Trustwave®

SERVICE DESCRIPTION

Accelerators for Microsoft Security

Overview

Trustwave Accelerators for Microsoft Security (**"Service"**) provide Client with a roadmap to accelerate value and security outcomes from Microsoft Security products. The Service is designed to outline the activities needed to set up aspects of Client's Microsoft Security environment, with the aim of increasing security maturity and identifying potential cost-saving initiatives.

Time Boxed

The Service is allocated a defined number of hours for delivery as indicated in the applicable SOW or Order Form. In this case, the scope of the Service is limited to the work Trustwave can deliver within the agreed number of hours.

The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Form between Trustwave and Client.

Service Features

The Service includes one (1) or more of the following accelerators (one (1) or more, **"Accelerators"**, and each, an **"Accelerator"**). The applicable Accelerator(s) will be indicated in a SOW or Order Form between Trustwave and Client.

Accelerators

Accelerator for Microsoft Defender XDR

The Accelerator for Microsoft Defender XDR provides Client with a roadmap to accelerate value and security outcomes from Microsoft Defender XDR. Trustwave will conduct the following reviews as part of the Service:

- **Security Entitlements:** Evaluate current security entitlements to understand what has been purchased and determine alignment with security needs.
- **Security Configurations:** Assess existing security configurations within each Defender XDR service to identify areas for improvement.
- **Use and Operation of Security Tools:** Review current use and operation of security tools with a view to improving their effectiveness.
- **Financials:** Identify redundancies and opportunities for rationalization in the Defender XDR technology stack to identify potential cost savings.

The Microsoft Security products covered under the Accelerator for Microsoft Defender XDR are:

- Microsoft Defender for Endpoint

- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Office 365
- Microsoft Defender for Servers
- Microsoft Defender Vulnerability Management

Accelerator for Microsoft Sentinel

The Accelerator for Microsoft Sentinel provides Client with a roadmap to accelerate value and security outcomes from Microsoft Sentinel. Trustwave will conduct the following reviews as part of the Service:

- **Workspace Architecture:** Assess workspace architecture to understand current deployments and identify areas for improvement.
- **Data Sources:** Evaluate data sources and log source types to understand data connections.
- **Roles and Permissions:** Assess roles and permission for users, groups, and services to evaluate excessive privileges.
- **Threat Intelligence:** Evaluate threat intelligence enablement to assess coverage and capabilities.
- **SIEM Content:** Evaluate SIEM use cases and analytics to assess comprehensiveness.
- **SOAR Playbooks:** Review inventory of playbooks, dashboards, and reporting metrics to assess the level of coverage.
- **Defender XDR Connectivity:** Evaluate connectivity to Defender XDR services to identify areas for optimization, if applicable.
- **Financials:** Evaluate current usage against cost model to identify potential cost savings.

The Microsoft Security product covered under the Accelerator for Microsoft Sentinel is:

- Microsoft Sentinel

Accelerator for Microsoft Security Copilot

The Accelerator for Microsoft Security Copilot provides Client with a roadmap to accelerate value and security outcomes from Microsoft Security Copilot. Trustwave will conduct the following reviews as part of the Service:

- **Environment:** Assess the environment based on best practices pertaining to permissions and access controls to identify areas for improvement.
- **Promptbooks:** Analyze core security operations detection, triage, and response promptbooks to understand capabilities.
- **Threat Intelligence:** Analyze the breadth and quality of threat intelligence to assess the level of coverage.
- **Use and Operation:** Review current use and operation of Security Copilot to identify potential improvements to its effectiveness.
- **Use Cases:** Identify use cases where security teams can gain benefits from Security Copilot.

The Microsoft Security product covered under the Accelerator for Microsoft Security Copilot is:

- Microsoft Security Copilot

For Trustwave to provide the Accelerator for Microsoft Security Copilot, Client must procure the necessary number of Security Compute Units (SCUs) from Microsoft. Trustwave will coordinate with Client to determine the number of SCUs required by Client for Trustwave to provide the Service.

Accelerator for Microsoft Purview

The Accelerator for Microsoft Purview provides Client with a roadmap to accelerate value and security outcomes from Microsoft Purview. Trustwave will conduct the following reviews as part of the Service:

- **Sensitive Information Types (SIT):** Review SITs to evaluate the effectiveness of data classification.
- **Sensitivity Labels:** Assess the application of data sensitivity labels to understand how data is protected and governed.
- **Information Protection:** Evaluate the strategies and tools in place for safeguarding sensitive information to identify areas for improvement.
- **Data Loss Prevention (DLP):** Review the mechanisms in place for preventing the unauthorized sharing or exposure of data to assess the level of coverage.
- **Data Coverage:** Review coverage across data sources to identify potential data exposure and areas for improvement.

The Microsoft Security product covered under the Accelerator for Microsoft Purview is:

- Microsoft Purview

The data sources in scope for the Accelerator for Microsoft Purview are the following online Microsoft 365 services: 1) Exchange Online, 2) OneDrive, 3) SharePoint Online, and 4) Teams.

Accelerator for Microsoft Entra ID

The Accelerator for Microsoft Entra ID provides Client with a roadmap to accelerate value and security outcomes from Microsoft Entra ID. Trustwave may conduct the following reviews as part of the Service, as agreed between Trustwave and Client during the kick-off meeting:

- **Authentication:** Assess authentication mechanisms, such as methods and conditional access, to identify areas for improvement.
- **Authorization:** Review authorization measures, such as role-based access control (RBAC) and group management, to assess appropriateness of permission levels.
- **Identity Protection:** Review identity protection capabilities, such as risk monitoring and investigation, to determine alignment with security objectives.
- **Device Management:** Analyze device management capabilities, such as device registration and device compliance, to review the level of security.
- **Application Management:** Analyze application management capabilities, such as application integration and single sign-on (SSO), to review the level of security.
- **Governance:** Review governance mechanisms, such as privileged identity management (PIM) and lifecycle workflows, to identify areas for improvement.
- **Security Posture Management:** Assess security posture management capabilities, such as Identity Secure Score and security baselines, to assess the level of coverage.

The Microsoft Security product covered under the Accelerator for Microsoft Entra ID is:

- Microsoft Entra ID

The Accelerator for Microsoft Entra ID covers features included as part of Client's Microsoft E5 license.

Tools and Methodologies

Trustwave will combine industry-standard, Microsoft-native, and proprietary tools to perform the Service to provide a comprehensive and effective review process.

Deliverables

Trustwave will produce the following key deliverables as part of the Service:

- **Roadmap:** High-level roadmap for implementing recommendations. This roadmap will consider gaps between current and optimal security configurations and/or capabilities, including recommendations for additional security configurations and/or capabilities to increase Client's security maturity.
- **Workshops:** Deep-dive workshop(s) on topics relating to Microsoft Security. The workshop(s) will focus on specific topics relating to the Microsoft Security area covered by the applicable Accelerator. Trustwave will conduct one (1) to three (3) workshops for Client (as specified in the applicable SOW or Order Form) on topics agreed between Trustwave and Client, with each workshop approximately sixty (60) minutes in duration.

Delivery and Implementation

Trustwave will work with Client to assess and determine areas of improvement for Client's Microsoft Security capabilities:

Discovery

Trustwave will work with Client to gather information that describes Client's Microsoft Security environment. This includes:

- Completing preparatory work and outlining requirements for the Service.
- Conducting a kick-off meeting with stakeholders to discuss objectives and delivery expectations, including escalation paths and governance.
- Developing a project plan with key activities, milestones, and timelines.
- Obtaining systems access with appropriate permission levels, as required.
- Collecting information on relevant security tools.

Client Obligations

For Trustwave to provide the Service, Client will:

- Provide contact details for and access to Client stakeholders and escalation points and remain available for communication from Trustwave;
- Attend a kick-off meeting and provide logistics support for booking meetings and arranging access to required personnel;
- Coordinate with Trustwave to discuss concerns and perceived threats, objectives, and delivery expectations, as well as develop a project plan;
- Provide Trustwave with access to systems with appropriate credentials, as reasonably requested by Trustwave; and
- Provide Trustwave with information on relevant security tools.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Establish engagement roles and responsibilities for stakeholders;
- Deliver and facilitate a kick-off meeting at a date and time agreed between Trustwave and Client;
- Coordinate with Client to discuss concerns and perceived threats, objectives, and delivery expectations, as well as develop a project plan; and
- Collect information on relevant Client security tools.

Analysis

Trustwave will examine applicable data and information and coordinate with Client stakeholders to assess Client's current Microsoft Security capabilities:

Accelerator for Microsoft Defender XDR

For the Accelerator for Microsoft Defender XDR, analysis may include:

- Evaluating security entitlements and configurations.
- Reviewing Client's Microsoft Secure Score and associated security metrics.
- Assessing compliance controls based on security features available in Defender XDR.
- Reviewing security tool usage and operations, identifying redundancies and opportunities for rationalization.
- Identifying Microsoft services outside of Defender XDR that Client is not currently using but which may help increase Client's security maturity.

Accelerator for Microsoft Sentinel

For the Accelerator for Microsoft Sentinel, analysis may include:

- Assessing workspace architecture.
- Evaluating data sources and log source types, including roles and permissions.
- Analyzing threat intelligence enablement and capabilities.
- Reviewing SIEM content, such as use cases and analytics, and inventory of SOAR playbooks.
- Reviewing SOC efficiency dashboards and reporting.
- Evaluating connectivity to Defender XDR services and/or third-party technologies.
- Assessing usage costs and determining where costs can be optimized.
- Assessing compliance controls based on security features available in Sentinel, including alignment with the MITRE ATT&CK framework and Cybersecurity Maturity Model Certification (CMMC) reporting enablement, where applicable.

Accelerator for Microsoft Security Copilot

For the Accelerator for Microsoft Security Copilot, analysis may include:

- Assessing the environment based on best practices pertaining to permissions and access controls.
- Identifying potential plugin enablement for Microsoft Security products and services.
- Reviewing dashboards, reporting, and security metrics.
- Assessing compliance controls based on security features available in Security Copilot.
- Analyzing core security operations detection, triage, and response promptbooks.
- Analyzing Client's adoption of threat intelligence in Security Copilot.

- Identifying and assessing potential use cases for Security Copilot, including planned, new, or existing deployments.
- Assessing SCU requirements based on security operations and planned usage.

Accelerator for Microsoft Purview

For the Accelerator for Microsoft Purview, analysis may include:

- Evaluating SITs and assessing custom types.
- Reviewing sensitivity labels and default classification.
- Analyzing strategies and tools in place for safeguarding sensitive information throughout its lifecycle, including compliance with applicable standards and requirements.
- Reviewing appropriate policies and procedures relating to data identification, data classification, data retention, data lifecycle management, and DLP.
- Reviewing coverage across data sources.
- Assessing roles and group assignments within Purview.

Accelerator for Microsoft Entra ID

For the Accelerator for Microsoft Entra ID, analysis may include:

- Assessing authentication mechanisms, such as methods, conditional access, password policies, external identity providers, and legacy authentication protocols.
- Review authorization measures, such as RBAC, attribute-based access control (ABAC), group management, and illicit consent grants.
- Review identity protection capabilities, such as risk monitoring, investigation, and Entra ID protection.
- Analyzing device management capabilities, such as device registration and device compliance.
- Analyzing application management capabilities, such as application integration, SSO, and application proxy.
- Reviewing governance mechanisms, such as PIM, lifecycle workflows, and identity governance.
- Assessing security posture management capabilities, such as Identity Secure Score and security baselines.
- Reviewing other considerations, such as multi-tenant environments, external collaboration, data residency, and compliance controls.

Client Obligations

For Trustwave to provide the Service, Client will:

- Provide feedback on Trustwave findings, as requested by Trustwave; and
- Participate in and understand materials explained during meetings, including discussions on inspections and controls analysis.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Assess data and information pertaining to Client's environment; and
- Review findings with Client and obtain feedback, as required.

Reporting

Trustwave will produce a roadmap that Client may utilize to accelerate Microsoft Security capabilities and increase security maturity. This includes:

- Conducting a gap analysis highlighting gaps between current and optimal security configurations and/or capabilities.
- Developing recommendations for additional security configurations and/or capabilities to increase Client's security maturity.
- Developing a high-level roadmap for implementing recommendations.
- Conducting deep-dive workshop(s) based on topics agreed between Trustwave and Client.

Client Obligations

For Trustwave to provide the Service, Client will:

- Review Trustwave's deliverables and attend review sessions conducted by Trustwave;
- Attend deep-dive workshop(s) conducted by Trustwave; and
- Support the identification of appropriate owners for Trustwave's findings and recommendations.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Present deliverables to Client for review and feedback;
- Deliver and facilitate deep-dive workshop(s) for Client stakeholders; and
- Conduct project close-out, confirming delivery of key activities and deliverables.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave's Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or in the applicable SOW or Order Form between Trustwave and Client.