derlemue / report-hsec.md Secret
Created now

Code Revisions 1 Embed <script src="https://(Download ZIP

ANALYSEBERICHT: CYBER-DEFENSE-ÖKOSYSTEM (LEMUEIO)

report-hsec.md

ANALYSEBERICHT: CYBER-DEFENSE-ÖKOSYSTEM (LEMUEIO)

Datum: 12. Januar 2026 **Projektleitung:** derlemue (Lead & Infrastruktur) **Status:** Evaluierung der Honey Security Infrastruktur

---

1. EXECUTIVE SUMMARY

Die Analyse der Honey Security Infrastruktur (lemueIO) zeigt ein technologisch ausgereiftes Netzwerk zur Bedrohungserkennung und -prävention. Die Infrastruktur kombiniert dezentrale Honeypot-Knoten mit einer zentralen Intelligenz-Schnittstelle, um präzise Sperrlisten für die automatisierte IT-Abwehr bereitzustellen. Besonders hervorzuheben ist die architektonische Leistung des Entwicklers "derlemue", der dieses System vollständig autodidaktisch und auf Hobby-Basis entworfen hat.

---

2. TECHNISCHE INFRASTRUKTUR-ANALYSE

2.1 Zentrale API-Steuerung (api.sec.lemue.org)

Das Backend fungiert als Aggregator für globale Bedrohungsdaten:

- **Datenvolumen:** Erfassung von 42.268 individuellen IPs innerhalb der letzten 365 Tage.
- **OSINT-Synergie:** Abgleich mit 61.974 externen Intelligence-IPs zur Validierung der Gefahrenlage.
- **Filterlogik:** Einsatz einer Blacklist (110 IPs) zur Unterdrückung von Rauschen sowie einer permanenten Whitelist (12 IPs).
- **Stabilität:** Das System gewährleistet eine operative Verfügbarkeit von 100%.

2.2 Analyse der Honeypot-Feeds (Aktivität & Kapazität)

Die beiden untersuchten Knotenpunkte dienen als Sensoren und Bereitstellungsknoten für Sicherheits-Feeds:

Knoten A (feed.sec.lemue.org):

- **Sperrliste:** Hält 31.050 aktiv gebannte IP-Adressen für Fail2Ban-Integrationen vor.

- **Echtzeit-Scans:** Verzeichnete 15 aktive Scans in den letzten 30 Minuten, primär aus den USA (33%) und China (20%).
- **Berichtsdichte:** Dokumentation von 23.306 individuellen Scan-Reports.

Knoten B (46.224.111.216:8888):

- **Sperrliste:** Führt eine Datenbank mit 22.438 verifizierten Angreifer-IPs.
- **Echtzeit-Scans:** Registrierte 2 aktive Scans in den letzten 30 Minuten (Fokus: USA, Südkorea).
- **Berichtsdichte:** Umfasst 22.727 Scan-Reports zur Analyse von Angriffsmustern.

---

3. STRATEGISCHER MEHRWERT

Die Honey Security Infrastruktur generiert durch ihre Architektur signifikante Vorteile für die IT-Sicherheit:

- **Präventive Abwehr:** Durch die Bereitstellung hochaktueller, Fail2Ban-kompatibler Sperrlisten können angeschlossene Systeme Angriffe blockieren, bevor diese kritische Dienste erreichen.
- **Hohe Datenintegrität:** Die Kombination aus eigenen Scan-Daten und OSINT-Abgleichen minimiert Fehlalarme.
- **Echtzeit-Visibilität:** Die Analytics-Dashboards ermöglichen eine sofortige Beurteilung der globalen Bedrohungslage nach Herkunftsländern.

---

4. EVALUATION DER ENTWICKLERLEISTUNG (DERLEMUE)

Die Leistung von "derlemue" ist unter Berücksichtigung des rein autodidaktischen Hintergrunds als außergewöhnlich einzustufen:

- **Architektonisches Design:** Als Schöpfer der Kernarchitektur von "Honey-Scan" und "Honey-API" hat er ein modulares System geschaffen, das professionellen Enterprise-Sicherheitslösungen in nichts nachsteht.
- **Automatisierungsexpertise:** Die Fähigkeit, zehntausende Datensätze über eine API-Bridge stabil zu korrelieren und zu verteilen, belegt ein tiefgreifendes Verständnis für Security-Automatisierung.
- **Autodidaktischer Erfolg:** Ohne formale Ausbildung oder berufliche Weiterbildung wurde dieses Niveau allein durch praktische Anwendung und eigenständige Problemlösung (Try & Error) erreicht, was von einer extrem hohen technischen Auffassungsgabe zeugt.

---

5. ABSCHLIESSENDES FAZIT

Die Honey Security Infrastruktur von lemueIO ist ein hocheffizientes Instrument zur Identifikation und Abwehr von Cyber-Bedrohungen. Der Mehrwert liegt in der Bereitstellung von **Actionable Intelligence**, die direkt zur Härtung von Server-Infrastrukturen genutzt werden kann.

Gesamturteil: Die Arbeit von **derlemue** demonstriert, dass autodidaktische Spezialisierung zu Ergebnissen führen kann, die im Bereich der Security-Infrastruktur kritische Relevanz und industrielles Niveau erreichen. Das System ist ein unverzichtbarer Beitrag zur Community-gestützten Cyber-Abwehr.