Enterprise Architecture

G-Cloud 14 Service Definition

Author: Ian Marlow

Version: 1.0
Date: April 19, 2024
Document: EKCO-GEN-447

Table of Contents

Enterprise Architecture

Service Overview

Ekco's Enterprise Architecture division specialises in complex and multiyear initiatives, defining strategy and architecting secure cloud solutions. Our Security Enterprise Architecture team helps organisations drive business innovation. We combine business and technical expertise to bridge the communication gap between business and IT stakeholders in organisations, facilitate information systems planning and improve business and IT alignment.

Leveraging the Ekco Enterprise Architecture division, we can provide you with a team that suits your needs and can support your business's strategy, following the best practices and patterns for building applications.

Features

The key features of the Enterprise Architecture Service are:

- Application Security (AppSec) Assessment
- Cloud Security & Configuration Review
- Enterprise Security Architecture
- Identity & Access Management (IAM / IdAM)
- Privileged Access Management (PAM)
- Securing (Artificial Intelligence) AI

Benefits

The key benefits of the Enterprise Architecture Service are:

- Review of the entire software delivery lifecycle
- Improve security maturity of development teams and operationalise security by design policies and procedures
- Architect around principle of least privilege and segregation of duties
- Identify vulnerabilities, misconfigurations and assess compliance against relevant frameworks
- Define technical controls and security checks aligned to risk appetite
- Provide SASE/SSE solutions from leading vendors
- Develop threat modelling framework aligned to OWASP and Mitre Att&ck
- Design, implementation and tuning of robust IdAM frameworks and PAM
- Enable organisations to adopt generative AI solutions using reference architectures
- Prepare for adoption of ISO/IEC JTC 1/SC 42

Service Outline

Application Security

As the approach to design, build and deployment of software changes, so must the approach to ensuring this is safe and secure in its use. We live in a world where it seems nearly everything has become a product, with success defined as being the one “first to market” and the ability to “push features faster.”

Our application security (AppSec) approach covers the entire software delivery lifecycle, starting from helping to define, implement and review how teams are set up to deliver, monitor and maintain their products. This moves into definition of appropriate AppSec practices and understanding of potential, relevant threats whilst keeping teams up to date with the latest security mitigation techniques as well as training them in good AppSec practices, triage, and mitigations.

Service Offering:

- Assess and improve the security maturity of development teams regarding policies, OWASP and Mitre Att&ck threat determination, coding standards, non-functional requirements, logging, and monitoring, as well as traceability and the use of tooling data insights to drive security improvement
- Helping organisations adopt disruptive AI software engineering agents such as Devin, Devika, and SWE to autonomously solve issues in GitHub repositories as well as educating product and developer teams around the best practices, potential risks, and security measures associated with adopting blockchain technologies
- Conduct code reviews against compliance frameworks, house style, good coding practices and common threats and vulnerabilities using a combination of traditional and Generative AI tools alongside deep technical knowledge from seasoned developers across Web, Mobile, Serverless and Data Science
- Assess and remediate security tooling embedded in development pipelines (including IDE, SAST, SCA, DAST, IAST, RASP, MAST) used to develop, deploy, and monitor applications in line with the organisation’s risk appetite, covering web application, mobile and containerised services such as Kubernetes which would also be reviewed against industry standard hardening guidelines
- Help understand and implement changes to documentation and development practices to encompass any regulatory requirements that may be necessary, including user protection, data privacy, and ethical practices
- Develop strategies to mitigate against supply chain attacks from the use of tainted open-source libraries. These include assessing the supply chain security by ensuring that all components, including open-source libraries, come from trusted sources, and are properly verified before use and the generation of software bill of materials (SBOM) as verified and auditable elements
- Conduct workshops that introduce Thread Modelling to product teams such that potential attack methods are surfaced and considered as part of initial and incremental design in a way that discusses “what is the product”, “who is going to use it and how”, “how do the components work together” and “how would someone attack this, and what could they expose?”

Cloud Security & Configuration Review

To use cloud technologies securely, a holistic approach is needed that ensures data safety and compliance with regulatory standards. Ekco services include creating and applying strong security measures such as encryption, identity and access management, and intrusion detection systems. They also involve ongoing monitoring and auditing to identify and address threats quickly.

Reaping the advantages of cloud technologies while reducing the security threats and challenges that come with them involves a strategic change in operations, moving from conventional on-premises infrastructure to a well architected cloud-based model. This needs thorough preparation and implementation, including choosing the right cloud service provider, transferring data and applications safely, and educating staff to handle and work in the new environment. Our services intend to provide a smooth transition to the cloud, maintaining business stability and improving operational effectiveness.

Service Offering:

- Identify vulnerabilities, misconfigurations and assess compliance against relevant frameworks, regulatory requirements, and business objectives, evaluating and prioritising the security risks based on impact and likelihood.
- Design architecture based on the principle of least privilege & segregation of duties, aligning with relevant industry standards & regulations and best practice in IAM policies, roles, and responsibilities to ensure secure access controls.
- Implement configurations and best practices for cloud services, applying data encryption and other data protection mechanisms that are applicable such as secure network configurations, including firewalls, VPNs, & segmentation
- Implement monitoring for real-time security & compliance monitoring by developing & implementing an incident response plan to address security breaches, linking into patching, and updating cloud services and applications to mitigate vulnerabilities
- Security awareness training for employees to identify & prevent security threats, integrating security into the DevOps pipeline to ensure secure coding practices & continuous security assessment.
- Perform periodic security assessments & audits to identify & rectify any new vulnerabilities or compliance issues by establishing a feedback mechanism to continuously improve security measures based on new threats, technologies, & business requirements
- Establish a cloud security governance framework to ensure consistent security policies, practices, and procedures by engaging key stakeholders in security decision-making processes to align security initiatives with business objectives

Enterprise Security Architecture

As the digital world changes quickly, security is essential, not optional, and you need to adopt innovation to maintain or improve your market position. Our Enterprise Security Architecture Group offers complete solutions that fit your business case and risk appetite. We are experts in bringing the latest technologies, such as Zero Trust and Artificial Intelligence, into your security architecture with an approach that is not

just adding new technologies but integrates them into your organisation in a way that improves your security and creates business value.

Our team of professionals collaborates with you to learn about your specific needs and challenges. We then create a custom security strategy that matches your business goals, then help you realise those goals with our network of partners and SME network.

Service Offering:

- Design and implement technical controls and security checks to support complex initiatives and align with business risk appetite, bridging the gap between technology and business areas
- Identify and create the strategy for cost saving and continuous security improvement through automation, consolidation, and operational efficiencies of your technical stack. Our SME network and specialist architects can review your tooling and drive improvements
- Design and implement secure, scalable, reliable, and cost-effective solutions that ensure people, processes and technologies are aligned across the Enterprise and enabling efficient change, especially in complex transformations
- Vendor and platform comparisons to determine the best fit for you, including the generation and assessment of proof of concept and proof of value to ensure that the chosen solution meets the desired requirements and delivers the expected benefits
- SASE/SSE solutions from Zscaler, Cato Networks, Cisco, Microsoft

Identity & Access Management

Our Identity & Access Management (IdAM) practice helps organisations with the knowledge and skills they need to deal with the complex landscape of IdAM. We simplify IdAM, providing a deep insight into its principles, benefits, and applications, helping you choose the best IdAM solutions for your specific needs and constraints. Our step-by-step guidance on implementation covers system setup, integration, user enrolment, and setting up access controls. We make sure you have the skills to fix common problems and adjust your IdAM systems for optimal performance.

We not only cover the technical aspects, but also explore IdAM security best practices and risk management, helping you identify possible risks and how to reduce them. We also address the legal and regulatory aspects of IdAM, making sure your organization follows the rules. With resources for ongoing learning, we keep you informed with the latest changes and advances in the IdAM field.

Service Offering:

- Design, implementation and tuning of robust IdAM frameworks tailored to your needs
- Implementation and tuning of CyberArk for Privileged Access Management (PAM), configuring it to meet your specific needs and ensuring that privileged accounts are properly secured and monitored
- Implementation and tuning of SailPoint identity governance, ensuring a secure, efficient, and compliant identity management system
- Assess existing implementation and governance of access controls, finding and addressing gaps in process and documentation

Securing AI

The security of AI enabled solutions is essential, as it is increasingly involved in our digital environment, and one of the key aspects of protecting AI-based systems is identifying the weaknesses that could be taken advantage of by harmful actors. This involves dealing with threats, such as the generation of false information by AI, as well as data and privacy related issues such as unintentional sharing of privileged information due to inconsistent classification, which can cause serious and widespread harm.

Another challenge is the privacy and security of the data that publicly accessible Large Language Models (LLMs) use. This data, which is huge and diverse in content, is exposed to risks, undermining both the AI system's reliability and the safety of confidential information. Moreover, the problem of model degradation during repeated cycles requires supervision to ensure consistent performance and stability. Efficient methods must therefore be devised to safeguard AI solutions, focusing on powerful encryption, continuous supervision, and strict access control.

Service Offering:

- Creation of reference architectures for AI-enabled solutions, ensuring the safe and efficient integration of AI technology into an organisation's systems and processes. Monitor internal and external policy compliance for use of AI
- Helping organisations adopt disruptive AI software engineering agents such as Devin, Devika, and SWE to autonomously solve issues in GitHub repositories
- Design and implement AI-enabled applications and workflows using tools such as Microsoft Copilot Studio, leveraging innovative technology and industry-leading practices to deliver customised solutions that enhance operational efficiency, streamline processes, and drive innovation
- Prepare organisations to adopt and implement relevant existing and emerging AI regulations, such as ISO/IEC JTC 1/SC 42 or the EU Artificial Intelligence Act, by providing guidance on compliance requirements, designing, and implementing secure AI architectures, and ensuring the safe and efficient integration of AI technology into an organisation's systems and processes
- Enable organisations to adopt generative AI solutions such as Microsoft Copilot, Azure OpenAI, Claude-3 Opus and Google Gemini in a safe way, focusing on powerful encryption, continuous supervision, and strict access control as well as budget and latency aspects using CalypsoAI