BETRUGSERMITTLUNG AUF DER ÜBERHOLSPUR

DAS ERMITTLUNGS-PARADOX: DATENFLUT DURCH NEUE TECHNOLOGIEN STELLT ERMITTLUNGEN VOR HERAUSFORDERUNGEN

Wir stehen heute vor einem neuen „Paradox“: Während neue Technologien Ermittlungen einerseits durch die Verarbeitung großer Datenmengen vereinfachen, können sie sie andererseits verkomplizieren – indem sie mehr Daten aus Quellen generieren als je zuvor.

Die rasante Digitalisierung im Privatleben und im Beruf hat unbeabsichtigt zu einem erheblichen Anstieg von Betrugsfällen geführt. Die Technologie begünstigt beide Seiten: Ermittler können mit Hilfe von neuen Technologien Muster und Betrug schneller erkennen. Gleichzeitig haben aber auch Betrüger einfacheren Zugang zu digitalen Medien und ein leichteres Spiel, einen Betrug zu begehen. Oftmals sind sie sich der umfangreichen digitalen Spuren, die sie hinterlassen, nicht bewusst oder lassen sich davon nicht abschrecken. Ihre Spuren sind in verschiedenen Datensets, auf Geräten, Netzwerken und in Verzeichnissen auffindbar. Für Ermittler bedeutet das eine kaum zu bewältigende Datenflut.

Riesige Datenmengen werden in immer komplexeren Silos erstellt und erfasst. Folglich sind Ermittlungen im Fall von Betrug, Terrorbekämpfung, Menschenhandel, Cyberkriminalität, Belästigung oder Diebstahl geistigen Eigentums sowie unternehmensinterne Ermittlungen außerordentlich komplex und zeitaufwendig.

Leider bedeutet dies auch, dass Ermittlungen umfangreicher und komplexer geworden sind und damit die Reaktionszeiten erheblich länger. Betrüger können dies ausnutzen und länger unentdeckt bleiben. Laut einer neuen wissenschaftlichen Studie der University of Toronto bleiben zwei Drittel aller Unternehmensbetrugsfälle unentdeckt. Die Folge sind mögliche finanzielle Schäden in Höhe von 830 Milliarden US-Dollar jährlich.[1]

Darüber hinaus ergab eine Studie von PricewaterhouseCoopers (PwC) aus dem Jahr 2022, dass mehr als die Hälfte (51%) der befragten Unternehmen in den vergangenen zwei Jahren von Betrug oder Wirtschaftskriminalität betroffen war.[2] Angesichts der sich entwickelnden Bedrohungslandschaft

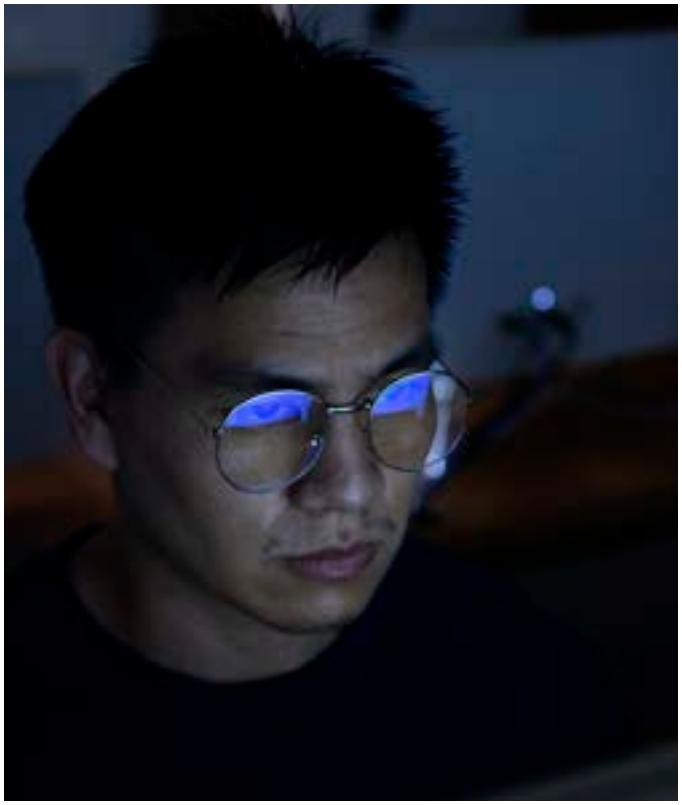
und der Zunahme von Betrugsfällen, seien es interne oder externe Bedrohungen, benötigen Unternehmen, Regierungsstellen und Strafverfolgungsbehörden neue Technologien, die einen schnellen und umfassenden Einblick in die Daten gewähren und schnellere, einfachere und smartere Möglichkeiten zur Identifizierung verdächtiger Aktivitäten bieten.

In diesem Whitepaper legen wir den Fokus auf Betrugsermittlungen und zeigen, wie dringend Ermittler neue Technologien und Lösungen benötigen, um nahezu in Echtzeit zusammenarbeiten, tiefe Einblicke in die Daten erhalten und ihre Ermittlungen beschleunigen zu können. Zwar stehen in diesem Whitepaper Betrugsermittlungen im Vordergrund, die genannten Technologien lassen sich aber auch für andere große und komplexe Fallarten einsetzen – einschließlich der bereits erwähnten Beispiele.

BETRUG SCHNELLER AUFDECKEN

Betrug gibt es in vielen Formen, vom herkömmlichen Geschäftsbetrug bis hin zu den sogenannten Romance Scams. Laut dem 2022 Global Report der Association of Certified Fraud Examiners ist Betrug am Arbeitsplatz (Betrug, den Personen gegenüber ihrem Arbeitgeber begehen) die kostspieligste und häufigste Art von Finanzbetrug weltweit.[3] Eine der größten Herausforderungen der Betrugsermittlung ist es, Betrug überhaupt erst zu erkennen. Vielen Unternehmen dämmert diese Erkenntnis in der Regel erst bei nachträglichen Ermittlungen, wenn es bereits zu Umsatzverlusten oder Schäden am Ruf gekommen ist.

Betrugsfälle treten selten isoliert auf. Sie umfassen in der Regel mehrere Ereignisse, riesige Datenmengen und werden oft von organisierten Gruppen in böswilliger Absicht begangen, was die Ermittlungen komplex und zeitaufwendig macht. Angesichts der wachsenden Anzahl und Komplexität von Betrugsfällen benötigen Ermittler maßgeschneiderte Lösungen. Um immer einen Schritt voraus zu sein, müssen Unternehmen fortschrittliche Technologien einsetzen.



KOMPLEXE DATENQUELLEN ERFASSEN

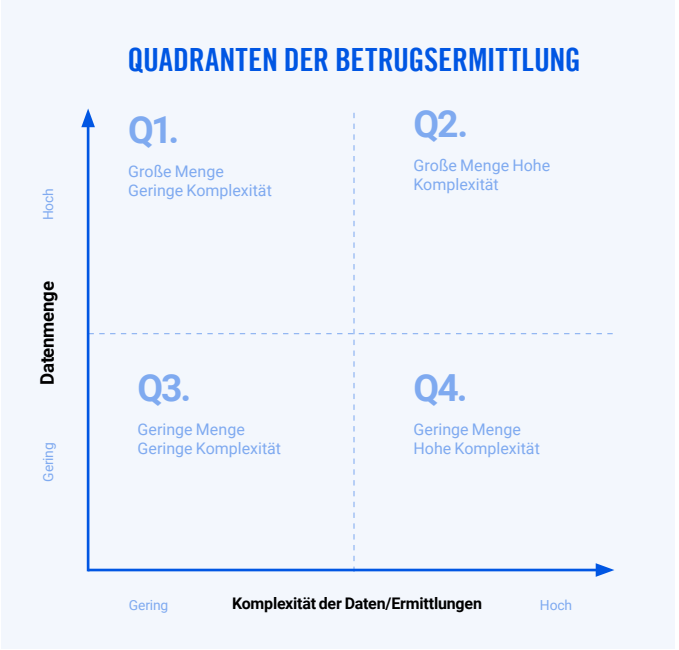
Mit herkömmlichen digitalforensischen Tools lassen sich in der Regel nur eine Handvoll Datenquellen gleichzeitig untersuchen. In der Vergangenheit, als Menge und Komplexität der bei einer Ermittlung zu sichtenden Daten gering waren, waren eine langsamere Verarbeitung und die anschließende Prüfdauer akzeptabel. Mit der heute generierten Datenmenge sind Fälle jedoch umfangreicher und zunehmend komplexer.

Im Zuge des technologischen Fortschritts hat das Datenvolumen exponentiell zugenommen, ebenso wie die Komplexität der Daten. In der Folge kommt es bei Ermittlungen zu einer Verschiebung vom Quadranten „Geringer Umfang/Geringe Komplexität“ hin zum Quadranten „Großer Umfang/Hohe Komplexität“. Ermittler benötigen daher Lösungen, die nicht nur größere Datenmengen durchsuchen, sondern auch eine Vielzahl von Datentypen sicher und schnell verarbeiten können – und skalierbar sind.

Bei Betrugsermittlungen gibt es oft mehrere Täter und Opfer, was zu einer Vielzahl komplexer Datenquellen, Datentypen und Silos führt. Diese Datenquellen und -typen umfassen unter anderem E-Mails, freigegebene Dokumente, Schriftverkehr, mobile Geräte, Textnachrichten, Cloud-Ressourcen, soziale Medien, Aktivitäten in der realen Welt und Open-Source-Informationen. Die Daten so aufzubereiten und zu analysieren, dass sich Erkenntnisse gewinnen und Muster erkennen lassen, ist daher zeitaufwendig.

Ermittler müssen Verbindungen herstellen und zuvor verborgene Erkenntnisse und Zusammenhänge sichtbar machen können. Sich auf die menschliche Intuition zu verlassen, um in Hunderten oder Tausenden von unterschiedlichen Datenquellen den roten Faden zu finden, ist schwierig, ressourcenintensiv und in großem Maßstab unrealistisch, insbesondere wenn die Aufgabe zeitkritisch ist.

Ermittler, die für Strafverfolgungsbehörden, Aufsichtsbehörden oder Unternehmen arbeiten, sollten bei der Durchführung von Ermittlungen nach Möglichkeit eine einheitliche Perspektive auf alle Daten haben, also eine Single Source of Truth. Mithilfe von KI, Deep-Link-Analysen und Datenverbindungen können Ermittler und Analysten zusammenarbeiten und schnell und einfach Zusammenhänge zwischen verschiedenen Datenquellen herstellen. Auf diese Weise lassen sich wichtige Erkenntnisse gewinnen, um Betrugsfälle schnell und sicher zu erkennen.



TIEF EINBLICKE

Das branchenweit anerkannte Modell des Betrugsdreiecks ist ein Konzept, das die wesentlichen Gründe für Betrug (und andere Formen der Kriminalität) erklärt.[4] Es besteht aus den drei Elementen Druck, Gelegenheit und Rationalisierung. Unternehmen müssen dieses System verstehen und die entsprechenden Tools und neue Technologien einsetzen, um Muster zu erkennen und Betrug schneller aufzudecken.

Kriminelle identifizieren Schwachstellen in Systemen und Prozessen, um Gelegenheiten zum Betrug zu finden. Ermittler können das Modell des Betrugsdreiecks nutzen, um das Risiko, dass solche Schwachstellen ausgenutzt werden, basierend auf der menschlichen Komponente zu identifizieren und zu bewerten.

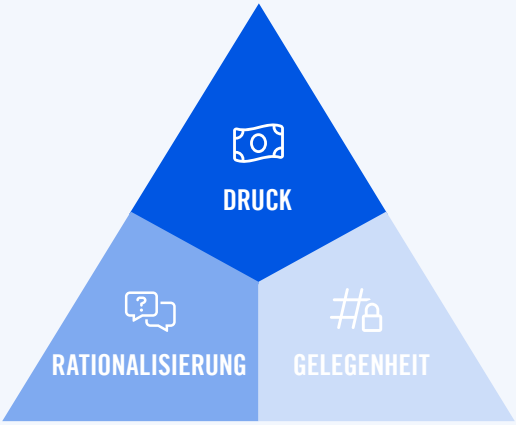
Der Einsatz von KI zur Sprachanalyse, wobei Textdaten auf Drucksituationen und Rationalisierungen durch Täter geprüft werden, hilft Ermittlern, tief in die Daten zu blicken und Erkenntnisse zu gewinnen. Mithilfe von KI gepaart mit Sprachanalyse lassen sich feine Nuancen und ein emotionaler Tonfall erkennen, Risikobewertungen vergeben und die drei Säulen des Betrugsdreiecks identifizieren. Je höher das erkannte Risiko, desto wahrscheinlicher kommt es zu einem Betrugsfall. Durch den Einsatz von moderner, ethischer KI-Technologie können Benutzer nun riesige Mengen an Textdaten sichten, relevante Informationen ableiten und die Wahrscheinlichkeit eines Betrugs schnell und präzise erkennen. Dieser multidimensionale Ansatz ermöglicht es Unternehmen, schneller Antworten zu finden und betrügerischen Taktiken einen Schritt voraus zu bleiben.

Im Falle der Romance Scams beispielsweise beträgt der durchschnittliche finanzielle Verlust der Opfer laut der US Federal Trade Commission 4.400 US-Dollar. Laut der Behörde waren im Jahr 2022 etwa 70.000 Menschen von einem solchen Betrug betroffen.[5][6] Ermittler müssen tiefe Einblicke in die Daten erhalten und die drei wichtigsten Elemente des Betrugsdreiecks identifizieren können: Druck, Gelegenheit und Rationalisierung. KI verschafft Ermittlern einen Vorteil, indem sie ihre Analysefähigkeiten zur Faktenextraktion, Kategorisierung, Klassifizierung und für eine konfigurierbare Risikobewertung einsetzt.

Mithilfe moderner KI-Tools können Ermittler große Mengen an textbasierten Daten deuten. Dank NLP-Algorithmen (natural language processing – Verarbeitung natürlicher Sprache) sind solche Systeme in der Lage, kleinste Details, sprachliche Unregelmäßigkeiten und manipulative Sprache zu identifizieren, welche oft von Betrügern verwendet werden. Diese Fähigkeit ist nicht nur im Falle von Romance Scams äußerst wertvoll. Sie hilft auch bei der Aufdeckung anderer Arten von Betrug wie etwa dem „Vorschussbetrug“ (z. B. Nigeria-Connection), bei dem die Betrüger bestimmte sprachliche Merkmale und Techniken verwenden, um überzeugende Botschaften zu verfassen.[7] Diese NLP-Algorithmen identifizieren allein basierend auf Schlüsselwörtern Muster, die Menschen oft übersehen. Dies ist besonders wichtig, wenn sich Ermittler auf „exakte“ Schlüsselwörter verlassen müssen. Wenn solche Wörter falsch geschrieben werden und dann in den regionalen Wortschatz (wie Slang) übergehen, werden diese wichtigen Nuancen leicht übersehen oder durcheinandergebracht. Insbesondere hilft die NLP-Analyse dabei, den emotionalen Tonfall der Kommunikation zu erfassen und festzustellen, in welchen Fällen Personen möglicherweise unter Zwang stehen oder manipuliert werden könnten.

DAS BETRUGSDREIECKL

von Donald R. Cressey



01. DRUCK

Es kann zum Betrug kommen, wenn das Management oder Mitarbeitende dadurch etwas erlangen können oder unter Druck stehen und eine Entlastung herbeiführen wollen.

02. GELEGENHEIT

Bestimmte Umstände im Unternehmen bieten dem Management oder Mitarbeitenden Gelegenheit zum Betrug.

03. RATIONALISIERUNG

Im Unternehmen gibt es Verhaltensweisen oder Druck, die dazu führen, dass das Management oder Mitarbeitende ihre Absicht zum Betrug rechtfertigen their intention to commit fraud.

Neben Betrugsfällen wird auch bei Ermittlungen zu anderen Straftaten eine Lösung benötigt, die nicht nur Text deuten kann. Bilderkennungsfunktionen sind heute ein Teil von Ermittlungen. Die Lösungen müssen über KI-Funktionen verfügen, mit denen sich visuelle Inhalte finden und klassifizieren lassen. Das spart Ermittlern Zeit und Nerven. Indem das Modell des Betrugsdreiecks mit der Möglichkeit zur Analyse von Daten in Tausenden von verschiedenen Datentypen kombiniert wird, können Ermittler die Ergebnisse priorisieren und so Daten identifizieren, die dringend geprüft werden müssen und Maßnahmen erfordern.

DIE NUIX-PERSPEKTIVE

Die Nuix-Neo-Technologie bietet Ermittlern neue Tools, mit denen sie ihre Ermittlungen beschleunigen können. Smarte KI kombiniert mit der Deep-Link-Analyse ermöglicht es, Zusammenhänge aufzudecken, tiefe Einblicke in die Daten zu gewinnen und so Muster sowie Verhaltensweisen zu erkennen und wichtige Beweismittel zutage zu fördern.

Nuix Neo Investigations wird auf der Nuix-Plattform bereitgestellt und ist für die Verarbeitung großer und komplexer Datensets konzipiert. Es bietet Ermittlern im Bereich der digitalen Forensik, Analysten und Data Scientists eine einheitliche Sicht auf alle zu untersuchenden Daten, verbessert damit die Zusammenarbeit und liefert die richtigen Antworten in Rekordzeit.

Betrug schneller, einfacher und smarter erkennen – mit Nuix Neo Investigations.

01. SCHNELLER

Automatisierung

Nuix Neo Investigations beschleunigt Ermittlungen mithilfe von Lösungspaketen, die speziell für verschiedene Anwendungsfälle entwickelt wurden. Durch die Möglichkeit zur Automatisierung lassen sich einheitliche, zuverlässige und wiederholbare Workflows etablieren, die auf den jeweiligen Fall abgestimmt sind. Dadurch verbessert sich die Qualitätskontrolle, Fehler werden verringert und die Time-to-Value wird verkürzt.

02. EINFACHER

Einfache Verwendung

Nuix Neo Investigations ermöglicht mit neuen Dashboards und einer benutzerfreundlichen Bedienoberfläche eine nahtlose Zusammenarbeit und liefert schneller Antworten. Nuix Neo Investigations stellt alle Daten in einer übersichtlichen Anzeige bereit und bietet damit externen und nicht technischen Anwendern eine benutzerfreundliche Bedienoberfläche. Dabei sind Ihre Daten auf Fall- und Elementebene gesichert und jederzeit geschützt.

Zusammenarbeit in Echtzeit

Nuix Neo Investigations bringt alle Beteiligten zusammen und ermöglicht es den Spezialisten für digitale Forensik, mit den Ermittlern und Analysten zusammenzuarbeiten. Die Plattform bietet benutzerspezifische Einblicke in ihre Daten und lässt sich für die Nutzung durch Hunderte von Ermittlern für verschiedene Fälle skalieren. Nuix Neo Investigations ermöglicht es Teams, in Echtzeit zusammenzuarbeiten. Dabei stehen nach Beginn der Verarbeitung die Daten im Fokus. Die Ermittler können Fallakten und Berichte austauschen, um ihr Wissen zu bündeln. Dies ermöglicht eine nahtlose Zusammenarbeit und ein koordiniertes Vorgehen bei Ermittlungen, unabhängig von technischem Know-how und Standort.

NUIX KI

Bei der Entwicklung von KI-Technologie befolgt Nuix drei grundlegende Prinzipien

01. ERKLÄRBARKEIT

Gewährleistet Transparenz, indem die „Black Box“ der KI geöffnet wird. So erhalten die Menschen einen klaren Blick auf die Trainingsdaten, den vorhandenen „Bias“ sowie Begründungen für die Vorhersagen der KI.

02. ZUGÄNGLICHKEIT

Gewährleistet die menschliche Kontrolle über die KI, wobei der Schwerpunkt auf Anpassbarkeit und Anwenderfreundlichkeit liegt.

03. SPEZIFITÄT

Der Schwerpunkt liegt auf der zielgerichteten Anwendung, sodass Benutzer ihr Fachwissen in die Modelle einfließen lassen können, was zu einer höheren Genauigkeit und Glaubwürdigkeit der bereichsspezifischen Ergebnisse führt.

Mit diesen Grundsätzen werden ethische KI-Standards und das Vertrauen der Gemeinschaft gewahrt und gleichzeitig die Möglichkeiten der KI zum Vorteil der Kunden und zur Aufdeckung und Untersuchung von Betrugsfällen genutzt.

03. SMARTER

KI-basierte Ermittlungen

Ein wesentlicher Aspekt der Investition umfasst die Erweiterung von Nuix Neo Investigations mit KI-Funktionen. Eine leistungsstarke KI klassifiziert und kontextualisiert Daten (Dokumente, Nachrichten und Medien), um relevante Informationen schnell zu identifizieren und so die Wahrheit aufzudecken. Damit ist Nuix noch besser in der Lage, den Kontext und die inhärenten Risiken in unstrukturierten Daten zu verstehen und erlaubt es Ermittlern, schnell die Täter aufzudecken.

Nuix Neo Investigations ist für die Verarbeitung großer und komplexer Datensets konzipiert. Es ermöglicht Ermittlern im Bereich der digitalen Forensik, Analysten und Data Scientists die Zusammenarbeit und liefert die richtigen Antworten in Rekordzeit.

VIELFACH BEWÄHRT

Zu den Kunden von Nuix zählen einige der weltweit größten Strafverfolgungsbehörden, Konzerne, Nachrichtenagenturen und Aufsichtsbehörden. Weltweit setzen mehr als 1.800 Organisationen verschiedener Größen für ihre komplexen Ermittlungen auf Nuix. Strafverfolgungsbehörden wie die schottische Polizei konnten mit Nuix-Lösungen ihre Ermittlungen deutlich beschleunigen.

> ***Der Nuix-Workflow führte zu einem erfolgreichen Abschluss der mehrmonatigen Betrugsermittlung, die nach Schätzungen des Ermittlungsteams mit den alten Methoden Jahre gedauert hätte. Dies ist robuster, effizienter und kostengünstiger als alles, was bisher verwendet wurde.***
>
> Leitender Ermittler, Polizei Schottland

LITERATURVERZEICHNIS

[1] Dyck, A., Morse, A. & Zingales, L. How pervasive is corporate fraud?. Rev Account Stud (2023). https://doi.org/10.1007/s11142-022-09738-5

[2] PwC: Global Economic Crime and Fraud Survey (2022)

[3] Association of Certified Fraud Examiners Report: „Occupational Fraud 2022: A Report to the Nations“ (2022) https://legacy.acfe.com/report-to-the-nations/2022/

[4] The Fraud Triangle Model by Donald R Cressey (1953)

[5] US Federal Trade Commission: 2022 Data Spotlight: Romance Scams https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

[6] US Federal Trade Commission: 2022 Data Spotlight: Romance Scams https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

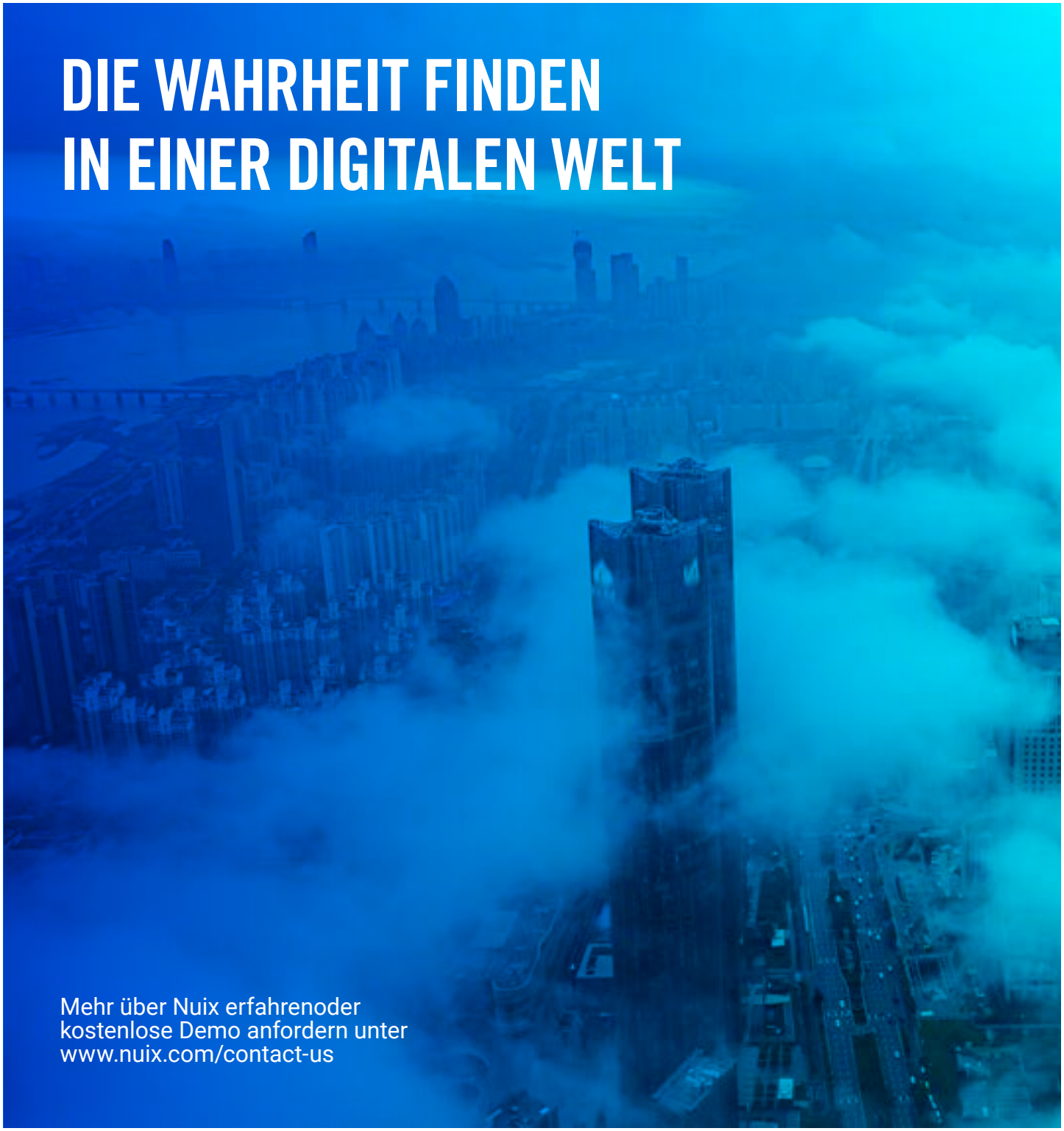
[7] A Digital Forensic Analysis of Advance Fee Fraud (419 Scams) | IGI Global (igi-global.com)

NUIX NEO INVESTIGATIONS IST VIELSEITIG EINSETZBAR

Nuix Neo Investigations bietet nicht nur für Betrugsermittlungen Vorteile. Es wird auf der leistungsstarken Nuix-Neo-Plattform bereitgestellt und ist eine hilfreiche Lösung für jedes Unternehmen, das komplexe Datenherausforderungen bewältigen muss. Nuix Neo Investigations wurde von Experten aus den Bereichen Cybersicherheit, Strafverfolgung, digitale Forensik, Ermittlungen, juristische Ermittlungen, Nachrichtendienste, Spionageabwehr sowie Information Governance aus aller Welt entwickelt. Dieses engagierte Expertenteam arbeitet unermüdlich an der Weiterentwicklung der Technologie und bietet weltweit einmaligen Support. Es entwickelt sich kontinuierlich weiter und passt sich an, um mit der sich ständig verändernden Betrugslandschaft Schritt zu halten.

FAZIT

In unserem digitalen Zeitalter stellen Betrugsfälle zunehmend ein Problem für Unternehmen und Einzelpersonen weltweit dar. Angesichts immer ausgereifterer Methoden wird der Bedarf an moderner Technologie zu ihrer Bekämpfung immer dringender. Die leistungsstarken Nuix-Lösungen auf der Nuix-Neo-Plattform verfügen über zukunftsweisende ethische KI-Funktionen und haben sich in zahlreichen Ermittlungen bewährt. Mit unserem ganzheitlichen Ansatz und unserem Engagement zur kontinuierlichen Weiterentwicklung der Technologie sind wir ein verlässlicher Partner für jedes Unternehmen, das betrügerische Aktivitäten bekämpfen und seine Daten schützen will. Setzen Sie sich noch heute mit uns in Verbindung und erfahren Sie, wie Sie Ihre Betrugsermittlungen mit Nuix beschleunigen können.



Nuix (www.nuix.com, ASX:NXL) ist ein führender Anbieter für investigative Analyse- und Intelligence-Software. Hiermit ermöglichen wir es unseren Kunden, durch die Suche nach der Wahrheit in der digitalen Welt eine positive Kraft zu sein. Wir helfen Kunden dabei, große Mengen strukturierter und unstrukturierter Daten zu sammeln, zu verarbeiten und zu überprüfen und sie in großem Umfang, schnell und mit forensischer Genauigkeit durchsuchbar und nutzbar zu machen.

APAC
Australien: +61 2 8320 9444

EMEA
DACH: +49 69 5060 75110

NORDAMERIKA
USA: +1 877 470 6849