

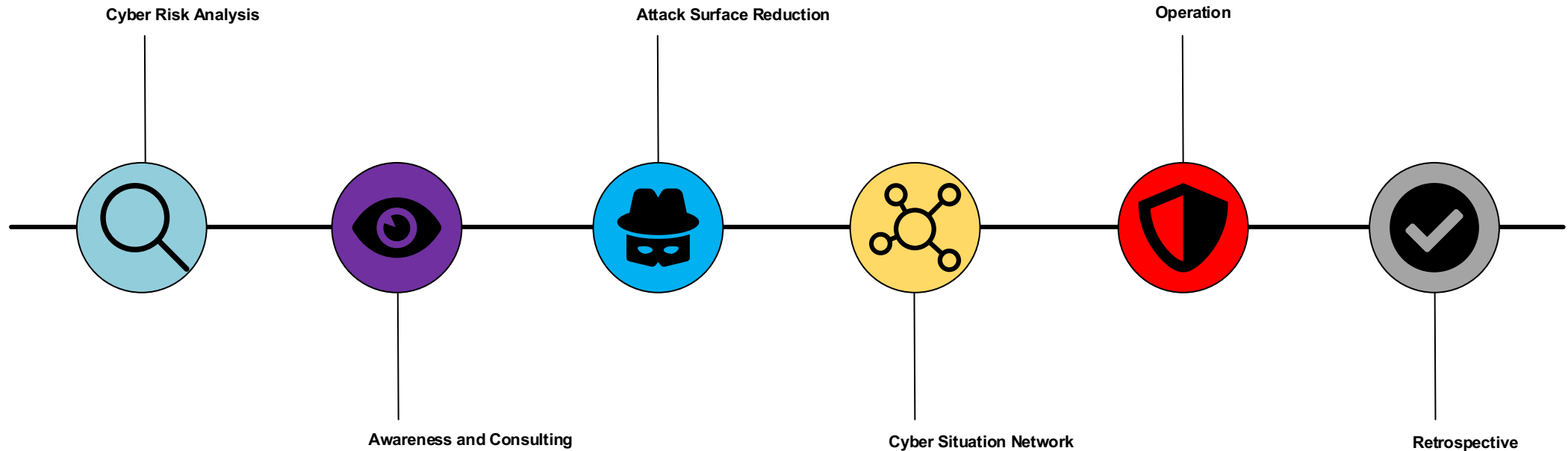
Absicherung von Grossveranstaltungen – wenn Digitales auf Physisches trifft



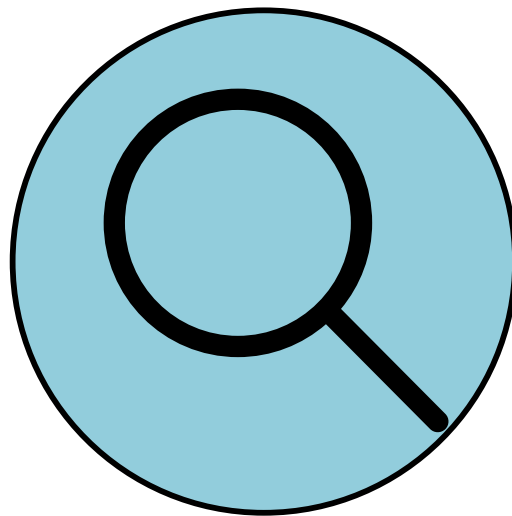


BACS Cyber Event Defence

Grundkonzept



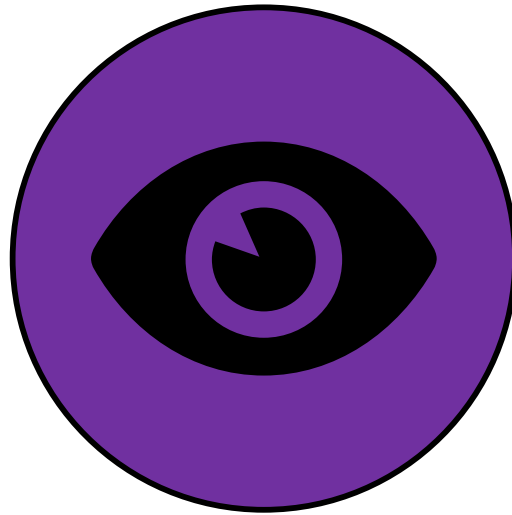
BACS Cyber Event Defence Cyber Risk Analysis



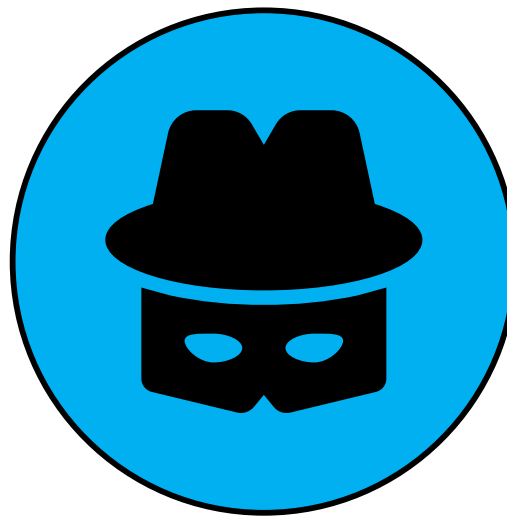


BACS Cyber Event Defence

Awareness und Consulting

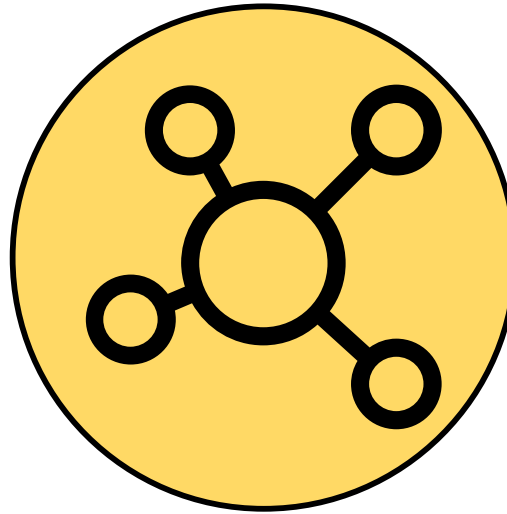


BACS Cyber Event Defence Attack Surface Reduction

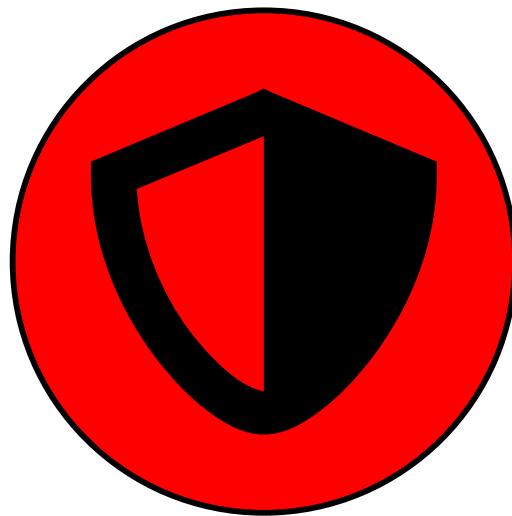




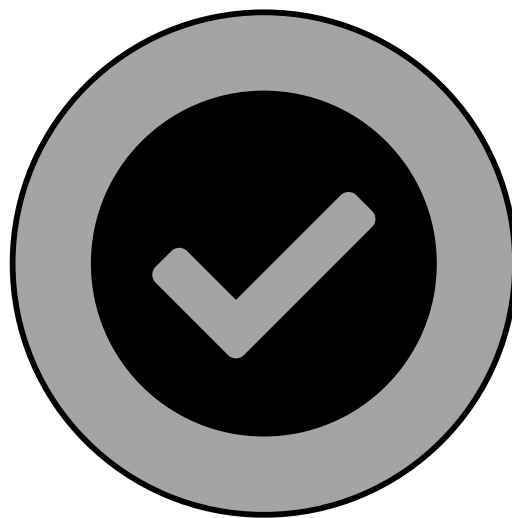
BACS Cyber Event Defence Cyber Situation Network



BACS Cyber Event Defence Operation



BACS Cyber Event Defence Retrospective



EURO ision

SONG CONTEST

BASEL 2025



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

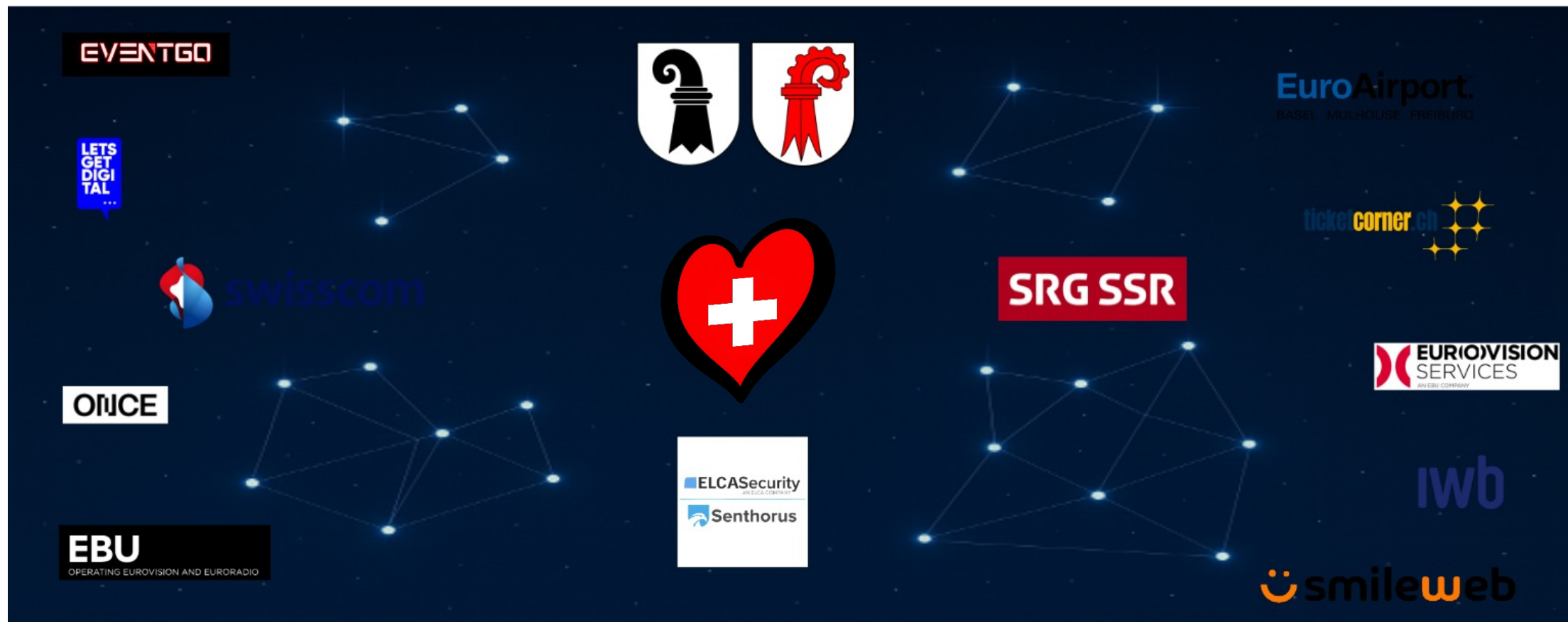
Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS





Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS





Main Venue





Public Viewing





Eurovision Village

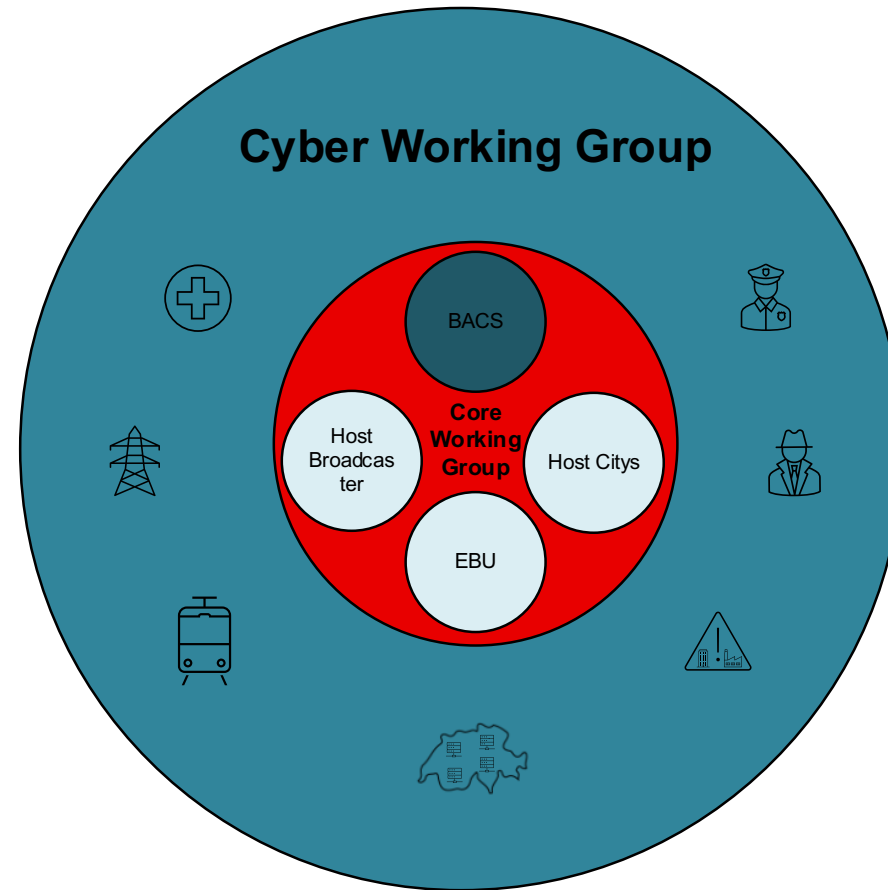




Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS



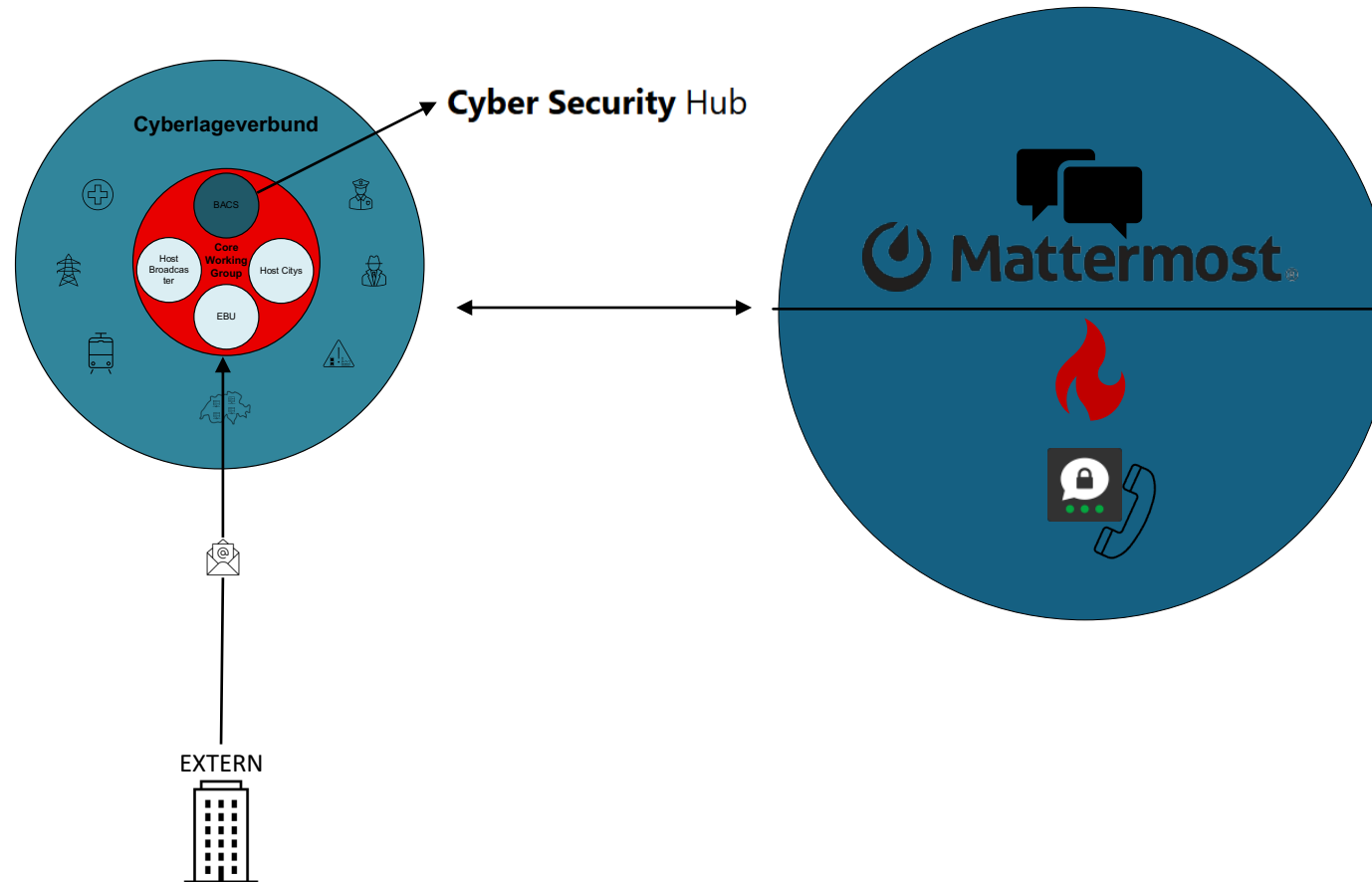
Cyber Task Force





Cyber Task Force

Communication





CWG Platforms

Channels

- Cyber Working Group (8 Members)
- Cyber Incidents (17 Members)
- Cybersec Teams (29 Members)
- Threat Intelligence Sharing (89 Members)



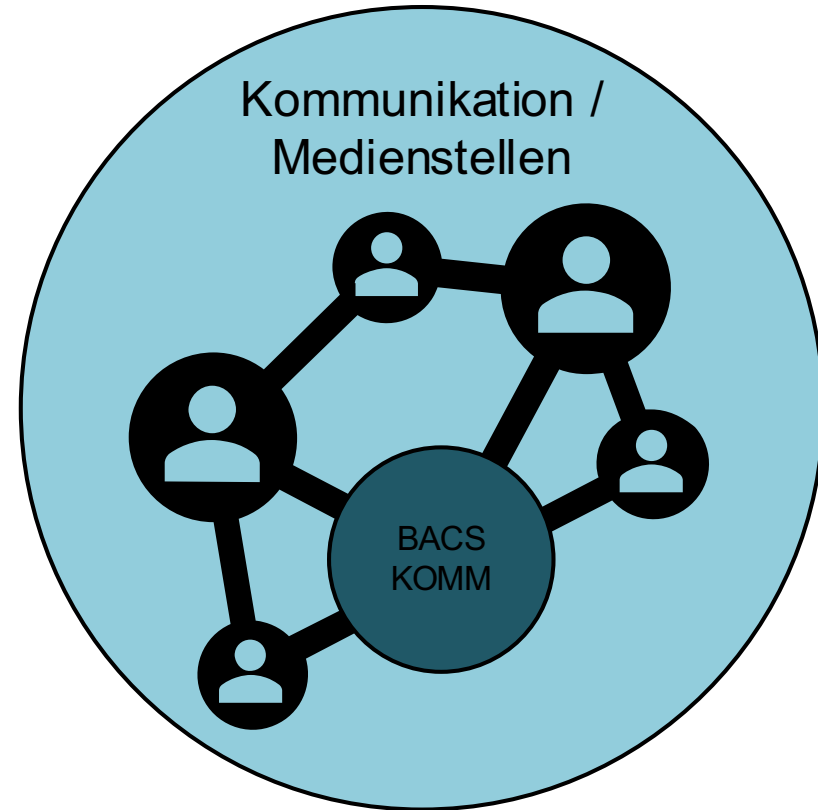
Incident Management Plattform

Communication / Media

Organisationsübergreifendes Netzwerk

Proaktive Kommunikation

Koordination von Krisenkommunikation

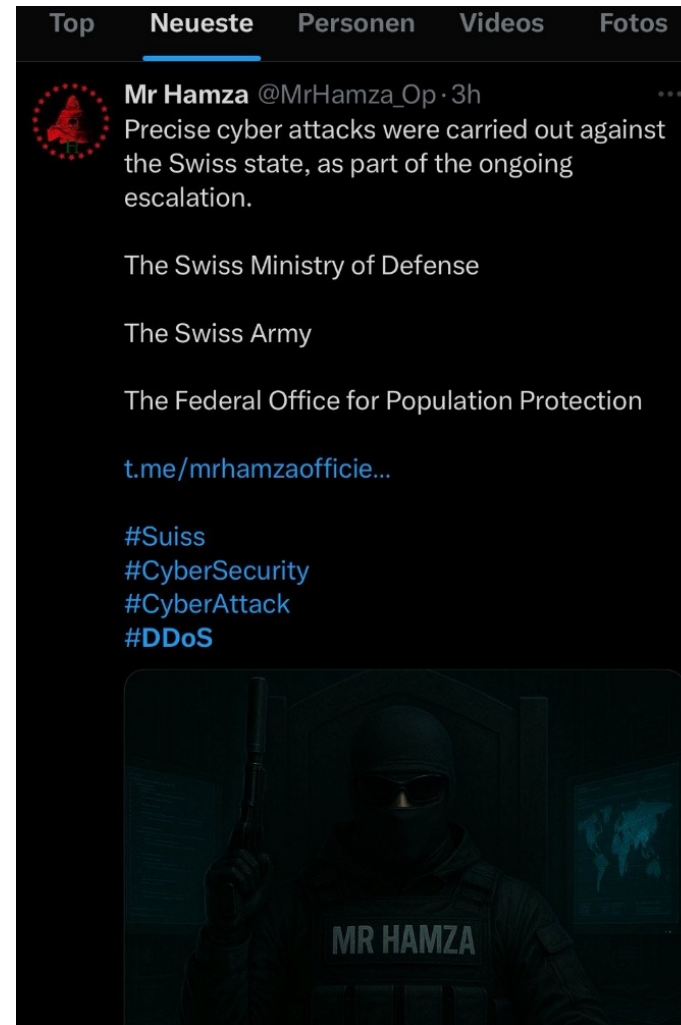




Incidents

Thursday, 8 May

130Gbit/s, 14 Mio pps





Incidents

Thursday, 15 May



JuanOlaSand | 🇹🇷 🇩🇪 🇫🇷 🇸🇪 🇦🇹 |

@JuanOlaSand



@YourAnonCentral Attack the Eurovision Song Contest televoting system, so Israel gets eliminated at semis and we avoid the artwashing of their genocide.



Incidents

Friday, 16 May



bluedeepsea 
@bluedeepse39827



WE NEED FIGHT BACK!!!! Hackers where are you! Do something! Put the photo of dead kid or this whore in IOF uniform next to that kid! They are mocking us! SABOTAGE FINALLE!!!! Destroy EBU! Criminal organizations supporting nazi and apartheid!



bluedeepsea 
@bluedeepse39827



[#Eurovision2025](#) [#Eurovision](#) [#eurovisiong](#)

Bring banners, bring Palestinian flags! Shout louder: Free Palestine! Be freaking RADICAL! That's NOT anymore song contest. EBU lied! Zionist slaves. Again fake applause! Don't you get it: israHell will again steal votes! Stop genocide!

2:06 AM · May 16, 2025 · **169** Views



Incidents

Friday, 16 May



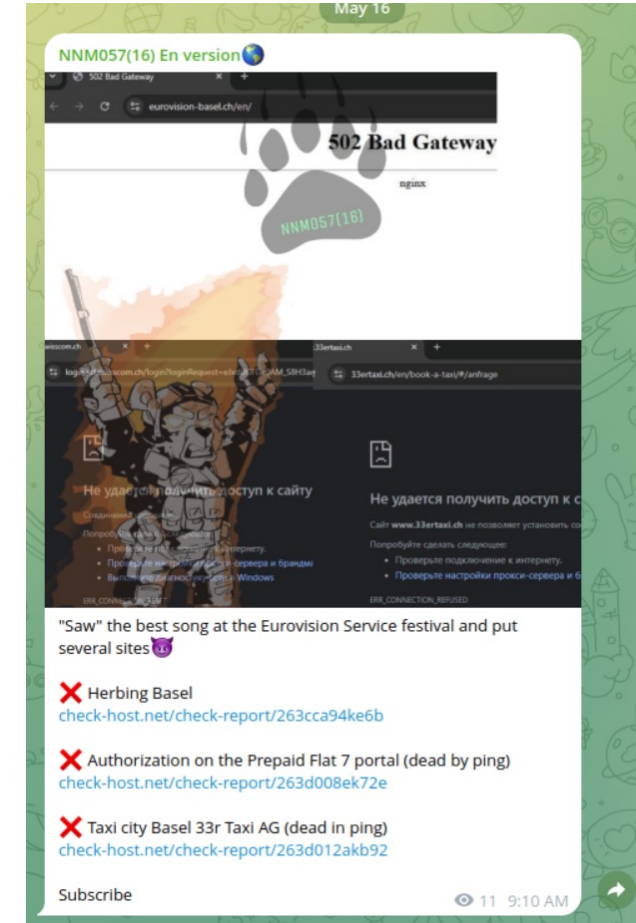
DDosia Targets Mo...

BOT 8:12

New Swiss Targets 🇨🇭 from DDosia Config:

Host	IP
www.bis.org	185.58.128.7
www.mini-cab.ch	193.108.137.49
www.bvb.ch	194.56.210.123

Host	IP
www.bis.org	185.58.128.7
www.mini-cab.ch	193.108.137.49
www.bvb.ch	194.56.210.123
www.blt.ch	94.230.213.53
eurovision-basel.ch	84.17.46.54
www.33ertaxi.ch	193.108.137.49
login.scl.swisscom.ch	195.186.211.241
www.taxi-zentrale.ch	193.108.137.49
www.swisscom.ch	195.186.208.154





NoName



GovCERT.ch Cyber Threat Intelligence

In this directory we post technical cyber threat intelligence and provide it as is under TLP:CLEAR.

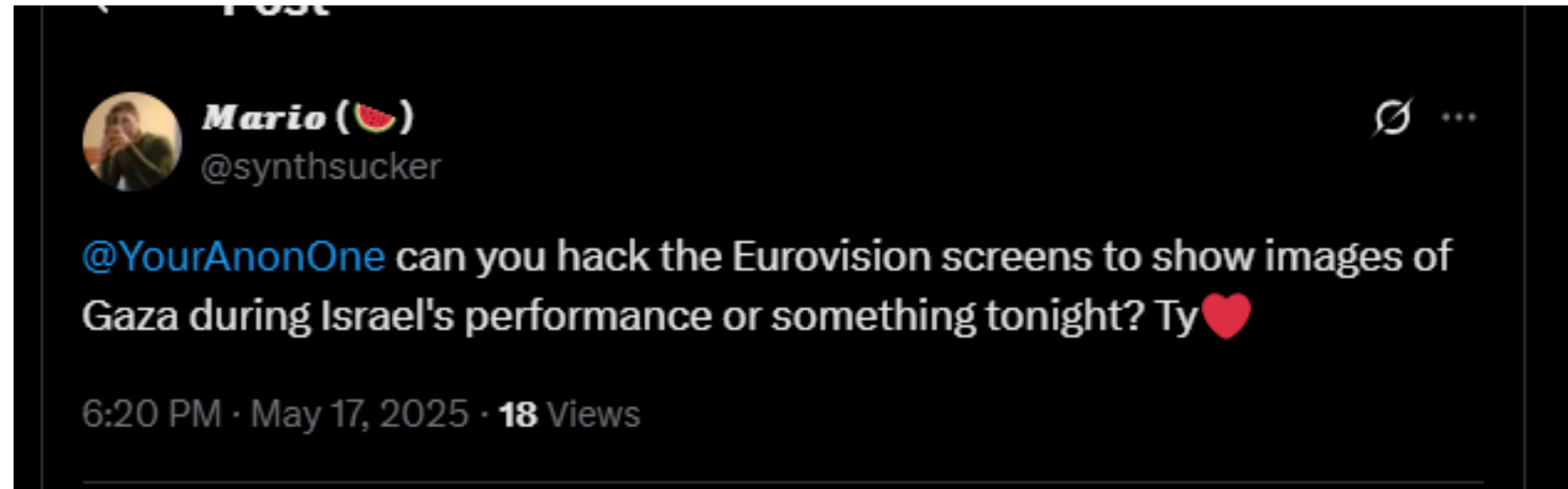
Table of Contents

- [OffensiveCIDs/Bruteforce.csv](#): Contains top CIDs (/24) involved in bruteforce attacks against O365 and edge devices (such as SSL-VPNs). You may not expect any legitimate traffic from these sources towards any internal resources.
- [OffensiveCIDs/Bruteforce_CIDR-only](#): This list contains the same data as [OffensiveCIDs/Bruteforce.csv](#) but just the CIDs (no additional information such as ASN or geo location). You may want to use this list in an automated manner for mitigating bruteforce attacks against O365 and edge devices (such as SSL-VPNs).
- [20250120_NoName057-DDoS-CH_CIDR-with-info.csv](#): Contains top CIDs (/24) that participated in DDoS attacks in the week of 2025-01-20 (week #4) against Swiss targets. These attacks were allegedly conducted by hacktivist group NoName057(16), using L7 attacks (HTTP/s GET flood). GovCERT.ch has contacted the abuse desks of the relevant network owners (AS) and asked them to take the appropriate actions to prevent further abuse of their service.
- [20250120_NoName057-DDoS-CH_CIDR-only.csv](#): This list contains the same data as [20250120_NoName057-DDoS-CH_CIDR-with-info.csv](#) but just the CIDs (no additional information such as ASN or geo location). You may want to use this list in an automated manner for temporarily blocking and mitigating NoName057(16) L7 DDoS attacks. Please consider that blocking CIDs will probably cause false positives. We therefore recommend



Incidents

Saturday, 17 May





Incidents

Saturday, 17 May

Events summary

[Learn more](#)

Action Host Country Source ASN Source IP Path ...

Total

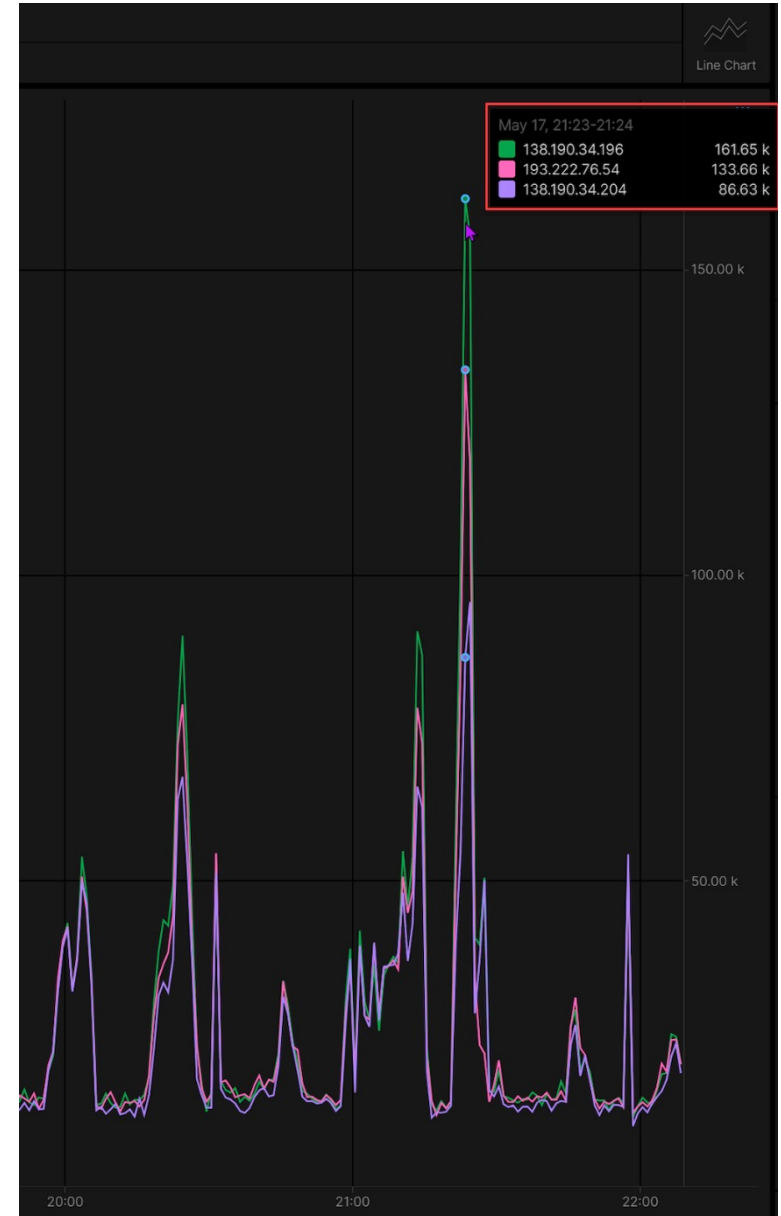
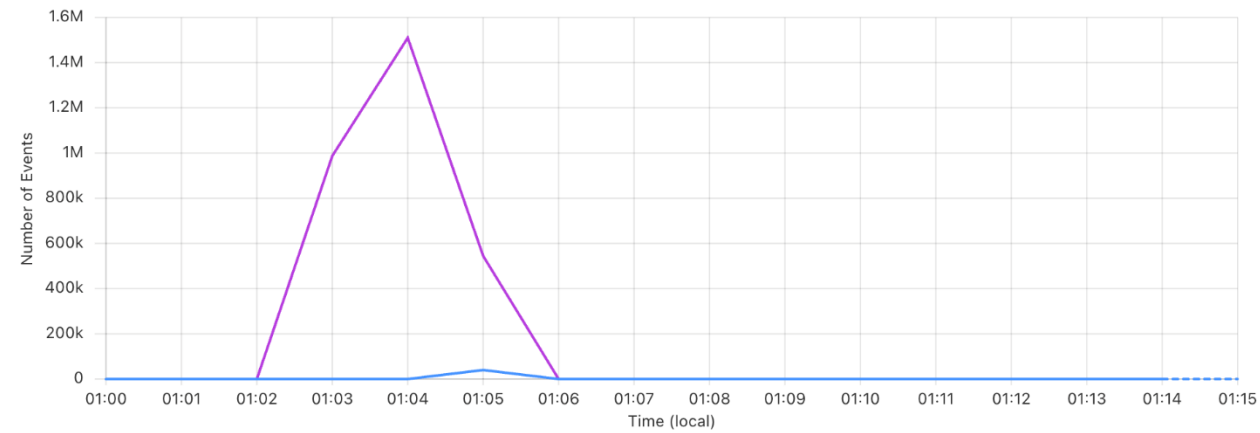
3.08M

Managed Challenge

3.04M

Block

39.94k



Ziele der SRG:

- Ein europäischer Song Contest für alle bedeutet auch Sicherheit für alle.
- Cybersicherheit ist für das Management, die Teilnehmer und das Publikum gleichermaßen von entscheidender Bedeutung.
- Der Schutz von Systemen, Daten und Menschen ist das Herzstück einer sicheren und inklusiven ESC. Deshalb war eine starke Sicherheitspartnerschaft unerlässlich.

Warum cybersicherheit? → Fakten / Hintergrund / Historie:

- 2019 Tel Aviv – KAN Online-Übertragung auf Meldungen von Aktivisten umgeschaltet
- 2021 Rotterdam – Streaming server gehackt
- 2024 Malmö – Streaming- und Webserver durch Cyberangriffe gestört (DDoS)

Unsere Mission:

Schutz des ESC aus Sicht der Cybersicherheit, einschliesslich:

- Menschen
- die Veranstaltung
- der Ruf der Schweiz



Das perfide Bündnis zwischen staatlichen Akteuren und Cyberkriminalität

DATENDIEBSTAHL

BLOCKIERUNG

SABOTAGE

MISSBRAUCH



MULTIPLIKATOR-
EFFEKT



CHAOS!

Komplexität und geteilte Verantwortung

ORGANISATOREN DER VERANSTALTUNG

MITARBEITER

BEHÖRDEN

LIEFERANTEN



IT / CYBERSICHERHEIT INDUSTRIE

Globaler Ansatz



NACHRICHTEN

INTELLIGENCE
EARLY DETECTION
Securing Systems
Hybrid Critical Systems

SECURING
CRITICAL SYSTEMS
Hybrid Resilience Plan

TESTS & QUALITÄT

HYBRIDE RESILIENZ

SIABBRATION
CRIT RESILIENCE PLAN

BÜNDELUNG & ZUSAMMENARBEIT

Schlüssel Erfolgsfaktor: *ESC2025 SANCTUARY*



THE ONION PRINCIPLE

FOCUS ON CRITICAL ASSETS

SIMPLE SETUP

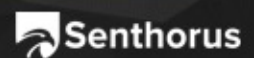


EUROVISION 2024

Voting system

1	SWITZERLAND	541	16	PORTUGAL	152	18	UNITED KINGDOM	46
2	CROATIA	547	11	GREECE	125	19	FINLAND	28
3	UKRAINE	409	12	GERMANY	112	20	ESTONIA	37
4	FRANCE	400	13	GEORGIA	84	21	SPAIN	30
5	ISRAEL	350	14	CYPRUS	71	22	SLOVENIA	27
6	IRELAND	274	15	LATVIA	64	23	AUSTRIA	24
7	ITALY	264	17	BERBEL	54	24	NORWAY	16
8	ARMENIA	183	18					
9	SWEDEN	174						

EUROVISION WORLD



Highlights und Kennzahlen

71 erkannte Risiken → 7 Kategorien

Training: 4 Tabletop cybersec Übungen

Rythmus: 6 Monate → Live

20+ Lieferanten bewertet

50+ Threat Intelligence & SM reports

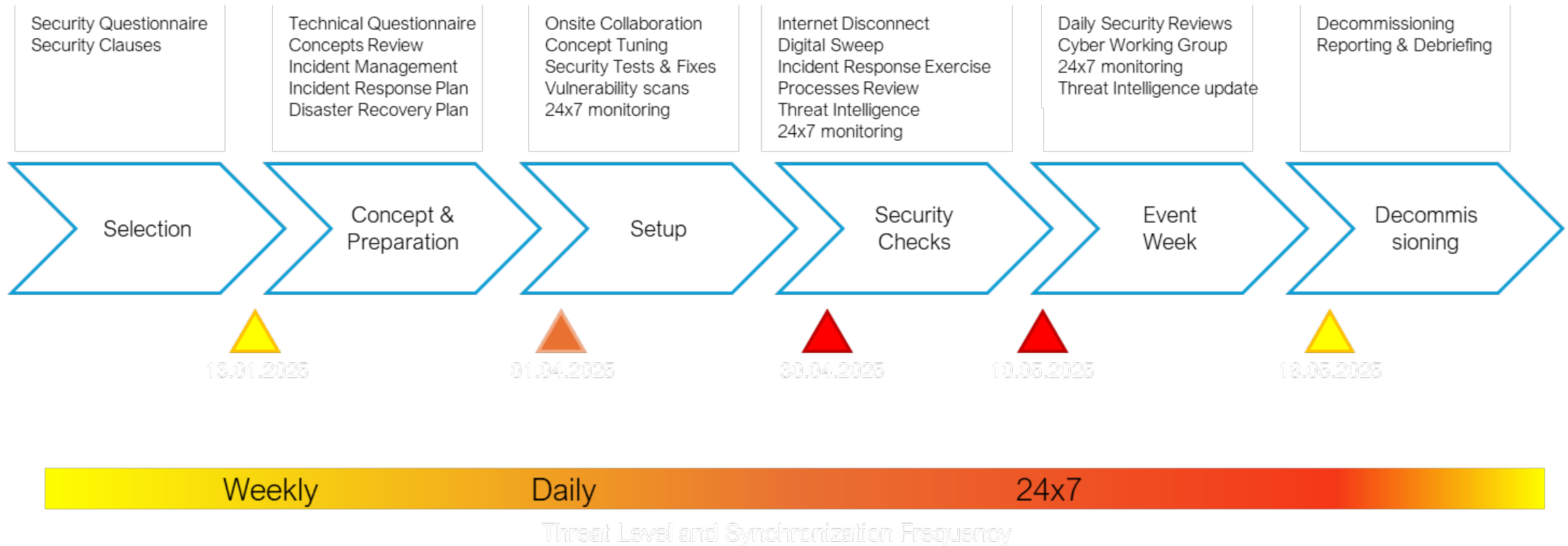
30+ tägliche «assets discoveries»

Echtzeit-Takedowns während 2 Wochen

Digital Sweeps



Zeitmanagement



Vom Risikomanagement zur Realität

DDoS

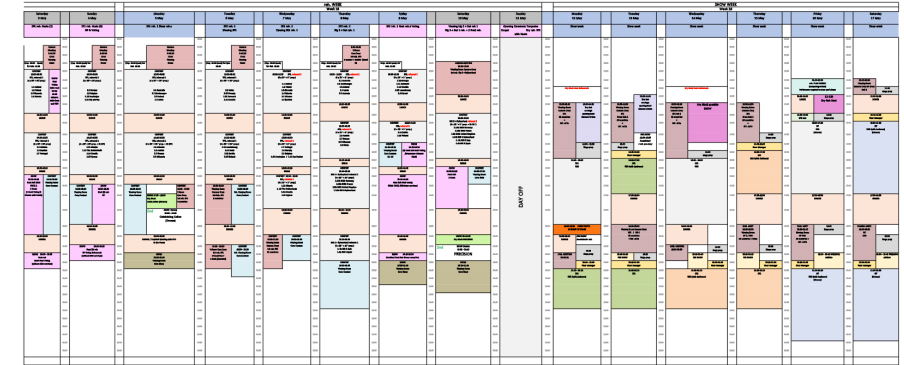
Unbefugter Videostream in sozialen Medien

Phishing-/Betrugskampagnen

Desinformationskampagnen

Erpressung und Bombendrohungen

Aktivismus Handlungsaufwurf



Wichtigste Erkenntnisse



KOMPLEXE ZIELE

DEMOKRATISCHES HERZ

ECHTE AUSWIRKUNGEN

ANTICIPATION

SICHERHEITSKETTE

ZUSAMMENARBEIT





Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS



THE WINNER IS...

