Cisco Advanced Phishing Protection: First Steps

Published Date: June 22, 2018

Identify Key Project Team Members

- **Executive Sponsor**: Point of escalation for critical issues/project roadblocks
- **Project Owner**: Responsible for the success of this project
- **Project Manager**: This person is the primary point of contact and serves as the interface to your organization. They are also responsible for ensuring the project moves forward on the agreed upon schedule and working with other internal groups and departments.
- **Deployment Engineer**: This person will become the expert in your deployment and also be the primary technical contact for the project.
- **Subject Matter Experts**: Technical leaders that provide input into the design and integration; they ensure decisions are in line with the organization's business strategy,
    - Messaging Architect
    - Security Architect

Required Steps Prior to First Customer Success Call

- Review User Guide
- Review training videos in eLearning Portal
    - Creating New Users - https://cl.ly/qrPd
    - Benefits of Domain Tagging - https://cl.ly/2A1m2w391L1Z
    - Inbox policies / whitelisting - https://cl.ly/1V2w1u463k3e
    - How do I re-configure the message recipients receive due to a triggered policy - https://cl.ly/1v381o3F0K0A

- Create users for team members who need to use the platform or receive email reports.

Initial Data Gathering

- What is your mail architecture: Create a diagram showing the end to end mail flow for determining optimal sensor placement in your environment
  - Choose one of the following architecture designs

Inline Sensor	In-Line In an in-line configuration, the Sensor acts as an MTA: it takes responsibility for accepting the message and delivering it to the next hop (usually another internal MTA). Customers utilizing in-line configurations can use the next-hop MTA to take action on incoming messages based on headers added by the Sensor.
Dual Delivery Sensor	The Sensor essentially acts as an SMTP "message sink;" it accepts copies of email messages over SMTP and extracts meta-data in a streaming fashion. Message bodies and attachments are discarded. No SMTP messages leave the Sensor. Dual-delivery is typically used for hosted email architectures like Office365 and G Suite.

  - Determine if the sensor be hosted or on-premises by your organization.
  - Are DKIM and SPF checks currently being performed? If not we recommend to enable DKIM and SPF.

  Note that data modeling will be slower to adjust and less complete without these authentication results.

- Review Requirements for Sensor Installation
  - Installing a Sensor - Chapter 1 of User Guide
- Capture key users or critical groups to be protected.
- Make note of your questions and provide the best times to schedule a call with you upon returning this prework guide.