DCSO

WebCast

Qualität und Schnelligkeit

Wie kann ich Indikatoren und technische Threat Intelligence effizient integrieren?

Thomas Hemker, CISSP, CISM, CISA, CDPSE

Christoph Lobmeyer

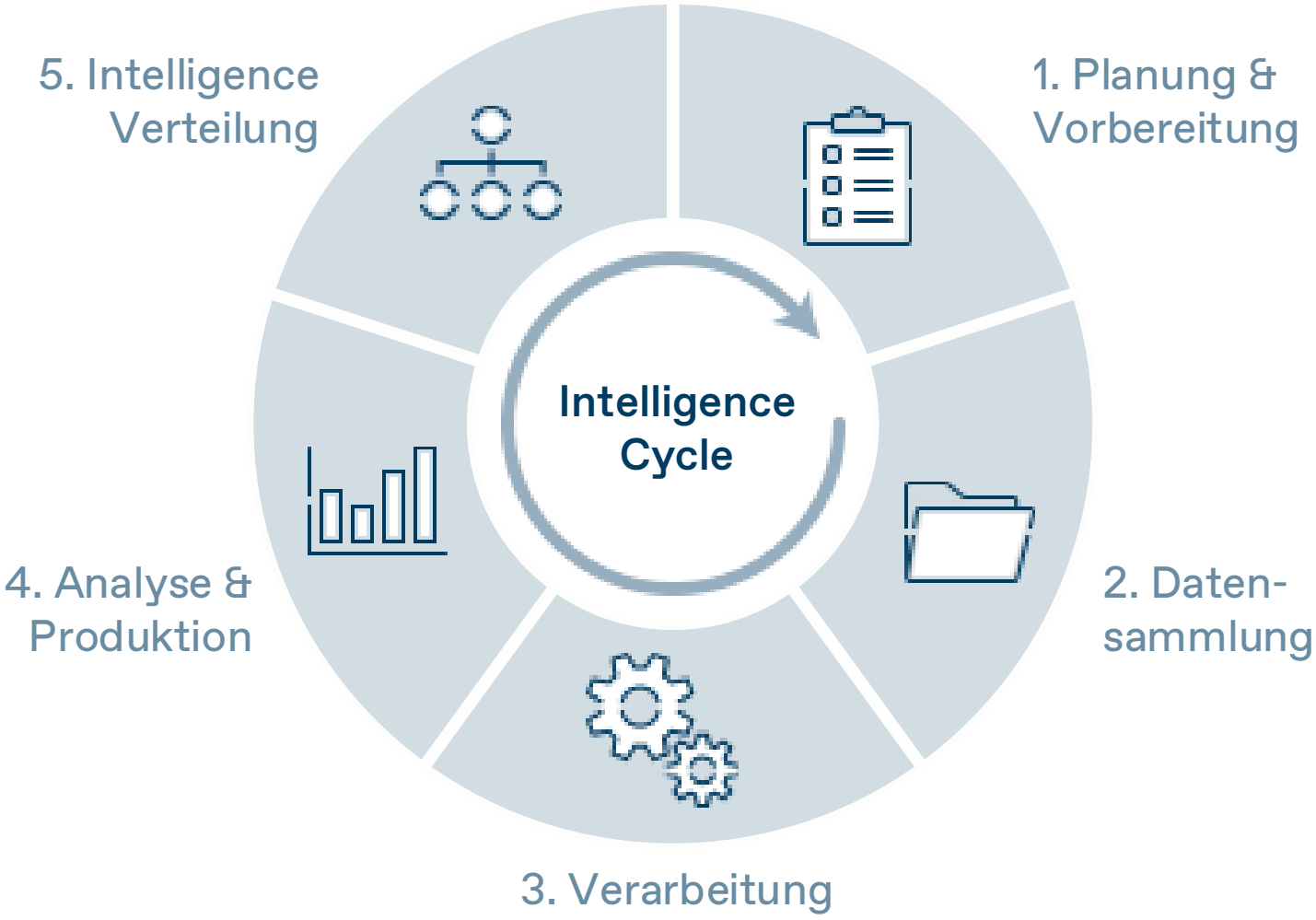
18.12.2025

TLP:CLEAR

DCSO TI Service

Kurze Übersicht

- Wir betreiben relevante Sharing Communities für die TI-Teams unserer Kunden.
- Wir bieten Berichte über unser Portal und technische Information über unsere MISP-Instanzen und eigene technische Plattform („TIE“).
- Wir sind einer der größten Managed Service Provider in Deutschland für die MISP-Instanzen unserer Kunden, welche diese für das Indicator Management und den Austausch benutzen.



Agenda

1 Grundlagen

2 Herausforderungen

3 Anwendungsfälle

4 Fragen und Antworten

1 Grundlagen

Was ist technische Threat Intelligence?

Einordnung von Threat Intelligence

Zielgruppengerechte Kommunikation

Strategisch

Ziel: Geschäftsleitung bei Entscheidungen zu unterstützen

C-Level Exec, Group Security, Business Stakeholders, Risiko Manager

Wirtschaft & Politik

(Industrie) Spionage
Sabotage

Reports | Presse

Dossiers

Operational

Ziel: Angreifer und ihre Vorgehensweise verstehen

Fähigkeiten, Motivation, Ziel
TTPs

Incident Responder, Threat Hunter, Netzwerk Architekten, System Administratoren, Schwachstellenmanagement, Red Teams, IT-Manager

TTPs | Fähigkeiten

Diamond Model

Taktisch

Ziel: Wissen anwenden, um Angriffe aufzuspüren

Informationen direkt in Detektions, Korrelations und Abwehrsysteme einspeisen

SOC-Team, SIEM, Sicherheitstechnologie

File Hashes | URLs, IPs

Domains, pDNS | Signatures

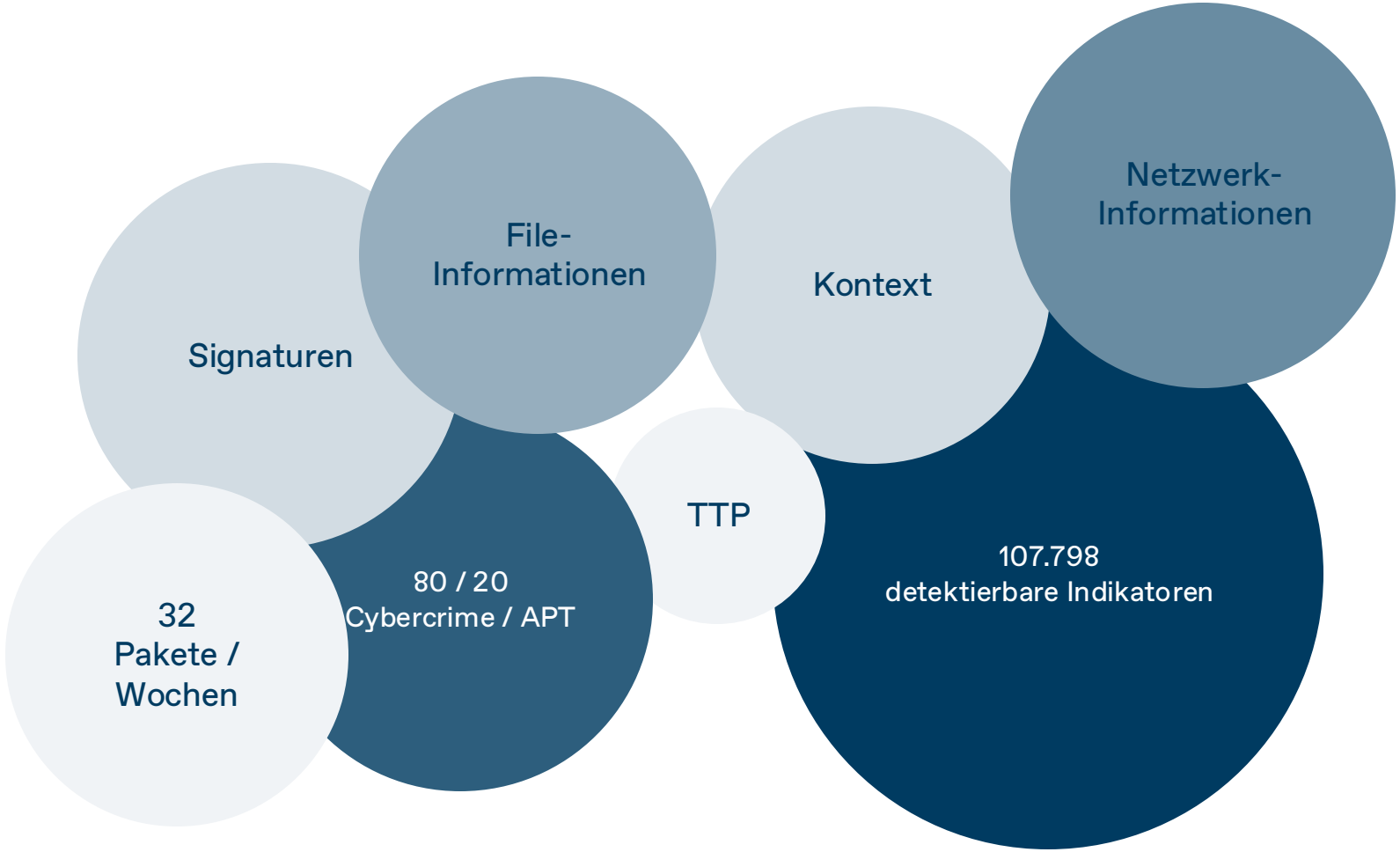
Technische Threat Intelligence

Beispiele (IP, Domain, Hash, URL, ...)

Indikatoren		Signaturen & Erkennungsmuster
Domains	evilcorp.com	YARA: Erkennung von Dateieigenschaften/-mustern
URLs	https://evilcorp.com/evil/a.php	Snort/Suricata: Erkennung von Netzwerkverkehr
Hash (z.B. SHA256)	e3b0c[...]52b855 (64 Zeichen)	Sigma: Erkennung in System-Protokollen
Dateiname & -pfad	C:/Users/Public/evilpath.exe	
IP-Adresse	106.52.185.141	

DCSO-Feed

Schwerpunkte und Kontext



2 Herausforderungen

Ist die Integration kompliziert?

Übliche Probleme

1

Schiere Menge an bereitgestellten Daten

Hoher Aufwand für die Integration in bestehende Sicherheitslösungen.

2

Mangel an Sektor-Spezifität

Indikatoren sind ggf. nicht relevant bzw. aussagekräftig für eigenes Umfeld.

3

Bias von Feed-Anbietern

Feed-Anbieter sind durch ihre Datengrundlage beschränkt.

4

Fehlender Kontext

Einige Indikator-Feeds stellen den Indikator bereit – ohne Kontext.

3 Anwendungsfälle

Wo kann ich technische TI einsetzen?

Sharing & Anreicherung

Managed MISP

- Hohe Flexibilität
- Abbildung von spezialisieren Workflows
- Umfangreiches Ökosystem
- Integration in existierende Communities

Konsum & Integration

Lösungsansätze

Um Indikator-Feeds in „Actionable Intelligence“ zu übersetzen, schlägt DCSO ein mehrstufiges Vorgehen vor, dass zwei Prioritäten berücksichtigt:

1. Reduktion von fehlerhaften Alarmen
2. Bereitstellung von Alarm-Kontext

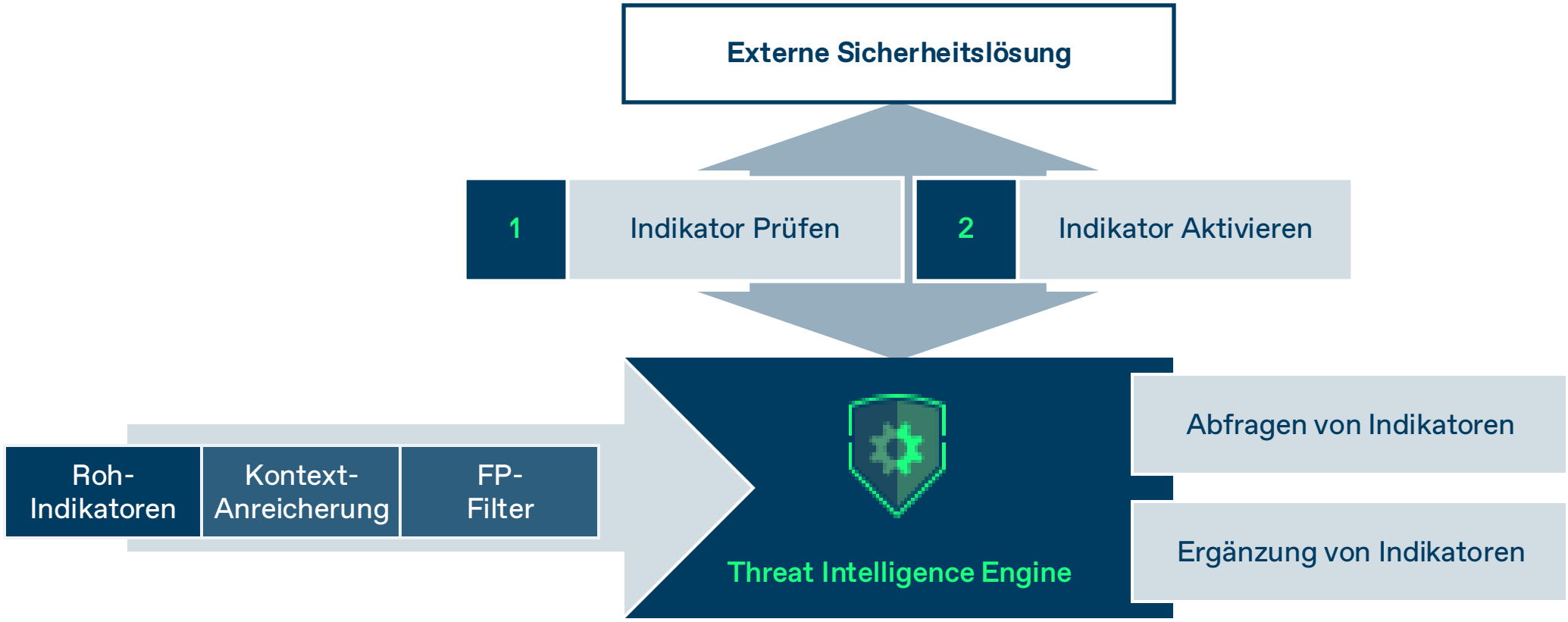
TI-Feeds

Qualitätssicherung

- False-Positive Überprüfung vor Import
- False-Positive Überprüfung vor Nutzung
- Kontinuierliches Analysten-Feedback
- Bereitstellung von umfangreichem Kontext
- Optimierung der Auslieferung

Threat Intelligence Engine

Architektur und Features



Anwendungsfälle

Wie kann ich technische TI einsetzen?

Teilen & Anreicherung	Konsum & Integration in Detektion
Erfordert eigene Threat Intelligence Kapazitäten	Legt den Schwerpunkt auf das Verständnis des Kontexts
Profitiert von aktiver Community Arbeit	Nutzt bestehende (vom Kunden eingekaufte) Quellen
Höhere Komplexität bei der Anbindung	Harmonisierung der Datenanbindung
Erlaubt Korrelation von Einzelereignissen	„Vereinheitlicht“ die Informationen aus den Quellen
Etablierte Open Source Lösung: MISP	DCSO-Lösung: Threat Intelligence Engine

TLP:CLEAR