MODERN AI

AI CYBERSECURITY PROGRAM

KEY AREAS & CORE CONTROLS

Secure AI. Protect Data. Govern Agents. Build Trust. Deliver Value.

1. DATA PROTECTION

- DLP (Data Loss Prevention)
- Encryption (At rest & in transit)
- Data masking & tokenization
- Data classification
- Retention & disposal controls

2. PROMPT SECURITY

- Prompt injection testing
- Input validation & sanitization
- Prompt logging & auditing
- Sensitive data detection and blocking

3. OUTPUT SECURITY

- Response filtering
- Harmful content control
- Citation & source validation
- Hallucination detection & review

4. MODEL SECURITY

- Model inventory & catalog
- Model validation & testing
- Provenance & integrity
- Drift monitoring
- Model retirement process

5. AGENT SECURITY

- Tool allowlists & restrictions
- Action approvals & guardrails
- Least privilege access
- Sandboxing & isolation
- Human-in-the-loop oversight

6. MCP SECURITY

- Connector validation
- Tool trust scoring
- Context boundary controls
- API & function restrictions

7. IDENTITY SECURITY

- SSO (Single Sign-On)
- MFA (Multi-Factor Auth)
- RBAC (Role-Based Access)
- PAM (Privileged Access Mgmt)
- Workload & service account governance

8. API SECURITY

- Strong authentication
- Rate limiting & throttling
- Schema validation
- WAF / API protection
- Abuse & anomaly detection

9. CLOUD / INFRASTRUCTURE

- CNAPP (Cloud Native Application Protection)
- Container & image security
- Secrets management
- Vulnerability management

10. LOGGING & MONITORING

- AI activity logging
- Prompt & output logging
- Agent action logging
- SIEM integration & alerting
- Real-time anomaly detection

11. INCIDENT RESPONSE

- AI-specific incident playbooks
- Data leakage response
- Rogue agent containment
- Model compromise handling
- Forensics & post-incident review

12. THIRD-PARTY RISK

- Vendor risk assessments
- Data processing agreements
- Model terms & licensing
- Data residency reviews
- Ongoing vendor monitoring

PROGRAM ENABLERS (CROSS-CUTTING FOUNDATIONS)

GOVERNANCE & POLICY
Strong governance, clear policies, defined accountabilities

RISK MANAGEMENT
AI risk assessments, classification & continuous review

COMPLIANCE & REGULATION
Align with NIST AI RMF, ISO 42001, GDPR, OSFI, and industry rules

PEOPLE & CULTURE & TRAINING
Awareness, upskilling and responsible AI adoption

SECURE BY DESIGN & DEFAULT
Security built into AI systems, tools and workflows

CONTINUOUS IMPROVEMENT & ASSURANCE
Measure, test, monitor and improve AI security maturity

OUR COMMITMENT: SECURE INNOVATION. TRUSTED AI. RESILIENT FUTURE.

MODERN AI