Azure Security Deployment

Cambay Solutions
Accelerating Digital Transformation

Microsoft Managed Partner

Whether your organization is considering the cloud or mid-way through migration or running complex applications & workloads in the cloud, you need to have complete visibility into your overall security and governance posture.

Implement **Azure Security Center and Azure Sentinel** with Cambay's solution templates to defend against threats and cyber-attacks while increasing your overall security posture.

Solutions

Azure Security Center (ASC) is an advanced, unified security management system that strengthens the security posture of data centers and threat protection for hybrid cloud workloads. ASC enables customers to gain insight into their security state across hybrid workloads, reduce exposure to cyberattacks, and respond to detected threats quickly.

Azure Sentinel, a cloud-native security information and event manager (SIEM) platform, provides integrated security management powered by AI. Azure Sentinel delivers intelligent security analytics and threat intelligence, providing alert detection, threat visibility, proactive hunting, and threat response.

Why Cambay

- Microsoft Managed Partner and Gold Competencies in Collaboration & Content and Cloud Productivity.
- Helping enterprises create digital experiences for employees that unite enterprises.
- Trusted digital workplace partner for several leading enterprises

Cambay's Azure Security Deployment – Scope

Cambay can have Azure Security Center enabled in your subscription, and then you can start ingesting the security alerts generated by ASC. Alerts can then be filtered and debugged on their way to Azure Sentinel for long-term storage, providing a richer set of threat detections.

Week 1 - Azure Security Center

- Configuration of 1 production environment (single tenant).

Week 2 - Azure Sentinel

- Configure 1 production environment.
- Review & initial setup for up to 2 data connectors - Azure Security Center and Syslog.

Week 3 - Analysis, Onboarding and Validation

- Analysis of the deployment model for ASC and on-premises servers, including connectivity and testing before pushing to production.
- Onboarding for up to 10 server agents – Minimum 5 Windows servers & 5 Linux Servers, with OS versions supported by select agents.
- Validate and activate a dashboard to visualize patch management.
- Onboarding of up to 4 Azure Cloud Services/Apps Services

Week 4 - Review & validation

- Analysis & review of available Analytics Rules (enable) with customization of up to 4 rules.
- Creation of up to 2 playbook notifications.
- Validate & generate up to 2 hunting queries.
- Validate and activate up to 4 workbooks for data displaying.

Week 5 - Security Policy

- Definition of a security policy for a max of 1 subscription.
- Resource security hygiene.

Week 6 - Working Sessions

- 2 working sessions to analyze ASC findings & recommendations.
- Up to 2 transfer knowledge & architectural sessions.