



Enterprise Security

G-Cloud 14 Service Definition

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



Table of Contents

Enterprise Security 2

 Service Overview 2

 Features 2

 Benefits..... 2

Service Outline 4

 Email Security 4

 Endpoint Security 4

 Password Management..... 5

 Secure Web Gateway 5

 Security Awareness Training 6

 Security Operations..... 6

 Security Technology Engineering..... 7

 Telecom Security..... 8

 Vulnerability Management 8



Enterprise Security

Service Overview

Ekco's Enterprise Security team focuses on driving security success with innovative, dynamic, and reliable security services. In today's rapidly evolving cyber threat landscape, cyber security teams worldwide face an ongoing battle against the latest and most sophisticated threats to their cloud services. To effectively combat these threats, they require not only the best tools and expertise but also industry-grade processes, automation, governance, and monitoring capabilities.

Ekco's Enterprise Security team strengthen an organisations overall cyber defence capabilities by assessing, implementing, migrating, optimising, and operating an organisations security stack. The team of experienced specialists safeguard against toolset misconfiguration while increasing return on investment, solution efficacy and elevating security operationally.

Features

The key features of the Enterprise Security Service are:

- Security Engineering
- Cybersecurity Technology Assessment
- Cybersecurity Technology Implementation
- Cybersecurity Technology Migration
- Security Operations
- Cybersecurity Operations Assessment
- Cybersecurity Operations Optimisation
- Cybersecurity Staff Augmentation
- Security Awareness Training
- Telecom Security

Benefits

The key benefits of the Enterprise Security Service are:

- Assessments of cybersecurity technology to optimise costs and streamline processes
- Assessments of cybersecurity operations to optimise costs and streamline processes
- Implementation of EDR, MDR and XDR solutions
- Implementation of vulnerability management platforms tailored to organisational needs
- Implementation of web gateway solutions customised to organisation's security posture
- Implementation of password management platforms tailored to organisational needs

- Implementation of a robust and adaptable cyber security operations function
- Simulate real-world phishing attacks to test employees' susceptibility
- Reinforce organisation's security policies and procedures and ensure compliance
- Evaluates threat detection, incident response and vulnerability management capabilities
- Increase organisation's ability to mitigate against email-based threats

Service Outline

Email Security

Ekco's Email Security services leveraging our expert engineering team, technology partnerships, and industry-leading practices, enable organisations to enhance their security posture and mitigate risks within the largest threat vector, Email, Ekco's Email Security services offer several stages including assessments, planning, design, implementation, migration, optimisation, monitoring, and training for numerous Email Security solutions.

Increase the organisations ability to mitigate against email-based threats with Ekco's Email Security services providing experienced and certified engineers to ensure Email Security tooling is setup to prevent email attacks are stopped before they get to the user's inbox.

Service Offering:

- Conduct comprehensive evaluations of email security technology deployments to understand strengths, weaknesses, and opportunities for enhancement
- Implement leading innovative email security technology solutions tailored to align with the organisation's security goals
- Shift from outdated email security products to state-of-the-art next-generation solutions, prioritising seamless integration to minimise disruptions
- Elevate existing email security infrastructures to maximise return on investment, bolster performance, reduce expenditure, and streamline operational workflows
- Monitor and Maintain Email Security so evolving attacks can be identified and swiftly adjust security measures accordingly

Endpoint Security

Ekco's Endpoint Security services offers a holistic approach to endpoint security, encompassing assessments, planning, design, implementation, migration, optimisation, monitoring, and training. By leveraging Ekco's expert engineering team, technology partnerships, and industry leading practices, we enable organisations to enhance their security posture and mitigate risks starting from securing their endpoints. Mitigate Against Misconfiguration Ekco's endpoint security services provide deeply experienced and certified engineers to configure and deploy your endpoint security solutions to the highest possible standards to enable the monitoring, detection, and response to advanced threats.

Service Offering:

- Evaluate endpoint technology deployments thoroughly to identify strengths, weaknesses, and opportunities for improvement
- Deploy the most advanced EDR, MDR and XDR technology solutions that are customised to fit the changing needs of an organisation's security posture

- Migrate from outdated endpoint products to the newest next-gen products, ensuring minimal disruption and optimal organisations security posture
- Enhance deployed endpoint solutions to optimise return on investment, improve performance, reduce costs, and streamline processes
- Actively monitor, detect, and respond to threats and enable quick response to incidents

Password Management

Ekco's Password Management services assess, implement, migrate, enhance, and manage organisations password management solution. Ekco's expert engineering team, technology partnerships, and industry-leading engineering practice, enables organisations to enhance their password management by centralising password security and streamlining user provisioning. The utilisation of weak and recycled passwords poses security vulnerabilities, increasing the likelihood of cyberattacks or data breaches for organisations.

To mitigate these risks, it is imperative for all businesses to adopt a robust password management solution. Ekco's Password Management services allow organisations to implement solutions to support a robust password security policy and in turn reduce exposure for users' credentials.

Service Offering:

- Assess existing password management deployments, benchmarking against industry best practices, and formulate an improvement roadmap
- Implement the most suitable password management platform tailored to the organisation's specific needs and requirements, ensuring optimal functionality and efficacy
- Migrate from outdated password management products to the latest best in-class platforms, ensuring increased protection
- Optimise already deployed password management solutions to enhance return on investment, improve performance, reduce costs, and streamline processes
- Manage and maintain password management platforms and programs to ensure adherence to security standards, facilitate seamless user access, and strengthen defences against unauthorised access or data breaches

Secure Web Gateway

Ekco's Secure Web Gateway services offer a complete approach to assessing, planning, designing, implementation, migration, optimisation, monitoring, and training for Secure Web Gateways. By leveraging Ekco's expert engineering team, technology partnerships, and industry-leading practices, we enable organisations to enhance their security posture and mitigate risks addressing concerns for multi-cloud enterprises. Mitigate Against Misconfiguration with Ekco's SWG services providing experienced and certified engineers to configure and deploy your SWG solutions to the highest possible standards to secure connectivity, improve visibility and enhance optimisation.

Service Offering:

- Evaluate web gateway technology deployments thoroughly to identify strengths, weaknesses, and opportunities for improvement
- Deploy the most advanced web gateway technology solutions that are customised to fit the changing needs of an organisation's security posture
- Migrate from outdated web gateway products to the newest next-gen products, ensuring minimal disruption and optimal organisation's security posture
- Enhance deployed web gateway solutions to optimise return on investment, improve performance, reduce costs, and streamline processes
- Secure Connectivity, Enhance Optimisation and Improve Visibility while integrating with your security stack

Security Awareness Training

As cyber threats become more numerous and sophisticated, it is essential to equip employees with the knowledge and skills to identify and respond to potential attacks. Employees are often the first line of defence against cyberattacks, but they can also be the weakest link if not adequately trained and aware of the risks. Ekco offers Security Awareness Training as a Service, a comprehensive solution that helps foster a culture of security awareness within your organisation.

Our service provides employees with the tools and knowledge they need to protect themselves and organisations from cyber threats. Ekco's Security Awareness Training ensures employees are prepared to defend against cyberattacks.

Service Offering:

- Engage employees with interactive and customisable training modules that cover various cyber security topics, such as phishing, ransomware, password management, social engineering, and more
- Simulate real-world phishing attacks to test employees' susceptibility and provide targeted feedback and training based on the results
- Reinforce organisation's security policies and procedures and ensure compliance with relevant industry regulations and standards
- Track and measure employees' progress and performance with detailed analytics and reporting dashboards
- Access expert support from our team of cyber security professionals who can provide guidance, assistance, and additional resources to enhance training effectiveness

Security Operations

Ekco Security's Security Operations service is a vital resource for organisations looking to strengthen their cyber security operations. This service helps organisations evaluate and implement a robust and adaptable cyber security operations function that can effectively and efficiently identify, respond to, and recover from incidents.

Staffed by industry experts with a track record of transforming Security Operations for numerous enterprises, Ekco's Security Operations Service is well-equipped to navigate the ever-changing cyber security landscape. With new risks and opportunities emerging on a daily basis, Ekco's Security Operations Service provides organisations with the protection they need to defend against cyber-attacks.

Service Offering:

- Evaluates your current processes, tools, and capabilities across various domains of cyber security operations, such as threat detection, incident response, vulnerability management, and compliance
- Identifies and classifies the risks and inefficiencies that may compromise your security posture, based on their severity and impact
- Provides a detailed report that contains both an executive summary for decision-makers and technical insights for SecOps teams, along with strategic recommendations for improving your cyber security operations maturity and effectiveness
- Supports you in implementing the recommendations and measuring the outcomes, ensuring that you achieve the desired results and benefits
- Offers you access to highly skilled and experienced cyber security professionals who can augment your existing staff, fill any skill gaps, and provide additional support for your operations

Security Technology Engineering

Ekco's Security Technology Engineering service offers specialised expertise in a comprehensive array of critical areas, including assessment, implementation, migration, and continuous monitoring of an organisation's cybersecurity technology landscape. Our primary objective is to ensure that every facet of our clients' security tooling is not only securely deployed but also optimised to its fullest potential, thereby guaranteeing that their investment yields maximum returns.

At Ekco, our highly qualified and experienced engineering team is dedicated to the meticulous construction and maintenance of technology solutions. We operate with a keen focus on aligning these solutions with our clients' unique business objectives, stringent security requirements, and the most current industry best practices.

Service Offering:

- Conduct comprehensive assessments of cybersecurity technology to pinpoint strengths, weaknesses, and areas for enhancement within existing deployments
- Deploy innovative cybersecurity technology solutions tailored to meet the evolving needs of an organisation's security posture
- Migrate legacy systems, data, and applications to modern platforms, prioritising minimal disruption and maximising operational efficiency
- Optimise cybersecurity technology performance, minimise costs, and streamline processes to fortify defences, reduce expenses, and enhance operational workflows

- Proactively monitor performance, security, compliance, and capacity to promptly detect and address issues, ensuring optimal resource utilisation and regulatory adherence

Telecom Security

EKCO's telecommunications security service relies on an expert team of dedicated security consultants with extensive experience within IT, networking and telecoms, who are certified in areas such as ISO27001, networking, cloud and security testing. The objective of this service is to ensure security compliance throughout your telecommunications IT and Network infrastructure, ultimately ensuring confidentiality, integrity and availability for the intricate and crucial telecoms infrastructure, which is heavily relied upon for national communication and the storage of large volumes of sensitive data.

The service includes offerings from secure by design, to penetration testing, to business-as-usual compliance, as well as many more to fit the needs of the client.

Service Offering:

- Secure by design process for project lifecycles including:
 - Scoping a project and engagement
 - Security requirements compliance review and sign off
 - Design reviews and sign off
 - Penetration testing and vulnerability scanning
 - Security reporting
 - Security sign off approvals
- Reoccurring penetration testing, vulnerability scanning and security reporting
- Ensuring a vulnerability management process and risk management process in line with company policies and procedures
- Ensuring company wide business-as-usual security compliance with policies and standards
- Configuration of security/network devices and software such as, WAF configuration and onboarding, firewall review and implementation, Microsoft 365 phishing activities, SIEM integration and onboarding, EDR configuration

Vulnerability Management

Ekco's Vulnerability Management services assess, implement, migrate, enhance, and manage organisations vulnerability management platforms and programs. Ekco's expert engineering team, technology partnerships, and industry-leading engineering practice, enables organisations to enhance their vulnerability management and remediation processes to address potential security weaknesses.

Enhancing the ability of Vulnerability Management solutions and teams' abilities to isolate and remediate against these weaknesses reduces the organisations overall risk exposure. Gaining visibility into vulnerabilities active within the organization allows for proactive risk mitigation, informed decision-

making, and the implementation of targeted security measures to safeguard critical assets and maintain operational resilience.

Service Offering:

- Assess existing vulnerability management programs and deployments, benchmarking against industry best practices, and formulate an improvement roadmap
- Implement the most suitable vulnerability management platform tailored to the organisation's specific needs and requirements, ensuring optimal functionality and efficacy
- Migrate from outdated vulnerability management products to the latest best in-class platforms, ensuring increased detection and focused remediation
- Optimise already deployed vulnerability management solutions to enhance return on investment, improve performance, reduce costs, and streamline processes
- Manage vulnerability management platforms and programs to ensure comprehensive coverage, timely response to emerging vulnerabilities, and continuous improvement in overall security posture