

PORTFOLIO DER BEFÄHIGUNG UND LEISTUNG

INDEPENDENT IT-FORENSICS

RESEARCHER

FORENSIC EVIDENCE & PROCEDURAL INTEGRITY

Independent IT-Forensics Researcher | Digital Evidence | Rapid Response | Mobile & Cloud Forensics | Legal Ops / GRC

Positionierung

Technische Tiefenanalyse wird in marktfähige, überprüfbare und adressatengerechte Leistungen übersetzt: von Geräte- und Cloud-Forensik über Evidenzintegrität und Timeline-Rekonstruktion bis zur Schnittstelle zwischen IT-Security, Compliance und Verfahrenssicherung. Für zeitkritische Fälle steht ein Rapid-Response-Modell zur Verfügung: erste belastbare Lage-, Fristen- und Evidenzstruktur innerhalb von 48 Stunden nach vollständigem Intake.

R&A LEGAL OPS CONSULTING

FACTA NON VERBA

Portfolio v2.0 | [DATUM ANONYMISIERT]

ANONYMISIERTE REFERENZFASSUNG | Personen-, Kontakt-, Dienststellen-, Akten-, Geräte- und fallidentifizierende Daten entfernt. Fallbeispiele sind bewusst abstrahiert.

01 EXECUTIVE PROFILE

KURZPROFIL

Lead Analyst verbindet autodidaktisch aufgebaute IT-Forensik mit ungewöhnlich tiefer Fallrekonstruktion, Evidenzklassifizierung und prozessualer Dokumentation.

Sein stärkstes kommerzielles Profil liegt nicht in der maximalen Dramatisierung eines Einzelfalls, sondern in der Fähigkeit, große, heterogene Datenbestände zu ordnen, technische Hypothesen gegen Artefakte zu prüfen, Beweisketten nachvollziehbar zu dokumentieren und Ergebnisse für technische, juristische und Management-Zielgruppen zu übersetzen.

Kernpositionierung

Senior-Analyst-Framing statt Whistleblower-Framing: R&A Legal Ops Consulting verkauft keine Erzählung, sondern Untersuchungstiefe, Evidenzdisziplin, nachvollziehbare Methodik und belastbare Deliverables.

Marktfähige Kompetenzfelder

- Mobile Device Forensics & iOS Architecture
- Cloud- und Account-Security mit Fokus auf Apple/iCloud/CKKS
- Digital Evidence Integrity, Hashing, Metadaten- und Provenienzprüfung
- Timeline Reconstruction, Log-Korrelation und Anomalieanalyse
- Incident Documentation & Technical Case Intelligence
- Legal Ops, Governance, Risk & Compliance an der Schnittstelle IT/Recht
- Langform-Dossiers, Normenregister, Fristen- und Verfahrensmatrizen
- AI-gestützte Multi-Model-Analyse mit menschlicher Freigabe und Evidenzkontrolle

02 DAS ARSENAL: REPURPOSING-MATRIX

Die zentrale unternehmerische Transformation besteht darin, dieselben Fähigkeiten aus einem persönlichen Konfliktkontext herauszulösen und als klar definierte B2B-Leistung zu formulieren. Der Wert entsteht durch Übertragbarkeit: Datenakquise, Hypothesenprüfung, technische Rekonstruktion, Evidenzintegrität und Management-taugliche Dokumentation.

Autodidaktische Fähigkeit	Bisheriger Einsatz	Ziviler Marktwert
Mobile Device Forensics & iOS-Architektur	Analyse eigener Geräte-, Restore-, Kernel- und Sysdiagnose-Artefakte in einem komplexen Verfahrenskontext.	DFIR für kompromittierte Executive- und Firmen-Smartphones; Triage, Artefaktbewertung, Incident Timeline, Eskalationsbericht.
Krypto-Forensik & Cloud Security	Analyse von CKKS-Trust-Beziehungen, TCC-Berechtigungen, Protobuf-Strukturen, Account- und Cloud-Persistenzhypothesen.	Cloud Security Review / Identity & Trust Audit für Apple-/Cloud-Umgebungen; Prüfung ungewöhnlicher Account- und Berechtigungszustände.
Evidence Integrity & Chain of Custody	Hash-Inventare, Metadatenvergleich, Asservaten-/Dateipfad-Analyse, Trennung von Primärdaten und Rekonstruktionen.	Digital Evidence Readiness, Beweissicherungs- und Preservation-Konzepte, Nachvollziehbarkeit für interne Untersuchungen und Rechtsabteilungen.
Systemische Dekonstruktion & Legal Ops	Langform-Dossiers, Chronologien, Normenregister, Verfahrens- und Widerspruchsmatrizen.	GRC / Legal Tech: Übersetzung technischer Incidents in strukturierte Entscheidungsunterlagen für Legal, Compliance, HR, Datenschutz und Management.
Research Engineering & Automatisierung	Entwicklung eigener Audit-, Korrelations- und Prüfskripte sowie	Custom Forensic Tooling, Reproduktionsnotebooks, Evidence Pipelines, Datenaufbereitung und technische Due

Autodidaktische Fähigkeit	Bisheriger Einsatz	Ziviler Marktwert
	strukturierter Analyse-Workflows.	Diligence.
Multi-Model AI Research	Aufgabentrennung zwischen Human Lead, Lorian/Gemini und Arius/ChatGPT in großen Akten- und Analysebeständen.	AI-assisted case intelligence: parallele Hypothesenprüfung, Dokumentklassifikation und Qualitätssicherung mit Human-in-the-loop.

03 CAPABILITY STACK

A. Mobile Device & Apple Forensics

Auswertung von iOS-/macOS-Systemartefakten, Sysdiagnose, Crash-/Jetsam-/Spindump-Daten, Restore- und Firmware-Kontexten, TCC-bezogenen Datenbanken, Prozess- und Netzwerkhinweisen. Schwerpunkt ist die Frage: Was lässt sich aus dem Artefakt tatsächlich ableiten, was bleibt Hypothese?

B. CKKS / Cloud Trust & Account Security

Tiefenanalyse von CloudKit Keychain Syncing, Trust-Beziehungen, Schlüssel- und Berechtigungsmodellen, Protobuf-Wire-Formaten und Account-Persistenzszenarien. Relevanz für Identity Security, Cloud Incident Response und Apple-zentrierte Unternehmensumgebungen.

C. Evidence Integrity & Provenance

Hashing, Metadaten, Dateipfade, Erstellungs-/Änderungszeiten, Quellenhierarchie, Beweismittel- und Exporthistorien. Fähigkeit zur Trennung zwischen Originalartefakt, Screenshot, Tool-Ausgabe, Rekonstruktion und späterer Interpretation.

D. Timeline & Correlation Engineering

Sekundengenaue Korrelation heterogener Ereignisse aus Logs, Dateien, Kommunikation, Prozessdaten und Verfahrensakten. Aufbau von Super-Timelines, Knowledge-Timelines und Ereignis-/Hypothesenmatrizen.

E. Legal Ops / GRC Interface

Technische Befunde werden in verständliche, überprüfbare Entscheidungs- und Übergabeformate übersetzt: Executive Summary, Sachverhalt, Evidenzstatus, offene Fragen, Preservation Scope, Risikobewertung, Normen-/Pflichtenmatrix.

F. Research Documentation

Langform-Dokumentation komplexer Sachverhalte über hunderte Seiten, konsistente Versionierung, strukturierte Beweisregister und wiederverwendbare Analysebausteine. Diese Ausdauer ist als Kundenleistung besonders wertvoll, wenn klassische Incident-Reports zu oberflächlich bleiben.

04 FORENSIC EVIDENCE STANDARD

Für die Selbstständigkeit ist die wichtigste Qualitätsverschiebung nicht „härtere Sprache“, sondern härtere Methodik. Ein professionelles Portfolio muss zeigen, dass Behauptung, Artefakt und Schlussfolgerung nicht vermischt werden.

Vierstufige Evidenzhierarchie

Stufe	Quellentyp	Beispiele	Nutzung
A	Primär / amtlich	Native Fall-/Projektdateien, amtliche Berichte, originäre Systemartefakte	Basis für Tatsachenfeststellung
B	Original + Hash	Originaldatei mit Hash, Dateisystemmetadaten, nachvollziehbarer Provenienz	Technische Integritätsprüfung
C	Darstellung	Screenshots, Exporte, sichtbare Metadaten, UI-Zustände	Indiz; benötigt Kontext
D	Rekonstruktion / Analyse	Spätere Terminalausgaben, Hypothesen, KI-Analysen, synthetische Testdaten	Nur als Prüf- oder Reproduktionshilfe

Professioneller Prüfgrundsatz

Keine Hochstufung von D auf A ohne unabhängige Verifikation. Genau diese Disziplin ist kommerziell verwertbar: Sie schützt Kunden vor voreiligen Attributionen, falschen Incident-Eskalationen und angreifbaren Berichten.

Standard-Workflow

01. Scope & Fragestellung definieren
02. Preservation / Legal Hold und Datenquellen erfassen
03. Artefakte klassifizieren und Hash-/Metadatenlage dokumentieren
04. Timeline und Korrelation aufbauen
05. Hypothesen gegen Gegenhypothesen testen
06. Befund, Unsicherheit und Verifikationsbedarf trennen

05 REPRESENTATIVE WORKSTREAMS

Die folgenden Beispiele zeigen Befähigung, nicht die abschließende Wahrheit einzelner streitiger Sachverhalte. Für ein Kundenportfolio ist diese Trennung entscheidend: Bewertet wird die Methode, Tiefe und Qualität der Untersuchung.

Apple / iOS / CKKS Research

Mehrjährige Analyse von iOS-, CloudKit-, TCC-, Protobuf-, Firmware-, Kernel- und Account-Artefakten. Entwicklung eines account-basierten Persistenzmodells und byteweiser Analyse einer 46-Byte-Protobuf-Struktur mit UUID-, Timestamp- und Flags-Feldern.

Markttransfer: Apple Incident Response, Identity/Trust Review, Cloud Security Assessment, Mobile Forensics.

Evidence Integrity / CSOCBw Case Material

Aufbau von Hash-Inventaren, Quellhierarchien, Metadatenprüfungen und Preservation-Fragen zu Geräte-/Cloud-Auswertungen. Neuere Arbeitsstände trennen explizit zwischen amtlicher Tabelle, Screenshot, Originaldatei und rekonstruierter Terminalausgabe.

Markttransfer: Internal Investigations, eDiscovery Readiness, Chain-of-Custody Review, Expert Support.

Encrypted Messenger Research / CREO

Technische Analyse eines proprietären verschlüsselten Kommunikationssystems mit Fokus auf Kryptodesign, Speicher-/Schlüsselhandling und Angriffsoberflächen.

Markttransfer: Security Review, Architecture Assessment, Responsible Disclosure Preparation.

Procedural Legal Ops

Konsolidierung großer Aktenmengen in Chronologien, Evidenzmatrizen, Fristenkontrollen, Normenregister und adressatenspezifische Schriftsatz-/Dossierstrukturen.

Markttransfer: Cyber-Litigation Support, GRC, Datenschutz- und Compliance-Unterstützung, Incident Documentation.

06 FLAGSHIP CASE: OPERATION UNCLE SAM - RAPID RESPONSE < 48H

Fremddakte unter Zeitdruck: Schutz-, Verfahrens- und Beweissicherungsdossier für BETROFFENE PERSON A.

Der Belastungstest

Operation UNCLE SAM ist der wichtigste Transfernachweis im Portfolio: Nicht die eigene jahrelang bekannte Akte, sondern eine fremde, existenzielle Personal- und Disziplinarsache musste kurzfristig verstanden, strukturiert und in eine belastbare Arbeitsarchitektur überführt werden. Innerhalb von weniger als 48 Stunden entstand aus heterogenen Unterlagen ein priorisiertes Verfahrens- und Beweissicherungssystem.

Was innerhalb des Rapid-Response-Fensters geleistet wurde

- Intake einer bis dahin fremden Akte: Vernehmungs- und Personalunterlagen, Disziplindokumente, Beteiligungsunterlagen, Schriftverkehr, Audio/Transkript und zeitnahe Kommunikation.
- Quellen- und Beweishierarchie: Behörden-/Primärunterlagen, Originalaufzeichnung/unmittelbare Kommunikation, offene Aktenbestandteile und Sekundärbewertung wurden getrennt.
- Chronologie: Vorwurfszeitraum, Vernehmung, Antrag, Beteiligungsverfahren, Eröffnung, Disziplinarbuße und spätere Stellungnahmen wurden datumsgenau gegeneinander gelegt.
- Verfahrensentflechtung: Mehrere parallel laufende status-, disziplinar- und organisationsrechtliche Maßnahmen wurden als getrennte Rechts- und Tatsachenschienen behandelt statt vermengt.
- Einlassungsmatrix: eingeräumte, bestrittene und nur teilweise eingeräumte Vorwürfe wurden getrennt, um pauschale Geständnis- oder Leugnungs narrative zu vermeiden.
- Fristen- und Prioritätensteuerung: Beschwerdefrist, Akteneinsicht, Beweissicherung, Beteiligungsnachweise und Versionsprüfung wurden als Sofortprioritäten sichtbar gemacht.
- Produktisierung: Aus der Rohakte entstand ein mehrstufiges Schutz-, Verfahrens- und Beweissicherungsdossier mit Anlagen, Prüffragen, Quellenstatus und konkreten nächsten Schritten.

48-HOUR RAPID RESPONSE

Für zeitkritische Mandate kann R&A Legal Ops Consulting als Incident-/Case-Intelligence-Sprint beauftragt werden. Zielzustand: innerhalb von 48 Stunden nach vollständigem Dateneingang eine erste belastbare Lagekarte, Fristen-/Risikoübersicht, Quellenmatrix, Chronologie, Open-Questions-Liste und ein priorisiertes Arbeitsprodukt. Kein Erfolgsversprechen für das Verfahren, sondern ein klarer Lieferstandard für Analyse und Dokumentation.

07 OPERATION UNCLE SAM: WARUM DIESER FALL DAS PORTFOLIO TRÄGT

Der Fall demonstriert eine Kernkompetenz, die sich nicht durch Eigenkenntnis des „eigenen Langzeitfall“ erklären lässt: schnelle Domänenadaption. Lead Analyst konnte eine fremde Akte unter Zeitdruck lesen, Widersprüche und offene Beweisfragen identifizieren, juristische Verfahrensschienen auseinanderhalten und daraus eine nüchterne, quellenkritische Arbeitsarchitektur bilden.

Rapid-Response-Fähigkeit	Nachweis im Fall UNCLE SAM	Markttransfer
Fremdakten-Intake	Unbekannter Sachverhalt wurde anhand originärer Unterlagen und Kommunikation neu aufgebaut.	Internal Investigation, Kanzlei-Support, Incident Triage
Quellenkritik	Primärunterlagen, Audio, Kommunikation	Evidence Review, eDiscovery,

	und Sekundärbewertung wurden nach Verwendungswert getrennt.	Compliance
Timeline Engineering	Die relevanten Ereignisse des Fallzeitraums wurden in eine prüffähige Chronologie gebracht.	Case Intelligence, Incident Reconstruction
Fristenradar	Rechtsbehelfs- und Sicherungsfristen wurden als Sofortprioritäten isoliert.	Emergency Case Support, Deadline Triage
Widerspruchsmatrix	Versionen, Beteiligungsschritte, Einlassungen und sonstige Schlüsseldaten wurden gegeneinander geprüft.	Document Review, Procedural Integrity
Deliverable Engineering	Aus Rohmaterial entstand ein strukturiertes Dossier mit Executive-, Beweis- und Verfahrensebene.	Rapid Reporting, Executive Briefing

Emergency Engagement - typischer 48h Ablauf

01. 0-2 h: Intake, Zieldefinition, Fristenscan, Datenquellen erfassen
02. 2-8 h: Dokumentklassifikation, Primärquellen priorisieren, Konflikt-/Lückenliste
03. 8-20 h: Timeline, Einlassungs-/Evidenzmatrix, Normen- und Zuständigkeitsmapping
04. 20-36 h: Gegenhypothesen, Qualitätskontrolle, Executive und Technical View
05. 36-48 h: konsolidiertes Rapid-Response-Pack, Übergabe, offene Punkte und nächste Sicherungsmaßnahmen

08 TECHNICAL FORENSICS: RESEARCH- UND EVIDENCE-ENGINEERING-PORTFOLIO

Die beigefügten technischen Ausarbeitungen bilden kein einzelnes Paper, sondern einen zusammenhängenden Research-Korpus. Für die Außendarstellung werden exploitnahe Details bewusst nicht als operative Anleitung wiedergegeben. Sichtbar gemacht werden die forensischen Fähigkeiten, die Labor- und Evidenzmethodik sowie die daraus ableitbaren Kundenleistungen.

Mobile / Firmware / Boot Chain

Analyse von Restore-Artefakten, IPSW-/Modell-Mismatches, Secure-Boot-/SEPOS-Indikatoren und hardware-nahen Angriffshypothesen. Einsatz als Plausibilitäts- und Artefaktprüfung, nicht als offensive Anleitung.

Kernel & Code Integrity

Korrelation von Kernel-/Kext-Artefakten, Code-Signing-/AMFI-Kontext, Speicher- und Load-Events sowie statischer Binäranalyse. Fähigkeit, beobachtete Systemzustände gegen technische Angriffshypothesen zu testen.

Sysdiagnose / TCC / Keychain

Extraktion, Normalisierung und Korrelation von TCC-, Keychain-, Security- und Systemereignissen. Fokus auf Herkunft, Zeitbezug, Berechtigungszustand, UI-/Prompt-Kontext und Gerätewechsel.

CKKS / Trust Circle / Account Persistence

Analyse von CloudKit Keychain Sync, Trust-Beziehungen, Legacy-Zuständen und geräteübergreifender Kontinuität. Der Research-Korpus untersucht ausdrücklich die Hypothese account-/cloudbasierter Persistenz.

Protocol & Protobuf Analysis

Byte- und feldorientierte Analyse von Protocol-Buffer-Strukturen, Varints, IDs, Zeit- und Flag-Feldern sowie manuellem Parsing/Encoding in isolierten Testumgebungen. Marktwert: Protokollanalyse, Reverse Engineering, Datenformat-Audit.

Timeline & Causality Engineering

Event-Korrelation über Restore, Kernel, Cloud, TCC, Netzwerk und Benutzerinteraktion. Eigene Parser und Kausalitätslogik dienen dazu, zeitliche Nähe, fehlende lokale UI-Ereignisse und alternative Erklärungen prüfbar zu machen.

Network / Cloud Traffic Review

Rekonstruktion von TLS-/HTTP2-/Private-Relay-bezogenen Sessions, Volumen- und Timing-Analyse sowie Mapping von Netzwerkereignissen zu Artefakten. Fokus auf beweisbare Metadaten statt spekulative Attribution.

Chain of Custody & Evidence Packaging

SHA-256-Hashing, Evidence Logs, manifestbasierte Übergabe, WORM-/Read-only-Prinzipien, UTC-Zeitstempel, signierte Transferpakete, Hash-Audits und dokumentierte Ursachenanalyse bei Mismatch.

Digital Twin / TRL-5 Reproduction

Modellhafte Reproduktion beobachteter Kausalketten in isolierter Laborumgebung. Ziel ist die technische Plausibilisierung und Reproduzierbarkeit ohne Verbreitung scharfer Schadsoftware.

Responsible Disclosure

Strukturierung eines Hersteller-/Prüfstellen-tauglichen Disclosure-Pakets mit Executive Summary, Impact, Artefaktindex, Hashes, Prüfplan, Remediation-Fragen und zweistufiger Rohdatenfreigabe unter kontrollierten Bedingungen.

Court-ready Technical Reporting

Executive Summary, Methodology, Findings, IOCs, Risiko-/Limitationskapitel, Gegenhypothesen, Artefaktinventar, Hash-/CoC-Anhänge und klar definierte externe Re-Validation als professioneller Gutachtenworkflow.

09 TECHNICAL TOOLCHAIN & DELIVERABLE ENGINEERING

Der technische Wert liegt nicht nur im Lesen von Logs. Der Arbeitsbestand zeigt den Aufbau eigener Analyse- und Verpackungslogik, mit der große Evidenzmengen reproduzierbar bearbeitet werden können.

- ChainOfCustodyManager: datebasierte SHA-256-Prüfung, Evidenzlog, finaler Bundle-Hash und paketierte Übergabe.
- Mach-O/Protobuf-Audit: Suche nach Protokollstrukturen und Provenienzmarkern in Binärdaten.
- Robust Log Parser: Streaming-Auswertung strukturierter Logdaten und Trennung von CKKS-, TCC- und lokalen UI-/Authentifizierungseignissen.
- Causality Engine: zeitliche Ausrichtung heterogener Events, statistische Korrelation und Export einer nachvollziehbaren Kausalitätsmatrix.
- CKKS Evidence Pipeline: Evidence Packaging, Parser, Reporting und reproduzierbare Arbeitsprodukte als wiederverwendbarer Forensik-Workflow.
- Gerichtsfester Prüfplan: Firmware/IPSW, Kernel/Kext, Sysdiagnose/TCC/Keychain, Netzwerk/iCloud, Media Recovery sowie Hash-/CoC-Audit werden als getrennte Artefaktgruppen behandelt.
- Laborprinzip: dynamische Tests isoliert/air-gapped; Originale bleiben unverändert, Arbeitskopien readonly; technische Schlussfolgerungen werden als vorläufig gekennzeichnet, bis unabhängige Laborprüfung vorliegt.

Typische technische Deliverables

- Evidence Register / Hash Manifest
- Artifact Inventory & Source Classification
- Super-Timeline / Event Correlation Matrix
- TCC / Keychain / CKKS Correlation Report
- Firmware / Restore / Kernel Evidence Review
- Network Metadata & Session Reconstruction
- Chain-of-Custody / Safe Material Transfer Package
- Digital-Twin Reproduction Note
- Responsible-Disclosure Package
- Executive + Technical + Legal/Compliance Views aus demselben Evidenzkern

Sicherheits- und Qualitätsgrenze

R&A Legal Ops Consulting positioniert exploitnahe Forschung als defensive Validierungs- und Forensikleistung. Kunden erhalten Nachweisführung, Reproduktion, Risikobewertung und Remediation-Input - keine unautorisierte Angriffsdurchführung.

10 OPERATING MODEL: DIE TRIADE ALS ANALYSEPIPELINE

Branding-Visual: Human Lead + KI-Copiloten. Arius und Lorien sind keine natürlichen Mitarbeiter, sondern Rollen für ChatGPT und Google Gemini.

Die Triade ist als Human-in-the-loop-Modell kommerziell nutzbar, wenn ihre Rollen sauber getrennt bleiben: Der Human Lead verantwortet Kontext und Freigabe; Lorien/Gemini dient als analytisches Radar; Arius/ChatGPT strukturiert, prüft und übersetzt technische Befunde in adressatengerechte Argumentations- und Dokumentformate.

HUMAN LEAD	LORIEN	ARIUS
Souverän / Human Lead	Analytisches Radar	Legal / Communication Layer
Scope, Primärkontext, Quellenbewertung, Entscheidung und finale Freigabe.	Breite Dokument-/Datenanalyse, Mustererkennung, technische Hypothesen und Gegenhypothesen.	Strukturierung, argumentative Prüfung, Risikoübersetzung und fertige Deliverables.
Qualitätssicherung Die KI darf keine Beweisklasse erzeugen, die das zugrunde liegende Artefakt nicht besitzt. Jede hochriskante Aussage wird auf Quelle, Gegenhypothese, Reproduzierbarkeit und Formulierung geprüft.		

11 SERVICES & COMMERCIAL OFFERING

48H Rapid Response / Emergency Case Intelligence

Zeitkritische Fremddaten, kurze Fristen und unübersichtliche Beweislagen: innerhalb von 48 Stunden nach vollständigem Intake eine erste belastbare Lagekarte, Quellenmatrix, Timeline, Fristen-/Risikoübersicht und priorisiertes Case Intelligence Pack.

DFIR / Mobile Forensics Review

Second-opinion Analyse kompromittierter Smartphones und zugehöriger Cloud-/Account-Artefakte; Fokus auf Timeline, Berechtigungen, Anomalien und nächste Sicherungsschritte.

Apple / iCloud Security Assessment

Analyse von Apple-ID, Trust- und Sync-Kontexten, TCC-/Account-Spuren und ungewöhnlichen Cloud-Zuständen. Keine Herstellerzertifizierung, sondern unabhängige forensische Prüfung.

Evidence Integrity Review

Prüfung von Hashes, Exporten, Metadaten, Dateipfaden, Chain-of-Custody und Beweissicherungsprozessen.

Incident & Case Intelligence

Konsolidierung unübersichtlicher Vorfälle in Executive Brief, technische Timeline, Evidenzregister, Hypothesenmatrix und Open Questions.

GRC / Legal Ops Support

Technische Sachverhalte für Compliance, Datenschutz, Rechtsabteilung oder externe Kanzlei übersetzen; Normen- und Pflichtenbezug ohne Rechtsberatung zu ersetzen.

Research & Reproduction Lab

Reproduzierbare Testumgebungen, Protokoll-/Formatdekodierung, Python-basierte Analysehilfen und dokumentierte Versuchsanordnungen.

AI-assisted Evidence Review

Strukturierte Nutzung mehrerer KI-Modelle für Dokumentenclustering, Gegenhypothesen, Extraktion und Qualitätsprüfung unter menschlicher Verantwortung.

12 CLIENT OUTCOMES

Kunden kaufen keine Terminologie. Sie kaufen Klarheit, Risikoreduktion und Handlungsfähigkeit. Deshalb wird jede Leistung in ein konkretes Ergebnis übersetzt.

Schnellere Entscheidungen	Ein komplexer Incident wird in wenige priorisierte Fragen, belastbare Fakten und nächste Handlungen zerlegt.
Weniger Fehlattribution	Technische Auffälligkeit, Hypothese und Täterschaft werden getrennt; alternative Ursachen werden sichtbar gemacht.
Bessere Beweissicherung	Preservation Scope, Hashing, Metadaten und Quellenstatus werden früh dokumentiert.
Übersetzbarkeit	Engineering, Management, Legal und Compliance erhalten unterschiedliche Sichten auf denselben Evidenzkern.
Auditierbarkeit	Jede wesentliche Schlussfolgerung lässt sich auf Quelle, Transformation und Unsicherheitsgrad zurückführen.
Langfristige Wissensbasis	Dossiers, Timelines und Register bleiben als Case Memory nutzbar, statt nach dem Incident im E-Mail-Verkehr zu zerfallen.

13 ENGAGEMENT MODEL & MARKET POSITIONING

Geeignete Mandate

- Akuter Fall mit kurzer Frist oder eskalierender Personal-/Compliance-/Beweislage, der binnen 48 Stunden strukturiert werden muss
- Executive- oder Mitarbeitergerät mit unklaren Auffälligkeiten
- Streit über Integrität oder Herkunft digitaler Beweismittel
- Incident mit vielen heterogenen Logs, Dokumenten und Zeitachsen
- Apple-/Cloud-/Account-Sicherheitsfragen ohne eindeutige Standardantwort
- Kanzlei oder Compliance-Team benötigt technische Übersetzung und Evidenzstruktur
- Interne Untersuchung benötigt unabhängige Second Opinion oder Preservation-Konzept

Abgrenzung

- Keine Rechtsberatung und keine anwaltliche Vertretung; technische und prozessuale Unterstützungsleistung.
- Keine Behauptung von Täterschaft ohne belastbare Attribution.
- Keine Offensive Security gegen Dritte ohne klare Autorisierung und Scope.
- Keine künstliche Hochstufung von Screenshots, Rekonstruktionen oder KI-Ausgaben zu Primärbeweisen.
- Keine Hersteller- oder Behördenzertifizierung vortäuschen; Qualifikation wird über Arbeitsproben, Methodik und Ergebnisse belegt.

Positionierungssatz

R&A Legal Ops Consulting steht für unabhängige technische Tiefenprüfung dort, wo Digitalforensik, Cloud-/Account-Security und Verfahrensintegrität ineinandergreifen - einschließlich 48h Rapid Response für zeitkritische Fremddaten und Incident-/Case-Triage.

14 EVIDENCE OF CAPABILITY

Der Drive-Bestand dokumentiert wiederkehrend dieselben Fähigkeitsmuster über mehrere Monate und Projekte hinweg. Für das Portfolio werden sie nicht als unumstrittene externe Tatsachenbehauptungen präsentiert, sondern als Arbeitsnachweise und Research-Artefakte.

Arbeitsnachweis	Belegt als Fähigkeit	Portfolio-Status
„Hochprofessionelles Portfolio der Befähigung und Leistung - Lead Analyst“ ([DATUM ANONYMISIERT])	Mobile/Cloud-Forensik, CKKS, Framework- und Dossierarbeit	Drive-Arbeitsdokument
„Forensische Validierung des CKKS-Vorfalles“ ([DATUM ANONYMISIERT])	Byte-Level-Protobuf-Dekodierung, Zeit-/Flags-Interpretation	Technische Research-Arbeit
„Forensisch-Technisches Hauptgutachten_GOTHAM_APT“ ([DATUM ANONYMISIERT])	Artefaktinventur, Hash-/Metadaten-, Timeline- und Strukturkorrelation	Gutachtenentwurf / Analyse
„Gesicherte Terminal-Ausgabe7.pdf“ und Hash-Inventare	Hashing, Dateiinventur, Artefaktlokalisierung; zugleich Beispiel für nötige Quellenkritik bei rekonstruierten Terminalausgaben	Arbeits-/ Beweissicherungsbestand
Legal-Ops / Master-Dossier-Bestände	Langform-Dokumentation, Evidenzhierarchien, Chronologien und Normenmatrizen	Case Intelligence / Legal Ops

Technischer Quellen- und Research-Korpus

Arbeitsdokument	Portfolio-Relevanz
-----------------	--------------------

Digital Kompromittierung durch AppleSync.pdf	CKKS-Übertragungsweg, Trust Circle, Gerätewechsel, TCC-/Keychain-Korrelation.
Einmaliger Nachweis einer kontobasierten Apple-APT durch Trust-Circle-Kompromittierung.pdf	Gesamtkette und Vergleich mit bekannten Angriffsmustern; forensische Einordnung.
Forensischer Responsible-Disclosure Report: Persistente Trust-Circle-Persistenz in Apples iCloud-Schlüsselbund-Architektur.pdf	Responsible Disclosure, Artefakt-/Prüfpaket, zweistufige Datenfreigabe, Hersteller-/Drittprüfung.
Fertiger Sicherheitsbericht (Markdown).pdf	Apple-Security-Bounty-orientierter Bericht mit Impact, Scope, Logs und Remediation-Fragen.
Fertiger Sicherheitsbericht (Markdown)(2).pdf	Zweite vorliegende Fassung desselben Security-Report-Arbeitsstands.
Forensisch-Technische Analyse und Reproduktion einer Hardware-basierten iOS-Exploit-Kette.pdf	Scientific Exploit Framework / Digital Twin; Hardware-, Kernel- und Cloud-Phasen als Laborreproduktion.
TECHNISCHES DOSSIER (Gerichtsfest).pdf	Gerichtsfester Workflow: Preservation, Hash Audit, Artefakttriage, externe Re-Validation, CoC/SMT.
Das Update für dein Framework_ CloudKitInjector (High-Fidelity).pdf	Protobuf-/Wire-Format-Arbeit und feldorientierte Analyse für isolierte Reproduktionsumgebungen.
CKKS Forensic Evidence Pipeline Gold Standard - Colab.pdf	Eigene Evidence-Pipeline mit Hashing, Packaging, Binary-/Log-Parsing und Kausalitätsauswertung.
die absolute Unabhängigkeit des „Ritterschlags“ mit der finanziellen pdf	Enthält zusätzlich technische Executive-Summaries und Anforderungen an unabhängige Tier-1-/Laborprüfung; prozessuale Teile werden im Portfolio getrennt behandelt.

15 90-DAY PROFESSIONALIZATION ROADMAP

0-30 Tage	Portfolio, Leistungsbeschreibungen und Standard-Templates finalisieren. Zwei anonymisierte Sample Reports erstellen: Mobile Forensics Review und Evidence Integrity Review.
31-60 Tage	Reproduzierbare Lab-Demos aufbauen: iOS/TCC/SQLite-Artefakte, Protobuf-Parsing, Hash-/Timeline-Workflow. Öffentliche Research Notes mit klarer Beweisklassifikation veröffentlichen.
61-90 Tage	Pilotmandate mit Kanzleien, IT-Dienstleistern, Datenschutz-/Compliance-Beratern oder mittelständischen Unternehmen. Feedback in Scope, Preisstruktur und Deliverables einarbeiten.

Empfohlene Angebotsbausteine

- Forensic Triage (fixed scope)
- Evidence Integrity Review (fixed scope)
- Case Intelligence Pack (project based)
- Apple/iCloud Research Assessment (project based)
- Legal/Compliance Technical Support (day rate / retainer)
- Research Lab & Reproduction (custom scope)

16 PROFESSIONAL STATEMENT

R&A LEGAL OPS CONSULTING

Die Befähigung ist real dort, wo sie überprüfbar wird: in sauberer Quellenarbeit, tiefen technischen Analysen, reproduzierbaren Prüfschritten und einer Dokumentation, die auch außerhalb des eigenen Narrativs Bestand hat. Genau diese Transformation macht aus jahrelanger Eigenforschung eine marktfähige Beratungsleistung.

Lead Analyst positioniert sich als unabhängiger IT-Forensik- und Research-Spezialist an der Schnittstelle von Digital Evidence, Mobile/Cloud Security und Procedural Integrity. Die Stärke liegt in der Ausdauer bei komplexen Datenlagen, der Fähigkeit zur technischen Tiefenbohrung, der schnellen Adaption an Fremddaten und der Übersetzung großer Beweisbestände in klare, nachvollziehbare Entscheidungsstrukturen. Operation UNCLE SAM demonstriert, dass diese Arbeitsweise auch unter akutem Zeitdruck auf einen zuvor fremden Fall übertragen werden kann.

Brand promise

ANALYZE. VERIFY. DOCUMENT. PROTECT. DELIVER.

FACTA NON VERBA

R&A Legal Ops Consulting | ra-legal-ops.de