Eastbay SOC Statement of Work

This Statement of Work (“SOW”) for the Global Security Operations Center (“SOC”) Service has been entered into pursuant to the purchase agreement between your organization (“You,” “Your” or “Client”) and Eastbay Cloud Services Inc. (“Eastbay”), and is subject to the terms and conditions of the Security Services Subscription Agreement, which can be found at Terms and Conditions | Eastbay I.T. Consulting Inc., as may be amended from time to time (collectively the "Agreement"). Such terms are incorporated by reference as if fully set forth herein.

Eastbay, in conjunction with the services of an approved third party will provide the SOC services in this SOW (“Third Party Provider”). You will be bound to the Terms of Use and Privacy Policies of the Third Party Provider as well. This SOW may change and Eastbay may update this SOW from time to time. It is your responsibility to check this SOW periodically for changes.

1. Service Description

a) Eastbay’s SOC Service provides monitoring, detection, investigation, escalation, and incident support for incidents within the current support toolset and visibility of the managed services. This SOW defines what is in scope, what is not in scope, and client responsibilities. The Client acknowledges and agrees that anything not specifically set forth herein as in scope is deemed out of scope.

2. SOC Services

a) SOC Services vary based on the security products purchased. Product specific variations will be defined in the "In Scope Services" section of this SOW. The following service definitions are common to all services.

2.1 Coverage Hours

a) 24x7: 24 hours a day, 7 days a week coverage

3. In Scope Services

3.1 Incident Investigation and Response

a) The SOC will provide monitoring, detection, investigation, escalation and incident support for all incidents within the current supported toolset and visibility of the managed services.

b) The SOC is responsible for incident monitoring, detection, analysis, investigation, escalation, and incident support. The SOC will be responsible for remote incident analysis and investigation to determine if alerts or security events warrant incident classification. If an event is classified as an incident by the SOC, the SOC will track the incident with You. The SOC will perform incident triage to include determining threat scope, urgency, potential impact and make recommendations designed to allow for remediation.

c) The SOC will remotely investigate initial security events identified by the SOC and escalate as appropriate in accordance with the established and agreed upon Service Level Objectives (SLOs). Events and incidents will be analyzed and investigated using the SOC's standard process and procedures. Escalations will follow established escalation paths and utilize contact information collected during onboarding and documented by SOC.

d) For incidents that are assigned to the Client after analysis, the Client is responsible for escalating incidents back to the SOC that require action or analysis by the SOC.

e) The SOC will be the collection point for additional group inputs for classification of security incidents. The potential exists for other entities to notify the SOC of possible events. In these relatively rare cases, the SOC will ensure outside sources of information are incorporated into established SOC workflow procedures. As events are pulled into the SOC Workflow, it is the SOC's responsibility to create and classify incidents. As the SOC is responsible for incident escalation and response, only the SOC has the authority to classify events or alerts as incidents to ensure due diligence of event investigation and accountability in reporting.

f) During incident investigation the SOC may perform the following activities:

- Perform analysis on client assets / traffic, document results noting attacker profiles.
- Assist in identifying potential impact of incidents on client systems and using available security tools to assist client in determining if data was exfiltrated.
- Document and track events (false positives and false negatives, blacklists, whitelists) within the Eastbay security toolset.
- Escalate incidents to identified client contacts for further remediation.

3.2 Testing of Monitoring and Response Capabilities

a) The Client may test SOC monitoring and response capabilities by staging simulated or actual reconnaissance activity, system, or network attacks, and/or system compromises. Such activities may be initiated directly by Client or by a contracted third party. Client shall notify the SOC testing email at least fourteen (14) days in advance of testing with the expectation that analyst activities will not be notified of testing. Testing performed on newly added (within 60 days) assets or data feeds should be communicated to the SOC via advance electronic or written notice to ensure SOC personnel have properly onboarded new information and that all monitoring and response capabilities are working properly. SLOs will not apply during the period of staged or testing activities.

3.3 Scheduled and Emergency Maintenance

a) Scheduled maintenance means any maintenance that is performed during a scheduled maintenance window or in which Client is notified at least one day in advance. Notice of scheduled maintenance will be provided to the Client's Authorized Point of Contact. Emergency maintenance means any non-scheduled, non-standard maintenance required by SOC. No statement in the section of any Services entitled "Service Level Objectives" shall prevent SOC from conducting emergency maintenance if it is critically necessary for the integrity and security of the Services. During such emergency maintenance, Client's Authorized Point of Contact will receive notification of initialization of the emergency maintenance, and of the completion of the emergency maintenance. The SOC will be relieved of its obligations under the applicable SLOs during scheduled and emergency maintenance.

3.4 File Sample Submissions

a) The EDR and SIEM SOC services may detect suspicious or malicious executable files on endpoints. Sometimes it is necessary to perform additional investigations to understand an attack. In these cases, Eastbay may retrieve file samples of suspicious or malicious files from an endpoint to perform additional analysis.

b) By allowing sample submissions, our analysts are enabled to provide more in-depth analysis and context to their investigations of potential incidents, as well as enhancing the detection and prevention of future incidents that may involve the same file(s).

c) Part of this process may require our analysts to automatically request samples of files, scripts or other source detected in Client environments to perform further analysis. In addition to our own in-house analysis, Eastbay may use outside services including but not limited to:

- VirusTotal
- Opswat MetaDefender
- Joe Sandbox

d) Unless the Client opts-out of File Analysis Submissions, the SOC will request samples from an endpoint and upload potentially malicious files for analysis as needed.

e) By allowing permission for the SOC to upload unknown binaries, SOC Analysts will either manually or automatically upload unknown binaries to outside analysis services:

- Sample binary or its hash representation will be submitted to the appropriate analysis service.
- Terms of Service and Privacy Policy for each service will apply. Terms & Conditions
- The SOC shall not be responsible for this submission or for any act or omission by any online service.

f) You are hereby advised some / most analysis services make the file metadata publicly available, along with scan results from numerous anti-virus products. Service providers may also make the files samples available for download to partners.

3.5 Host Isolation Terms

a) With our EDR offerings, Eastbay SOC has the ability to isolate machines on a Client's network that have an agent installed. The SOC uses host isolation to prevent the spread of malicious code by preventing a compromised machine from communicating to other network devices on the Internet or the Client's network. The isolated machine will maintain connectivity to SOC and allow our analysts to continue investigation without risking other network devices to malicious code or active attacks.

b) Unless the Client opts-out, Eastbay will isolate potentially compromised machines. Eastbay will manually isolate the machine using the installed Endpoint Agent and notify the client of the isolation via an incident for escalation. The machines will remain in isolation until the threat has been remediated or the client has specifically said they accept the risk and request the SOC to remove the isolation.

- The client commits to identifying production impacting servers and assets that are NOT to be isolated unless the client has given written authorization. Client recognizes they assume all risk for non-isolated machines and the spread of any attack profile due to this.

- The SOC commits to isolating machines that are NOT on the unauthorized list only to prevent the spread of malicious code and lateral movement by suspected attackers.

- The SOC will escalate all incidents that require isolation to the client for their visibility and active feedback on the incident.

c) Clients are hereby advised that the SOC has the functionality to isolate machines on your network with installed Eastbay EDR offerings, that the SOC has the ability to use this function to protect the network, and that the isolated machines will lose all connectivity to all other devices on the network.

3.6 Automated Remediation

a) Some incidents can be remediated by the Eastbay EDR agents. These remediation actions are visible in the endpoint console. Clients can opt-out of allowing SOC Analysts to execute the automated remediation actions on affected endpoints. The current remediation actions that can be performed are,

but are not limited to:

- Kill Process
- Quarantine Files
- Remediate Threat
- Rollback Threat

b) Clients are hereby advised that the SOC has the functionality to remediate machines on your network, that the SOC has the ability to use this function to protect the network, and that the SOC is not liable for downtime as the result of remediation actions that were taken.

4. Out of Scope Services

1. The SOC Service does not modify network configurations, including firewalls, nor does it provide support for troubleshooting network performance or function.
2. Fix database corruption issues
3. SOC Service will not perform any virtualizations on a backup solution.
4. Client Training
5. Contacting Client 3rd party vendors for support or security involvement
6. Under no circumstance will the SOC Service engage in financial transactions on Client's behalf
7. Hardware-related issues (hard disk, memory, power supply, etc.). All hardware and/or equipment issues will be escalated to the Client for remediation
8. Issues detected with the Eastbay non-security platforms.
9. Internet service provider (ISP) outages
10. Hardware, software, or ISP vendor ticketing and management

11. On-site support at client locations

12. Anything not specifically identified as in scope.

5. Client Responsibilities

a) Client understands that SOC's performance of the services is dependent in part on the Client's compliance with the requirements of this SOW. The Client understands that it is responsible for timely delivery of the items and information listed in the following sections of this SOW. Additionally, the Client understands that it must perform the tasks, and provide access to Client or Client's employees, consultants, business processes, and/or systems as contemplated herein for SOC to be able to perform such services efficiently. The following list is required for the SOC's ability to perform the Services: The Client shall provide reasonable assistance to the SOC for performance under this SOW, including helping troubleshoot technical issues within the Client's environments as well as any services provided by third parties to the client that may affect the delivery of the Services.

b) SOC services are dependent of the connectivity of the tools utilized. Client is responsible for maintaining a proper Internet connection sized appropriately to handle the load of the SOC tools and monitoring activities on their network and any network supported by the SOC services.

c) Provide SOC with accurate and up-to-date information including, the name, email, landline, and mobile numbers for all designated authorized Client Points(s) of Contact ("POC(s)"). SOC will also supply an accurate and up-to-date list of its POCs for Client.

d) Notify Eastbay at least twenty-four (24) hours in advance of any scheduled maintenance, network or system administration activity that would affect SOC's ability to perform under this SOW.

e) Maintaining current maintenance, supported versions and technical support contracts with Client's software and hardware vendors for any device affected by this SOW.

6.1 Client Environment Failures

a) The Client agrees that the Third Party Provider and Eastbay will not be liable for any failure to provide the SOC Services if such failure is caused by Client's failure to meet the applicable requirements for each Service. At a minimum, Client is responsible for ensuring the following environmental failures do not negatively impact the Services:

- Service interruptions, deficiencies, degradations or delays due to any Client supplied internet or private access whether provided by Client or third parties engaged by Client, or equipment when provided by Client or third parties engaged by Client.

- Failure or deficient performance of Client-supplied power, equipment, services, or systems not provided by Third Party Provider or Eastbay. Client's election to not release a service component for testing and/or repair and to continue using the service component.

- Client's failure to adhere to SOC recommended configurations on managed or unmanaged equipment that affects the Service.

- Client's failure to deploy SOC Agents within monitored networks.

- Service interruptions, deficiencies, degradations, or delays during any period when a service component is removed from Service for maintenance, replacement, or rearrangement purposes by Client's submission without a mutually agreed upon change order form.

- Failure to provide a suitable secure environment for on-premise devices, including, but not limited to secure mounting/racking, appropriate cooling and air handling, secure from theft, loose wires bundled neatly, etc.

- Service interruptions, deficiencies, degradations, or delays in Service caused by a piece of equipment, configuration, routing event or technology required to be operative in order to perform under this SOW that is under the management and control of Client.

6. Service Level Objectives:

Eastbay and Third Party Provider endeavors to provide the following service levels:

- EDR Initial Threat Analysis SLO: Completed within 1 hour of awareness of alert from Third Party Provider to Eastbay and incident created if necessary.

- Perch Initial Threat Analysis SLO: Completed within 4 hours of awareness of alert from Third Party Provider and incident created if necessary.

- Client Created Ticket Initial Response SLO: Varies by priority (Low – 4 hour, Medium – 4 hour, High – 2 hour, Urgent – 1 hour)

    - Method of contact - email defaults to 4 hours, 7am EST to 5pm EST, m-f
    - Calls – Instantaneous – Severity is set on call with investigation, escalation
    - Voicemails are 1 hour SLO
- Voicemail Response: All voicemails to the SOC are classified as Urgent tickets with a 1 hour initial response goal.

7. How to contact the SOC Service:

Client can contact the SOC via Phone or using the methods listed below. Eastbay prioritizes incoming real time alerts and phone calls utilizing the SLOs listed above:

- For Critical Incident Support utilize our SOC emergency call line at:

    Canada: 416-848-9493, Option 1

- For non-urgent requests open tickets by emailing our dedicated SOC Client support address helpdesk@eastbay.ca

The Client shall not initiate calls or chats directly with individual Eastbay SOC Service technicians on their private lines.