Unlocking
Infinite
Possibilities

xencia

XENSHIELD365
XDR based Managed Support

Security Challenges

Managed Detection & Response

- Having challenges managing security for complex hybrid environment?
- Is your Team spending lot of time and efforts in analysing multiple security tools and its events & alerts?
- Do you need more Realtime alerting & visibility into your endpoint intrusions & threats?

Cloud Security

- Are your cloud workloads sufficiently protected and scored against industry benchmarks?
- Do you have protection specific to the cloud workloads you are running?
- Are your source code base and CI CD pipelines safeguarded?

Endpoint Security & Mgmt.

- Is your IT team overwhelmed by variety of types, versions, models of devices?
- Finding difficult to manage applications and its configurations for different groups of users?
- Are you finding difficult to manage policies for Cross-platform OS and BYOD?

Xencia's Solutions to your Challenges

- ✓ Unified threat and alert management for a complex hybrid environment
- ✓ Save time and efforts in focusing efforts on single log analytics platform
- ✓ AI & ML based threat and alert processing eliminating noisy alerts and false positives

- ✓ Industry standards-based security assessment scoring
- ✓ Very specific workload-based protection assessment rather than generalized
- ✓ Protection for your DevOps

- ✓ Unified management of devices and applications saving time and efforts and improved efficiency
- ✓ Productivity saved can be used for new business initiatives

xencia

Xencia Security Services

Managed Detection & Response
24X7 SOC

- ✓Incident Monitoring and Reporting
- ✓Threat Detection and Hunting
- ✓SIEM Event correlation
- ✓Security policy setup
- ✓Vulnerability Scanning and Patching
- ✓Root Cause Analysis
- ✓24x7 SOC

Security Consultation:

- ✓Expert Investigation
- ✓Implementation and management

Cloud Security

- ✓ Solution Assessment & Consultation
- ✓ Workshops & POC
- ✓ Implementation
- ✓ 24x7 Managed Support

Endpoint Security & Mgmt.

- ✓ Solution Assessment & Consultation
- ✓ Workshops & POC
- ✓ Implementation
- ✓ 24x7 Managed Support

xencia

Xencia Security Tech Stack

Managed Detection & Response

- Microsoft Sentinel
- Microsoft Defender for Cloud
- Microsoft 365 Defender
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender Vulnerability Management
- Microsoft Defender Threat Intelligence

Cloud Security

- Microsoft Defender for Cloud
- Microsoft Defender Cloud Security Posture Mgmt.
- Microsoft Defender for DevOps
- Microsoft Defender External Attack Surface Management
- Azure Firewall
- Azure Web App Firewall
- Azure DDoS Protection
- GitHub Advanced Security

Endpoint Security & Mgmt.

- Microsoft Intune core capabilities
- Microsoft Defender for Endpoint
- Microsoft 365 Defender
- Microsoft Intune Endpoint Privilege Management
- Microsoft Intune Remote Help
- Microsoft Defender for IoT
- Microsoft Defender for Business
- Microsoft Defender Vulnerability Management

xencia

XenSHIELD365 / SOC Lite

Managed Detection and Response (MDR)

Managed Detection and Response (MDR) is a proactive cybersecurity service that provides continuous monitoring, threat detection, and incident response. It combines human expertise with advanced technologies to identify and mitigate cyber threats in real-time.

XENSHIELD with Defender XDR:

- **Microsoft Defender XDR:** Offers a unified security platform integrating multiple layers of protection across endpoints, email, identities, and cloud environments.
- **Unified Visibility:** Provides a comprehensive view of threats and vulnerabilities across the organization, enabling a proactive response.
- **Automated Response:** Allows for automated actions to contain threats swiftly and efficiently, reducing manual intervention.

Why XENSHIELD Matters:

- **Rapid Threat Response:** Addresses threats in real-time, reducing the dwell time of attackers within the network.
- **Expertise and Resources:** Access to skilled security analysts and cutting-edge tools for comprehensive threat management.
- **Scalability and Flexibility:** Adaptable services that can scale with the evolving security landscape and organizational needs.

Key Tasks of XENSHIELD:

- **Continuous Monitoring:** 24/7 surveillance of Computer & Mobiles, Networks Devices, IoT Devices, and cloud environments to detect anomalies and potential threats.
- **Threat Detection:** Team utilizes advanced analytics, AI, and threat intelligence to identify suspicious activities and potential security breaches.
- **Incident Response:** Swift and coordinated action to contain and remediate security incidents, minimizing impact and preventing further damage.
- **Forensics and Analysis:** Investigates incidents to understand the attack vectors, methodologies, and potential weaknesses for future prevention.

Team Composition

- ✓Highly skilled security analysts with 20+ Azure Certifications
- ✓Azure Sentinel Analyst
- ✓Threat hunters
- ✓Incident responders
- ✓Automation Specialists
- ✓Dedicated Team Leads and Managers

Key Capabilities

- ✓Real-time Threat Detection:
- ✓Advanced analytics and AI-driven insights
- ✓Rapid incident triage and investigation
- ✓Playbook-driven response for consistency
- ✓Threat Hunting, Proactive searching for hidden threats
- ✓Identify vulnerabilities before they're exploited.
- ✓Customized tailored solutions for unique business needs
- ✓24/7 Availability to Emphasize the round-the-clock monitoring and response.

xencia

Success Story - SOC Lite MDR (Managed Detection and Response)

Client Profile

A US Based state-chartered Savings Bank which is one of the largest Maine-based with 54 branches across the state. The Bank has roughly $7.4 billion in assets. The customer is looking for Security Operations Centers (SOCs) for security, resilience, and compliance of their operational product host environment.

Business Challenges

- A pilot environment to test host their products & services required necessary security controls and protection
- Round the clock observation and quick response to incidents were mandated to minimize attack spreads
- Compliance to various base security protocols are mandatory for their products host environment and ensure there are no unknown vulnerabilities

Solution

- **Threat Detection and Monitoring**: For Bank we are providing a Managed proactive SOC service delivering 24x7 coverage.
- **Incident Response and Remediation:** Our SOC experts configure Microsoft 365 Defender to your environment, help to define detection and prevention policies, and continuously work with you to fine-tune your deployment as new risks are identified
- Defender Experts for Hunting are a proactive threat hunting service for Microsoft Defender XDR.
- We have enabled Defender for Cloud with Plan 2 Subscription and Implemented Endpoint protection, Vulnerability assessment, Agentless scanning for all the servers and integrated these services Defender for 365 (XDR).

Additional Enablement for Bank Services

- Vulnerability Assessment
- Agentless Scanning
- Suggestions on Security Remediations to Improve the Secure Score.

xencia

Thank You

INDIA
#432, 2nd Floor, 7th Main,
80 Feet Road,
1st Block, HRBR Layout,
Kalyan Nagar, Bengaluru – 560043
P: +91-80-40954277

India
M32, #173, 6th Floor, Block B, Tecci Park , OMR, Sholinganallur,
Chennai 600119.

USA
2300 Lakeview Parkway,
Suite 700, Alpharetta,
Georgia - 30009
United States
P: +1 920 5580089

SINGAPORE
51 Changi Business Park,
Central 2,
#04-05, The Signature
Singapore – 486066
P: +65 90272617

www.xencia.com

xencia
Unlocking Infinite Possibilities