Vision and Scope



Advanced Threat Analytics Implementation Services

Prepared for

[Type Customer Name Here]

3/9/2018

Version 0.1 Draft

Prepared by

**[Update Author in Doc Properties]**

Contributors

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 Problem statement 8](#_Toc507589769)

[2 Business opportunity 9](#_Toc507589770)

[2.1 Opportunity statement 9](#_Toc507589771)

[3 Project vision and scope 11](#_Toc507589772)

[3.1 Vision statement 11](#_Toc507589773)

[3.2 Benefits analysis 11](#_Toc507589774)

[3.3 Requirements 13](#_Toc507589775)

[3.3.1 Business requirements 14](#_Toc507589776)

[3.3.2 User requirements 14](#_Toc507589777)

[3.3.3 Operational requirements 15](#_Toc507589778)

[3.3.4 System requirements 15](#_Toc507589779)

[3.3.5 Security requirements 16](#_Toc507589780)

[3.4 Scope of project 17](#_Toc507589781)

[3.4.1 Solution components in scope 18](#_Toc507589782)

[3.4.2 Out-of-scope Solution components 22](#_Toc507589783)

[3.5 Constraints 23](#_Toc507589784)

[3.6 Objectives 24](#_Toc507589785)

[3.6.1 Business objectives 24](#_Toc507589786)

[3.6.2 Technical objectives 25](#_Toc507589787)

[3.7 Deliverables 25](#_Toc507589788)

[3.8 Production deployment criteria 26](#_Toc507589789)

[3.9 Operational criteria 27](#_Toc507589790)

Table of Tables

[Table 1: Business requirements 14](#_Toc507589791)

[Table 2: User requirements 14](#_Toc507589792)

[Table 3: Operational requirements 15](#_Toc507589793)

[Table 4: System requirements 16](#_Toc507589794)

[Table 5: Security requirements 16](#_Toc507589795)

[Table 6: In-scope Solution components 22](#_Toc507589796)

[Table 7: Solution components: Out of scope 22](#_Toc507589797)

[Table 8: Constraints 24](#_Toc507589798)

[Table 9: Engagement deliverables 25](#_Toc507589799)

[Table 10: Acceptance criteria 27](#_Toc507589800)

[Table 11: Operational criteria 28](#_Toc507589801)

**Spell/grammar check is turned ON within all Services Delivery Method (SDM) Word templates.** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar red mark-ups. To turn this feature off, do the following:

1. Click **File**.
2. Click **Options** on the left.
3. Click **Proofing**.
4. Scroll to the bottom and check the following boxes:



**To remove all the Visible Guidance (hot pink text with gray background) all at once:**

1. Press **Ctrl-H** and, in the **Find and Replace** dialog box, place the cursor is in the **Find what** box.
2. In the bottom left, click **More**.
3. On the **Format** menu, in the bottom left, click **Style**.
4. In the **Find Style** dialog box, scroll down to the bottom and click **Visible Guidance**, and then click **OK**.
5. In the **Find and Replace** dialog box, make sure the **Replace with** box is empty.
6. Click **Replace All**.
7. If not empty, click **Format**, click **Style**, select **(no style)**, click **OK**, and then click **Replace all** again.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

**Save as PDF** and send the PDF version to the customer.   
~ OR ~

Inspect the document and **remove comments, revisions, any document properties** you do not want included, personal information, and hidden text. For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

**Template Guidance**

**Description:** The Vision/Scope document represents the ideas and decisions developed during the Envisioning phase. The goal of the phase, represented by the content of the documentation, is to achieve team and customer agreement on the desired Solution and overall project direction (i.e., project goals, constraints, etc.)

The Vision/Scope document is organized into three main sections:

**Business Opportunity**: A description of the customer’s situation and needs

**Scope:** The boundary of the Solution defined though the range of features and functions that can be accomplished within project constraints; what is out of scope, a release strategy and the criteria by which the Solution will be accepted by users and operations.

**Solution Design Strategies:** The architectural and technical designs used to create the customer’s Solution within the project constraints

**Note:** In this template, you must enter specific project information in certain placeholder areas. To view the fields containing these placeholders:

1. Click on **File** and, in the left pane, click **Options**.
2. In the left pane, click **Advanced** and, in the **Advanced** pane, scroll down to the **Show document content** section.
3. In the **Field shading** menu, click **Always**.
4. Click **OK**.

Throughout the template, look for shaded text. Where shaded text appears, click the field and follow instructions.

Depending on the complexity of the project, not all of the sections might be filled out, or some sections might be cut back significantly.

**Justification:** Vision/Scope documentation is usually written at the strategic level of detail and is used during the Planning phase as the context for developing more detailed technical specifications and project management plans. It provides clear direction for the project team; outlines explicit, up-front discussion of project goals, priorities and constraints; and sets customer expectations.

**Team Role Primary:** Product Management is the key driver of the Envisioning phase and is responsible for facilitating the team to the Vision/Scope approved milestone. Product Management defines the customer needs and business opportunity, or problem addressed by the solution.

**Team Role Secondary:** Program Management is responsible for articulating the Solution Concept, Goals, Objectives, Assumptions, Constraints, Scope and Solution Design Strategies sections of this document.

1. Problem statement

**Guidelines for a Problem Statement**

**Purpose:** Provides the business description of the customer’s situation, outlining the motivation for the project

**Responsibility:** Product Management

**Length:** Less than one page, ideally a paragraph

**Guidelines:** Stay at a high level, use clear business language; address why you want to do it and what you want to do; look at known issues

Cyberattacks Both targeted and broadly distributed attacks, aim for credential theft attacks leveraging stolen user accounts from users and administrators to gain access to organizations’ environments and to perform attacks from the inside. This makes it even more difficult to detect attacks. Microsoft’s Identity Security and Protection team has seen a 300 percent increase in a user accounts attacked over the past year (2017). [[1]](#footnote-2)After web-app attacks, cyber espionage attacks were the most common in 2017 according to 2017 Data Breach Investigations Report, Edition 10.[[2]](#footnote-3)

In today’s constantly evolving threat landscape, not only threat protection, but threat detection is becoming ever more important.

Without a strong detection system, effective safeguarding, and response plan process controls in place, several things might occur. The identities of individuals might be compromised, businesses might lose customers as a result of reputational damage, and companies might lose control of trade secrets and intellectual property—they might even lose their competitive edge in the market.

Attackers have been shown to reside within a network an average of 140 days before they are detected. In the vast majority of attacks, attackers compromise user credentials, and they are increasingly using legitimate IT tools rather than malware.

In today’s modern IT environment, recognizing the following threat elements[[3]](#footnote-4) is imperative for your organization:

* Before being detected, attackers on average, stay in a network more than **140 days** undetected.
* Cybercrime costs the global economy an estimated **$500 billion**.
* **Over 60%** of all network intrusions are traced back to compromised credentials.
* A data breach costs a company an average of **$3.8 million.**

1. Business opportunity

In this section, write a statement of the customer’s situation, expressed in business language rather than technical terms. This section should demonstrate Microsoft’s understanding of the customer’s current environment and its desired future state. This information is the overall context for the project.

Staying current with cyber security is a challenge. Advanced Threat Analytics (ATA) evolves continually and is updated with state-of-the-art cybersecurity protection that keeps pace with modern attacks. Using information from multiple data-sources and leveraging machine learning to learn the behavior of users and other entities in an organization, abnormal behavior is identified, and attacks detected. Any suspicious activity is displayed in user friendly dashboard helping to react fast and efficiently to potential attacks.

With Advanced Threat Analytics, [Type Customer Name Here] gains a sensor to any suspicious activities involving the organizations domain controllers.

As a result of this engagement, [Type Customer Name Here] has the opportunity to be educated on the latest threat landscape that Microsoft Advanced Threat Analytics (ATA) detects against and how to build an effective plan to respond to the threat indicators ATA discovers. This engagement also focuses on the architecture and deployment of ATA within [Type Customer Name Here]’s enterprise to complement and further enhance their detection strategy.

* 1. Opportunity statement

Describe the customer’s current situation that creates the need for the project. You may include a statement of the customer’s opportunity and the impact of capitalizing on that opportunity (product innovation, revenue enhancement, cost avoidance, operational streamlining, and leveraging knowledge). You may also include a statement of the customer’s problem/situation and the impact of solving the problem or how the Solution will create business value (revenue protection, cost reduction, regulatory compliance, alignment of strategy and technology). Include a statement that connects the customer’s opportunity/problem to the relevant business strategy and drivers. Write the Opportunity Statement concisely using a business executive’s voice.

**Justification:** The Opportunity Statement demonstrates that Microsoft understands the customer’s situation from the business point of view and provides the project team and other readers with the strategic context for the remaining sections.

ATA might provide a simpler and faster way for [Type Customer Name Here] to understand what is happening within their network by identifying suspicious activity through using User and Entity Behavior Analytics (UEBA), and providing clear and relevant threat information on a simple attack timeline.

This Solution focuses on the detection core and how [Type Customer Name Here] will respond to the threats ATA detects. Having an effective response plan for the threat indicators will prepare [Type Customer Name Here] to respond appropriately based on the severity of the discovered threat. It will also help [Type Customer Name Here] prioritize threats based on an understanding of the threats as a result of the response planning exercise that is part of this engagement.

1. Project vision and scope
   1. Vision statement

**Guidelines for a Vision Statement**

**Purpose:** Establish the long-term vision and provide design-making content. Provide unbounded view of the Solution.

**Responsibility:** Product Management

**Length:** One paragraph or even a sentence fragment.

**Guidelines:** Balance all the interests to arrive at a single vision statement; surface enterprise architecture implications early.

Clearly and concisely, describe the future desired state of the customer’s environment once the project is complete. This can be a restatement of the opportunity; however, it is written as if the future state has already been achieved. This statement provides a context for decision-making. It should be motivational to the project team and the customer.

**Justification:** A shared vision statement among all team members helps help make sure that the Solution meets the intended goals. A solid vision builds trust and cohesion among team members, clarifies perspective, improves focus, and facilitates decision-making.

ATA prepares [Type Customer Name Here] to detect threats that are malicious activities targeted at Active Directory Domain Services (Active Directory (AD) DS) credentials. This project’s vision is to implement threat-detection capabilities, to identify threats posed against user and entity credentials, and prepare the organization to effectively respond to the threats ATA identifies.

Microsoft will assist [Type Customer Name Here] in achieving this vision by educating, preparing, designing, and implementing the ATA Solution.

* 1. Benefits analysis

Describe how the customer will derive value from the proposed Solution. Connect the business goals and objectives to the specific performance expectations realized from the project. These performance expectations should be expressed numerically. This section could be presented using the following subsections:

1. Business Goals and Objectives
2. Business Metrics
3. Business Assumptions and Constraints
4. Benefits Statement

**Justification:** Benefits Analysis demonstrates that Microsoft sufficiently understands the customer’s situation. It also defines the customer’s business needs, which may provide vital information for making Solution/technology recommendations. Modify this section or elaborate if you feel this information is not suitable for your customer.

ATA automatically analyzes, learns, and identifies abnormal authentication behavior on your network—alerting you to possible indicators of compromise. Microsoft Services will implement a well-thought-out design of the Solution and [Type Customer Name Here] will have the confidence to understand the severity of the indicators ATA produces and can respond appropriately.

During this engagement, the following potential benefits can be gained:

**Instruction:** Use the following text if you are delivering ATA version 1.8:

**Discovery of abnormal user behavior:** Using behavioral analytics and leveraging machine learning, ATA will uncover questionable activities and abnormal behavior in users and devices, such as anomalous logins, unknown threats, password sharing, lateral movement, and modification of sensitive groups.

**Identification of malicious attacks:** ATA detects known malicious attacks almost instantly, including Pass the Ticket, Pass the Hash, Overpass the Hash, forged PAC (Microsoft Security Bulletin 14-068), Golden Ticket, Skeleton Key malware, malicious replications, reconnaissance, brute force, and remote execution.

**Identification of security issues and risks:** ATA identifies security issues and risks, including such as Broken Trust, weak protocols and known protocol vulnerabilities.

**Instruction:** Use the following text if you are delivering ATA version 1.9:

**Discovery of abnormal user behavior:** Using behavioral analytics and leveraging machine learning, ATA will uncover questionable activities and abnormal behavior in users and devices, such as anomalous logins, unknown threats, password sharing, lateral movement, and modification of sensitive groups.

**Identification of malicious attacks:** ATA detects known malicious attacks almost instantly, including Pass the Ticket, Pass the Hash, Overpass the Hash, Privilege escalation using forged authorization data, Golden Ticket, Skeleton Key malware, malicious replications, malicious service crations, reconnaissance, brute force, and remote execution.

**Identification of security issues and risks:** ATA identifies security issues and risks, including such as weak protocols and known protocol vulnerabilities.

**Delivering a sensible design and thoughtful implementation:** By following the Microsoft Solutions Framework (MSF), Microsoft Services prepares a more secure, well-thought-out design and implementation.

**Understanding and responding to attacker behaviors:** The Advanced Threat Analytics Implementation Services (ATAIS) methodology will educate you on the specific threats ATA detects and how to appropriately respond to them—allowing you to make more informed decisions on mitigations and develop your long-term threat-detection strategy.

**Development and integration of ATA-specific response planning:** Microsoft Services will help you understand the suspicious indicators discovered by ATA, the necessary response actions, and how to integrate them into your existing response plan.

* 1. Requirements

Identify what the Solution must do. These requirements can be expressed in terms of functionality (for example, a registration website Solution will allow the users to register for events, arrange for lodging, and so on) and the rules or parameters that apply to that functionality (for example, the user can register only once and must stay in lodging approved by the travel department). Requirements exist at both the user level and the organizational level. Note the [Requirements Document](https://spsites.microsoft.com/sites/bizdesk/SDMPlus/SDM%20TemplateDL/RequirementsDocument.docx) is also available if a separate document is needed to document requirements. This is often the case in projects with larger scopes and greater complexity. For smaller projects, this Vision Scope document will likely suffice and this document can be considered optional.

**Justification:** User and organizational requirements are the key input to developing product scope and design strategies. Requirements are the bridge between the usage analysis and Solution description. A complete Statement of Requirements demonstrates that Microsoft understands its customer’s needs. The statement also becomes the baseline for more detailed technical documentation in the Planning phase. Good requirements analysis lowers the risk of downstream surprises.

BR = Business Requirement

UR = User Requirements

OR = Operational Requirements

TR = Technical Requirement, which is where all ATA requirements would be

SR = Security Requirements

The following section outlines the requirements of the envisioned Solution to be deployed as part of this engagement.

* + 1. Business requirements

Business requirements define the needs of the organization with regard to the Solution. They define what the Solution must deliver to capitalize on a business opportunity or to manage business challenges. Modify the section below.

This engagement’s business requirements address the enterprise’s unique threat-detection needs. It is imperative that [Type Customer Name Here] understands their goals and challenges. These will vary based on many factors, but some common areas that [Type Customer Name Here] might require include:

**Instructions:** Increase the identification codes as you continue to add requirements for future tracking. The following have been provided as an example. **Please add rows and update or change to your needs.**

Table 1: Business requirements

| Identification Code | Requirement |
| --- | --- |
| BR1 | Improve existing response plan processes. |
| BR2 | Activate a more robust threat-detection strategy. |
| BR3 | The Solution must pose minimum risk to the environment and the operational well-being of the business. |
| BR4 | Microsoft needs to review and provide input for [Type Customer Name Here]’s current response plan related to ATA detections. |

* + 1. User requirements

User requirements address individual or groups of users. These have a special focus on information delivery mechanisms (for example, dashboards, reports, ad-hoc navigation). Modify this section based on your customer requirements.

The following table describes user requirements that must be considered during all phases of the engagement.

**Instructions:** Increase the identification codes as you continue to add requirements for future tracking. The following have been provided as an example. Please add rows and update or change to your needs.

Table 2: User requirements

| Identification Code | Requirement |
| --- | --- |
| UR1 | [Type Customer Name Here] will identify administrators of the Solution. |
|  |  |
|  |  |

* + 1. Operational requirements

Provide an overview of the needs for the Solution from the perspective of operations and IT, that is, to make sure that the Solution can be deployed and operated successfully alongside other systems. Operational requirements describe the qualities of service that must be supported, such as security, performance, and availability. Elaborate in the section and tables below.

The following table describes the operational requirements that must be considered during all phases of the engagement.

**Instructions:** Increase the identification codes as you continue to add requirements for future tracking. The following have been provided as an example. Please add rows and update or change to your needs.

Table 3: Operational requirements

| Identification Code | Requirement |
| --- | --- |
| OR1 |  |
| OR2 | Clear backup guidance needs to form part of the operational excellence of the Solution. |
| OR3 | Microsoft needs to provide clear deployment guidance so [Type Customer Name Here] can reinstall the Solution, if necessary. |
| OR4 | During the engagement, operational guidance will be given to [Type Customer Name Here] before, during and after the installation of ATA making sure the Solution is working as expected.  Microsoft will provide an operations guide detailing tasks which have to be performed after the solution is up and running. |
| OR5 | [Type Customer Name Here] will identify responsibilities for the different roles for operating the Solution. |

* + 1. System requirements

The following table describes the system requirements that must be considered during all phases of the engagement.

**Instructions:** Increase the identification codes as you continue to add requirements for future tracking. The following have been provided as an example. Please add rows and update or change to your needs.

Where there are options, select the appropriate text and delete the non-relevant option.

Table 4: System requirements

| Identification Code | Requirement |
| --- | --- |
| SR1 | Option 1: The system will to be deployed on a virtualized platform.  Option 2: The system will to be deployed on a physical platform. |
| SR2 | Make adequate storage available based on the technical design strategy envisioned. |
| SR3 | Make adequate hardware specifications available based on the technical design strategy envisioned. |
| SR4 | Option 1 (Lightweight Gateway): The Solution will be deployed using minimal hardware taking an agent-based approach where possible.  Option 2 (port-mirrored gateway): The Solution will be deployed in a manner which does not add additional compute resources to existing systems.  Option 3 (combination Lightweight Gateway and Port Mirrored Gateways): Where possible, the Solution will be deployed with minimal costs and impact to existing systems. |

* + 1. Security requirements

Identifying the security requirements is the first step to help ensure the security of the proposed Solution. The security requirements can be used to direct the following subsequent security activities:

Focus on what to look for in the Threat Modeling activity.

Focus on what to concentrate on for the Security Code Review and Inspection.

What areas to be aware of when doing the Secure Deployment activity.

What concerns may have to be addressed in the Security Response Plan.

The primary architect and Security SME should use the security requirements section of the Security Architecture document to state the Solution’s security requirements.

The following table describes the security requirements that must be considered during all phases of the engagement.

Table 5: Security requirements

| Identification Code | Requirement |
| --- | --- |
| SECR1 | The education workshops will prepare [Type Customer Name Here] to understand the specific threat indicators ATA discovers. |
| SECR2 | The response plan and workshops will help [Type Customer Name Here] to understand, identify, and prioritize the threat indicators and respond to these threats appropriately. |
| SECR3 | Communications to the administration portal should be encrypted. |
| SECR4 | Communications between the Center and the Gateway should be encrypted. |
| SECR5 | Option (port-mirrored gateway deployment): Where possible, the detection service should remain invisible (hidden) from potential attackers in a way that the detection service does not show up as a running agent on any end-state system. |

* 1. Scope of project

Guidelines for a Scope Statement

**Purpose:** Map reality against the vision and establish what the customer deems to be essential for success that can be accomplished within the project’s constraints. Shift less essential features into future releases.

**Responsibility:** Program Management

**Length:** As succinct as possible (one to two pages).

**Guidelines:** Be SMART (Specific, Measurable, Achievable, Results-based, Time-oriented). Clearly state what is out of scope.

Place a boundary around the Solution by detailing the range of features and functions, by defining what is out of scope (what will not be part of the project or not being completed by Microsoft Services; be as specific as possible and don’t assume that something is understood), and by discussing the criteria by which the Solution will be accepted by users and operations. The scope clearly delineates what stakeholders expect the Solution to do, thus making it a basis for defining project scope and for performing many types of project and operations planning.

**Instructions:** Replace these with the appropriate items as listed within the “Objectives” and “Services Areas within Scope” sections located within the Statement of Work for your project. Make sure to adjust any in- or out-of-scope items based upon your Envisioning workshops. Note that all changes must go through the formal change-management process and must be approved to be contained within the Vision and Scope document.

The scope of this engagement consists of intake and review, envisioning, planning and developmental exercises, and analysis and interviews with functional area stakeholders. This culminates in the delivery of a cybersecurity implementation and execution roadmap that is tailored to [Type Customer Name Here]’s unique mission or business requirements and priorities.

The following section outlines the scope items of this engagement. Specifically, this engagement will provide an understanding of the threats that ATA can provide detection services for, assist with the creation of a response plan specific to the events that ATA might identify, and assist with the design and deployment of ATA to monitor for threats to [Type Customer Name Here]’s production AD DS environment.

* + 1. Solution components in scope

Review this scope section with care. Elaborate more on or remove the elements mentioned below.

Instructions: You may update this from the actual statement of work for your project so you have the appropriate specifics.

The following items are regarded as in-scope when preparing to design and implement ATA to provide threat-detection services in [Type Customer Name Here]’s production AD DS environment. The scope items should align to that of the agreed Statement of Work (SOW) document.

The following table details the specific items to include to support this scope.

| Area | Description | Assumptions |
| --- | --- | --- |
| ATA Envisioning Workshop | Microsoft will conduct one (1) ATA envisioning workshop to discuss project requirements, objectives, confirms in scope and out of scope criteria, deliverables, acceptance and operational criteria, high level architectural and technical design strategies, and constraints. | Personnel who would be responsible for making decisions if ATA detects a threat must attend these sessions.  Personnel who will be responsible for designing, deploying, and operating ATA must attend these sessions. |
| ATA Vision and Scope | Microsoft will provide an ATA Vision and Scope document, written in Microsoft Word, that will reflect the details and decisions made during the ATA Envisioning Workshop. | The preliminary document will be shared with the customer during a review meeting, at which time feedback will be gathered. Microsoft will take this feedback and make agreed-upon updates to create a final version. |
| Educational Workshops | Microsoft will conduct two (2) educational workshops that will be focused on the following topic areas (one workshop per topic area):   * Credential Theft Scenarios Workshop * Advanced Threat Analytics Overview and Technical Deep Dive | Personnel who would be responsible for making decisions if ATA detects a threat must attend these sessions.  Personnel who will be responsible for designing, deploying, and operating ATA must attend these sessions. |
| ATA Response Planning Workshops | Microsoft will conduct four (4) workshops and up to two (2) tabletop incident response scenarios, during which Microsoft personnel will help build a response plan that is specific to events that ATA might identify. The workshops will cover the following topic areas (one workshop per topic area):   * Response Team Identification and Responsibility Definition * ATA Event Definition and Classification * ATA Event Handling and Response Process Definition * Organizational Communication Process Definition | Personnel who are responsible for the topic areas listed at left should attend the workshops. |
| ATA Response Plan | Microsoft will provide an ATA response plan document, written in Microsoft Word, that will reflect decisions that were made during the ATA response planning workshops. | The preliminary document will be shared with the customer during a review meeting, at which time feedback will be gathered. Microsoft will take this feedback and make agreed-upon updates to create a final version. |
| ATA Design Workshops | One design workshop is in scope. Consider adding additional design workshops if the in scope design includes multiple forests, or is overly large and complex.  Microsoft will lead one (1) design workshop that will be used to determine the specific ATA design that will be required to address the in-scope solution. | Personnel who will be responsible for designing, deploying, and operating ATA must attend these sessions. Decisions that will affect the final design will be made during the meetings. |
| Solution Design | Microsoft will provide a solution design document, written in Microsoft Word, that will detail the ATA design that will be deployed to meet the scope of this project. | The preliminary document will be shared with the customer during a review meeting, at which time feedback will be gathered. Microsoft will take this feedback and make agreed-upon updates to create a final version. |
| Test Planning Workshop | Microsoft will lead a single test planning workshop that will be used to define system testing cases and ATA configuration validation test cases. | Personnel who define test cases and processes must attend and provide input into the test planning process. |
| Test Plan | Microsoft will provide a test plan, written in Microsoft Word, that will detail necessary testing and validation procedures that will be used to validate the system functionality of ATA. | This document will be shared with the customer during a review meeting, at which time agreements will be made that the test cases will satisfy the validation of the deployed environment. This document will be in preliminary format until the test cases have been completed and test results have been documented in the test plan document. |
| Implementation Guide | Microsoft will provide an implementation guide, written in Microsoft Word, that details the steps required to install and configure ATA. | The preliminary document will be shared with the customer during a review meeting at which time feedback will be gathered. Microsoft will take this feedback and make agreed-upon updates to produce a final version. |
| Production Deployment of ATA | Update the following information based on the needs of your customer. Make sure this corresponds with what you have included in the ATDIS work breakdown structure (WBS) (Microsoft Project file) so it is scaled properly for your customer. Also, update the number of in-scope AD DS forests.  Microsoft will help the customer deploy **one ATA Center** and provide **up to eight (8) hours** of ATA Gateway deployment assistance designed to monitor:   * [Enter AD DS Forest FQDN Here] | Microsoft will help the customer deploy ATA into a production environment. |
| ATA Tuning | Microsoft will assist the customer with reviewing of events that were identified by ATA after installation **for up to eight (8) hours** and will help address any performance or detection issues that were identified during this time. | The customer will assign operational staff that will work side by side with the Microsoft team to review any events that ATA captures and to determine, follow up on, and address any performance issues as they occur. This assistance is **limited to eight (8) hours**. |
| Operations Guide | Microsoft will provide an operations guide, written in Microsoft Word, to provide basic guidance about maintaining ATA. | The preliminary document will be shared with the customer during a review meeting, at which time feedback will be gathered. Microsoft will take this feedback and make agreed-upon changes to create a final version. |

Table 6: In-scope Solution components

* + 1. Out-of-scope Solution components

Review this scope section with care. The customer must be responsible for configuring their SIEM Solutions. Elaborate more or remove on the elements mentioned below.

The following scope items are regarded as out of scope in preparing for, designing, and implementing ATA to provide threat-detection services for [Type Customer Name Here]’s production AD DS environment. The scope items should align to that of the agreed SOW document.

The following table details the specific items that will not be included to support this scope.

Table 7: Solution components: Out of scope

| Solution component | Description and considerations | Scope assumptions |
| --- | --- | --- |
| Response plan | Define a complete environmental response plan for [Type Customer Name Here]. Microsoft will provide only input into the existing response plan and process. | It is assumed that [Type Customer Name Here] has an existing plan for responding to ATA discovery elements; Microsoft can help improve this plan. |
| Product licensing | Licenses for Windows Server 2012 R2, or Windows Server 2016 (Datacenter or Standard edition) | [Type Customer Name Here] is responsible for obtaining all product licenses. |
| Public key infrastructure (PKI) deployment | A PKI Solution to deploy certificates. | [Type Customer Name Here] is responsible for all PKI requirements and issuing certificates. |
| Secure Sockets Layer (SSL) certificates | Issuing certificates from an internal PKI. Certificate requirements are outlined in the software requirements section of this document. (See software requirements for each ATA role.) | [Type Customer Name Here] is responsible for all SSL certificates required to deploy ATA. |
| Port mirroring | Configuring port mirroring. | If the use of a standard ATA Gateway is required, ATA requires that port mirroring be configured between the in-scope domain controllers (DCs) that will be monitored and the corresponding ATA Gateway. [Type Customer Name Here] is responsible for configuring port mirroring. |
| Security information and event management (SIEM) integration | Integration of SIEM information into ATA | Configuring ATA to pull information in from a SIEM solution will be out of scope for this engagement. [Type Customer Name Here] is responsible for following the integration guidelines for the supported SIEM solutions online. |

* 1. Constraints

**Guidelines for Documenting Constraints**

**Purpose:** Identify any business, project or technical constraints that will need to be considered in design of the Solution.

**Responsibility:** All

**Length:** As succinct as possible (one to two pages).

**Guidelines:** Identify those factors that will be critical to accurately designing the Solution for all team perspectives.

**Instructions:** As, or if, you have identified constraints for your delivery, use the following table to populate your list. These will be important to capture and illustrate, as they will serve as supporting material during your design sessions in the Planning phase. Your constraints might also result in risks that should be documented in a Risk Assessment Plan during your engagement.

Table 8: Constraints

| Identification code | Explanation |
| --- | --- |
| C1 | Windows Server 2008 or later DCs required. (2008 R2 is using an ATA Lightweight Gateway) |
| C2 | Physical versus virtual DCs will dictate where the Gateway servers will be located as part of the envisioned Solution and Solution design. |
| C3 | Stable network connection between the Gateway and the Center. See network requirements on the Gateway and Center. |
| C4 | Meet port-mirroring requirements to reach DCs in scope of this engagement. We recommend reaching all DCs for maximum threat discovery and detection capabilities. |
| C5 | Change controls for server implementations. |
| C6 | The internal PKI needs to issue a certificate to the ATA Center for the service communication, and ATA Console access. |

* 1. Objectives

See the preceding vision statement for the goal of this engagement. The vision statement provides context for decision-making during the later stages of this project when discussing features, cost, and delivery schedule. It is not provided to be a legally binding contract for the Solution. Any revisions of this document provide the detail scope of what will and will not be accomplished to meet the vision statement. The core features to be activated by the Solution can be characterized by the following specific goals and objectives.

* + 1. Business objectives

Describe the business objectives the customer is trying to achieve. Elaborate more on the elements mentioned below.

The business objectives of this engagement are to address the [Type Customer Name Here]’s unique threat detection needs with a Solution that will provide actionable telemetry. The Solution includes the following:

Implementing a threat-detection Solution that identifies and provides alerts on potential cybersecurity attacks against AD DS credentials.

Establishes a response plan for how the organization will respond to threats that the threat-detection Solution identifies.

Provides education about the common threats ATA detects and how to prioritize a response based on the threats discovered.

* + 1. Technical objectives

Describe the technical objectives the customer is trying to achieve. Elaborate more on the elements mentioned below.

This engagement will achieve the following outlined technical objectives:

* The ability to analyze data to and from the DCs by means of nonintrusive port mirroring.
* After ATA has performed for the required baseline learning period (30 days), any deviations to the baseline will be flagged as potential threat indicators.
* The Solution hardware and storage requirements will be configured to have maximum impact for effective detections.
  1. Deliverables

The following table lists the key project service deliverables for this engagement.

Table 9: Engagement deliverables

| Project phase | Service deliverable name | Service deliverable descriptions | Acceptance criteria |
| --- | --- | --- | --- |
| Envision | Vision and Scope | A document that includes the project vision, all agreed-on requirements, and a Solution design approach. | The document is delivered and accurately describes the elements as described in this table. |
| Plan | ATA Response Plan | A document that provides information about the roles and responsibilities for responding to events that ATA identifies. It also includes event identification, risk classifications, and response and communications processes. | The document is delivered and accurately describes the elements as described in this table. |
| Plan | Solution Design | A document that details the technical configuration of the Solution. | The document is delivered and accurately describes the elements as described in this table. |
| Build | Implementation Guide | A document that includes step-by-step instructions for deploying ATA into a production environment. | The document is delivered and accurately describes the elements as described in this table. |
| Build | ATA System Testing | The completion of all test cases as identified in the Test Plan document and according to the in-scope Solution. | The activity is performed accurately as described in this table. |
| Build | Test Plan | A document that includes all final test results and notes for completing each defined test case in the document. | The document is delivered and accurately describes the elements as described in this table. |
| Stabilize | Operations Guide | A document that details how to operate and manage the ATA system. | The document is delivered and accurately describes the elements as described in this table.  This document does not contain information or processes specific to responding to a detected event. Those items are documented in the ATA Response Plan. |
| Deployment | Implementation | Implementation of the Solution. | The deployment of the Solution per the agreed-on Solution Design document. |

* 1. Production deployment criteria

Define the metrics that must be met in order for the customer to understand that the Solution meets its requirements.

**Justification:** Acceptance criteria communicate to the project team the terms and conditions under which the customer will accept the Solution.

The following table describes the acceptance criteria for a successful engagement.

**Instructions:** Increase the identification codes as you continue to add requirements for future tracking. The following have been provided as an example. Please add rows and update or change to your needs.

Also, you may need to remove specific items if your scope has omitted anything. Read through them carefully to make sure they all apply to your delivery.

Table 10: Acceptance criteria

| Identification code | Requirement |
| --- | --- |
| PDC1 | ATA is successfully intercepting network traffic to and from the DCs. |
| PDC2 | ATA Gateways are successfully gathering entity information from the DCs. |
| PDC3 | [Type Customer Name Here] fully understands each of the threats for which ATA provides detection services. |
| PDC4 | An ATA Response Plan that accurately reflects the plan for events that ATA might detect. |
| PDC5 | [Type Customer Name Here] understands the ATA Response Plan and how to approach and prioritize threats ATA discovers. |
| PDC6 | Vision and Scope: A document that accurately reflects the scope of the work to be performed, requirements of the Solution, and an expected Solution design strategy that will be expanded on during the Plan phase. |
| PDC7 | Solution Design: A document that accurately records the configuration of the envisioned and deployed Solution. |
| PDC8 | Solution Test Plan: A document that accurately and completely reflects all test cases that need to be validated for system functionality. |
| PDC9 | Solution Implementation Guide: A document that provides step-by-step instructions for implementing the in-scope Solution of ATA components. |
| PDC10 | Solution Operations Guide: A document that contains operational information specific to operating and managing the ATA deployment. |
| PDC11 | Informal knowledge transfers during the engagement of ATA design, implementation, and testing elements. |

* 1. Operational criteria

Define the conditions and circumstances by which the customer’s operations team determines that the Solution is ready to deploy in their production environment. Once deployed, the customer takes ownership of the Solution. This section may specify the customer’s requirements for installing the Solution, training operators, diagnosing and managing response plans, and so on.

**Justification:** Operational criteria communicate to the project team the terms and conditions under which the customer will allow deployment and ultimately sign off on the project. This information provides a framework for planning the Solution’s deployment.

The following table outlines the operational criteria for a successful engagement.

Table 11: Operational criteria

| Identification code | Requirement |
| --- | --- |
| OC1 | ATA administrators can access the ATA Console. |
| OC2 | The ATA Console displays detected suspicious activities on the attack timeline. |
| OC3 | ATA alerts allow administrators to interact and facilitate human acknowledgement and input. |
| OC4 | ATA makes heath state alerts available. For example, when communication between the gateway and the Center is disrupted or when the user account that is used for cataloging entities from AD expires. |
| OC5 | The Solution allows for the configuration of RADIUS accounting for VPNs, and exclusion of internal penetration testing tools subnets, or IPs. |
| OC6 | [Type Customer Name Here] can back up and restore the ATA database and can move the database to another drive or volume. |

1. Source: http://download.microsoft.com/download/F/C/4/FC41DE26-E641-4A20-AE5B-E38A28368433/Security\_Intelligence\_Report\_Volume\_22.pdf [↑](#footnote-ref-2)
2. Verizon: 2017 Data Breach Investigations Report, Edition 10 [↑](#footnote-ref-3)
3. <https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics> [↑](#footnote-ref-4)