Securing Your Digital World

InfoGuard
SWISS CYBER SECURITY

360° Cyber Security

Cyber Defence
Incident Response
Managed Security & Network
Penetration Testing & Red Teaming
Security Consulting

Cyber-Angriffe verhindern, erkennen und abwehren

Thomas Meier, CEO InfoGuard AG

Warum Cyber Security wichtig ist

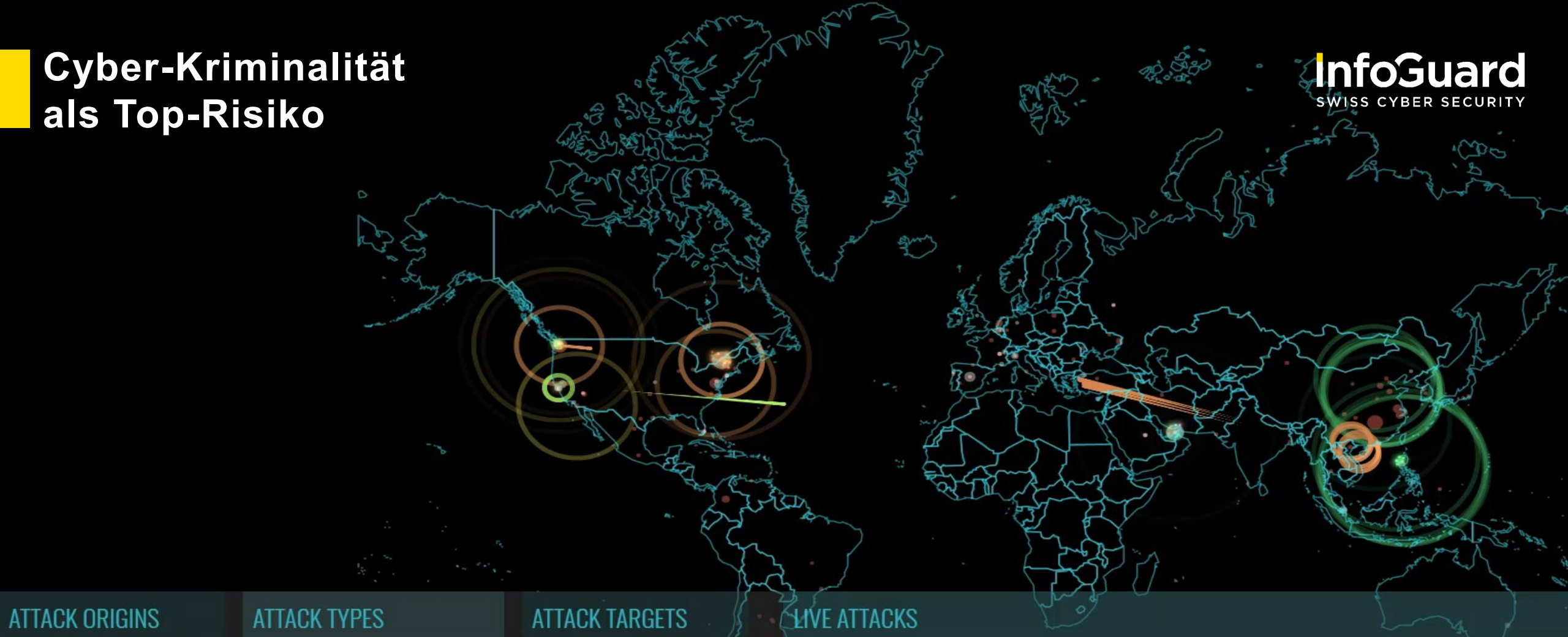
Digitalisierung

Compliance

Risiko

Cyber-Kriminalität als Top-Risiko

InfoGuard
SWISS CYBER SECURITY



ATTACK ORIGINS

#	COUNTRY
237	China
233	United States
19	Colombia
18	Netherlands
16	Ukraine
10	South Korea
8	Switzerland
7	Turkey
7	Poland

ATTACK TYPES

#	PORT	SERVICE TYPE
183	25	unknown
134	8080	unknown
110	23	telnet
26	3389	unknown
20	3306	unknown
17	445	unknown
16	5900	unknown
12	50864	unknown
11	53413	unknown

ATTACK TARGETS

#	COUNTRY
315	United States
172	United Arab Emirates
52	Spain
21	Singapore
14	Italy
11	Philippines
8	France
6	Belgium
5	Australia

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	AT
12:12:32.557	Vietnam Post And Telecom Corporation	14.162.143.153	Hanoi, VN	Aix-En-Provenc...	te
12:12:32.556	Vietnam Post And Telecom Corporation	14.162.143.153	Hanoi, VN	Aix-En-Provenc...	te
12:12:32.556	Vietnam Post And Telecom Corporation	14.162.143.153	Hanoi, VN	Aix-En-Provenc...	te
12:12:32.556	Vietnam Post And Telecom Corporation	14.162.143.153	Hanoi, VN	Aix-En-Provenc...	te
12:12:32.022	Microsoft Corporation	157.56.111.253	Redmond, US	De Kalb Junctio...	un
12:12:31.542	Microsoft Corporation	65.55.169.246	Washington, US	De Kalb Junctio...	un
12:12:31.540	Carinet Inc.	209.126.136.2	San Diego, US	Lynnwood, US	un
12:12:31.539	China Unicom Hebei Province Network	110.228.126.108	Shijiazhuang, CN	Nama, PH	un
12:12:31.539	China Unicom Hebei Province Network	110.228.126.108	Shijiazhuang, CN	Nama, PH	un

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

Luzerner Zeitung

Nach Cyberattacke bei CPH-Gruppe: Papiermaschinen stehen still

Es bleibt unklar, was genau in der Nacht auf den 7. Januar am Hauptsitz der börsenkotierten CPH-Gruppe in Perlen passiert ist.

10.01.2022

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

Luzerner Zeitung

Cyber-Attacke: Comparis wird von Hackern erpresst

Der grösste Vergleichsdienst der Schweiz ist Opfer einer Attacke von kriminellen Cyber-Hackern geworden. Lösegeld will das Unternehmen keines

08.07.2021

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

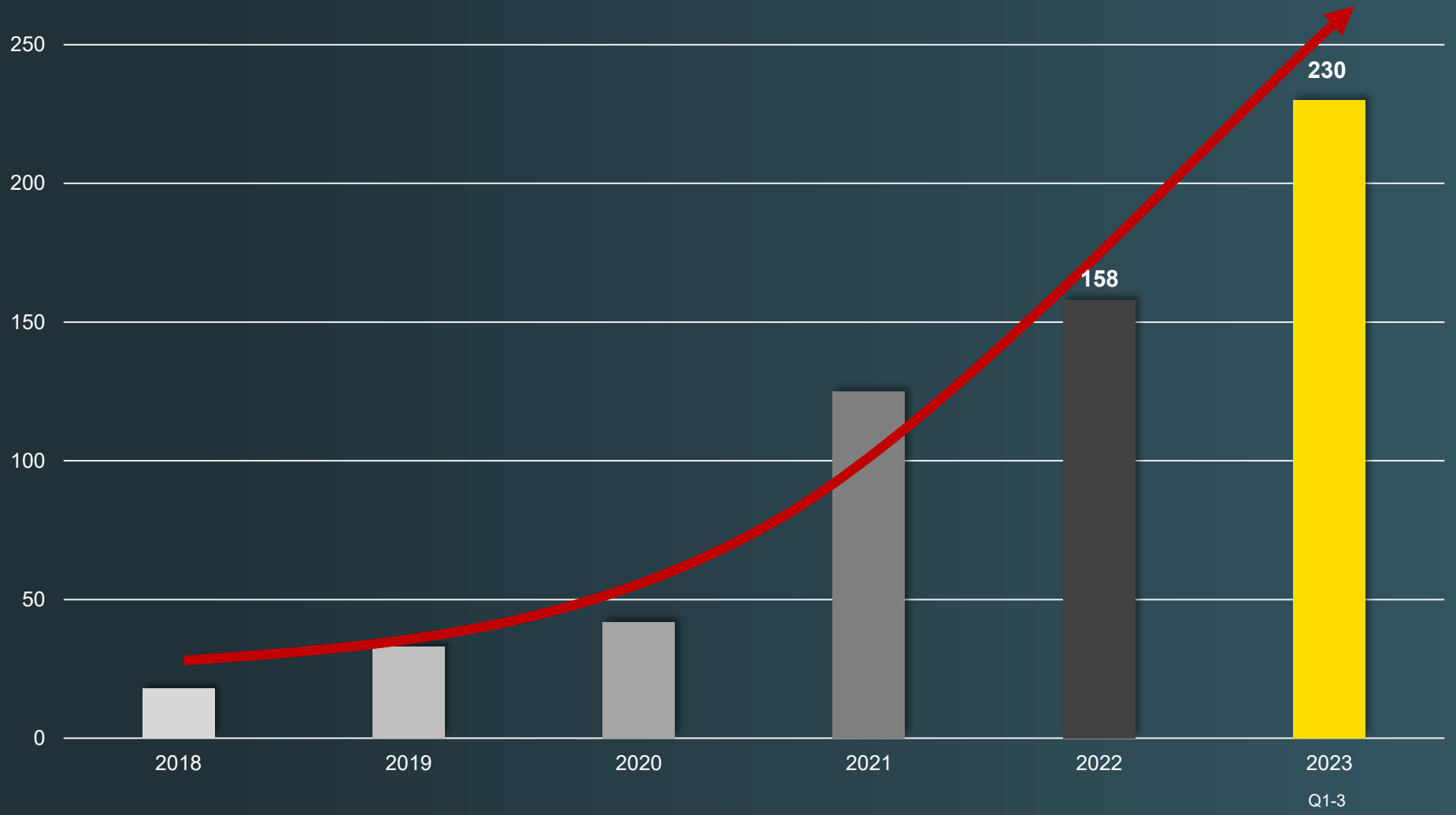
Inside IT

Ransomware-Angriff auf die Brugg Group betrifft weltweite ...

September 2020, wurde bei der Brugg Group eine Cyberattacke festgestellt. Dabei hätten die Täter vereinzelt Daten auf einigen IT-Systemen...

17.09.2020

Bedrohungslage – Bearbeitete Sicherheitsfälle durch InfoGuard



Aufgrund unserer hohen Fallzahlen sammeln wir täglich neue Informationen über die Bedrohungslage.

Business-Modell Cyber-Kriminalität

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.***.**		Lucerne	OS: Win2008/7	Admin: No					

Angriff und Erpressung

InfoGuard
SWISS CYBER SECURITY

Angriffsvektoren

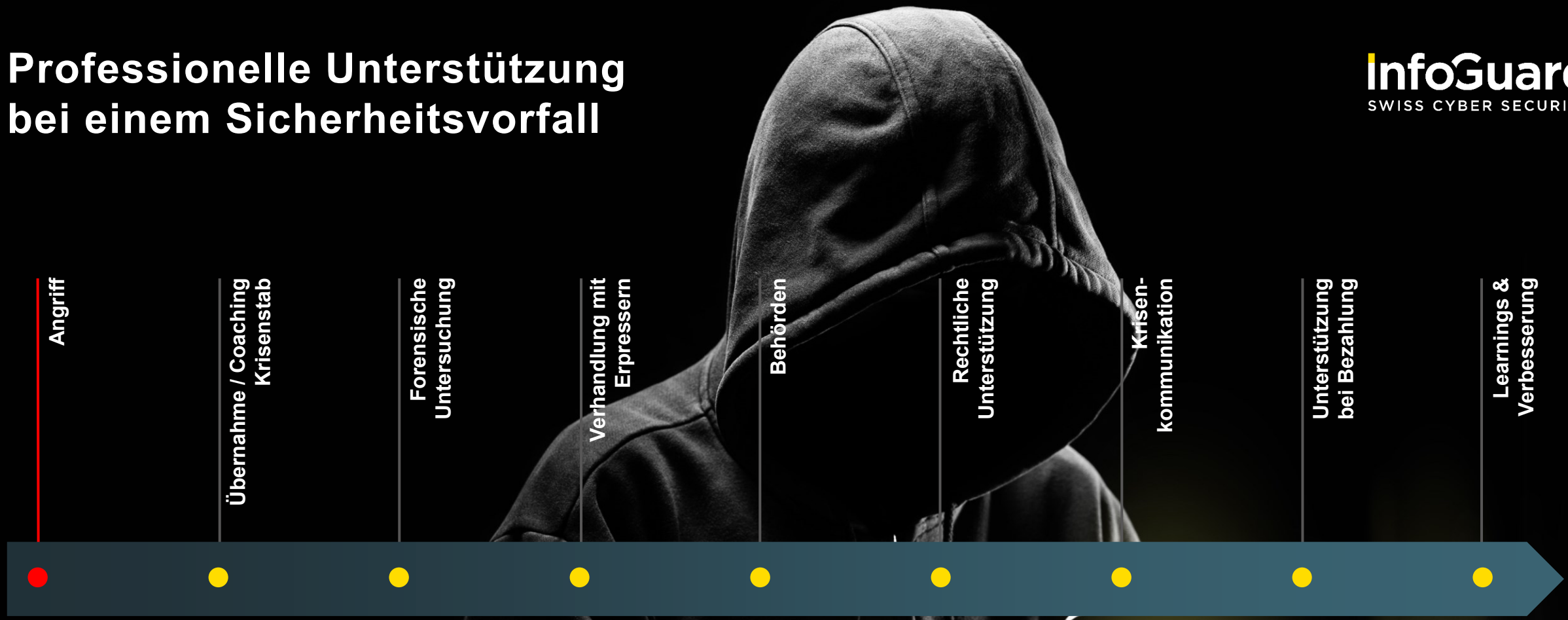
- Phishing
- Fehlende 2-Faktor-Authentisierung
- Schwachstelle am Perimeter

Strategie der Angreifer

- Verschlüsselte Daten
- Veröffentlichung sensibler Daten
- Information an Kunden und Partner
- Analyse der Daten und gezieltes Blaming

Professionelle Unterstützung bei einem Sicherheitsvorfall

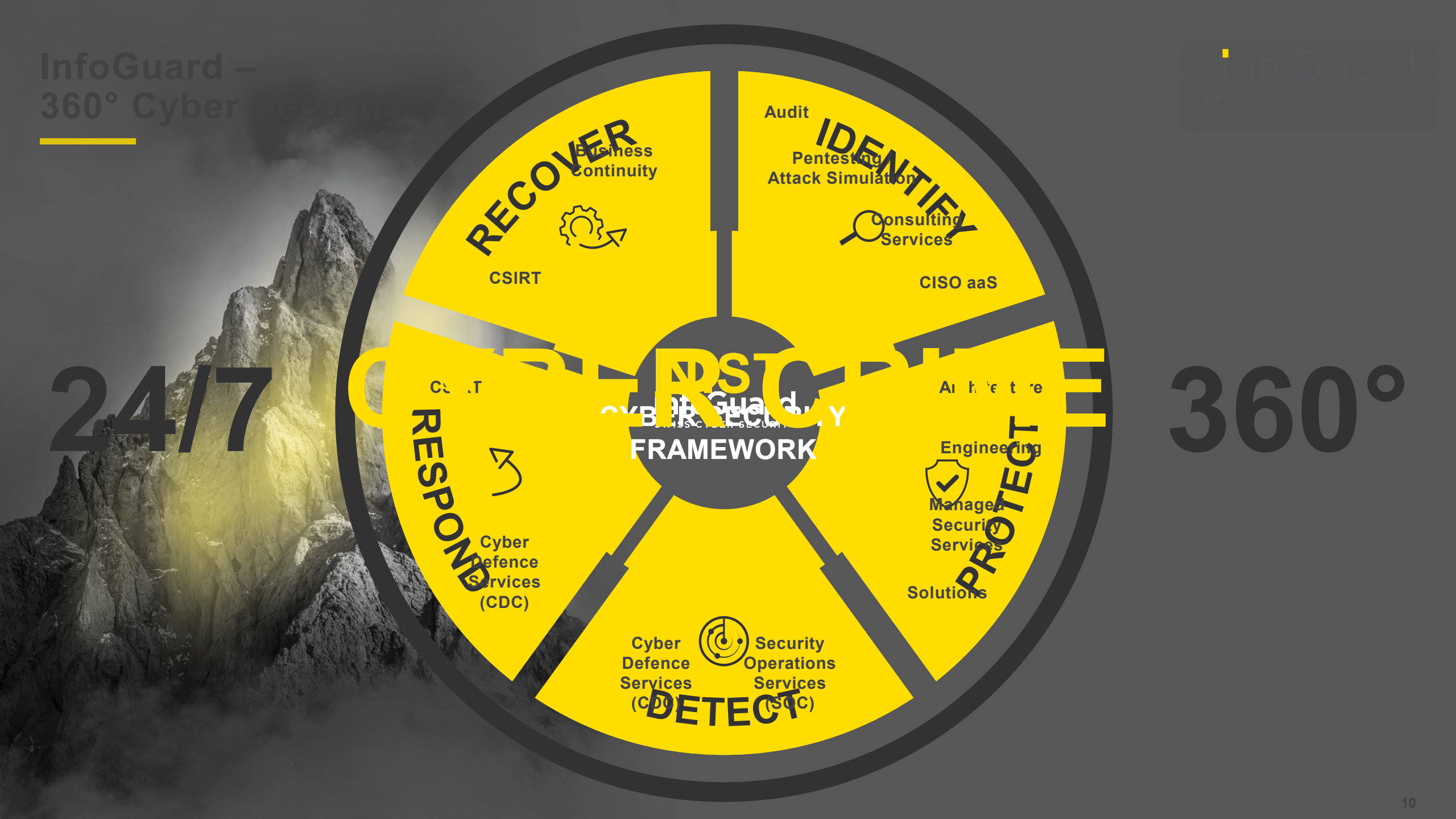
InfoGuard
SWISS CYBER SECURITY



InfoGuard CSIRT

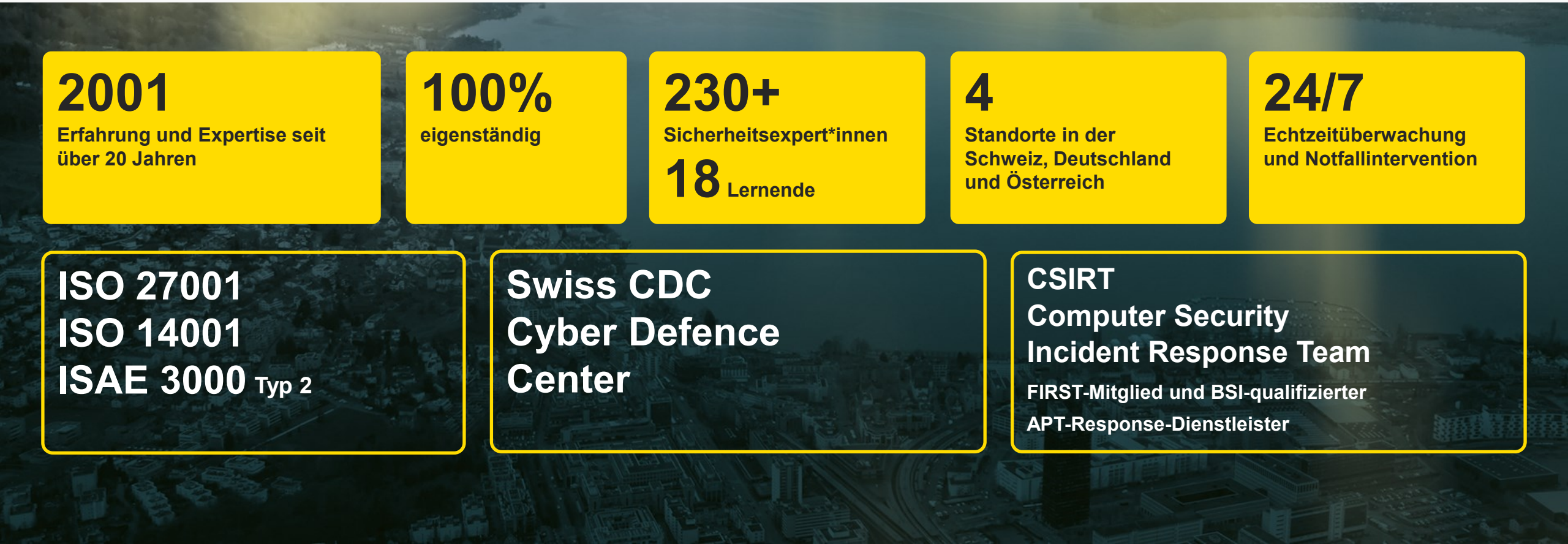
Gesicherter Wiederanlauf / Aufbau

InfoGuard – 360° Cyber Security



Cyber Security ist unsere Leidenschaft

InfoGuard
SWISS CYBER SECURITY



2001
Erfahrung und Expertise seit über 20 Jahren

100%
eigenständig

230+
Sicherheitsexpert*innen

18 Lernende

4
Standorte in der Schweiz, Deutschland und Österreich

24/7
Echtzeitüberwachung und Notfallintervention

ISO 27001
ISO 14001
ISAE 3000 Typ 2

Swiss CDC
Cyber Defence Center

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


InfoGuard
CYBER
DEFENCE
CENTER
SUMMARY DASHBOARD
DUTY INFORMATION
ONBOARDING
SECURITY OFFENSES
37
12
1

Vertrauen in unsere Expertise

400+ Kunden in der Schweiz


InfoGuard
SWISS CYBER SECURITY
Gerne beantworte
ich Ihre Fragen


InfoGuard
SWISS CYBER SECURITY
Anhang

Bewährte organisatorische Massnahmen

InfoGuard
SWISS CYBER SECURITY

Cyber-Angriffe verhindern oder die Auswirkungen der Angriffe eindämmen.

1

Etablieren Sie eine Sicherheitsorganisation (**CISO-Rolle**).

2

Stellen Sie sicher, dass das **Krisenmanagement** im Falle einer Krise **funktionsfähig** ist. Erstellen Sie dazu Aufgabenlisten, Kontaktadressen der wichtigsten Entscheidungsträger und Hilfsmittel sowie ein **Kommunikationskonzept**.

3

Stellen Sie sicher, dass ein schneller **Notbetrieb möglich** ist. Dazu müssen Sie die **zeitkritischen Prozesse kennen** und ggf. Workarounds definieren.

4

Überprüfen Sie regelmässig Ihre Pläne, Abläufe, Hilfsmittel und verantwortlichen Personen, bspw. mit Table-Top-Übungen oder jährlichen Reviews.

Bewährte organisatorische Massnahmen

InfoGuard
SWISS CYBER SECURITY

Cyber-Angriffe verhindern oder die Auswirkungen der Angriffe eindämmen.

5

Schulen Sie Ihre Mitarbeitende regelmässig in Security-Awareness-Trainings.

6

Stellen Sie sicher, dass Sie Ihre **IT** möglichst **schnell wiederherstellen** können bspw. mit einem funktionierenden **Backup-Konzept** (Offline).

7

Ziehen Sie den Abschluss einer **Cyber-Versicherung** in Erwägung.

8

Richten Sie ein **Wallet für Kryptowährungen** ein.

Bewährte technische Massnahmen

InfoGuard
SWISS CYBER SECURITY

1

Erhöhung der **Detektions- und Reaktionsfähigkeiten** um Cyber-Angriffe zu erkennen oder die Auswirkungen der Angriffe einzudämmen.

2

Verwendung einer **Multi-Faktor-Authentisierung** (MFA) für alle externen Schnittstellen, beispielsweise Outlook Web Access.

3

Einsatz von **starken Passwörtern** (Komplexität und Minimum 12 Zeichen).

4

Einschränken und Kontrolle von **administrativen Schnittstellen** und Einschränken von Benutzerprivilegien**.**

Bewährte technische Massnahmen

InfoGuard
SWISS CYBER SECURITY

5

Einsatz von **E-Mail & Web-Proxy-Lösungen**, um den Download von Dateien wie .exe zu unterbinden.

6

Exponierte Dienste und Systeme regelmässig auf **Schwachstellen** überprüfen und zeitnah aktualisieren.

7

Umsetzung eines **DMZ-Konzeptes** mit einer **Trusted Zone** und **Netzwerk-segmentierung**.

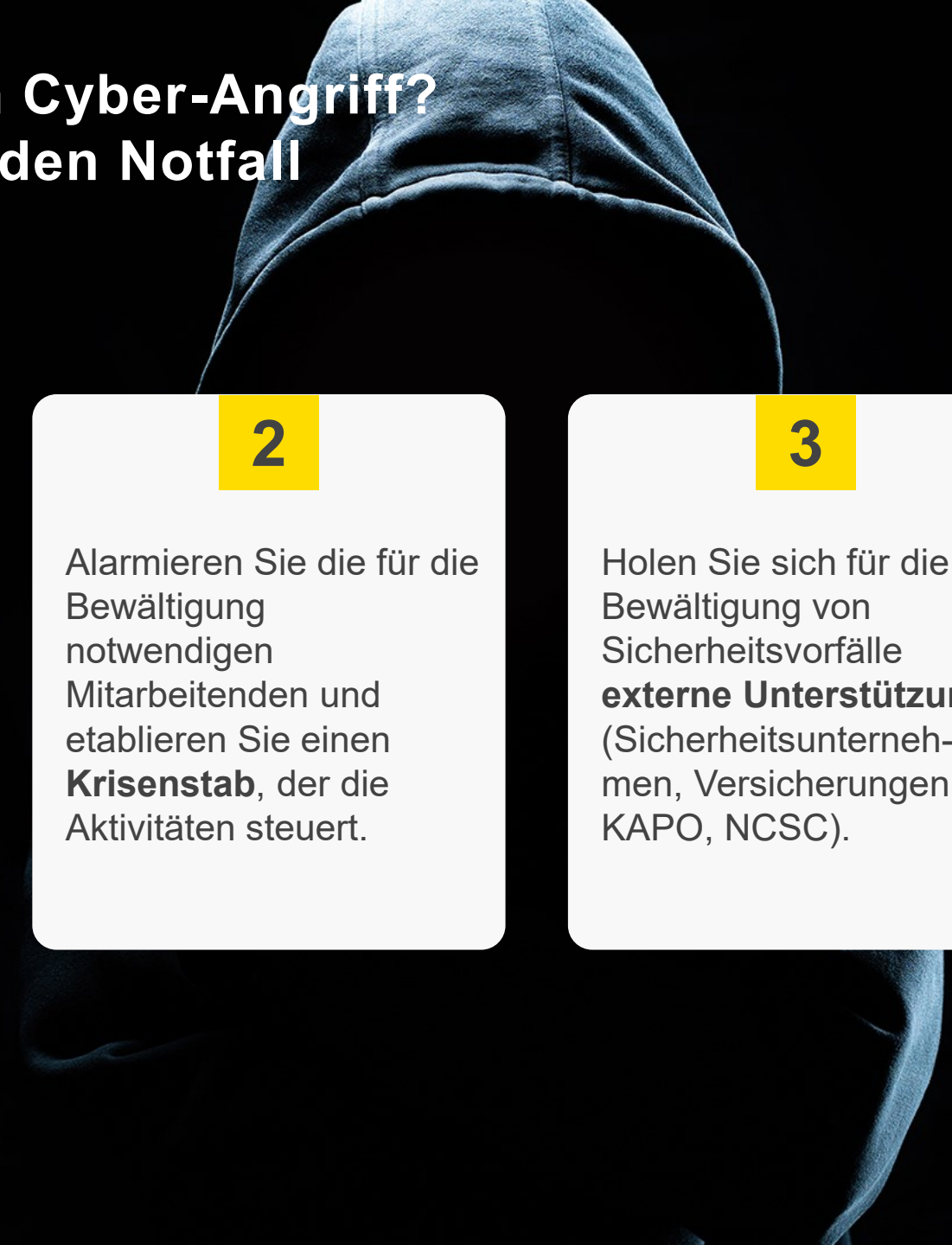
8

Verwendung und Umsetzung **verschlüsselter Protokollen** (FTP mit SFTP und HTTP mit HTTPS ersetzen) sowie unsichere Protokollversionen TLSv1 und SSLv3 unterbinden.

FTP: File Transfer Protocol, SFTP: Secure File Transfer Protocol, HTTP: Hypertext Transfer Protocol, HTTPS: Hypertext Transfer Protocol Secure, TLS Transport Layer Security, SSL: Secure Sockets Layer

Was tun bei einem Cyber-Angriff? 8-Punkte-Plan für den Notfall

InfoGuard
SWISS CYBER SECURITY



1

Bleiben Sie **ruhig** und gehen Sie **strukturiert** an die Lösung der Probleme.

2

Alarmieren Sie die für die Bewältigung notwendigen Mitarbeitenden und etablieren Sie einen **Krisenstab**, der die Aktivitäten steuert.

3

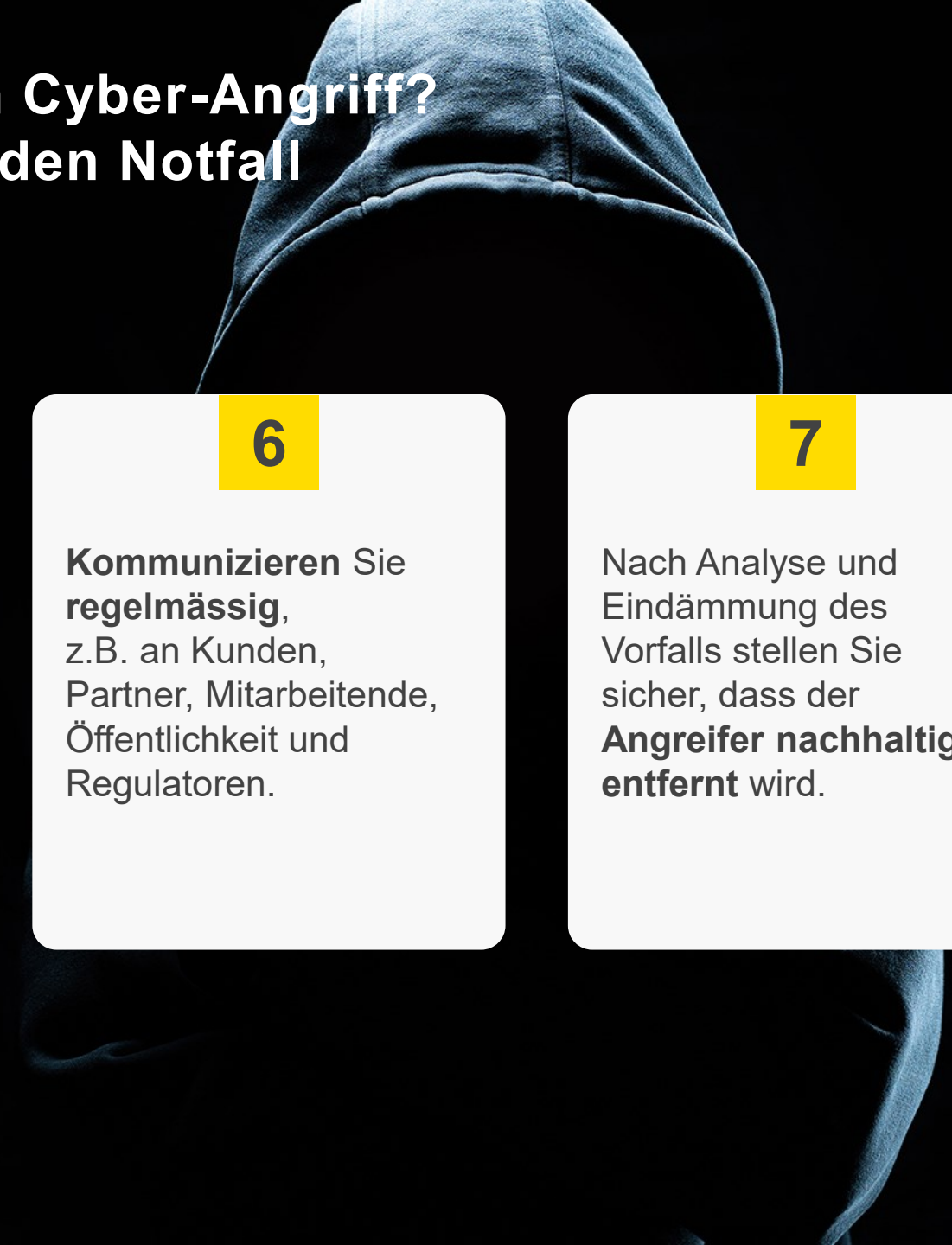
Holen Sie sich für die Bewältigung von Sicherheitsvorfälle **externe Unterstützung** (Sicherheitsunternehmen, Versicherungen, KAPO, NCSC).

4

Bestimmen Sie gemeinsam mit Experten, welche **Sofortmassnahmen** eingeleitet werden müssen.

Was tun bei einem Cyber-Angriff? 8-Punkte-Plan für den Notfall

InfoGuard
SWISS CYBER SECURITY



5

Sorgen Sie dafür, dass Ihre **wichtigsten Prozesse weiter-betrieben** werden können – manchmal sind diese auch ohne IT betreibbar (inklusive Zahlungsverkehr).

6

Kommunizieren Sie **regelmässig**, z.B. an Kunden, Partner, Mitarbeitende, Öffentlichkeit und Regulatoren.

7

Nach Analyse und Eindämmung des Vorfalls stellen Sie sicher, dass der **Angreifer nachhaltig entfernt** wird.

8

Bereinigen Sie Ihre IT-Systeme schrittweise und stellen Sie Ihre **Handlungsfähigkeit** wieder her.