



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

 **ELCAsSecurity**
AN ELCA COMPANY

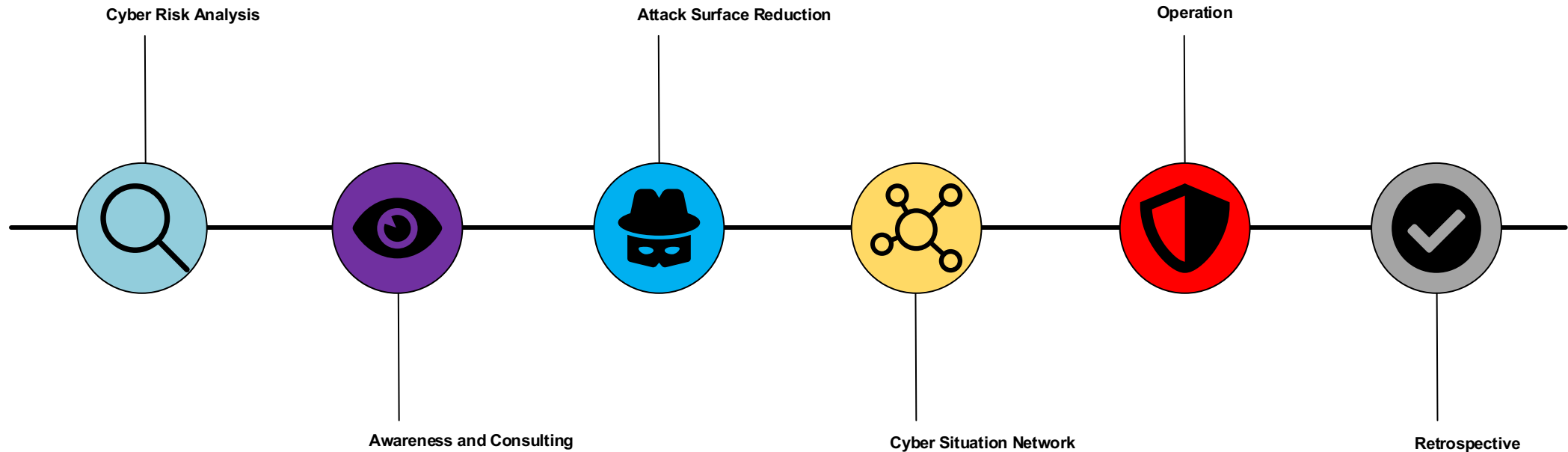
Sécurisation des événements majeurs – quand le numérique rencontre le physique





OFCS Cyber Event Defence

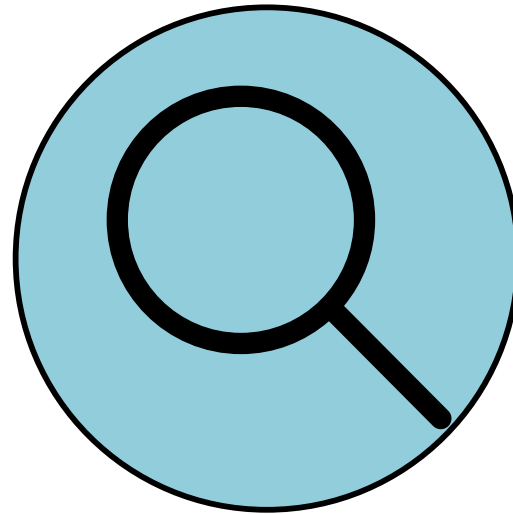
Concept de base



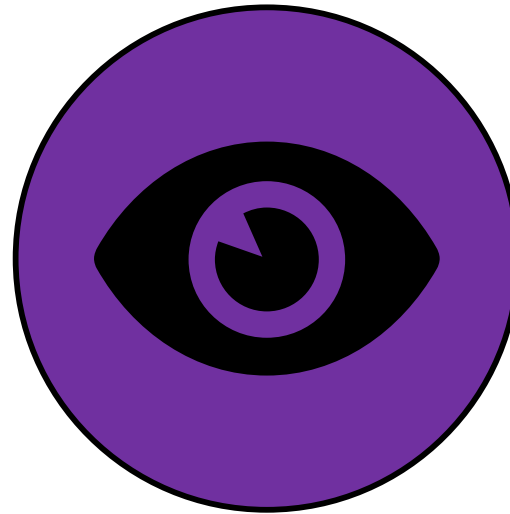


OFCS Cyber Event Defence

Cyber Risk Analysis



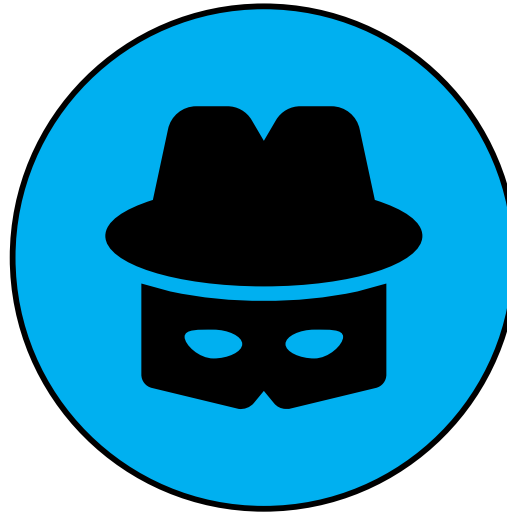
 **OFCS Cyber Event Defence**
Sensibilisation et conseil



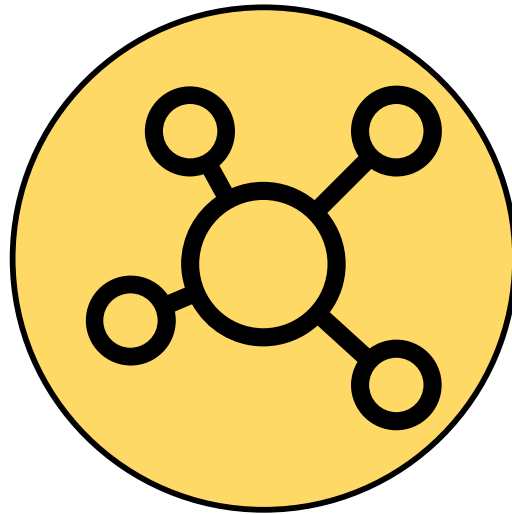


OFCS Cyber Event Defence

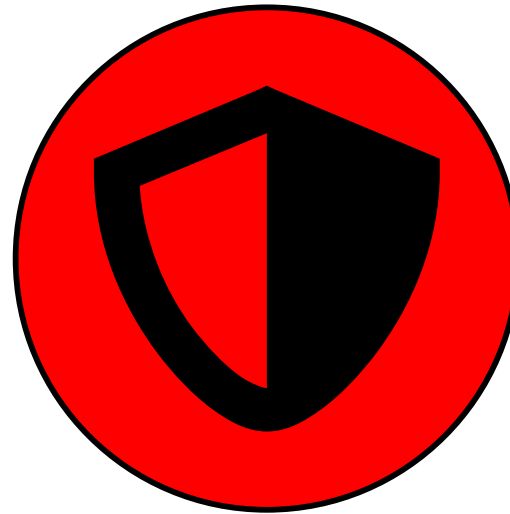
Réduction de la surface d'attaque



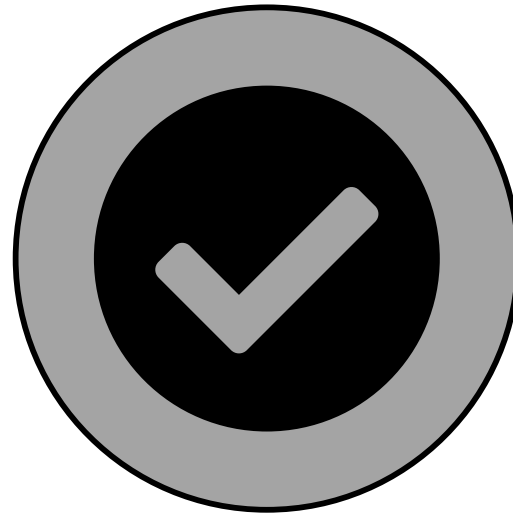
 **OFCS Cyber Event Defence**
Réseau de situation Cyber



 **BACS Cyber Event Defence**
Operation



BACS Cyber Event Defence Retrospective





Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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





Main Venue





Public Viewing



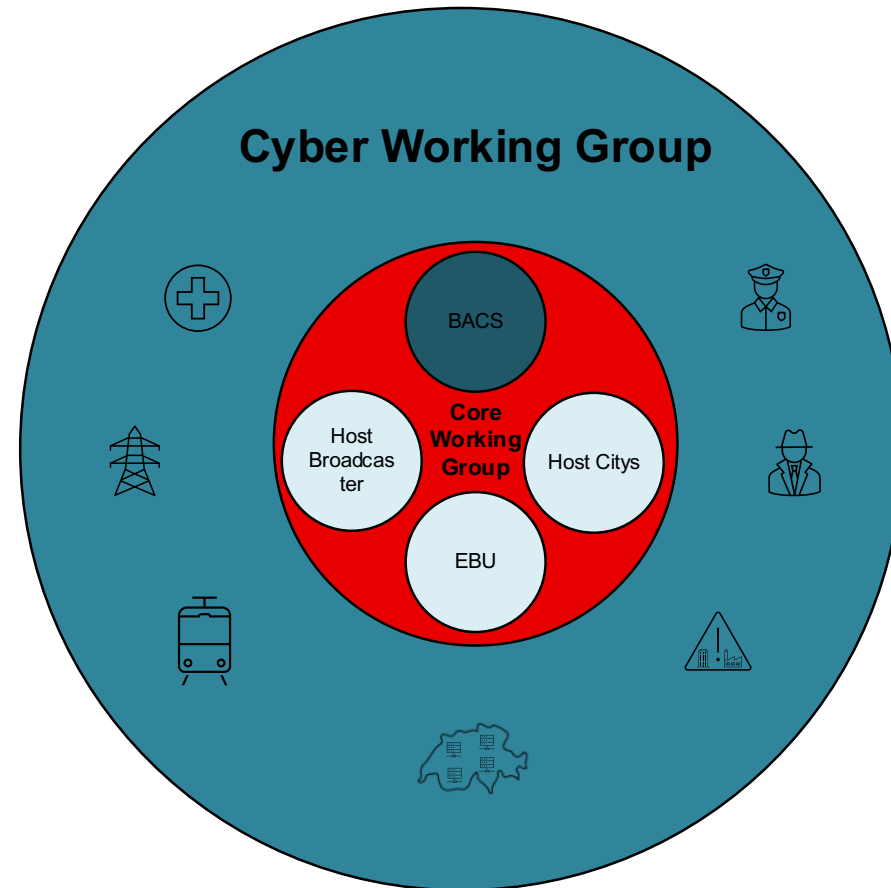


Eurovision Village





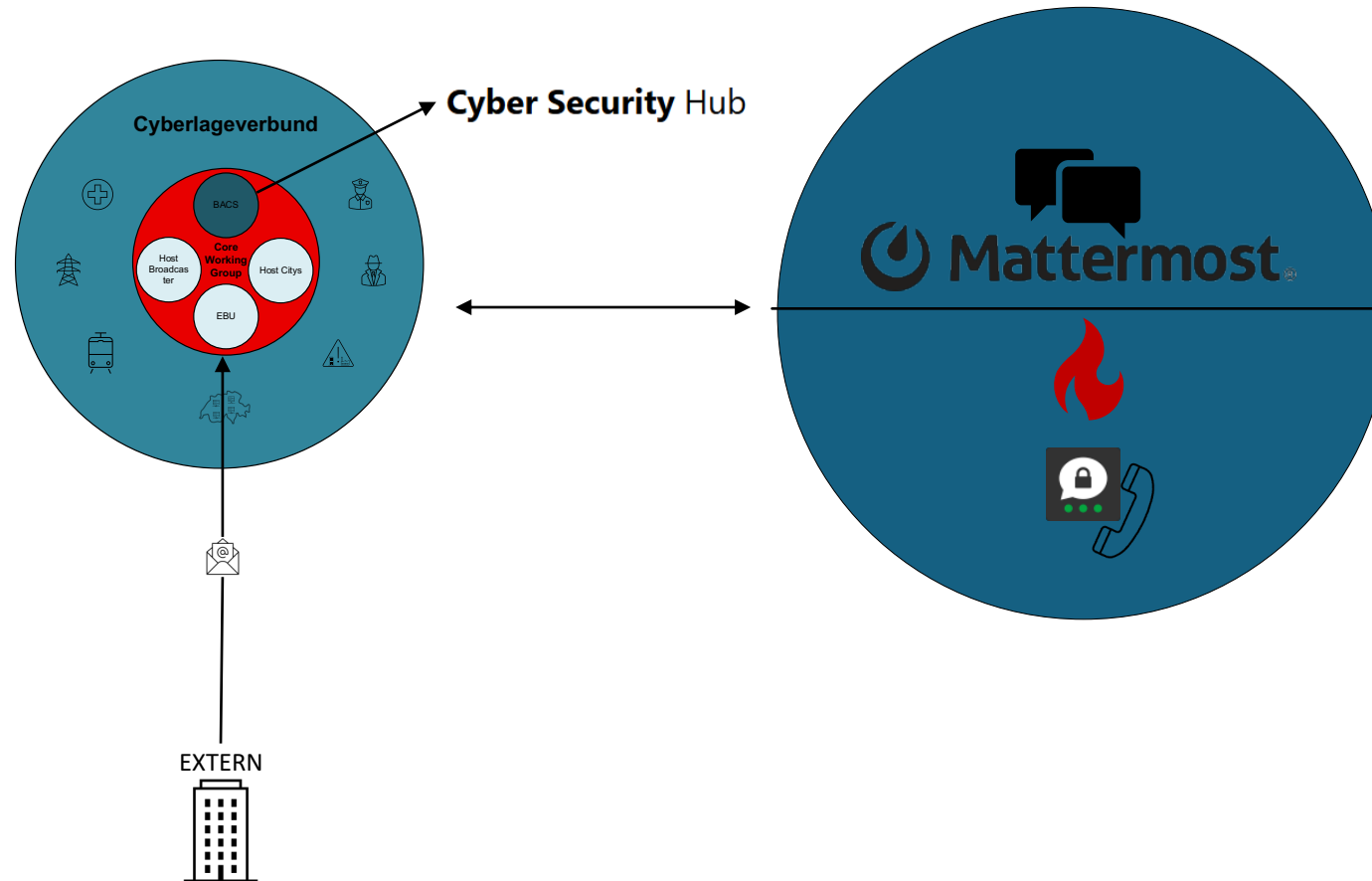
Cyber Task Force





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)



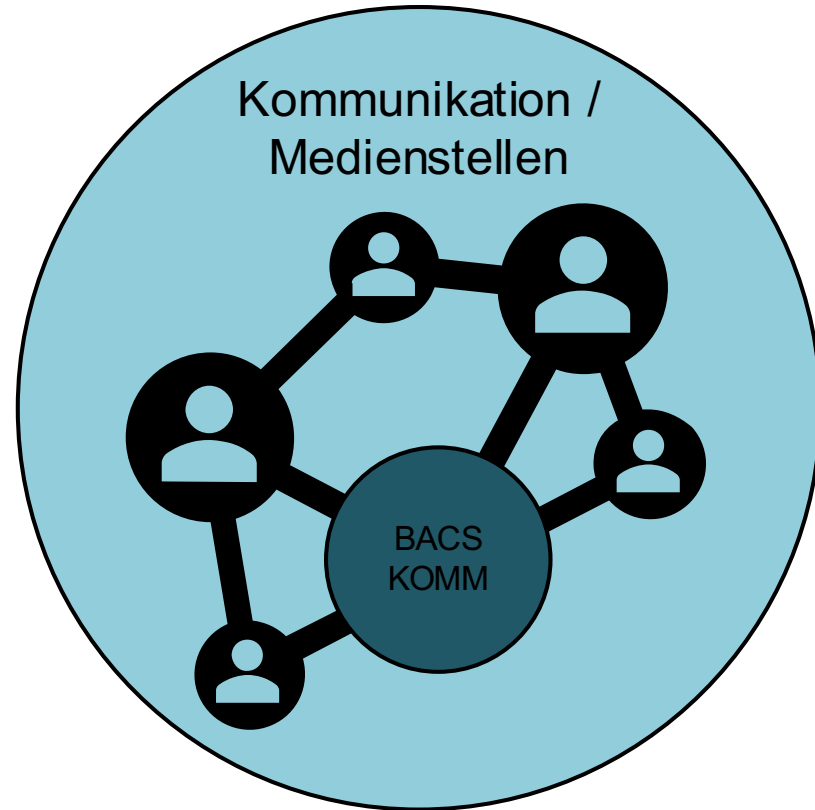
Incident Management Plattform

Communication / Media

Réseau interorganisationnel

Communication proactive

Coordination de la communication de crise

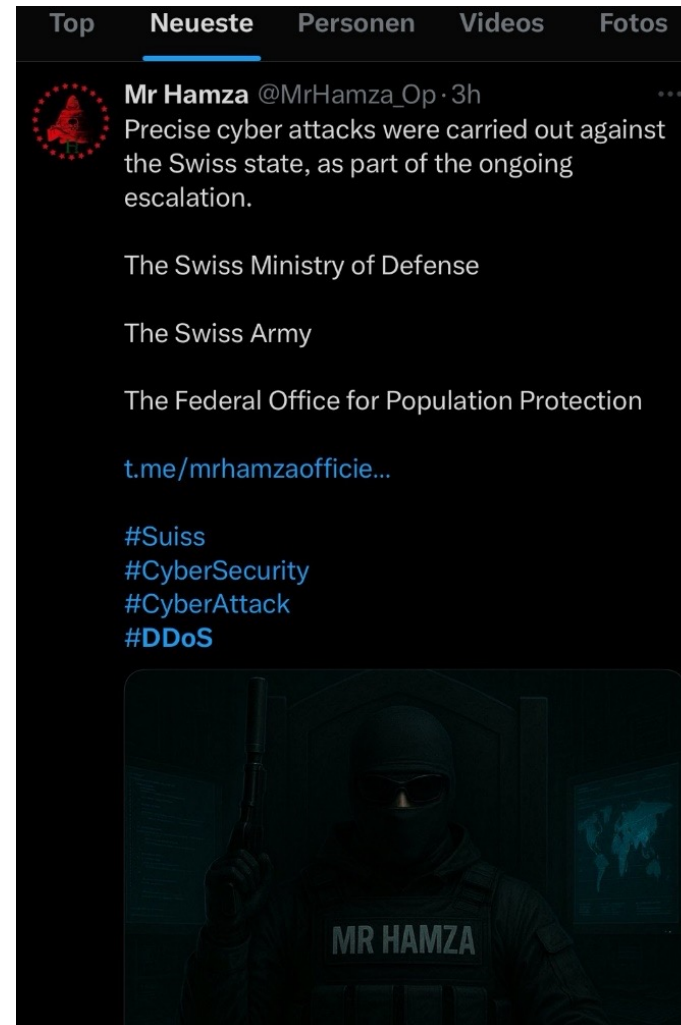




Incidents

Thursday, 8 May

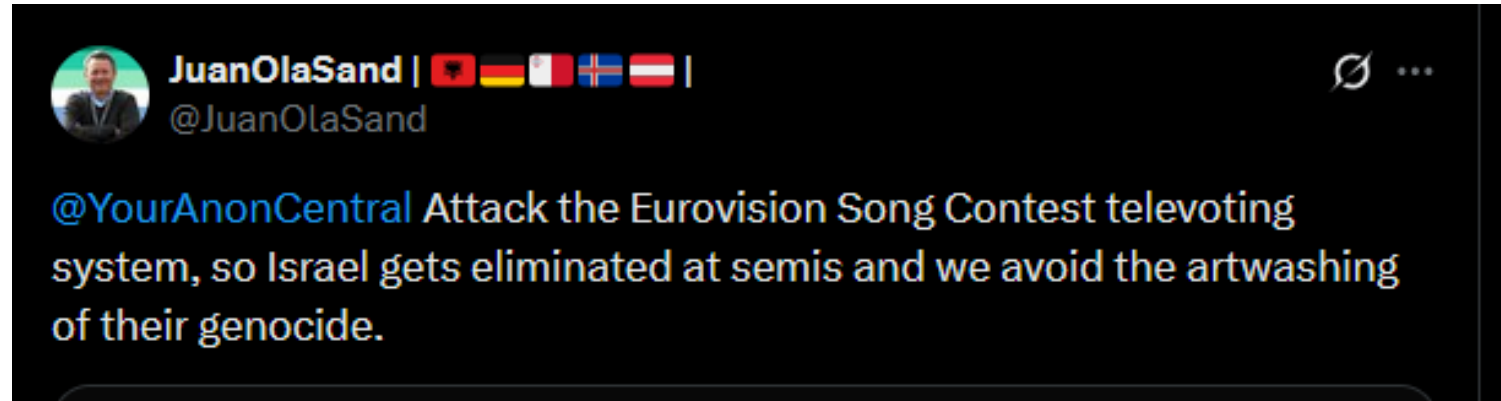
130Gbit/s, 14 Mio pps





Incidents

Thursday, 15 May





Incidents

Friday, 16 May





Incidents

Friday, 16 May

May 16



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

May 16

NNM057(16) En version

502 Bad Gateway

nginx

NNM057(16)

Не удается получить доступ к сайту

Не удается получить доступ к сайту

Сайт www.33ertaxi.ch не позволяет установить соединение с сервером.

Попробуйте сделать следующее:

- Проверьте подключение к интернету.
- Проверьте подключение к серверу и брандмауэр.
- Проверьте настройки прокси-сервера и брандмауэра.

"Saw" the best song at the Eurovision Service festival and put several sites 🇨🇭


- ✗ Herbing Basel
check-host.net/check-report/263cca94ke6b
- ✗ Authorization on the Prepaid Flat 7 portal (dead by ping)
check-host.net/check-report/263d008ek72e
- ✗ Taxi city Basel 33r Taxi AG (dead in ping)
check-host.net/check-report/263d012akb92

Subscribe

11 9:10 AM



NoName



[GovCERT.ch Cyber Threat Intelligence](#)

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

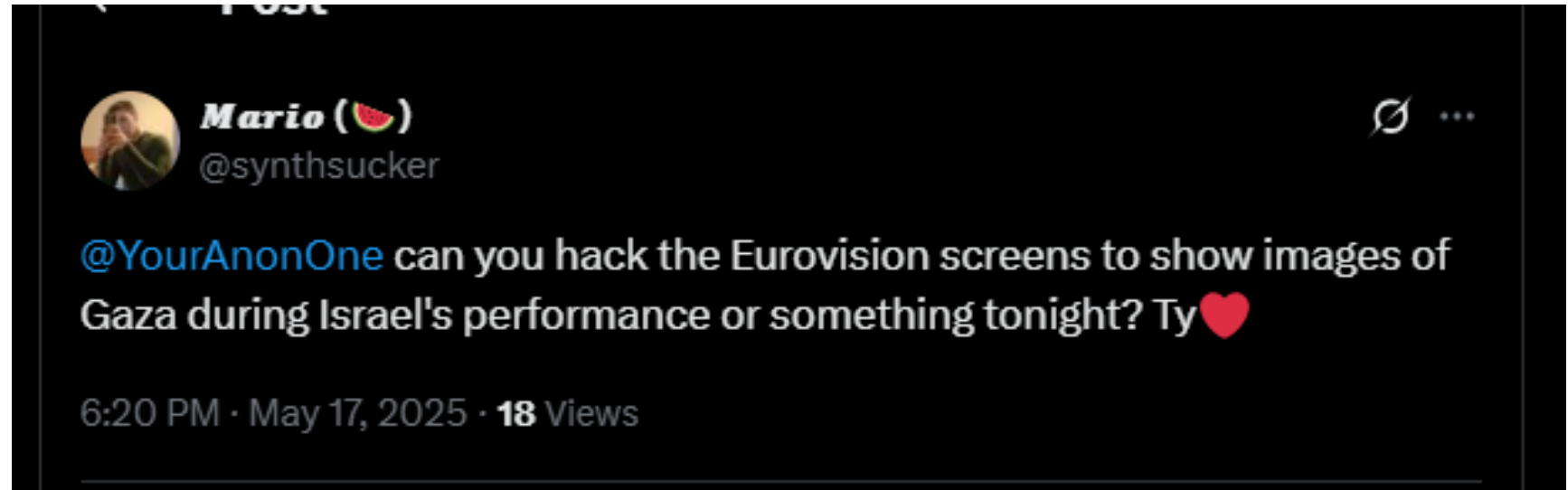
[Table of Contents](#)

- [OffensiveCIDRs/Bruteforce.csv](#): Contains top CIDRs (/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.
- [OffensiveCIDRs/Bruteforce_CIDR-only](#): This list contains the same data as [OffensiveCIDRs/Bruteforce.csv](#) but just the CIDRs (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 CIDRs (/24) that participated in DDoS attacks in the week of 2025-01-20 (week #4) against Swiss targets. These attacks were allegedly conducted by hacker 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 CIDRs (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 CIDRs will probably cause false positives. We therefore recommend



Incidents

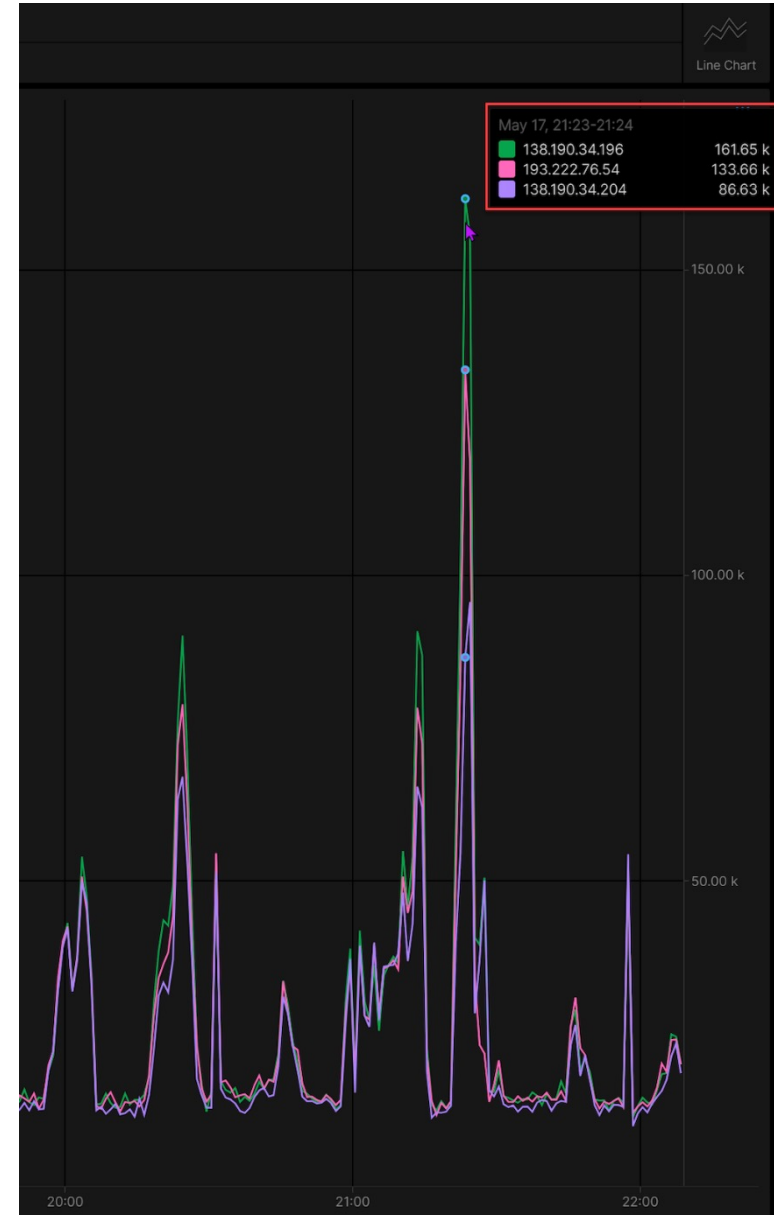
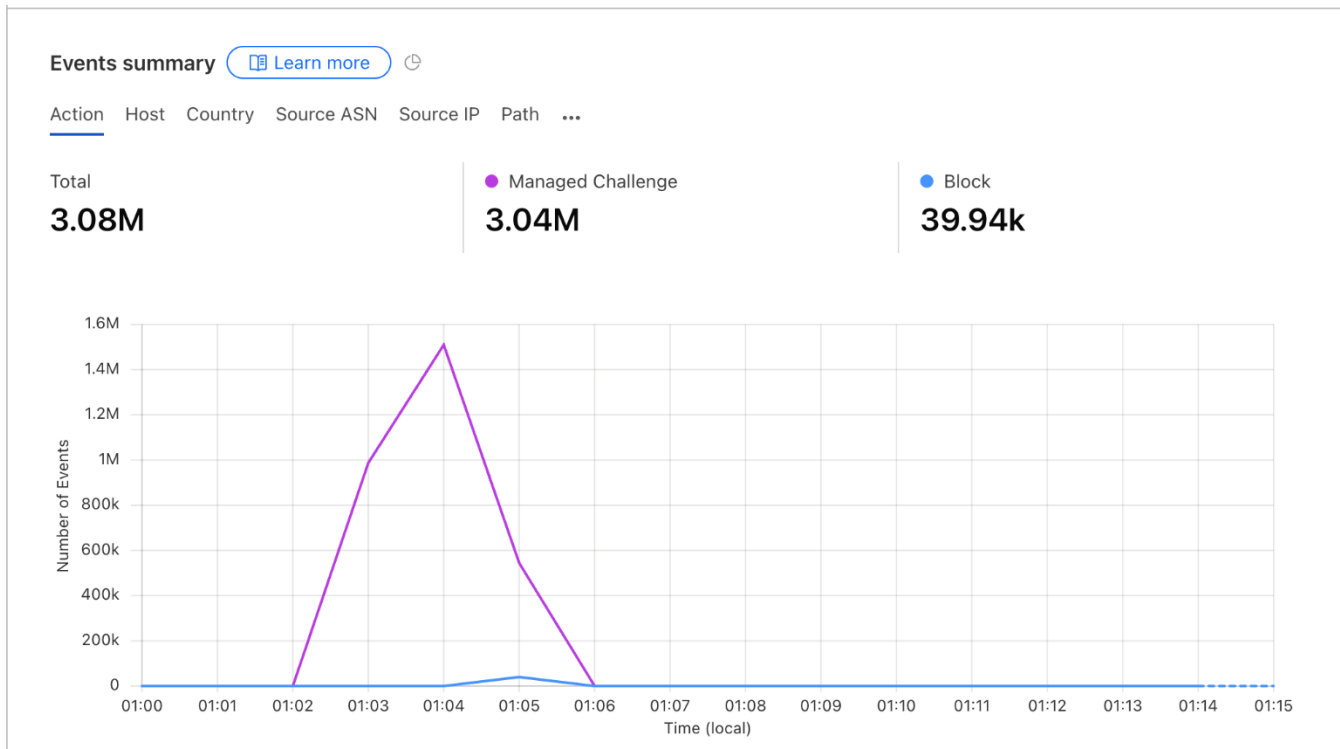
Saturday, 17 May





Incidents

Saturday, 17 May



Objectifs de la SSR:

- Un concours européen de la chanson pour tous, c'est aussi la sécurité pour tous
- La cybersécurité est essentielle tant pour la direction que pour les participants et le public.
- La protection des systèmes, des données et des personnes est au cœur d'une ESC sûre et inclusive. C'est pourquoi un partenariat solide en matière de sécurité était indispensable.

Pourquoi Cybersécurité? → Faits / Historique:

- 2019 Tel Aviv – KAN Diffusion en ligne basculée sur les messages des militants
- 2021 Rotterdam – Streaming server hackés
- 2024 Malmö – Streaming- et Webserver détruits par une cyberattaque (DDoS)

Notre Mission:

Protège l'ESC d'un point de vue cybersécurité, incluant:

- les gens
- l'événement
- la réputation de la Suisse



shutterstock.com - 2374013201

Alliance perfide entre les acteurs étatiques et la cybercriminalité

VOL DE DONNÉES

BLOCKAGE

SABOTAGE

ABUS



Effet
multiplicateur



CHAOS !

Complexité et responsabilité distribuée

ORGANISATEURS DE L'ÉVÉNEMENT

COLLABORATEURS

AUTORITÉS

FOURNISSEURS



FOURNISSEURS IT / CYBERSÉCURITÉ

Approche globale



Facteur clé de succès: *ESC2025 SANCTUARY*

Senthorus
24/7 SOC

THE ONION PRINCIPLE

FOCUS ON CRITICAL ASSETS

SIMPLE SETUP

DARKTRACE

CLOUDFLARE

Microsoft

ELCASecurity
AN ELCA COMPANY

Senthorus

St Jakobshalle

St Jakob Stadium

Voting system

Rank	Country	Points	Rank	Country	Points	Rank	Country	Points
1	SWITZERLAND	411	16	PORTUGAL	152	18	UNITED KINGDOM	46
2	CROATIA	347	17	GREECE	123	19	FINLAND	28
3	UKRAINE	309	18	GERMANY	112	20	ESTONIA	37
4	FRANCE	273	19	GEORGIA	84	21	SPAIN	30
5	ISRAEL	253	20	CYPRUS	71	22	SLOVENIA	27
6	IRELAND	234	21	LATVIA	64	23	AUSTRIA	24
7	ITALY	214	22	ARMENIA	53	24	NORWAY	16
8	ARMENIA	183	23	SWEDEN	47			
9	SWEDEN	174						

Highlights und chiffres clés

71 risques identifiés → 7 catégories

Training: 4 exercices Tabletop cybersec

Rythme: 6 mois → Live

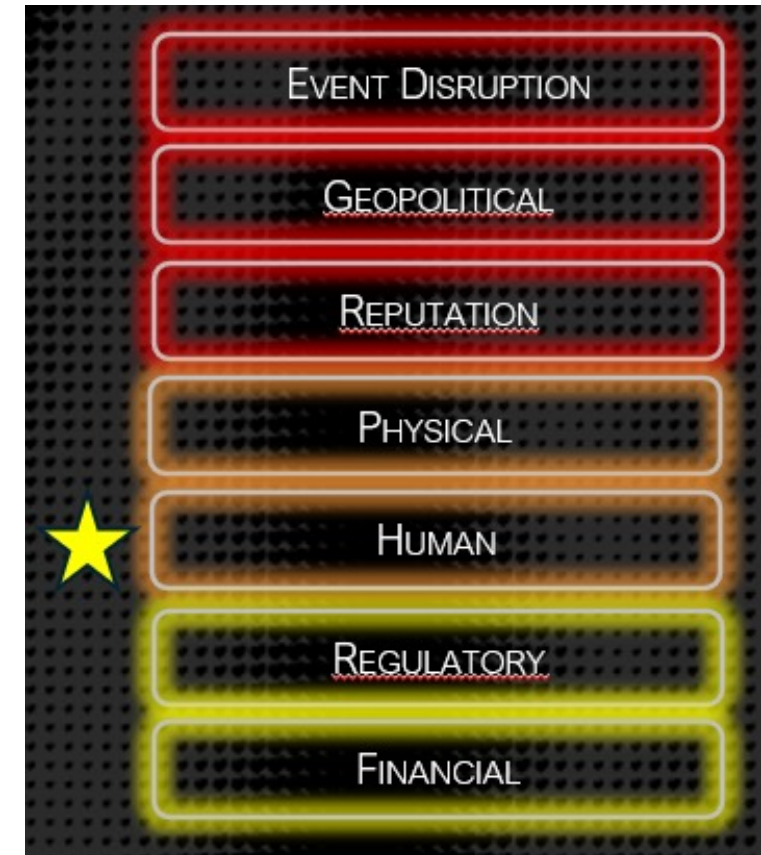
20+ fournisseurs évalués

50+ rapports Threat Intelligence & SM

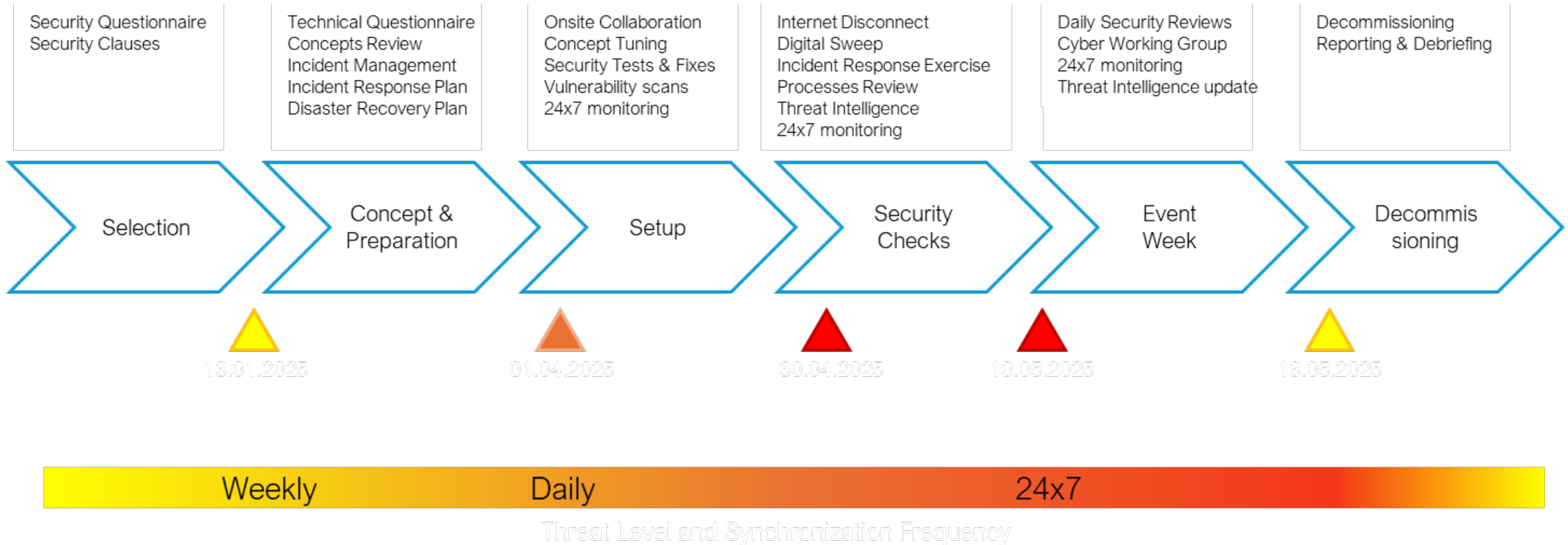
30+ «assets discoveries» journaliers

Takedowns en temps réel pendant 2 sem.

Digital Sweeps



Timeline



De la gestion de risque à la réalité

DDoS

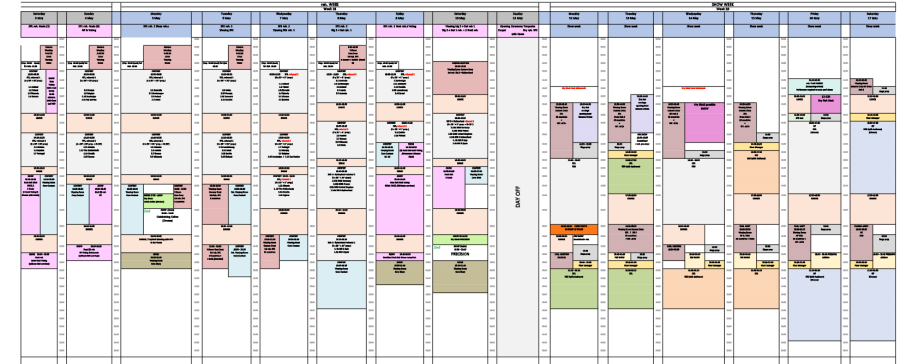
Videostream non autorisé sur SM

Campagnes de phishing et fraude

Campagnes de désinformation

Chantages et menace à la bombe

Appels à l'action d'activistes



The diagram is a dense grid of colored rectangles (pink, blue, green, orange, grey) connected by thin lines. It appears to be a network topology or a process flow chart. The columns are organized into sections, with some larger grey vertical bars acting as dividers. The overall structure is highly detailed and technical.



Prise de conscience



CIBLES COMPLEXES

CŒUR DÉMOCRATIQUE

IMPACT DIRECT

ANTICIPATION

CHAÎNE SÉCURITAIRE

COLLABORATION





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



THE WINNER IS...

