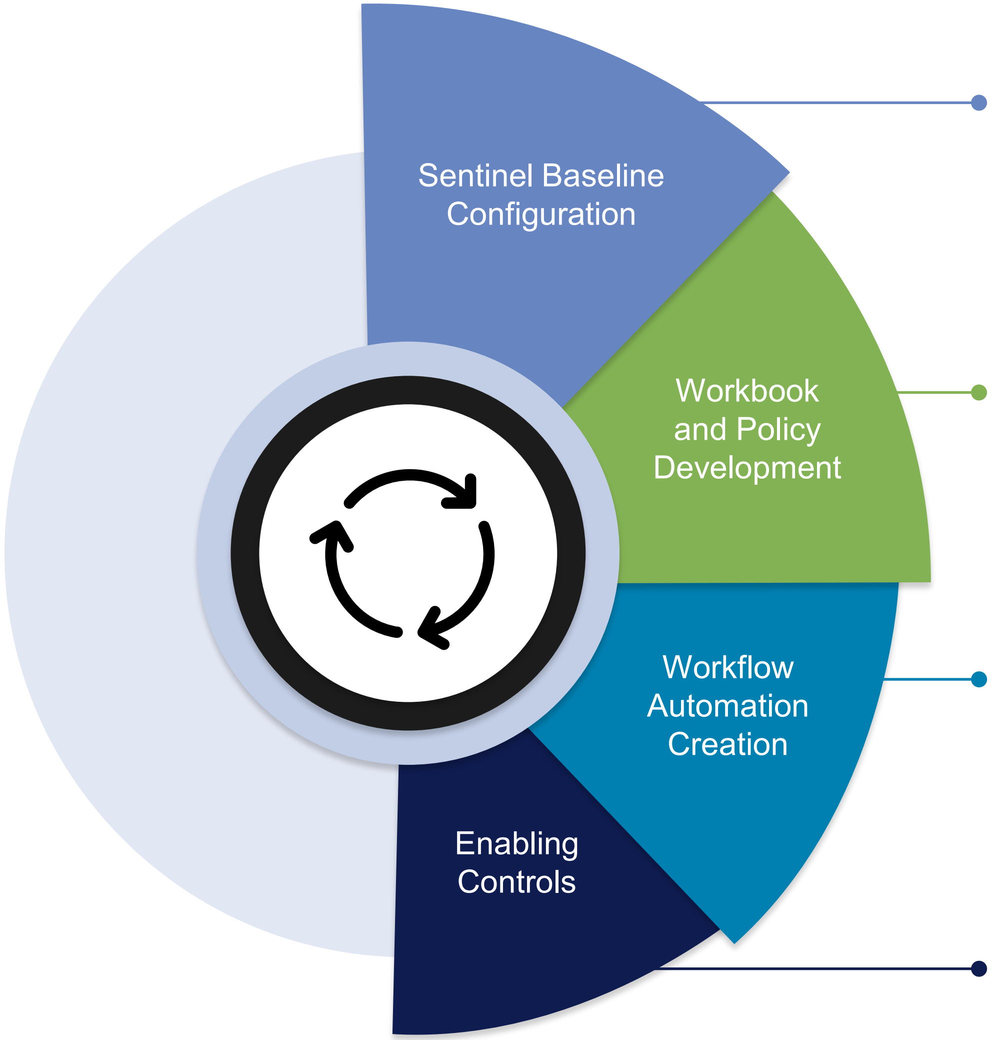
Overview of the NTT DATA Microsoft Sentinel Implementation Phases



Sentinel Baseline Configuration

- If not already active in the customer’s Azure environment, install and configure Microsoft Defender for Cloud.
- Built-in Microsoft connectors will be onboarded to provide rich data insights that will be surfaced with the Microsoft Sentinel console
- Non-Microsoft data connectors (i.e. AWS via CloudTrail) will be enabled within Microsoft Sentinel.
- Associated Defender for Cloud metrics and controls discussed as critical priorities during the advisory workshops will also be enabled.
- Installation of one SysLog or CEF Agent on supported Linux virtual machine for event collection and forwarding to Sentinel
- Connect up to two subscribed Threat Intelligence feeds supported by Sentinel. Note: Azure Active Directory Global Admin or Application Admin will be required.

Workbook and Policy Development

.

- Up to five workbooks will be created to surface deeper insights on critical use cases the client wishes to assess at a more granular level, as determined during the advisory workshop engagement.
- Import existing Watchlists based on current threats and provide templates for development of additional watchlists

Workflow Automation Creation

- Workflows can include all subscriptions or in-scope resources (at scale), or be scoped to specific environments, subscriptions or workloads.
- Develop agreed workflows for in-scope resources.
- Work with the client’s technical team to test the workflows to verify the remediation action aligns to the trigger.

Enabling Controls

- Enroll additional log sources to meet design criteria.
- Assess security patterns from the captured alerts received after Defender for Cloud and Sentinel implementation phases
- Adjust automated governance activities and policies as indicated by the alert behaviors and patterns, with the client’s approval
- Finalize documentation required for managed services and steady-state support.

Validate the controls and meet the objectives by enabling Controls Assess usage and performance patterns from the captured alerts established during the preceding phases.

Configure governance controls based on required modifications as indicated during the testing process.