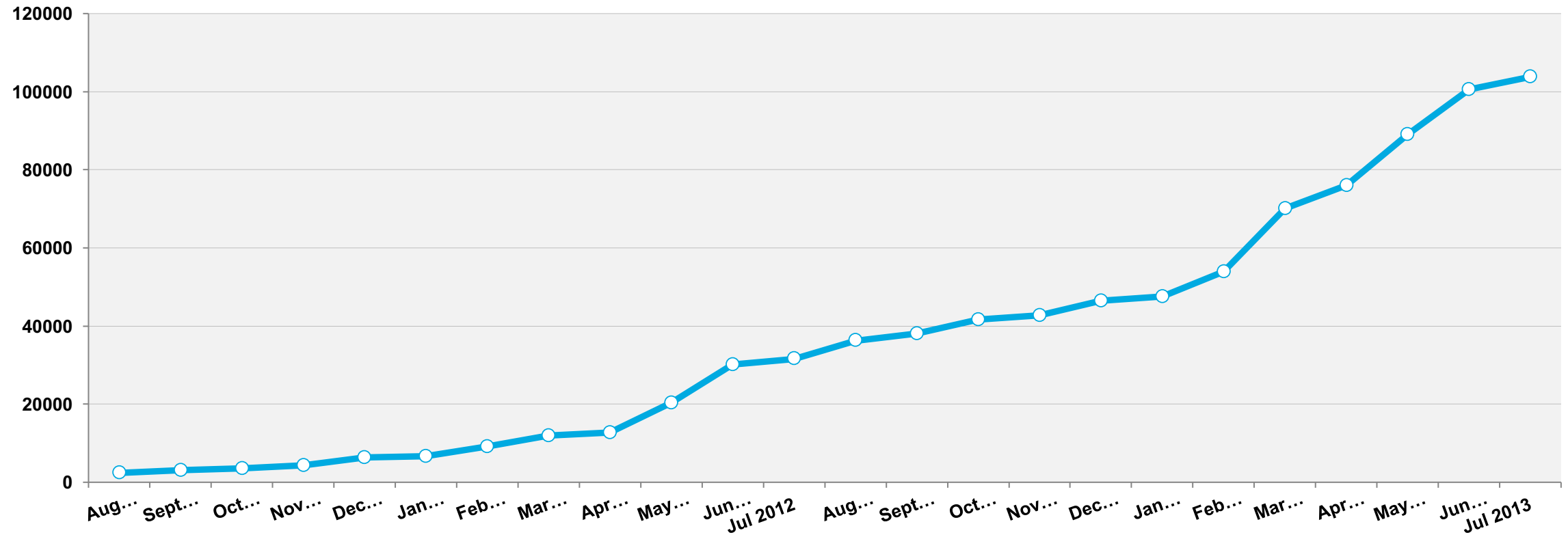
Calendrier



Diverses applis installées

Nombres de variantes de maliciels pour les appareils mobiles

Nombre de variantes uniques



Pronotics

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



Consignes de survie dans le cyberespace

▪ Avant l'attaque

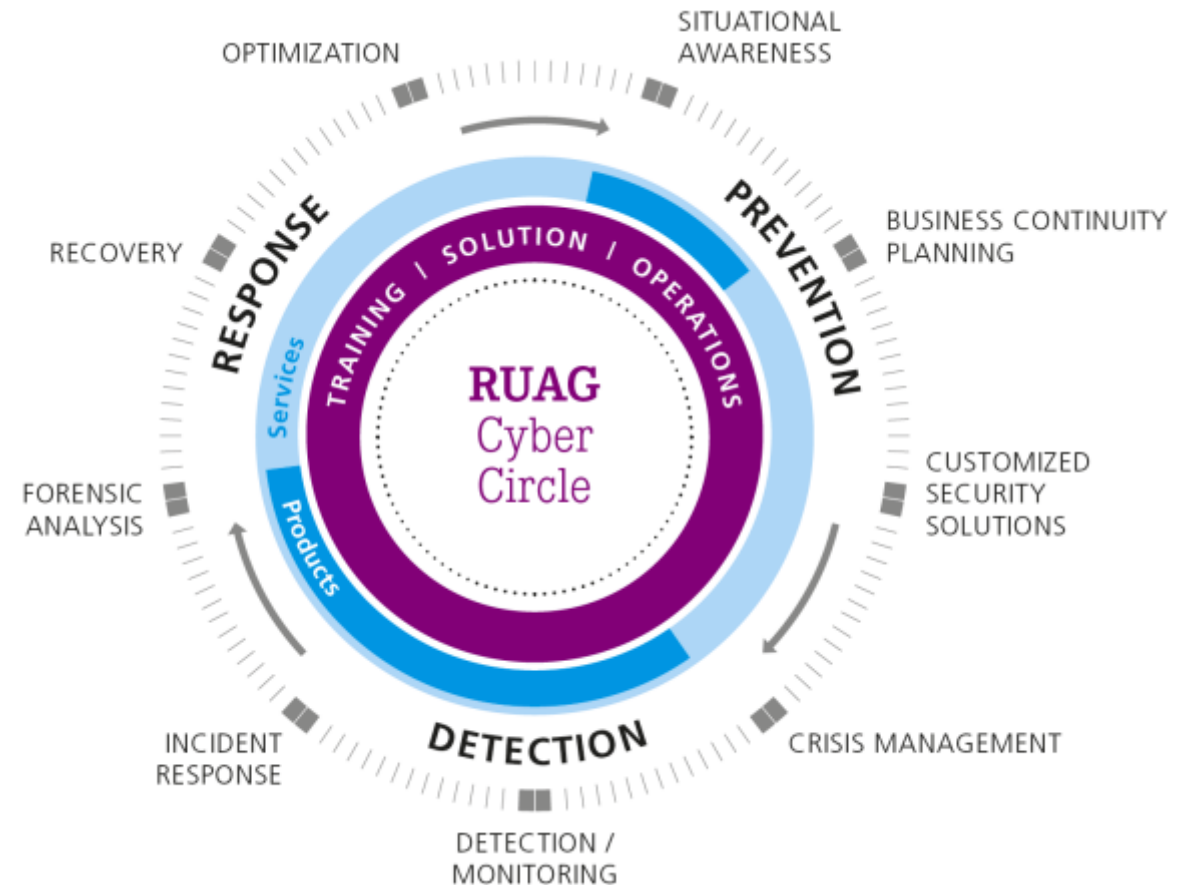
- Bien connaître la situation
- Définir la protection requise
- Renforcer les systèmes

▪ Durant l'attaque

- Détecter au plus tôt les attaques
- Maintenir la capacité de résilience
- Conduire pour traverser la crise

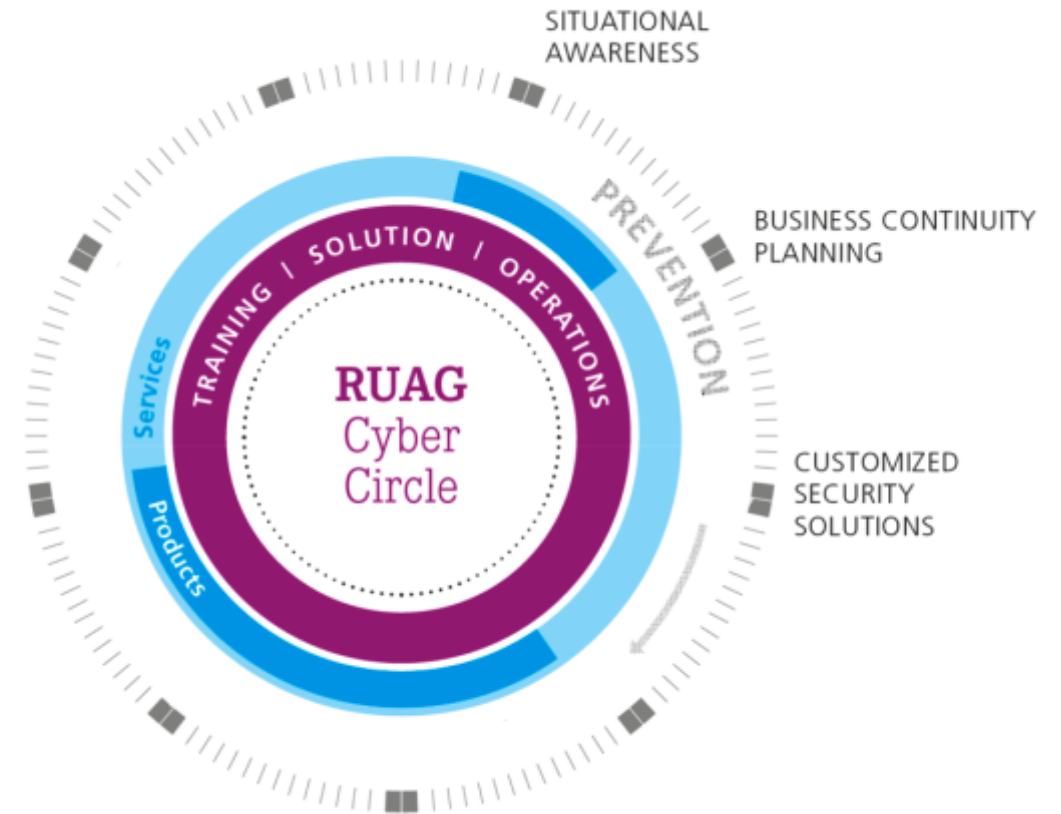
▪ Après l'attaque

- Sauvegarder les preuves
- Restaurer la productivité
- Tirer les enseignements



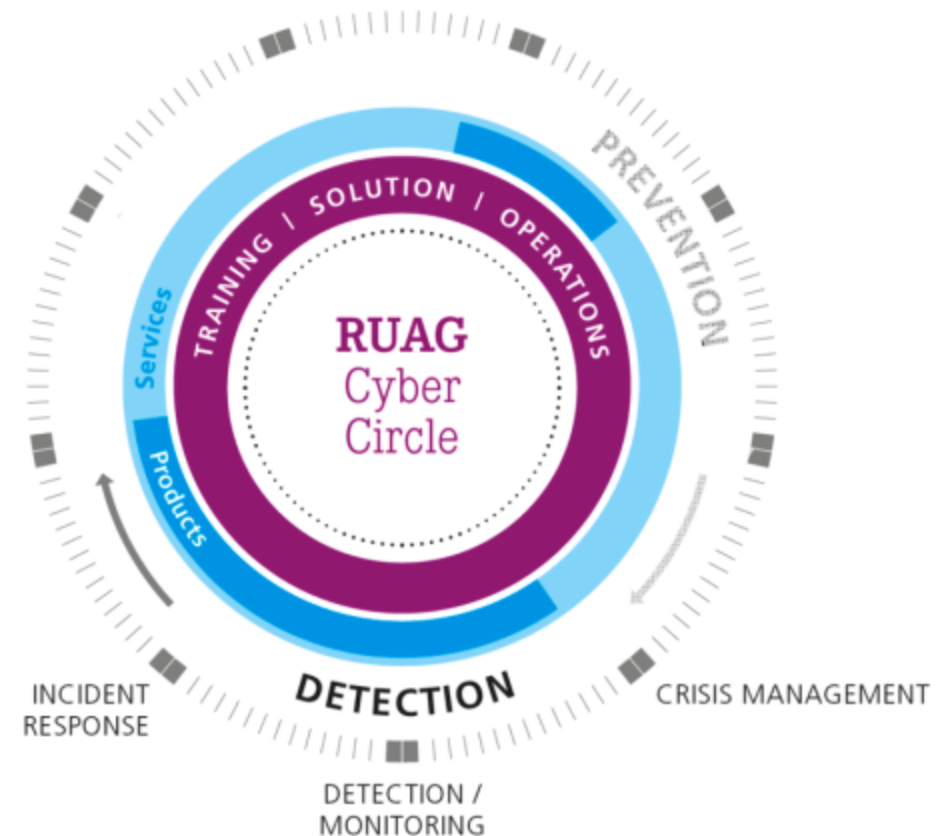
Contre-mesures – prévention

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



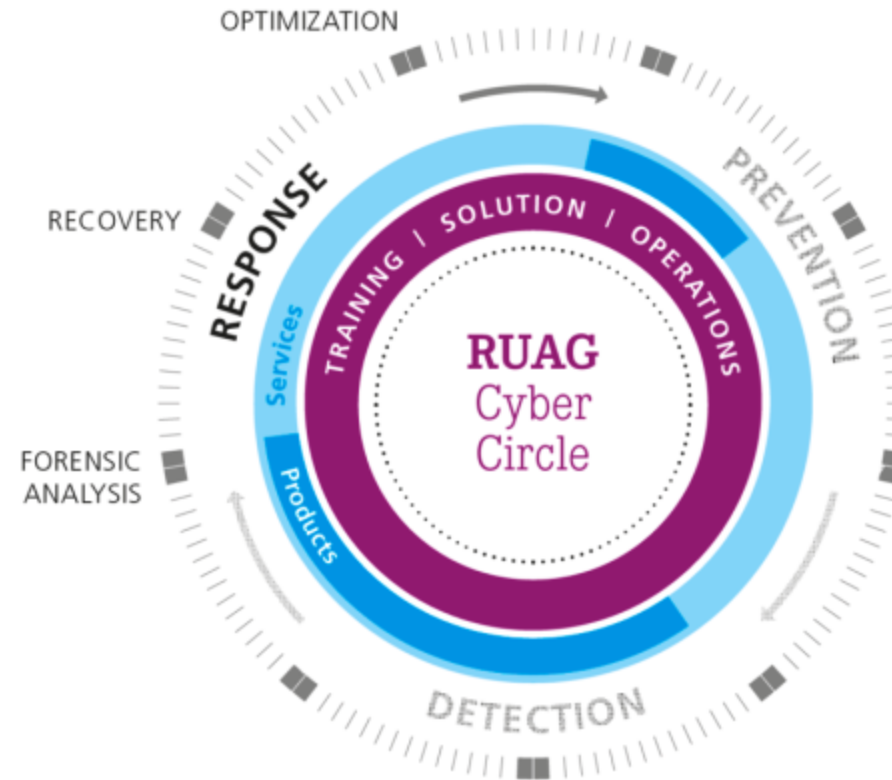
Contre-mesures – détection

- 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



Contre-mesures – réponse

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



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

