51.3397° N 12.3731° E

LEIPZIG · GERMANY

MISSION BRIEF

DAS KUNDENMAGAZIN VON POINT OF RESOLUTION

AUSGABE 03 · SEPTEMBER 2026

CAPABILITY IM DETAIL · SITUATIONAL UNDERSTANDING

RISK INTELLIGENCE

SITUATIONAL AWARENESS · EARLY WARNING · DECISION SUPPORT

Wie aus Signalen belastbares Lageverständnis wird – und warum eine Analyse, die ihre eigene Unsicherheit verschweigt, für Entscheider wertlos ist.

EVIDENZSTATUS

SIGNAL **VERIFIED** **ASSESSED** **DECISION RELEVANT**

EDITORIAL

Das Problem ist nicht der Mangel an Information.

Kaum eine Organisation, mit der wir sprechen, hat zu wenig Meldungen. Die meisten haben zu viele. Sensordaten, Betriebsmeldungen, Behördeninformationen, Presse, Wetterdienste, Hinweise von Mitarbeitenden – und mitten darin die Frage, welche dieser Informationen eine Entscheidung tatsächlich verändern würde.

Risk Intelligence beantwortet genau diese Frage. Sie trennt konsequent, was beobachtet, was bestätigt und was daraus geschlossen wurde. Sie benennt, welche Annahmen eine Bewertung trägt. Und sie sagt, wie belastbar die Bewertung ist – auch dann, wenn die Antwort unbequem lautet: nicht besonders.

Diese Ausgabe zeigt den Weg vom schwachen Signal bis zum Decision Point: Detection, Verifikation und Quellenbewertung, Confidence und Kalibrierung, Bias-Kontrolle, Abhängigkeiten und Kaskaden, Frühwarnung, Lagebild und Entscheidungsunterstützung.

Ein Kapitel widmet sich der Bias-Kontrolle. Das wirkt für ein Kundenmagazin ungewöhnlich akademisch – aber die häufigste Ursache für Fehleinschätzungen ist nicht fehlende Information. Es ist die Information, die wir bevorzugen, weil sie zu unserer bisherigen Annahme passt.

Unser Ziel ist nicht, Unsicherheit zu verstecken. Unser Ziel ist, Unsicherheit so weit zu reduzieren und zu strukturieren, dass verantwortbare Entscheidungen möglich werden.

INGO ZIMMER

Founder & Mission Director

> *„The challenge is not access to information. The challenge is knowing what can be trusted — and what it means.“*
>
> RISK INTELLIGENCE PORTFOLIO, V1.0

IMPRESSUM

Herausgeber: Ingo Zimmer / POINT OF RESOLUTION,
Haferkornstraße 15, 04129 Leipzig, Germany.
Telefon +49 173 83 27 807 · contact@pointofresolution.com
pointofresolution.com

Verantwortlich für den redaktionellen Inhalt: Ingo Zimmer.
Redaktion und Gestaltung: POINT OF RESOLUTION.
Ausgabe 03, September 2026. POINT OF RESOLUTION ist derzeit eine Geschäftsbezeichnung von Ingo Zimmer.
Stand: 20. September 2026.

IN DIESER AUSGABE

Inhalt

ZU DIESER AUSGABE

Risk Intelligence ist keine Software und kein Datenabonnement. Sie ist eine Arbeitsweise: Informationen erkennen, verifizieren, einordnen, bewerten – und die verbleibende Unsicherheit ausweisen, statt sie sprachlich zu verstecken.

CAPABILITY IM DETAIL · AUFTAKT

„Wir betrachten Risiko nicht als Zustand, sondern als Lage.“

Risk Intelligence erkennt risikorelevante Informationen systematisch, verifiziert sie, setzt sie in Kontext und bewertet sie – um daraus belastbare Entscheidungsgrundlagen zu entwickeln.

DREI ANALYTISCHE EBENEN · KLAR GETRENNT

SIGNAL	Eine Beobachtung oder Meldung wurde erfasst; der Wahrheitsgehalt ist noch nicht ausreichend geprüft.
VERIFIED INFORMATION	Quelle, Inhalt, Zeitbezug, Ort und Plausibilität wurden geprüft oder unabhängig bestätigt.
ASSESSMENT	Aus mehreren Informationen und Annahmen wurde eine analytische Bewertung abgeleitet.

01 / WAS RISK INTELLIGENCE VERBINDET

Sechs Fähigkeitsbereiche, ein Lageverständnis

Risk Intelligence verbindet Bedrohungen, Assets, Abhängigkeiten, Ereignisse und Indikatoren zu einem fortlaufenden Bild – nicht zu einem Registereintrag.

Risikoanalyse	Risiken, Verwundbarkeiten, Auswirkungen und Kritikalität strukturieren.
Threat Intelligence	Bedrohungsakteure, Fähigkeiten, beobachtbare Aktivitäten und relevante Veränderungen bewerten.
OSINT & Verification	Öffentliche Informationen erfassen, prüfen und von unbestätigten Signalen trennen.
Situational Awareness	Ereignisse, Assets, Geografie, Zeit und Abhängigkeiten in einem gemeinsamen Lagebild zusammenführen.
Monitoring & I&W	Frühindikatoren definieren, Veränderungen beobachten und Eskalationsschwellen erkennen.
Decision Support	Bewertungen in klare Optionen, Prioritäten und Entscheidungspunkte überführen.

INTELLIGENCE CYCLE STATT EINZELANALYSE

Das Lagebild ist kein Endprodukt, das einmal erstellt und abgelegt wird. Jede neue Information kann bestehende Annahmen bestätigen, relativieren oder widerlegen.

GRUNDSATZ

Information allein erzeugt noch keine Intelligence. Entscheidend ist die Qualität der Bewertung unter Unsicherheit.

02 / ABGRENZUNG

Warum Risikoanalyse allein nicht ausreicht

Risiken entwickeln sich: Infrastruktur altert, Abhängigkeiten verschieben sich, Informationslagen verändern sich. Eine Bewertung zum Stichtag beantwortet das nicht.

KLASSISCHE BETRACHTUNG	RISK-INTELLIGENCE-ERWEITERUNG
Welche Risiken bestehen?	**Was verändert sich gerade?**
Wie hoch sind Eintrittswahrscheinlichkeit und Schaden?	**Welche Indikatoren verändern unsere Bewertung?**
Welche Maßnahme ist grundsätzlich vorgesehen?	**Welche Option ist unter den aktuellen Bedingungen sinnvoll?**
Welche Assets sind kritisch?	**Welche Abhängigkeiten und Kaskaden verändern ihre Kritikalität?**
Welche Informationen liegen vor?	**Was ist bestätigt, was fehlt – und wie sicher ist die Bewertung?**

BEIDES GEHÖRT ZUSAMMEN

Traditionelle Risikoanalysen bleiben ein wichtiges Instrument. Risk Intelligence ersetzt sie nicht – sie ergänzt die Momentaufnahme um laufende Beobachtung und Neubewertung.

03 / VON SIGNAL ZU ENTSCHEIDUNG

Sieben Stufen, konsequent getrennt

Professionelle Risk Intelligence trennt Beobachtung, Verifikation, analytische Bewertung und Entscheidung. Jede Stufe hat eine Leitfrage und ein Ergebnis.

01	**COLLECT**	Welche Informationen und Signale sind relevant?	**Strukturierter Informationsbestand**
02	**VERIFY**	Was ist bestätigt, was unbestätigt?	**Information mit Quellenstatus**
03	**CONTEXTUALISE**	Wie hängt die Information mit Assets, Raum, Zeit und Abhängigkeiten zusammen?	**Einordnung ins operative Umfeld**
04	**ASSESS**	Welche Bedeutung und welche Auswirkungen entstehen?	**Bewertung mit Confidence**
05	**PRIORITISE**	Was muss jetzt beachtet werden?	**Priorisierte Risiken und Bedarfe**
06	**INFORM**	Wer benötigt welche Information zu welchem Zeitpunkt?	**Adressatengerechtes Produkt**
07	**REVIEW**	Was hat sich verändert und war die Bewertung richtig?	**Kalibrierung und Lessons Learned**

DER EINSTIEG IST IMMER DIE ENTSCHEIDUNG

Welche Entscheidung muss vorbereitet werden – und welche Information kann diese Entscheidung tatsächlich verändern? Daraus folgt der Collection Plan, nicht umgekehrt.

04 / DETECTION

Kritische Entwicklungen kündigen sich leise an

Selten durch eindeutige Warnungen. Häufig durch kleine Veränderungen, Anomalien oder wiederkehrende Abweichungen vom erwarteten Normalzustand.

MÖGLICHE SIGNALE

- wiederkehrende technische Auffälligkeiten und Zustandsveränderungen
- ungewöhnliche Bewegungs-, Zugangs- oder Nutzungsmuster
- Störungen einzelner Dienstleister oder Versorgungswege
- zunehmende Ereignisdichte in einem definierten Raum
- auffällige Informations- oder Social-Media-Aktivitäten
- Veränderungen regulatorischer, politischer oder wirtschaftlicher Rahmenbedingungen
- Wetter- und Umweltentwicklungen mit möglicher Infrastrukturwirkung
- Anomalien in Sensor-, Betriebs- oder Kommunikationsdaten

PATTERN RECOGNITION – VIER ANALYSEEBENEN

SIGNAL

Was wurde beobachtet?

PATTERN

Tritt die Beobachtung wiederholt oder gemeinsam mit anderen Indikatoren auf?

RELEVANCE

Besitzt die Veränderung Bezug zu einem kritischen Asset, Prozess oder Auftrag?

ESCALATION

Verändert sich daraus der Handlungs- oder Informationsbedarf?

DER VERGLEICHSMASSSTAB

Ein einzelner Hinweis kann bedeutungslos sein. Mehrere korrelierende Hinweise können ein Muster ergeben. Deshalb interessiert nicht nur das Ereignis, sondern die Veränderung im Verhältnis zum erwarteten Normalzustand.

05 / VERIFICATION & SOURCE ASSESSMENT

Geschwindigkeit zählt. Informationsqualität entscheidet.

Quellen- und Informationsbewertung bleiben getrennt: Eine zuverlässige Quelle kann eine falsche Information weitergeben – und eine unbekannte Quelle eine richtige.

Herkunft	Primär- oder Sekundärquelle? Direkte Beobachtung oder Weitergabe?
Zeitbezug	Wann wurde die Information erzeugt – und wann verbreitet?
Interessen	Welche Motivation oder mögliche Verzerrung besitzt die Quelle?
Plausibilität	Ist der Inhalt technisch, geografisch und zeitlich plausibel?
Corroboration	Existieren unabhängige Bestätigungen oder Gegeninformationen?
Historie	Wie zuverlässig waren Quelle und Informationstyp in der Vergangenheit?

VIER ELEMENTE JEDER BEWERTUNG

INFORMATION
Was wissen wir tatsächlich?

ASSUMPTION
Was nehmen wir an, weil Informationen fehlen?

ASSESSMENT
Welche Schlussfolgerung ziehen wir daraus?

CONFIDENCE
Wie belastbar ist diese Schlussfolgerung?

WAS ES NICHT IST

Öffentliche Quellen liefern Informationen, nicht automatisch Intelligence. Erst Verifikation, Kontextualisierung und die Verbindung mit internen oder technischen Quellen machen daraus einen belastbaren Intelligence-Beitrag.

06 / CONFIDENCE, CALIBRATION, BIAS CONTROL

Gute Analyse klingt nicht sicher. Sie ist ehrlich.

Confidence beschreibt die Belastbarkeit einer Bewertung – nicht die Wahrscheinlichkeit eines Ereignisses. Unsicherheit sichtbar zu machen ist Voraussetzung belastbarer Entscheidungen.

LOW	Begrenzte Informationsbasis, wesentliche Unsicherheiten oder widersprüchliche Hinweise.
MODERATE	Mehrere belastbare Hinweise, aber relevante Lücken oder alternative Erklärungen bleiben bestehen.
HIGH	Breite und konsistente Informationsbasis mit nur begrenzten wesentlichen Unsicherheiten.

SECHS VERZERRUNGEN · ANSÄTZE ZUR BIAS-KONTROLLE

Confirmation Bias

Bestätigende Informationen werden bevorzugt. Gegenmaßnahme: alternative Hypothesen, Gegenindikatoren, Red Team.

Anchoring

Frühe Informationen prägen spätere Bewertungen zu stark. Gegenmaßnahme: Bewertung mit neuen Daten bewusst neu aufsetzen.

Availability Bias

Leicht erinnerbare Ereignisse werden übergewichtet. Gegenmaßnahme: Basisraten, Historie und Vergleichsdaten.

Normalcy Bias

Warnsignale werden unterschätzt, weil bisher nichts passiert ist. Gegenmaßnahme: Trigger vorab definieren.

Groupthink

Abweichende Sichtweisen werden zu früh harmonisiert. Gegenmaßnahme: unabhängige Bewertung, dokumentierte Gegenpositionen.

Overconfidence

Unsicherheit wird kleiner dargestellt, als sie ist. Gegenmaßnahme: Confidence Statements und Kalibrierung.

CALIBRATION

Bewertungen werden später mit der tatsächlichen Entwicklung abgeglichen. So wird sichtbar, wo Risiken systematisch über- oder unterschätzt und Annahmen zu lange beibehalten wurden.

07 / SITUATIONAL, ASSET & GEOSPATIAL INTELLIGENCE

Ein Lagebild erklärt, warum ein Ereignis relevant ist

Nicht nur, was passiert. Sondern auch, was es bedeutet – und welche Entwicklung daraus entstehen kann.

Was passiert?

Erfassung und Verifikation relevanter Ereignisse.

Was bedeutet es?

Kontextualisierung mit Assets, Abhängigkeiten, Raum, Zeit und Auftrag.

Was könnte daraus entstehen?

Bewertung plausibler Entwicklungen, Wirkungen und Eskalationspfade.

ASSET INTELLIGENCE

Standorte & Anlagen	Funktion, Kritikalität, Betriebsstatus, Redundanz, Wiederherstellungszeit.
Netze & Korridore	Verbindungen, Engpässe, Querungen, Abhängigkeiten, alternative Wege.
Menschen & Funktionen	Schlüsselrollen, Erreichbarkeit, Exposition, Ersatzmöglichkeiten.
Dienstleister & Lieferketten	Kritische Leistungen, Vorlaufzeiten, Single Sources, Alternativen.
Kommunikation & IT	Abhängigkeit, Reichweite, Stromversorgung, Redundanz, Offline-Fähigkeit.

GEOSPATIAL RISK INTELLIGENCE

Position, Entfernung, Wirkbereich, Zugänglichkeit, Gelände, Verkehrsachsen und Nachbarsysteme machen aus der Meldung „Ereignis an Ort X“ die entscheidende Frage: Welche operative Bedeutung hat dieses Ereignis für unsere Assets und Funktionen?

08 / DEPENDENCIES & THREAT INTELLIGENCE

Das Risiko liegt selten im ersten Ereignis

Kritische Infrastruktur besteht nicht aus isolierten Objekten, sondern aus Abhängigkeiten. Sie bestimmen, wie weit eine Störung tatsächlich wirkt.

Energie	Ausfall von Pumpen, Steuerung, Beleuchtung, Telekommunikation oder Zugangssystemen.
Telekommunikation	Verlust von Fernüberwachung, Alarmierung, Koordination und Datenübertragung.
Wasser / Entwässerung	Einschränkung von Betrieb, Kühlung, Hygiene, Löschwasser oder Zugang.
Verkehr / Logistik	Personal, Ersatzteile oder Einsatzmittel erreichen den Standort verzögert.
IT / Cloud / OT	Steuerung, Dokumentation oder operative Prozesse stehen nur eingeschränkt zur Verfügung.

CASCADING EFFECTS

Ein Stromausfall beeinträchtigt die Telekommunikation; dadurch fällt die Fernüberwachung aus; Störungen werden später erkannt; Entscheidungen verzögern sich.

THREAT INTELLIGENCE – SECHS BETRACHTUNGEN

ACTOR

Wer könnte Einfluss auf das System nehmen?

CAPABILITY

Welche realistischen Fähigkeiten sind erkennbar?

OPPORTUNITY

Welche Zugänge, Schwachstellen oder Zeitfenster bestehen?

ACTIVITY

Welche beobachtbaren Aktivitäten verändern die Lage?

INTENT

Welche Hinweise auf Zielsetzungen gibt es – und wie belastbar sind sie?

IMPACT

Welche missions- oder betriebsrelevanten Folgen wären möglich?

09 / INDICATIONS & WARNINGS

Frühwarnung beginnt nicht mit dem Alarm

Sie beginnt mit der Frage, welche beobachtbaren Veränderungen auf eine relevante Entwicklung hindeuten könnten – und ab welchem Punkt sie das tun.

Indicator	Welche konkrete Veränderung ist beobachtbar?
Source	Wo und wie kann sie erkannt werden?
Expected Pattern	Welches normale Verhalten dient als Vergleich?
Threshold	Ab welchem Wert oder Muster wird die Veränderung relevant?
Confidence	Wie belastbar ist die Beobachtung?
Escalation Level	Welche Stufe wird bei Kombination oder Überschreitung ausgelöst?
Responsible Function	Wer bewertet oder bestätigt den Indikator?
Required Action	Welche Information oder Maßnahme folgt daraus?

EARLY WARNING LOGIC

NORMAL

Kein relevanter Abweichungstrend. Beobachtung im Regelbetrieb.

WATCH

Einzelne Veränderungen oder schwache Signale erfordern erhöhte Aufmerksamkeit.

WARNING

Mehrere Indikatoren oder ein Schwellenwert verändern die Risikobewertung.

CRITICAL

Akute oder stark eskalierende Entwicklung mit unmittelbarem Entscheidungsbedarf.

10 / CRITICAL EVENT INTELLIGENCE

Wenn die Lage schneller ist als das Lagebild

Während dynamischer Ereignisse stabilisiert Critical Event Intelligence den Informations- und Entscheidungsprozess – mit sieben Kernfragen.

Was ist bestätigt?	Verifizierter Ereignisstand mit Zeitbezug.
Was ist unbestätigt?	Separierte Meldungen mit Prüfstatus.
Was fehlt?	Priorisierte Intelligence Requirements.
Was ist betroffen?	Assets, Funktionen, Menschen, Routen und Abhängigkeiten.
Welche Wirkung ist sichtbar?	Aktuelle technische, operative und organisatorische Auswirkungen.
Was könnte folgen?	Plausible Folgewirkungen und Szenarien.
Welche Entscheidung steht an?	Decision Point, Zeitfenster und Informationsbedarf.

COMMON OPERATING PICTURE

Events

Verifizierte Ereignisse, Zeitlinie, Status, offene Prüfungen.

Map Layer

Lage, Wirkbereiche, Assets, Zugänge, Routen, Sperrungen.

Asset Status

Betriebszustand, Kritikalität, Schäden, Verfügbarkeit, Recovery.

Dependencies

Betroffene Versorgung, Kommunikation, Logistik, Folgeprozesse.

Requirements

Offene Informationsbedarfe und Verantwortlichkeiten.

Decisions & Actions

Entscheidungen, Decision Points, Maßnahmen, Wirksamkeitskontrolle.

SITUATION REPORT

Ein SITREP muss nicht lang sein. Er muss aktuell, verifiziert und entscheidungsrelevant sein – mit Zeitstempel, Quellenstatus, offenen Fragen, Confidence und nächster Review-Zeit.

11 / DECISION SUPPORT & DELIVERABLES

Analyse ohne Entscheidungsfähigkeit ist wertlos

Vollständige Information ist in realen Lagen selten verfügbar. Entscheidend ist der Unterschied zwischen „noch nicht alles wissen“ und „noch nicht entscheidungsfähig sein“.

DREI SZENARIEN STATT EINER ANGENOMMENEN ZUKUNFT

MOST LIKELY

Die auf Basis aktueller Informationen plausibelste Entwicklung.

MOST DANGEROUS

Weniger wahrscheinlich, aber besonders folgenreich – und vorbereitungsrelevant.

ALTERNATIVE

Eine relevante alternative Erklärung, die bestehende Annahmen herausfordert.

ESKALATIONSPFAD

1	**Ausgangslage**	Normalzustand, bekannte Risiken, Baseline.
2	**Veränderung**	Erste Indikatoren und Abweichungen.
3	**Verdichtung**	Mehrere Hinweise, höheres Confidence-Level, neue Informationsbedarfe.
4	**Eskalation**	Decision Point, Kommunikation, Schutz- oder Contingency-Maßnahmen.
5	**Ereignis**	Aktive Lageführung, Critical Event Intelligence, Recovery-Vorbereitung.

TYPISCHE DELIVERABLES

Risk Intelligence Assessment · Threat Landscape · Asset Intelligence Profile · Critical Dependency Map · Indicator & Warning Matrix · Monitoring Concept und Watchlist · Executive Intelligence Brief · Situation Report · Geospatial Risk Map · Scenario Assessment und Eskalationsmatrix · Communication & Warning Architecture · Lessons-Learned Assessment

12 / CAPABILITY ASSESSMENT

Wie gut ist Ihre Risk Intelligence?

Bewertet wird nicht, wie viele Risikoberichte vorliegen, sondern wie gut Informationen in belastbares Lageverständnis überführt werden. Sechs Dimensionen, je 20 Punkte – jede einzeln ausgewertet, damit ein gutes Gesamtergebnis keine Fähigkeitslücke verdeckt. Der Self-Assessment-Bericht wird lokal im Browser erzeugt; Assessment-Daten werden nicht automatisch an POINT OF RESOLUTION übertragen.

A · Information & Source Discipline	**20**
B · Verification & Analytical Confidence	**20**
C · Situational & Dependency Awareness	**20**
D · Indications & Early Warning	**20**
E · Decision & Response Intelligence	**20**
F · Learning, Calibration & Resilience	**20**

WELCHE ENTSCHEIDUNG MÜSSEN SIE GERADE OHNE BELASTBARE LAGE TREFFEN?

pointofresolution.com/mission-request.html

POINT OF RESOLUTION
DEFENSE & INFRASTRUCTURE SECURITY

POINT OF RESOLUTION · Ingo Zimmer · Haferkornstraße 15 · 04129 Leipzig · Germany
+49 173 83 27 807 · contact@pointofresolution.com · pointofresolution.com