Security Information & Event Management (SIEM) Deployment

SCOPE DEFINITION FORM

Infopercept

SECURE • OPTIMIZE • STRENGTHEN

Questionnaire

The Approach and methodology followed for implementing SIEM differs depending on both the type and business use of the systems in question. To ensure that we completely understand your requirements, we request you to answer the following questions about your enterprise's systems, so that the test scope and area of focus can be effectively determined.

- The number of geographically independent locations that will be monitored by the SIEM Solution.

- The number of network segments on each physically/geographically independent location.

- What is the required time period for which logged data/information is to be archived/stored (Number of Years)?

- Is there any compliance requirement, if so which compliance standards is the organization complying with (ISO 27001, PCI DSS, HIPAA Etc.)?

- Does the organization have a SOC team?

- Does the organization have a list of use cases you would like to build in the initial phase of implementation

- Is Redundancy or HA required? If so at what level – Manager or indexers level?

Questionnaire

- Type of source devices from which logs/events will be collected for monitoring. Please fill out the following table for this purpose. Also add the device information that is not listed in the in the table.

Application and Network Devices Information

Type of Device	Network Location (Trusted or DMZ)	Quantity

Questionnaire

Please add your custom application and device information in the following columns

Type of Device	Network Location (Trusted or DMZ)	Quantity

Infopercept

SECURE • OPTIMIZE • STRENGTHEN

Corporate Office:
Infopercept Consulting Pvt. Ltd.
H-1209, Titanium City Center, Satellite, Ahmedabad-380015.
India.

www.infopercept.com | Follow us on -