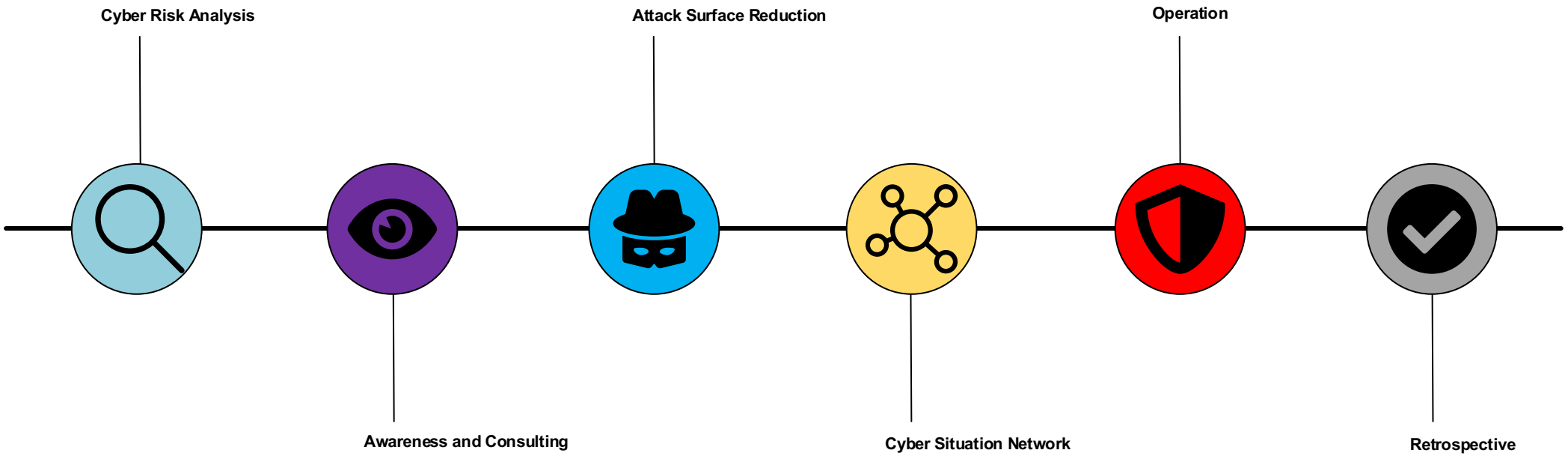
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

ELCASecurity
AN ELCA COMPANY

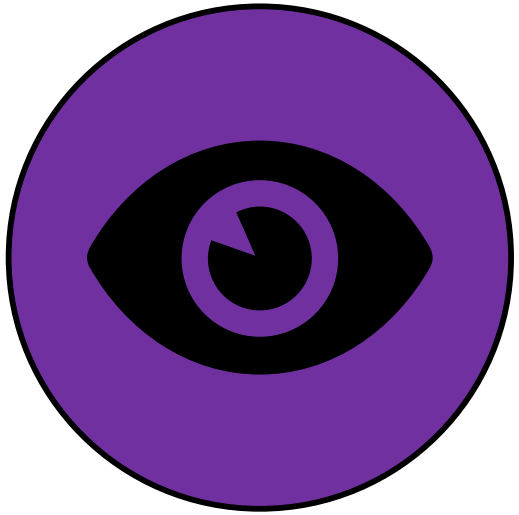
Sécurisation des événements majeurs – quand le numérique rencontre le physique

OFCS Cyber Event Defence
Concept de base



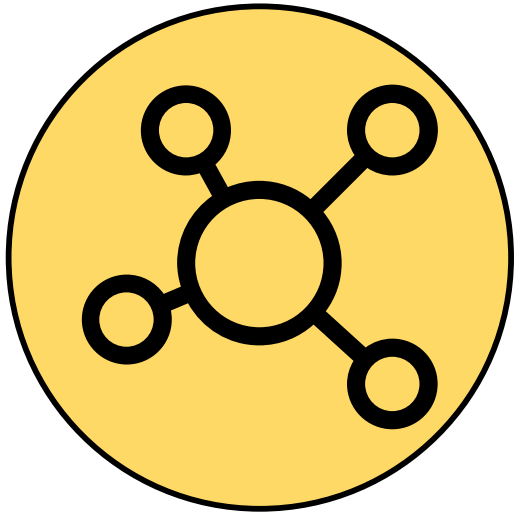
OFCS Cyber Event Defence
Cyber Risk Analysis

OFCS Cyber Event Defence
Sensibilisation et conseil

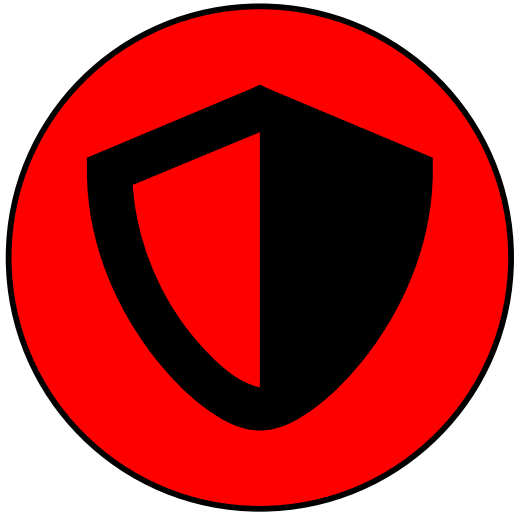


OFCS Cyber Event Defence
Réduction de la surface d’attaque

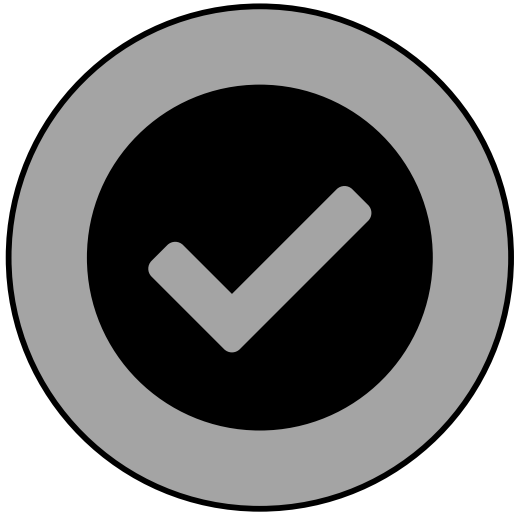
OFCS Cyber Event Defence
Réseau de situation Cyber



BACS Cyber Event Defence
Operation



BACS Cyber Event Defence
Retrospective



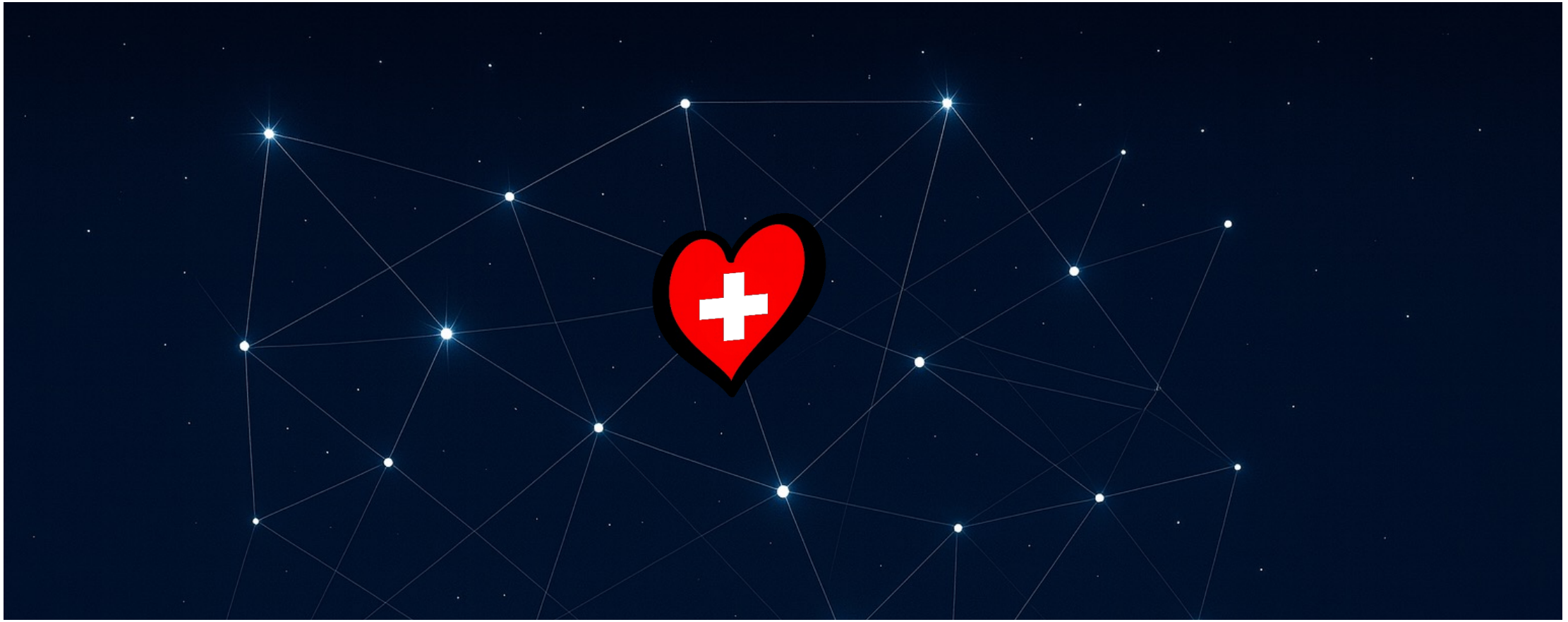
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

EUROVISION 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

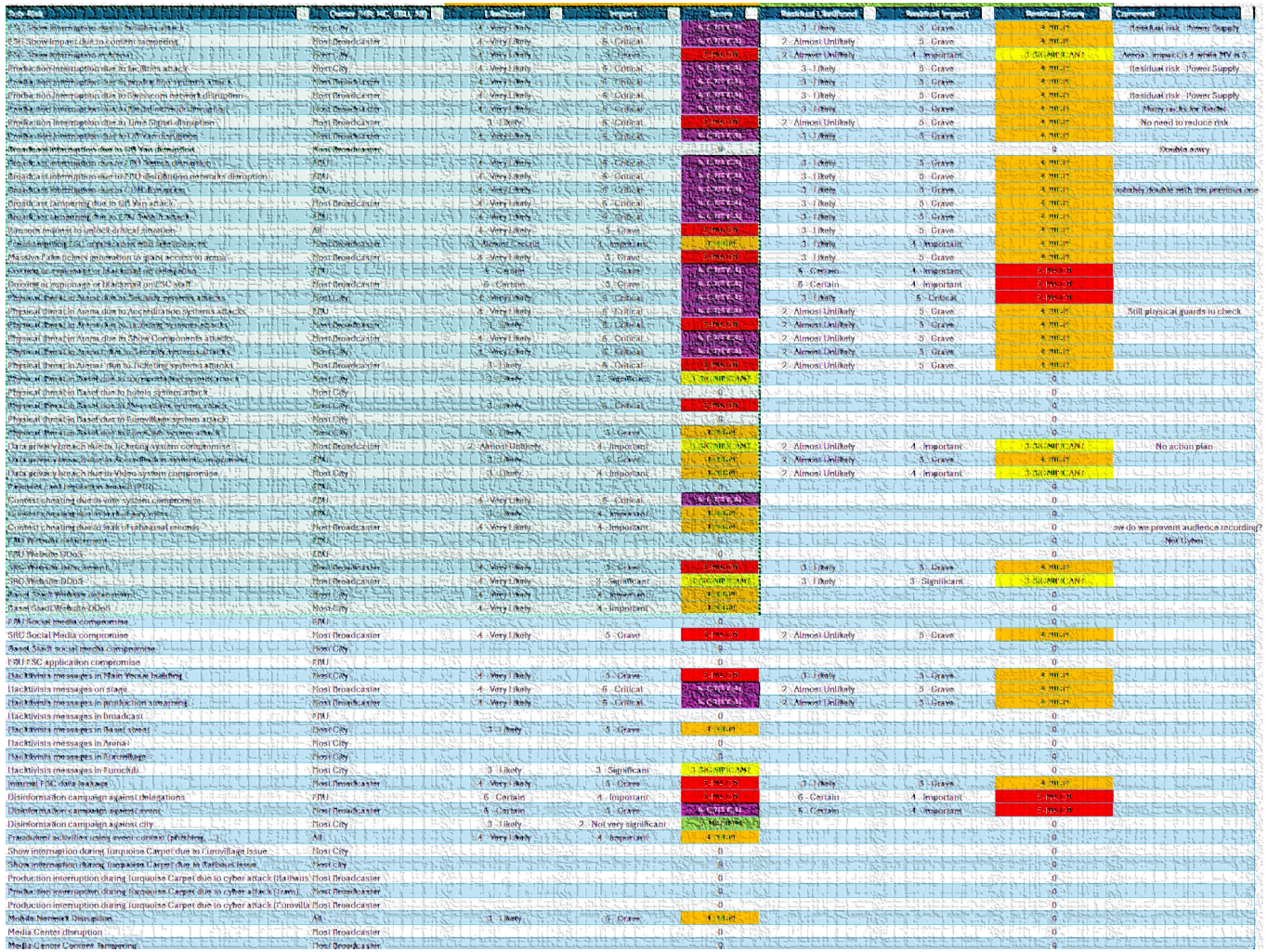
Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

Main Venue

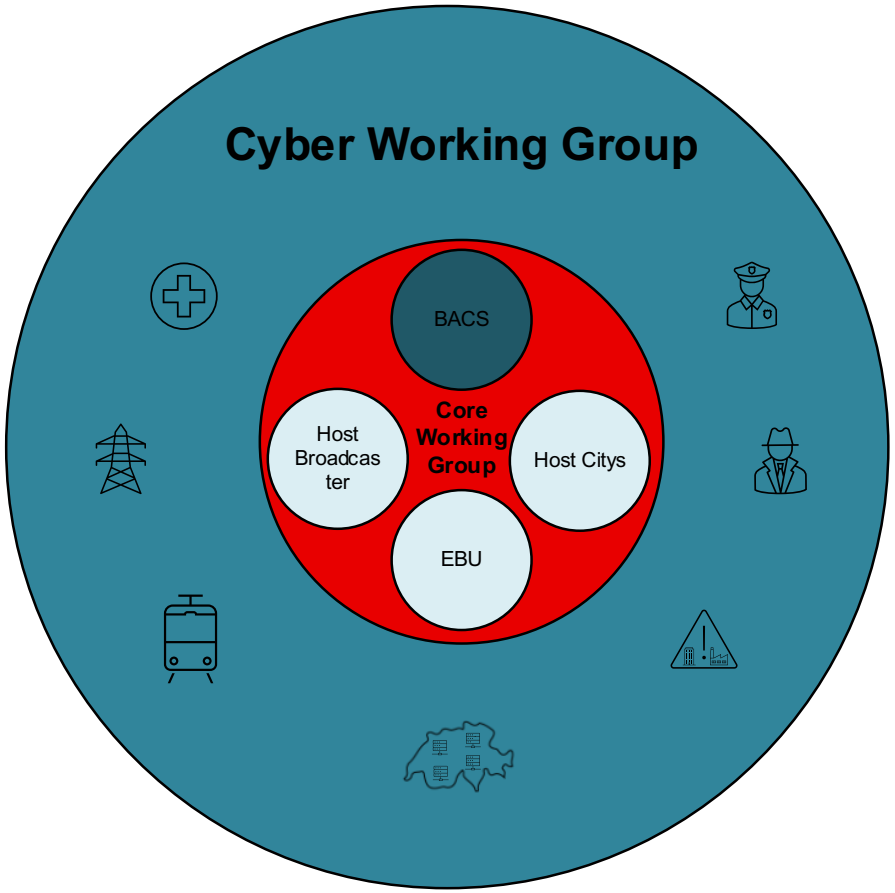
Public Viewing

Eurovision Village

Cyber Risk Analysis

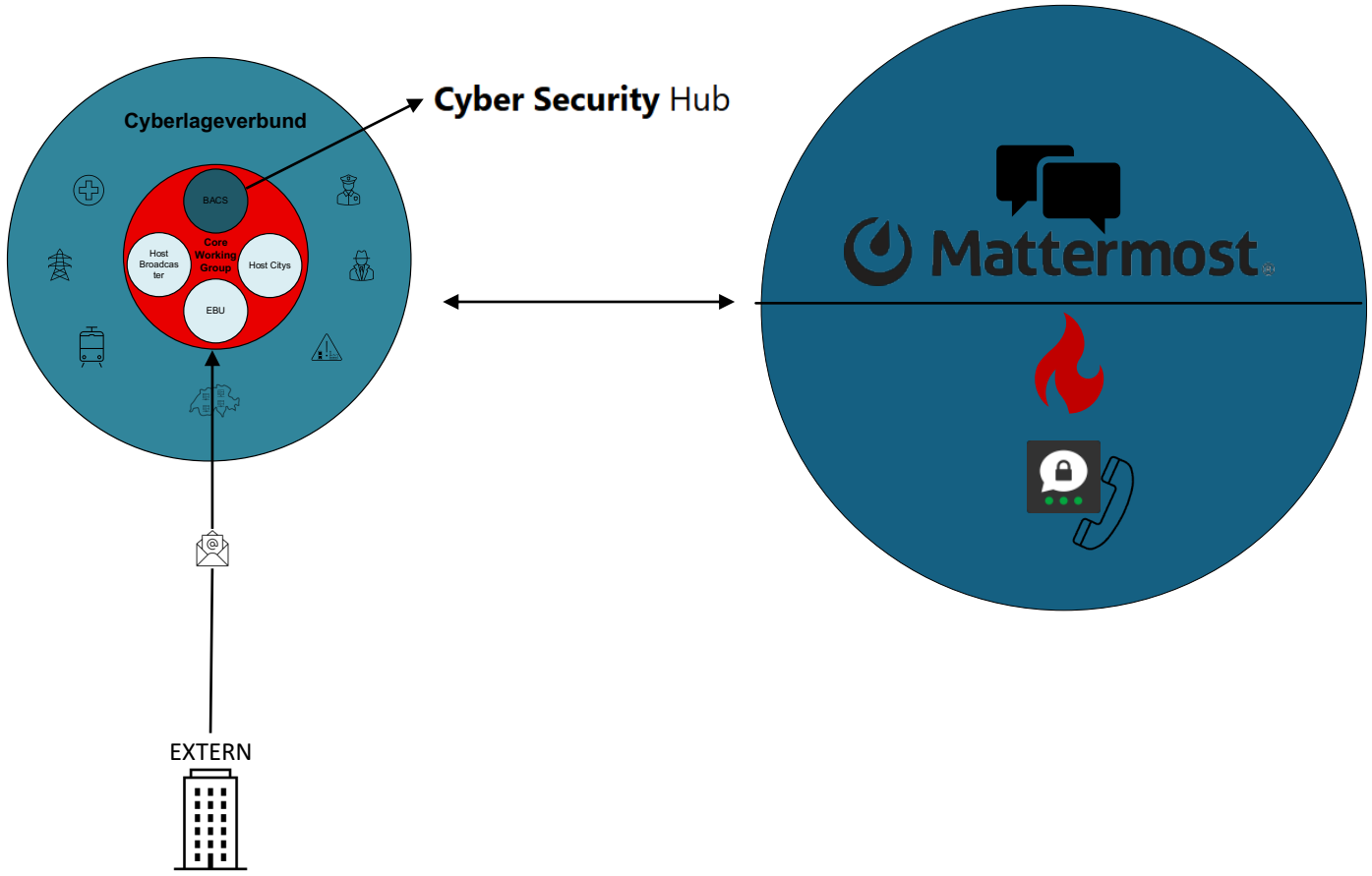


Cyber Task Force



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)

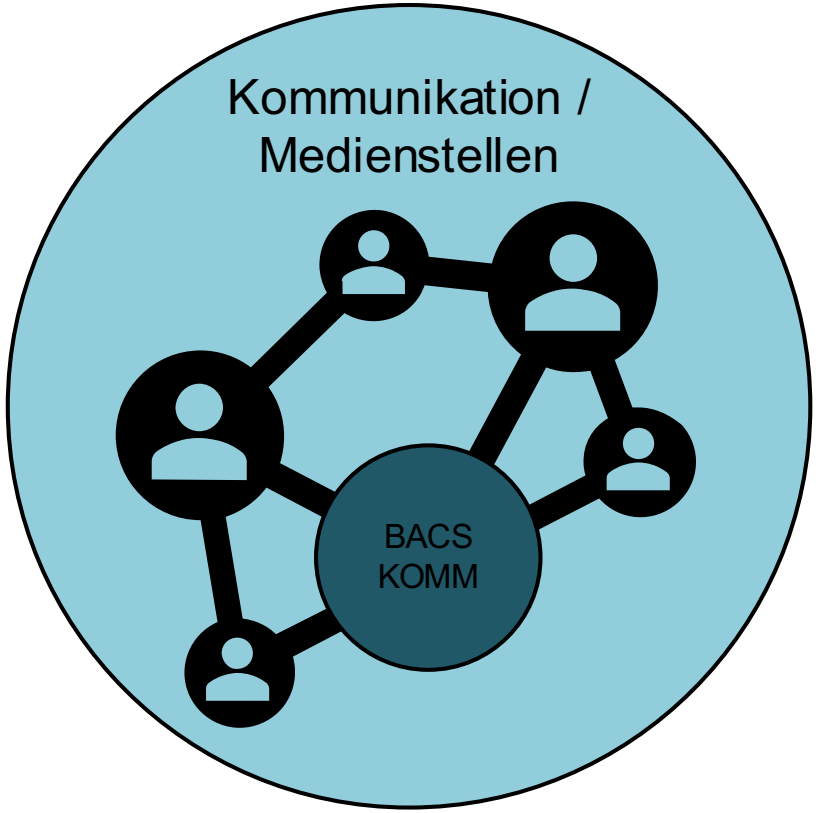
Incident Management Plattform

Communication / Media

Réseau interorganisationnel

Communication proactive

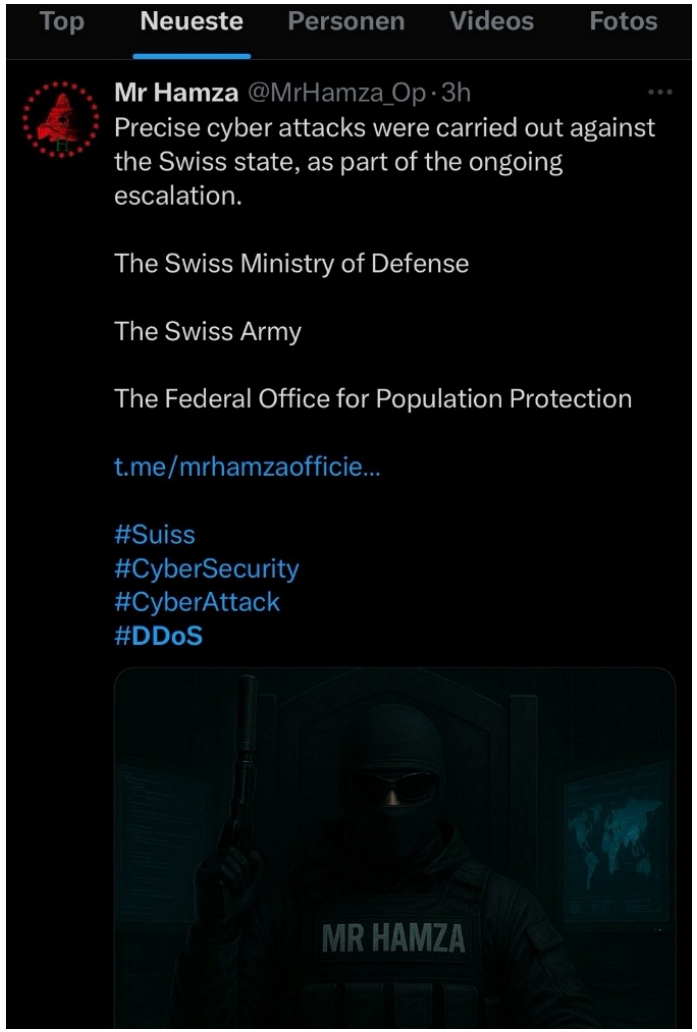
Coordiation de la communication de crise



Incidents

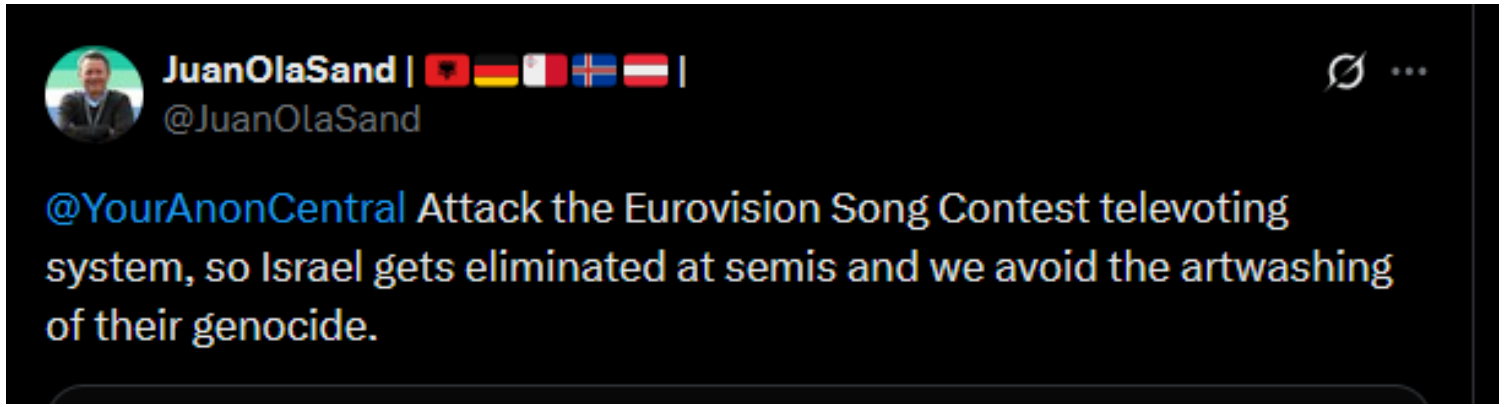
Thursday, 8 May

130Gbit/s, 14 Mio pps



Incidents

Thursday, 15 May



Incidents

Friday, 16 May

Incidents

Friday, 16 May

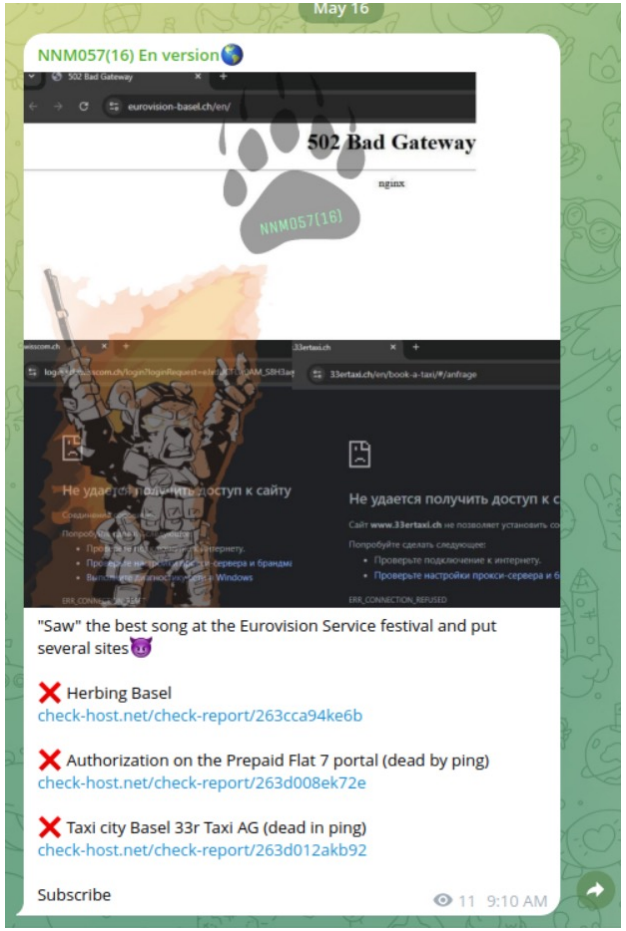
May 16

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

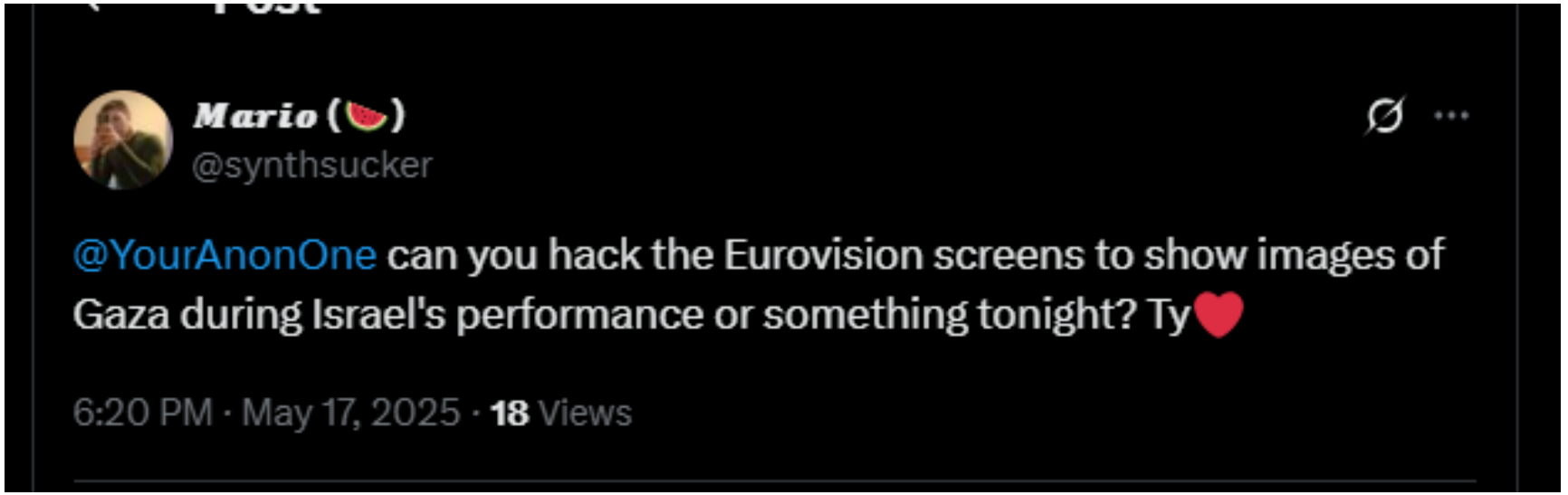


NoName


MALWARE
MALWARE
MALWARE
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 ressources.
OffensiveCIDRs/Bruteforce_CIDR-only: This list contains the same data as OffensiveCIDRs/Bruteforce.csv but just the CIDRs (no additional information such as ASN on 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 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 CIDRs (no additional information such as ASN on 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

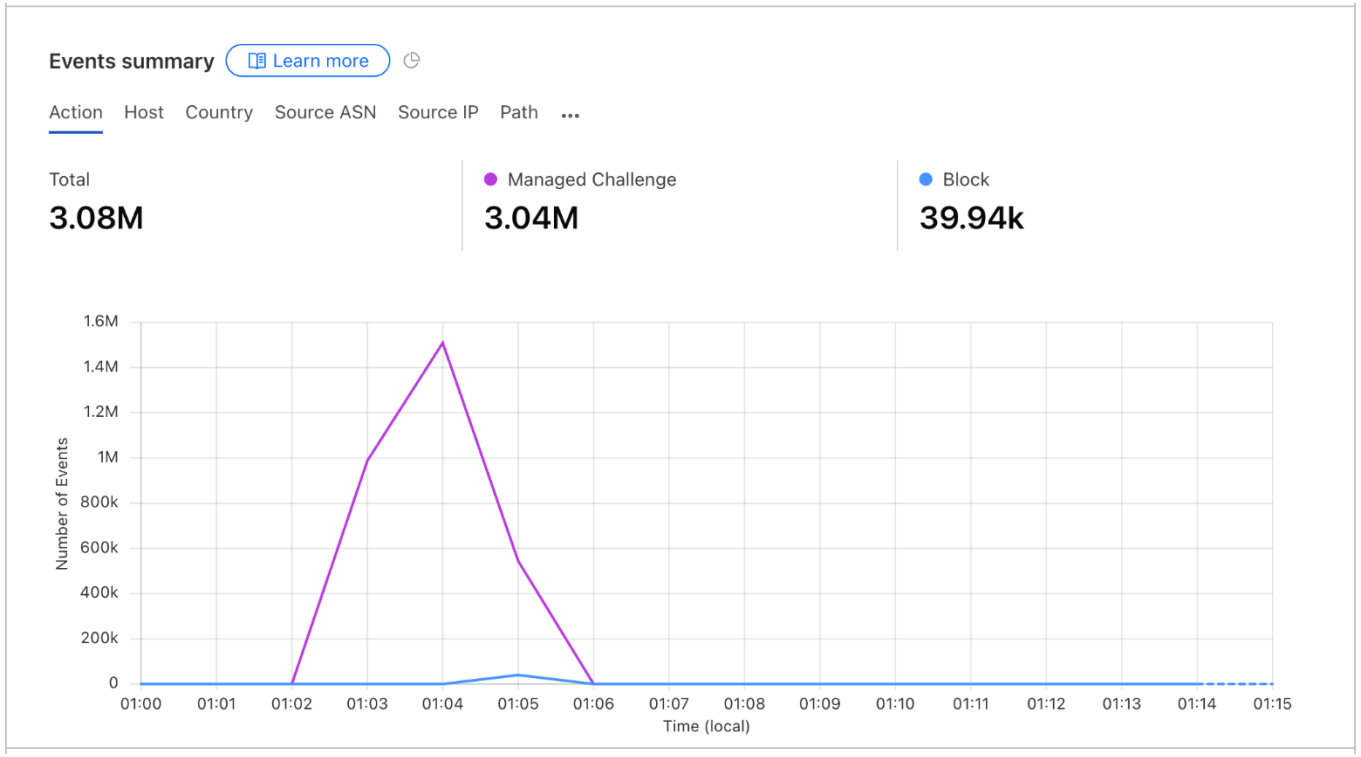
Incidents

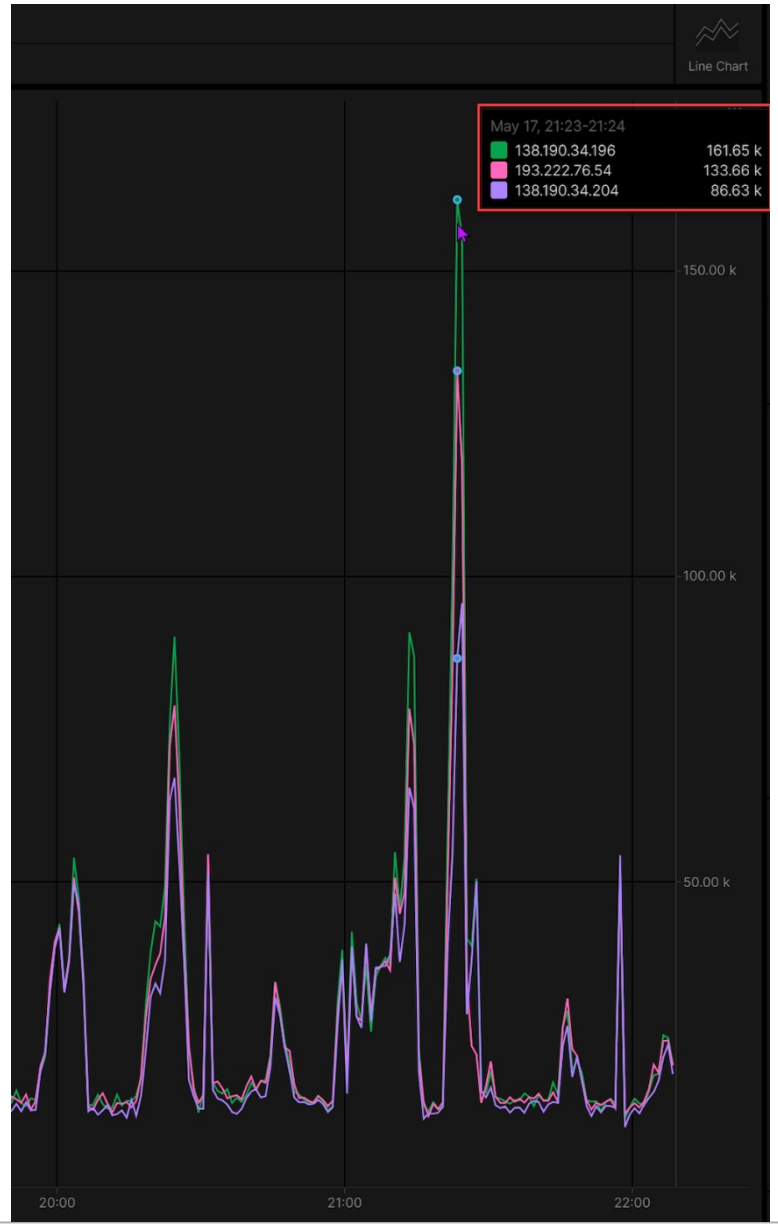
Saturday, 17 May



Incidents

Saturday, 17 May





ELCASecurity en tant que partenaire de la SSR: Point de vue de l'industrie

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

Alliance perfide entre les acteurs étatiques et la cybercriminalité

- VOL DE DONNÉES
- BLOCKAGE
- SABOTAGE
- ABUS

Effet multiplicateur

CHAOS !

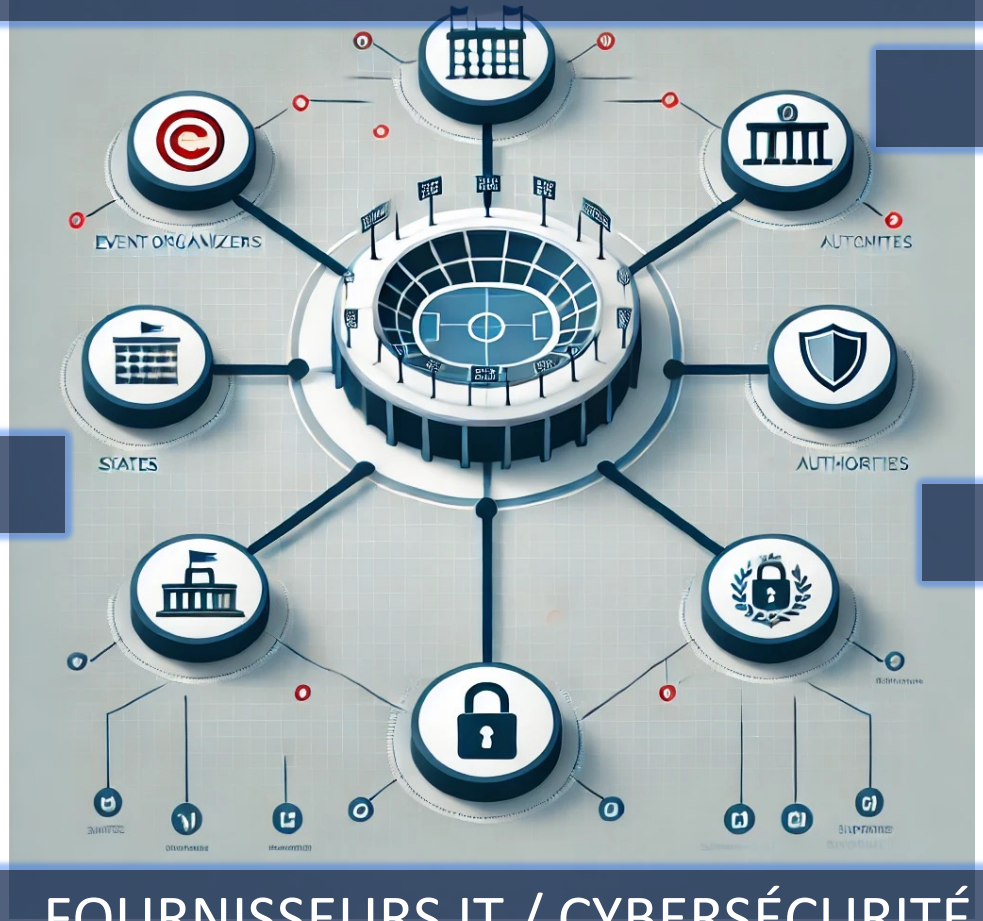
Complexité et responsabilité distribuée

ORGANISATEURS DE L'ÉVÉNEMENT

COLLABORATEURS

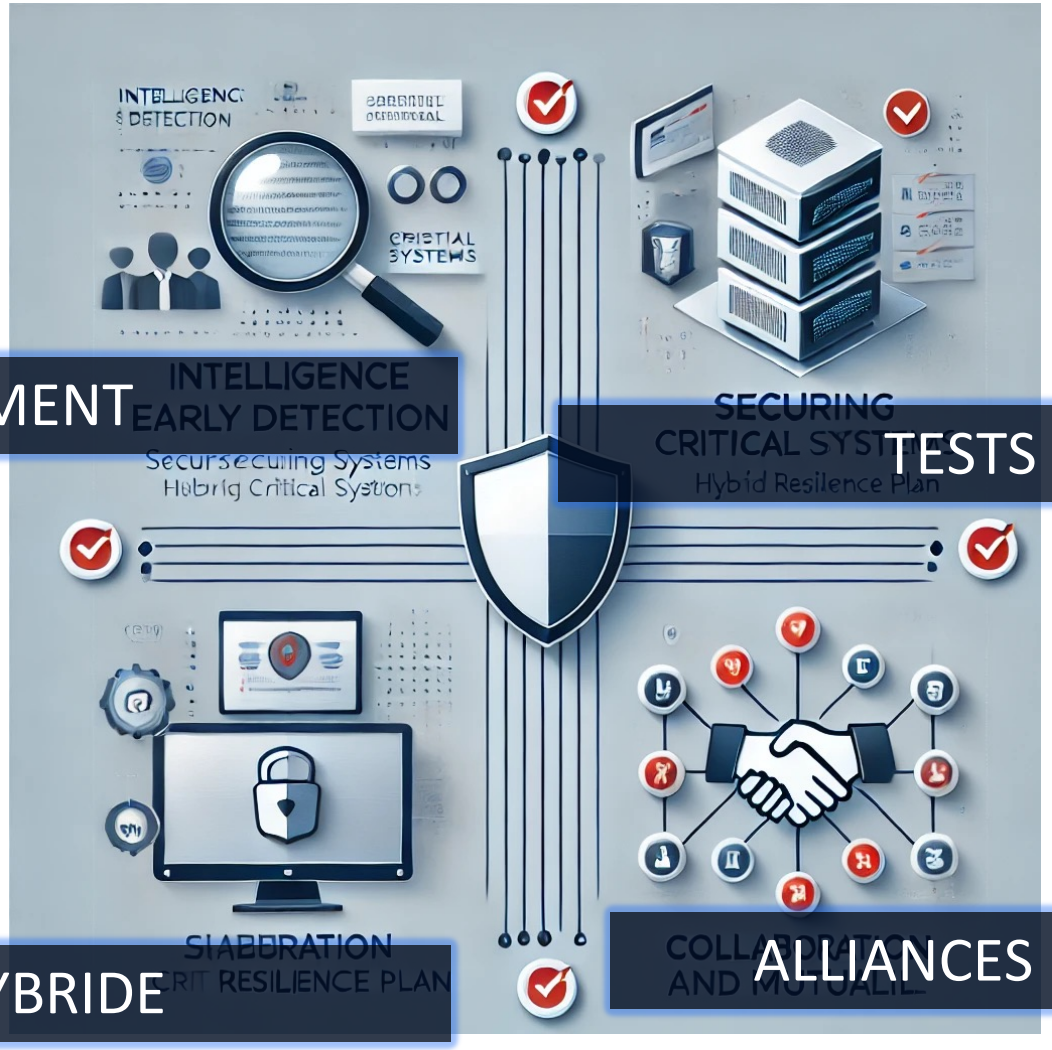
AUTORITÉS

FOURNISSEURS



FOURNISSEURS IT / CYBERSÉCURITÉ

Approche globale



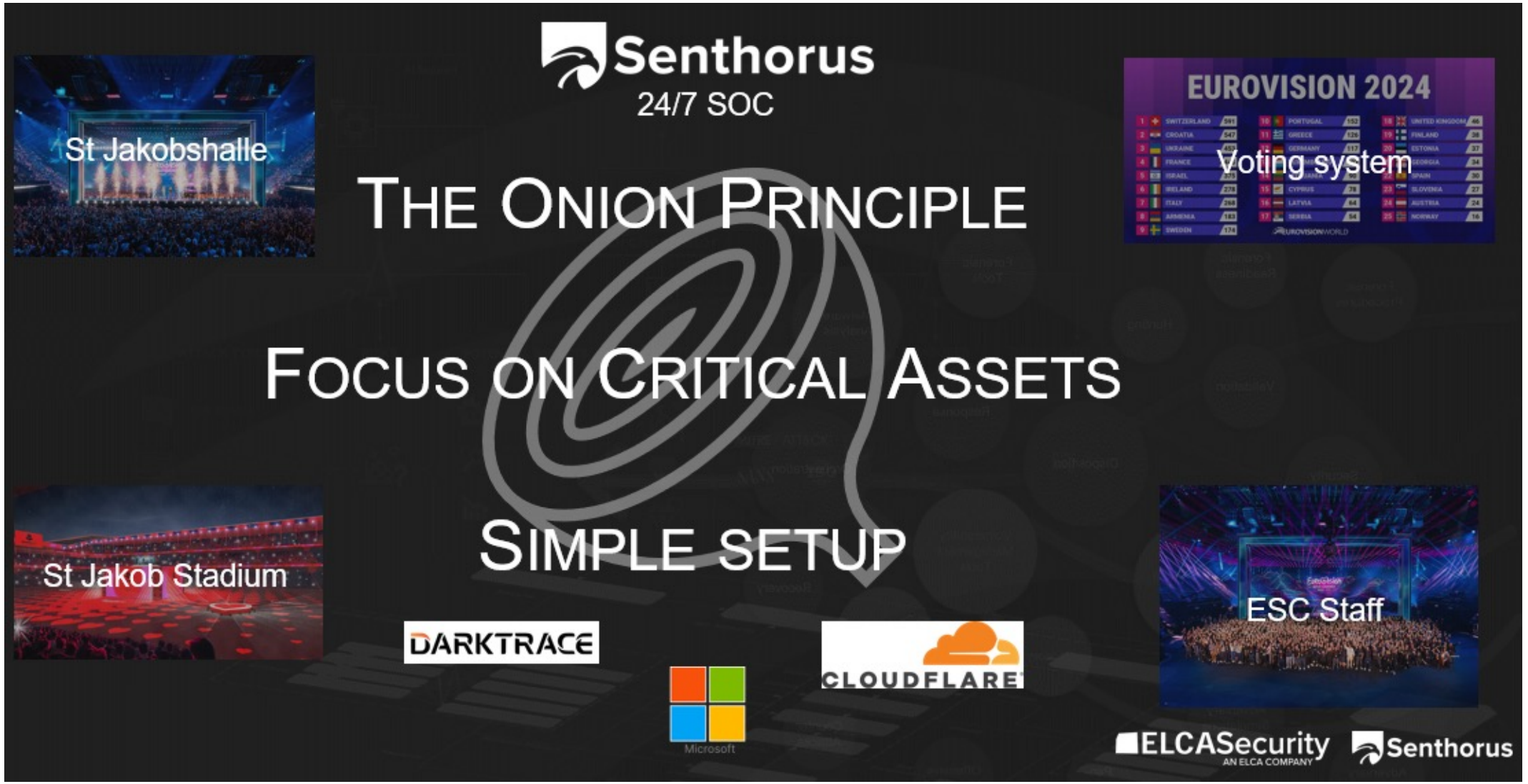
RENSEIGNEMENT

TESTS & QUALITÉ

RÉSILIENCE HYBRIDE

ALLIANCES ET COLLABORATION

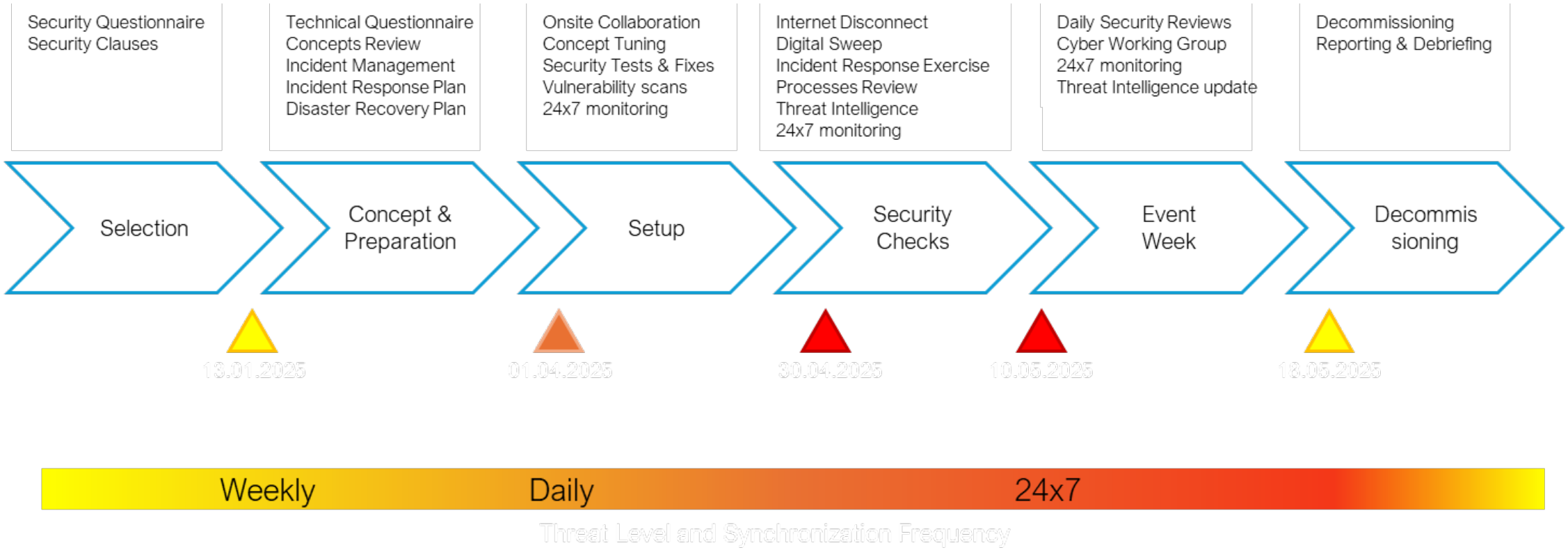
Facteur clé de succès: *ESC2025 SANCTUARY*



Highlights und chiffres clés

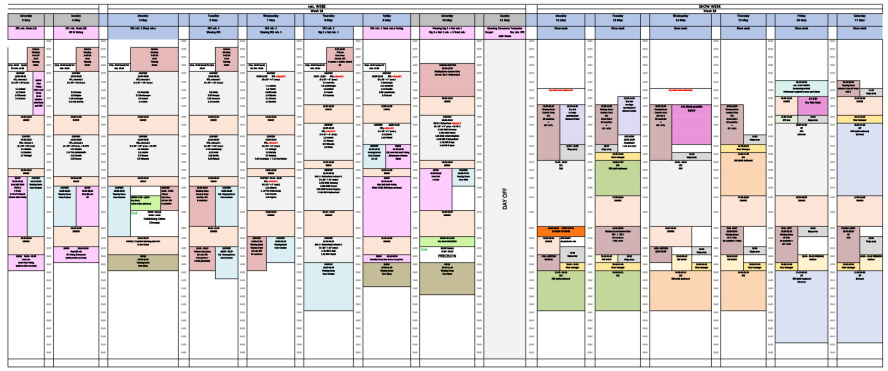
- 71 risques identifiés → 7 catégories
- Training: 4 exercices Tabletop cybersec
- Rythme: 6 mois → Live
- 20+ fournisseurs évalués
- 50+ rapports Threat Intelligence & SM
- 30+ «assets discoveries» journaliers
- Takedowns en temps réel pendant 2 sem.
- Digital Sweeps

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



Prise de conscience

CIBLES COMPLEXES

CŒUR DÉMOCRATIQUE

IMPACT DIRECT

ANTICIPATION

CHAÎNE SÉCURITAIRE

COLLABORATION

THE WINNER IS…