Engagement Delivery Guide



Advanced Threat Analytics Implementation Services

29-Jun-16

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. Introduction
   1. Overview

Today, the topic of cybersecurity has moved from IT and the datacenter to the highest levels of the boardroom. Attacks and threats have grown substantially more sophisticated in frequency and severity.

What’s at stake? Everything from customer privacy to brand identity, executive’s reputations and beyond. Without a strong defense system in place, the identities and bank accounts of individuals can be hacked, businesses stand to lose customers, and companies can lose control of trade secrets, intellectual property, their competitive edge, and even their standing in the stock market.

* Average time attackers stay in a network before detection is over **200 days**
* Estimated cost of cybercrime to the global economy is **$500 billion**
* **Over 75%** of all network intrusions are traced back to compromised credentials
* Average cost of a data breach to a company is **$3.5 million**

The Advanced Threat Analytics Implementation Services (ATAIS) is a 3-week engagement where Microsoft Services will envision, plan, design and implement ATA as a User and Entity Behavioral Analytics (UEBA) platform.

This behavioral analytics platform is a pure detection solution that helps customers identify indicators of threat and compromise. ATA tries to eliminate the environmental user and entity behavior blind spot by means of detection. Attackers take advantage of these blind spots to streamline their malware dropping and attack techniques in order to gain control of resources, exfiltration information or simply destroy systems.

* 1. Response

We align to the Cybersecurity framework where we look at the core elements of Identify, Protect, Detect, Response and Recovery.

* **Identify** – Identification of high-valued assets
* **Protect** – Protection of the high-valued assets
* **Detect** – Effective detection strategy against the high-value assets
* **Response** – How to tactically and strategically plan a cybersecurity response.
* **Recover** – How to tactically and strategically execute a recovery based on the response plan.

This engagement focusses on the detection core and how the customer will respond to the threats detected by ATA and act on them.

This offering works in conjunction with an effective and tested response plan owned by the customer. ATA is not a protection solution other than providing telemetry or detection data to respond to and act upon. It’s a highly effective detection solution. The objective of this offering is to focus on the detection of indicators of threat discovered by ATA and how to respond to them as part of a bigger strategy. The holistic response plan for the customer environment is not in the scope of this offering.

The response on these threat discoveries will be key and is discussed in more detail in this offering. (See ATAIS-Response Plan)

* 1. Who Should Read This Guide

This document is designed to assist the security expert(s) and engagement managers responsible for delivering the ATAIS. This document will also assist Engagement Managers to understand how the offering is built and what is available for use before, during and after the engagement.

* 1. How to Use This Guide?
* This document will help the security expert(s) ensure they have an understanding of all deliverables that are required as part of this Microsoft Services offering, as well as provide a baseline set of skills necessary to successfully implement this offering.
* This offering aims to make envisioning and implementing ATA in a customer environment a more predictable experience, and leaving the customer with valuable knowledge in understanding the technology and process required to use the solution with confidence.
* The goals for the ATAIS offering are to:
  + Help customers build a thought process on effective response initiative with regards to ATA detections.
  + Help the customer understand the modern threat landscape that ATA will detect and display.
  + Help the customer understand the value ATA will bring to their overall threat detection strategy.
  + Architect and deploy ATA in their environment.
* This Consultant Delivery Guide is intended to provide guidance to you as the security expert, to be able to deliver the solution using the structured approach that has been used in the field to successfully deliver similar engagements.

1. Assumptions

This Pre-Engagement Guide makes the following assumptions:

* The business development process has already happened. If not, consult the Pricing and Scoping Guide for pricing information and the Statement of Work (SOW) template for a detailed description of the scope and goals of the engagement.
* The customer will meet the engagement and solution requirements/restrictions.
* The consultants will meet or exceed the experience and knowledge requirements provided in Section 5, “Consultant Experience Requirements.”
* The consultants will provide feedback to the offering team to improve the overall quality of this material after an engagement has taken place.
* The customer can meet the hardware/software requirements and network configurations outlined in the Vision and Scope document.

1. Offering Goals

* Inform Customers on the importance of security and how Microsoft approaches security
* Gain a better understanding of customer goals and vision for the future pertaining to their detection strategy.
* Guide the customer to optimize their response plan by understanding what the solution detects.
* Deploy Microsoft Advanced Threat Analytics as a threat detection service for customers.

1. Bill of Materials

Table : Bill of Materials - Delivery

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Description | Type | Phase |
| ATAIS-Engagement Kick-Off Presentation | Engagement kick-off Guide | PowerPoint Presentation | Envision |
| ATAIS-Education Workshop |  | PowerPoint Presentation | Envision |
| ATAIS Envisioning Workshop |  | PowerPoint Presentation | Envision |
| ATAIS-Vision Scope | Engagement Vision and Scope agreement | Word Document | Envision |
| ATAIS Security Incident Response Tabletop Exercise (1 and 2) | Used to help the customer learn about, and validate their response plan for, responding to security incidents. | PowerPoint Presentation | Plan |
| ATAIS-Response Planning Workshop |  | PowerPoint Presentation | Plan |
| ATAIS-Response Plan Template | A response plan guide outlining the process of what to do if a serious threat is discovered. | Word Document | Plan |
| ATAIS-Design Workshop |  | PowerPoint Presentation | Plan |
| ATAIS-Solutions Design | Detailed Solutions Design | Word Document | Plan |
| ATAIS-Implementation Guide | Implementation Guide of the solution | Word Document | Build |
| ATAIS-Test Case | Test case scenarios verified and accepted | Word Document | Stabilize |
| ATAIS-Operations Guide | How to operate the solution once implemented | Word Document | Stabilize |
| ATAIS-Engagement Close-out Presentation | Engagement Close-out Guide | PowerPoint Presentation | Deploy |

1. Project Manager
   1. Delivery Management

The delivery of this engagement follows standard MSF delivery methodologies and it is expected that a Project Manager will be involved at a minimum, 10% of the total time of the engagement (4 hours per week).

* + 1. Pre-Engagement

Prior to stepping foot onsite with the customer and kicking off this engagement, the following steps must be completed:

* Have your delivery professional or professionals review the *Engagement Delivery Guide*.
* Make sure that your delivery professional or professionals understand the delivery model and processes that are used for the engagement delivery.
* Do your best to ensure that the customer includes the recommended roles in the SOW as a part of your project. Their participation, while explained clearly in the SOW, is crucial to the educational, response planning, solutions design and deployment of this solution.
* Schedule the kickoff meeting with the customer, and make sure that they have prescheduled all educational workshop sessions with appropriate personnel and accommodations for the number of people in each session.
  + 1. Engagement Delivery
       1. Envision

This engagement begins with a kickoff and envisioning workshops (day one), progresses through the delivery of the education workshop sessions and completes with the documentation of a Vision and Scope document.

During this phase, it will be important that you ensure the customer has appropriate rooms for the education workshop sessions and that the rooms identified can hold the appropriate number of people. It’s also possible that the required personnel for each session may differ. Use the following guidance to help determine who should attend which session:

Table : Envision

| Workshop Title | Suggested Attendees | Duration |
| --- | --- | --- |
| Understanding of the Cybersecurity Framework | Leadership team and any member who will a role in the response plan process that will be defined. | 4 hours |
| Advanced Threat Analytics Overview and Technical Deep Dive | Leadership and IT Professionals who need to have a high-level understanding of what Microsoft Advanced Threat Analytics provides the organization. | 4 hours |
| Credential Theft Scenarios | IT professionals who will be responsible for managing and operating the ATA deployment including personnel who will be included in the technical aspect of the response process. | 4 hours |
| ATAIS Envisioning Workshop | IT professionals who will be responsible for managing and operating the ATA deployment including personnel who will be included in the technical aspect of the response process. | 2 hours |

After the education and envisioning workshops have completed, the delivery team will document the Vision and Scope document. This document will be delivered to the customer for review and a review meeting will be held to capture any customer feedback. Once feedback has been integrated, the final Vision and Scope document deliverable will be delivered to the customer for sign-off and approval.

* + - 1. Plan

The Plan phase of the engagement focuses on three key areas; Response Planning, Solution Design and Test Planning. The following guidance will help you through each of the areas of this phase.

* + - * 1. Response Planning

The response planning workshops and security incident response tabletop exercises are intended to help guide the customer through:

* Examine the customer’s processes for responding to ATA-related events using their current response processes in a controlled, classroom-based scenario
* Identifying the teams and resources which should be included in the response plan and a definition of their responsibilities (RACI)
* Defining events that ATA may detect and establishing an organizational risk classification for each event.
* Definition of the response plan specific to each ATA event
* Definition of a communication plan (this may differ depending on the risk classification of the event)

**Note:** The ATA Response Plan template provides a listing of all events that ATA may detect, the definition of the event and the severity that the product associates to the event. These will be used to help the customer properly define the event for their environment but the definitions need to be clear to the customer. Risk classification is the process in which the organization determines the importance and significance of the possible threat to their business and only the customer can define this.

Our team will facilitate each workshop session by leading them through what it means to define the team, processes, responses and communication plans and will use a structured approach to help accommodate this. Please make sure all appropriate personnel are in attendance to complete this activity. As each workshop completes, decisions should have been made and/or processes should have been defined. These should be immediately transferred into the ATA Response Plan template document provided with the offering materials.

* + - * 1. Solutions Design

The solution design portion of the engagement focuses on deciding what type of ATA deployment is required to meet the customers in-scope solution and the requirements outlined in the Vision and Scope document.

The purpose of the design sessions is to:

* Determine how many ATA Center deployments are required
* Determine what type and how many ATA Gateway systems are needed (Lightweight Gateway vs. Standard Gateway)
* Identify hardware or virtual machine needs for each ATA system
* If using a standard ATA Gateway, discuss port mirroring with the network team

As a result of the design sessions, the customer should have all the information needed to build the base server operating systems for the deployment of ATA. The delivery team will document this in the Solutions Design document.

* + - * 1. Test Planning

Test planning activities for the deployment and system testing of ATA should take minimal time as it focuses on validating that ATA is functional and able to capture traffic to and from the domain controllers that it is monitoring. The ATAIS offering provides a Test Plan template with the common items which require validation and testing for all deployments.

* + - 1. Build

During the Build phase, the team constructs all aspects of the solution. It is important that all required systems, including base OS and image deployment, be completed by the customer prior to starting this phase. The scope provided includes time to validate pre-requisite configurations before installing and deploying ATA. Use this time to make sure everything is ready for deployment.

Once pre-requisites have been validated, the installation of ATA may be completed in the Deploy Phase.

If the customer chooses to deploy ATA into a test lab environment prior to production deployment, this should be completed in the Build Phase of the engagement.

* + - 1. Stabilize

This phase includes System Testing activities. This process includes following all test cases listed in the Test Plan document and recording the test results in the Test Plan document template that was agreed upon in the Plan phase of this project.

At the end of this phase, we will provide the customer with an Operations Guide which provides them with operational information for managing ATA moving forward. Please note that this guide does not include response processes. Those items are listed in the ATA Response Plan.

* + - 1. Deploy

The Deploy phase includes all the activities needed to deliver the solution as indicated by the specification and plan. By the "Deployment Complete" milestone in this phase, the deployed solution should be providing the expected business value to the customer, and the team should have effectively concluded the activities needed to reach this goal. The customer must agree that the team has met its objectives before it can close out the project. This requires a stable solution, as well as clearly stated success criteria.

This engagement has also been scoped to include a minimum of eight hours of tuning assistance. During this time, the customer is responsible for bringing anything that ATA discovers to our attention so we may assist them with determining if the detected item is an actual issue or a potential false-positive entry where configuration enhancements may be necessary to adjust the ATA configuration to remove false-positive detections. It’s important to note that the identification of the issue is the customer’s responsibility. We provide guidance and assistance should there be configuration changes which will help mitigate the false-positive finding.

Any configuration changes made to mitigate false-positive detections should be updated in the Solutions Design document and shared with the customer.

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.

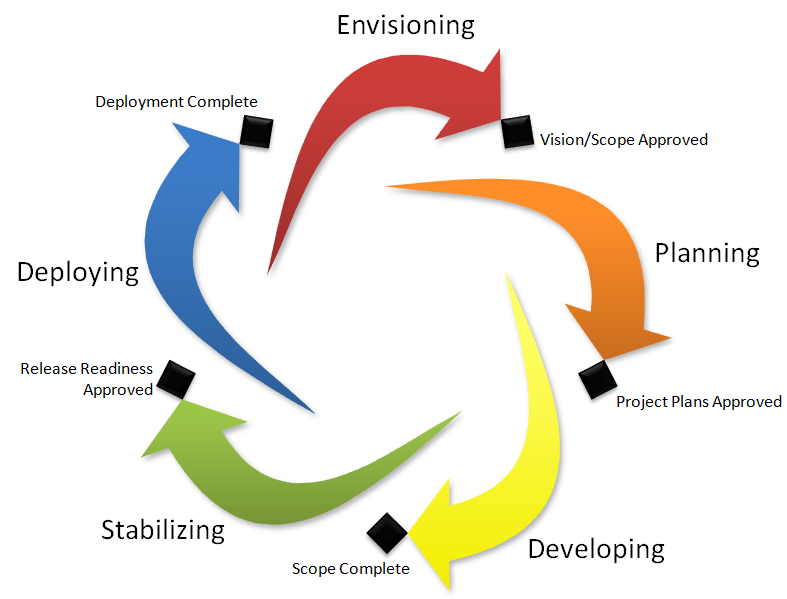


Figure : MSF Phases and Milestones

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

