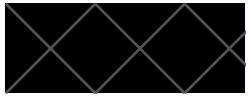
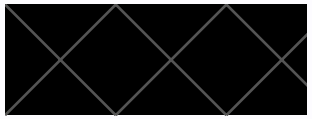
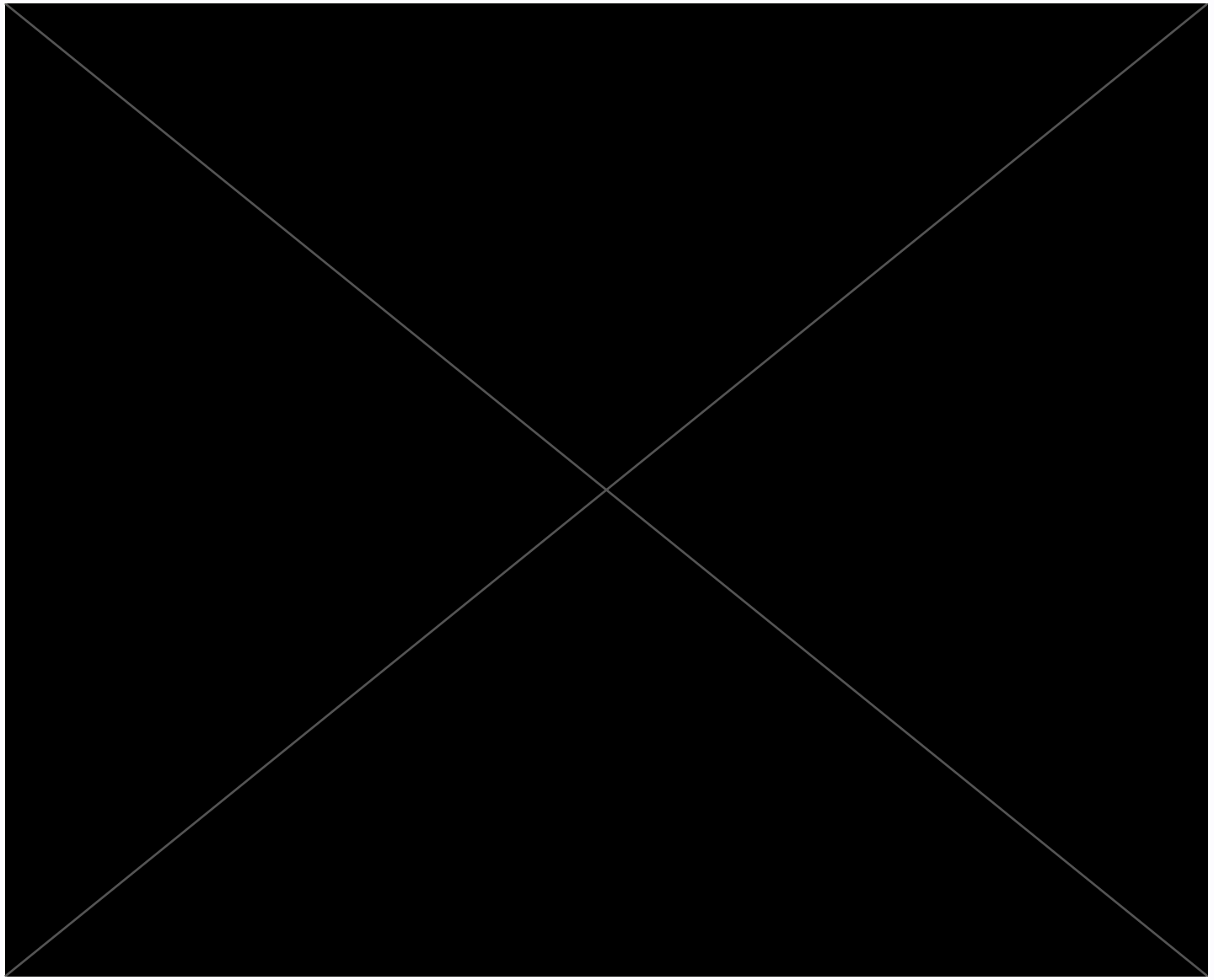
Informationszufluss statt Datenabfluss

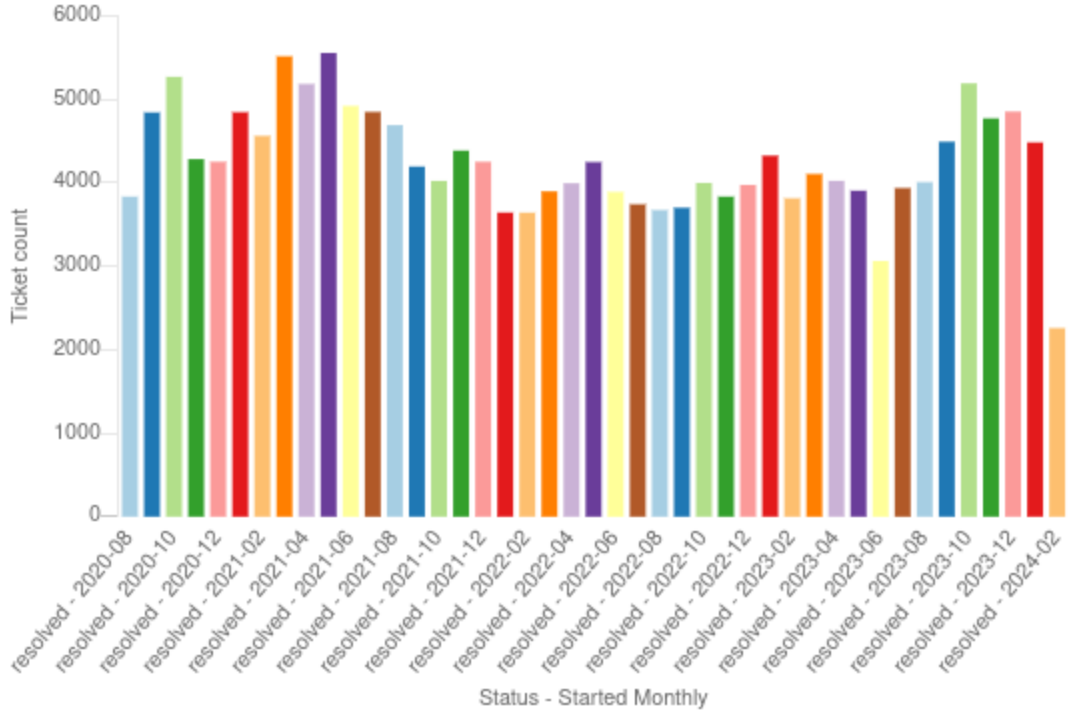
 als Informationsdrehscheibe

- Security Analyst für 
- ~~Digitaler Feuerwehrmann~~
  - Incident Response
- ~~Professioneller Wahrsager~~
  - Fokus auf Strategische Threat Intelligence



Automatisiert

- Informationen zu Sicherheitsproblemen aus verschiedensten Quellen
- Automatisierte Verteilung - via IntelMQ
  - `tech-c`, `abuse-c`, ..
- MiLlIoNeN vOn SiChErHeItsLüCkEn?



Status	Started Monthly	Ticket count
	2020-08	3835
	2020-09	4843
	2020-10	5270
	2020-11	4284
	2020-12	4253
	2021-01	4846
	2021-02	4563
	2021-03	5516
	2021-04	5185
	2021-05	5556
	2021-06	4922
	2021-07	4850
	2021-08	4691
	2021-09	4195

Manuell

- Publikationen auf unserer Webseite
- Mailinglisten
  - Daily, Warning, ..
- Direkter Kontakt - z.B. Responsible Disclosure

Akt I

- "Hidden Champion" in Österreich 🤝 CVE-2022-3759
- Automatische Information per Mail
- Keine Reaktion ..

Warum?

- Technische Probleme mit Abuse-Adressen
  - `/dev/null` kann verlockend sein
- Mangelndes Interesse der Verantwortlichen
- "Halbe Strecke"-Problem

Akt II

[TLP:CLEAR]

$Organisation klopft bei uns an ..

[TLP:CLEAR]

Wir klopfen bei $Firma an ..

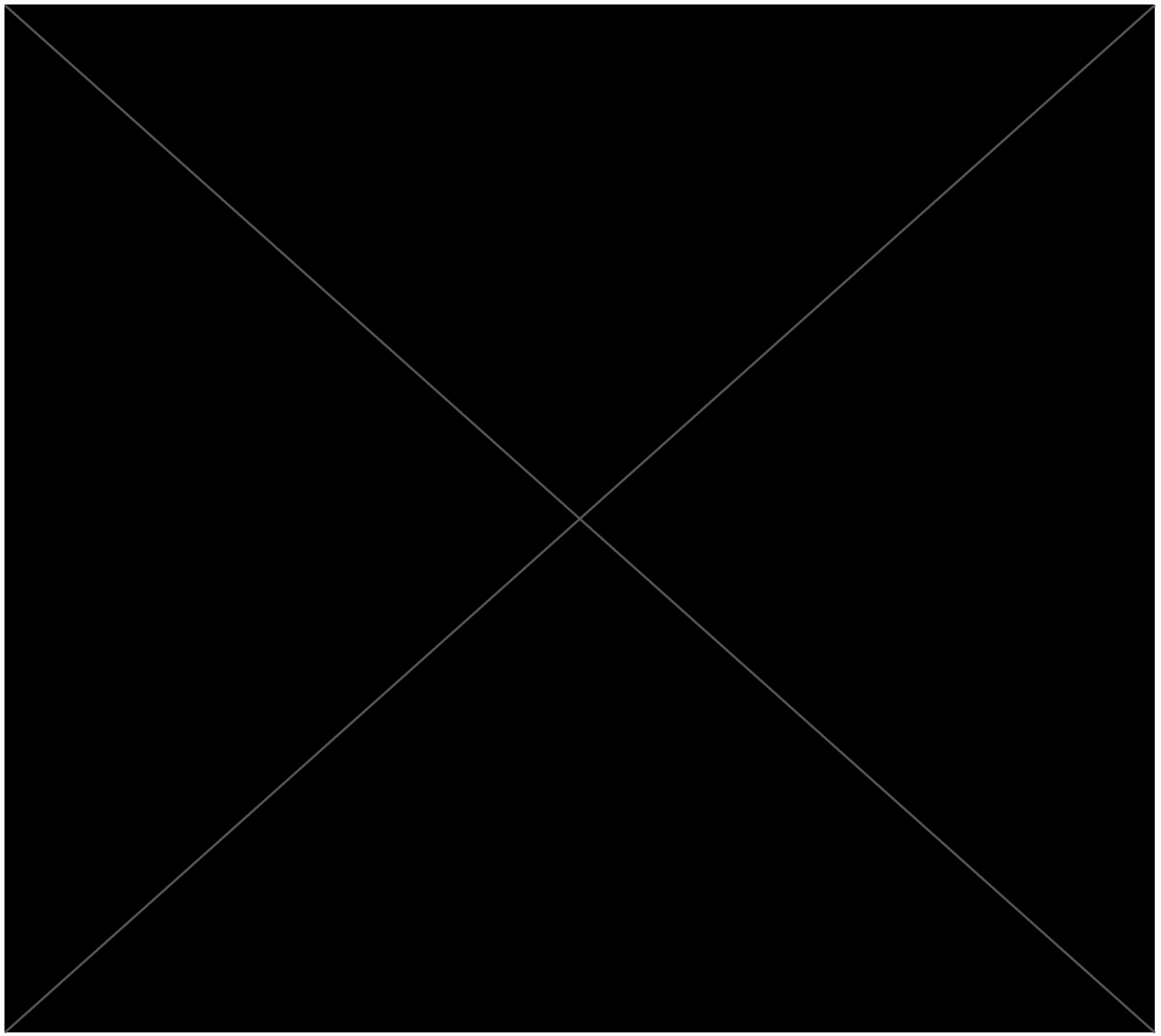
- Direkter Kontakt per Mail: Keine Reaktion
- Direkter Kontakt per Telefon: Keine Reaktion
- Telefonisches Durchhangeln: Spezielle Reaktion

Akt III

[TLP:CLEAR]

$Firma klopft bei uns an ..

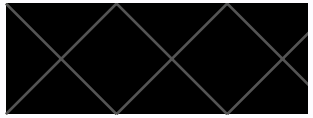
[TLP:CLEAR]



Manchmal hat man Pech ..

- Die Benachrichtigung kam an, der Urlaub dazwischen
- (Zeitliche Korrelation) == Kausalzusammenhang
- Unerwartet motivierter Angreifer

Zusammengefasst

-  ist mehr als nur digitale Feuerwehr
- Wir sind auf Unterstützung angewiesen!
- ~~Urlaubsvertretungen einplanen~~
  - Business Continuity Management!

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?