ArmorPoint Guided Implementation

Service Details

Contents

PRICING AND PAYMENT METHOD 3
GUIDED IMPLEMENTATION SERVICE DETAILS 3
PROJECT SCOPE 3
1.1.1 Phase 1: ArmorPoint Installation 3
1.1.2 Phase 2: ArmorPoint Validation 5
1.1.3 Phase 3: ArmorPoint Optimization 6
EXCLUSIONS 7
MISCELLANEOUS 9
CONTRACTUAL CHANGES 9

ArmorPoint Guided Implementation Scope

PRICING AND PAYMENT METHOD

ArmorPoint offers these services for a one-time fee as stated in the signed order form, unless otherwise expressly agreed upon in. All fees are due upon receipt of invoice

Payment methods are electronic funds transfer (ACH) or credit card. Payment will be processed upon invoice due date.

This Service Agreement may change and ArmorPoint may update this Service agreement from time to time. It is your responsibility to check this Service Agreement periodically for changes.

GUIDED IMPLEMENTATION SERVICE DETAILS

ArmorPoint will provide a consultative service to guide Client's ArmorPoint implementation as indicated in the scope below. Our Guided Implementation service is intended to be an advisory consulting engagement and does not include any technical installation ("hands on keyboard") within Client's infrastructure. The Guided Implementation service will focus on preparing the Client's environment for a successful ArmorPoint installation with an emphasis on technology best practices, service process validation and continuous service optimization. The service will enable both Client and ArmorPoint resources to be better prepared during full service to execute the ArmorPoint Security Operations Center service. The Guided Implementation project duration is estimated at 6 to 12 weeks from project Kick-Off. Please note that the actual Kick-Off date will be determined by ArmorPoint and shared with Client in a timely manner. The project duration may be affected by any number of circumstances, some of which may be unforeseen.

PROJECT SCOPE

1.1.1 Phase 1: ArmorPoint Installation

The Installation phase consists of a series steps and meetings to ensure the proper installation of the various components of ArmorPoint, including agent installation, network sensor installation and API integration setup. Generally, the below information is accurate and will closely match the actual project as is proceeds forward. However, various factors may come into play that could potentially impact the overall project, the timeline and the duration. As a result, the actual installation phase may vary slightly from what appears below:

- Pre-Installation Discovery
    - Client is responsible for providing the following information to ArmorPoint:
        - User Account Credentials
        - Incident Management Contact Tree
        - Network Sensor Discovery & Network Diagram
        - Client's Security Profile Overview

- Kick-Off call with ArmorPoint
    - Meet your ArmorPoint Technical Specialist team to review the project timeline.
    - Access to the ArmorPoint Portal is granted to pre-determined users.
    - Initial Portal review is completed.
- Agent Deployment
    - With guidance from the ArmorPoint Technical Specialist team, Client is responsible for deploying the provided software agents to the licensed devices via the approved methods provided by ArmorPoint.
    - Regarding the Endpoint Detection & Response (EDR) agents, with guidance from the ArmorPoint team, Client is responsible for enabling the appropriate policies.
    - Client is responsible for initial and future agent deployment and policy adjustment; if technical assistance is needed, an additional Scope of Work will be needed.
- API Integration Setup
    - With guidance from the ArmorPoint Technical Specialist team, Client is responsible for providing the accurate information needed to enable the agreed upon API integrations and completing the ArmorPoint integration card/s.
    - The ArmorPoint team is responsible for verifying the completion of the API integrations and notifying Client of completion.
    - Once completed, Client is responsible for notifying the ArmorPoint SOC team via a Ticket of any changes to the connected API service (i.e. credential refresh, IP changes, and upgrades/downgrades, API token refreshes); failure to do so may result in a malfunctioning API connection.
- Network Sensor Deployment
    - With guidance from the ArmorPoint Technical Specialist team, Client is responsible for deploying the provided network sensor, whether Physical or Virtual, following the provided instructions.
    - The ArmorPoint team is responsible for verifying the completion of network log ingestion and notifying Client of completion.
    - Client is responsible for notifying the ArmorPoint SOC team via a Ticket of any changes to the connected Network Sensor, including location changes, Internal IP address change, network routing changes, among other network related configurations; failure to do so may result in network logs not being ingested.
- ArmorPoint Orientation
    - The ArmorPoint team will, at an agreed upon scheduled time and date, provide a full orientation of the ArmorPoint Portal, including an open Q&A.

- The Orientation call will serve as the completion of the installation phase and ArmorPoint will begin scheduling the next phase of the project.

1.1.2 Phase 2: ArmorPoint Validation

The Validation phase consists of a series steps and meetings to ensure the proper setup of the various components of ArmorPoint, including proper log ingestion for all components, threat detection validation, and confirmation of dashboarding and alerting. Generally, the below information is accurate and will closely match the actual project as is proceeds forward. However, various factors may come into play that could potentially impact the overall project, the timeline and the duration. As a result, the actual installation phase may vary slightly from what appears below:

- Endpoint Agent Validation
  - The ArmorPoint Technical Specialist will review and provide recommendations on Client's endpoint logging to verify that ArmorPoint is receiving the desired log types, including any audit policies configured.
  - ArmorPoint may recommend generic and/or specific changes be made to Client's logging strategy and Client is responsible for implementing those changes.
  - The ArmorPoint Technical Specialist will provide recommendations on Client's future deployment strategy for any remaining in-scope endpoints (i.e. workstations and servers), if applicable.
- Network Sensor Validation
  - The ArmorPoint Technical Specialist will review and provide recommendations on Client's network logging to verify that ArmorPoint is receiving the desired log types, including network log types and devices.
  - ArmorPoint may recommend generic and/or specific changes be made to Client's network logging strategy and Client is responsible for making those changes.
  - The ArmorPoint Technical Specialist will provide recommendations on Client's future deployment strategy for any remaining in-scope network devices, if applicable.
- API Integration Validation
  - For in-scope API Integrations, the ArmorPoint Technical Specialist will review and provide recommendations on Client's integration logging to verify that ArmorPoint is receiving the desired log types.
  - ArmorPoint may recommend generic and/or specific changes be made to Client's API logging strategy and Client is responsible for making those changes.

  - The ArmorPoint Technical Specialist will provide recommendations on Client's future deployment strategy for any remaining in-scope API integrations, if applicable.
- Notification Policy Validation
  - The ArmorPoint Technical Specialist, along with Client participation, will review and configure any additional Notification Policies needed outside of the Default Policies included at time of deployment, not to exceed three (3) additional Notification Policies.
  - If any additional policies are created, including the three (3) offered, Client is responsible for the future maintenance of those Custom Notification Policies.
- Alerting Validation
  - Once the notification policies have been validated, ArmorPoint will provide Client with a one-time ArmorPoint Alert Assessment to validate the alerting process to ensure proper configuration and visibility. At the completion of the assessment, ArmorPoint will provide Client with an executive summary deliverable, and will make recommendations for next steps, if any.
  - The Alerting validation is a non-intrusive assessment that will test to see if necessary alerts are triggering properly within Client's environment.
  - The Alerting Validation will serve as the completion of the validation phase and ArmorPoint will begin scheduling the next phase of the project.

1.1.3 Phase 3: ArmorPoint Optimization

The Optimization phase consists of a series steps and meetings focusing on the optimization of ArmorPoint services, including Security Operation Runbook review, Incident Response Plan review, and tuning priorities for Client's environment. Generally, the below information is accurate and will closely match the actual project as is proceeds forward. However, various factors may come into play that could potentially impact the overall project, the timeline and the duration. As a result, the actual installation phase may vary slightly from what appears below:

- ArmorPoint Runbook Review
  - The ArmorPoint team will provide a standard Security Operation runbook and review the standard runbook with Client.
  - Client, with guidance from the ArmorPoint Technical Specialist team, is responsible for requesting any modifications to the standard runbook.
  - Once the initial runbook is presented and understood, both Client and ArmorPoint are responsible for signing off on the completion.
  - A fully customized Runbook Creation is not part of this scope.

- Incident Response Plan Review
    - ArmorPoint provides a standard Incident Response plan; if Client has their own Incident Response plan, Client is responsible for providing that plan to the ArmorPoint team.
    - In the event of a Client Incident Response plan, the ArmorPoint Technical Specialist will document the plan within the ArmorPoint Portal and get Client sign-off on accuracy and completion.
    - Note: If Client does not possess an Incident Response plan, Client acknowledges that they will be utilizing the ArmorPoint provide Incident Response plan.
    - A fully customized Incident Response Plan creation is not part of this scope.
- Client Tuning Process
    - During the lifetime of the engagement, ArmorPoint will come across a wide variety of circumstances that require the tuning and optimization of the alerting rules within Client's environment; with this in mind, Client is responsible, with guidance from the ArmorPoint Technical Specialist team, for providing the initial guidance and requirements for tuning.
    - Once the initial tuning runbook is agreed upon, both Client and ArmorPoint are responsible for signing off on the completion.
    - In the event that Client does not have any initial requirements for tuning, Client agrees to follow ArmorPoint SOC's best practices regarding tuning.
    - The client tuning process will serve as the completion of the optimization phase and ArmorPoint will officially move Client to 'full production'.
    - At this time, regardless of percentage of completion, Client will fully transition to the ArmorPoint SOC operational service and will cease to receive support from Project Management and ArmorPoint Technical Specialist, unless otherwise stated in the Order Form.

EXCLUSIONS

- Implementation of technology services is not included within this Statement of Work.
- Security Remediations are not included
- Creation of application or network drawings, application dependency mappings, and as-built application, system and network documentation is not included.
- Configuration Assessment of Existing Security Tools is not included
- Any work or services not expressly provided for herein
- Any application development or integration efforts not expressly provided for herein
- Any actual hardware purchases for on-premise needs
- Any migration or upgrade of infrastructure (servers, network, etc.)

- Any actual implementation of the recommendations made by ArmorPoint unless specified in this document
- Any efforts tied to re-installing OS due to virus or malware or any system instability after the removal of a virus
- Any software license or physical hardware expenses
- Any software license that's not explicitly mentioned, and not covered by ArmorPoint
- All Travel and lodging costs.

Any additional work requested beyond the scope of this Agreement will be expressly set forth by subsequent agreement, including, but not limited to, a Client Change Request ("CCR").

MISCELLANEOUS

This Agreement and all corresponding schedules, quotes, exhibits, the ArmorPoint Terms of Service ("the TOS"), and/or Change Orders comprises the entire agreement between the parties and replaces any oral or written agreements between ArmorPoint and Client.

CONTRACTUAL CHANGES

Changes are a natural thing and Client is a continuously evolving business. To facilitate the change process, ArmorPoint has designed the following Governance structure:

Change To	Vehicle	Process
Service Scope	Change of scope presented with justification and supporting data. Changes that cause a change to the monthly cost to Client of more than $1,000 will require further Executive Approval through A Contract Change process.	CCR
New project or effort	Each proposed effort or initiative will be presented to executive leadership and/or board with supporting charter, solution outline and estimates.	Client Dashboard / Real Time
Change to the overall service requirements and performances	Each change will be presented to the Executive and be processed with further Executive Approval	Contract CCR or Addendum
Change to the scope, terms and conditions of the current	Each change will be presented to the Executive and be processed with further Executive Approval	Contract Addendum
Change to the MSA	Each change or group of changes will be reviewed and discussed with each party's legal team until final agreement. No change will be presented for approval that has not met with joint agreement first.	Contract Change