Slide 9: Security Teams - AI Security & Governance

Objective: Define security and governance skills needed to protect AI systems and ensure responsible AI implementation.

Layout Composition:
The slide is a flex-col with a header sized to its content, a main body that grows, and a footer sized to its content. The main body is a grid with two columns (1fr 1fr) and three rows (auto auto auto). Top row spans both columns for security overview, middle row has two threat categories, bottom row has governance and compliance.

Content Breakdown:

- Block 1:
- Block Type: Text
- Placement: Header section
- Component Schema: “Role Header”
- Content:
  Role_Title: “Security Teams”
  Role_Icon: “Lock”
  Subtitle: “AI Security, Governance & Risk Management”
  Persona_Badge: “Primary: AI Worker”
- Creative Brief: Title text-6xl with red accent color (security role). Icon inline with title. Persona badge as small chip/pill. White text.
- Block 2:
- Block Type: Text
- Placement: Top row, spanning both columns
- Component Schema: “AI Security Landscape Card”
- Content:
  Section_Title: “AI-Specific Security Landscape”
  Icon: “ShieldAlert”
  Overview: “AI systems introduce unique security challenges beyond traditional application security”
  Key_Concerns: [
  “Model theft and intellectual property protection”,
  “Adversarial attacks and input manipulation”,
  “Data poisoning and training data integrity”,
  “Model inversion and privacy leakage”,
  “Prompt injection and jailbreaking (LLMs)”,
  “Supply chain risks in ML dependencies”
  ]
- Creative Brief: Wide card with slate-800 background, red accent border. Header with icon, text-2xl. Overview text in italic, text-xl. Key concerns as two-column bullet list, text-lg. Professional security-focused styling.
- Block 3:
- Block Type: Text
- Placement: Middle-left column

- Component Schema: “Threat Protection Skills Card”
- Content:
  Section_Title: “Threat Protection & Detection”
  Icon: “Shield”
  Skill_Categories: {
  “Model Security”: [
  “Secure model storage and access control”,
  “Model watermarking and provenance tracking”,
  “Adversarial robustness testing”,
  “Input validation and sanitization”
  ],
  “Data Security”: [
  “Training data access controls”,
  “PII detection and anonymization”,
  “Differential privacy implementation”,
  “Secure multi-party computation”
  ]
  }
- Creative Brief: Card with slate-700 background, red accent header. Two skill categories stacked. Bold category names (text-xl), bullets in text-base. Clear separation between categories.

- Block 4:

- Block Type: Text
- Placement: Middle-right column
- Component Schema: “Monitoring & Response Card”
- Content:
  Section_Title: “Monitoring & Incident Response”
  Icon: “AlertTriangle”
  Skill_Categories: {
  “Security Monitoring”: [
  “Model behavior anomaly detection”,
  “API abuse and rate limiting”,
  “Data exfiltration detection”,
  “Model drift as security indicator”
  ],
  “Incident Response”: [
  “AI-specific incident playbooks”,
  “Model rollback and containment”,
  “Forensic analysis for ML systems”,
  “Breach notification for AI systems”
  ]
  }
- Creative Brief: Matching card style to Block 3. Red accent throughout. Same structure and typography.

- Block 5:

- Block Type: Text
- Placement: Bottom-left column

- Component Schema: “Governance Framework Card”
- Content:
  Section_Title: “AI Governance Framework”
  Icon: “FileText”
  Components: [
  “AI usage policies and standards”,
  “Model risk assessment frameworks”,
  “Ethical AI review boards”,
  “Third-party AI vendor risk assessment”,
  “AI inventory and asset management”,
  “Model documentation requirements”
  ]
- Creative Brief: Card with slate-700 background, red accent. Header with icon, text-xl. Components as bullet list, text-base. Professional, policy-focused presentation.

- Block 6:

- Block Type: Text
- Placement: Bottom-right column
- Component Schema: “Compliance Requirements Card”
- Content:
  Section_Title: “Compliance & Regulatory”
  Icon: “Scale”
  Requirements: {
  “Privacy Regulations”: [“GDPR data rights”, “CCPA transparency”, “Right to explanation”],
  “Industry Standards”: [“NIST AI Risk Management”, “ISO/IEC 23894”, “OWASP ML Top 10”],
  “Government AI”: [“FITARA compliance”, “OMB AI guidance”, “Procurement standards”]
  }
- Creative Brief: Matching card style. Red accent. Three requirement categories with bold headers (text-lg) and sub-items (text-base). Compact, scannable layout.

- Block 7:

- Block Type: Text
- Placement: Footer
- Component Schema: “Simple Footer”
- Content:
  Footer_Text: “Training estimate: 40-60 hours | Prerequisites: Strong security fundamentals, risk management”
- Creative Brief: Centered, text-base, opacity-70.