Virtual CISO - Security Incident Response Planning

eSentire will review, assess and assist in developing a cybersecurity incident response plan appropriate to Client's business needs and in consideration of regulatory and legal requirements applicable to Client. eSentire will conduct one (1) workshop session with Client to collect information, interview appropriate stakeholders and key or relevant personnel, and develop a scenario framework for assisting Client to develop a cybersecurity incident report plan. Cybersecurity Incident Response Planning may also include:

i. Providing documentation of Client's event defense measures currently in place;
ii. Discussing with Client's subject matter expert(s) to identify "most likely" cybersecurity scenarios (for example, financial loss due to threat or breach, denial of service, viral outbreak of breach, 'threats made);
iii. Meeting with Client's subject matter expert(s) and other appropriate designates (for example, Client's management team, human resources, or information technology personnel, 'business drivers') to confirm approach in developing a cybersecurity incident response plan for Client;
iv. Reviewing Client's existing disaster recovery plan(s) and/or business continuity plan(s);
v. Reviewing any past vulnerability audit(s) or penetration test(s) conducted by or on behalf of Client;
vi. Performing 'dry run' simulations of likely cybersecurity incident scenarios; and
vii. Providing a logbook of responses to initial 'dry-run simulation identified in (vi) above.