Skillmine
Technology • Consulting • Services

# How Skillmine's Cybersecurity Managed Services enabled KSA's largest credit card service provider to strengthen its cybersecurity posture.

The client is a leading global premium credit card services company in the Kingdom of Saudi Arabia, headquartered in the USA. The company employs around 50,000 people around the globe, generates a revenue of 30 billion US dollars and has been rated as the 22nd best brand in the world. The client was in pursuit of heightened system visibility and fortified cybersecurity. They reached out to Skillmine, which helped them augment their security measures and gain comprehensive insights into their existing systems.

# **Business** Challenges

- Lack of visibility/centralized view of infrastructure.
- Team members required frequent skill upgrade training.
- Lack of problem management and knowledge management.
- Service reporting and metrics were ad-hoc and inconsistent.
- Security operations and threat management were poorly configured.
- Difficulty managing the operational lifecycle of the existing security environment.

- Obsolete and non-supportable end-user computing equipment and operating systems.
- Multiple challenges with new application rollouts to be adapted and ratified for PCI standards.
- Absence of enterprise security solutions for vulnerability management and data protection.
- Out-dated security infrastructure meant an inability to cope with new and evolving security threats.
- Poor mechanisms of Governance, Risk and Compliance (GRC) as per SAMA requirements.
- Lack of skillset and specialization to manage internal vulnerability and threat management solutions.

# **Solutions** Offered

## Information security consulting.

01 A dedicated ODC was set up at Skillmine's Bangalore facility for managed security and infrastructure services.

02 Design and deployment of security and infrastructure monitoring and response solutions.

03 Recurring vulnerability, threat assessment and remediation from remote ODC.

04 Management, support and enhancement of data protection solutions remotely.

05 A 24/7 command centre was set up with relevant monitoring tools.

06 Formulation of event management, incident management and major incident management process.

07 Fine-tuning of the existing tools and features.

08 Moved the service from ODC to 100% onsite in KSA, post maturity.

# Execution:
# Skillmine Approach and Methodology

- Created a hybrid-abled technical team of offshore and onsite teams of people.
- Refreshed the entire GRC structure with IT risk, policies, processes, procedures, and KPIs and established an IT security council headed by the CEO to meet quarterly. This was aligned with the regulatory compliance (SAMA and NIST).
- Reconfigured and upgraded various IT security solutions for endpoint, network, database, web, email, and data security over 18 months to tighten tech security.
- Created a comprehensive user training awareness program. Also, established the third-party audit mechanisms for AESA.
- Created and implemented a SOC service to monitor security alerts and threats. Deployed brand protection mechanisms.
- Undertook quarterly VAPT exercises to remediate newer vulnerabilities. Tested policies and evidence for ISO and PCI compliance.
- Established a metrics-based dashboard for measuring the coverage and effectiveness of the IT Security posture.
- Created a comprehensive user training awareness program. Also, established the third-party audit mechanisms for AESA.

# **Business** Impact

- Adherence to the required security posture standards like SAMA, CSF, NIST, and PCI DSS.
- Better visibility into the client's devices to ensure overall security posture and compliance through the implementation of data protection solutions.
- Lowered TCO for security infrastructure operation, maintenance and incident response.
- Enabled the client to focus its resources on more s trategic and tactical business requirements.
- Existing features were better utilized, and the procurement of extra tools was discouraged. This improved availability and efficiency.
- Faster response and resolution to IT incidents resulted in lesser revenue loss.
- Proactive monitoring of critical IT systems.

# Results and Benefits

Over 200 thousand emails were identified per week.

More than 20 malware was detected and nullified per week.

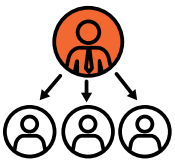
Spam mail was reduced by 80% over the period of six months.

Identified and quarantined more than 300 threats every month.

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

Covered more than six locations across the Middle East of AESA, Riyadh, Dubai and UAE.

The user training awareness program covered over eight functional departments with 600+ user bases.



Managed over 600+ endpoint protection programs updated in less than ten days across the state.

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

Skillmine
India | KSA | UK | USA



Stay connected