SMART

TECHNOLOGY SOLUTIONS

CLOUD & DEVOPS

SOFTWARE DEVELOPMENT

BUSINESS APPS

Cybersecurity Solutions

SMART helps organizations and businesses achieve the highest possible level of security for their technology assets and information by providing experienced cybersecurity professionals skilled in the latest security technologies and techniques.

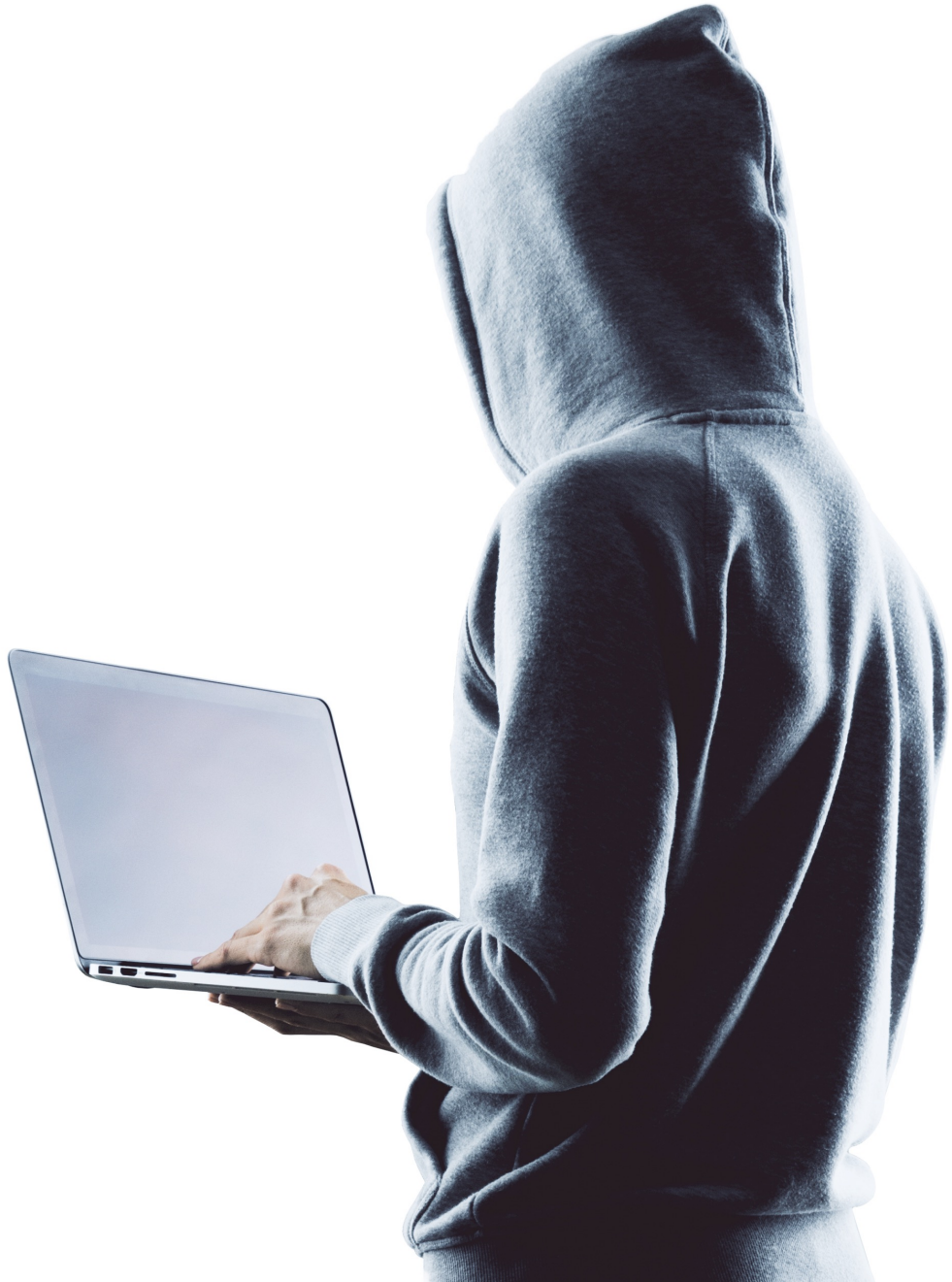

TABLE OF CONTENT

Assessment & Monitoring

Identify potential security risks and vulnerabilities.

Review security policies and procedures

Provide recommendations for improving the organization's security posture

Conduct regular security assessments and audits.

Provide ongoing security awareness training for employees.

Conduct penetration testing, vulnerability scanning, and risk assessments

Conduct security awareness training for employees

Continuously monitor an organization's networks and systems for potential security incidents or breaches

Use advanced security tools and platforms, such as firewalls, intrusion detection and prevention systems, and security information and event management (SIEM) solutions

Assessment & Monitoring Solutions

- Security Design & Architecture
- SIEM security information & events management
- SOC Analysis L1, L2, L3
- MSSP Managed Security Services Provider
- Threat detection and Incident response
- Vulnerability & Risk Management

Network Security

Network access control services: Ensure only authorized users and devices can access organizational networks and systems.

Firewall services: Block unauthorized access to networks

PAM systems: Manage and monitor privileged accounts.

Intrusion detection and prevention services: Detect and prevent potential security threats.

Network segmentation: Divide a network into smaller subnetworks to improve security and reduce the risk of unauthorized access.

IAM systems: Ensure only authorized users have access to sensitive information and systems.

Virtual Private Network (VPN) services: Provide secure remote access to organizational systems and data.

Network Security Solutions

- NGFW next generation-firewall
- ML Machine learning Firewalls
- IPS intrusion prevention system
- IDS intrusion detection system
- VPN Virtual Private Network
- ZTNA Zero-Trust Network Access
- NAC Network Access Control
- PAM (Privileged Access Management)
- IAM (Identity and Access Management)
- SASE (Secure Access Service Edge)
- CASB (Cloud Access Security Broker)
- SD-WAN software-defined wide area network
- Load Balancing (LTM , GTM) local & Global traffic

Application Security

Protect software applications from potential security threats and vulnerabilities.

Identify and mitigate security risks throughout the software development lifecycle, from design to deployment.

Typically include a range of security measures, such as:

- Code review and analysis
- Web application firewall (WAF) services
- Penetration testing
- Security testing and validation
- Secure coding practices

Application Security Solutions

- WAF web application firewall
- Penetration testing
- Code, Configuration Review and Analysis
- Web Proxy (Explicit – Reverse)

Endpoint Security

Monitors endpoints for signs of cyber-attacks or malicious activity

Provides real-time threat detection and response capabilities.

Collects data on endpoint activity, network traffic, and system events.

Analyzes and correlates data to identify potential threats.

Key features include:

- Forensic analysis
- Reporting and alerts
- Endpoint monitoring
- Threat detection
- Incident response

Solution:

- EDR Endpoint detection & response
- XDR Extended Detection and Response

Email Security

Secure Email Gateways

Spam Filters

Email Encryption Tools

Anti-Phishing Tools

Email Authentication

Phishing Simulation and User Training

Secure Messaging Platforms

Solutions:

- Email security system

Cloud Security

Secures cloud-based infrastructure, applications, and data.

Protects against threats such as data breaches, cyber-attacks, and unauthorized access.

Key features:

Identity and access management (IAM): Manages user access to cloud-based resources and data and enforces security policies.

Network security: Protects cloud-based infrastructure from cyber-attacks with firewalls and intrusion detection and prevention systems.

Data protection: Encrypts and protects data stored in the cloud to prevent unauthorized access.

Vulnerability management: Identifies and addresses security vulnerabilities in cloud-based infrastructure and applications.

Compliance management: Helps organizations comply with regulatory requirements and industry standards.

Network Security Solutions

- Cloud Firewall, FwaaS (Firewall as a services)
- Cloud IPS/IDS
- Privacy management system
- IAM identity access management
- MDM mobility device management
- Cloud EDR
- Cloud SIEM & SOAR

Data Security

Protect sensitive data from unauthorized access, theft, or modification.

Use a combination of technologies and processes to ensure confidentiality, integrity, and availability of data.

Key features include:

Data encryption: Protects sensitive data at rest and in transit.

Data loss prevention (DLP): Monitors data access and usage, prevents data leakage or theft.

Solution:

- DLP Data lose prevention.

THEY'RE PART OF OUR SUCCESS

www.smart.sa +966593440030 920024779 info@smart.sa

Saudi Arabia | GCC | Africa