

Service Description

Emergency Incident Response

Overview

ISecuris's Emergency Incident Response service ("Service") consists of an allotment of hours that may be purchased for ISecuris to assist in the event of a cybersecurity incident. ISecuris provides Client with access to a number of experts capable of assisting in the technical investigation of a cybersecurity event. The following description sets out the Service's parameters, which may be further modified by an applicable SoW between ISecuris and the Client.

Service Features

ISecuris once contacted by a prospective Client will "Scope" out the incident. The scoping will confirm:

- The scale of the incident
- Goals of any investigation
- An initial estimate of hours
- A contact number within ISecuris in case of emergency.

When proceeding beyond scoping and officially engaging, ISecuris will provide the Client with next steps, which may include:

- Analysis of data either captured through remote software or provided by the client.
- Computer forensics (laptop, desktop, servers, and disk imaging)
- Network forensics
- Active network monitoring
- Malware analysis
- Ransomware support
- Remediation consulting

Client acknowledges that ISecuris only commits to providing the Service through remote delivery. ISecuris may recommend onsite delivery at its sole discretion. Any onsite delivery will be agreed upon between ISecuris and the Client.

Client acknowledges that additional hours may be needed to ensure a complete response by ISecuris.

ISecuris Requirements

- Subject to Client fulfilling its obligations, ISecuris will:
- Assign a lead investigator and respond to the Incident in a timely manner;
- Triage the incident and work with the Client to determine the appropriate next steps to investigate the Incident;
- summarize the nature of ISecuris's recommended response and its containment efforts;
- Capture and analyze relevant data in order to work towards providing the Client with an understanding of:



- ◆ Nature of the incident
- ◆ Root cause of the incident
- ◆ Impact and extent of the incident
- Advise the client on methodologies and technologies to assist in the investigation.
- Advise the client on remediation activities; and
- Produce a final report detailing the background, conduct and outcomes of the Service.

Client Requirements

For ISecuris to provide a comprehensive service, the Client is expected to:

- Clearly disclose the nature of the incident and any updates as the incident changes;
- Provide ISecuris access to necessary systems to perform the Service;
- Remain in communication with ISecuris through the duration of the Service;
- Deliver to ISecuris requested information, data, artifacts or telemetry relating to the Service;
- Where additional or extended services are required, Client acknowledges that they may need to purchase additional services.