

### Dark Web Monitoring - Schedule CS-3

Effective Date: October 14, 2025 | Supersedes prior versions.

#### Service Summary

Service Provider shall provide Dark Web Monitoring services to identify potential exposures of Client credentials, domains, or other monitored data on publicly available breach repositories and dark web sources. This service is designed to provide early warning of possible credential compromise but does not prevent breaches, control third-party data leaks, or guarantee detection of all compromised data.

#### Scope of Services

- Continuous monitoring of Client's primary domain(s) and designated email addresses for evidence of credential exposure.
- Scanning of known breach databases, underground forums, and other available dark web sources.
- Alerts and notifications when new exposures involving monitored identifiers are detected.
- Reporting of monitoring results within Service Provider's ticketing platform.
- Advisory on recommended remediation steps (e.g., forced password resets, MFA enforcement) when exposures are identified.

#### Exclusions

- Prevention of breaches, leaks, or compromise events.
- Real-time monitoring of all dark web sources; Service is limited to repositories and feeds accessible by the monitoring platform.
- Monitoring of non-approved or personal email domains unless expressly authorized.
- Liability for third-party data breaches, leaks, or compromises outside Service Provider's control.
- Forensic investigation, root cause analysis, or incident response (available separately).

#### Client Responsibilities

- Provide Service Provider with approved domain(s) and email addresses to monitor.
- Promptly act on recommendations following exposure alerts (e.g., password changes, MFA activation).
- Educate end-users on password hygiene and credential security.
- Understand that monitoring is informational and requires Client action to mitigate risks.

#### General Terms

- Dark Web Monitoring is a detection and notification service only; it does not prevent credential compromise.
- Client acknowledges that this Service is one element of a layered security strategy. While monitoring reduces risk by providing visibility into exposed credentials, no single control or combination of controls can guarantee complete protection or eliminate all vulnerabilities. Even the most advanced systems remain subject to bypass or compromise. Service Provider strongly recommends implementing complementary safeguards – such as endpoint detection and response (e.g., Adlumin XDR), multi-factor authentication, conditional access policies in Microsoft 365/Intune/Entra ID, email filtering, DNS filtering, and security awareness training – to achieve stronger overall resilience.
- All response times for dark web-related service requests are governed by the Service Level Objectives in Schedule A of the Master Service Agreement.
- Fees for this Schedule are billed in accordance with the Payment Terms of the Master Service Agreement. Required platform licensing is included in Service Provider's standard service fees unless otherwise specified. Additional costs (e.g., optional hardware, custom configurations, or third-party integrations outside standard service) may apply and will be billed separately.