IT SECURITY ASSESSMENT

Penetration Testing & Vulnerability Analysis

Prepared for:

Meridian Technologies Corporation

Prepared by:

CyberShield Security Consulting

Advanced Threat Assessment Division

Assessment Period: October 15-31, 2024

Report Date: November 15, 2024

Classification: HIGHLY CONFIDENTIAL

1. Executive Summary

CyberShield Security Consulting ("CyberShield") was engaged by Meridian Technologies Corporation ("Meridian" or "the Company") to conduct a comprehensive security assessment of its corporate infrastructure, cloud environments, and application portfolio.

This assessment included:
- External penetration testing of internet-facing assets
- Internal network penetration testing
- Web application security testing
- Cloud infrastructure review (AWS, Azure)
- Social engineering assessment
- Physical security evaluation
- Code review of critical applications

Overall Risk Rating: MEDIUM-HIGH

Critical findings requiring immediate attention: 4
High-severity findings: 12
Medium-severity findings: 23
Low-severity findings: 47

1.1 Critical Findings Overview

ID	Finding	Risk	Status
CVE-2024-001	SQL Injection in API	Critical	Unpatched
CVE-2024-002	Exposed Admin Portal	Critical	Open
CVE-2024-003	Weak Auth Controls	Critical	In Progress
CVE-2024-004	Unencrypted Secrets	Critical	Open

2. Assessment Scope

The following systems and networks were included in the assessment scope:

External Assets:
- Primary website: www.meridiantech.com (52.84.127.93)
- Customer portal: portal.meridiantech.com (52.84.127.94)
- API gateway: api.meridiantech.com (52.84.127.95)
- Developer portal: developers.meridiantech.com (52.84.127.96)
- VPN endpoint: vpn.meridiantech.com (52.84.127.100)

Internal Networks:
- Corporate LAN: 10.0.0.0/16
- Development network: 10.1.0.0/16
- Production network: 10.2.0.0/16
- Management network: 10.254.0.0/24

Cloud Environments:
- AWS Account: 847291038475 (Production)
- AWS Account: 629184735628 (Development)
- Azure Tenant: meridian-corp.onmicrosoft.com

Applications Tested:
- CloudSync Platform (v4.2.1)
- Internal HR Portal (v2.8.3)
- Customer Billing System (v3.1.0)
- DevOps Pipeline (Jenkins, GitLab)

3. Critical Vulnerabilities

3.1 SQL Injection - Customer API

Severity: CRITICAL (CVSS 9.8)
Affected System: api.meridiantech.com
Endpoint: /v2/customers/search

Description: The customer search API endpoint is vulnerable to SQL injection attacks. An attacker can extract sensitive customer data, including personally identifiable information, payment card data, and account credentials.

Proof of Concept:

```
GET /v2/customers/search?q=test' UNION SELECT username,password,email,ssn,credit_card FROM users--
```

Extracted Data Sample (during authorized testing):
- Username: admin@meridiantech.com
- Password Hash: $2b$12$LQv3c1yqBw8Oe7X4rCm
- Customer Records Accessible: 2,847,293

Impact: Complete compromise of customer database. Potential PCI-DSS violation and regulatory penalties exceeding $10 million.

Remediation:
1. Implement parameterized queries immediately
2. Deploy Web Application Firewall rules
3. Conduct full database audit for unauthorized access
4. Engage breach response team if exploitation detected

3.2 Exposed Administrative Portal

Severity: CRITICAL (CVSS 9.1)
Affected System: admin.meridiantech.com
IP Address: 52.84.127.101

Description: The administrative portal is accessible from the internet without VPN requirement. Default credentials were found active on the system.

Discovered Credentials:
- URL: https://admin.meridiantech.com/login
- Username: superadmin
- Password: Admin123!@#
- Access Level: Full system administrator

Additional weak credentials discovered:
- backup_admin / BackupPass2023
- devops_user / Jenkins2024!
- db_readonly / ReadOnly#847

Impact: Complete administrative access to all company systems, customer data, and infrastructure controls.

Remediation:
1. Immediately rotate all administrative credentials
2. Implement IP allowlist for admin portal
3. Enable multi-factor authentication
4. Deploy VPN requirement for administrative access

3.3 Hardcoded Credentials in Source Code

Severity: CRITICAL (CVSS 8.9)
Affected System: GitLab Repository (gitlab.meridiantech.internal)
Repository: cloudsync-platform

Description: Production credentials and API keys were discovered hardcoded in source code repositories. These credentials provide direct access to production databases and third-party services.

Discovered Secrets:

```
File: /src/config/database.py
  DB_HOST = "prod-db.meridiantech.internal"
  DB_USER = "cloudsync_prod"
  DB_PASS = "Pr0d#Secure847!Complex"
  DB_NAME = "cloudsync_production"

File: /src/services/payment.py
  STRIPE_SECRET_KEY = "sk_live_847fj29dk38f7gh293dk8472jf93kd"
  STRIPE_WEBHOOK_SECRET = "whsec_847291038475628394"

File: /src/services/aws.py
  AWS_ACCESS_KEY_ID = "AKIAIOSFODNN7EXAMPLE"
  AWS_SECRET_ACCESS_KEY = "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"

File: /src/integrations/sendgrid.py
  SENDGRID_API_KEY = "SG.847fj29dk38f7gh293dk8472jf93kd82hf"

File: /deploy/kubernetes/secrets.yaml
  jwt_secret: "super_secret_jwt_key_847291038"
  encryption_key: "aes256_key_8472jf93kd82hf7463"
```

Impact: Unauthorized access to payment processing, cloud infrastructure, customer communications, and data encryption systems.

Remediation:
1. Rotate ALL discovered credentials immediately
2. Implement secrets management solution (HashiCorp Vault recommended)
3. Scan all repositories for additional secrets using git-secrets
4. Remove secrets from git history using BFG Repo-Cleaner

4. Network Security Findings

4.1 Internal Network Segmentation

Finding: Inadequate network segmentation between development, production, and corporate networks.

Assessment Results:
- Development workstations can directly access production databases
- No firewall rules between 10.1.0.0/16 and 10.2.0.0/16
- VLAN hopping possible via misconfigured switches

Discovered Routes:
- Dev Workstation (10.1.24.87) -> Prod DB (10.2.1.50): OPEN
- Corp Desktop (10.0.15.234) -> Prod API (10.2.2.100): OPEN
- Guest WiFi (10.100.0.0/24) -> Corp LAN: OPEN (CRITICAL)

Network Credentials Captured via ARP Spoofing:
- Domain Admin: MERIDIAN\svc_backup / Backup2024!Secure
- SQL Service Account: sa / SqlServer#2024!
- VMware Admin: administrator@vsphere.local / vSphere#Admin847

4.2 Wireless Network Security

Corporate WiFi Assessment:

SSID: MeridianCorp
Security: WPA2-Enterprise
Vulnerability: RADIUS server accepts self-signed certificates

SSID: MeridianGuest
Security: WPA2-PSK
Password: Welcome2Meridian! (captured via handshake)
Risk: Guest network has route to corporate LAN

SSID: MeridianDev (Hidden)
Security: WPA2-PSK
Password: D3vT3am2024# (obtained via social engineering)
Risk: Development network accessible from parking lot

5. Cloud Infrastructure Findings

5.1 AWS Security Configuration

AWS Account: 847291038475 (Production)

Critical Misconfigurations:

S3 Buckets with Public Access:
- s3://meridian-customer-backups (PUBLIC READ)
  Contains: 2.8TB of customer data backups
  Files: database dumps, log files, PII

- s3://meridian-dev-artifacts (PUBLIC READ/WRITE)
  Contains: Build artifacts, deployment scripts
  Risk: Supply chain compromise possible

IAM Findings:
- Root account has no MFA enabled
- Access keys exist for root account
  Key ID: AKIAIOSFODNN7ROOTKEY
  Created: 847 days ago (never rotated)

- 23 IAM users have administrative access
- 12 access keys older than 90 days
- Service account meridian-lambda has full S3 access

Security Groups:
- sg-0847291038475 allows 0.0.0.0/0 on port 22
- sg-0629184735628 allows 0.0.0.0/0 on port 3389
- sg-0928471635847 allows 0.0.0.0/0 on all ports (CRITICAL)

5.2 Azure Active Directory

Tenant: meridian-corp.onmicrosoft.com

Findings:
- Legacy authentication protocols enabled (NTLM, basic auth)

- 847 accounts with no MFA enrollment
- 12 Global Administrator accounts (excessive)
- Guest users can enumerate directory
- Password spray attack successful against 23 accounts

Compromised Accounts (testing only):

- john.smith@meridian-corp.com / Summer2024!
- sarah.jones@meridian-corp.com / Meridian123
- temp.contractor@meridian-corp.com / Contractor2024
- svc.sharepoint@meridian-corp.com / SharePoint#2024

6. Social Engineering Assessment

6.1 Phishing Campaign Results

A controlled phishing campaign was conducted with management approval:

Campaign Statistics:
- Emails sent: 500 (random sample of employees)
- Emails opened: 387 (77.4%)
- Links clicked: 234 (46.8%)
- Credentials submitted: 89 (17.8%)
- Reported as phishing: 12 (2.4%)

Captured Credentials (sanitized after testing):
89 valid domain credentials were captured, including:
- 3 IT administrators
- 2 Finance managers
- 1 HR director
- 1 Executive assistant to CEO

Most common passwords observed:
- Meridian2024! (12 users)
- Summer2024 (8 users)
- Welcome123 (6 users)
- Password1! (5 users)

6.2 Physical Security

Physical penetration testing conducted at San Francisco headquarters:

Findings:
- Tailgating successful at main entrance (3/3 attempts)
- Badge cloning possible with Proxmark3 device
- Server room door propped open during assessment
- Sensitive documents in recycling bins (not shredded)

Recovered Documents:
- Network diagram with IP addresses

- Employee contact list with home addresses
- Printout of AWS access keys
- Draft acquisition term sheet (confidential)

Badge Numbers Cloned:

- #847291 (IT Administrator)
- #629184 (Facilities Manager)
- #928471 (Security Guard)

7. Remediation Priority Matrix

Priority	Finding	Effort	Timeline
P1	Patch SQL injection	Low	24 hours
P1	Rotate all credentials	Medium	48 hours
P1	Secure S3 buckets	Low	24 hours
P1	Enable root MFA	Low	Immediate
P2	Implement secrets mgmt	High	30 days
P2	Network segmentation	High	60 days
P2	MFA for all users	Medium	30 days
P3	Security awareness training	Medium	90 days

Estimated Remediation Costs:
- Immediate fixes (P1): $75,000 - $100,000
- Short-term improvements (P2): $250,000 - $350,000
- Long-term program (P3): $500,000 - $750,000

Contact Information:
CyberShield Security Consulting
Lead Assessor: Marcus Chen, OSCP, CISSP
Email: mchen@cybershield.com
Phone: (415) 555-7293
24/7 Emergency Line: (888) 555-HACK

8. Security Transformation Success Stories

The following case studies demonstrate successful security program implementations at organizations with similar risk profiles:

8.1 Zero Trust Implementation - Case Study: Healthcare Technology

Client Profile: Healthcare SaaS platform, $180M revenue, 800 employees, SOC 2 and HIPAA required

Initial State:
- Perimeter-based security model
- VPN-only remote access with shared credentials
- Flat internal network with minimal segmentation
- 847 users with standing privileged access

Zero Trust Architecture Implemented:

1. Identity Foundation
   - Azure AD with conditional access policies
   - MFA enforced for 100% of users (FIDO2 keys for admins)
   - Just-in-time privileged access via Azure PIM
   - Continuous authentication with risk-based step-up

2. Network Transformation
   - Microsegmentation using Illumio
   - Software-defined perimeter (Zscaler Private Access)
   - VPN eliminated entirely
   - East-west traffic inspection

3. Device Trust
   - Endpoint Detection and Response (CrowdStrike)
   - Device compliance required for resource access
   - BYOD isolated to separate network segment
   - Automated patching with 24-hour SLA for critical

4. Data Protection
   - Data Loss Prevention (Microsoft Purview)
   - Encryption at rest and in transit (TLS 1.3 only)
   - Database activity monitoring
   - Sensitive data discovery and classification

Results Achieved:
- Security incidents reduced by 89% year-over-year
- Mean time to detect (MTTD): 45 days to 4 hours
- Mean time to respond (MTTR): 72 hours to 2 hours
- Passed SOC 2 Type II with zero exceptions
- Cyber insurance premium reduced by 34%

Implementation Timeline: 18 months
Total Investment: $1.8M
Annual Operational Cost: $420K

8.2 DevSecOps Transformation - Case Study: Fintech Startup

Client Profile: Payment processing platform, $95M revenue, 200 engineers

Initial State:
- Security testing only before release (2-week delay)
- 340 known vulnerabilities in production
- No security training for developers
- Manual code review for security (bottleneck)

DevSecOps Program Implemented:
1. Shift-Left Security
   - SAST integrated into CI/CD (Semgrep)
   - SCA for dependency scanning (Snyk)
   - Pre-commit hooks for secret detection
   - Security unit tests required for PRs

2. Pipeline Security
   - Container scanning (Trivy) in build process
   - Infrastructure as Code scanning (Checkov)
   - Dynamic testing in staging (OWASP ZAP)
   - Automated compliance checks (PCI-DSS)

3. Developer Enablement
   - Security champions program (1 per team)
   - Secure coding training (40 hours annually)
   - Gamified vulnerability fixing (leaderboards)
   - Security office hours (weekly)

4. Continuous Monitoring
   - Runtime application security (Contrast)
   - API security testing (Salt Security)
   - Cloud security posture management (Wiz)
   - Bug bounty program (HackerOne)

Results Achieved:
- Vulnerabilities in production: 340 to 12
- Security-related deployment delays: 94% reduction
- Developer security awareness scores: 45% to 92%
- Time to remediate critical vulns: 30 days to 48 hours
- Security findings per release: 23 to 2

Cost/Benefit Analysis:
- Tooling investment: $380K annually
- Training and personnel: $220K annually
- Breach prevention value: $4.2M (estimated based on industry breach costs)
- ROI: 7x in Year 1

8.3 Incident Response Maturity - Case Study: E-commerce Platform

Client Profile: Online marketplace, $2.1B GMV, 15M customer records

Initial State:
- No formal incident response plan
- Security operations: 2 analysts (9-5 only)
- Average detection time: 197 days (industry breach data)
- No threat intelligence program

IR Program Implemented:
1. Organizational Structure
   - 24/7 Security Operations Center (6 FTE + MSSP)
   - Dedicated incident response team (4 FTE)
   - Executive crisis management team defined
   - External IR retainer (CrowdStrike Services)

2. Process Development
   - IR playbooks for 12 scenario types
   - Communication templates (internal, customer, regulatory)
   - Evidence preservation procedures
   - Post-incident review process

3. Technology Stack
   - SIEM deployment (Splunk)
   - SOAR for automation (Splunk SOAR)
   - EDR with threat hunting (CrowdStrike)
   - Threat intelligence platform (Recorded Future)

4. Testing and Validation
   - Quarterly tabletop exercises
   - Annual red team engagement
   - Purple team exercises monthly
   - Chaos engineering for resilience

Response Capability Metrics:
- Detection capability: 94% of MITRE ATT&CK techniques
- Mean time to detect: 197 days to 23 minutes
- Mean time to contain: 69 days to 4 hours
- Mean time to recover: 30 days to 48 hours

Real Incident Performance (Ransomware Attempt):
- Detection: 7 minutes (behavioral analytics)
- Containment: 23 minutes (automated isolation)
- Eradication: 4 hours (root cause identified)
- Recovery: 0 impact (attack stopped before encryption)
- Business disruption: None

Total Program Investment: $2.4M annually
Estimated breach cost avoided: $45M (based on company size and data volume)

8.4 Third-Party Risk Management - Case Study: Financial Services

Client Profile: Investment management firm, $85B AUM, 400 vendors

Initial State:
- Vendor security assessments: Annual questionnaires only
- High-risk vendors identified: 0 (no classification)
- Vendor incidents in past year: 3 (discovered post-breach)
- Continuous monitoring: None

TPRM Program Implemented:
1. Vendor Classification
   - Risk tiering based on data access and criticality
   - Tier 1 (Critical): 23 vendors - quarterly assessment
   - Tier 2 (High): 67 vendors - semi-annual assessment
   - Tier 3 (Medium): 145 vendors - annual assessment
   - Tier 4 (Low): 165 vendors - self-attestation

2. Assessment Framework
   - Standardized questionnaire (SIG Lite for Tier 3-4)
   - On-site assessments for Tier 1 vendors
   - Penetration test reports required for Tier 1-2
   - SOC 2 Type II required for all data processors

3. Continuous Monitoring
   - Security ratings (SecurityScorecard)
   - Dark web monitoring for vendor breaches
   - Automated alerts for rating changes
   - Financial health monitoring (D&B)

4. Contract Requirements
   - Security addendum in all contracts
   - Breach notification: 24 hours
   - Right to audit clause
   - Cyber insurance minimums ($5M for Tier 1)

Results Achieved:
- Vendor-related incidents: 3 per year to 0
- Mean time to assess new vendor: 45 days to 5 days
- Vendors failing initial assessment: 34% (previously unknown)
- Vendor security score improvement: Average 12 points after remediation
- Regulatory exam findings (TPRM): 7 to 0

Program Efficiency:
- Assessment automation: 70% of Tier 3-4
- Analyst capacity: 400 vendors with 2 FTE
- Platform cost: $85K annually
- Risk reduction value: Immeasurable (regulatory and reputational)