BORNSEC
BORN TO SECURE

Attacklens
ATTACK SURFACE MANAGEMENT PLATFORM

AttackLens
Dark Web Monitoring

AttackLens Dark Web Monitoring is a capability that continuously scans deep web + dark web ecosystems to detect:

- Leaked credentials (emails, passwords)
- Exposed company data (files, APIs, secrets)
- Brand mentions in hacker forums
- Sale of access to your infrastructure
- Discussions targeting your organization

How does it work?

Data Collection

Crawl sources like:

- Dark web forums (TOR)
- Telegram / Discord groups
- Paste sites (e.g., dumps)
- Breach databases

Correlation

Match findings with:

- Domains
- Employee emails
- IPs / assets
- Brand keywords

Validation

- Remove noise (duplicate/old leaks)
- Verify authenticity of data

Risk Prioritization

- Critical → Active credentials/access
- High → New breach data
- Medium → Mentions/chatter

Alerting & Action

- Real-time alerts
- Suggested remediation:
  - Reset credentials
  - Block access
  - Takedown requests

Info@attacklens.ai | +918040273737

Features

Credential Exposure Monitoring

Detect leaked:

- Employee credentials
- Admin accounts
- API keys

Brand & Reputation Protection

Detect:

- Fake domains
- Phishing kits
- Brand impersonation

DarkWeb Intelligence Correlation

Link dark web findings with:

- Your attack surface
- Known vulnerabilities
- Misconfigured assets

Breach & Data Leak Detection

Monitor:

- Data dumps
- Customer data leaks
- Internal documents

Executive / VIP Monitoring

Track exposure of:

- CXO emails
- Personal accounts
- Social engineering risks

AI-Based Signal Filtering

- Reduce noise (huge problem in dark web tools)
- Provide:
  - Confidence score
  - Context
  - Exploitability

AttackLens goes beyond traditional dark web monitoring by correlating leaked data, attacker chatter, and credential exposure directly with your real attack surface, turning raw intelligence into actionable risk.

Use Case

A developer's credentials appear in a Telegram dump

AttackLens does:

- Maps email → GitHub + cloud access
- Detects exposed API keys
- Flags exploitable assets
- Triggers priority alert