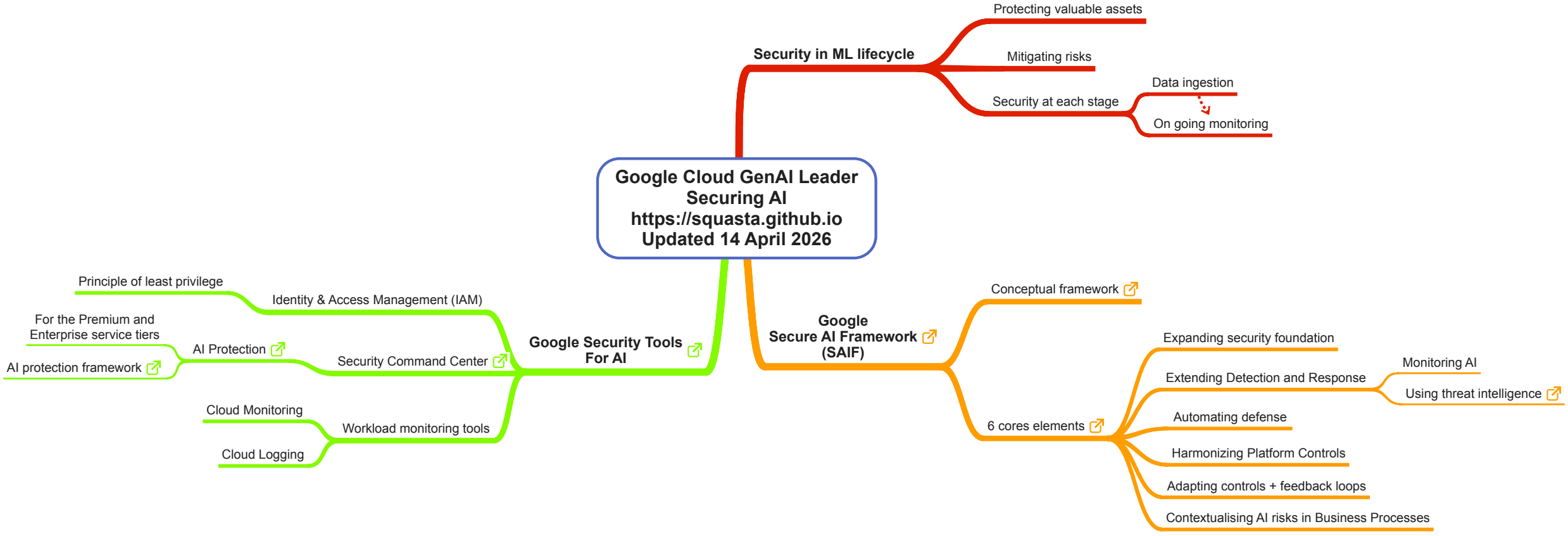
Google Cloud GenAI Leader
Securing AI
https://squasta.github.io
Updated 14 April 2026
Security in ML lifecycle
Protecting valuable assets
Mitigating risks
Security at each stage
Data ingestion
On going monitoring
Google Security Tools For AI
Identity & Access Management (IAM)
Principle of least privilege
Security Command Center
AI Protection
For the Premium and Enterprise service tiers
AI protection framework
Workload monitoring tools
Cloud Monitoring
Cloud Logging
Google Secure AI Framework (SAIF)
Conceptual framework
6 cores elements
Expanding security foundation
Extending Detection and Response
Monitoring AI
Using threat intelligence
Automating defense
Harmonizing Platform Controls
Adapting controls + feedback loops
Contextualising AI risks in Business Processes