Cross Pillar COE

Security Services COE

- Cloud Security
- Gen AI Security
- Application Security
- DevSecOps
- Governance Risk & Compliance

Cyber Security Services

Cloud Security

- Cloud Security Posture Management
- Cloud Native Application Protection Platform
- Cloud Governance Risk & Compliance

Gen AI Security

- Secure LLM Engineering
- Model & Prompt Injection Defense
- API & Access Security
- Monitoring & Abuse Prevention

Application Security

- SAST, DAST & SCA
- VAPT
- API Security Testing
- Runtime Application Self Protection

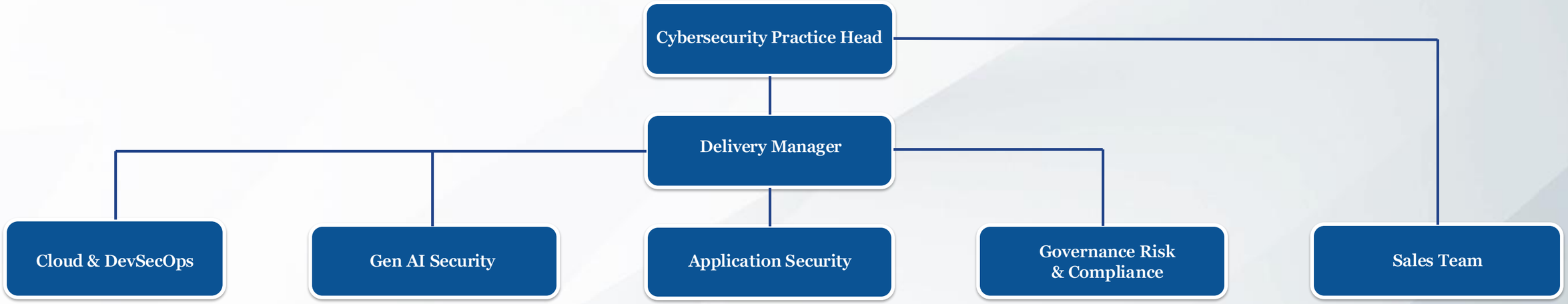
DevSecOps

- Infrastructure as Code Scanning
- Shift Left Security
- Security as Code
- Automated Security Gates

GRC

- Gap Assessment & Readiness Review
- Policy & Procedure Development
- Security Control Implementation
- Risk Assessments & Evidence Gathering
- Audit Support & Remediation

Security Team Structure



Role	Count	Summary
Cloud Engineers	4 (shared)	Available for security-related deployments and configurations
DevOps Engineers	4 (shared)	Support for CI/CD, infrastructure hardening, and secure pipeline setup
Security Test Engineers	2	Application Security (AppSec) testers, 2–4 weeks average engagement
Compliance Officers / Auditors	3	Support for regulatory and standards compliance per engagement
GenAI Test Engineers	3	Focused on validating GenAI functionality and safety
GenAI Security Team	4	1 Architect with strong security background, 2 Secure Devs, 1 DevOps (borrowed)
Sales Leader	1	One sales leader to help us guide our efforts with knowledge of existing projects within Accion

Security Services - 1

1. Security Risk Management, Governance & Compliance

- Risk Assessments
- Compliance Audits (GDPR, HIPAA, PCI-DSS, SOC 2, ISO 27001, NIST CSF, CCPA, EU AI Act, NIST AI RMF)
- Policy Development
- Third-Party Risk Management
- Governance Frameworks
- Regulatory Advisory
- Data Privacy Services
- AI Governance

2. Identity & Access Management (IAM)

- Privileged Access Management (PAM)
- Federated Identity
- Multi-Factor Authentication (MFA)
- Identity Governance & Administration (IGA)
- Customer Identity & Access Management (CIAM)
- Identity Lifecycle Management

Security Services - 2

3. Data Security & Privacy

- Data Loss Prevention (DLP)
- Encryption Services
- Data Masking/Tokenization
- Data Discovery & Classification
- Database Security
- AI Data Privacy

4. Network & Infrastructure Security

- Firewall Management
- Intrusion Detection/Prevention (IDS/IPS)
- VPN & Zero Trust Network Access (ZTNA)
- DDoS Mitigation
- Network Segmentation
- Email Security

Security Services - 3

5. Endpoint & Mobile Security

- Endpoint Detection & Response (EDR/XDR)
- Mobile Device Management (MDM)
- Antivirus/Anti-malware
- Hardware Security
- IoT/OT Security

6. Application Security

- Penetration Testing
- SAST/DAST/IAST
- API Security
- Container Security
- Threat Modelling

7. Cloud Security

- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection (CWPP)
- Cloud Data Security
- Cloud-Native Security
- Hybrid Cloud Security

Security Services - 4

8. Threat Management

- Threat Intelligence
- SIEM/SOAR
- Threat Hunting
- Vulnerability Management
- Malware Analysis

9. Incident Response, Forensics & Recovery

- Digital Forensics
- Incident Response Retainers
- Ransomware Mitigation
- Disaster Recovery Planning
- AI Incident Response

11. Managed Security Services (MSS)

- Managed Detection & Response (MDR)
- Vulnerability Scanning as-a-Service
- Managed Firewall/IDS
- Compliance Monitoring

Security Services - 5

12. Secure Software Engineering

- Secure SDLC Integration
- Code Review Services
- DevSecOps Automation
- SBOM Management

13. Secure Development Using Generative AI

- AI-Assisted Secure Coding
- Prompt Security Engineering
- AI-Augmented Testing
- AI Threat Modelling
- Compliance Automation
- AI Framework Implementation

14. Secure Development of Generative AI Systems

- AI Model Security
- AI Supply Chain Security
- AI Data Privacy
- AI Incident Response
- AI Regulation Compliance