



**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](mailto:rukhsar.khan@idoubles.net) & [yusuf.khan@idoubles.net](mailto:yusuf.khan@idoubles.net)

#gerneDu

... where the skies are so blue ...\*

\* Lynyrd Skynyrd – Sweet Home Alabama

# ... 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?**

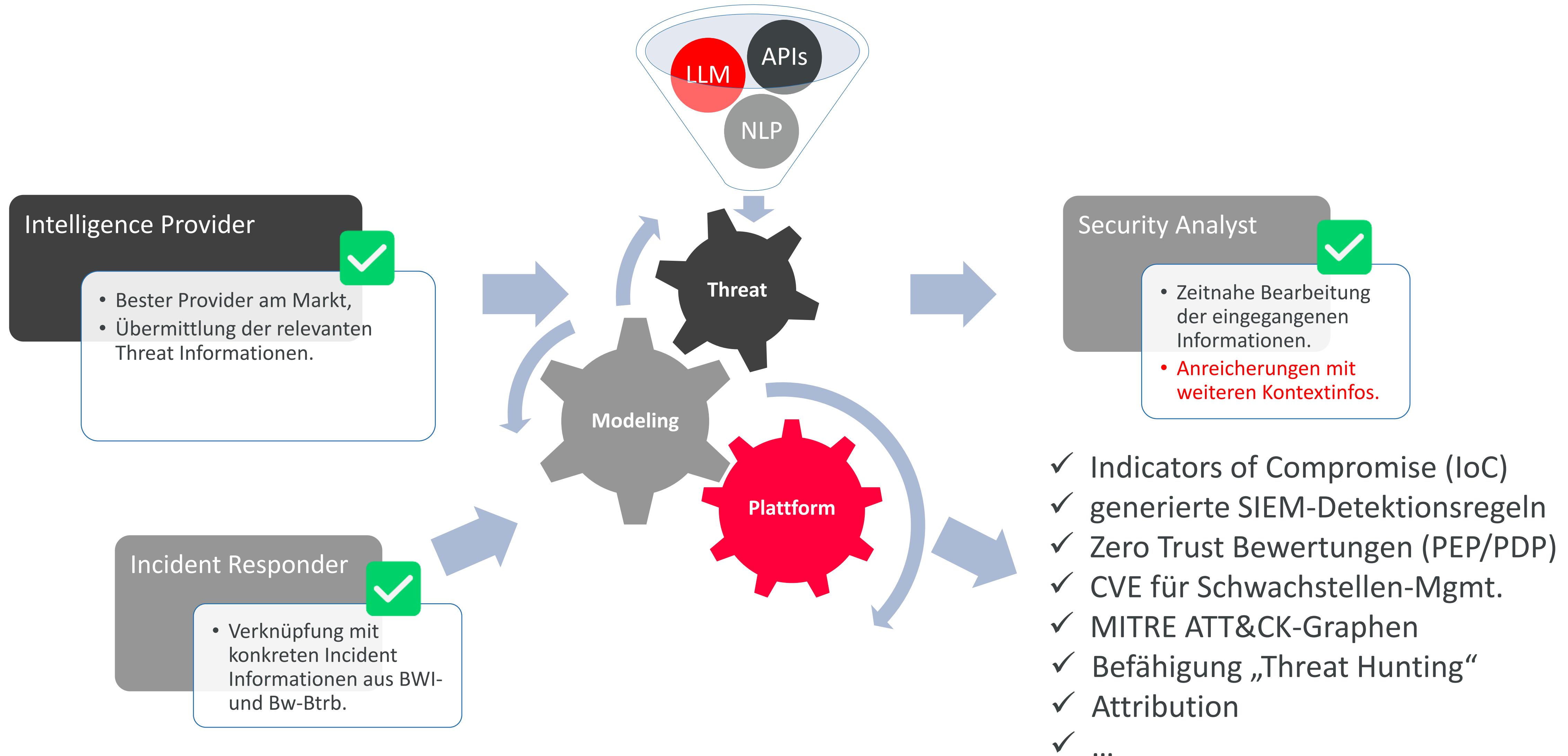
# Cyber Threat Management @ BWI

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

# Experience: Threat Intel done wrong...



# Vision: „Threat Intel done right...“

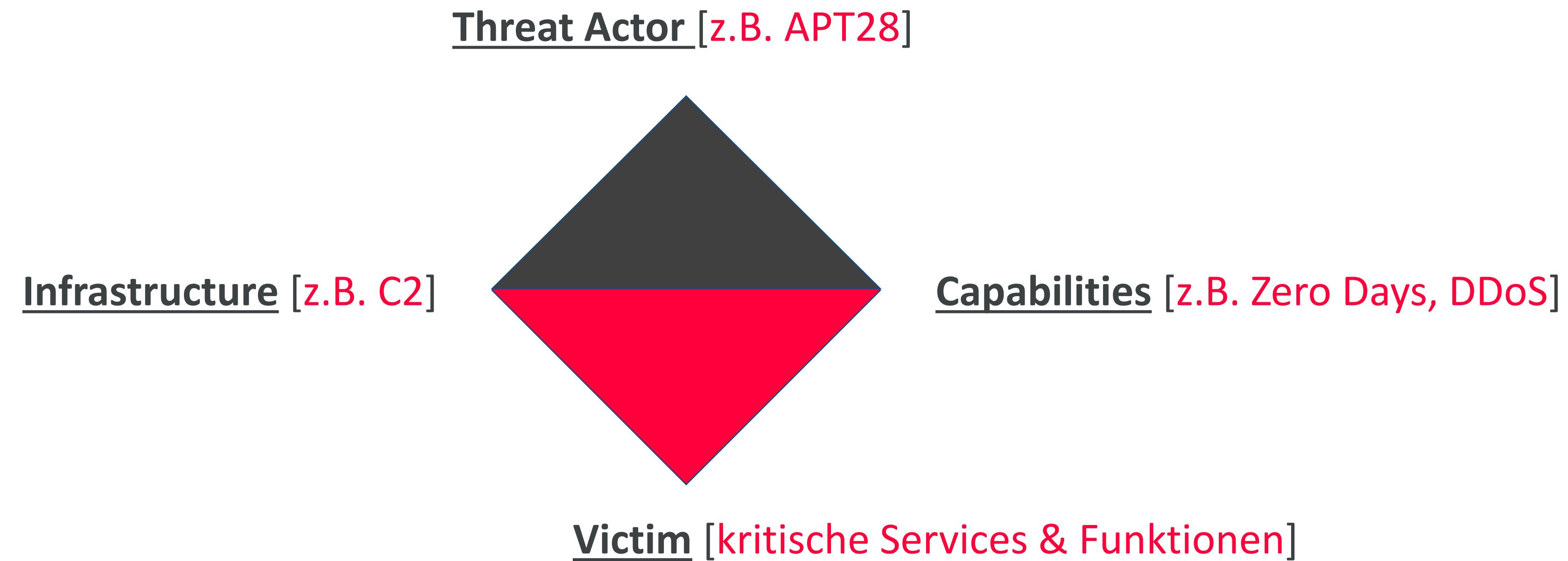


# Exkurs: MITRE ATT&CK

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	11 techniques	16 techniques	23 techniques	14 techniques	45 techniques	17 techniques	33 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/4)	Application Layer Protocol (0/5)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (0/1)	
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Command and Scripting Interpreter (0/12)	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/7)	BITS Jobs	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Automated Collection	Data Encoding (0/2)	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Deploy Container	Cloud Application Integration	Boot or Logon Autostart Execution (0/14)	Debugger Evasion	Deobfuscate/Decode Files or Information	Cloud Service Dashboard	Remote Service Session Hijacking (0/2)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	ESXi Administration Command	Compromise Host Software Binary	Boot or Logon Initialization Scripts (0/5)	Deploy Container	Forced Authentication	Cloud Service Discovery	Remote Services (0/8)	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Email Bombing
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replication Through Removable Media	Exploitation for Client Execution	Create Account (0/3)	Create or Modify System Process (0/5)	Direct Volume Access	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage	Endpoint Denial of Service (0/4)	Financial Theft	
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Input Injection	Input Injection	Inter-Process Communication (0/3)	Create or Modify System Process (0/5)	Domain or Tenant Policy Modification (0/2)	Input Capture (0/4)	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Web Service (0/4)	Firmware Corruption
Search Open Websites/Domains (0/3)	Supply Chain Compromise (0/3)	Native API	Native API	Domain or Tenant Policy Modification (0/2)	Email Spoofing	Execution Guardrails (0/2)	Modify Authentication Process (0/9)	Debugger Evasion	Taint Shared Content	Data from Information Repositories (0/5)	Hide Infrastructure	Inhibit System Recovery	
Search Victim-Owned Websites	Trusted Relationship	Scheduled Task/Job (0/5)	Event Triggered Execution (0/17)	Event Triggered Execution (0/17)	Escape to Host	Execution Guardrails (0/2)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (0/4)	Ingress Tool Transfer	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (0/2)
	Valid Accounts (0/4)	Serverless Execution	Exclusive Control	Exclusive Control	Exploitation for Defense Evasion	File and Directory Permissions Modification (0/2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery	Data from Local System	Non-Application Layer Protocol	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking (0/4)
	Wi-Fi Networks	Shared Modules	External Remote Services	External Remote Services	Exploitation for Privilege Escalation	Hide Artifacts (0/14)	Network Sniffing	File and Directory Discovery	Data from Network Shared Drive	Protocol Tunneling	Protocol Staging (0/2)	Service Stop	System Shutdown/Reboot
		Software Deployment Tools	Hijack Execution Flow (0/12)	Hijack Execution Flow (0/12)	Hijack Execution Flow (0/12)	Impair Defenses (0/11)	OS Credential Dumping (0/8)	Group Policy Discovery	Data from Removable Media	Proxy (0/4)	Remote Access Tools (0/3)	Traffic Signaling (0/2)	
		System Services (0/3)	Implant Internal Image	Process Injection (0/12)	Impersonation	Impersonation	Steal Application Access Token	Log Enumeration	Data from Network Shared Drive	Data Staged (0/2)	Email Collection (0/3)	Web Service (0/3)	
		User Execution (0/4)	Modify Authentication Process (0/9)	Scheduled Task/Job (0/5)	Indicator Removal (0/10)	Indicator Removal (0/10)	Steal or Forge Authentication Certificates	Network Service Discovery	Data from Removable Media	Input Capture (0/4)	Screen Capture		
		Windows Management Instrumentation	Modify Registry	Valid Accounts (0/4)	Indirect Command Execution	Masquerading (0/11)	Steal or Forge Kerberos Tickets (0/5)	Network Share Discovery	Peripheral Device Discovery	Permission Groups Discovery (0/3)	Video Capture		
			Office Application Startup (0/6)		Power Settings	Modify Authentication Process (0/9)	Steal Web Session Cookie	Network Sniffing	Process Discovery	Process Discovery			
			Pre-OS Boot (0/5)		Scheduled	Modify Cloud Compute Infrastructure (0/5)	Unsecured Credentials	Query Registry	Query Registry	Query Registry			
								Remote System Discovery	Remote System Discovery	Remote System Discovery			

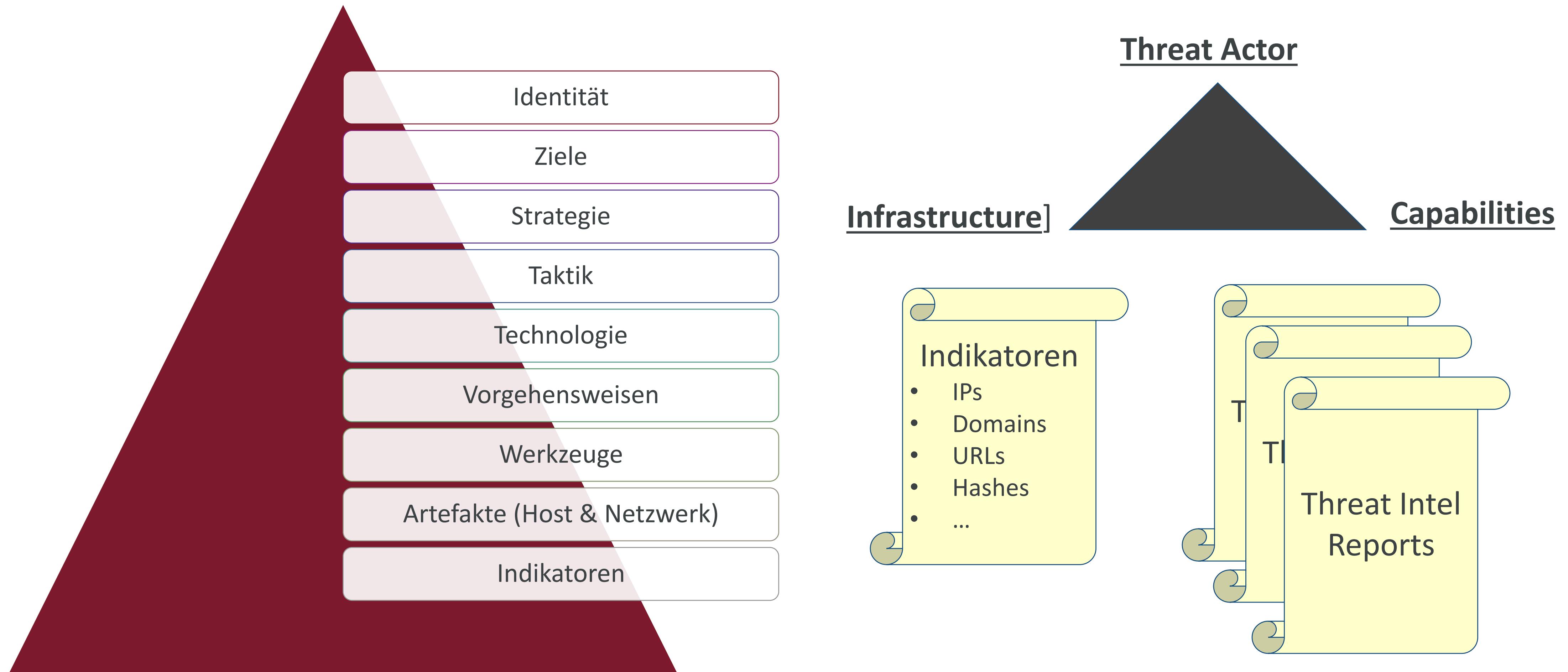
# Threat Modeling Platform

## Diamond Model



# 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 Bedrohungakteure 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](mailto:rukhsar.khan@idoubles.net) und [yusuf.khan@idoubles.net](mailto:yusuf.khan@idoubles.net) für euch erreichbar!

# Herzlichen Dank für eure Aufmerksamkeit!