Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

CISO Sprechstunde

05.06.2024

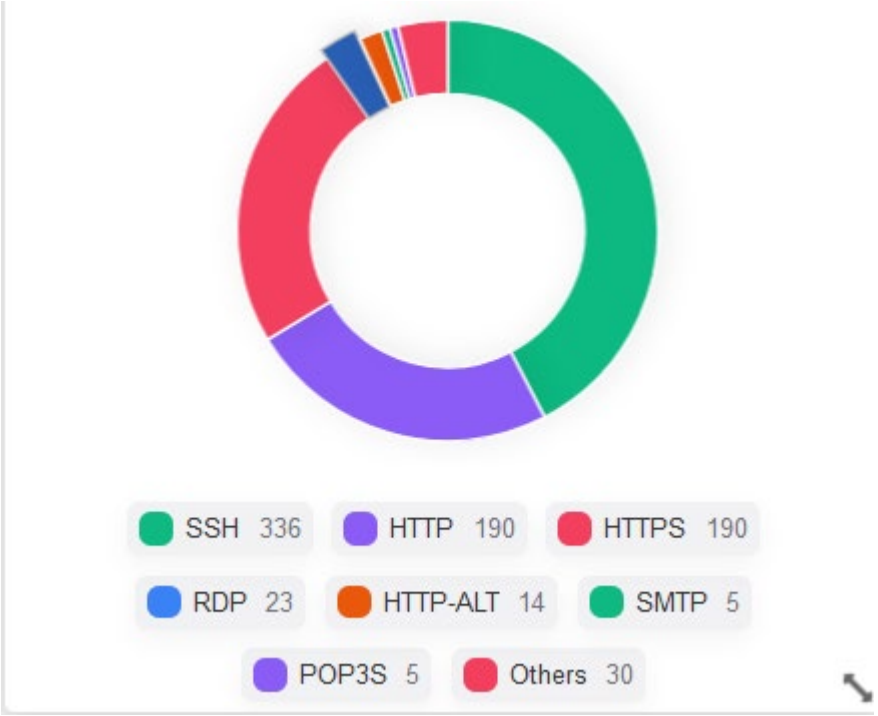
Informationssicherheit
Aktuelles aus der FAU

Aktuelles aus der FAU

- Informationssicherheitsleit- und –richtlinie: leider noch immer nicht verabschiedet

- Kritische Ports im Internet
  - RDP
  - X-Windows
  - SSH

- Keine Login-Seiten mit
  http (ohne Verschlüsselung)



FAU Credentials im Darknet

- Verwenden Sie bitte keine IDM-Kennungen und Passwörter auf Plattformen außerhalb der FAU

Black Market | Botnet Data | PII Exposure | IM Content | Suspicious Content

Black Market ID	Source	Stealer Log Preview	Related Assets	Price	Status	Obtain Progress	Discovery Date
Market-27072840	Genesis	Preview Not Found		0 $	Action Waiting	REQUEST OBTAIN	2024-02-20
Market-27072630	Genesis	Preview Not Found		0 $	Action Waiting	REQUEST OBTAIN	2024-02-20
Market-26927646	Russian Market	Open Preview	studon.fau.de, account.cip.cs.fau.de, ...	10.00 $	Action Waiting	REQUEST OBTAIN	2024-02-16
Market-26927585	Russian Market	Open Preview	studon.fau.de, campo.fau.de	10.00 $	Action Waiting	REQUEST OBTAIN	2024-02-16
Market-26927552	Russian Market	Open Preview	est.cs.fau.de	10.00 $	Action Waiting	REQUEST OBTAIN	2024-02-16
Market-26927525	Russian Market	Open Preview	campo.fau.de	10.00 $	Action Waiting	REQUEST OBTAIN	2024-02-16
Market-26786564	Russian Market	Open Preview	groupware.fau.de, campo.fau.de	9.00 $	Action Waiting	REQUEST OBTAIN	2024-02-12
Market-26786537	Russian Market	Open Preview	faumail.fau.de, campo.fau.de	10.00 $	Action Waiting	REQUEST OBTAIN	2024-02-12
Market-26786519	Russian Market	Open Preview	faumail.fau.de	10.00 $	Action Waiting	REQUEST OBTAIN	2024-02-12
Market-26782780	Russian Market	Open Preview	studon.fau.de, est.cs.fau.de, ...	5.00 $	Action Waiting	REQUEST OBTAIN	2024-02-12
Market-26782758	Russian Market	Open Preview	adfs.fauad.fau.de, studon.fau.de, ...	8.00 $	Action Waiting	REQUEST OBTAIN	2024-02-12
Market-26782588	Russian Market	Open Preview	adfs.fauad.fau.de, lists.fau.de, ...	10.00 $	Action Waiting	REQUEST OBTAIN	2024-02-12

Records per page: 25 1

ISMS: Aufbau eines Risikomanagements

Quelle: HITS IS

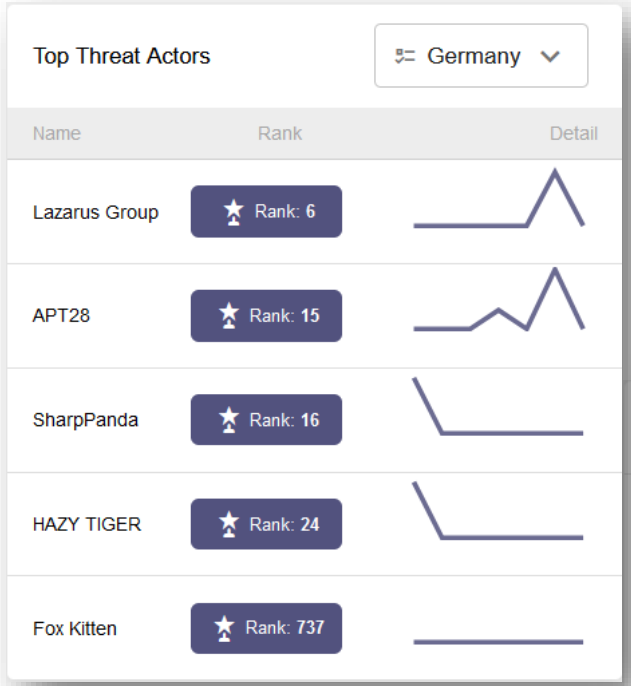
BCM: Notfallbewältigung im GRC-Tool

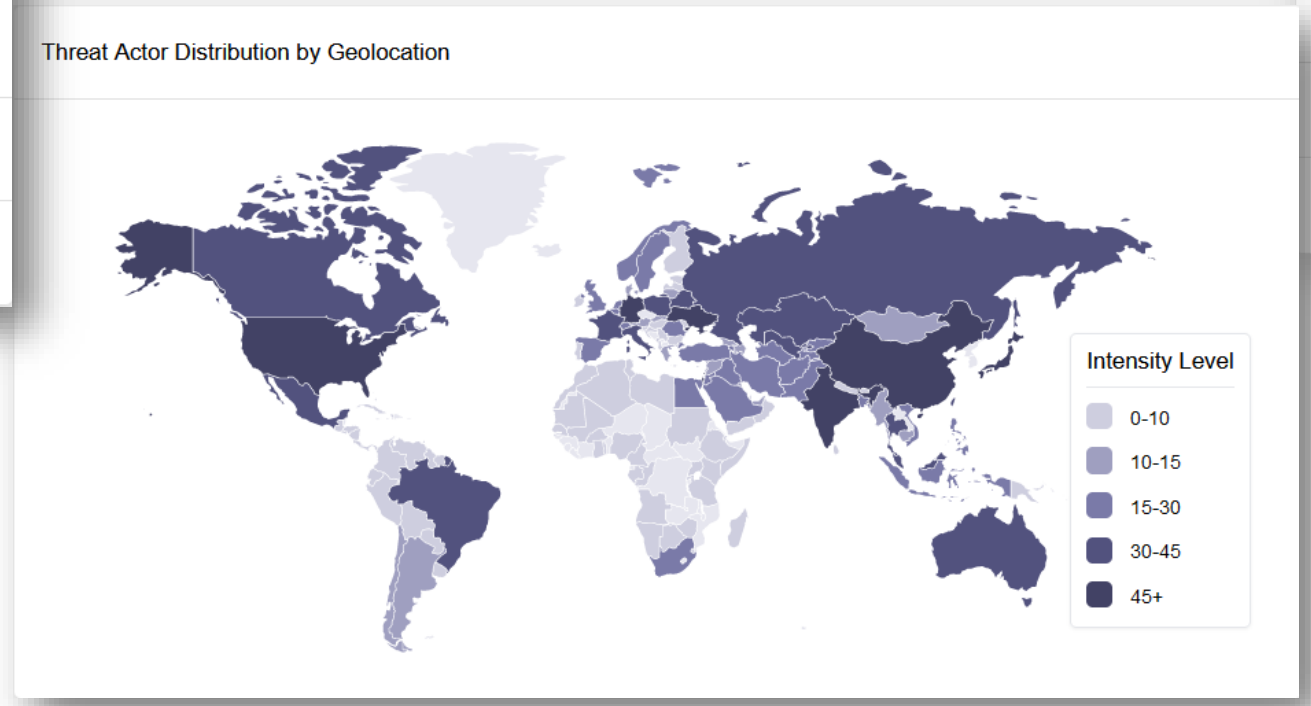
Quelle: HITS IS

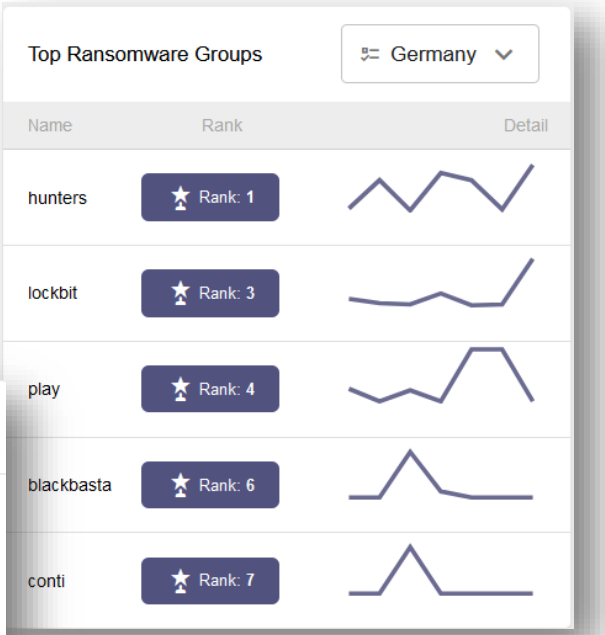
Informationssicherheit
Aktuelles aus der Welt

Operational Intelligence Trends

SOCRadar

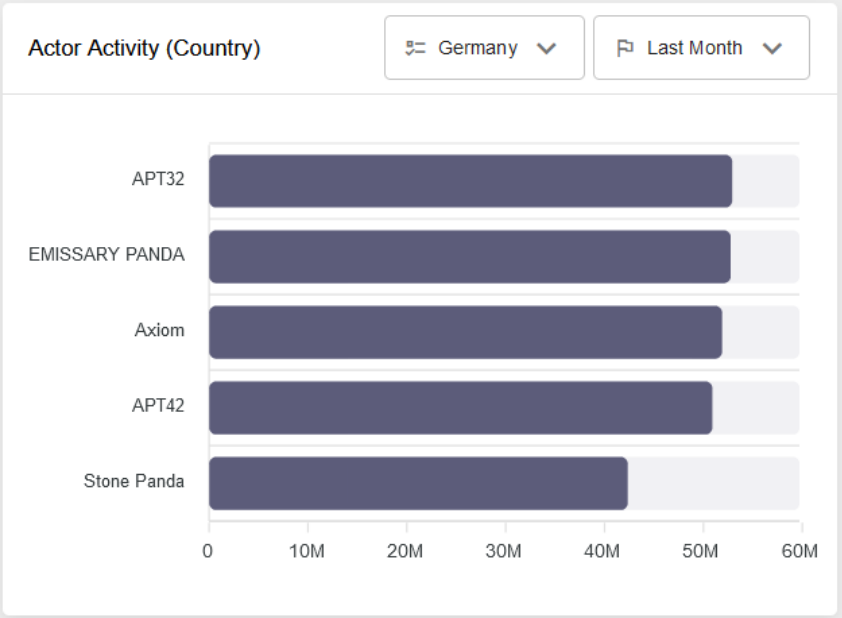


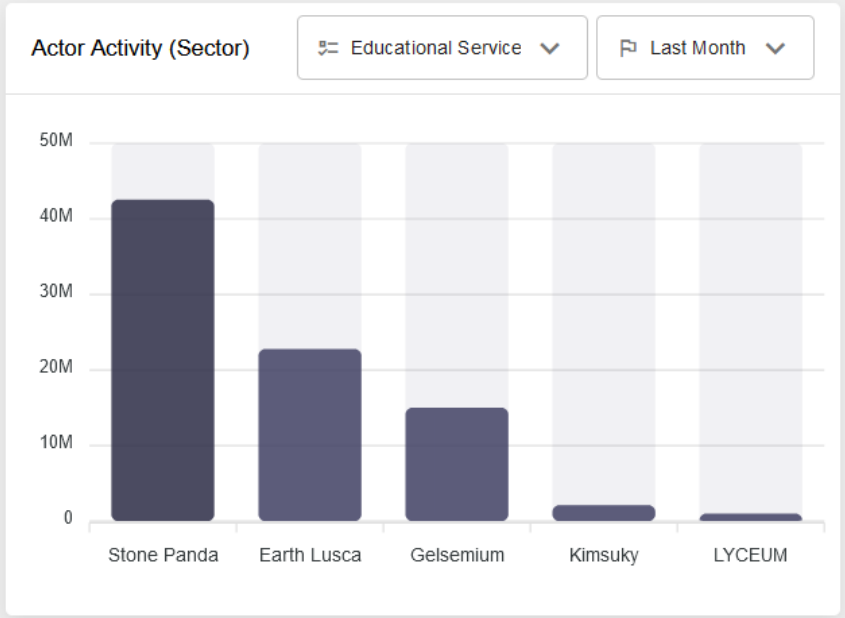


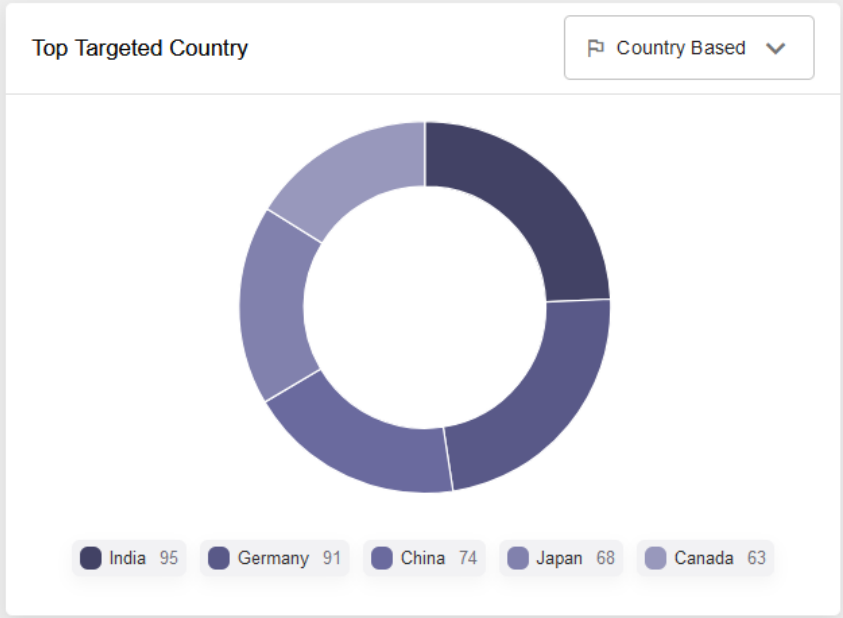


Threat Actors

SOCRadar







Threat Actor | Malware | IOC

Threat Actors

SOCRadar

Stone Panda

Rank: 628

0	0	236
Audience	News	IOC

Description:

Description of Etda: menuPass is a threat group that appears to originate from China and has been active since approximately 2009. The group has targeted healthcare,...

Target Sectors:

Public Administration - Space & Defense - Energy & Utilities - Chemical&Pharmaceutical Manufacturing - National Security&International Affairs - Telecommunications -...

Target Countries:

Hon... | Net... | India | +26

Associated Malware/Software

UP... | Mim... | pwd... | +15

Related CVE's

CVE-20... | CVE-20...

ATT&CK IDs

T1569 -... | T1059 -... | T1102 -... | +31

Lazarus Group

Rank: 6

54.1K	0	12.7K
Audience	News	IOC

Description:

Description of Etda: (Malwarebytes) Lazarus Group is commonly believed to be run by the North Korean government, motivated primarily by financial gain as a...

Target Sectors:

Public Administration - Space & Defense - Energy & Utilities - National Security&International Affairs - Telecommunications - Electrical&Electronical Manufacturi...

Target Countries:

Ban... | Japan | Gua... | +19

Associated Malware/Software

win.... | win.... | Wan... | +143

Related CVE's

CVE-20... | CVE-20... | CVE-20... | +66

ATT&CK IDs

T1059.... | T1505 -... | T1135 -... | +165

APT28

Rank: 15

6.6K	2	1.4K
Audience	News	IOC

Description:

Description of Etda: APT 28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Departmen...

Target Sectors:

Air Transportation - Construction - Public Administration - Educational Services - Energy & Utilities - Automotive - Chemical&Pharmaceutical Manufacturing - National...

Target Countries:

Uzb... | Spain | India | +49

Associated Malware/Software

TCP | xtun... | Dro... | +157

Related CVE's

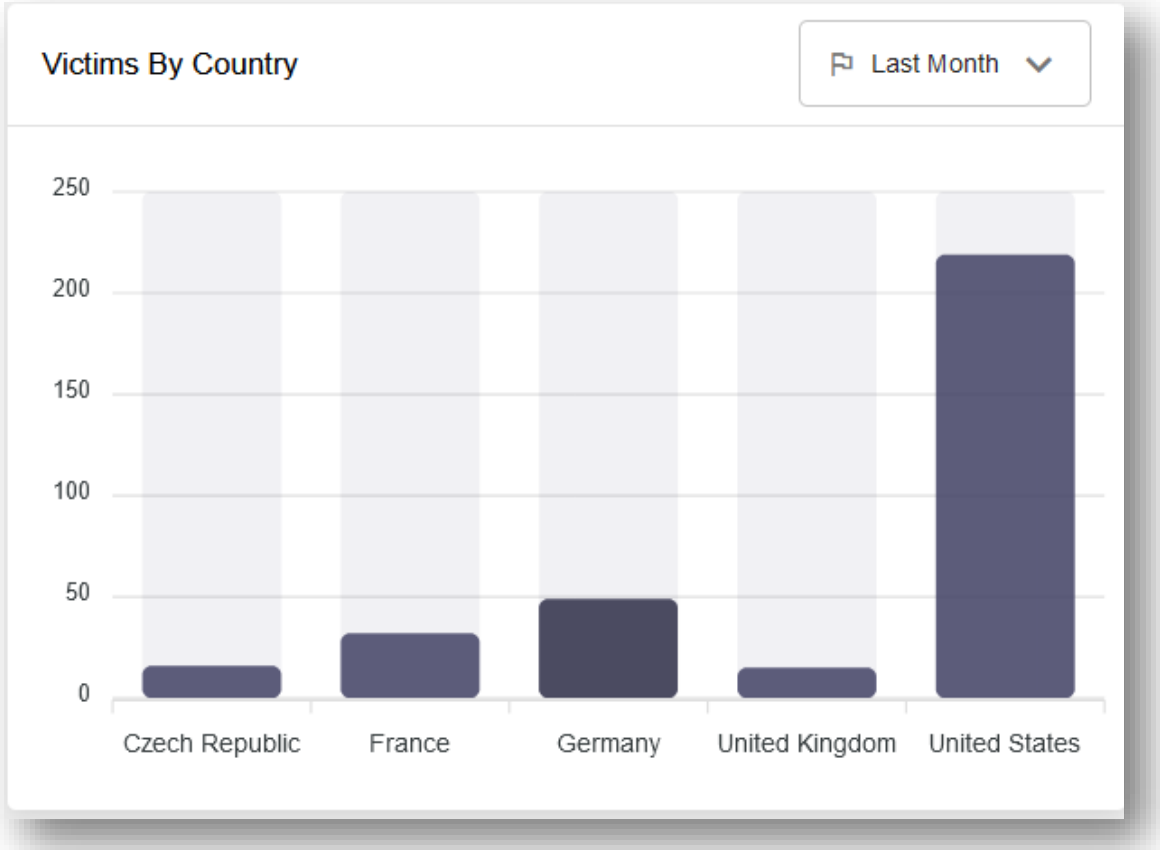
CVE-20... | CVE-20... | CVE-20... | +32

ATT&CK IDs

T1564.... | T1056.... | T1546.... | +139

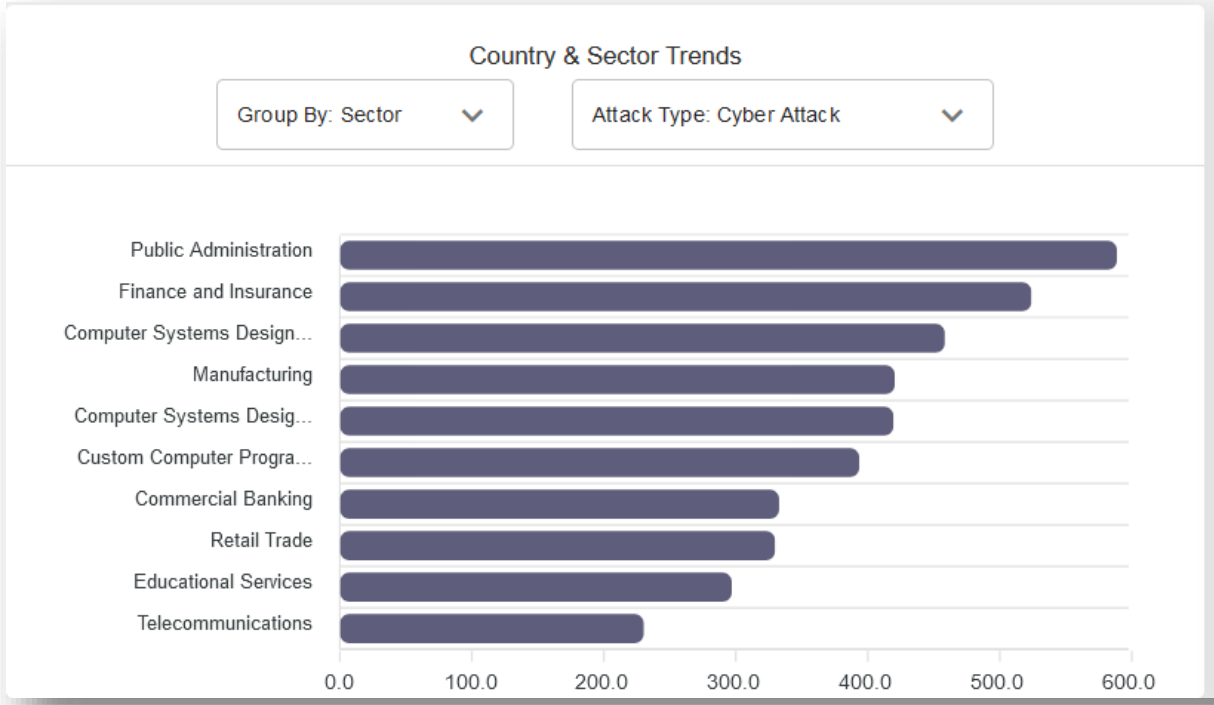
Ransomware Intelligence

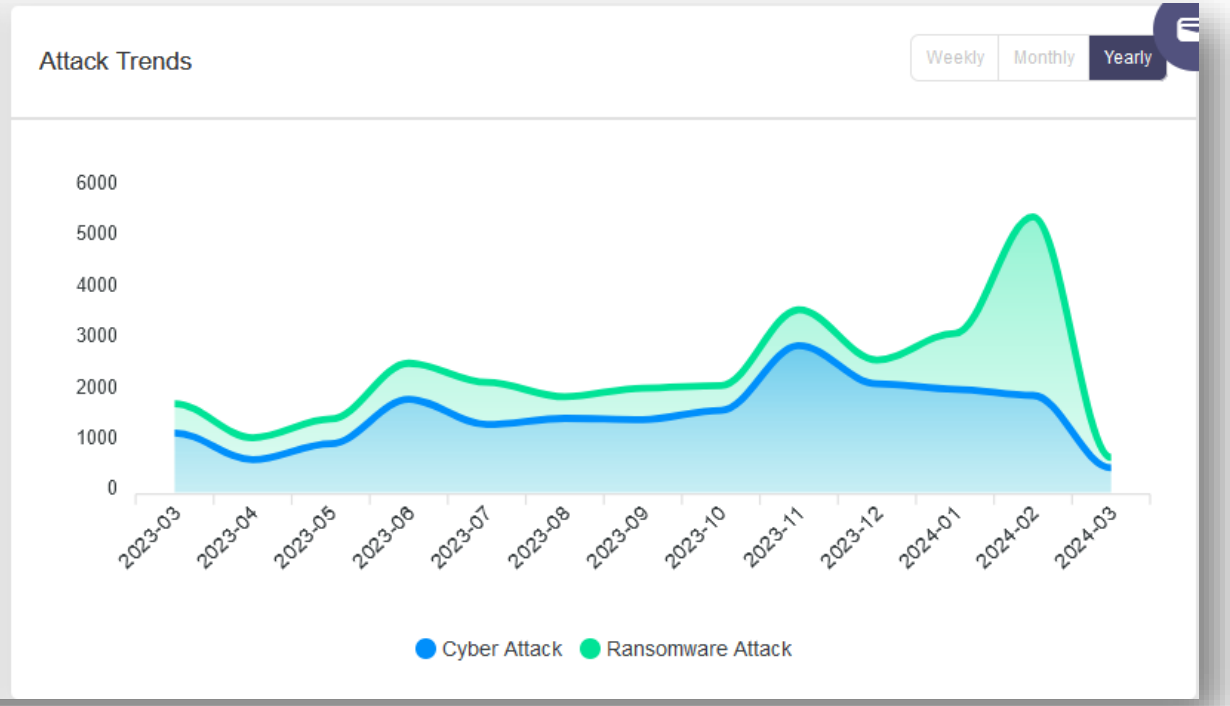
SOCRadar



Global Trends

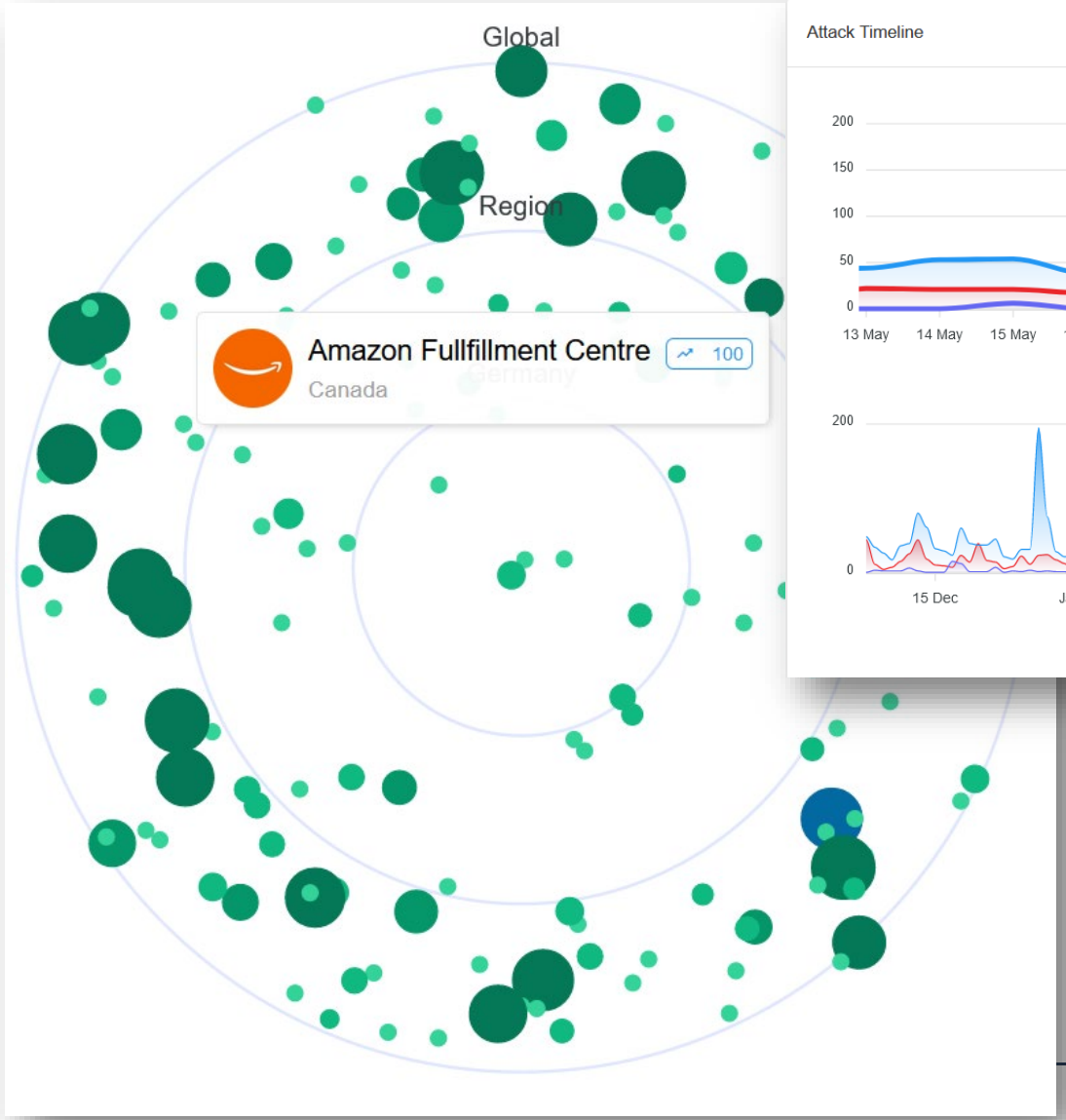
SOCRadar

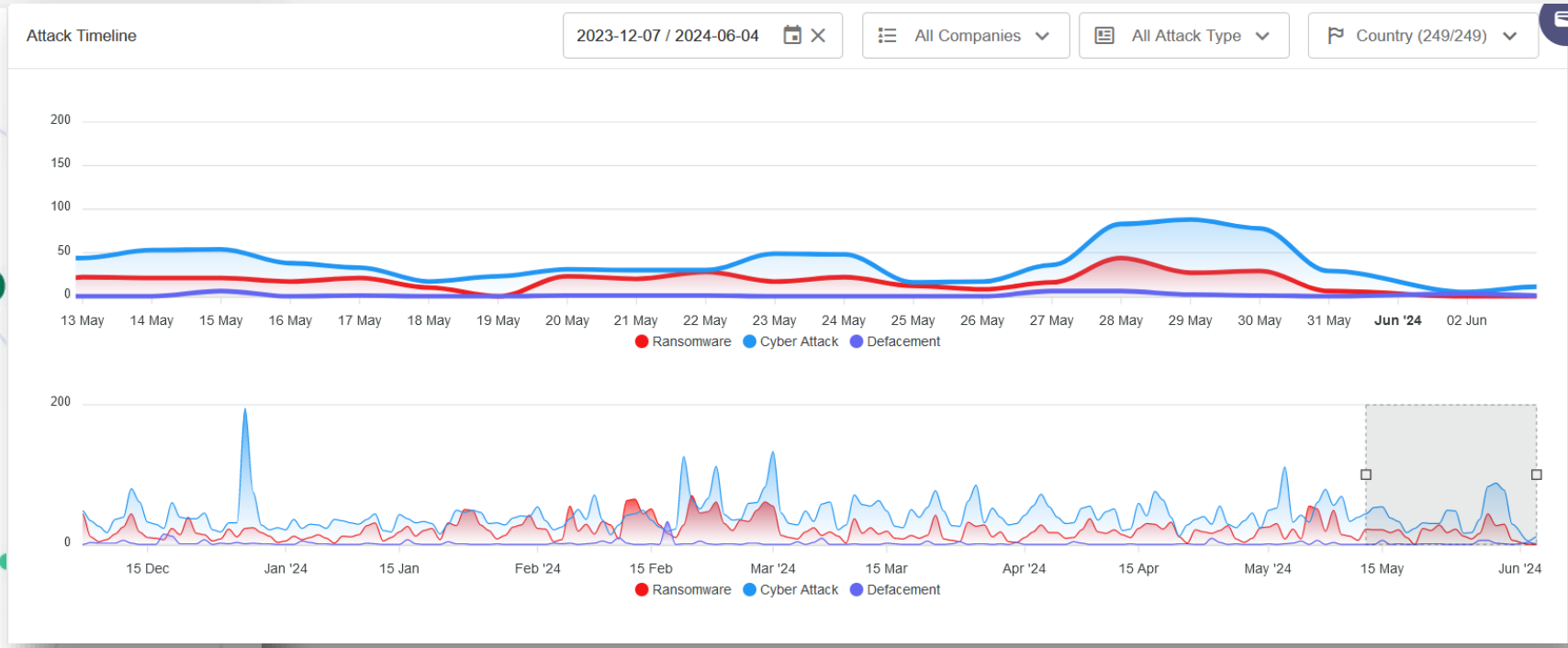




Lieferketten Kontakte und deren Angriffe

FAU Kontakte (SOCRadar)





Ihre Fragen?

Ihre Themen?

Ihre Bedürfnisse?

Backup und mehr?

Wie sichern Sie Ihre Infrastruktur/Daten?

Welche Verfügbarkeiten sind für Sie notwendig?

Asset Management?

Was benötigen Sie?