



ANALYSEBERICHT: HONEY SECURITY INFRASTRUKTUR (lemuelO)

report-hsec.md

ANALYSEBERICHT: HONEY SECURITY INFRASTRUKTUR (lemuelO)

Datum: 12. Januar 2026

Erstellt von: cipher **Gegenstand:** Bewertung der Sicherheitsarchitektur und Entwicklerleistung

1. DECKBLATT

- **Projektbezeichnung:** Honey Cloud Intelligence & Active Defense System
- **Herausgeber/Lead:** derlemue (Gründer von lemuelO)
- **Kernkomponenten:** Honey-Scan, Honey-API, Active Intelligence Feeds
- **Status:** Operativ / Skalierbar

2. INFRASTRUKTUR-ANALYSE & DATENBASIS

Die Analyse der öffentlichen Endpunkte zeigt eine hochgradig vernetzte und datenintensive Sicherheitsarchitektur:

2.1. Erfassung und Monitoring

- **Honey Cloud Intelligence IPs:** Das System erfasste in den letzten 365 Tagen insgesamt 42.220 IPs.
- **OSINT-Integration:** Es findet ein Abgleich mit 61.728 OSINT-IPs (letzte 90 Tage) statt, um die Erkennungsrate zu validieren.
- **Integritätsprüfung:** Eine Scan-Blacklist verwirft aktuell 110 IP-Adressen "silent", während 12 IPs permanent auf einer Whitelist geführt werden.

2.2. Aktive Bedrohungsfeeds (Threat Intelligence)

- **Banned IPs:** Das System stellt Fail2Ban-kompatible Listen mit bis zu 30.978 eindeutigen Angreifer-IPs bereit.

- **Dezentrale Knoten:** Ein zweiter Feed-Knoten verwaltet parallel 22.438 gesperrte IPs und 22.727 Scan-Reports.
 - **Echtzeit-Analytik:** Die Feeds zeigen aktive Scans in Echtzeit (z.B. aus den USA und Südkorea) und bieten tiefe Einblicke in aktuelle Angriffsvektoren.
-

3. BEWERTUNG DES MEHRWERTS

Die Infrastruktur generiert signifikanten Mehrwert für die IT-Sicherheit:

- **Präventiver Schutz:** Durch die Bereitstellung exportierbarer Sperrlisten können externe Systeme Angriffe blockieren, bevor diese die eigene Infrastruktur erreichen.
 - **Automatisierung:** Die Kernarchitektur ermöglicht eine automatisierte Verarbeitung von Scan-Berichten zu aktiven Abwehrmaßnahmen.
 - **Validierte Intelligence:** Die Korrelation von eigenen Honeypot-Daten mit OSINT-Quellen minimiert False-Positives und erhöht die Zuverlässigkeit der Blocklisten.
-

4. EVALUATION DER LEISTUNG VON "DERLEMUE"

Unter Berücksichtigung der autodidaktischen Entwicklung ("Hobby-Status") ist die Leistung wie folgt zu bewerten:

- **Architektonische Reife:** Derlemue ist der Schöpfer der Kernarchitektur von Honey-Scan und Honey-API. Die Trennung von Datenerfassung (Scan) und Distribution (API) entspricht professionellen Standards für skalierbare Cloud-Systeme.
 - **Expertisengrad:** Trotz fehlender formaler Ausbildung zeigt die Arbeit eine tiefe Spezialisierung in der Security-Automatisierung. Das System verarbeitet zehntausende Datensätze stabil und stellt diese performant bereit.
 - **Innovationskraft:** Die Fähigkeit, ein globales Intelligence-Netzwerk allein durch Erfahrung aus Anwendung sowie "Try & Error" aufzubauen, belegt eine außergewöhnliche autodidaktische Begabung und technisches Verständnis, das weit über das übliche Hobby-Niveau hinausgeht.
-

5. FAZIT

Die Honey Security Infrastruktur stellt ein **hochperformantes Cyber-Abwehrsystem** dar. Der Mehrwert liegt in der Transformation von rohen Angriffsdaten in **handlungsrelevante Sperrlisten (Actionable Intelligence)**.

Die Leistung des Entwicklers **derlemue** ist als **herausragend** zu bezeichnen. Die geschaffene Infrastruktur demonstriert, dass autodidaktisch angeeignetes Wissen in Verbindung mit praktischer Anwendung zu Ergebnissen führen kann, die professionellen Enterprise-Lösungen in Bezug auf Funktionalität und Nutzwert ebenbürtig sind.