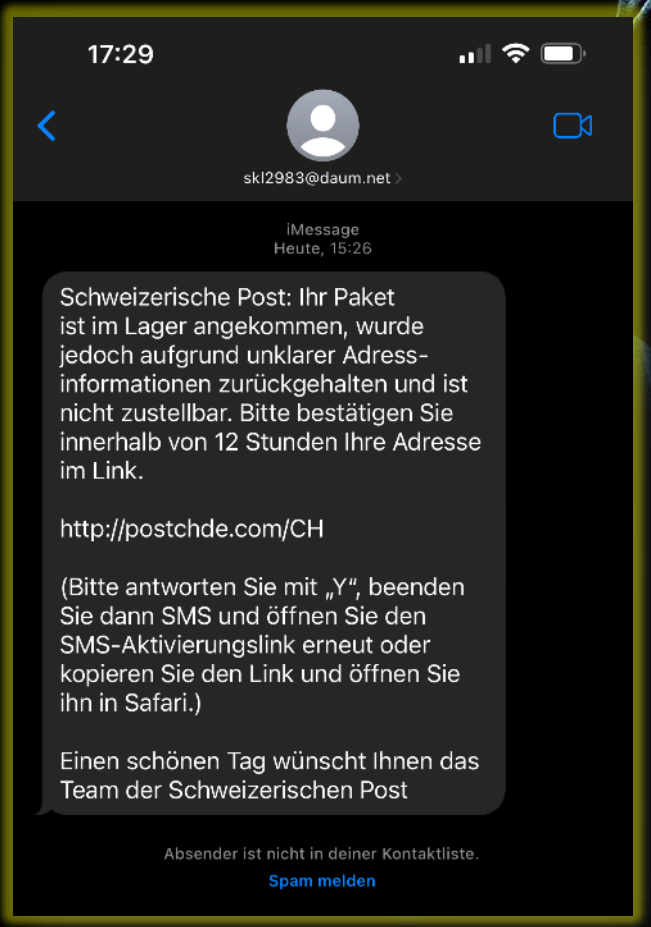

Securing
Your Digital
World
ASA | SVV
Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni
Swiss Insurance Association
InfoGuard
SWISS CYBER SECURITY
Cybercrime
Die Rolle der Incident Responder
Ernesto Hartmann, Chief Cyber Defence Officer

Geschäftsmodell Cybercrime

InfoGuard
SWISS CYBER SECURITY

Business Case mit unerschöpflichem Potential

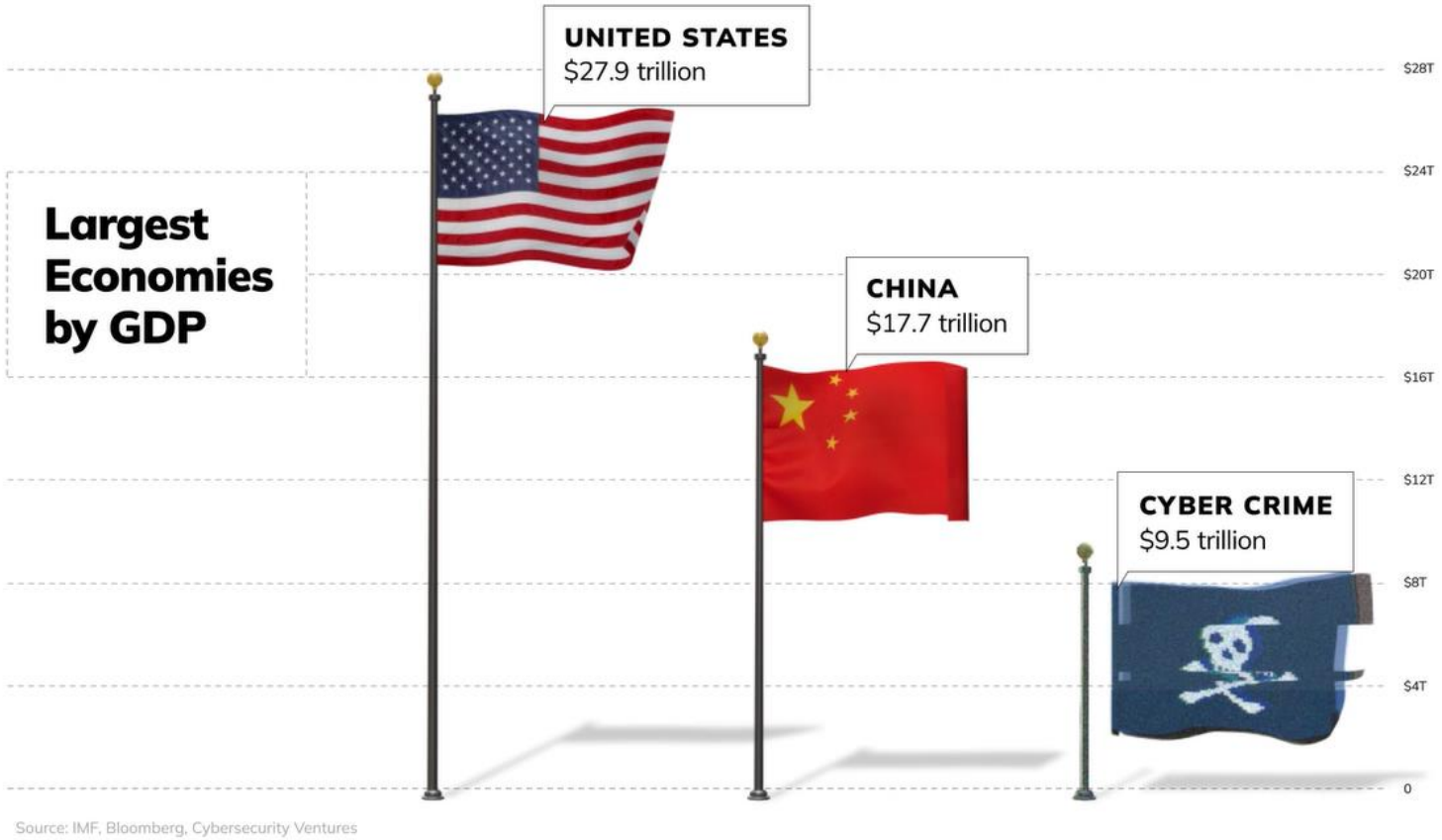
InfoGuard
SWISS CYBER SECURITY

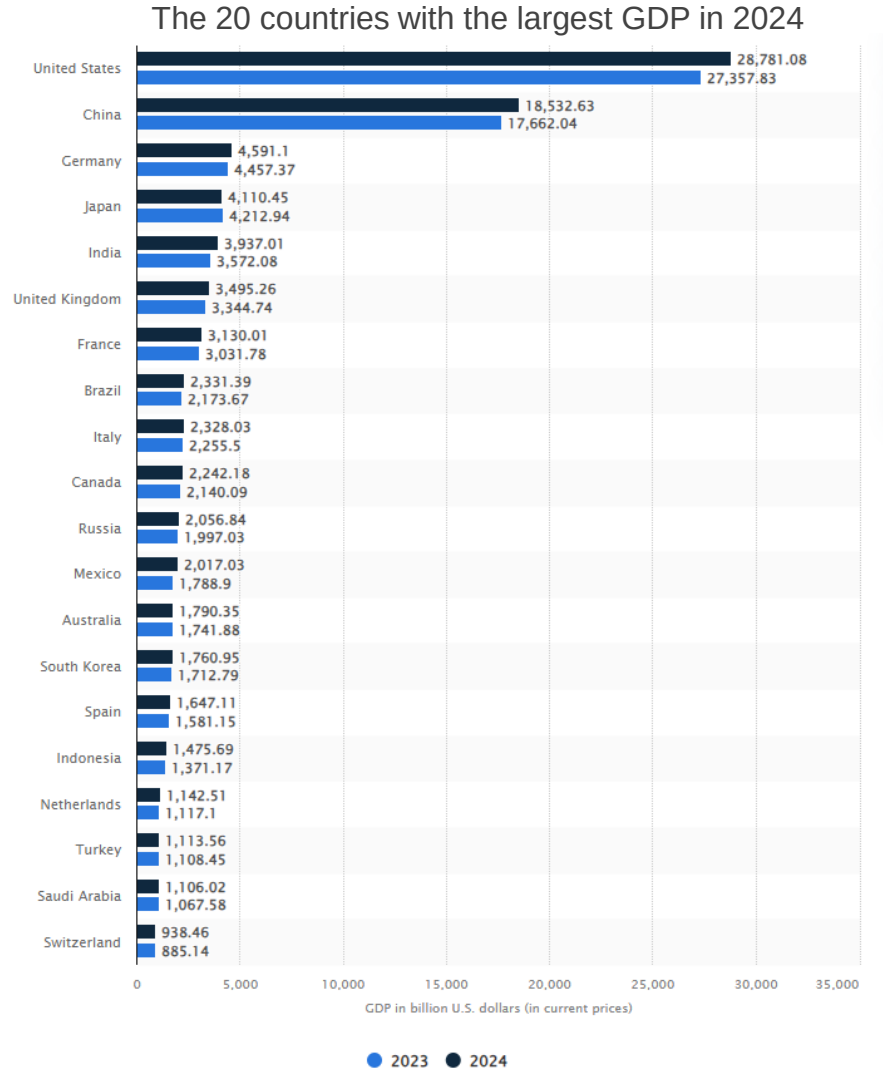


SMISHING

> Jede digitalisierte Person auf dieser Welt ist ein potenzielle(s)r ~~Opfer~~ Kunde

Die drittgrösste Volkswirtschaft der Welt hat böse Absichten – und sie wird weiter wachsen…





Source: Bloomberg

Aktuelle Bedrohungslage Schweiz

InfoGuard
SWISS CYBER SECURITY

Watson

Autohändler Emil Frey ist von Cyberattacke betroffen: Website offline

Die Emil-Frey-Gruppe ist das neuste Opfer einer Cyberattacke. Laut dem Schweizer Unternehmen mit rund 22'000 Angestellten sind mehrere...

12.01.2022

bz Basel

Auch Psychiatrie Baselland Opfer einer Cyberattacke: Ausmass noch unbekannt

Der Neubau der Kinder- und Jugendpsychiatrie auf dem Areal der Psychiatrie Baselland in Liestal. Die gesamte Institution wurde jetzt Opfer einer...

16.10.2023

Inside IT

Schoggifabrikant Läderach von Ransomware-Attacke ...

Die Produktion, Logistik und Administration des Chocolatiers sollen vom Cyberangriff betroffen sein. Der Verkauf in den Filialen funktioniert...

06.09.2022

Aargauer Zeitung

Siegfried Zofingen: Cyber-Attacke hat Folgen für Mitarbeiter

Der Cyber-Angriff auf das IT-Netzwerk des Pharma-Unternehmens Siegfried Gruppe mit Hauptsitz in Zofingen hat Folgen für die Mitarbeiter. 15.06.

15.06.2021

St. Galler Tagblatt

Lösegeld - Nach Cyber-Angriff: Erpresser erhöhen Druck auf Peter Spuhlers Stadler Rail

Nach Cyber-Angriff: Erpresser erhöhen Druck auf Peter Spuhlers Stadler Rail. Die Cyberkriminellen, die Anfang Mai ins IT-Netzwerk des...

06.07.2020

Beobachter
https://www.beobachter.ch › digita · Translate this page

Hacker erpressen Bernina und fordern 1,3 Millionen

28 Apr 2023 — Unbekannte **Cyberkriminelle** sind bei der Schweizer Traditionsfirma **Bernina** an die Falsche geraten. Die Chronologie einer skrupellosen Erpressung, ...

Inside Paradeplatz

V-Zug wehrt Cyber-Attacke ab

V-Zug wehrt Cyber-Attacke ab ... Vor Jahresfrist war bereits mit der Stadler Rail von Unternehmer Peter Spuhler ein Betrieb aus dem...

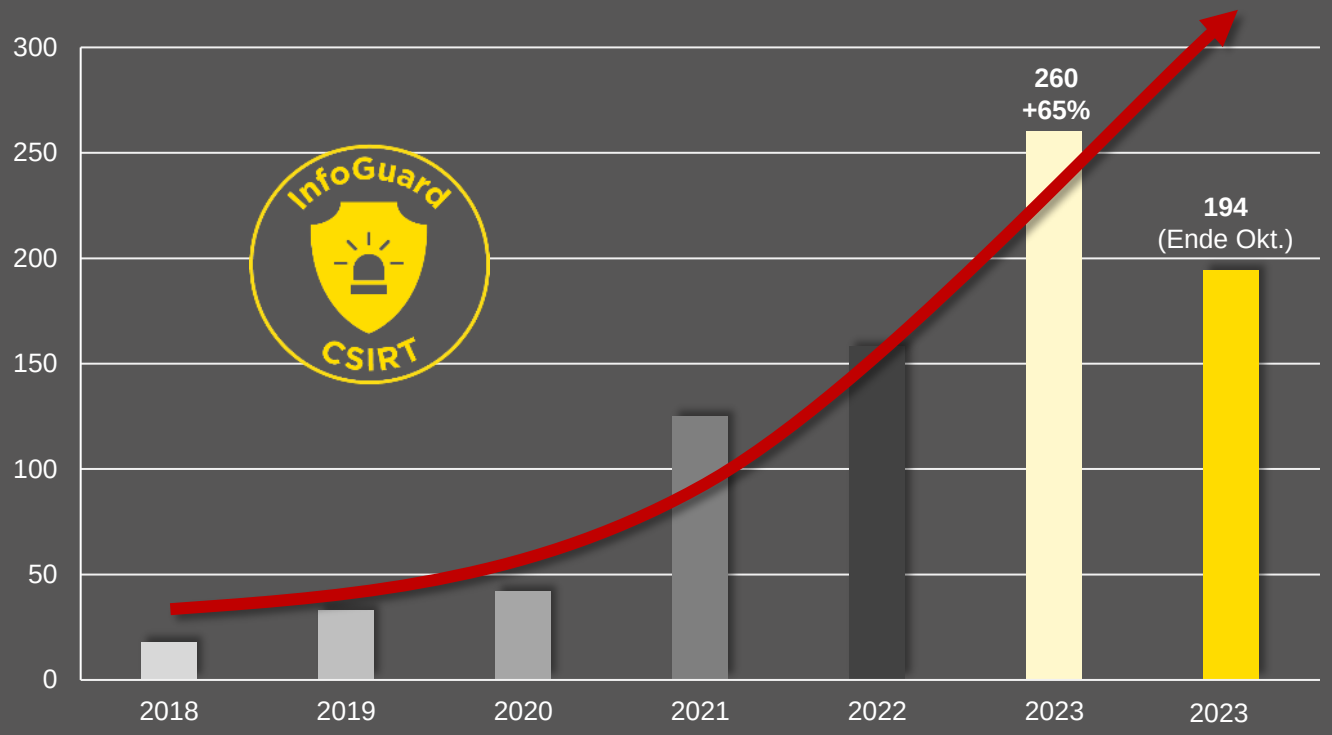
28.07.2021

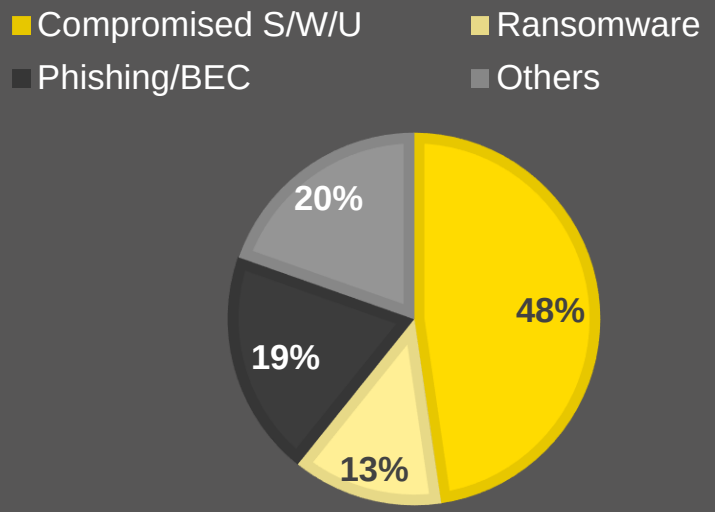
Berner Zeitung
https://www.bernerzeitung.ch › Bern › Bern/Mittelland

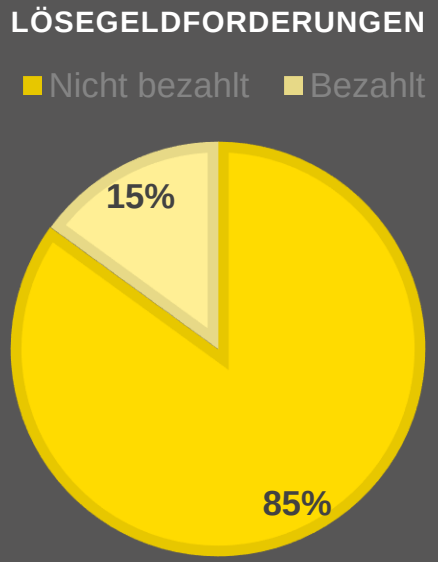
Hackerangriff in Zollikofen: Gemeinde wieder am Netz ...

28.11.2023 — Seit dem 22. November ist die **Gemeinde Zollikofen** nur eingeschränkt erreichbar gewesen. Nun sind die Systeme wieder hochgefahren worden.

Bedrohungslage – Bearbeitete Sicherheitsfälle durch das CSIRT



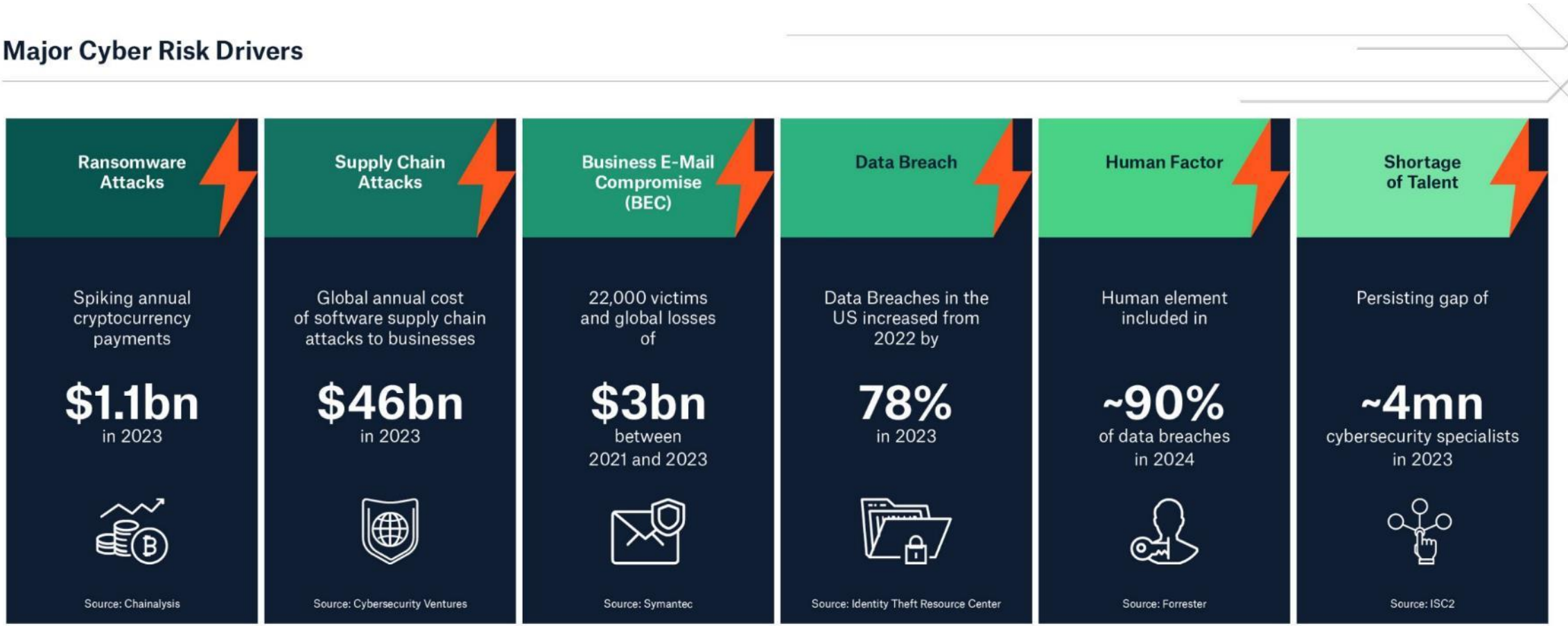




Hohe Fallzahlen ermöglichen tagesaktuelle Informationen über die Bedrohungslage.

Source InfoGuard CSIRT

Sicht eines Rückversicherers
Aktuelle Cyber-Risikolandschaft – Hotspots



Quelle Munich Re

Cyberkriminelle sind in Lieferketten organisiert.

InfoGuard
SWISS CYBER SECURITY

REMOTE ACCESS BROKER → INITIAL ACCESS BROKER → RANSOMWARE AFFILIATES → RANSOMWARE OPERATORS / DEVELOPERS

Mask	Country	State / City	Details		Info	Vendor	Blacklist	Price	Action
195.141.***.** ISP: Sunrise Communications AG		Zurich Zurich	OS: Win2008/7 Proc: Intel Core i7 7840K RAM: 6 GB | 16.71 / 73.13 Mbit/s	Admin: No Paypal: No NAT: No	ⓘ	de####ok (platinum)	BL	$ 6.00	Buy
178.192.***.** ISP: Swisscom (Schweiz) AG - Bluewin		Lucerne Emmenbruecke	OS: Windows Proc: - RAM: - GB | - / - Mbit/s	Admin: - Paypal: - NAT: -	-	RDP (platinum)	BL	$ 10.00	Buy
188.61.***.** ISP: Swisscom (Schweiz) AG - Bluewin		Zurich Zurich	OS: Windows Proc: - RAM: - GB | - / - Mbit/s	Admin: - Paypal: - NAT: -	-	RDP (platinum)	BL	$ 10.00	Buy
83.79.***.** ISP: Swisscom (Schweiz) AG - Bluewin		Ticino Locarno	OS: Windows Proc: - RAM: - GB | - / - Mbit/s	Admin: - Paypal: - NAT: -	-	RDP (platinum)	BL	$ 10.00	Buy
81.6.***.** ISP: green.ch AG		Lucerne Eich	OS: Win2008/7 Proc: Intel/Amd RAM: 2 GB | 1 / 1 Mbit/s	Admin: No Paypal: Yes NAT: Yes	ⓘ	jS####ow (platinum)	BL	$ 6.00	Buy
20.199.***.** ISP: Microsoft Corporation		Zurich Zurich	OS: Windows Proc: - RAM: - GB | - / - Mbit/s	Admin: - Paypal: - NAT: -	-	RDP (platinum)	BL	$ 10.00	Buy
46.140.***.** ISP: UPC Schweiz GmbH		Geneva Carouge	OS: Windows Proc: - RAM: - GB | - / - Mbit/s	Admin: - Paypal: - NAT: -	-	RDP (platinum)	BL	$ 10.00	Buy
109.164.***.** ISP: Swisscom (Schweiz) AG - Cybernet		Solothurn Deitingen	OS: Win2008/7 Proc: RAM: - GB | - / - Mbit/s	Admin: No Paypal: - NAT: -	ⓘ	am####mg (platinum)	BL	$ 6.00	Buy

IR-727 –
Erworbene Darknet Accounts werden monetarisiert!

InfoGuard
SWISS CYBER SECURITY

Original-Ton der Angreifer:

«I've got access to your O365 after I bought stealer logs https://[redacted]. It was Racoon to be more exact. One of your employees, [redacted], downloaded malware, and I guess Windows Defender was just turned off, because it's almost impossible to make any popular stealer like Redline, Racoon, Vidar to be FUD, especially spreading exe within tons of users. The attack was not targeted at you, I was looking for citrix accesses, but it turned out that the credentials for citrix was not valid.»

Werden Ihre Zugangsdaten im Darknet gehandelt?
Wir finden es für Sie heraus!

Source InfoGuard CSIRT

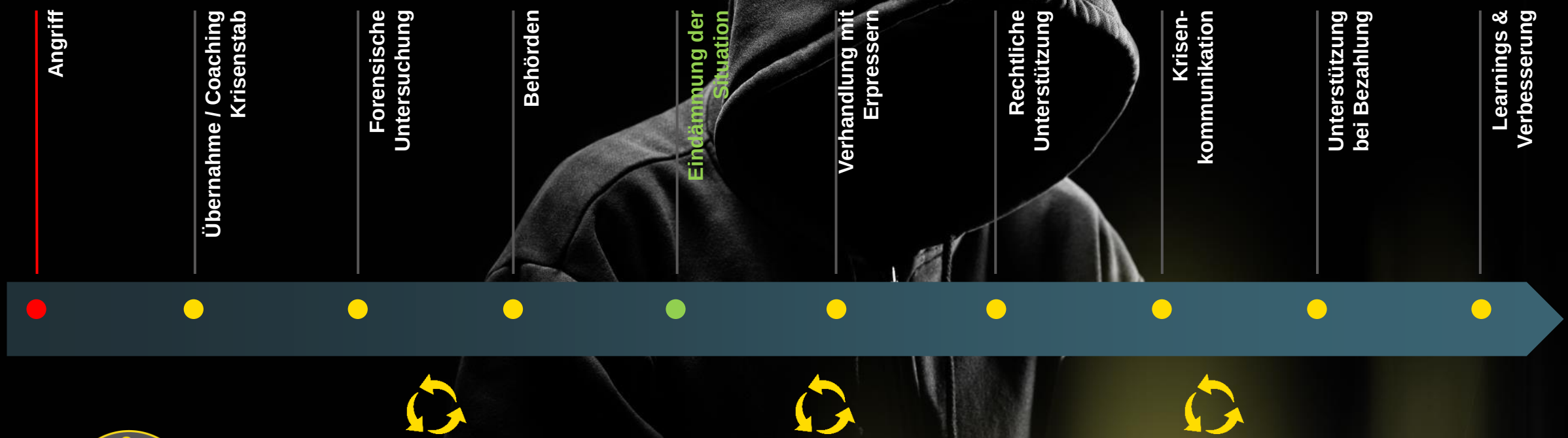
InfoGuard
SWISS CYBER SECURITY

Das Internet ist das Rückgrat der Computerkriminalität!

Wir müssen unsere Angriffsfläche verringern.

Die Rolle der Incident Responder im ~~Detail~~ Wandel

InfoGuard
SWISS CYBER SECURITY



InfoGuard CSIRT

Schutz vor einem Geschäftsausfall | Gesicherter Wiederanlauf / Aufbau

Schadensprävention | Schadensbewältigung

InfoGuard CSIRT – Prioritäten bei einem IR-Fall

InfoGuard bearbeitet Vorfälle effizient und anhand der folgenden drei Parameter:

1. **Wertschöpfungskette sichern oder wiederherstellen**
   Aufrechterhaltung oder Wiederherstellung der Business-Tätigkeit des Kunden um weiteren Schaden zu vermeiden.

2. **Verlust minimieren**
   Wenn Daten abhanden gekommen oder modifiziert worden sind, müssen negative Auswirkungen bewertet werden. Daher fokussieren wir uns auf Beweise für Exfiltration und Datenmanipulation.

3. **Sicherheit nachhaltig optimieren**
   Wir wollen die Sicherheit des Kunden nachhaltig optimieren – und Angriffe verhindern. Aus diesem Grund analysieren wir, die gesamte Angriffskette bis hin zum Ursprung (Patient-Zero).

Der Nutzen einer professionellen Incident Response für Versicherer und Versicherte

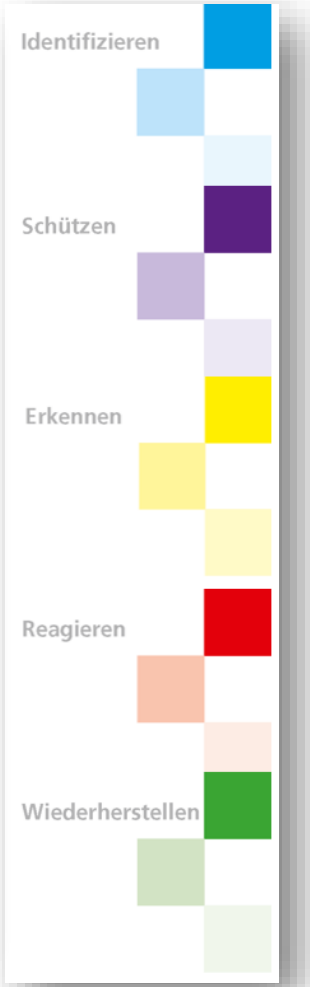
- Kompromissloser Fokus auf die **schnelle und sichere Wiederherstellung der Business-Handlungsfähigkeit**
  Effektive & effiziente Forensik-Methodik schafft **Sichtbarkeit innerhalb von Minuten** und skaliert auf grosse Umgebungen
  Sicherer Wiederaufbau auf kompromittierter Umgebung (und letztem Backup) dank forensischer Expertise und Erfahrung aus hunderten von Sicherheitsvorfällen
- Geschädigte und Versicherungen schätzen die **schnelle Wiederherstellung** und damit **Reduzierung des Business-Impacts**
- Professionelle Incident Response macht den **Kunden sicherer**

Wie kann ich Risiken minimieren?

Es braucht eine umfassende Sicherheit

Der IKT-Minimalstandard ist aus dem NIST Cyber Security Framewok entstanden.

Ein Angriff ist unausweichlich, nebst der Prävention sind die Erkennung und Reaktion im Sicherheitsdispositiv zentral.



Es müssen alle IKT-Minimalstandard Disziplinen adressiert werden:

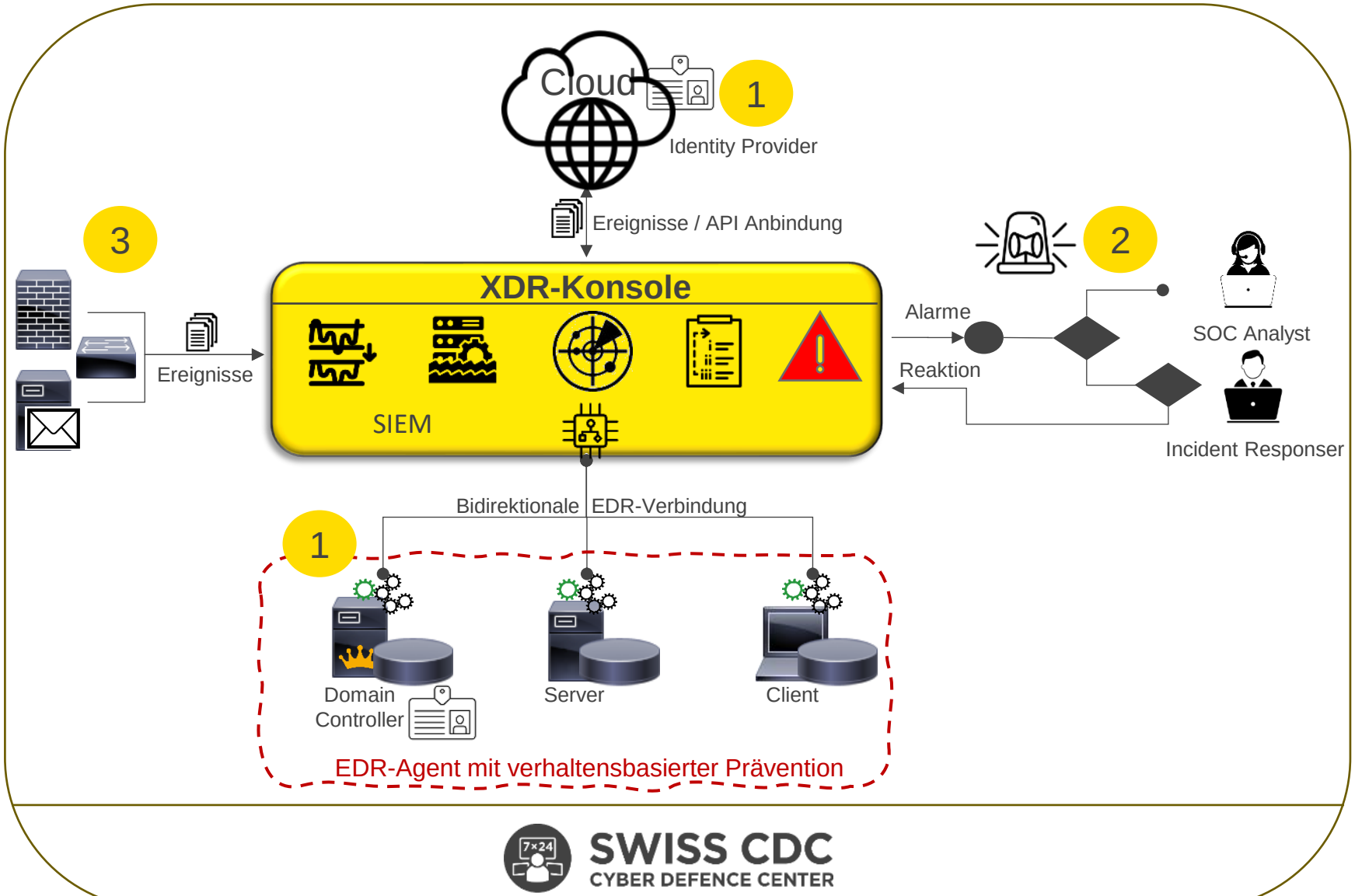
- **Identifizieren** – Sie müssen wissen, was besonders schützenswert ist und die Gefahren aus dem Internet kennen.
- **Schützen** – Zum Grundschutz gehört heute, nebst regelmässigen Software-Update und Multi-Faktor-Authentisierung, ein verhaltensbasierter Antivirus Schutz dazu.
- **Erkennen** – Ein Angriff muss durch eine digitale Alarmanlage erkannt werden.
- **Reagieren** – Bei einem Angriff muss effektiv und effizient reagiert werden, um den Angriff sofort zu stoppen.
- **Wiederherstellen** – Nach einem Geschäftsausfall muss die Wertschöpfung, so schnell wie möglich, wieder hergestellt werden.

Die Resilienz lässt sich mit einem SOC erheblich steigern.

InfoGuard empfiehlt bei der Implementierung folgende Reihenfolge.

Schützen, Erkennen und Reagieren

1. Herstellung der Prävention und Visibilität – Systeme und Identitäten
2. 7x24 Handlungsfähigkeit erlangen mit integriertem CSIRT / Incident Response
3. Visibilität erweitern mit SIEM & NDR Fähigkeiten



«SOC-Resilienz reduziert die Versicherungsrisiken»

24/7
Swiss CDC
Cyber Defence
Center

80+
Experten im
CDC & CSIRT

300+
CDC- & CSIRT-
Kunden

2012
Erfahrung & SOC-
Kompetenz

ISO 27001
ISO 14001
ISAE 3000 Typ2

CSIRT
Computer Security
Incident Response Team
FIRST-Mitglied und BSI-qualifizierter
APT-Response-Dienstleister

Kein MDR-Kunde mit substanziellem Business Impact seit 2015!

Securing Your Digital World – Today and Beyond

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz
T +41 41 749 19 00

info@infoguard.ch
www.infoguard.ch

Ernesto Hartmann, Chief Cyber Defence Officer
ernesto.hartmann@infoguard.ch
T direkt +41 41 749 19 53