Trustwave®

SERVICE DESCRIPTION

Emergency Incident Response

Overview

Trustwave's Emergency Incident Response service ("**Service**") provides Client with access to a team of experts capable of assisting in the technical investigation of a recent cybersecurity incident. 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 Phases

The Service is comprised of the following phases:

Phase 0 – Contact

Prior to Trustwave commencing the Service, Client will call Trustwave's publicly available Breach Hotline number or use a dedicated email contact point. Client should provide Trustwave with the details relating to the requested investigation assistance and their desired outcomes. Trustwave and Client will work together to scope, price, and document the Service in a SOW or Order Confirmation.

Phase 1 – Engagement

Trustwave will assist Client with the technical investigation of the cybersecurity incident indicated in the applicable SOW or Order Confirmation ("**Incident**"). This may include the following activities by Trustwave (depending upon what is legally permitted within the relevant jurisdiction(s) or what is applicable to Client):

- Use of remote agents and remote analysis of data supplied by Client
- Deployment of Trustwave representatives to onsite locations (to be determined solely by Trustwave)
- Electronic break-in compromise (cause, source, and extent) determination
- Computer forensics (laptop, desktop, servers, and disk imaging)
- Network forensics
- Active network monitoring
- Malware analysis
- Keyword searching, data culling, and electronic discovery
- Ransomware support
- Remediation consulting

Client Obligations & Acknowledgements

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

- clearly disclose the nature of the Incident and provide ongoing updates as facts change;
- provide Trustwave with access to its systems as necessary to perform the Service;

- remain in communication with Trustwave through the duration of the Service;
- deliver to Trustwave any requested information, data, logs, code, artefacts, or telemetry relating to or needed to further the Service;
- provide Trustwave with all relevant documents that are required to conduct the investigation;
- provide Trustwave with any available and applicable decryption keys or passwords required to access the data if encryption is used within the environment under investigation; and
- keep Trustwave informed of any developments in the investigation including progress reports, problems encountered, changes in the aims, or closure of the investigation.

  Where additional or extended services are required, Client acknowledges that Client may need to purchase additional services.

Trustwave Obligations

For this phase and subject to the above, Trustwave will:

- lead the technical response to the Incident in line with the requirements of Client's IR management team (IRMT) which are identified to Trustwave in writing;
- advise the Client on the nature of Trustwave's recommended response and its containment efforts;
- capture and analyze relevant data in order to work towards providing Client's IRMT with an understanding of:
  - nature of the Incident
  - root cause of the Incident
  - impact and extent of the Incident
- advise Client's IRMT on methodologies and technologies to assist in the investigation, and their deployment;
- advise Client's IRMT on remediation activities; and

Phase 2 – Reporting

Following completion of Phase 1, Trustwave will deliver a final report detailing the nature, scope, conduct, and outcomes of its investigation and its recommendation and conclusions.

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 Confirmation between Trustwave and Client.