INFORMATION SECURITY

Assessment, Governance & Solution

INFOSEC SOLUTIONS & SERVICES

REVERE TECHNOLOGIES (KE) LIMITED

INTRODUCTION

Revere Technologies is a leading information security services & solutions provider in Sub-Saharan Africa at large enabling customers to protect their critical information and infrastructure through a prudent combination of people, process and technology. With a unique business model, strong values and philosophy, combined with trained, certified and highly experienced workforce, Revere Technologies delivers deep insight and value to customers seeking a partner they can trust and consult. With our customer-centric approach we are motivated to provide our customers with specially tailored services providing protection against external as well as internal threats and reduce business risk to improve security posture, achieve regulatory compliance and increase efficiency.

Technology trends such as Cloud Computing, Digitization, Internet of Thing, Collaboration, and Externalization are redefining the way in which an enterprise needs to look at information security. In the current scenario, perimeters are non-existent and traditional approaches adopted for data security services are no longer sufficient. With cyber-attacks growing exponentially, enterprises are rushing to find the best way to reduce risks and limit the impact of breaches. The major challenges being faced by enterprises today are defending and protecting assets, detecting and stopping threats, identifying, managing accessing, and ensuring compliance.

Our “Information Security Services & Solutions” helps our customers move from a “Static” to a “Dynamic” posture to deal with an ever-escalating threat landscape, offering full spectrum of services and solutions.

INFOSEC SOLUTIONS & SERVICES

- **Information Security Services**
  - Information Security Assessment & Audits
  - Vulnerability Assessment Penetration Testing
  - Information Security Management System Framework Development, Implementation and Deployment – ISO 27001
  - Information Security Risk Management
  - PCI DSS Implementation

- **Data Protection**
  - Data Loss Prevention (DLP), Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.
  - Database Security, Database security covers and enforces security on all aspects and components of databases. This includes: Data stored in database, Database server, Database management system (DBMS) and other database workflow applications.

- **Identity & Access Management**
  - Multi-factor Authentication, Multi-factor authentication (MFA) is a method of confirming a user's claimed identity in which a user is granted access only after successfully presenting 2 or more pieces of evidence (or factors) to an authentication mechanism.
  - Privileged Access Management (PAM), Privileged account management can be defined as managing and auditing account and data access by privileged users. Privileged Access Management report provides analysis, key findings, and recommendations to help organizations secure, manage, and monitor privileged accounts and access.

- **Network Access Control (NAC)**
  - Network access control, solution support network visibility and access management through policy enforcement on devices and users of corporate networks. With organizations now having to account for exponential growth of mobile devices accessing their networks and the security risks they bring, it is critical to have the tools that provide the visibility, access control, and compliance capabilities that are required to strengthen your network security infrastructure.

- **Security Information and Event Management (SIEM)**
  - Security information and event management (SIEM) is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system. SIEM provides real-time analysis of security alerts generated by applications and network hardware.

- **Vulnerability Management**
  - Vulnerability management is the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities", particularly in software. Vulnerability management is integral to computer security and network security.

- **End-Point Security (EDR)**
  - Endpoint security refers to securing endpoints, or end-user devices like desktops, laptops, and mobile devices. Endpoints serve as points of access to an enterprise network and create points of entry that can be exploited by malicious actors. Endpoint security software protects these points of entry from risky activity and/or malicious attack.

- **Web Application Security**
  - Web application security is a branch of Information Security that deals specifically with security of websites, web applications and web services. At a high level, Web application security draws on the principles of application security but applies them specifically to Internet and Web systems.

- **Email Security**
  - Email security describes different techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss or compromise. Email is often used to spread malware, spam and phishing attacks. Attackers use deceptive messages to entice recipients to part with sensitive information, open attachments or click on hyperlinks that install malware on the victim’s device. Email is also a common entry point for attackers looking to gain a foothold in an enterprise network and obtain valuable company data.

- **Cyber Threat Intelligence / SOC Operations**