ATAIS - Engagement Delivery Guide



Advanced Threat Analytics Implementation Services

14-Sep-17

Version

Prepared by

**Author**

Contributors

**Add Contributors to Doc Properties**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 0.1 | Initial draft for review/discussion |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 6](#_Toc454533592)

[1.1 Overview 6](#_Toc454533593)

[1.2 Response 6](#_Toc454533594)

[1.3 Who Should Read This Guide 7](#_Toc454533595)

[1.4 How to Use This Guide? 7](#_Toc454533596)

[2 Assumptions 8](#_Toc454533597)

[3 Offering Goals 8](#_Toc454533598)

[4 Bill of Materials 9](#_Toc454533599)

[5 Project Manager 10](#_Toc454533600)

[5.1 Delivery Management 10](#_Toc454533601)

[5.1.1 Pre-Engagement 10](#_Toc454533602)

[5.1.2 Engagement Delivery 10](#_Toc454533603)

[6 Experience Requirements 14](#_Toc454533604)

[6.1 Project Manager Experience Requirements 14](#_Toc454533605)

[6.2 Consultant Experience Requirements 15](#_Toc454533606)

[7 Business Scenario Addressed 17](#_Toc454533607)

[8 Key Tasks Addressed 17](#_Toc454533608)

[9 Project Approach, Timeline and Service Deliverables 18](#_Toc454533609)

[9.1 Approach 18](#_Toc454533610)

[9.2 Timeline 19](#_Toc454533611)

[9.3 Deliverables 19](#_Toc454533612)

[9.4 Work Breakdown Structure – Framework 21](#_Toc454533613)

List of Tables

[Table 1: Bill of Materials - Delivery 9](#_Toc454533614)

[Table 2: Envision 11](#_Toc454533615)

[Table 3: Engagement Deliverables 19](#_Toc454533616)

List of Figures

[Figure 1: MSF Phases and Milestones 18](#_Toc454533617)

1. Introducción
   1. Descripción General

Hoy día, el tópico de ciberseguridad se ha desplazado desde TI y el datacenter a los niveles más altos de decisión. Los ataques y amenazas han crecido siendo substancialmente más sofisticados en frecuencia y severidad

¿Qué está en juego? Todo, desde la privacidad del cliente hasta la identidad de la marca, la reputación de los ejecutivos y más aún. Sin la instalación de un sistema fuerte de defensa, las identidades y el banco de cuentas de individuos pueden ser hackeadas, los negocios pueden perder clientes y las compañías pueden perder el control de los acuerdos comerciales, propiedad intelectual, su ventaja competitiva e incluso su posición en el mercado de valores.

* El porcentaje de tiempo que los atacantes permanecen en la red antes de su detección es sobre **200 días**.
* El costo estimado de cibercrimen a la economía global es de **$500 billones**.
* **Sobre el 75%** de todas las intrusiones de red son seguidas de compromiso de credenciales.
* El costo promedio de una brecha de datos a una compañía es de **$3.5 millones**.

El Servicio de Implementación de Advanced Threat Analytics (ATAIS) es una iniciativa que dura 3 semanas donde los Servicios de Microsoft entregarán una visión, plan, diseño e implementación de ATA como una plataforma de Análisis de Comportamiento de Usuarios y Entidades (UEBA).

Esta plataforma de análisis de comportamiento es una solución de detección pura que ayuda a los clientes a identificar indicadores de amenazas y compromisos. ATA trata de eliminar los puntos ciegos del comportamiento de usuarios y entidades mediante la detección. Los atacantes toman ventaja de esos puntos ciegos para optimizar sus técnicas de implementación y técnicas de ataque para poder tomar el control de recursos, extracción de información o simplemente destruir sistemas.

* 1. Respuesta

Nosotros nos alineamos al framework de ciberseguridad donde tomamos en cuenta los elementos principales de Identificar, Proteger, detectar, Responder y Recuperar.

* **Identificar** – Identificación de los activos de mayor valor.
* **Proteger** – Protección de los activos de mayor valor.
* **Detectar** – La estrategia de detección efectiva para los activos de mayor valor.
* **Respuesta** – Como planear táctica y estratégicamente un plan de respuesta de ciberseguridad.
* **Recuperar** – Como ejecutar una recuperación táctica y estratégicamente basándose en el plan de respuesta.

Esta iniciativa se enfoca principalmente en la detección y como el cliente responderá a las amenazas detectadas por ATA y actuar sobre ellas.

Esta iniciativa trabaja en conjunto con un plan de respuesta efectivo y probado de propiedad del cliente. ATA no es una solución de protección distinta a entregar telemetría o detección de datos para responder y actuar sobre los hallazgos. Es una solución de detección altamente efectiva, El objetivo de esta iniciativa es enfocarse sobre la detección de indicadores de amenazas descubiertos por ATA y como responder a ellos como parte de una estrategia mayor. El plan de respuesta total para el ambiente del cliente no está dentro del alcance de esta iniciativa.

La respuesta sobre esas amenazas descubierta serán claves y discutidas con mayor detalle en esta iniciativa. (Ver Plan de Respuesta-ATAIS)

* 1. ¿Quién Debería Leer esta Guía?

Este documento está diseñado para asistir a o a los expertos en seguridad y Engagement Managers responsables de entregar ATAIS. Este documento también asistirá a los Engagement Managers para entender como esta iniciativa está construida y que está disponible para usar antes, durante y después de la iniciativa.

* 1. ¿Cómo usar esta guía?
* Este documento ayudará a o a los expertos en seguridad a asegurarles que tengan un entendimiento de todos los entregables que son requeridos como parte de esta iniciativa de Microsoft Services, como también para entregar una base de habilidades necesarios para implementar exitosamente esta iniciativa.
* Esta iniciativa tiene como objetivo hacer que la visión e implementación de ATA en un ambiente de cliente sea una experiencia más predecible y dejar al cliente con un conocimiento de valor en el entendimiento de la tecnología y procesos requeridos para usar la solución confiadamente.
* Los objetivos de la iniciativa son:
  + Ayudar a los clientes a construir un proceso bien pensado sobre las respuestas efectivas referentes a las detecciones de ATA.
  + Ayudar al cliente a entender el panorama moderno de amenazas que ATA detectará y mostrará.
  + Ayudar al cliente a entender el valor que ATA entregará a su completa estrategia de detección de amenazas.
  + Generar la arquitectura y la instalación de ATA en su ambiente.
* Esta Guía de Entrega de Consultores está diseñada para entregar una guía para el experto en seguridad, para que sea capaz de entregar in a solución usando el enfoque estructurado que ha sido usado en terreno para entregar exitosamente iniciativas similares.

1. Supuestos

Esa guía de Pre-Entrega hace los siguientes supuestos:

* El proceso de desarrollo del negocio ya ha sucedido. Si no, consulte la Pricing and Scoping Guide para información de precio y la plantilla del Statement of Work (SOW) para una descripción detallada del ámbito y objetivos de la iniciativa.
* El cliente cumple con los requerimientos/restricciones de la iniciativa y solución.
* Los consultores cumplen o exceden los requerimientos de experiencia y conocimiento detallado en la Sección 5, “Requerimientos de Experiencia del Consultor”.
* Los consultores entregarán retroalimentación al equipo de la iniciativa para mejorar toda la calidad de este material después que una iniciativa se ha ejecutado.
* El cliente puede cumplir los requerimientos de hardware/software y configuraciones de red indicadas en el documento de Visión y Alcance.

1. Objetivos de la Iniciativa

* Informar a los Clientes sobre la importancia de la seguridad y como Microsoft se enfoca en la seguridad.
* Obtener un mejor entendimiento de los objetivos del cliente y la visión para el futuro perteneciente a su estrategia de detección.
* Guiar al cliente para optimizar su plan de respuesta, entendiendo lo que la solución detecta.
* Implementar Microsoft Advanced Threat Analytics como un servicio de detección de amenazas para los clientes.

1. Lista de Materiales

Tabla : Lista de Materiales - Entrega

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre | Descripción | Tipo | Fase |
| ATAIS-Presentación de Kick-Off de la iniciativa | Guía de Kick-Off de la iniciativa | Presentación PowerPoint | Visión |
| ATAIS-Taller de Educación |  | Presentación PowerPoint | Visión |
| ATAIS-Taller de Visión |  | Presentación PowerPoint | Visión |
| ATAIS-Visión y Alcance | Acuerdo de Visión y Alcance de la iniciativa | Documento Word | Visión |
| ATAIS-Ejercicio de Respuesta a Incidentes de Seguridad (1 y 2) | Usada para ayudar al cliente a aprender y validar su plan de respuesta para responder a incidentes de seguridad. | Presentación PowerPoint | Planificación |
| ATAIS-Taller de Plan de Respuesta |  | Presentación PowerPoint | Planificación |
| ATAIS-Plantilla de Plan de Respuesta | Una guía detallada de plan de respuesta de qué hacer si es descubierta una amenaza. | Documento Word | Planificación |
| ATAIS-Taller de Diseño |  | Presentación PowerPoint | Planificación |
| ATAIS-Diseño de la Solución | Diseño detallado de la solución | Documento Word | Planificación |
| ATAIS-Guía de Implementación | Guía de Implementación de la solución | Documento Word | Construcción |
| ATAIS-Casos de Prueba | Escenarios de casos de Prueba verificados y aceptados | Documento Word | Estabilización |
| ATAIS-Guía de Operaciones | Como operar la solución una vez implementada | Documento Word | Estabilización |
| ATAIS-Presentación de Cierre de la Iniciativa | Guía de cierre de la iniciativa | Presentación PowerPoint | Deploy |

1. Project Manager
   1. Administración de la Entrega

La entrega de esta iniciativa sigue los estándares de la metodología de entre MSF and se espera que un Project Manager esté involucrado en un mínimo de 10% del tiempo total de la iniciativa (4 horas por semana)

* + 1. Pre-Iniciativa

Antes de poner un pie en el cliente e iniciar esta iniciativa, los siguientes pasos se deben completar:

* Hacer que el profesional o profesionales de entrega revisen la *Engagement Delivery Guide*.
* Asegurarse que el profesional o profesionales entiendan el modelo de entrega y los procesos que son usados para la entrega de la iniciativa.
* Hacer todo lo posible para asegurar que el cliente incluya los roles recomendados en la SOW como parte del proyecto. Su participación, mientras se explique claramente en el SOW, es crucial en la educacional, plan de respuesta, diseño de la solución e implementación de esta solución.
* Agendar las reuniones de kick-off con el cliente y asegurarse que ellos tienen que pre agendar todas las sesiones con el personal apropiado y acomodaciones para el número de personas en cada sesión.
  + 1. Entrega de la Iniciativa
       1. Visión

Esta iniciativa comienza con un kick-off y taller de visión (día uno), progresa a través de la entrega de las sesiones de talleres educacionales y se completa con la documentación de un documento de Visión y Alcance.

Durante esta fase, será importante asegurar que el cliente tiene las salas apropiadas para las sesiones de los talleres de educación y que en esas salas alcancen para el número de personas. También es posible que el personal requerido para cada sesión sea diferente. Utilice la siguiente guía para ayudar a determinar quién debería asistir a cada sesión:

Tabla : Visión

| Título del Taller | Audiencia Sugerida | Duración |
| --- | --- | --- |
| Entendimiento del Framework de Ciberseguridad | Equipo líder y cualquier miembro que tendrá un rol en el proceso del plan de respuesta que será definido. | 4 horas |
| Resumen y Revisión Técnica en Profundidad de Advanced Threat Analytics | Equipo líder y profesionales TI quienes necesitan tener un alto entendimiento de lo que entrega Microsoft Advanced Threat Analytics a la organización. | 4 horas |
| Escenarios de Robos de Credenciales | Profesionales TI quienes serán responsables de administrar y operar la Implementación de ATA, incluyendo al personal que estará incluido en los aspectos técnicos del plan de respuesta. | 4 horas |
| Taller de Visión de ATAIS | Profesionales TI quienes serán responsables de administrar y operar la Implementación de ATA, incluyendo al personal que estará incluido en los aspectos técnicos del plan de respuesta. | 2 horas |

Después que los talleres de educación y visión se hayan completado, el equipo de entrega será documentado en el documento de Visión y Alcance. Este documento será entregado al cliente para revisión y una reunión de revisión se llevará a cabo para capturar cualquier retroalimentación del cliente. Una vez que el cliente haya entregado sus comentarios, la versión final del documento de Visión y Alcance será enviado al cliente para su firma y aprobación.

* + - 1. Planificación

La fase de planificación estará enfocada en tres áreas principales; Plan de Respuesta, Diseño de la Solución y Planificación de Pruebas. La siguiente guía le ayudará a la entrega de cada una de las áreas de estas fases

* + - * 1. Planificación de Respuesta

Los talleres de planificación de respuesta y los ejercicios de respuesta a incidentes de seguridad son entendidos para ayudar al cliente a través de:

* Examinar los procesos del lciente para responder a eventos relacionados con ATA usando sus procesos de respuesta en un escenario controlado, basado en una sala de clases.
* Identificar los equipos y recursos que serán incluidos en el plan de repuesta y una definición de sus responsabilidades (RACI)
* Definir los eventos que ATA puede detectar y establecer una clasificación de riesgo para cada evento.
* Definición del plan de respuesta específico para cada evento de ATA.
* Definición de un plan de comunicación (este puede diferir dependiendo de la clasificación de riesgo del evento)

**Nota:** La plantilla del Plan de Respuesta de ATA entrega un listado de todos los eventos que ATA puede detectar, la definición del evento y la severidad que el producto le asocia al evento. Estos se usarán para ayudar al cliente a definir correctamente el evento para su entorno, pero las definiciones deben ser claras para el cliente. La clasificación de riesgo es el proceso en el cual la organización determina la importancia y significancia de las posibles amenazas a su negocio y sólo el cliente puede definir esto.

Nuestro equipo facilitará cada sesión de taller llevándolos a través de lo que significa definir el equipo, procesos, respuestas y planes de comunicación y usará un enfoque estructurado para ayudar a acomodar esto. Por favor, asegurar que el personal adecuado esté entre los asistentes para completar esta actividad. Cuando cada taller se complete, las decisiones se deben haber realizado y/o los procesos deben haber sido definidos. Estos deberían ser transferidos inmediatamente al documento de Plan de Respuesta de ATA que se entrega en los materiales de la iniciativa.

* + - * 1. Diseño de la Solución

La porción de diseño de la solución de esta iniciativa se enfoca sobre decidir que tipo de implementación de ATA es requerida para cumplir la solución dentro del alcance del cliente y los requerimientos detallados en el documento de Visión y Alcance.

El propósito de las sesiones de diseño es:

* Determinar cuántas instalaciones de ATA Center son requeridas.
* Determinar qué tipo y cuántos sistemas ATA Gateway son necesarios (Lightweight Gateway vs. Standard Gateway).
* Identificar hardware o máquinas virtuales necesarias para cada sistema ATA.
* Si se utilizará un ATA Gateway estándar, discutir port mirroring con el equipo de red.

Como resultado de las sesiones de diseño, el cliente debería tener toda la información necesaria para construir el sistema operativo base para la instalación de ATA. El equipo de entrega documentará esto en el documento de Diseño de la Solución.

* + - * 1. Planificación de Pruebas

Las actividades de planificación de pruebas para la implementación y pruebas de sistema de ATA deberían tomar un tiempo mínimo y estarán enfocadas sobre la validación que ATA está funcionando y es capaz de capturar el tráfico desde y hacia los controladores de dominio que están monitoreando. La oferta de ATAIS entrega una plantilla de Plan de Pruebas con los elementos comunes que requieren validación y pruebas para todas las implementaciones.

* + - 1. Construcción

Durante la fase de construcción, el equipo construirá todos los aspectos de la solución. Es importante que todos los sistemas requeridos, incluyendo el SO base y la implementación de la imagen, sean completados por el cliente antes de iniciar esta fase. El ámbito entregado incluye tiempo para validar los prerrequisitos para validar las configuraciones antes de instalar e implementar ATA. Use este tiempo para asegurarse que todo esté listo para instalar.

Una vez que los prerrequisitos hayan sido validados, la instalación de ATA será completada en la Fase de Implementación.

Si el cliente elige implementar ATA dentro de un ambiente de laboratorio antes de la implementación en producción, esto debería ser completado en la Fase de Construcción de esta iniciativa.

* + - 1. Estabilización

Esta fase incluye actividades de Pruebas de Sistemas. Este proceso incluye seguir todos los casos indicados en el documento de Plan de Pruebas y guarda los resultados de las pruebas en el documento de Plan de Pruebas que fue acordado en la fase de Planificación de este proyecto.

Al final de esta fase, entregaremos al cliente una Guía de Operaciones la que provee la información operacional para administrar ATA en el futuro. Por favor, hay que considerar que esta guía no incluye procesos de respuesta. Esos elementos están indicados en el Plan de Respuesta de ATA.

* + - 1. Implementación

La fase de implementación incluye todas las actividades necesarias para entregar la solución como se indicó en el plan y la especificación. Para el hito “Implementación Completada” de esta fase, la solución implementada debería ser entregada de acorde a la expectativa de valor de negocio para el cliente y el equipo debería haber concluido efectivamente las actividades necesarias para alcanzar este objetivo. El cliente debe estar de acuerdo que el equipo cumpla con los objetivos antes que pueda cerrarse el proyecto. Esto requiere una solución estable, como también criterios de éxito claramente enunciados.

Esta iniciativa también considera dentro del alcance un mínimo de ocho horas de asistencia por implementación. Durante este tiempo, el cliente es responsable de entregar cualquier cosa que ATA descubra para nuestra atención para que podamos asistirlo determinando si el elemento detectado es un incidente actual o un potencial falso-positivo mientras las mejoras de configuración pueden ser necesarias para ajustar la configuración de ATA para remover las detecciones de falsos-positivos. Es importante notar que la identificación de un incidente es responsabilidad del cliente. Nosotros entregaremos guía y asistencia sobre cuáles deberían ser los cambios a la configuración que permitirán mitigar los hallazgos de falsos-positivos.

Cualquier cambio hecho a la configuración para mitigar las detecciones de falsos-positivos deberían ser actualizadas en le documento de Diseño de la Solución y compartida con el cliente

1. Experience Requirements
   1. Project Manager Experience Requirements

The ATAIS Project Manager needs to comply to the following solution elements in order to ensure successful deployment of this engagement.

* A Project Manager should be familiar with the Enterprise Mobility Suite (EMS) SKU offered by Microsoft.
* A Project Manager should be familiar with the Cybersecurity Framework Core elements of Protect, Detect, Respond.
* A Project Manager should have attended the sales/marketing training for ATA to understand the basics of the solution and its value.
* A Project Manager should have a basic understanding of cybersecurity response.

**Pre-engagement**

* Ensure that the consultant / architect is familiar with the solution.
* Ensure that the WBS has been received that accompanies the SOW. You can use the WBS as a baseline project plan.
* Ensure that Project Manager has read and understands the response document as part of this offering.

**During-engagement**

* Ensure that clear Conditions of Satisfaction (CoS) is agreed during the kick-off and envisioning phase.
* Ensure that clear assumptions and acceptance criteria are agreed upon during the Envisioning phase.
* Ensure the customer understands the importance of a response plan.
* During the deployment of ATA in the customer production environment, ATA can start detecting threats immediately. Some threats can take some time to learn (up to 30 days).
* Do not try and remediate discoveries of ATA as part of this engagement. Follow the response process outlined by this offering.
* During this time, be prepared to answer customers’ questions and receive escalations from the Consultant \ Architect for certain detections that could cause uncomfortable situations with the customer.
* Update the project plan at the reach of each milestone agreed with the customer.

**Post-Engagement**

* Communicate all concerns and questions of the customer to the account team.
* Ensure the customer understands the threats and how to respond to them effectively.
* Some threats could require special response teams to engage with separate contractual agreements from the customer. These teams could be from Microsoft or 3rd party. The customer can opt to resolve the threats themselves.
  1. Consultant Experience Requirements

The ATAIS is delivered by two key skillsets:

* Cyber/Security skills for the design of the technology solution
* IT Service Management (ITSM) skills to define the appropriate incident response plans and actions

These skillsets can exist in one adequately qualified resource, or two resources can be leveraged. Given that activities for each skillset stream likely will involve different customer resources (e.g., technical team for design and deploy, ITSM/Security team for response definition), both streams can run in parallel – thereby reducing the total length of the engagement (not the work needed) down from the recommended three (3) weeks.

The ATAIS Consultant(s) \ Architect(s) needs to comply to the following solution elements in order to ensure successful deployment of this engagement.

Optimal candidate profile will include:

Cyber/Security portion:

* A Consultant \ Architect who has delivered Advanced Threat Analytics engagements before or has extensive knowledge of the solution
* A Consultant \ Architect who has extensive knowledge of Port Mirroring configurations and using NetMon 3.4.

**Note:** Do not install Message Analyzer, Wireshark, or other network capture software on the ATA Gateway. If you need to capture network traffic, install and use Microsoft Network Monitor 3.4.

* A Consultant \ Architect who understands the threat landscape that ATA detects against.
  + Read and understand the Pass-the-Hash whitepapers v1 and v2. - <http://www.microsoft.com/en-us/download/details.aspx?id=36036>
  + Forged PAC (Privilege Attribute Certificate)

Microsoft Security Bulletin MS14-068 – Critical

<https://technet.microsoft.com/en-us/library/security/ms14-068.aspx>

<https://support.microsoft.com/en-us/kb/3011780>

* + DNS Reconnaissance
  + Brute Force Attacks
  + Skeleton Key Malware
  + Remote Code Execution

ITSM portion:

* A Consultant \ Architect who has or is familiar with an IT Infrastructure Library (ITIL) Expert certification.
* A Consultant \ Architect from an existing ITSM services practice that is dedicated to ITSM services for Microsoft customers (e.g., ITSM consultants, ITSM PFE resources).
* Experience with incident and problem management response processes, particularly around security and cyber response.

For both portions, all Consultants \ Architects should be familiar with the Cybersecurity Framework Core elements of Protect, Detect, Response.

Formal ATAIS training may be completed on-demand via the Involve platform [here](https://www.msinvolve.com/msi-core/DirOD/71708.aspx).

**Pre-engagement**

* Ensure that the customer can accommodate the port mirroring requirements to the domain controllers if implementing a full ATA Gateway.
* Ensure that the hardware requirements in the Statement of Work has been identified by the customer and has been allocated for this engagement.
* Ensure that [KB3047154](https://support.microsoft.com/en-us/kb/3047154) is not installed on the virtualization host. This is highly unlikely but worth the due diligence. This will may cause port mirroring to stop working properly.
* The solution requires more 2 or more domain controllers, even in a test environment.

**During-engagement**

* During the deployment of ATA in the customer production environment, ATA can start detecting threats immediately. Some threats can take some time to learn (up to 30 days).
* Ensure that the Consultant \ Architect has read and understands the response document as part of this offering.
* Do not try and remediate discoveries of ATA as part of this engagement. Follow the response process outlined by this offering. Notify your engagement manager of customer concerns during this time.

**Post-Engagement**

* Communicate all concerns and questions of the customer to the account team and the engagement manager.
* Ensure the customer understands the threats and how to respond to them effectively.
* Some threats could require special response teams to engage with separate contractual agreements from the customer. These teams could be from Microsoft or 3rd party. The customer can opt to resolve the threats themselves.

1. Business Scenario Addressed

The objective of this engagement is to address the enterprise’s unique threat detection needs. It is imperative that you understand the customer goals and challenges. These will vary based on many factors but some common areas that customers require assistance on may include:

* Understanding today’s modern threat landscape.
* Guidance on how to improve their response processes.
* What are the unique cybersecurity configuration and solutions the customer has available to address their mitigation needs? This could be new solutions or offerings from Services or the customer could be already licensed for.

1. Key Tasks Addressed

The key tasks of the Advanced Threat Analytics Implementation Services offering are to:

* Understand organizational goals to use ATA as a technology to provide insight into indicators of threat and compromise.
* Uncover the current state of “assume breach”
* Educate the customer on what the modern threats are designed to do and what adversaries are trying to achieve.
* Provide guidance on how to align their response processes to effectively respond to threats. This will be done my means of a ATA specific response plan.
* Provide the architecture, design and implementation of the ATA solution with the customer. Please review the scoping and pricing guide for details.

1. Project Approach, Timeline and Service Deliverables
   1. Approach

Microsoft Services leverages the Microsoft Solutions Framework (MSF) to execute this project, a five-phase project approach that has been executed across multiple engagements of various project types and sizes.

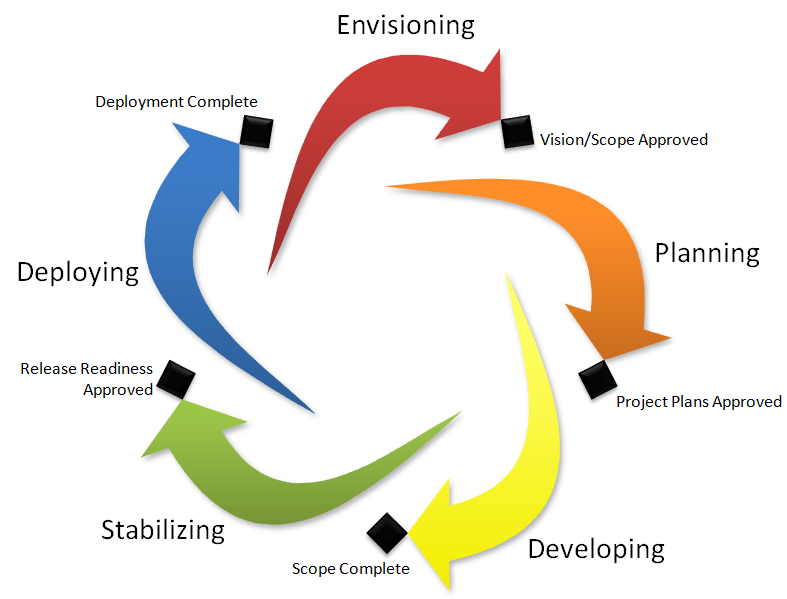


Figure : MSF Phases and Milestones

The project will be managed through structured project phases using phase-gate milestones and deliverables to mark the approved completion of each phase prior to moving on to the next phase. This project will follow all MSF project phases.

* 1. Timeline

The recommended timeline is available as part of the Work Breakdown Structure project plan that accompanies this offering bill of materials. The timeline based on the WBS is 15 days or 3-weeks of work. During the pricing and scoping of the solution, be sure to reference the pricing and scoping guide for additional scoping and price impact considerations.

* 1. Deliverables

The following is a list of the key project Service Deliverables that will be produced within this engagement.

Table : Engagement Deliverables

| Project phase | Service deliverable name | Service deliverable descriptions | Acceptance criteria |
| --- | --- | --- | --- |
| Envision | Vision and Scope | A Microsoft Word document that contains a description of the customer’s situation and needs, the boundary of the solution defined though the range of features and functions, the solutions design strategies that will form the starting point used to create the customer’s solution. Designs at this stage will be conceptual in nature to provide input to development of the Solutions Design. This document includes the project vision, all agreed-upon requirements, and a solution design approach. | Document accurately reflects the scope of the work to be performed, requirements of the solution and an expected solution design strategy that will be built upon during the Plan phase. |
| Plan | ATA Response Plan | The ATA Response Plan is a Microsoft Word document which provides information about the roles and responsibilities for responding to events ATA identifies. It also includes event identification and risk classifications and response and communications processes. | Document accurately reflects the response plan for events that ATA may detect. |
| Plan | Solutions Design | Description of the technical functionalities in a document according to the agreed format defined in the template (Exhibit n) of this SOW | Document accurately reflects in-scope requirements gathered. |
| Plan | Draft Test Plan | Describes the strategy and approach used to plan, organize, and manage the project’s testing activities. It identifies testing objectives, methodologies and tools, expected results, responsibilities, and resource requirements. The Test Plan document details all test cases for the solution and is provided in draft format until the test cases have been completed and documented. | Document accurately and completely reflects all test cases that need to be validated for system functionality. |
| Build | Implementation Guide | Includes step-by-step instructions for the deployment of Advanced Threat Analytics into a production environment. | Document provides step-by-step instructions for implementing the in-scope solution. |
| Build | Advanced Threat Analytics System Testing | The completion of all test cases as identified in the Test Plan document and according to the in-scope solution. | Successful System Testing. |
| Build | Final Test Plan | The Test Plan, in final format, includes all test results and notes for executing each defined test case in the document. | Document contains complete test results, including failures, and all test cases result in an eventual successful execution. |
| Stabilize | Operations Guide | The Operations Guide provides details surrounding how to operate and manage the Advanced Threat Analytics systems. | Document contains operational information specific to the operations and management of the Advanced Threat Analytics deployment.  This document does not contain information or processes specific to responding to a detected event. Those items are documented within the “ATA Response Plan” document. |

* 1. Work Breakdown Structure – Framework

