PROTECT

DARKNET MONITORING SERVICE

The Darknet Monitoring Service offers customers external, keyword-based monitoring of relevant sources on the clearnet, deep web and darknet. The aim is to detect leaks or signs of planned attacks at an early stage before operational damage occurs.
Results are provided in the form of alerts and monthly status reports.
The product is technically purely passive (no connection to customer systems) and fully GDPR-compliant.

KEY FEATURES

- Monitoring of up to 100 freely definable search terms (e.g. domains, user names, project names, IPs, brand terms)
- Continuous analysis of relevant platforms on the Clearnet, Deep Web & Darknet
- Alert when new hits are found (source, time, context, risk assessment)
- Categorisation according to criticality (info / suspected / confirmed)
- Alarm dispatch via encrypted email (PGP or S/MIME) or customer portal
- Monthly overview report with findings status and recommendations
- GDPR-compliant implementation without access to customer systems
- No system integration required

DELINEATION

CONTAINED

- Passive monitoring of defined sources
- Alerting when external data is found
- 100 terms included
- Technically independent service
- Pure detection performance

NOT RECEIVED

- Active attack detection in the network (MDR)
- Incident response or forensics after a discovery
- Expansion to over 100 terms (individual agreement)
- No automated integration into customer systems
- No action derivation without additional service

MH SERVICE
WORLD OF FORENSICS