InfoGuard
SWISS CYBER SECURITY

CYBER DEFENCE AUS DER SCHWEIZ

Die schnelle Erkennung und Reaktion auf einen Hackerangriff ist entscheidend

Mein Name ist Stefan Rothenbühler, und ich jage Hacker.

InfoGuard
SWISS CYBER SECURITY

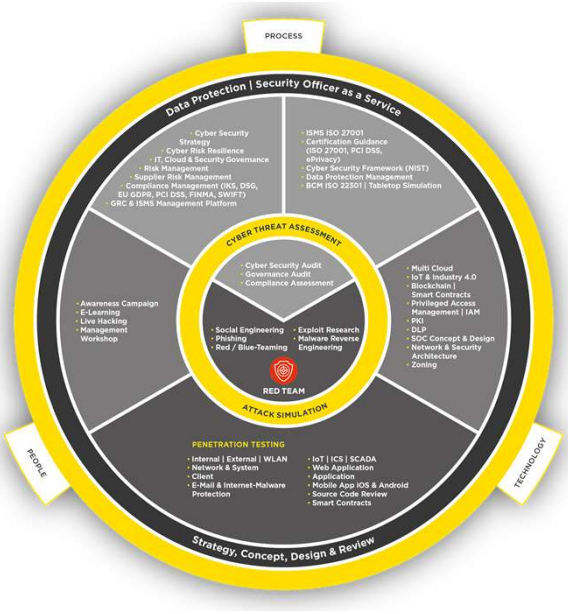
BSc. Hochschule Luzern/FHZ
MAS in Informationssicherheit
Offensive Security Certified Professional

- seit 2018 Senior Cyber Security Analyst bei Intelligence & Investigations, InfoGuard AG
- 2016 – 2018 Penetration Tester im InfoGuard AG Red Team
- 2009 – 2016 Systems Engineer Swisscom AG (@bluewin.ch)
- 2007 – 2009 SUN Campus Ambassador Hochschule Luzern
  Junior Systems Engineer Enterprise LAB HSLU
- seit 2000 in der IT tätig (Lehre als UNIX Systems Engineer V-ZUG AG)

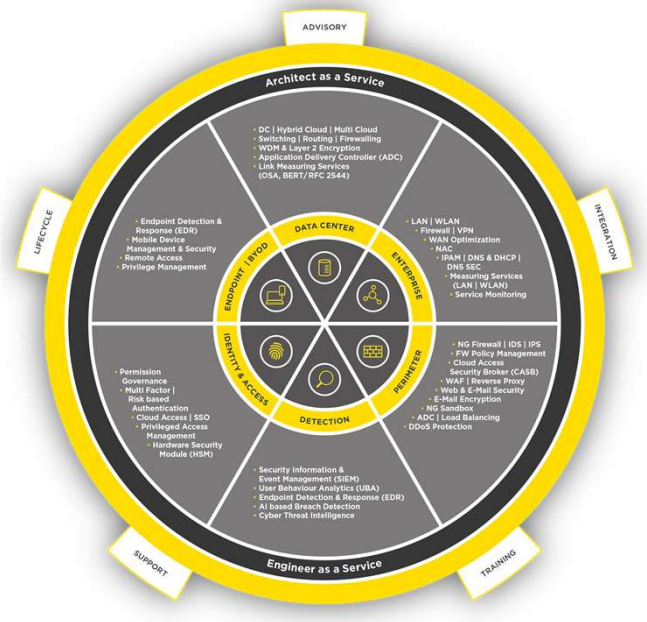
INFOGUARD –
Der Schweizer Cyber Security Experte

InfoGuard
SWISS CYBER SECURITY

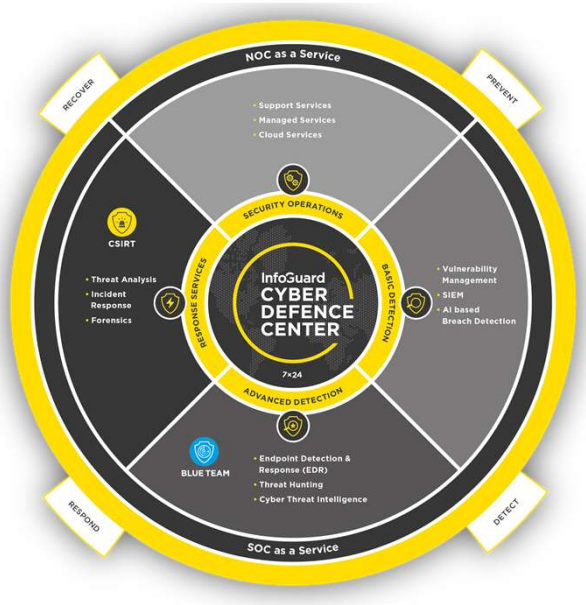
SECURITY CONSULTING SERVICES



NETWORK & SECURITY SOLUTIONS



CYBER DEFENCE SERVICES



130+
SICHERHEITSEXPERTEN IN ZUG UND BERN

100%
IM BESITZ DES SCHWEIZER MANAGEMENTS

KOMPETENZ SEIT
1988

ISO 27001
ZERTIFIZIERT

SWISS CDC
CYBER DEFENCE CENTER

SWISS DC
DATA CENTER

InfoGuard RED TEAM

InfoGuard BLUE TEAM

CSIRT

IT-Sicherheit früher – Prävention

InfoGuard
SWISS CYBER SECURITY

IT Sicherheit heute

InfoGuard
SWISS CYBER SECURITY

Der Hacker zielt auf die IT-Infrastruktur. (Bild: Karin Hofer / NZZ)

Wie ein Schweizer KMU ohne Lösegeld, dafür mit Militärtaktik einen Hackerangriff überlebt hat

Cyber-Attacken auf Unternehmen nehmen zu. Die meisten Opfer versuchen, nichts davon an die Öffentlichkeit dringen zu lassen. Beim Handelsunternehmen Offix ist das anders.

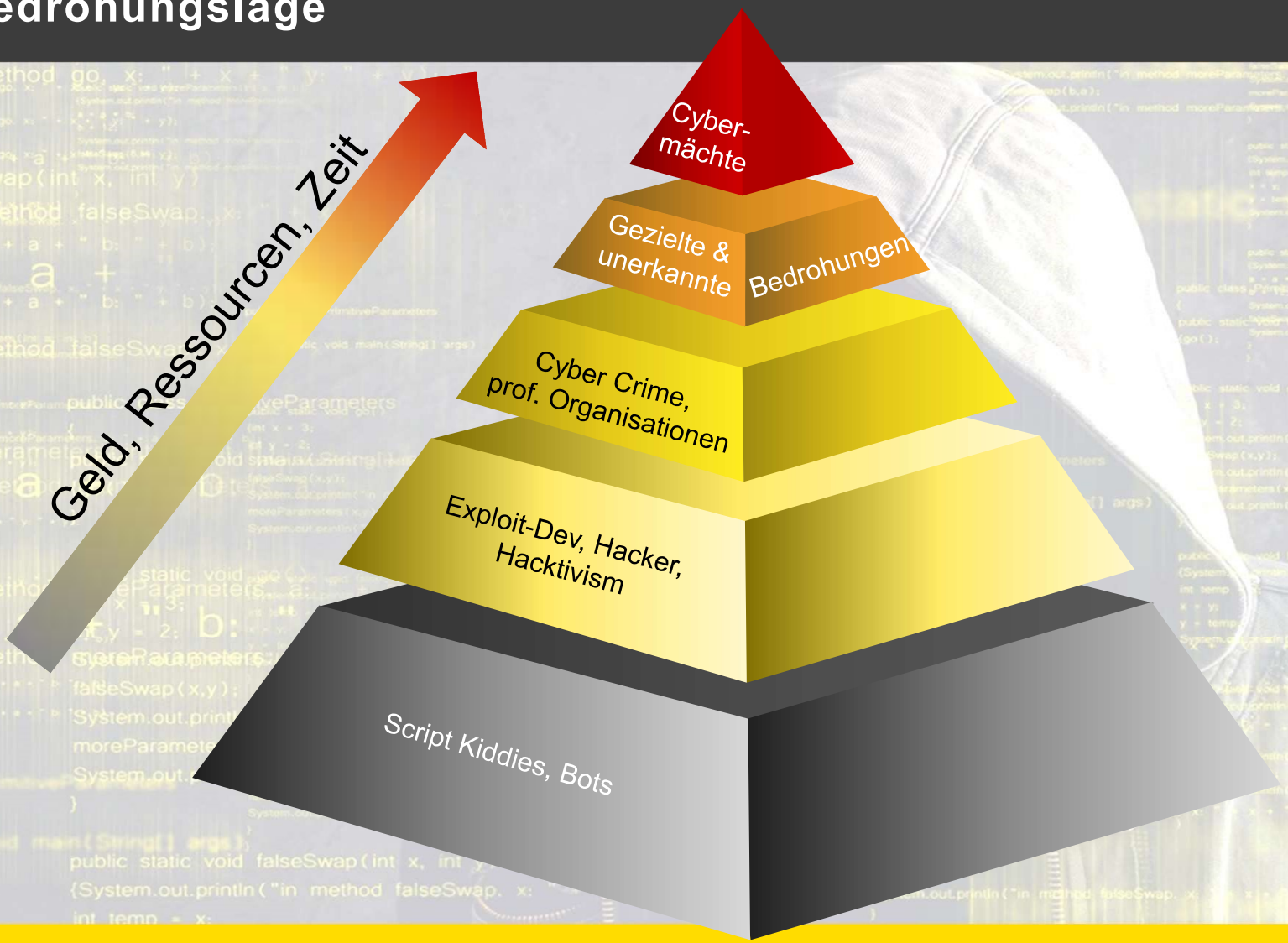
EMOTET, TRICKBOT UND RYUK – DAS SCHLIMMSTE TRIO SEIT ES COMPUTERVIREN GIBT?

Veröffentlicht am 05. Aug 2019 | von Stefan Rothenbühler | Cyberrisiken | 0 Kommentare

The Data Breach Question: No Longer an "If" But "When"

October 13, 2015 | Kevin Cunningham | View from Kevin

Bedrohungslage



Phasen der IT Security

InfoGuard
SWISS CYBER SECURITY

Prevent

Fortlaufende Behebung von Verwundbarkeiten und Stoppen von Angriffen

Detect

Erkennen der wichtigsten Bedrohungen mittels advanced analytics und forensics

Respond

Angemessene und schnelle Reaktion auf Security Events und Incidents

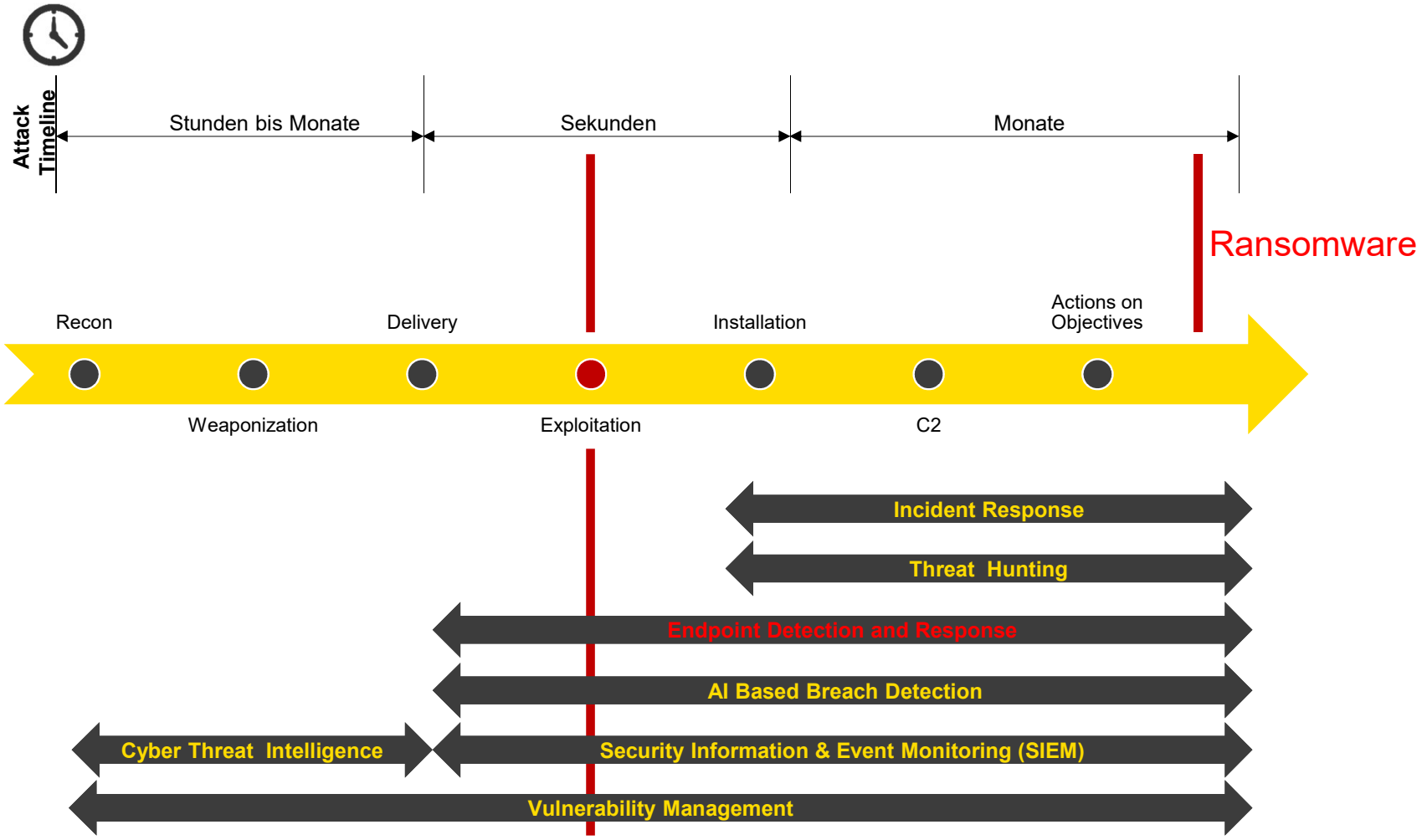
Detection und Prevention

- Fokus meistens auf präventiver Technologie
- Detection und response auf dem Vormarsch aber viel geringere Priorität als Prävention

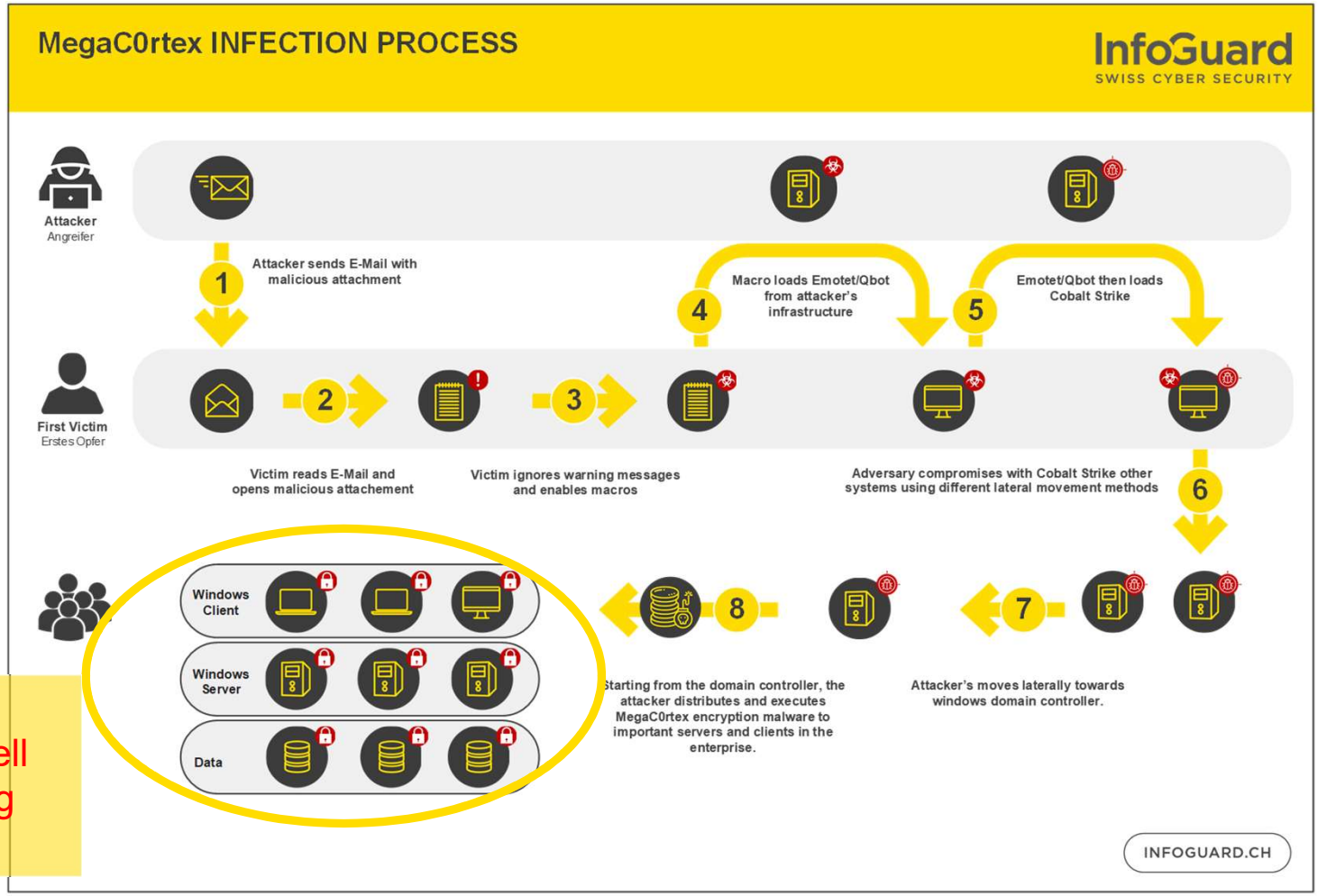
Response

- Möglichst schnell
- Möglichst automatisiert
- Möglichst umfassend

Prävention / Erkennung von Threats

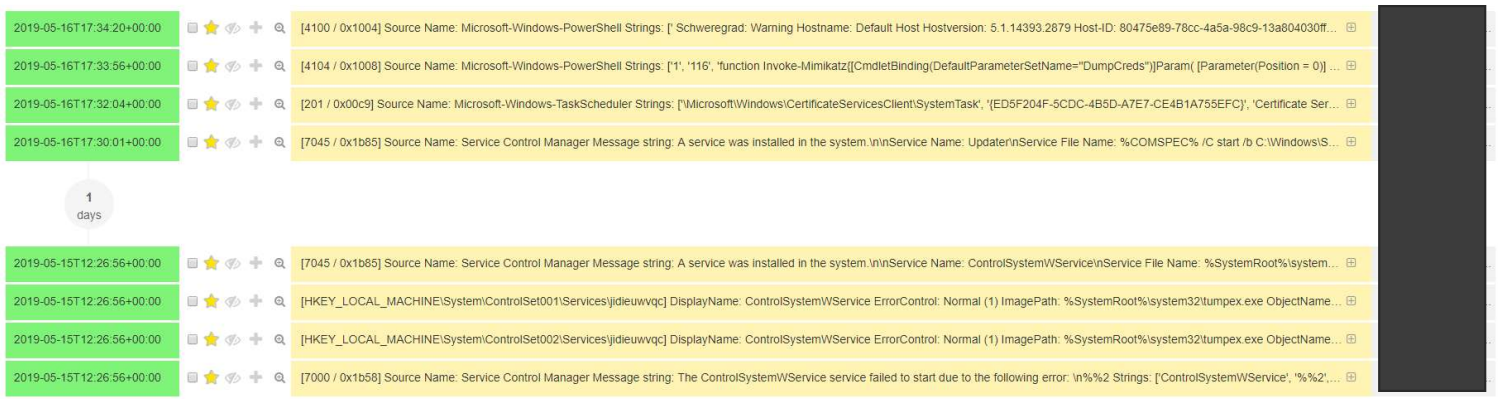


Beispiel: Emotet, Cobalt Strike und MegaC0rtex



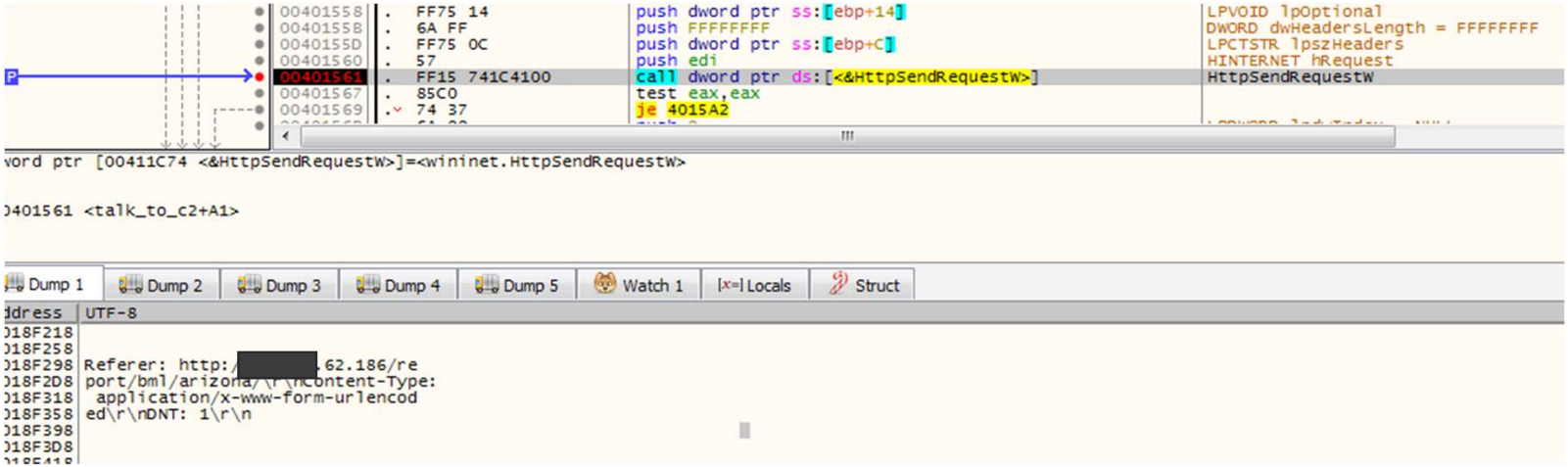
Game Over
Wenn nicht schnell genug und richtig reagiert wird.

Analyse eines Angriffs



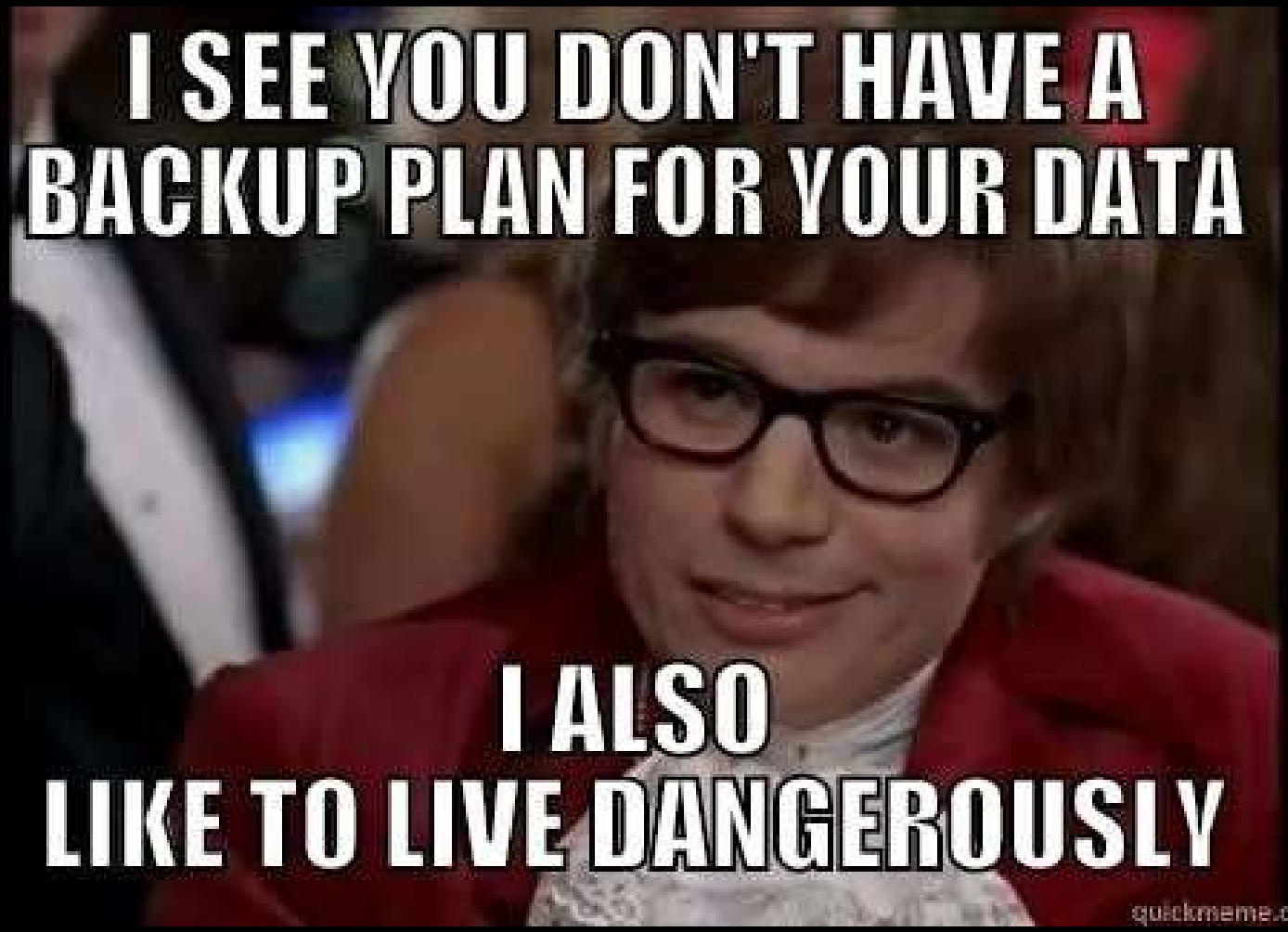
Supertimeline

Malware analysis



Lessons Learned – Offline Backup

InfoGuard
SWISS CYBER SECURITY



Lessons Learned – Zeitverlust beim IR Setup

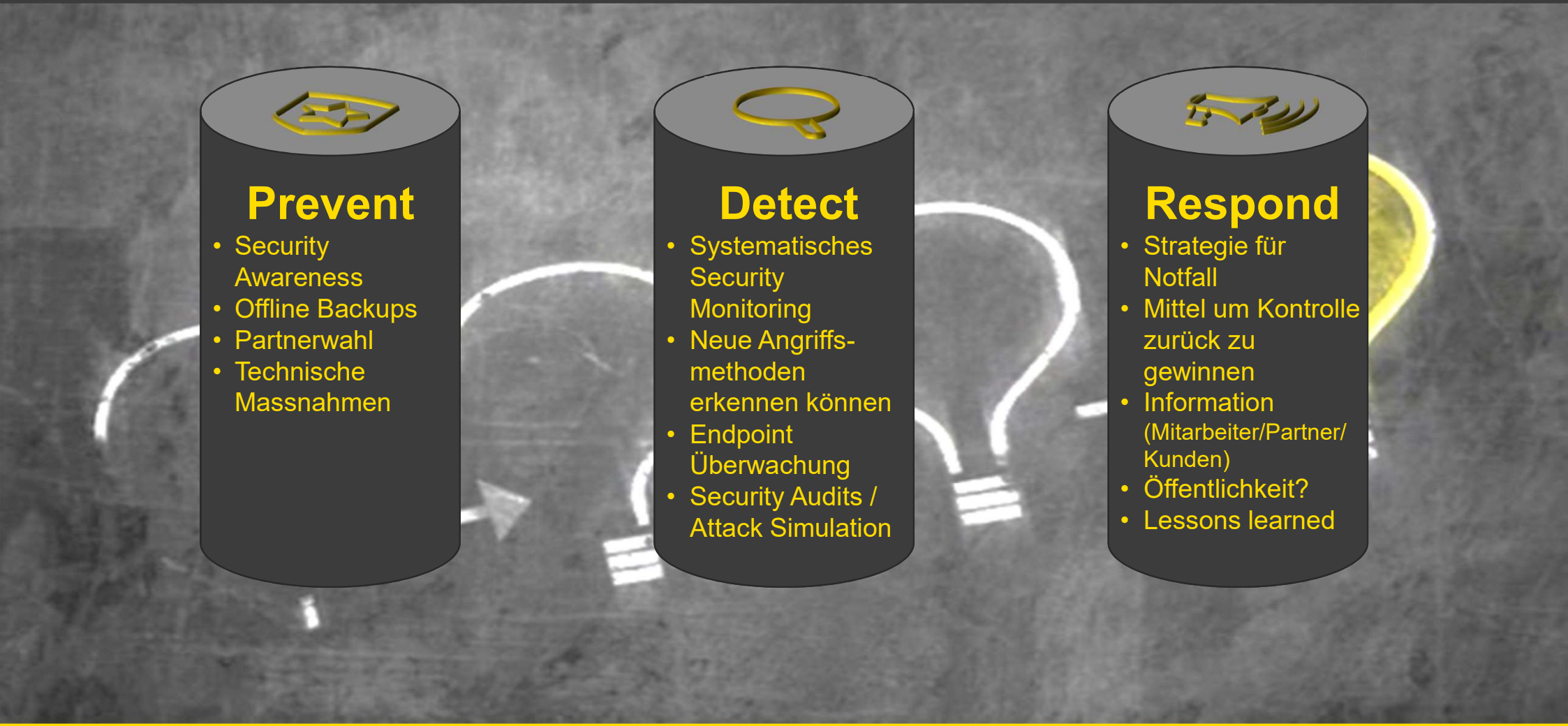
InfoGuard
SWISS CYBER SECURITY

Lessons Learned – Prioritäten

- Betrieb wieder herstellen
  - Aufbau einer neuen Umgebung?
  - Systeme eins nach dem anderen wieder aufschalten?
- Angreifer aussperren
  - Ist der Angreifer wirklich draussen?
  - Hintertüren?
  - Containment-Strategie?
- Forensics vs. Kontrolle?

Lessons Learned – Prevent, Detect & Respond

InfoGuard
SWISS CYBER SECURITY



Prevent

- Security Awareness
- Offline Backups
- Partnerwahl
- Technische Massnahmen

Detect

- Systematisches Security Monitoring
- Neue Angriffs-methoden erkennen können
- Endpoint Überwachung
- Security Audits / Attack Simulation

Respond

- Strategie für Notfall
- Mittel um Kontrolle zurück zu gewinnen
- Information (Mitarbeiter/Partner/ Kunden)
- Öffentlichkeit?
- Lessons learned

Lessons Learned – Prevent, Detect & Respond

InfoGuard
SWISS CYBER SECURITY

Prevent

- Security Awareness
- Offline Backups
- Partnerwahl
- Technische Massnahmen

Detect

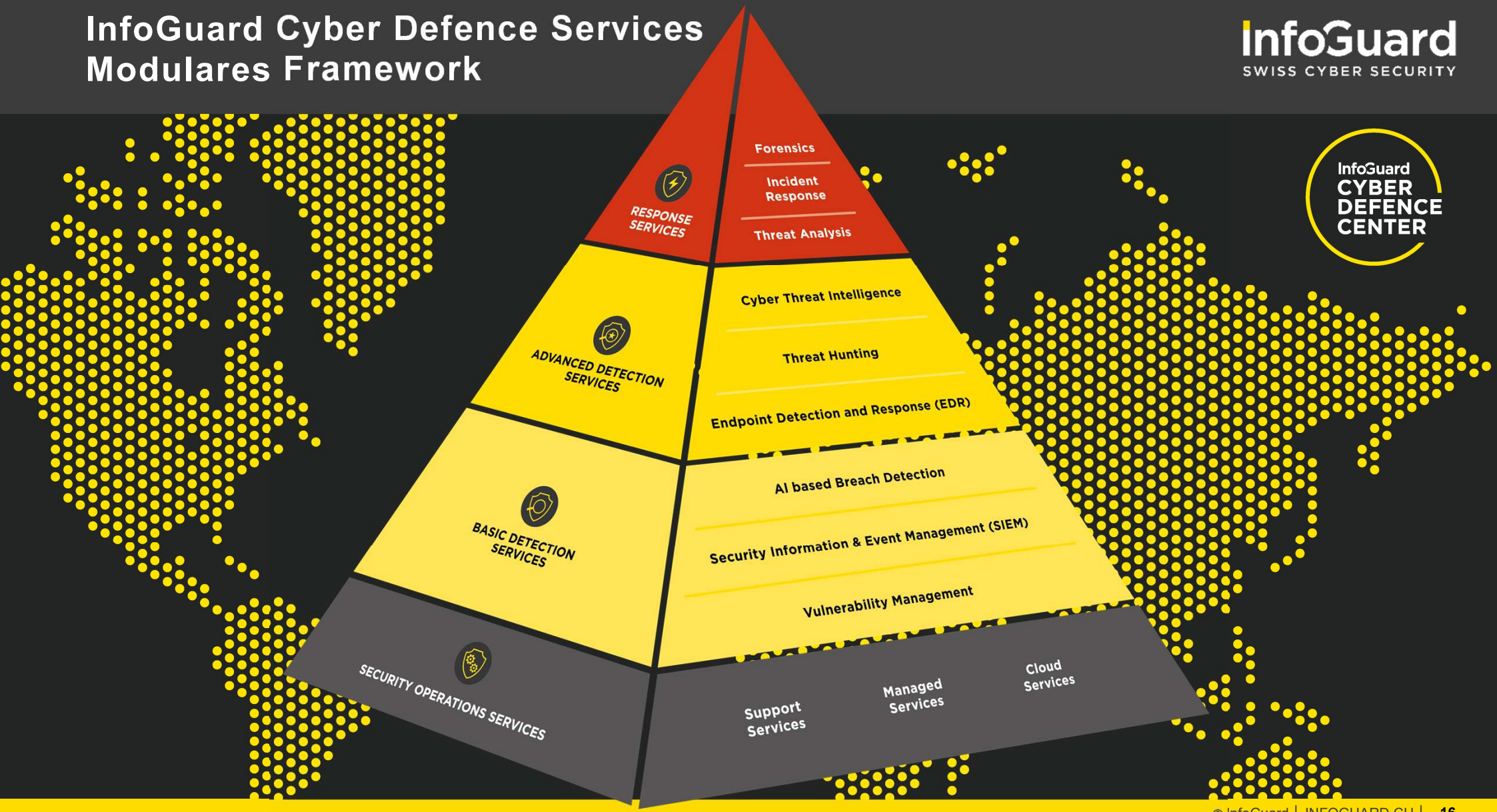
- Systematisches Security Monitoring
- Neue Angriffsmethoden erkennen können
- Endpoint Überwachung
- Security Audits/Attack simulation

Respond

- Strategie für Notfall
- Mittel um Kontrolle zurück zu gewinnen
- Information (Mitarbeiter/Partner/ Kunden)
- Öffentlichkeit?
- Lessons learned

InfoGuard Cyber Defence Services
Modulares Framework

InfoGuard
SWISS CYBER SECURITY



InfoGuard
CYBER
DEFENCE
CENTER

InfoGuard Cyber Defence Services

Sicherheitskompetenz aus der Schweiz!

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz

Telefon +41 41 749 19 00
www.infoguard.ch