BWI

IT für Deutschland

# Steckbrief

## Rukhsar & Yusuf Khan (Vater & Sohn)

- Dienstleister und externe Berater im Auftrag der BWI
- Firma: IdoubleS (https://www.idoubles.net)
- Rukhsar: CEO und Trusted Cyber Security Advisor
- Yusuf: CTO und Senior Cyber Security Consultant
- Kontakt: rukhsar.khan@idoubles.net & yusuf.khan@idoubles.net

**#gerneDu**



Bildquelle: BWI/Fotodatenbank

20. Januar 2026

# … where the skies are so blue … *

* Lynyrd Skynyrd – Sweet Home Alabama

Bildquelle: Manfred Rinderspacher, Mannheimer Morgen
https://www.mannheimer-morgen.de/fotos_fotostrecke,-fotostrecke-auffaellige-kondensstreifen-am-himmel-der-region-_mediagalid,37591.html

# … where the skies are so blue (and the governor's, too)*

* Lynyrd Skynyrd – Sweet Home Alabama

- Was für ein Flugobjekt hat dieses Artefakt verursacht? [Art]
- Wer besitzt diese Art von Flugobjekt? [Akteur]
- Was können diese Modelle [Fähigkeiten]
  - Welche Reichweite?
  - Welche Optik?
  - Welche Waffensysteme?
  - […]
- Von wo starten diese Flugobjekte? [Ursprung]
- Wohin könnte das Flugobjekt unterwegs sein? [Ziel]
- Gibt es bekannte Schwachstellen auf diese Flugobjekte [Verteidigungsvektoren]
- […]

- **Wen haben wir wie zu informieren? Welche Details werden benötigt?**

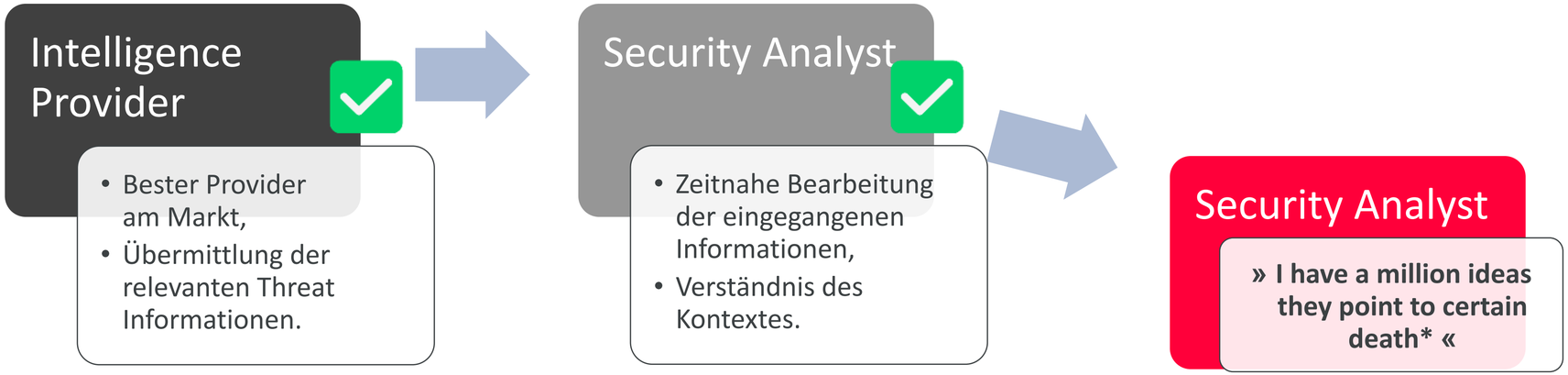
Bildquelle: Manfred Rinderspacher, Mannheimer Morgen
https://www.mannheimer-morgen.de/fotos_fotostrecke,-fotostrecke-auffaellige-kondensstreifen-am-himmel-der-region-_mediagalid,37591.html

# Cyber Threat Management @ BWI

## Es ist nicht genug zu »wissen«, man muss es auch »anwenden«

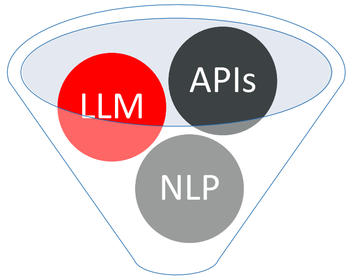
Bildquelle: BWI

# Experience: Threat Intel done wrong…



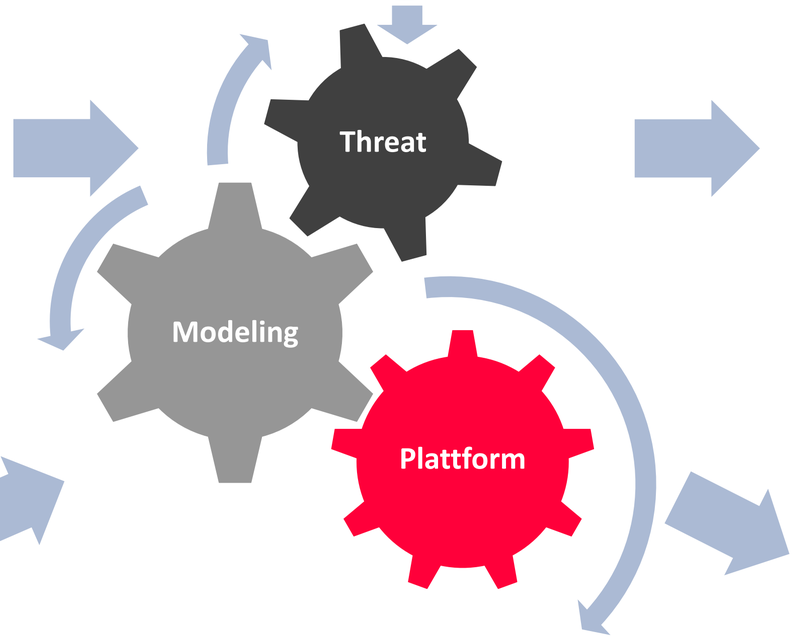

* Douglas Adams – Per Anhalter durch die Galaxis

# Vision: „Threat Intel done right…“




**Intelligence Provider**

- Bester Provider am Markt,
- Übermittlung der relevanten Threat Informationen.




**Incident Responder**

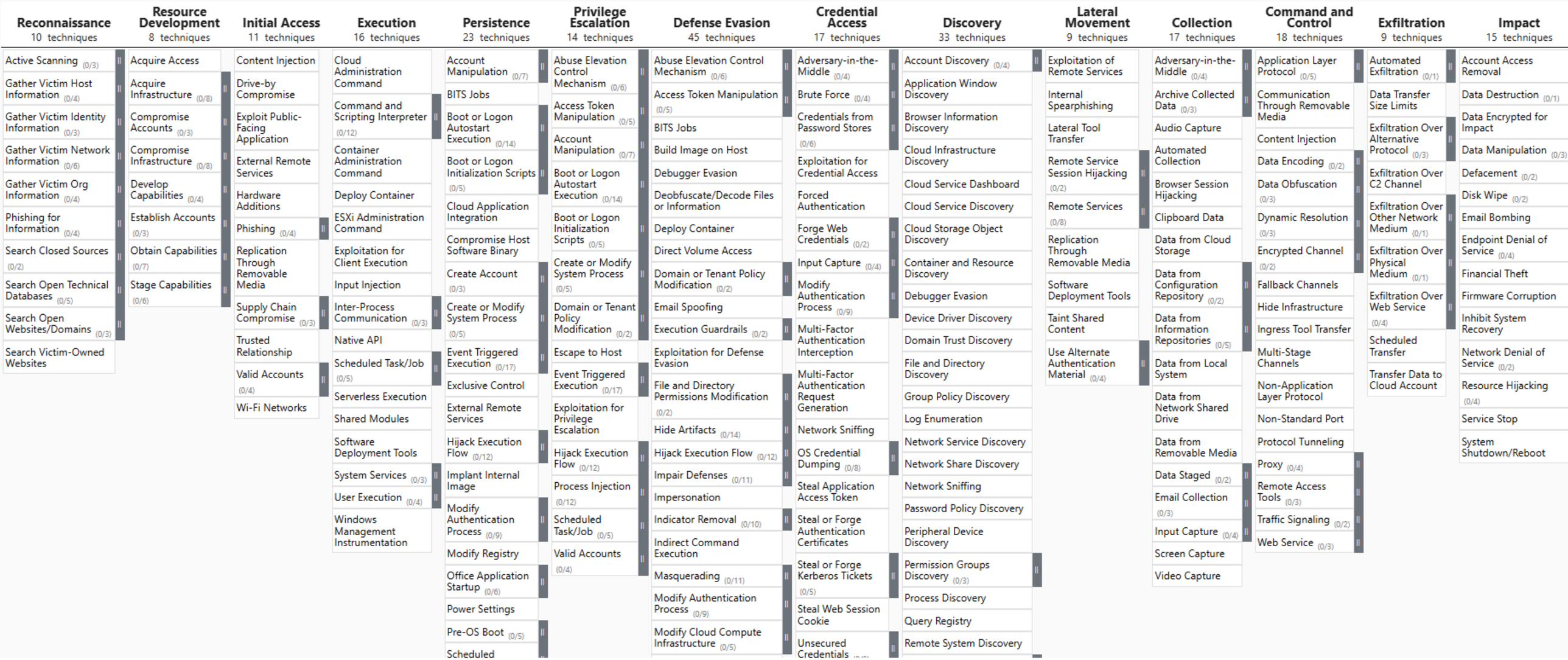
- Verknüpfung mit konkreten Incident Informationen aus BWI- und Bw-Btrb.

**Security Analyst**

- Zeitnahe Bearbeitung der eingegangenen Informationen.
- Anreicherungen mit weiteren Kontextinfos.

- ✓ Indicators of Compromise (IoC)
- ✓ generierte SIEM-Detektionsregeln
- ✓ Zero Trust Bewertungen (PEP/PDP)
- ✓ CVE für Schwachstellen-Mgmt.
- ✓ MITRE ATT&CK-Graphen
- ✓ Befähigung „Threat Hunting“
- ✓ Attribution
- ✓ …

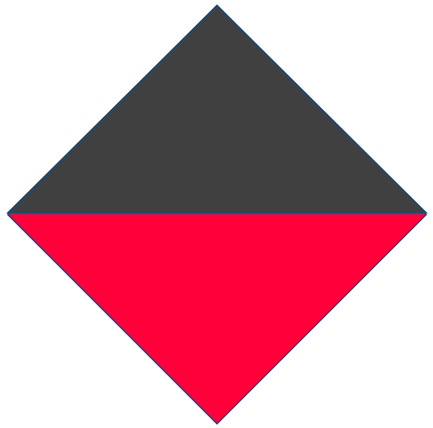
# Exkurs: MITRE ATT&CK



# Threat Modeling Platform
# Diamond Model

**Threat Actor** [z.B. APT28]

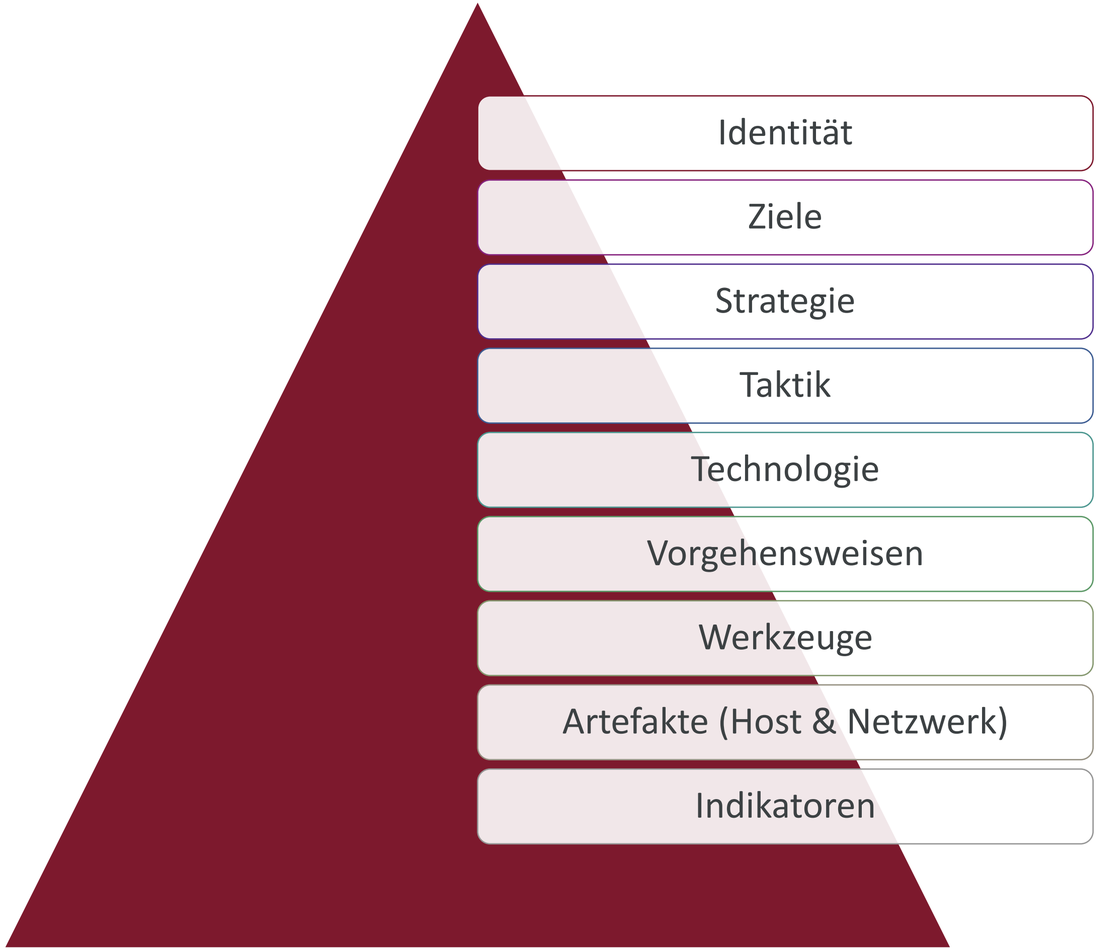
**Infrastructure** [z.B. C2]

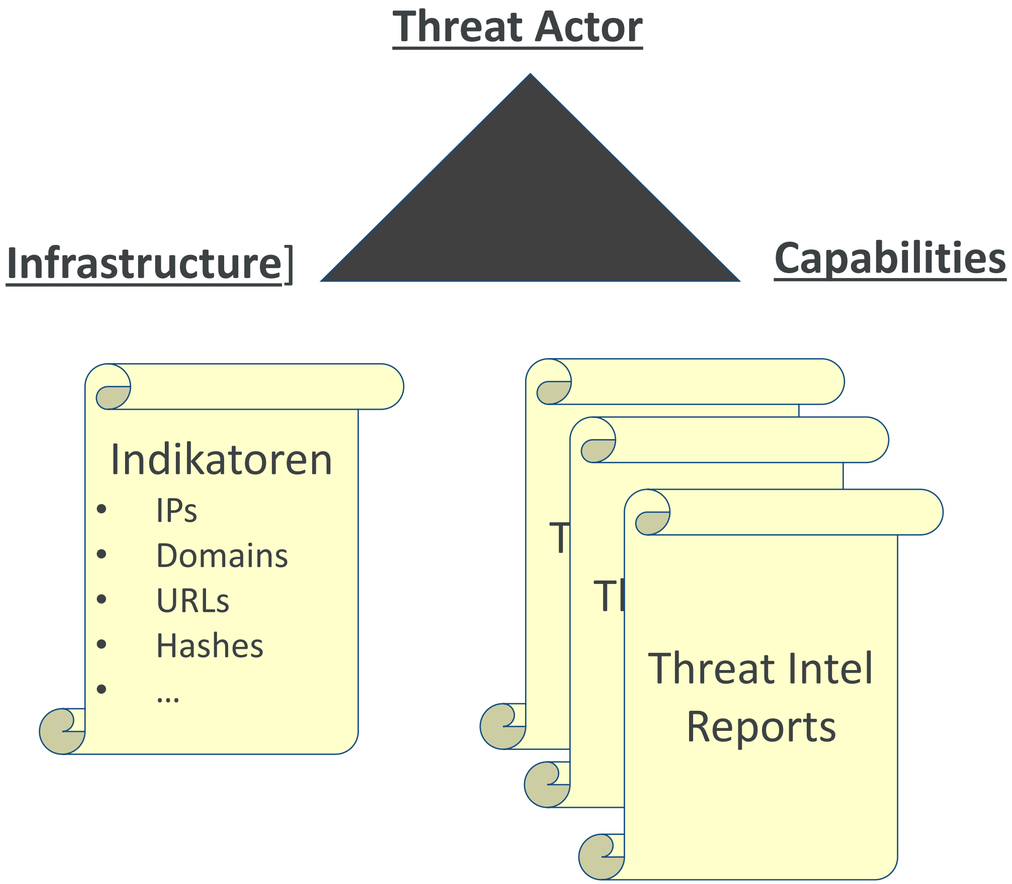


**Capabilities** [z.B. Zero Days, DDoS]

**Victim** [kritische Services & Funktionen]

# Threat Modeling Platform
# Detection Maturity Level (DML)



# Validierungsszenarien, Projektmeilensteine 2025

- Deployment der IdoubleS-Plattform in einer relevanten Umgebung (Testumgebung/Labor) bei BWI
- Beginn der Pilotierung während der Beta-Entwicklungsphase. Im Rahmen von Testversion 1.1 wurden folgende Aktivitäten durchgeführt:
  - Testszenario 1, Q3/2025: Priorisierung relevanter Bedrohungsakteure und Bedrohungs-Szenarien
  - Testszenario 2, Q4/2025: Automatisierte, bedrohungszentrische Cyber Threat Modellierung

# IdoubleS Plattformdemo und Validierungsergebnisse

- Bedrohungszentrische Plattformdemo
- Validierungsergebnisse Testszenario 2
  - Automatisierte, bedrohungszentrische Cyber Threat Modellierung
  - Aufbau einer Baseline
  - Prüfen von automatisierten Ergebnissen gegen die Baseline
  - Ermitteln der Genauigkeit (Accuracy) von AI/NLP

# IdoubleS Community Maßnahmen

- **Webinar**: Intelligence-driven Threat Hunting for improving SOC maturity level (Webinar: Intelligence-driven Threat Hunting for improving SOC maturity level - IdoubleS resources)
- **Cyber Threat Modelling by leveraging an open-source attack graph and activity thread graph tool** (https://www.idoubles.net/resources/cyber-threat-modelling-by-leveraging-open-source-attack-graph-and-activity-thread-graph-tool)
- Bei Rückfragen sind wir gerne über rukhsar.khan@idoubles.net und yusuf.khan@idoubles.net für euch erreichbar!

# Herzlichen Dank für eure Aufmerksamkeit!

Bildquelle: BWI