Service Name: SYNERGY ADVISORS - Azure Sentinel & Security Center (ASC)- Deployment v1.0

Categories: Security/Implementation

Gold competencies:

- Security
- Cloud Platform
- Cloud Productivity
- Collaboration
- Datacenter
- Enterprise Mobility Management
- Messaging
- Application Development
- Project and Portfolio Management (Silver)

Solutions Areas: Security

Industries:

- Financial Services
- Healthcare
- Media & Communications
- Manufacturing and energy
- Government
- Retail and consumer goods
- Others

Overview

Microsoft Azure Sentinel is a cloud native SIEM (Security Information Event Management) and Security Orchestration Automated Response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing alert detection, threat visibility, proactive hunting, and threat response.

Azure Security Center (ASC) is a security management tool that enables companies to gain insight into their security state across hybrid cloud workloads, reduce possible exposure to cyberattacks, and respond to detected threats quickly.

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

NOTE: Azure Security Center generates alerts according to, and based on, different resource types in your environment.

Synergy Advisors' Azure Sentinel & Security Center (ASC) - Deployment v1.0 helps your organization accelerate the implementation timelines of Azure Sentinel and Azure Security Center, thus reducing possible attacks and risk and increasing your security posture, with the help of our team of expert consultants and architects.
In today's data-driven world, information security is paramount for companies of all industries. Without proper security, data breaches can occur, resulting in costly financial and critical data loss, as well as leaks in private customer information.

Deployment Scope & Activities

Microsoft Azure Sentinel & Azure Security Center Deployment

- **Azure Sentinel**
  - Configure 1 production environment **(Single Log Analytics Workspace)**
  - Workloads
    - **Data Connectors**
      - Review & initial setup for up to 2 data connectors
        - Azure Security Center Connector
        - Syslog Connector
    - **Analytics**
      - Analysis & review of available Analytics Rules (enable) with customization of up to 4 rules
      - Creation of up to 2 playbook notifications
      - Validate and generate up to 2 hunting queries
      - Validate and activate up to 4 workbooks for data displaying
- **Azure Security Center**
  - Configuration of 1 production environment **(Single tenant)**
  - Workloads
    - **Deployment**
      - Analysis of the deployment model for Azure Security Center and on-premises servers, including connectivity and testing before full deployment into production
      - Onboarding for up to 10 server agents. (Azure servers or on-premises with direct internet connectivity)
        - A minimum of 5 Windows servers, with the Operating System versions supported by the agent (EventViewer log monitoring configuration and equipment IIS logs)
        - A minimum of 5 Linux Servers, with the versions of the Operating System supported by the agent

- Validate and activate a dashboard to visualize patch management

- Onboarding of up to 4 Azure Cloud Services/Apps Services

- **Security Policies**
  - Definition of a security policy for a maximum of 1 subscription
- **Resource Security Hygiene**
  - 2 working sessions to analyze ASC findings and recommendations
  - Up to 2 transfer knowledge and architectural sessions (2 hours each)

- **Document Deliverables**
  - General configuration document (playbooks, queries, rules generated during deployment) with screenshots
  - Basic configuration document (screenshots) of Azure Sentinel (Playbooks, Queries, Rules generated during deployment)
  - Basic configuration document (screenshots) of Azure Security Center (Security Policy generated during deployment

- **Document Deliverables**
  - Design guides
  - Step by step guides
  - Training material

Out of Scope Activities

Anything not listed in the above **"Deployment Scope Activities"** section is considered out of scope for this **" Azure Sentinel & Azure Security Center - Deployment "** engagement, including the following:

- Configuration of pre-requisites
- Required licensing of Microsoft and Azure solutions
- Configuration of peripheral communication devices and permissions
- Setup of network communications permissions
- Third-party products integration
- Formal training
- Integration with third party products.
- Review or assessment of other Azure subscriptions
- Remediation plan of vulnerabilities or findings
- Operating systems configurations, beyond the required installation of the agents

NOTE: Synergy may present to the customer a paid contract or SoW with all the activities associated scoped for evaluation and customer acceptance. It may not cover all the customer's activities and needs. For additional scenarios, Synergy Advisors will present a

separate offer or would adjust a paid agreement that can be accepted or rejected by the customer without penalties. Synergy Advisors will not generate any invoice to customers that is not supported by a previously signed paid contract or SoW.

Pricing Variability
Pricing variations based on the following:

- Time & Material
- On-premises architectures
- Customer's change management processes
- Maturity of client's security environment
- Travel requirements have an impact on the total project amount
- Others

Requirements
Customer may meet with:

- Licensing requirements
- Browser requirements
- Hardware & software requirements

*Full list of requirements would be presented in a SOW or a formal agreement for acceptance and acknowledgment.