

CASE STUDY OF

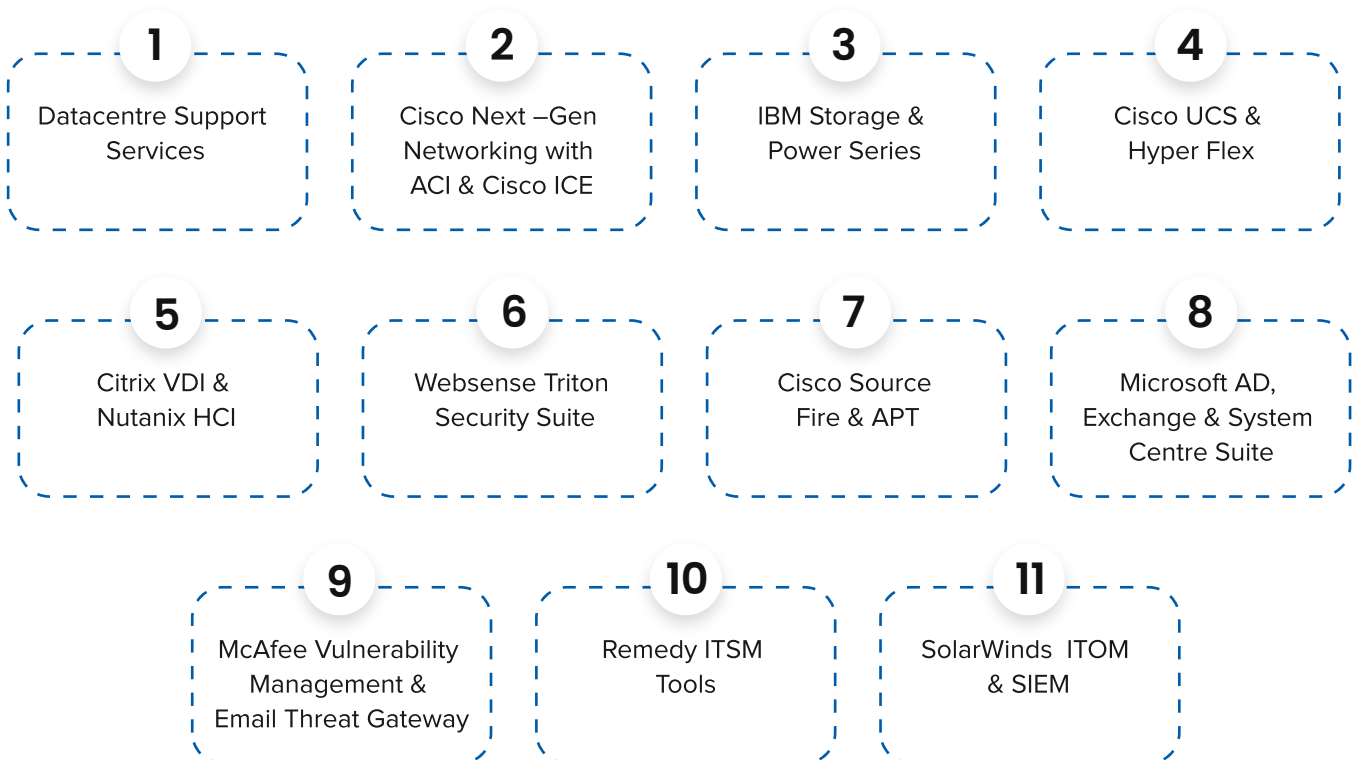
CYBER SECURITY MANAGED SERVICES

Largest Credit Card Service provided in KSA

The Client is a leading Global Premium Credit Card services company in Kingdom of Saudi Arabia and headquartered in USA with Revenue of 30 Billion US\$. The organisation has been rated as 22nd best Brand in the World and employee's 50000 people around the Globe.

- Out-dated security infrastructure meant an inability to cope with new and evolving security threats.
- Poor mechanisms of governance risk and compliance as per SAMA requirements.
- Lack of skillset & specialization to manage Internal vulnerability management & threat management solutions.
- Absence of enterprise security solutions for vulnerability management & Data protection.
- Had difficulty managing operational lifecycle of existing security environment.
- Obsolete and non-supportable end user computing equipment and operating systems.
- No Visibility/Centralized view of Infrastructure.
- Team members require frequent Skill upgrade trainings.
- Reactive and firefighting mode.
- No Problem Management & Knowledge management.
- Service reporting and metrics are adhoc and inconsistent.
- The security operations and threat management were poorly configured.
- There were multiple challenges with new application role outs of American express to be adapted and ratified for PCI standards.

Technology Backdrop



Skillmine Solution

- Information Security Consulting.
- Dedicated ODC Setup at Skillmine Bangalore Facility for Managed Security & Infrastructure Services.
- Design & Deployment of Security & infrastructure monitoring and response Solution.
- Recurring Vulnerability, Threat Assessment & Remediation from remote ODC.
- Management, Support & Enhancement of Data Protection Solutions Remotely.
- A 24X7 Command Centre Setup with Relevant Monitoring Tools.
- Formulation of Event Management, Incident Mgmt & Major Incident management process.
- Fine tuning of the existing tools and features.
- Post Maturity from ODC, moved the Service Back to 100% onsite in KSA.



How did we do?

- Created a Hybrid abled technical team of offshore & onsite team of people.
- Refreshed the entire GRC structure with IT Risk, Policies, Processes, Procedures, KPIs and establishing an IT Security Council headed by CEO to meet quarterly. This was aligned with the regulatory compliance (SAMA & NIST).
- Reconfiguration and upgrades of various IT Security solutions for end point, compute, network, database, web, email and data security over 18 months to tighten the Tech security.

4 Created & Implemented a SOC Service to monitor Security alerts and threats. deployed brand protection mechanisms.

5 Undertook quarterly VAPT exercises to remediate newer vulnerabilities. Tested policies and evidence for ISO & PCI compliance.

6 Established the Metrics based dashboard for measuring the coverage & effectiveness of the IT Security posture.

7 Created a comprehensive a User Training Awareness program. Also, established the Third Party Audit mechanisms for AESA.

Business Benefits

- Adherence to the required security posture standard like SAMA CSF NIST and PCI DSS.
- Better visibility into their devices to ensure overall security posture and compliance through implementation of Data Protection Solutions.
- Lowered its TCO for security infrastructure operation, maintenance and incident response.
- Skillmine enabled the client to focus its resources on more strategic and tactical business requirements.
- Processes and systems ensure proactive and effective management of security infrastructure.
- Existing features are better utilised and discouraged the procurement of extra tools. Improved availability, and efficiency.
- Faster response and resolution to IT incidents resulting in lesser revenue loss.
- Higher quality and reliability of IT infrastructure services.
- Proactive Monitoring of Critical IT systems.



Data Points

6+

Locations

Covered more than six locations across middle east of AESA, across Riyadh and Dubai and UAE.

200+

Virtual machines

Implemented the security solutions across both the data centres with more than 200+ virtual machines compute area, across 1200+ network nodes.

600+

User bases

The user training awareness program was covered for more than 8+ functional departments covering 600+ user bases.

200k

Emails

Over 200 thousand emails being identified for quarantine per week.

80%

Reduced

Spam mail was reduced by 80% over the period of six months.

4k+

Low Vulnerabilities

Eradicated up over 570 medium vulnerabilities and 4000+ low vulnerabilities.

600+

End point

Managed more than 600+ end point protection programmes which are updated in less than 10 days across the state.

300

Threats

Identified more than 300 threats every month and quarantined.

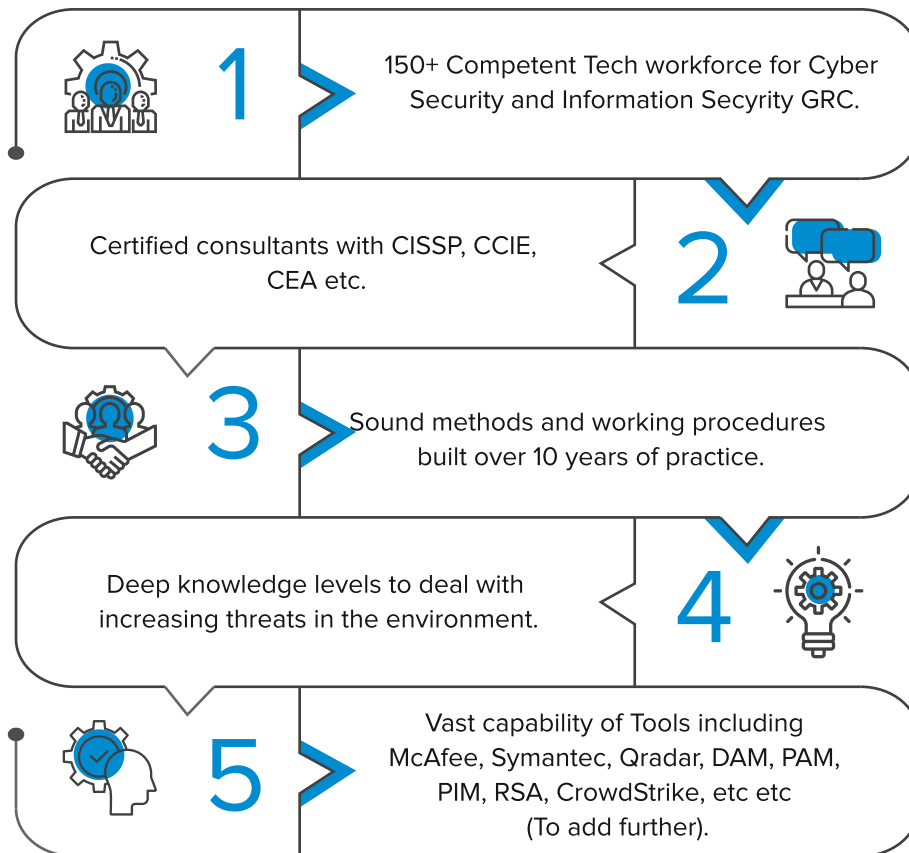
20+

Malware detected

More than 20 malwares detected and nullified per week.



Capability & Competency



For more information
Contact: info@skill-mine.com
Visit us: skill-mine.com

 **Skillmine**
Technology • Consulting • Services

India | KSA | UK | USA