Cyber Risk Advisor Services

Services Description.

The Cyber Risk Advisor Services ("Cyber Risk Advisor" or the "Service") is an eSentire service which assists Clients in evaluating and reducing their overall cyber security risk, while also ensuring that Clients benefit from the full outcomes of their eSentire MDR service. The Service relies on collaboration between Client and its eSentire Cyber Risk Advisor, enabling eSentire to provide customized guidance on how Client can improve its overall cyber security posture.

The Cyber Risk Advisor will provide the following outcomes:

- Dedicated Point of Contact. The Cyber Risk Advisor will be Client's dedicated point of contact for technical, deployment, architecture, or service questions. The Cyber Risk Advisor will be familiar with Client's infrastructure, enabling tailored guidance and answers to questions.
- Architecture Review. eSentire will collaborate with Client to understand and document the architecture of all on-prem and cloud-based services. This includes incorporation of the eSentire MDR Service to ensure sensors are appropriately deployed to provide maximum visibility. Architecture documents will be stored by eSentire for future reference during risk reduction roadmap planning.
- Implementation Guidance. eSentire will provide customized deployment guides, to ensure that the eSentire MDR service is appropriately setup within Client 's on-prem and cloud-based infrastructure.
- Operational Review. Post deployment, eSentire will conduct an operational review with Client, including an overview of the workflows for each signal type that is part of Client's eSentire MDR service.
- Alerting Overview. eSentire will provide an overview of the alert workflows and review the alert templates used as part of Client's eSentire MDR service.
- Allow & Block List Recommendations. eSentire will provide recommendations for updates to Client's allow/block lists for various network infrastructure (e.g., Firewalls), based on learnings from investigations performed as a result of signals ingested.
- Insight Portal Overview. eSentire will conduct a walk-through of the Insight Client portal, outlining the metrics and information available to assist Client in understanding the value of its eSentire MDR service.
- Security Tooling Coverage Map. eSentire will collaborate with Client to develop a Security Tooling Coverage Map, which will incorporate both Client owned security tools and eSentire MDR services. This Security Tooling Coverage Map will be used as the basis for identification of gaps in security posture and identification of additional security tools or eSentire MDR signals to mitigate the gaps identified.
- Cyber Risk Reduction Roadmap. Leveraging the Architecture Review documentation and Security Tooling Coverage Map, eSentire will collaborate with Client to develop a Cyber Risk Reduction Roadmap. This deliverable will provide Client the ability to plan and budget for future enhancements to their cyber security tooling, ensuring that Client has appropriate tooling to provide adequate visibility to threats against their on-prem and cloud-based infrastructure.
- Proactive Security Recommendations. eSentire will provide recommendations to changes in the setup, configuration, or deployment of Client's security tooling and/or the eSentire MDR service, based on insights learned from findings during investigations performed.
- Headline Threat/Breach Briefing. eSentire will provide a report outlining our assessment of a high-impact threat or breach event, which has been reported by major news agencies or cyber security publications. At the request of Client, eSentire will also provide a live walkthrough/overview of the threat briefing, to assist Client in understanding the potential impact to their business/infrastructure, should Client be impacted by the threat.

- TRU Positives Overview. At the request of Client, eSentire will provide a live overview of an eSentire "TRU Positives" report. The TRU Positives report covers a recent investigation conducted by eSentire, which resulted in the identification of a threat event for an anonymous Client.
- Weekly Threat Briefing. eSentire will provide a weekly report to Client, outlining threats discovered and any outstanding actions assigned to eSentire or Client.
- Risk Report. eSentire will provide Client with a risk report outlining Client's current risk rating, based on inputs about Client's security awareness program, industry, operating geographies, etc.
- Service Review. eSentire will conduct a monthly service review, which will cover the following:
  - Signal sources subscribed to
  - Deployment status of each signal source
  - License utilization for each signal source
  - Outstanding actions
  - Review of planned Client infrastructure changes which could impact eSentire MDR service
  - Threat trends specific to Client's deployment
  - Review of Cyber Risk Advisor deliverables
- Executive Meeting Support. eSentire will aid Client developing reports, presentation content or other information required for executive meetings, to demonstrate the value of eSentire MDR services and current cyber security posture.
- Annual Business Review. eSentire will conduct an annual business review with Client, at which time the Cyber Risk Reduction Roadmap will be reviewed, to assist Client with budget planning to support investment and approvements to Client's cyber security roadmap.
- Security Tooling Feedback. eSentire will, to the best of its ability, assist Client with the evaluation of new security tooling. This does not include eSentire conducting a Proof-of-Concept deployment of the security tooling. eSentire will assist Client with identifying the cyber security gaps that the proposed tooling would address and the potential effectiveness of the tooling.

Client Responsibilities.

The Cyber Risk Advisor program is Client is responsible for:

- Providing and/or assisting with the development of architecture diagrams for on-prem and cloud-based infrastructure
- Performing the required Client-side setup and configuration for deployment of the eSentire MDR service
- Provide information about Client owned security tooling, which is outside of eSentire's MDR service, to assist with development of Cyber Risk Reduction Roadmaps
- Making the required configuration changes, to address security recommendations
- Participate in meetings required to achieve the outcomes defined above