MH SERVICE
WORLD OF FORENSICS

RAPID THREAT HUNTER

Plattform zur schnellen und kollaborativen Aufklärung von Cyber Threat Events

- Schnelle und präzise Verfolgung von lateraler Bewegung in angegriffenen Systemen mit ersten validen Ergebnissen bereits innerhalb einer Stunde!
- Volle Analyse (Triagierung) eines Artefaktes in 2 Stunden
- Belegbare Identifikation von lateralen Bewegungen mit Zeitstempel, Beschreibung und Bewertung. Je nach Fall bereits umgehend nach Analyse des zweiten Artefakts.

ZUGESCHNITTEN AUF IHRE INDIVIDUELLEN BEDÜRFNISSE, READY TO WORK!

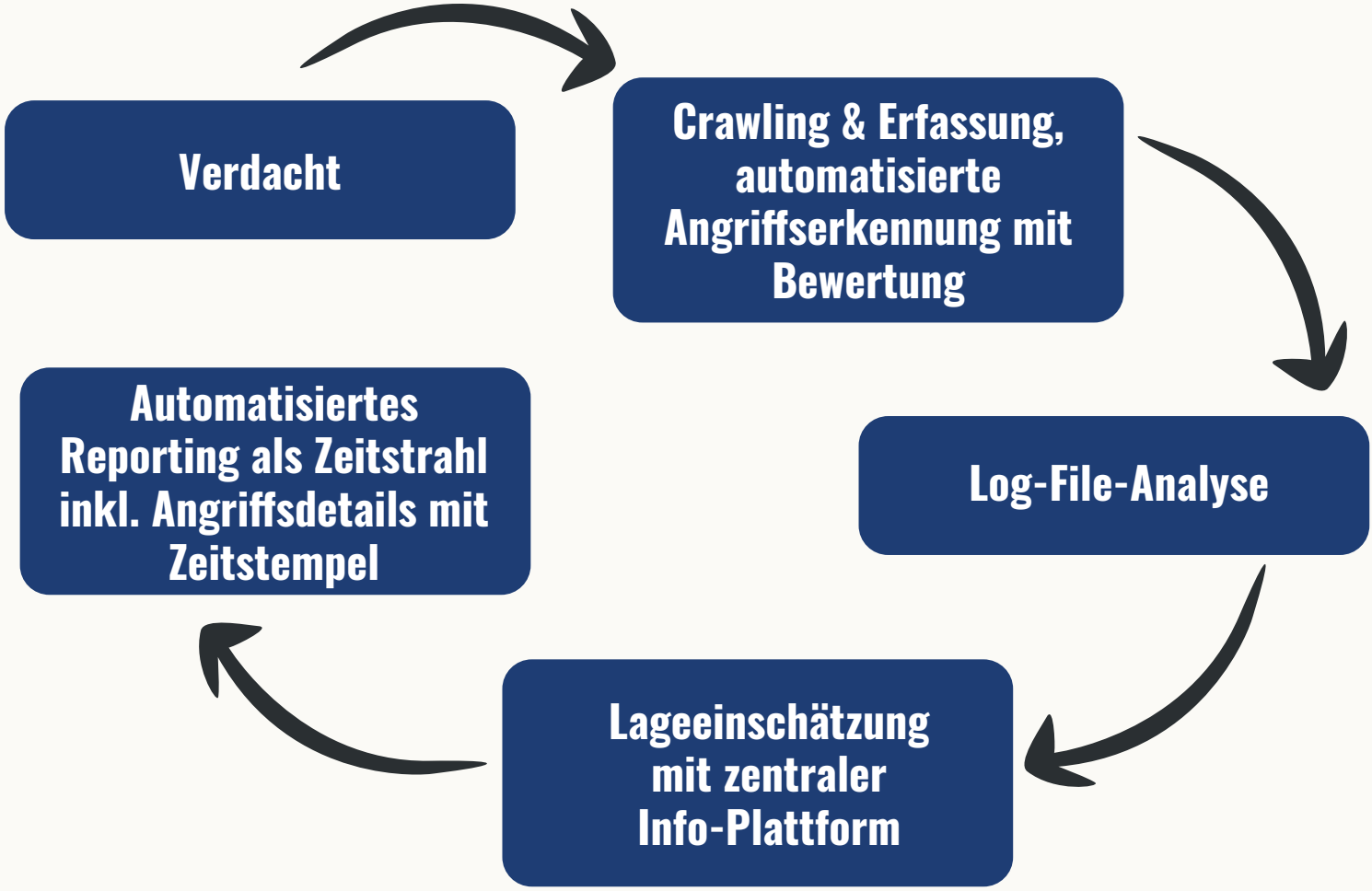
• **Ready to work**	Kein Zeitverlust durch langwierige Einrichtung von Tools und Infrastruktur, denn jede Sekunde zählt
• **Kompletter Workflow**	Schnelle Erfassung, Analyse mit Bewertungen, Maßnahmenergreifung
• **One-Click Forensik**	Prozess direkt im System anstoßen – einfache forensische Datenakquise auch für nicht-technisches Personal
• **Malware-forensische Sicherheit**	Durchdachte Sicherheitseinrichtung mit gehärteter Plattform ermöglicht sicheres Arbeiten beim Umgang mit infizierten Systemen
• **Skalierbarkeit**	Individuell anpassbar je nach Umfang und Anzahl der Mitarbeiter, sowie notwendigen Sicherheitsstandards

5-10 User - CPU: 48C/96T RAM: 384GB MVME-Storage: 32TB 25Gbit Ethernet
10-25 User - CPU: 96C/192T RAM: 768GB MVME-Storage: 64TB 25Gbit Ethernet
25+ User - CPU: 192C/384T RAM: 1,5TB MVME-Storage: 128TB 25Gbit Ethernet

ZUGESCHNITTEN AUF IHRE INDIVIDUELLEN BEDÜRFNISSE, READY TO WORK!

• **On Prem**	Analyse findet On Premise statt, außerhalb von Clouds und anderen kommerziellen Datenprodukten
• **Proprietäres Kommunikationssystem**	Sicherer Austausch von Daten und IOCs ohne Nachverfolgbarkeit von außen
• **Ortsungebunden**	Bearbeitung von Cyber Threat Events direkt im Feld oder von beliebigen weltweiten Standorten sowie im Homeoffice
• **Kollaborations- und Mandantenfähigkeit**	Kollaborative Triagierung von Cyber Threat Events im Law Enforcement als auch im Incident Handling Bereich
• **Vermeidung von Gefahrenüberhängen**	Möglichkeit der umgehenden Erkennung von Gefahrenüberhängen aus der Triage-Analyse
• **Begleitendes Onboarding**	Optimale Nutzung der Plattform für schnelle und präzise Ergebnisse

WORKFLOW ZUM FESTSTELLEN KONSISTENTER ANGRIFFSVERHALTEN



Sicherheitskonzept
Alles On Premise – Eigene Datenbanken – Keine Cloudservices – Sicher vor Fremdzugriff

Kernbestandteile
Erfassung - Analyse - Kollaboration - Output – Datentransfer

Ready to work XXL für Behörden:
>> Rollout-Fähigkeit dank SiKo, VVT, Schwellwertanalyse

Weitere Infos zum Rapid Threat Hunter hier!