Trustwave®

SERVICE DESCRIPTION

Customized SIEM Optimization Program

Overview

The Trustwave Customized SIEM Optimization Program ("**Service**") provides Client with enhanced Security Information and Event Management ("**SIEM**") environment support through custom use case and analytic rule ("**Use Case**") development and implementation, as well as threat monitoring advisory. The Service is designed to enable continuous improvement and to advance the maturity of Client's SIEM environment.

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 the following features:

Custom Use Case Development and Implementation

Trustwave will collaborate with Client to design, develop, and implement customized Use Cases within Client's SIEM environment, tailored to address the evolving threat landscape and Client's specific Use Case requirements, priorities, and risk profile. Client's SIEM platform will be identified in the applicable SOW or Order Form between Trustwave and Client. As part of this Service feature, Trustwave will:

- Identify and prioritize security challenges and objectives in collaboration with Client;
- Develop Use Cases that align with requirements to integrate into Client's SIEM environment;
- Test and validate the functionality of each Use Case;
- Fine-tune Use Case parameters to optimize performance and alignment with existing detection mechanisms; and
- Document all Use Cases and integrate them into Client's operational workflows to enhance Client's overall threat detection and response capabilities.

Threat Monitoring Advisory

Trustwave will provide expert insights into threat monitoring gaps, emerging risks, and SIEM optimization opportunities through ongoing discussions with Client. The goal of threat monitoring advisory is to help refine detection priorities, align monitoring efforts with business risk, and identify potential threat monitoring enhancements to maximize the effectiveness of Client's SIEM environment.

Service Package

- The Service includes a total of ninety (90) hours of support, which is comprised of eighty (80) hours of consulting support and ten (10) hours of project management support.
- Client will have ninety (90) days ("**Engagement Period**") to use the purchased hours, starting on a date mutually determined by Trustwave and Client. Any unused hours will expire on the last day of the Engagement Period. Trustwave will coordinate with Client to confirm the start date and manage delivery expectations.
- Client may choose to purchase additional Engagement Periods in ninety (90)-hour increments ("**Increment**") at any time. For each Increment, Client will have an additional ninety (90) days to use the total purchased hours before the hours expire.
- The scope of the Service is limited to the work Trustwave can deliver within the purchased number of hours and may be customized by Trustwave and Client in an applicable SOW or Order Form.

Delivery and Implementation

Trustwave will guide Client through the following four (4) key phases as part of the Service delivery process:

Phase 1 – Discovery and Planning

Trustwave will collaborate with Client to understand Client's specific security objectives, existing SIEM environment, and operational requirements. This phase aims to establish the foundation for a tailored and effective Service.

Client Obligations

For Trustwave to provide the discovery and planning phase of the Service, Client will:

- Provide contact details for and access to Client stakeholders, including 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 develop the project governance and oversight process;
- Coordinate with Trustwave to discuss concerns and perceived threats, objectives, and delivery expectations;
- Provide Trustwave with access to Client's systems with appropriate credentials, as reasonably requested by Trustwave; and
- Provide Trustwave with relevant information on SIEM capabilities, existing Use Cases, security policies, and relevant security tools.

Trustwave Obligations

As part the discovery and planning phase of the Service, Trustwave will:

- Deliver and facilitate a kick-off meeting at a date and time agreed between Trustwave and Client;
- Establish the project governance and oversight process, including the project plan and roles and responsibilities, together with Client;
- Coordinate with Client to discuss concerns and perceived threats, objectives, and delivery expectations;
- Establish a process for coordinating with stakeholders to gather input and track progress against defined objectives; and
- Collect relevant information on Client's SIEM capabilities, existing Use Cases, security policies, and relevant security tools.

Phase 2 – Use Case Analysis and Development

Trustwave will collaborate with Client on the design and development of custom Use Cases aligned with Client's security monitoring requirements. This phase aims to adapt Client's SIEM environment to emerging threats.

Client Obligations

For Trustwave to provide the Use Case analysis and development phase of the Service, Client will:

- Communicate to Trustwave any organizational priorities or emerging requirements;
- Engage in feedback sessions with Trustwave to assess the proposed Use Cases; and
- Approve Use Cases proposed by Trustwave for implementation as prescribed by Trustwave.

Trustwave Obligations

As part of the Use Case analysis and development phase of the Service, Trustwave will:

- Analyze Client's SIEM and threat monitoring environment, including existing Use Cases;
- Design custom Use Cases based on reviews and findings on Client's SIEM environment; and
- Conduct feedback sessions with Client to confirm that Use Cases align with Client's evolving security needs.

Phase 3 – Use Case Implementation

Trustwave will implement the identified Use Cases and tune configurations to optimize their effectiveness in addressing security incidents. This phase aims to implement Use Cases that are effective and responsive to emerging threats.

Client Obligations

For Trustwave to provide the Use Case implementation phase of the Service, Client will:

- Provide Trustwave with necessary access to the SIEM environment for deployment; and
- Share feedback with Trustwave on Use Case performance and incident trends.

Trustwave Obligations

As part of the Use Case implementation phase of the Service, Trustwave will:

- Implement the Use Cases in Client's SIEM environment;
- Analyze the performance and effectiveness of the implemented Use Cases;
- Tune alerting to within prescribed thresholds;
- Provide Client with appropriate supporting information on the new or modified Use Cases, including the purpose and description of each Use Case to support operating procedures; and
- Provide recommendations for continuous improvement.

Phase 4 – Threat Monitoring Advisory

Trustwave will assess the monitoring capabilities of Client's SIEM environment, focusing on alignment with security objectives and offering detailed insights and strategic recommendations for continuous improvement. This phase aims to enhance the overall monitoring capabilities of Client's SIEM environment.

Client Obligations

For Trustwave to provide the threat monitoring advisory phase of the Service, Client will:

- Attend review sessions conducted by Trustwave;
- Attend workshops conducted by Trustwave, as applicable; and
- Support the identification of appropriate owners for Trustwave's findings and recommendations.

Trustwave Obligations

As part of the threat monitoring advisory phase of the Service, Trustwave will:

- Confirm the inclusion of the Use Cases in Client's overall inventory;
- Outline recommendations for future improvements to enhance SIEM performance and maturity, potentially including analytics, automation, and reporting enhancements;
- Facilitate workshops on topics of interest or emerging requirements, as applicable; and
- Confirm 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.