RISK MANAGEMENT & INTELLIGENCE POLICY

Risk Management & Intelligence Policy

Grundprinzipien, Risikokategorien und methodische Leitlinien von NAVINATION.
Verbindliche Grundlage für alle Reports, Bewertungen und Beauftragungen.

NAVINATION liefert keine Sicherheitsbewertungen, sondern Sichtbarkeits- und Risikoindikatoren auf Basis externer Beobachtung und probabilistischer Analyse. Kurz: Wir messen Exposure, nicht Sicherheit.

NAVINATION · Christian Frahm
Jasminweg 8 · 70597 Stuttgart

01 / ZWECK

Geltungsbereich

Dieses Dokument definiert die Grundprinzipien, Risiken, Haftungsgrenzen und methodischen Leitlinien von NAVINATION. Es gilt als verbindliche Grundlage für interne Mitarbeiter, externe Partner sowie für die Einordnung aller Reports und Bewertungen.

02 / GRUNDPRINZIP

NAVINATION ist kein Security-Audit

NAVINATION ist kein Security-Audit, kein Penetration-Test und keine Zertifizierungsinstanz.

NAVINATION IST	NAVINATION IST NICHT
• External Exposure Intelligence	• Penetration Testing
• Reconnaissance Intelligence	• Vulnerability Scanning
• Cyber Risk Indicator Platform	• Security Audit oder Compliance Audit
• External Visibility Analytics	• IT-Sicherheitsprüfung oder Zertifizierung
• Exposure Monitoring	• Red Team / Blue Team / SOC / Managed Security

> **Alle Ergebnisse sind probabilistisch, indikativ, interpretationsbasiert, Momentaufnahmen und abhängig von Datenqualität und -verfügbarkeit.**

03 / METHODIK

Die Intelligence-Kette

Jede NAVINATION-Analyse basiert auf einer mehrstufigen Verarbeitungskette. In jeder Stufe können Fehler entstehen. NAVINATION bewertet daher niemals absolute Sicherheit, sondern ausschließlich Risikoindikatoren.

Schritt 3 (Datenstrukturierung) und Schritt 6 (Human-in-the-Loop) sind explizit ausgewiesen, weil sie methodisch wesentlich sind: Schritt 3 überführt die Rohdaten vollständig und regelbasiert in ein strukturiertes Analysedokument — kein Ermessen, keine Selektion. Schritt 6 stellt sicher, dass kein KI-System die manuelle Browser-Verifikation kritischer Findings ersetzt.

04 / RISIKOKATEGORIEN

Bekannte Risiken und Grenzen

KATEGORIE	BESCHREIBUNG
Data Risk	Risiken bei der Datenerhebung: unerkannte Systeme (False Negative), fehlinterpretierte Systeme (False Positive), DNS-Fehler, Geo-Lokations-Fehler, CDN-Verzerrungen, Routing-Unterschiede, zeitliche Veränderungen, Honeypots. *Grundsatz: Erhobene Daten sind Indikatoren, keine Beweise.*
TLS-Zertifikat-Inhaberschaft	Bei Hosts die über CDN- oder Infrastruktur-Anbieter (Cloudflare, AWS, Akamai u.a.) bereitgestellt werden, ist das extern sichtbare TLS-Zertifikat das des Anbieters, nicht des Kunden. Eine direkte TLS-Qualitätsbewertung der Kunden-Infrastruktur ist in diesen Fällen extern nicht möglich. NAVINATION kennzeichnet Zertifikate entsprechend als Provider- oder Kundenzertifikat und schließt Provider-Zertifikate aus der TLS-Qualitätsbewertung aus. *Grundsatz: TLS-Signale beschreiben die extern sichtbare Zertifikatsschicht — nicht zwingend die interne TLS-Konfiguration des Kunden.*
Asset Attribution Risk	Das größte Risiko ist die falsche Zuordnung von Assets zu Unternehmen. Ursachen: Shared Hosting, Dienstleister-Infrastruktur, Tochterunternehmen, alte Domains, Cloud Shared Services. NAVINATION verwendet ein Confidence-Modell (Level A–E). *Grundsatz: Asset-Zuordnung ist eine Wahrscheinlichkeitsaussage, kein Eigentumsnachweis.*
KI-Interpretationsrisiko	Die Analyse erfolgt unter Einsatz von Large Language Models. Die Rohdaten werden in einem deterministischen Strukturierungsschritt vollständig und regelbasiert aufbereitet, die Klassifikation durch ein adversariales Prüfmodell auf Konsistenz und Signaldeckung geprüft. Kritische Findings werden zusätzlich manuell im Browser verifiziert (Human-in-the-Loop). Trotz dieser Maßnahmen können Fehlinterpretationen nicht vollständig ausgeschlossen werden.
Scoring Risk	Scores sind Orientierungswerte, keine absoluten Sicherheitsbewertungen. Risiken: falsche Gewichtung, unvollständige Daten, fehlende Assets, Fehlinterpretation durch Kunden. Ein direkter Vergleich zwischen verschiedenen Organisationen ist nur eingeschränkt aussagekräftig, da Infrastrukturentscheidungen wie CA-Strategie, CDN-Einsatz und Hosting-Modell die Messbasis strukturell beeinflussen. Das Risikomodell umfasst ab Version 2.3 eine eigenständige TLS-Qualitätsdimension, die ausschließlich auf extern sichtbaren Kundenzertifikaten basiert.
Reporting Risk	Reports können bei M&A, Unternehmensbewertung, Versicherungen oder Investitionsentscheidungen verwendet werden. In diesen Fällen ist ergänzende interne und externe Fachprüfung zwingend erforderlich.

Asset Attribution Confidence

Nur Assets mit ausreichender Confidence dürfen in Scores einfließen.

LEVEL	BEDEUTUNG	SCORE
A	Bestätigt – direkte Zuordnung eindeutig	**Ja, volle Gewichtung**
B	Sehr wahrscheinlich – starke Signale	**Ja, volle Gewichtung**
C	Wahrscheinlich – moderate Signale	**Ja, reduzierte Gewichtung**
D	Unsicher – schwache Signale	Nur mit Hinweis
E	Kein verwertbares Signal	Nein

06 / GRUNDREGELN

Verbindlich für alle NAVINATION Reports

#1	Ergebnisse basieren auf öffentlich verfügbaren Informationen.
#2	Ergebnisse sind Momentaufnahmen. Verfügbarkeit und Erreichbarkeit einzelner Systeme zum Scan-Zeitpunkt können durch Faktoren außerhalb des Zielunternehmens beeinflusst worden sein.
#3	Ergebnisse können unvollständig sein. Eine Garantie für die Vollständigkeit der erfassten Infrastruktur kann nicht übernommen werden.
#4	Asset-Zuordnungen sind probabilistisch.
#5	Scores sind Risikoindikatoren, keine Sicherheitsbewertungen.
#6	Keine Aussage über interne Sicherheit.
#7	Keine Aussage über tatsächliche Schwachstellen.
#8	Keine Aussage über Kompromittierung.
#9	Keine vollständige Asset-Inventarisierung möglich.
#10	Findings sind Ausgangspunkt für interne Prüfprozesse.

07 / LEITPRINZIPIEN

Unser Selbstverständnis

01
Wir beobachten, wir greifen nicht an.

02
Wir bewerten Sichtbarkeit, nicht Sicherheit.

03
Wir liefern Indikatoren, keine Beweise.

04
Wir arbeiten mit Wahrscheinlichkeiten, nicht mit Gewissheiten.

05
Der größte Risikofaktor ist unbekannte Infrastruktur.

06
Scores sind Vergleichswerte, keine Wahrheiten.

07
Asset-Zuordnung ist probabilistisch.

08
Jeder Report kann unvollständig sein.

09
Findings sind Ausgangspunkt für interne Prüfprozesse.

10
NAVINATION reduziert Unsicherheit über externe Sichtbarkeit — ersetzt aber niemals interne Sicherheitsprüfungen.