



What Do We Provide

We provide Consultation and Managed Security Services for clients to implement through any stages of the ISO2700 series accreditation life-cycle. This includes first assessment and gap analysis based on the generally-accepted phases of PDCA (Plan-Do-Check-Act).

- **Scope Definition:** This phase is done with the client's top management to discuss and define in detail the responsibilities, inputs, outputs and deliverables, timelines, deadlines, budget and agreements.
- **Gap Analysis:** We conduct a Gap Analysis of client organization versus the standard.
- **Risk Assessment:** We then identify your critical information assets, classify them and create the asset inventory.
- **Client Readiness:** Next, we assure that the client team and the MR (management representative) are ready to avoid any unnecessary delays when starting the implementation.

LOG MANAGEMENT

■ Log Retention

Provided as a seamless service, the Log Retention service allows the customer to offload the management and maintenance burden while retaining full access to the appliances. It also satisfies security and compliance requirements for log collection, storage and reporting through the capture and aggregation of millions of logs generated every day by disparate assets and data sources.

■ Log Monitoring

The Log Monitoring service monitors, correlates and analyzes your security logs and alerts across virtually any security technology and critical information asset in your environment. 24x7 vigilant event log monitoring identifies anomalies and helps to respond to threats in real-time. Compliance becomes easier when you can demonstrate controls and produce digitally signed reports containing all the activities from across your environment.



■ Log Monitoring Services Key Benefits:

- **Protect systems and data:** 24x7 monitoring to alert you to threats before damage is done
- **Simplify compliance:** satisfy regulatory requirements using fewer resources
- **Improve response time:** apply action-based insights from rapid analysis of log activity
- **Aggregate information:** capture millions of logs generated everyday by disparate assets

"Advanced" Threat-Intelligence

- We will provide the option for utilization of our private Threat-Intelligence Datasets under a trial period. Metrics will be provided in regards to the effectiveness of the Threat-Intelligence integration.

Support

- We offer a **24/7/365** standard support package via phone or a customer portal, and Web knowledge bases.
- You will also have the substantial benefit of a subject matter expert at your disposal **24/7**. Our Information Security Analyst is experienced in both **General Excepted Log Monitoring Practices and Specific Adherence to Compliance Standards**.



info@johnsnowlabs.com



+1 (302) 786-5227



www.johnsnowlabs.com