



## **DARK WEB MONITORING**

Proactive Detection of Exposed Credentials and Data

### ● **IDENTIFYING DATA EXPOSURE BEFORE IT BECOMES AN INCIDENT**

Stolen credentials and leaked data are frequently traded on the dark web. These exposures often occur long before organisations become aware that their accounts or information have been compromised.

Dark Web Monitoring continuously scans the surface web, deep web and dark web for data linked to your organisation. When compromised credentials or sensitive information are discovered, alerts are generated so that action can be taken quickly.

Early detection helps organisations reduce the risk of account compromise, phishing attacks and ransomware incidents.

### ● **WHAT DARK WEB MONITORING DELIVERS**

- Continuous monitoring of domains and credentials across dark web sources
- Detection of exposed usernames, passwords and leaked data
- Automated alerts when new exposures are discovered
- Clear reporting on compromised accounts and risk exposure
- Improved visibility into external cyber threats



## HOW DARK WEB MONITORING REDUCES CYBER RISK

| Challenge                 | Dark Web Monitoring Benefit                             |
|---------------------------|---------------------------------------------------------|
| Hidden credential leaks   | Identifies compromised email accounts and passwords     |
| Limited threat visibility | Monitors dark web marketplaces and breach databases     |
| Compliance pressure       | Provides audit-ready reporting on exposure detection    |
| Ransomware risk           | Early detection reduces the likelihood of account abuse |

## HOW THE SERVICE WORKS

-  **Domain and Credential Monitoring**  
Domains and associated email accounts are monitored across breach databases and dark web sources.
-  **Continuous Scanning**  
Automated scans identify newly exposed credentials, leaked data and other indicators of compromise.
-  **Immediate Alerts**  
Alerts are generated when exposures are detected so remediation can begin quickly.
-  **Reporting and Analysis**  
Reports provide visibility into affected accounts and exposure history.
-  **Response Guidance**  
Recommendations help organisations address compromised credentials and strengthen security controls.

## OUTCOMES OF DARK WEB MONITORING

- Early detection of compromised credentials
- Improved visibility into external cyber threats
- Faster response to potential breaches
- Stronger security posture and compliance readiness
- Reduced risk of account compromise and ransomware entry

Email [support@duxnet.co.za](mailto:support@duxnet.co.za) to book Dark Web Monitoring

**Duxbury Networking** | [www.duxbury.co.za](http://www.duxbury.co.za) | [info@duxnet.co.za](mailto:info@duxnet.co.za)

**Johannesburg** (011) 351 9800 | **Cape Town** (021) 423 7115 | **Durban** (087) 943 9076