MAGNET FORENSICS®

DFIR in der Praxis

Schnellere Ermittlungen mit modernen investigativen Lösungen

AXIOM CYBER™ | VERAKEY™ | AUTOMATE™ | REVIEW®

Triage → Collection → Automation → Kollaboration

[DER MOMENT DANACH]

Digitaler Forensiker / IR-Analyst

Denkt:

Welcher Endpoint? Wann? Welche Artefakte beweisen den Initialkompromiss?

Braucht:

Vollständige Daten. Schnell. Ohne physischen Zugriff.

Staatsanwalt / HR & Legal

Denkt:

Ist das gerichtsverwertbar? DSGVO-konform? Verhältnismäßig?

Braucht:

Dokumentierte Chain of Custody. Gerichtsfeste Erkenntnisse. Keine Lücken.

CISO / Behördenleitung

Denkt:

Was bedeutet das? Müssen wir melden? Wie schnell kann ich eine Entscheidung treffen?

Braucht:

Klarer Report. Sofort. In ihrer Sprache, nicht in Tool-Outputs.

Corporate oder Strafverfolgung: Alle stellen dieselbe Frage. Heute zeigen wir die Antwort.

Solutions Consultant
Since May 2022

Technical Pre-Sales
March 2018 – April 2022

Workgroup-Server Engineer
High-End Server Engineer
Systems Support Professional - Santa Clara, CA USA
(5yrs on intl. assignment)
Principal Support Engineer f. Cloud systems
March 2001 – Feb. 2018

User Help Desk for Sun Microsystems
High-End Server remote monitoring
March 2000 – Feb. 2001

System Engineer
Windows, Linux, Novell-Network
June 1999 – Dec. 1999

DST - Dieckmann Systemtechnik GmbH

Niels Renken

Solutions Consultant, EMEA

niels.renken@magnetforensics.com

AGENDA

Was Sie heute erwartet

01
Der Ermittlungs-Workflow
Triage → Collection → Automation → Review: Wie die Teile zusammenspielen

02
Magnet AXIOM Cyber
Endpoint, Cloud, IoT & Mobile: Alles in einer Plattform

03
Magnet VERAKEY
Mobile Forensik mit FFS-Extraktion: consent-basiert, schnell, vollständig

04
Magnet AUTOMATE
Automatisierung vom ersten Alert bis zum fertigen Bericht

05
Magnet REVIEW
Kollaborative Analyse für Security, HR und Legal: in einem Workspace

06
Real-World Szenarien & Diskussion
Wie Ihre Organisation von diesem Stack profitiert

DER WORKFLOW

Eine Untersuchung. Vier Phasen. Ein Ökosystem.

1

Triage & Scope

Was ist passiert? Welche Systeme? Wo beginnen?

AXIOM CYBER™

2

Collection

Remote. Mobile. Cloud. Vollständig & forensisch integer.

AXIOM CYBER™ +VERAKEY™

3

Processing & Automation

Automatisch klassifizieren, analysieren, priorisieren.

AUTOMATE™

4

Collaborative Review

Security, HR, Legal Gemeinsam, sicher, auditierbar.

REVIEW®

Der entscheidende Vorteil: Alle vier Tools teilen denselben Datensatz, kein Re-Import, keine Medienbrüche, keine Zeitverluste.

#1

MAGNET AXIOM CYBER™

Magnet AXIOM Cyber - Die Investigation Platform

Endpoint-Forensik

Windows, Mac, Linux: lokal oder remote, mit vollem Artefakt-Support.

Cloud & SaaS

Microsoft 365, Google Workspace, Slack, Box, Dropbox, direkt in den Fall.

Mobile Integration

iOS & Android über iTunes, MVT oder direkt. Nahtlose VERAKEY-Integration.

IoT & BYOD

Smart Devices, Wearables, Netzwerk-Logs: auch atypische Quellen.

Warum AXIOM CYBER™ ?

- Remote Collection ohne physischen Zugriff
- 71 % der Teams kämpfen damit. AXIOM löst es
- Multisource-Analyse in einem Case File
- KI-gestützte Artefakt-Klassifikation
- Unterstützt 500+ Artefakt-Typen
- Integrierte Timeline-Analyse
- YARA & MITRE ATT&CK Mapping eingebaut
- Exportfertige Reports für Legal & HR

59 % der DFIR-Professionals nutzen Remote-Computer-Daten regelmäßig : AXIOM Cyber macht das möglich, ohne Reisetätigkeit und ohne Datenverlust. (Magnet DFIR Report 2026)

MAGNET FORENSICS®

MAGNET AXIOM CYBER™

Drei Szenarien - eine Plattform

Ransomware Incident Response

- Remote-Triage von 50 Endpoints in < 2 h
- Cloud-Logs (M365) parallel erfassen
- YARA & MITRE ATT&CK Mapping automatisch
- Initialkompromiss identifiziert in Stunden, nicht Tagen

Insider Threat / HR-Ermittlung

- Endpoint + Email + Cloud in einem Case
- Timeline: Was hat wer wann gemacht?
- Exportierbare Erkenntnisse für Legal
- Chain of Custody lückenlos dokumentiert

M&A Due Diligence / IP-Schutz

- Scope: alle Geräte + Cloud-Repos
- Keyword-Search über alle Quellen
- Report für Management in Stunden
- Kein Rückgriff auf externe FSP nötig

Alle Szenarien: ein Case File, ein Workflow, eine Wahrheit, kein Datenexport zwischen Tools erforderlich.

MAGNET VERAKEY™

Magnet VERAKEY -Mobile Forensik der nächsten Generation

Warum Mobile der blinde Fleck ist:

65,5 % der DFIR-Teams sehen mehr mobile Geräte in Fällen

49,9 % scheitern an limitierten Daten-Extraktionen

46,7 % können nicht remote auf Geräte zugreifen

68 % bevorzugen FFS - aber bekommen oft nur Logical

Magnet DFIR Report 2025

VERAKEY™ löst das:

- Full File System (FFS) Extraktion - iOS & Android
- Consent-basiert - DSGVO-konform, auditierbar
- Schnell - kein Jailbreak, kein Root erforderlich
- Keychain & verschlüsselte Daten entschlüsselbar
- Gelöschte Artefakte wiederherstellbar
- Direkt in AXIOM Cyber Case integriert

VERAKEY ist consent-basiert: HR & Corporate BYOD.

Mobile-Beweise für jeden Stakeholder

Opfer- & Zeugengeräte / LE

Strafverfolgung, Opfer- oder Zeugengerät

Quellen: WhatsApp, Signal, Standortdaten, Fotos, Anrufprotokolle

Consent liegt vor -FFS-Extraktion vollständig & gerichtsverwertbar ohne Datenverlust.

HR & Compliance (Corporate)

Mitarbeiter-Fehlverhalten / Datenleck

Quellen: SMS, Telegram, Kamera-Uploads, App-Nutzung, Cloud-Sync

Consent-basierte Extraktion - rechtlich sauber, DSGVO-konform.

Legal / Staatsanwaltschaft

eDiscovery & Litigation Support

Quellen: E-Mails, Kalendereinträge, Dokumente, Cloud-Sync-Daten

Chain of Custody + Report direkt aus VERAKEY - gerichtsfähig für beide Rechtssysteme.

Incident Response / IT-Forensik

Account Compromise via Mobilgerät

Quellen: MFA-Apps, Token, Browser-Sessions, Phishing-Mails, MDM-Logs

Beweist ob Gerät kompromittiert war - schliesst BYOD-Lücke vollständig.

MAGNET AUTOMATE™

Magnet AUTOMATE - Von Stunden zu Minuten

Das Problem:

39,6 % nennen zeitintensive Routineaufgaben als große Herausforderung

39 % fühlen sich ausgebrannt - Tendenz steigend

51 % nutzen bereits Automation-Tools, der Rest verliert Zeit

7,1 Ø Tools pro Fall - Integration ist manuell & fehleranfällig

Magnet DFIR Report 2025 & 2026

Jede Stunde, die ein Analyst mit manuellem Kopieren verbringt, ist eine Stunde, die er nicht mit Analysieren verbringt. AUTOMATE gibt diese Zeit zurück.

MAGNET AUTOMATE™ löst das:

- Vollautomatische Erfassung & Verarbeitung nach Trigger
- Vordefinierte Playbooks -Case-Type wählen, loslegen
- Parallele Verarbeitung mehrerer Endpoints gleichzeitig
- KI-gestützte Klassifikation ohne manuelle Sichtung
- Auto-Report-Generierung für verschiedene Zielgruppen
- Integration mit SIEM, SOAR, Ticketing (via API)
- Von Alarm zu erstem Bericht: Stunden → Minuten

Vor AUTOMATE vs. Danach

❌ Ohne AUTOMATE

- Manuelles Starten jeder Erfassung … pro Endpoint
- Warten auf Verarbeitung, dann manuell prüfen
- Verschiedene Outputs … mehrere Tools, kein Kontext
- Report manuell zusammenstellen … Stunden Arbeit
- Analyst als Engpass, kein Parallelisieren möglich
- Burnout durch repetitive, zeitintensive Prozesse

✅ MAGNET AUTOMATE™

- ✓ Alert triggert automatisch das passende Playbook
- ✓ Parallele Erfassung aller definierten Quellen
- ✓ Einheitlicher Output … ein Case, eine Wahrheit
- ✓ Report automatisch generiert … in Minuten
- ✓ Keine manuellen Fehler, keine Medienbrüche mehr
- ✓ Kapazität für 3x mehr Fälle gleichzeitig

Magnet DFIR 2026: Durchschnittlich 7,1 Tools pro Fall: AUTOMATE ist der Klebstoff, der daraus einen Workflow macht.

#4

MAGNET REVIEW®

Magnet REVIEW - Einer sichert, alle analysieren

Das Kollaborations-Problem:

- Security, HR und Legal brauchen dieselben Daten - aber sehen unterschiedliche Dinge
- Forensik-Analyst kann keine PPTX-Datei exportieren und auf Nachfragen warten
- Externe Anwälte oder Aufsichtsbehörden brauchen Zugang — sicher & auditiert
- Kommentare & Erkenntnisse landen in E-Mails oder Slack — unkontrolliert
- Jede Runde Review kostet Stunden, nicht Minuten

Magnet DFIR 2026: Real-Time Collaboration wuchs um +24 % YoY als Haupttreiber für SaaS-Adoption. REVIEW ist die Antwort darauf.

REVIEW® löst das:

- Sichere, rollenbasierte Zugriffssteuerung
- Analyst, Reviewer, Manager … jeder sieht was er braucht
- Kommentare & Tags direkt an Artefakten
- Aufgaben & Workflows direkt zuweisbar
- Web-basiert (SaaS / On-Prem), kein lokales Tool
- Automatische Audit-Logs aller Aktivitäten
- Externe Reviewer einladen, ohne Dateiexport

MAGNET REVIEW®

Wer sieht was - und warum das zählt

🔍 Digitaler Forensiker / IT- Analyst

Sieht: Volle Artefakt-Ansicht & Timeline

Tut: Taggt IOCs, annotiert Beweise, erstellt forensische Timeline

👤 HR Manager / Ermittlungsleiter

Sieht: Kommunikations-Artefakte & Verhaltens-Timeline

Tut: Bewertet Sachverhalt, leitet Disziplinar- oder Strafmassnahmen ein

⚖️ Staatsanwalt / Legal / Compliance

Sieht: Relevante Dokumente, Reports & Chain of Custody

Tut: Prüft Verwertbarkeit, genehmigt Findings, bereitet Anklageschrift vor

📊 CISO / Behördenleitung

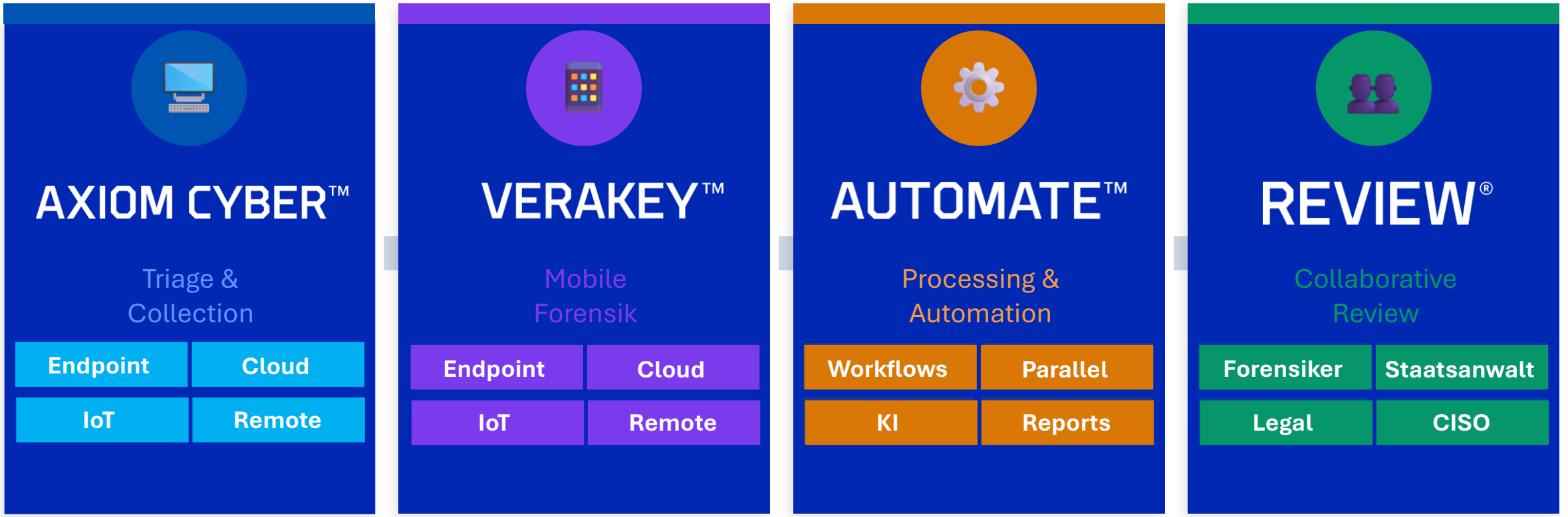
Sieht: Executive Summary & Lage-Dashboard

Tut: Entscheidet, genehmigt Meldepflichten, kommuniziert nach außen

Keine E-Mail-Anhänge. Kein Dateiexport. Keine unkontrollierten Kopien. Vollständige Audit-Trails, von Anfang bis Ende.

DER MAGNET-STACK

Alle vier Tools - ein vollständiger Untersuchungsworkflow



Das Ergebnis: Kürzere Ermittlungszeiten. Weniger Burnout. Bessere Entscheidungen. Für Security, HR, Legal und Management … gleichzeitig.

ZUSAMMENFASSUNG

Was Sie heute mitgenommen haben

MAGNET AXIOM CYBER™

Ermöglicht vollständige Remote-Erfassung & Multisource-Analys. Ein Case File für alles.

MAGNET VERAKEY™

Schließt die Mobile-Lücke: FFS-Extraktion, DSGVO-konform, gerichtsfähig.

MAGNET AUTOMATE™

Eliminiert Routinearbeit. Playbooks/Workflows starten automatisch, Kapazität verdreifacht sich.

MAGNET REVIEW®

Verbindet Forensiker, Staatsanwalt, HR und CISO sicher, auditiert, ohne Dateiexport. Für Corporate und Strafverfolgung.

Fragen & Diskussion

Quellen dieser Präsentation:

Magnet Forensics: 2025 & 2026 State of Enterprise DFIR Report
BSI: Lagebericht IT-Sicherheit Deutschland 2025
Bitkom: Wirtschaftsschutz 2025 Verizon: Data Breach Investigations Report 2025
IBM: Cost of a Data Breach 2025
WEF: Global Cybersecurity Outlook 2026

Read the report

State of Enterprise DFIR **2026 Report**

And lets connect:

After this presentation at our booth,

via Email:
Niels.Renken@magnetforensics.com,

Via LinkedIn:
https://www.linkedin.com/in/nielsrenken