Enterprise Architecture Security Services

A customised approach to change implementation while enforcing cyber security best practices.

Securing AI

AI-supported processes will provide improvements in efficiency and productivity, but only if implemented safely and responsibly.

IAM Services

Full-service Identity and Access Management. Strategy, Technology consolidation. Maturity improvement.

Security Architecture

Complex project support. Design and Implementation of technical controls and security checks.

Application Security

Modern development processes, regulations and the surge in supply chain attacks mean demonstrating good practices like Secure SDLC and Code Reviews are now critical.

PAM Services

Privileged Access Management, provides a secure, governed and controlled layer of security We use best practices to reduce the risks associated with your highly privileged credentials.

Cloud Security

Ensure the secure adoption and migration of your data, applications and infrastructure to the cloud. Navigating the complexities of cloud security, ensuring compliance with industry standards and regulations.

Improvement

Automation and cost saving by driving continuous security improvement by consolidation and operationalisation of your security tech stack. Our SME network and infrastructure architects can review your security tools and drive improvements and/or the adoption of technology.

Strategy

The design and implementation of secure, scalable, and cost-effective solutions. Ensure people, processes and technologies are aligned across the enterprise. Alignment of projects and resources helps to drive efficient change.

Innovation

Zero Trust Architecture, AI, Vendor replacement. To stay relevant, you need to constantly innovate. Define clear requirements, before any vendor selection. Engage on a POC of tailored solutions, agree on fit. Establish effort and roadmap.

Management, Governance, Strategy

PMO - Project Management – Governance – Success Management – Intervention – Client Delivery – Quality

Application Security and Blockchain

- Strategic Alignment
- Security Maturity
- Secure SDLC
- K8 security
- Regulatory Compliance
- Dependability & Open-Source management
- Thread Modeling & Contextual Training
- Quality Assessment & Improvement

Identity and Access Management

- Strategy and Roadmaps
- Implementation AD, B2B, B2C
- PAM – CyberArk
- Governance - SailPoint
- Assessments, Standard, Policy writing
- Identity management
- Access management
- Create Technical documentation

AI Security

- Design Green Field Environments
- Secure Architecture for use of AI
- Monitor internal and external policy compliance for use of AI
- AI regulation compliance
- Secure adoption of generative AI
- Microsoft Copilot

Enterprise Architecture

- Architecting & designing solutions
- Review architecture and solution design artifacts
- Provide technical direction and lead
- Ensure suitable sizing of solutions
- Drive, Plan & Develop blueprints
- Collaborate & Guide with other teams

Cloud Security

- **Design, plan, implement & maintain the network infrastructure**
- **Troubleshooting issues which arise**
- **Ensuring compliance with legislation**
- **Secure and monitor networks**
- **Design and implement Private access to Public Cloud Services**

SIEM, Network And Infrastructure Architecture

- Cloud first technology
- Architecture & Design
- Review and Assessments
- Performance optimizations and cost efficiencies
- Secure and align solution with business requirements
- Provide 3rd level support when required
- Maintain & manage patch management& update processes

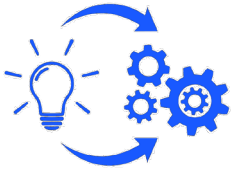
Cloud Security

Assessment & Planning

- Identify vulnerabilities, misconfigurations
- Implement or assess compliance.
- Understand business objectives and regulatory requirements.
- Evaluate and prioritise security risks based on impact & likelihood.

Design & Architecture

- Design architecture considering the principle of least privilege & segregation of duties.
- Align the designs with relevant industry standards & regulations.
- Define IAM policies, roles, and responsibilities to ensure secure access controls.



Implementation & Configuration

- Implement configurations and best practices for cloud services.
- Apply data encryption and other data protection mechanisms that are applicable.
- Set up secure network configurations, including firewalls, VPNs, & segmentation.

Monitoring & Management

- Implement monitoring for real-time security & compliance monitoring.
- Develop & implement an incident response plan to address security breaches.
- Regularly update & patch cloud services & applications to mitigate vulnerabilities.

Training & Awareness

- Security awareness training for employees to identify & prevent security threats.
- Integrate security into the DevOps pipeline to ensure secure coding practices & continuous security assessment.

Review & Optimisation

- Perform periodic security assessments & audits to identify & rectify any new vulnerabilities or compliance issues.
- Establish a feedback mechanism to continuously improve security measures based on new threats, technologies, & business requirements.

Cloud Security Governance

- Establish a cloud security governance framework to ensure consistent security policies, practices, and procedures across the organization.
- Engage key stakeholders in security decision-making processes to align security initiatives with business objectives.

info@ek.co