



1 Business Opportunities – shibboleth.mintel.com

Key evidence: 5 high-risk issues; 6 medium-risk issues; 257 shared domains; 10 unusual port assignments; 23 endpoints with deprecated TLS; 92 unencrypted URLs

1.1 Top Opportunities

1. Infrastructure Security Assessment

- Problem: Shared hosting environment with 257 domains increases attack surface.
- Impact: High risk of unauthorized access and data breaches.
- Service: Infrastructure Security Assessment.
- Scope: Segregate critical services, implement access controls.
- Evidence: 257 shared domains on `insights.mintel.com`.
- ROI: Reduced risk of data breaches and improved security posture.

2. Web Application Penetration Testing

- Problem: 92 URLs using unencrypted HTTP expose data to interception.
- Impact: Potential data breaches and loss of confidentiality.
- Service: Web Application Penetration Testing.
- Scope: Implement HTTPS, enforce redirection and HSTS policies.
- Evidence: URLs such as `http://13.134.195.126:80`.
- ROI: Enhanced data integrity and user trust.

3. Cloud Security Review

- Problem: Unusual port assignments indicate potential security evasion.
- Impact: Increased vulnerability to unauthorized access.
- Service: Cloud Security Review.
- Scope: Standardize port assignments, implement network segmentation.
- Evidence: OpenVPN on port 443, 10 high-risk ports.
- ROI: Improved network security and reduced risk of misconfiguration.

4. API Penetration Testing

- Problem: Medium-risk API surface vulnerabilities.
- Impact: Potential unauthorized access and data leaks.
- Service: API Penetration Testing.
- Scope: Secure API endpoints, enforce authentication and access controls.
- Evidence: API surface analysis identified as medium risk.
- ROI: Strengthened API security and reduced risk of data exposure.

5. SSL/TLS Upgrade Implementation

- Problem: 23 endpoints using deprecated TLS protocols.
- Impact: Vulnerability to cryptographic attacks.
- Service: Advanced Security Solutions.
- Scope: Upgrade to TLS 1.2 or higher, prefer TLS 1.3.
- Evidence: Endpoints using TLS 1.0 and 1.1.
- ROI: Enhanced encryption standards and compliance with security best practices.

1.2 Proposed Offer

- Scope: Comprehensive assessment and remediation of identified vulnerabilities.
- Deliverables: Detailed security reports, remediation plans, and implementation support.
- Timeline (weeks): 8-12 weeks for full implementation and verification.



1.3 30/60/90 & KPIs

- 30d: Initiate infrastructure and web application assessments.
- 60d: Complete cloud security review and API testing.
- 90d: Implement SSL/TLS upgrades and verify remediation.
- KPIs: Reduction in high-risk vulnerabilities; improved security posture score; compliance with security standards.

1.4 Objections & Responses

- **Objection:** Cost of implementation is high. **Response:** The investment reduces long-term risks and potential breach costs.
- **Objection:** Disruption to operations during implementation. **Response:** We ensure minimal disruption with phased implementation and testing.
- **Objection:** Current security measures are deemed sufficient. **Response:** The assessment reveals critical gaps that need addressing to prevent breaches.
- **Objection:** Lack of internal resources to manage changes. **Response:** We provide full support and training to your team for seamless integration.

1.5 Immediate Next Steps

- Client: Review and approve proposed security services.
- Consultancy: Prepare detailed project plan and resource allocation.
- Joint: Schedule kickoff meeting to align on objectives and timelines.