Trustwave®

SERVICE DESCRIPTION

Enterprise Penetration Testing

Overview

Trustwave's enterprise penetration testing service ("**Service**") provides large organizations with access to onshore, remote delivery of global, CREST-accredited tests from Trustwave SpiderLabs. A SpiderLabs Technical Account Management team member (TAM) oversees delivery of the Service. The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Confirmation between Trustwave and Client.

Service Features

The Service includes the following features:

Technical Account Manager (TAM)

Trustwave will provide a dedicated onshore TAM. The TAM acts as a point of contact (POC) and is responsible for:

- Scoping assistance per test based on the number of days required to accomplish each test
- Scheduling Client tests
- Escalating Client requests or issues
- Providing quality assurance across the program by ensuring that issues have the same ratings across all tests
- Assisting Client with interpretation of the testing results
- Conducting quarterly business reviews (QBRs)
- Running ad-hoc client presentations
- Performing up to ten (10) percent of the penetration testing (if applicable). The remainder of the penetration testing will be conducted offshore in Manila.

Client Obligations

For Trustwave to provide this feature of the Service, Client will:

- Assign a POC to act as the primary liaison between Trustwave and Client.

CREST- Accredited Processes

Trustwave is CREST Member Company. Trustwave will perform the Service under the CREST name utilizing CREST consultants. All Trustwave delivery locations are CREST-accredited, including Trustwave's center of excellence in Manila.

Delivery

Services

Trustwave will deliver one or more of the following test types remotely as part of the Service:

- Internal Infrastructure
- External Infrastructure
- Web Application Testing (External & Internal)
- API Testing (External & Internal)

The following test types are not included in the Service (although they can be offered and scoped separately):

- Red and Purple Teaming
- On-site delivery beyond ad-hoc reporting and QBR's
- Managed Vulnerability Scanning (MVS)
- Bespoke Testing
- Testing on a staff augmentation basis

For "internal" testing, where Trustwave cannot directly access the resource, Trustwave will provide a Virtual Report Penetration Testing (VRPT) unit to facilitate remotely executed testing. A VRPT is a Client-installed device that allows Trustwave to securely access resources that are not directly accessible via the internet. For "external" testing, where Trustwave can directly access the resource, Trustwave will not provide a VRPT.

Reports

Trustwave will grant Client access to the Trustwave Fusion platform, from which Client may view and download its penetration testing (PT) report. The Trustwave Fusion platform also supports an application programmable interface (API), from which PT results can be exported and then digested into Client's internal ticketing systems for accurate and more automated vulnerability tracking and mitigation.

Client Obligations

For Trustwave to provide this feature of the Service, Client will:

- Install and configure the VRPT under Trustwave instruction, if applicable

Core Trustwave Features

The Service includes the following core features which are standard to many of Trustwave services:

Trustwave Fusion Platform

The Trustwave Fusion platform is Trustwave's proprietary cloud-based cybersecurity platform. Client will be automatically enrolled in the Trustwave Fusion platform as a part of the Service. Client will have access to the following on the Trustwave Fusion platform:

- Vulnerability findings and support tickets
- Client's reports and dashboards
- Request methods for change support and management
- Multiple methods for Client to securely communicate with Trustwave and the ability to upload

documentation, security policies, and more

Additional Information

The Service, which is only available for high-value call-off contracts and is subject to a minimum committed spend of $250,000 USD over the Term of the contract (which may be multi-year), will be based on the number of tests multiplied by the number of days required to complete each test, also known as testing-days-effort. Trustwave may aggregate days effort into “buckets” of small, medium, or large by application or infrastructure size or test criticality, subject to negotiation with the Client. Trustwave will ensure that the effort associated with these buckets is pre-agreed with the Client. Client may not roll over or extend unused but committed contract spend beyond the Term.

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 Statement of Work or Order Confirmation between Trustwave and Client.