



BWI

IT für Deutschland

Steckbrief

Rukhsar & Yusuf Khan (Vater & Sohn)



#gerneDu

- 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

... 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?**

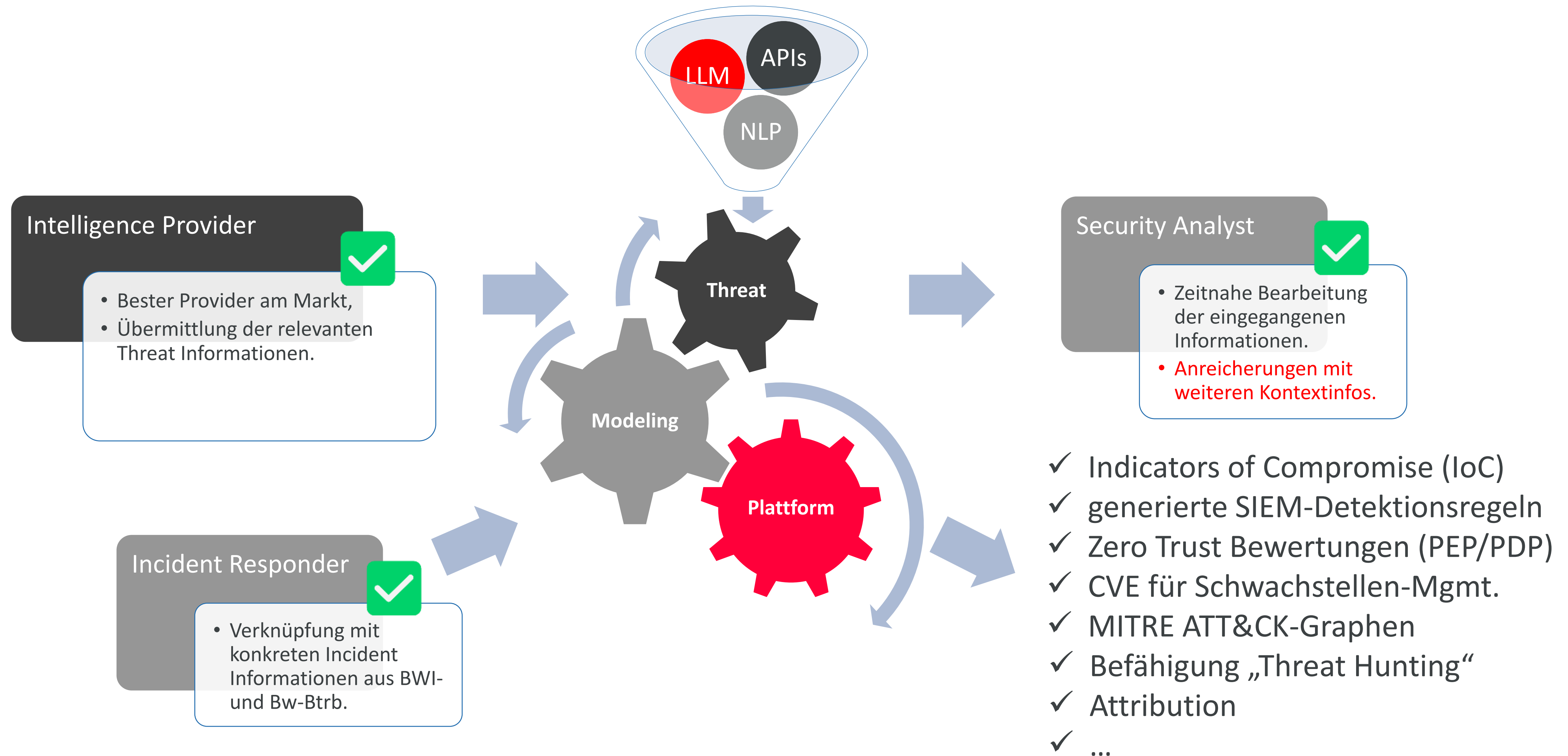
Cyber Threat Management @ BWI

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

Experience: Threat Intel done wrong...



Vision: „Threat Intel done right...“

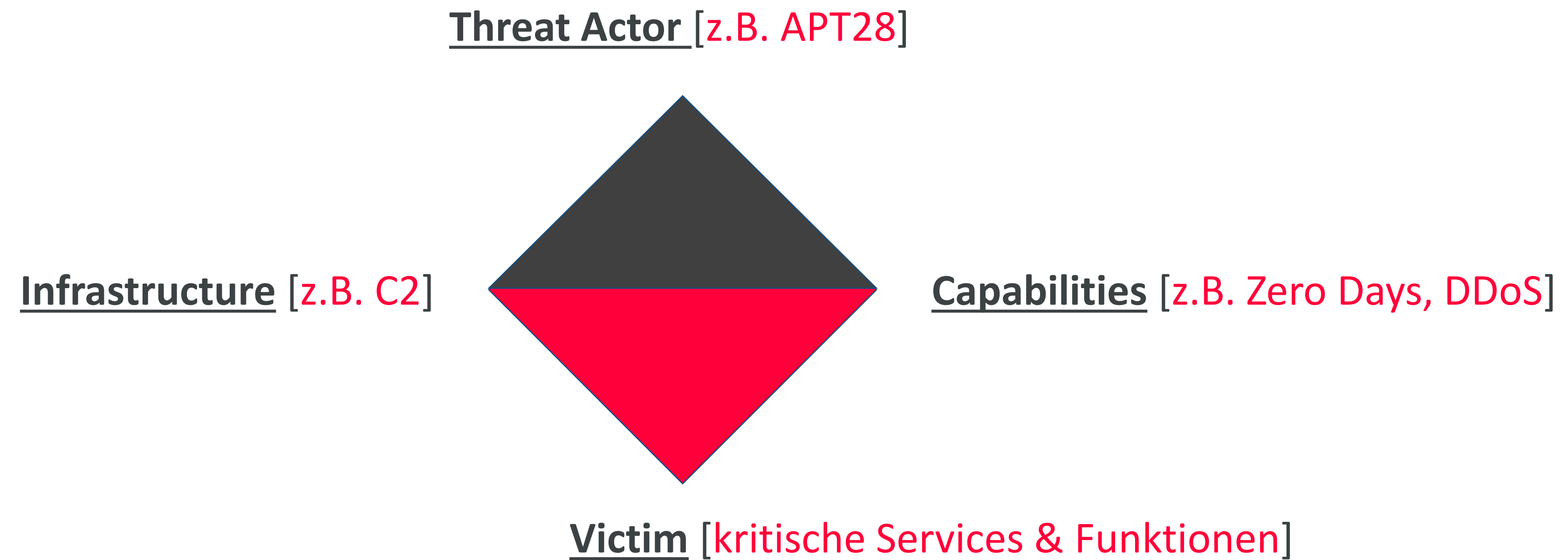


Exkurs: MITRE ATT&CK

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

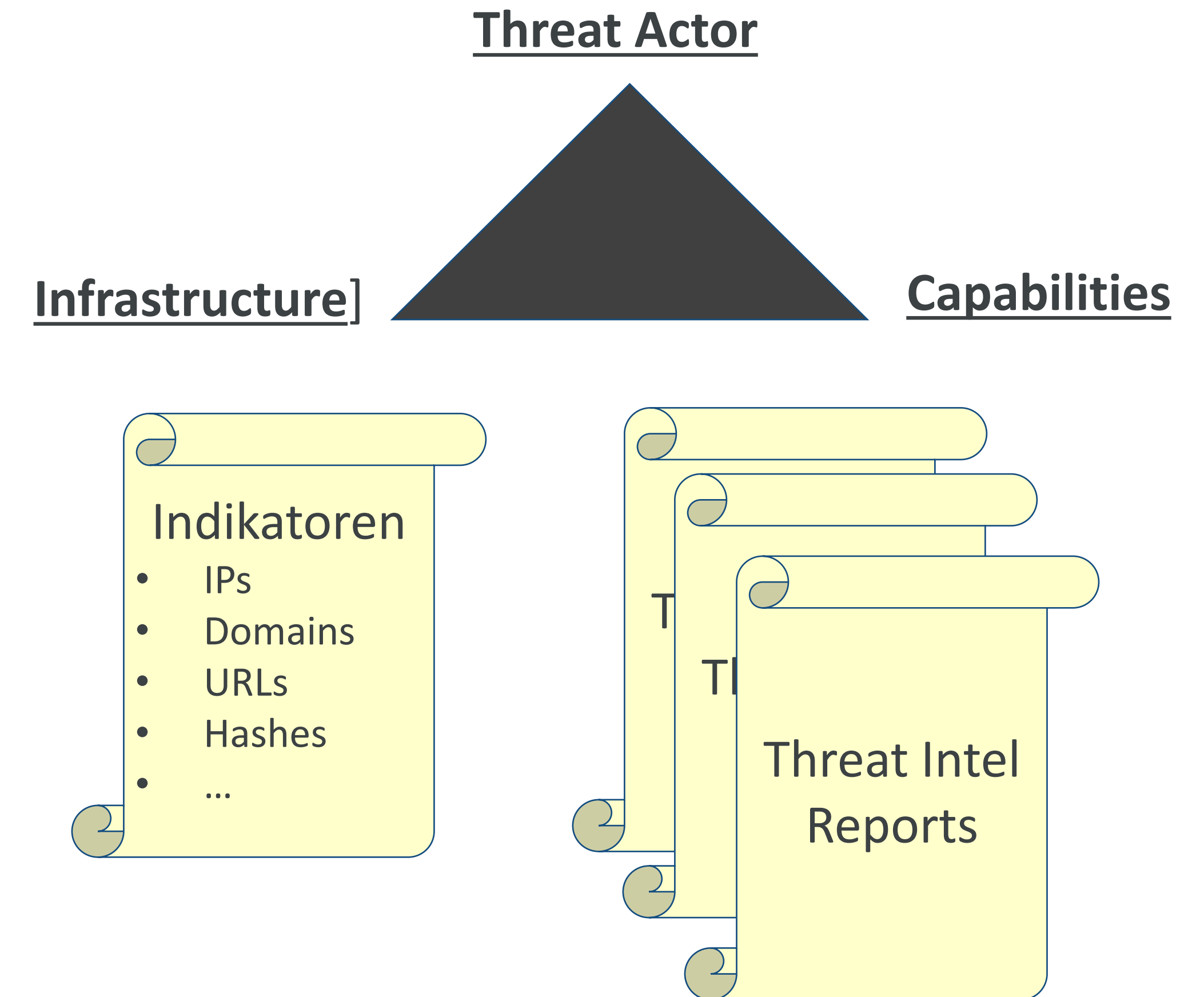
Threat Modeling Platform

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 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!