DENAE | Deutsches Netzwerk für Ausländische Einflussforscher

Aufklärungs- und OSINT-Prioritäten

Einführungsvorlesung

Aufklärungszyklus

Problemstellung und Handlungsplanung

Fristen der Bewertung, Quellenidentifizierung, Budgetierung, Auswahl des Ausführenden oder des Teams

Sammlung und Primärverarbeitung von Informationen

Methoden hängen von der Art der Quellen ab

Analyse der Informationen und Erstellung eines Berichts

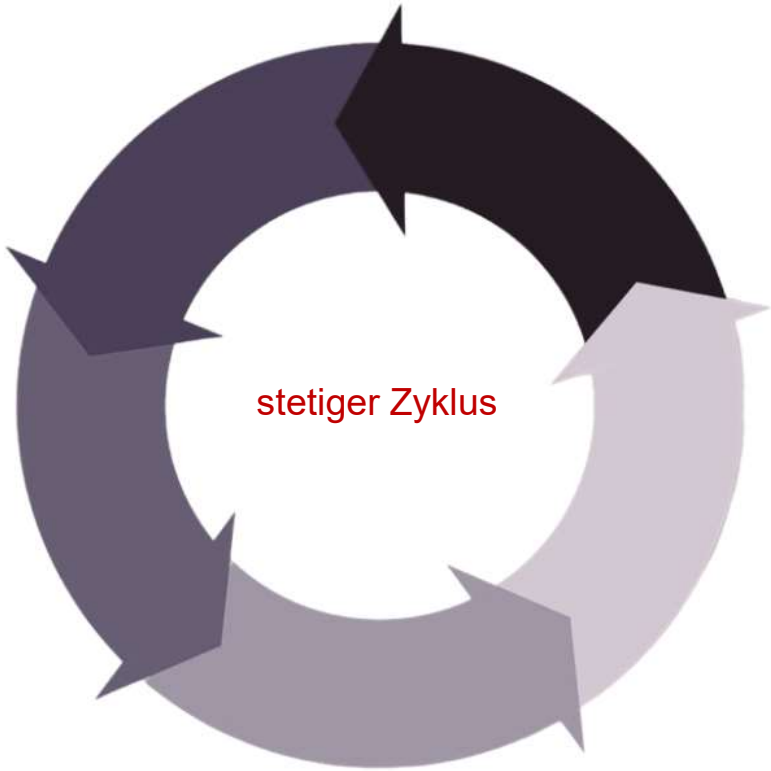
Berichtsformat ist kunden- und aufgabenabhängig

Übermittlung des Berichts

Bereitstellung von Informationen für den Entscheidungsträger

Feedback

Neue Problemstellung oder Überarbeitung der aktuellen Aufgabe



Aufklärungsschwerpunkte

Arten von Informationsquellen

Leute

HumINT (Human Intelligence) – Interview, Umfrage, Verhandlungen, Aufnahmegespräch, Teilnahme an Plattformen für Kommunikation, soziales Ingenieurwesen, Spionagedienst.

Offene Quellen

OSINT (Open Source Intelligence) - Soziale Netzwerke, Messenger, staatliche Register, einschließlich Statistiken, Ausschreibungen und Schiedssprüche, Veröffentlichungen in den Medien usw.

Geografische Daten

GeoINT (Geospatial Intelligence) - Auswertung von Satellitenbildern, Fotos und Videos zur Lokalisierung von Objekten.

Ermittlungstechnik

SigINT (Signals Intelligence) - elektronische Aufklärung im engeren Sinne, MASINT (Measurement and Signature Intelligence) - Erfassung von Informationen über Kameras und Mikrofone.

Historische Hintergründe

Herkunft der Standards

Die Kategorisierung stammt aus dem Interagency Standard des US-Militärs. Der Begriff OSINT wurde in den USA Ende der 1980er Jahre im Zusammenhang mit der Reform der Nachrichtendienste geprägt.

- HumINT stand im Einklang mit den Aufgaben der CIA (Central Intelligence Agency, CIA)
- SigINT- stand im Einklang mit den Aufgaben der Nationalen Sicherheitsbehörden (National Security Agency, NSA)
- GeoINT- stand im Einklang mit den Aufgaben der Nationalen Agentur für Geospatiale Aufklärung (National Geospatial-Intelligence Agency, NGA), usw.

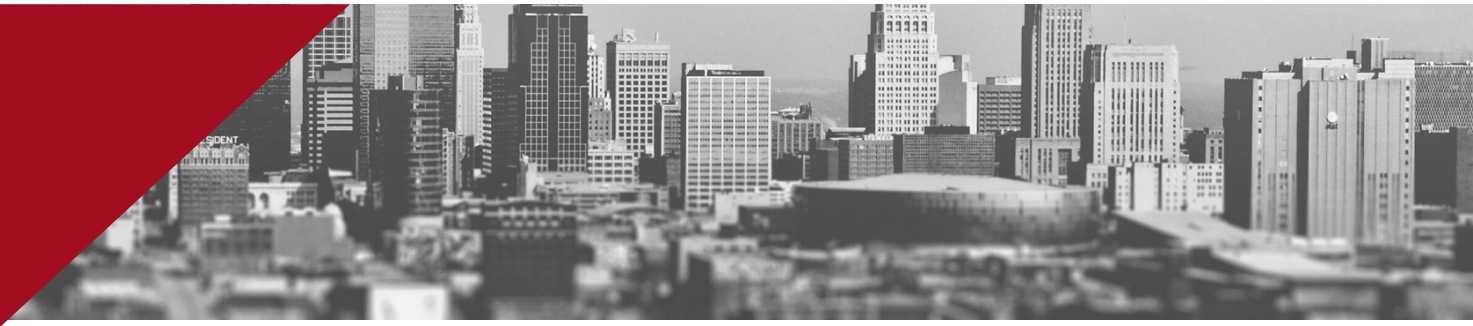
Früher

HumINT, SigINT und GeoINT sind die drei Hauptbereiche des Informationsbeschaffung.

Jetzt

HumINT, SigINT und GeoINT veredeln und ergänzen Open-Source-Daten mit OSINT-Methoden

Weitere Spezialisierung



- SocmINT (Social Media) - Arbeit mit sozialen Netzwerken, Monitoring und Analyse
- FinINT (financial) - Finanzermittlungen einschließlich Aufklärungen zu Kryptowährungen
- TechINT (technical) - Wissenschaftliche und technische Aufklärung (Militärtechnik)
- AdINT (advertising) - Erfassung über die IDs von Werbung in Suchmaschinen und sozialen Netzwerken
- LeakINT (lecks) - Intelligenz in der Leckage-Datei

DENAE

OSINT (Open-Source Intelligence)

Wichtige OSINT-Fragen

Wo suchen?

Welche Quellen nutzen wir?

Offene Quellen
Soziale Netzwerke, Messenger, offene Daten aus staatliche Register, einschließlich Statistiken, Ausschreibungen Schiedssprüche, Veröffentlichungen in den Medien, wissenschaftliche Forschung, soziale Umfragen, Bibliotheken, Archive.

Wie man sucht?

Welche Tools?

Tools
Web- oder mobile Anwendungen, On-Premise-Software, Cloud-Lösungen, usw.

DENAE

Auswahl der Arbeitstools

Alles ausprobieren, eigene Serviceliste erstellen

Sehr arbeitsintensiv und nicht immer gerechtfertigt.

Empfohlene Services nutzen

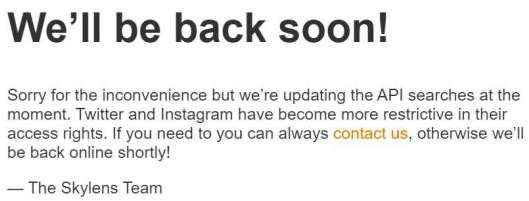
Spart Zeit und Geld.

Jede Richtung der Aufklärung setzt Teamarbeit voraus. Jeder Teilnehmer ist auf seinen Bereich spezialisiert und erstellt sein eigene Serviceliste.

OSINT Beschränkungen

Nicht für jedes Problem ist OSINT eine Lösung

- Ein Übermaß an unzuverlässigen und veralteten Informationen. Es wird der Begriff Validated OSINT, OSINT-V, eingeführt, der eine Kategorie von Informationen mit hohem Vertrauensgrad bezeichnet, die von einem Spezialisten auf der Grundlage der Ergebnisse der Analyse und Validierung aller verfügbaren Quellen bereitgestellt werden.
- Die Staaten schränken den freien Zugang zu Informationen ein.
- IT-Unternehmen schränken die Überwachungsmöglichkeiten ein: Twitter, Instagram und Facebook beschränken den Zugang zu APIs, was die automatische Überwachung und Analyse



- Regionsspezifische rechtliche Beschränkungen: Das Speichern von Datenbanken mit Lücken birgt rechtliche Risiken und zwingt die Analysten zu Aktivitäten in einer unsicheren „Grauzone“.
- Risiken bei der Kompromittierung von Ermittlungen oder Kunden - Systeme erfassen Benutzeranfragen und einige Dienste benachrichtigen Objekte über die Erfüllung von Anfragen. Dies erfordert einige Anstrengungen zur Wahrung der Vertraulichkeit.