# NTT DATA Sentinel Advisory Engagement Overview

## Zero Trust Assessment

- Conduct a zero trust assessment, and review high-level environment architecture and security solutions currently in place
- Discuss business concerns and requirements
- Output - Zero trust evaluation report and top line objectives, concerns and requirements, as well as a strategic roadmap to reach zero trust

## Introduction to Microsoft Sentinel

- Review Sentinel features and functionality and how these can be used to protect your IT environment
- Discuss how Sentinel capabilities can address your concerns and specific goals to accomplish
- Output - Prioritized list of objectives to address the Sentinel features that address your requirements

## Data Source Identification

- Identify data sources that will send information to Sentinel
- Prioritize data sources
- Identify solution for non-Azure devices
- Output – Defined approach to identify and on-board data sources for Sentinel

## Workbook/Use-Case Selection

- Review Microsoft-provided Workbooks and Use Cases
- Agree on relevant workbooks and Use Cases and determine priority
- Identify future custom workbooks and Use Cases
- Output - Defined process to implement and test Workbooks and Use Cases within Azure Sentinel

## Integration with Other Tools

- Review other Microsoft Security tools and plan for integration to realize maximum overall protection
- Review plan to integrate Sentinel into customer or NTT DATA ITSM and other security solutions to aggregate and correlate events and to implement single pane of glass for analysis.

## Security Automation

- Review security automation and customer's approach to automating security responses
- Identify existing automated response capabilities and prioritize implementation
- Identify custom automation requirements and prioritize
- Output – Configuration and Implementation plan for automation

## Threat Hunting

- Review and identify existing KQL queries, including Microsoft-provided and in NTT GitHub repos
- Create any KQL queries specific to the customer's environment or industry
- Output - agreed upon test plan to validate KQL queries and submit to GitHub repository

## Design Guide

- Summarize all gathered intel & established parameters, configuration details and data.
- Output – a design guide, architectural diagram, an implementation plan combining your requirements and NTT best-practices, as well as an operations guide, covering procedures, escalation processes, & service parameters