SERVICE DESCRIPTION

Splunk Technology Implementation Services

Service Scope

Trustwave Technology Implementation Services provides a set of offerings focused on the plan, design, and implement phases of your Splunk network security solution.

The Services include specific pre-defined deliverables and will be completed at a time mutually agreed to between Client and Trustwave. The objective of the Services is to partner with Client in maximizing the time to value investment made in Splunk through a new installation, upgrade and optimization, migration with Trustwave Managed Security Services.

The Consulting and Professional Service does not manage the capabilities of Splunk or ongoing Threat Detection. Threat Detection and Response services are available in the Service Description Trustwave Managed SOC.

The Trustwave project team will approach this engagement with the following goals:

- Understand Client's business requirements and critical objectives;
- Tailor Trustwave's core project approach with Client for transparent timelines and milestones;
- Facilitate weekly status and project governance calls to proactively handle problem management and Client success;
- Communicate all travel requests at least two weeks in advance to effectively coordinate scheduling and minimize costs.

Trustwave has defined the effort into five (5) logical phases:

- Phase 1 – Project Initiation
- Phase 2 – Design and Architecture
- Phase 3 – Implementation/Migration
- Phase 4 – Knowledge Transfer
- Phase 5 – Maintenance (optional)

Assumptions

The following assumptions have been made in anticipation of this effort:

- Work under this SOW will be performed at Client's facilities except for any project-related activities which Trustwave and Client agree be performed remotely or at Trustwave's premises in order to complete the obligations and responsibilities under this SOW.

- Any additional fees will be first agreed to in writing by Client.
- Trustwave will provide the Services under this SOW during normal business hours, 8:30 AM to 5:15 PM, local time, Monday through Friday, except holidays.
- Client will provide sufficient access to the hardware and software environments being used for the project, including network connectivity and required authorizations.
- Client will provide resources with sufficient data security knowledge for this project.
- Client will ensure sufficient security and compliance user participation.
- Client will ensure sufficient access to Database administrators, Network and System Administrators as needed.
- Client will ensure that a proven backup and recovery strategy is in place for the systems being upgraded.
- Client will ensure that all hardware and software requirements have been met and configuration recommendations have been followed prior to the start of the Project. Client acknowledges that Splunk technology will not be installed without minimum specifications and may not perform optimally unless system sizing recommendations have been met. Any delays encountered as a result of system specifications or recommendations not being met are Client's responsibility.
- Client will test the Splunk technology solution according to the schedule and procedures outlined jointly with Trustwave.
- Client and Trustwave will ensure the steps outlined in the project plan are achieved in a timely manner.
- To complete certain Tasks and Deliverables under this SOW, Trustwave may request access to specific servers, network equipment, etc., as needed. Such access and related activities will only be performed with Client's explicit authorization, and always under direct Client supervision.
- Where used, "Duration" refers to man effort and not elapsed time.

Exclusions

- Trustwave will not provide structure cabling, poer, patch cords or racks.
- Offering does not include performing Proof of Concept effort.
- Offering does not include customization or plug-in (e.g. report, API, alert), unless otherwise stated.
- Offering does not include whole network or infra redesigning effort.
- Offering does not include load/performance testing.
- Offering does not include vulnerability testing/penetration testing.
- Offering does not include external backup, logging and monitoring solution
- Support for operation tasks (e.g. change request), is not part of the scope. Username and password shall be handed over to Client operation team to perform operation tasks (e.g. check log, implementing Change Request, add/edit/remove policy).
- The Services do not include an assessment of Client's organization, personnel, or IT infrastructure compliance to existing policies, practices, standards, guidelines, processes, or procedures, and is not intended to provide assurance of compliance with any industry, regulatory, or legislative requirements.
- Any additional actions not defined in this SOW or scope are excluded.
- Services beyond the number of man-hours defined in the scope are excluded.

Facilities

Client will provide Trustwave and its personnel with facilities that Trustwave may reasonably require to perform the Services, in particular: supplies, furniture, computer facilities, telephone/fax communications, and broadband access via network connectivity capability and other facilities. The Trustwave project team will be located in an area adjacent to Client's subject matter experts and technical personnel and all necessary security badges and clearance will be provided for access to this area. Client will be responsible for ensuring that Client has appropriate backup, security and virus-checking procedures in place for any computer facilities Client provides or which may be affected by the Services.

Completion Criteria

Trustwave will have fulfilled its obligations under this SOW when any one of the following occur:

1. Trustwave accomplishes the activities defined in detailed SOW, in accordance with the terms and conditions set forth in the Agreement, including but not limited to the warranties contained therein, including delivery to Client of the Materials agreed to, if any;
2. Trustwave provides a defined number of man-hours of Services as specified in the scope;
3. Client or Trustwave terminates the project in accordance with the provisions of the Agreement; or
4. The end of the one-year term of this SOW.

Services Delivery Coordination

To facilitate delivery of the Services described in this SOW, both Trustwave and Client will provide a designated Point of Contact (PoC) to perform the following:

Trustwave-designated PoC will:

- Review the SOW and any associated documents with Client-designated PoC;
- Coordinate and manage technical activities of Trustwave's personnel;
- Work with Client-designated PoC to establish project governance and maintain communication;
- Work with Client-designated PoC to assist in the preparation of the project plan, which lists activities, assignments and performance milestones of this SOW;
- Review and administer Project Change Control Procedure upon approval with Client-designated PoC;
- Complete and return any Client questionnaires or checklists with five (5) days of receipt, if applicable;
- Serve as conduit between Trustwave project team and all Client personnel participating in Services;
- Obtain and provide applicable information, data, consents, decisions and approvals as required by Trustwave to perform the Services in timelines described in the Service;
- Help resolve Service issues and escalate issues to the Client organization, as applicable;
- Prepare, attend and deliver status reports as applicable; and
- Deliver all Trustwave deliverables in this SOW;

Client-designated PoC will:

- Review the SOW, and any associated documents, with Trustwave-designated PoC;
- Establish and maintain communication with Trustwave assigned resources;
- Measure, track, and evaluate progress against the project plan;
- Resolve deviations from the project plan with Client project team and Trustwave;
- Facilitate delivery of Client data collection for delivery to Trustwave-designated PoC.

Project Phases & Timelines

This section defines the project phases. Our current estimate, based on our present knowledge, outlines a man-hour initiative as agreed by the parties in the scoping document:

Phase 1: Project Initiation

Estimated Duration: TBD Network Engineer man-hours TBD Project Manager man-hours

The purpose for this activity is to kick off the project and set expectations with the Client.

Trustwave will work with Client to review the current infrastructure, change control, and other project processes and expectations. Trustwave will initiate data gathering process to receive initial information about the Client environment and security posture.

	Task	Participants
1	Set project expectation with Client	Client and Trustwave
2	Provide initial environment information, including disposition of security monitoring, sensors and other log source information, possible detection rules, reports and dashboards and current security posture	Client
3	Initial project plan creation	Trustwave

Data gathered from Client's environment:

a) Complete inventory of all auditing and logging devices, including firewalls, IDSes, servers, workstations, routers, switches, firewalls, and wireless
b) Current state network design
c) Current log management state, monitoring and controls, general security posture
d) Security team capabilities and workflows for reporting, alerting and incident response

Note: For Clients that cannot provide the information above, an assigned Network Engineer should be scoped.

Phase 1 Deliverables:

- Initial Project Plan
- Log sources and log management documentation
- Splunk architecture/sizing strawman

Phase 2: Design & Architecture

Estimated Duration: TBD Network Engineer man-hours TBD Project Manager man-hours

The purpose of this activity is to help the project team scope and design the implementation based on business needs and technical environment. The Trustwave project team will work with Client to gather necessary data from network administrators/designers, system administrators and information security personnel.

Phase 2 Requirements

- Complete pre-engagement data gathering

Phase 2 Tasks:

	Task	Participants
1	Existing log source and log management documentation.	Client
2	Scoping of Splunk deployment functions and requirements, including in scope log sources, appropriate Splunk configuration including parsers, use cases, indexes, reports, retention.	Client and Trustwave
3	Documentation of key functions/requirements and a test plan to ensure full validation during the deployment.	Client and Trustwave
3.1	Data flow mapping/Data Acquisition/Indexing – Determining best methods for transport of log and audit data from in scope log sources, parsing of collected logs, efficient storage and indexing and retention policies of raw and parsed data.	Client and Trustwave
3.2	Threat detection use cases, alerting criteria.	Client and Trustwave
3.3	Reporting and data access.	Client and Trustwave
4	Definition of system access and user controls.	Trustwave
5	Update of project plan with timelines and responsibilities.	Trustwave

The design document and accompanying deployment diagrams may cover the following elements.

Network Topology

- Current Topology
- Future Topology
- Private Cloud
- Public Cloud

- Splunk Technology
  - In scope log sources
  - Connectors and parsers for in scope log sources
  - Splunk configuration recommendations
    - Sizing
    - Data acquisition, indexing and retention policies
    - Use cases and correlations

        - Reports and other data access
    - Analyst workflows and interactions with upstream MSS (if applicable)

Phase 2 Deliverables:

- Project Plan for deployment
    - Roles and responsibilities
    - Timeline and milestones
- Overview and detailed diagrams
- Use case/key requirements documentation

Phase 3: Implementation and Validation

Estimated Duration: TBD Network Engineer man-hours TBD Project Manager man-hours

During the implementation phase Trustwave will, with Client assistance, implement the Splunk technology design and equipment scoped in Phase 2.

Guided by the agreed-on design documentation, the implementation phase will follow the ensuing high-level outline. Trustwave will validate implementation according to the design document and remain onsite for up to one half day as well as provide remote standby where needed.

Phase 3 Requirements

The following must be completed prior to start of work. Client has:

- Accepted the design documentation
- Prepared hardware and software platforms and made available for implementation
- Assigned a Project Technical Lead who will be the primary contact during the implementation
- Approved all necessary appropriate change requests, if needed, and agreed on change control windows.

Phase 3 Tasks

	Task	Participants
1	Technology Deployment - Depending on your network topology, a deployment may require more than one Splunk appliance at more than one location.	Client and Trustwave
2	Technology Configuration – Based on phase two design and architecture, Splunk will be configured to support log collection, parsing, storage, indexing, correlation/use cases for alerting, reporting and other data access.	Client and Trustwave

3	Post-Migration Threat Assessment – Trustwave will perform a post-migration Threat Assessment of live traffic. Based on the Analysis, Trustwave will provide additional documented changes to configurations to further secure the client network. The results of the Threat Analysis will be appended to the approved design documentation	Trustwave

Phase 3 Deliverables:

- Completed implementation as per design document (Phase 2)
- Updated design documentation with any agreed changes made during deployment.

Phase 4: Knowledge Transfer

Estimated Duration: TBD man-hours per quarter / Included in implementation time scope

Trustwave will ensure that Client is familiar with the deployed solution. This will be achieved through a handover process. Knowledge transfer to the team occurs interactively during the engagement and covers the installation, configuration, and basic administration of the Splunk solution.

Phase 4 Tasks:

	Task	Participants
1	Review as-built document. This document consists of non-default setting/parameter configured during deployment, not a how-to guide.	Client and Trustwave
2	Knowledge transfer activities with reference to implementation solution.	Client and Trustwave
3	Review the actions and decisions that were taken during Phase 3.	Client and Trustwave
4	Review the actions and remediations taken during the project to go over an operations knowledge transfer.	Client and Trustwave
5	Review procedures for contacting Trustwave Maintenance Support where applicable	Client and Trustwave

Phase 5: Maintenance Health Check

Estimated Duration: TBD man-hours per quarter

On a selected periodic basis, Trustwave staff will remotely access each of the security products deployed at the Client site to perform a system review.

Trustwave will verify the following as part of a health check service:

- Verify current patch levels.
- Audit log review
    - Identification of any performance issues.
    - Identification of any potential security issues.
- Old or unused policies verification and recommendation.

Note: Additional checks are continuously added based on Trustwave's best practices for deployment and maintenance.

Phase 5 Deliverables:

- Health Status report.
- Recommended remediation activities (if applicable)

Project Staffing

Trustwave will coordinate Trustwave resources and provide project management inputs to Client's project manager.

Roles and Responsibilities

Success of this project is dependent on the parties' mutual understanding of roles and responsibilities. This section details Client and consultant participation and responsibilities.

Client Project Manager

Prior to the start of this SOW, Client will designate a person to be the Client Project Manager who will be the focal point for Trustwave communications relative to this project and will have the authority to act on behalf of Client in all matters regarding this project. Client Project Manager's responsibilities include:

- Manage Client personnel and responsibilities for this project.
- Serve as the interface between Trustwave and all Client departments participating in the project.
- Administer the Project Change Control Procedure with the Trustwave Implementation Manager.
- Participate in project status meetings.
- Help resolve project issues and escalate issues within Client's organization, as necessary.
- Review with the Trustwave Implementation Manager any of Client's invoice or billing requirements. Requirements that deviate from Trustwave's standard invoice format or billing procedures may have an effect on price, and will be managed through an Addendum.

Client IT Responsibilities

- Provide supervised access to hardware, software, database, and network, when needed.
- Validate deployed solution and assume maintenance of it at the end of implementation phase.

Client Network and/or Security Administrator

- Provide appropriate subject matter experts to participate in the project.
- Provide policy and reporting requirements.
- Review and approve solution designs.
- Design and develop any new change control processes required to maintain DarkTrace technology solution.
- Approve the promotion of the system to production.

Trustwave Project Management

- Create project plan with timelines as well as roles and responsibilities based on Design Document.
- Align Trustwave resources with tasks and coordinate work schedule. Work with Client Project manager to ensure appropriate resources are booked as required while deployment work is in progress.
- Lead weekly project status meetings to ensure all parties are inline with progress and next steps.
- Track project progression and measured milestones to help ensure timely delivery.

Trustwave Network Engineer

- Provide input in requirements gathering to tailor Splunk technology solution to Client environment.
- Provide expertise in deployment and customization of deployed hardware and software.
- Provide product knowledge transfer to Client. This supplements formal Splunk technology training with specifics of how solution was customized for Client's network.
- Provide standard product documentation, as necessary.
- Provide all Trustwave deliverables for signoff.