DerTreasurer
ROUNDTABLE

Digital-konferenz

Fokus: Cash Management

21. April 2020

VERANSTALTER

DerTreasurer
NACHRICHTEN FÜR DIE FINANZABTEILUNG

MITVERANSTALTER

SWIFT

DerTreasurer ROUNDTABLE

WICHTIGE HINWEISE

- Schließen Sie alle anderen Programme im Hintergrund.
- Die Links zu den einzelnen Slots haben Sie per E-Mail erhalten.
- Informationen zu den Mitschnitten und den freigegebenen Präsentationen erhalten Sie in den kommenden Tagen.

DerTreasurer
ROUNDTABLE

TECHNISCHE PROBLEME?

- Häufig gestellte Fragen: https://www.dertreasurer.de/events/webinare/faq/
- Nutzen Sie die Chatfunktion im Webinartool.
- Schreiben Sie uns eine Mail an webinar@dertreasurer.de.

DerTreasurer ROUNDTABLE

PRAXISVORTRAG

Cybersecurity & Treasury: Angriffsmuster, Angriffsziele, Erkennungs- und Abwehrstrategien

Frank Reiländer
CGI

CGI

CGI

Experience the commitment®

Cybersecurity & Treasury

Angriffsmuster, Angriffsziele, Erkennungs- und Abwehrstrategien

Praxisdialog zur digitalen Roundtable-Veranstaltung

21. April 2020

Frank Reiländer, CGI Deutschland B.V. & Co. KG

DerTreasurer

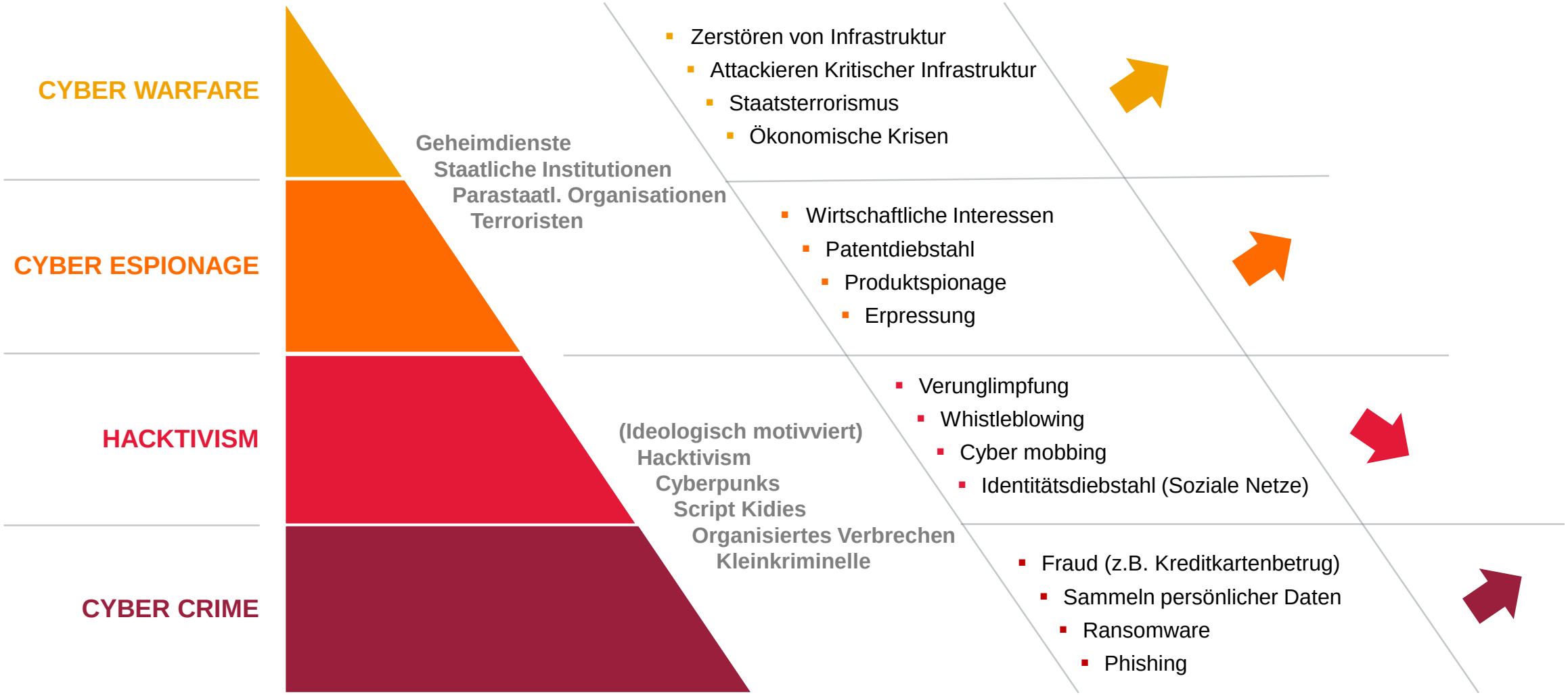
NACHRICHTEN FÜR DIE FINANZABTEILUNG

Themen des Praxisdialogs

- **Wer** bedroht meine Daten**?**
- **Was** könnte ein Angreifer wollen**?**
- **Wie** läuft ein beispielhafter Angriff ab**?**
- **Was passiert** bis und bei Entdeckung**?**
- **Wie** sollte ich auf den Angriff **reagieren?**
- **Wie** kann ich mich **schützen?**

Nutzen Sie die Dialogmöglichkeiten…

Herausforderungen unserer Zeit: Wachsendes Risiko an Cyberangriffen



Evolution von Cyber Defense Techniken

- DMZ – Demilitarized Zone
- IDS – Intrusion Detection System
- IPS – Intrusion Prevention System

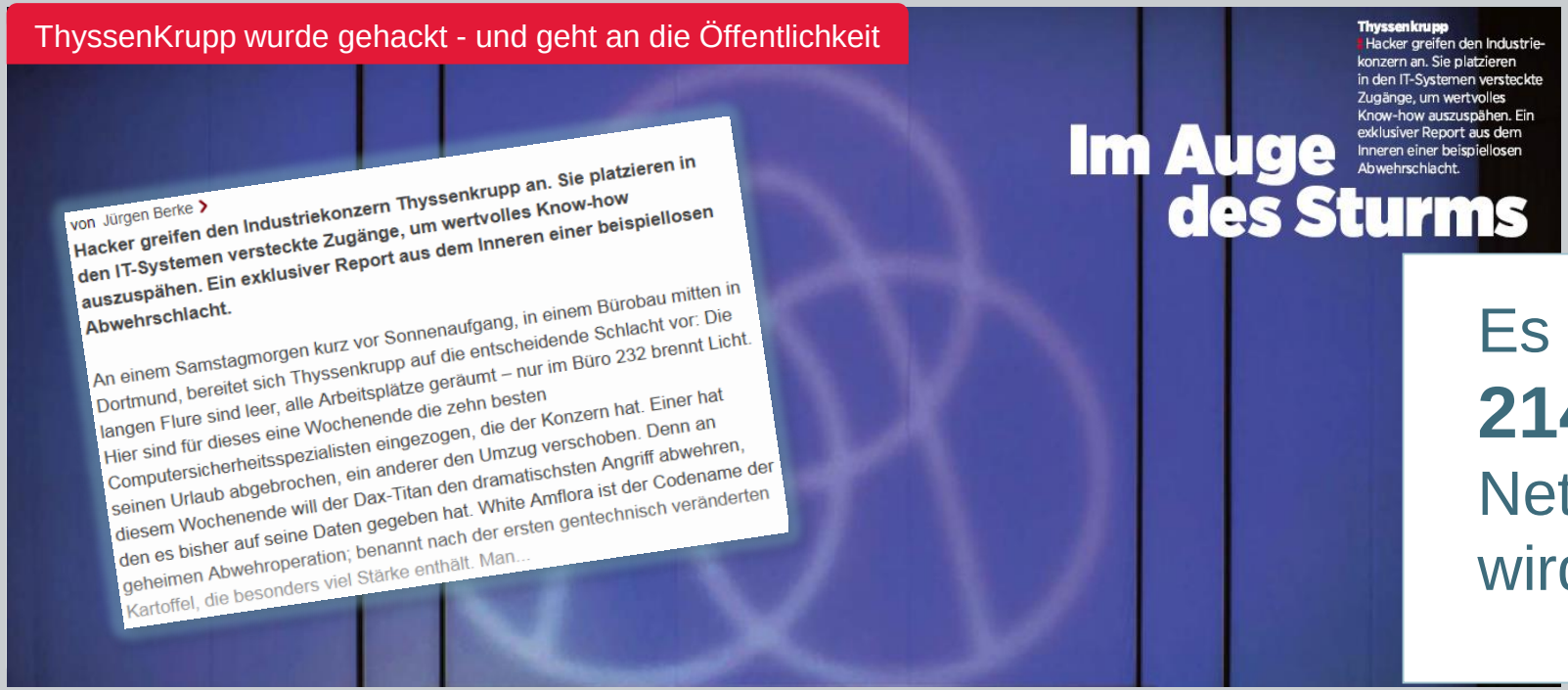
Klassische Konzepte sind unzureichend!

Angriffsziele und –folgen im Cash Management

- eBAM: Kein Zugriff auf Kontoverwaltungen
- Cash-Pooling/Cash Concentrating: Keine Abforderung von Guthaben auf “Töchterkonten“ und damit nicht effiziente Nutzung von vorhandenem Working Capital
- Zahlungen bleiben hängen wegen nicht vorhandener Kontodeckung
  - z.B. sind Gehaltszahlungen kritisch
- Manipulation von Stammdaten
  - Kontoinformationen,
  - Währungspositionen
- Blindflug von Informationsgehalt – insbesondere bei Lahmlegen von Informationsaustausch zwischen Bank und Firma
- Eingriff auf vertrauliche Finanzunterlagen, Kreditunterlagen, Forderungsbeständen
  - Eventuell Einflüsse auf Rating
  - Ad-hoc Risiko bei Veröffentlichung von „Gerüchten“?
    - Verschlechterte Rating/Bonität
      => Höhere Refinanzierungskosten

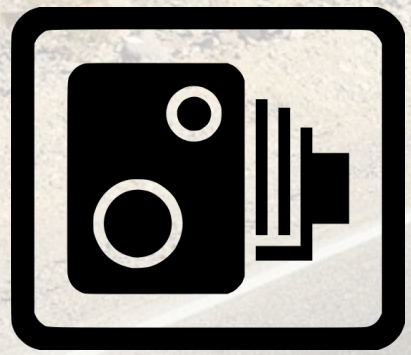
Herausforderungen unserer Zeit: Nachgewiesene Fälle von Cyberspionage

ThyssenKrupp wurde gehackt - und geht an die Öffentlichkeit

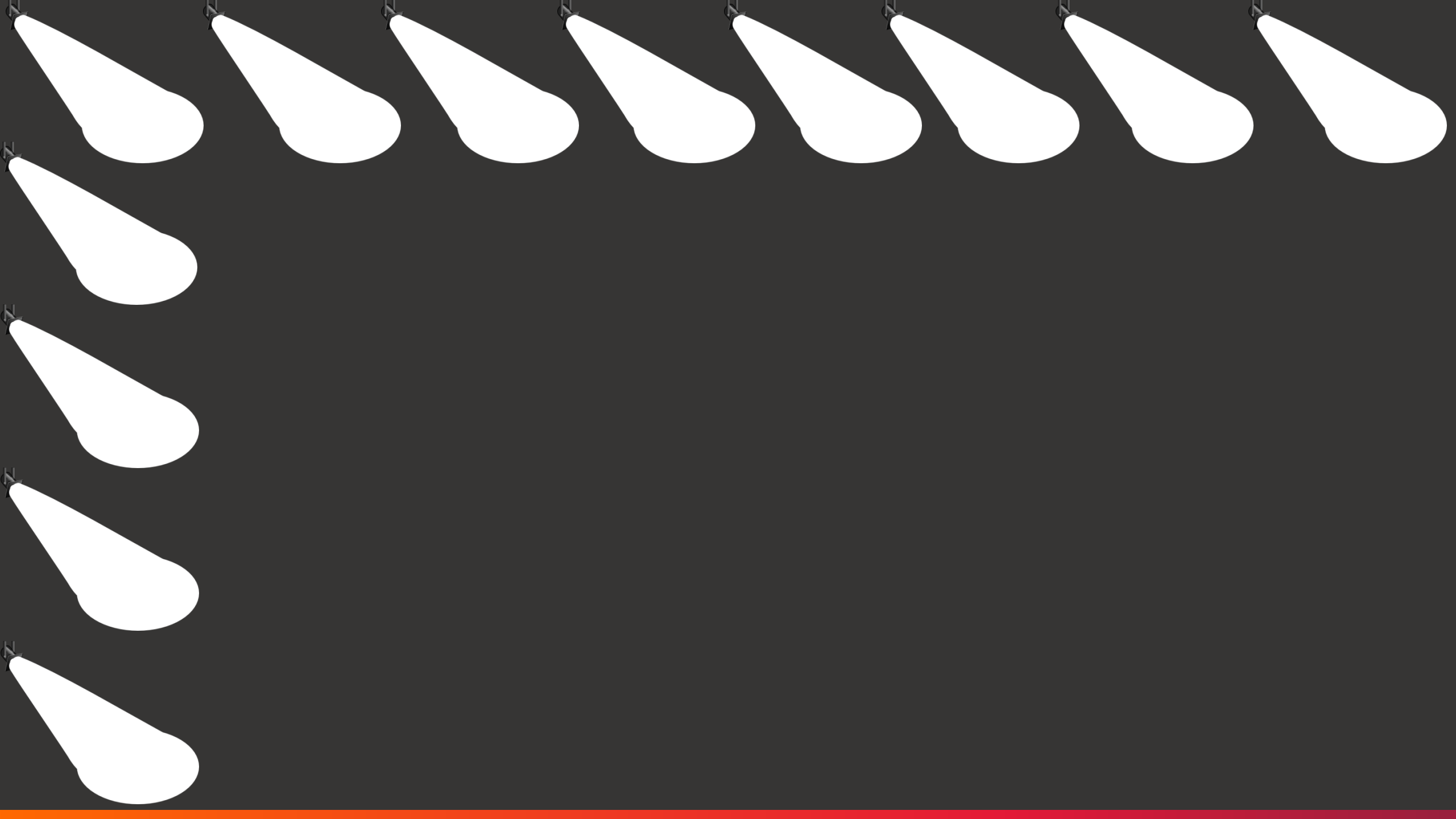


Es dauert im Durchschnitt **214** Tage, bevor ein Netzwerk-Hack entdeckt wird

Quellen: Wirtschaftswoche (Druckmedien) 09.12.2016, PWC Studie 2015

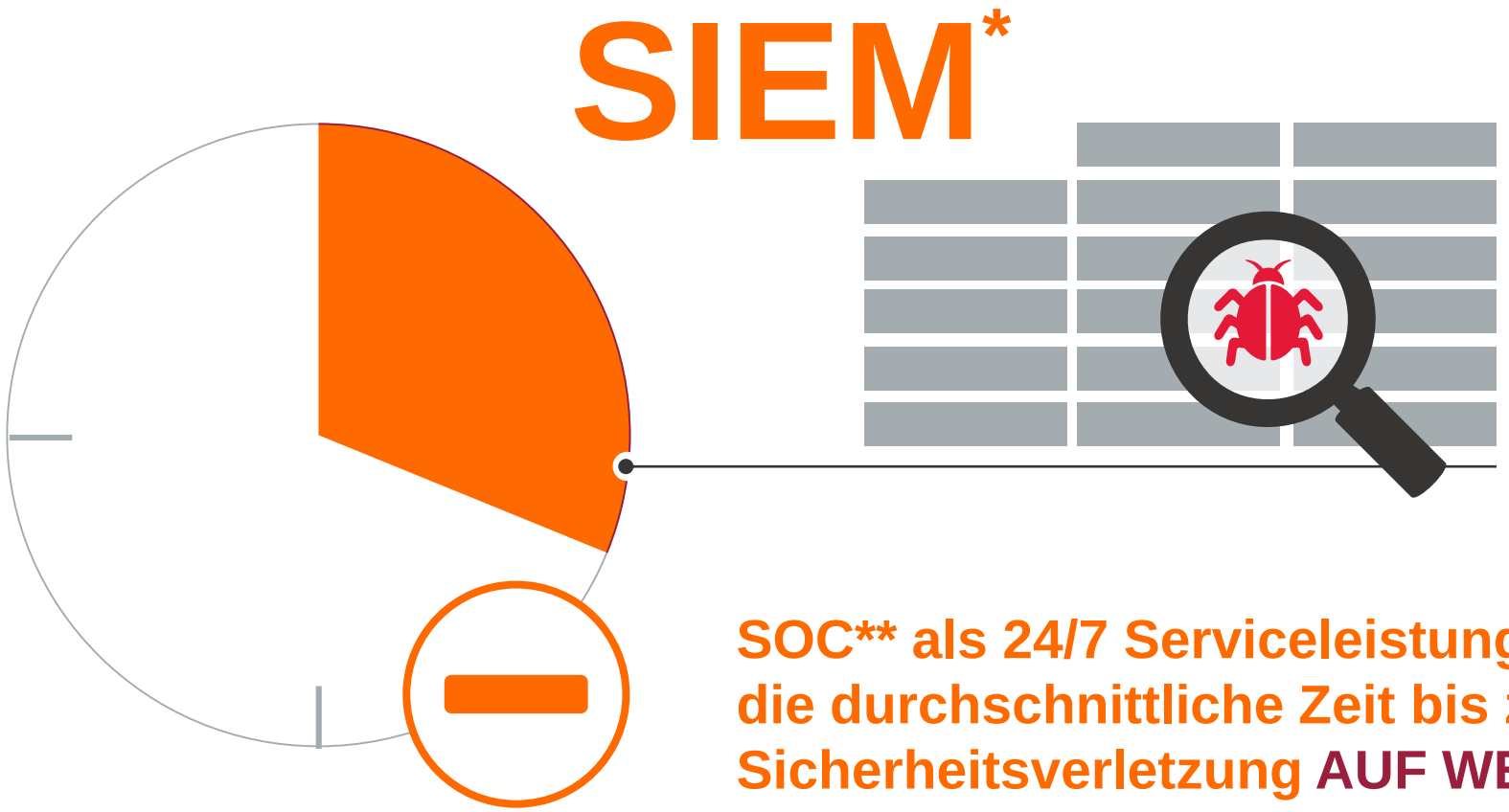


Sehen wir eigentlich, was in unserem Netz passiert?



Situational Awareness!

Frühzeitige Identifizierung von Bedrohungen



Es dauert **im Durchschnitt 214** Tage, bevor ein Einbruch ins Netzwerk entdeckt wird

SOC als 24/7 Serviceleistung REDUZIERT die durchschnittliche Zeit bis zur Entdeckung einer Sicherheitsverletzung AUF WENIGE STUNDEN.**

*SIEM – Security Incident & Event Monitoring
**SOC – Security Operation Center

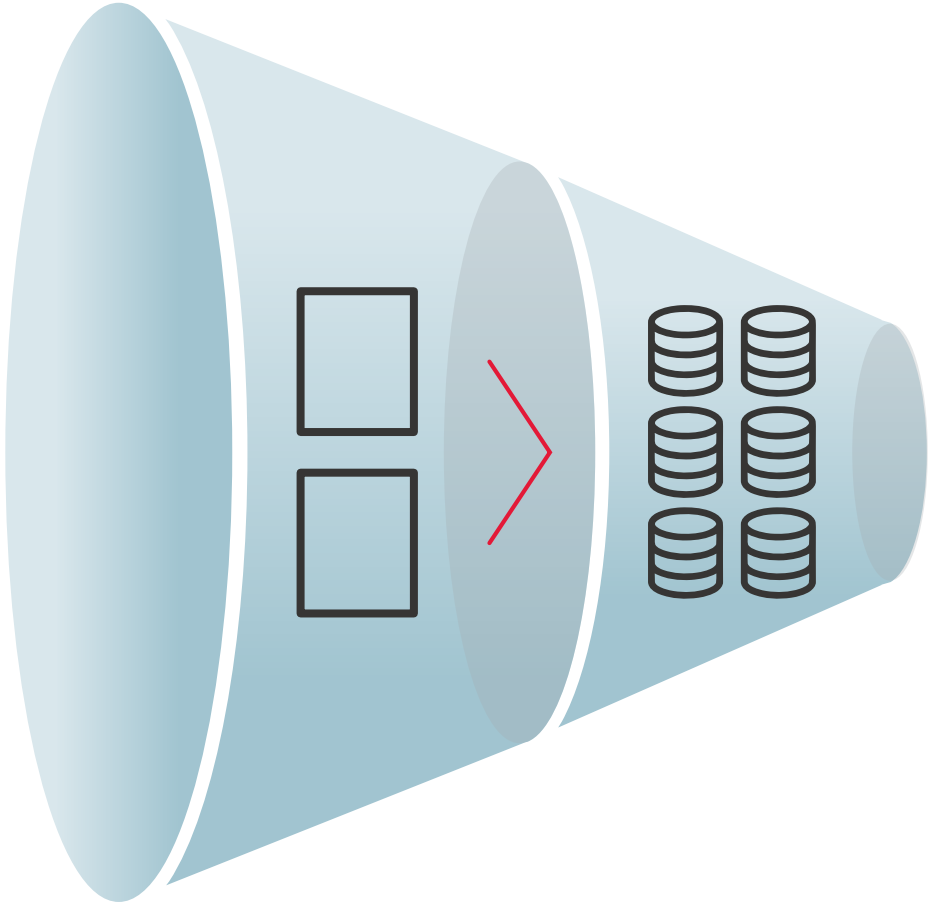
SIEM auf einen Blick:
von der Datenerhebung bis zu den Ergebnissen

SAMMELN

Verlaufsdaten
- Firewall
- DNS
- IPS/IDS
- Domaincontroller
- Mailgateway
- Proxy

Kontextbezogen
- Bestandsdaten
- CMS Daten
- Personaldaten
- DHCP
- Schwachst.-Scans
- Bedrohungserk.

NORMALISIEREN **SPEICHERN**



- Übersicht
- Korrelation & Alarme
- Berichte
- Suchen

Inside SOC


Statistics today
Events 24 000 000
Alerts 115
Incidents 18
Notifications 6
Unassigned alerts
CRITICAL 0
HIGH 2
MEDIUM 15
LOW 30

Plug critical holes!

Schäden und Schutzmaßnahmen im Treasury

Auswirkungen eines Cyber-Angriffs auf Treasury (verbunden mit kompletten IT-Ausfall):

- Kein Forderungsmanagement & damit verbunden: Kreditausfallrisiko
- Kein Währungshedging
- Verlust der Zahlungsfähigkeit (kritisch für jede Firma: Illiquidität = Insolvenz)

Notendige Maßnahmen:

- Schutz der ZV-Infrastruktur, am Besten durch „Abdocken“ von der Außenwelt (Fremdeinfälle reduzieren)
- Aktives Risikomanagement (SIEM-Management)
- Datenstromüberwachung

Hauptprobleme:

- Interne Sicherheitslücken
- Fehlende Sorgfalt im Umgang mit vertrauenssensiblen Daten

Lösungsansätze:

- Security Assessments / Beratung
- Prüfung der Infrastruktur unter Anwendung des SWIFT-CSCF

STOP playing whack a mole!

Lassen Sie uns über Ihre Themen sprechen!

Frank Reiländer
Vice President | Head of Cybersecurity

Mobil: +49 176 1044 5878
E-Mail: frank.reilaender@cgi.com

https://de.cgi.com/cybersecurity

Cybersecurity is part of everything we do…

DerTreasurer
ROUNDTABLE

WEBINARRAUM-WECHSEL

PRAXISVORTRAG | 16.20-17.00 Uhr

Was neue Technologien für das Treasury leisten

DerTreasurer
ROUNDTABLE

Digital-konferenz

Fokus: Cash Management

21. April 2020

VERANSTALTER

DerTreasurer
NACHRICHTEN FÜR DIE FINANZABTEILUNG

MITVERANSTALTER

SWIFT