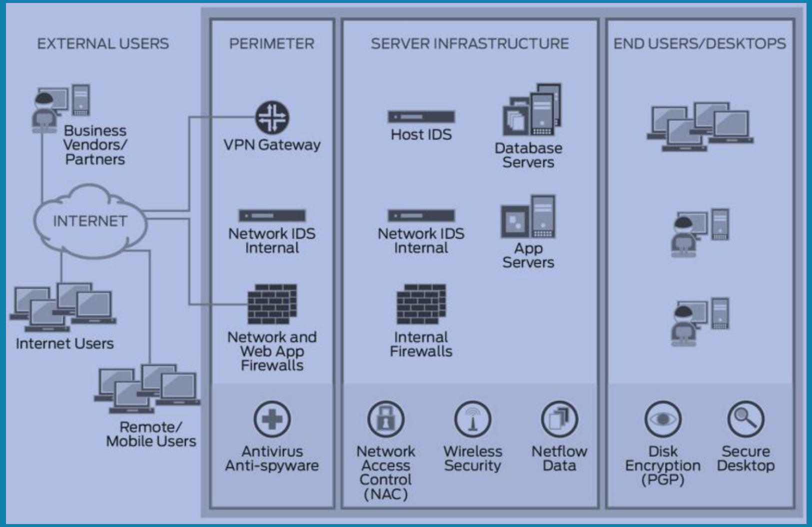
SIEM CHALLENGES AND LIMITATIONS



DISCLAIMER

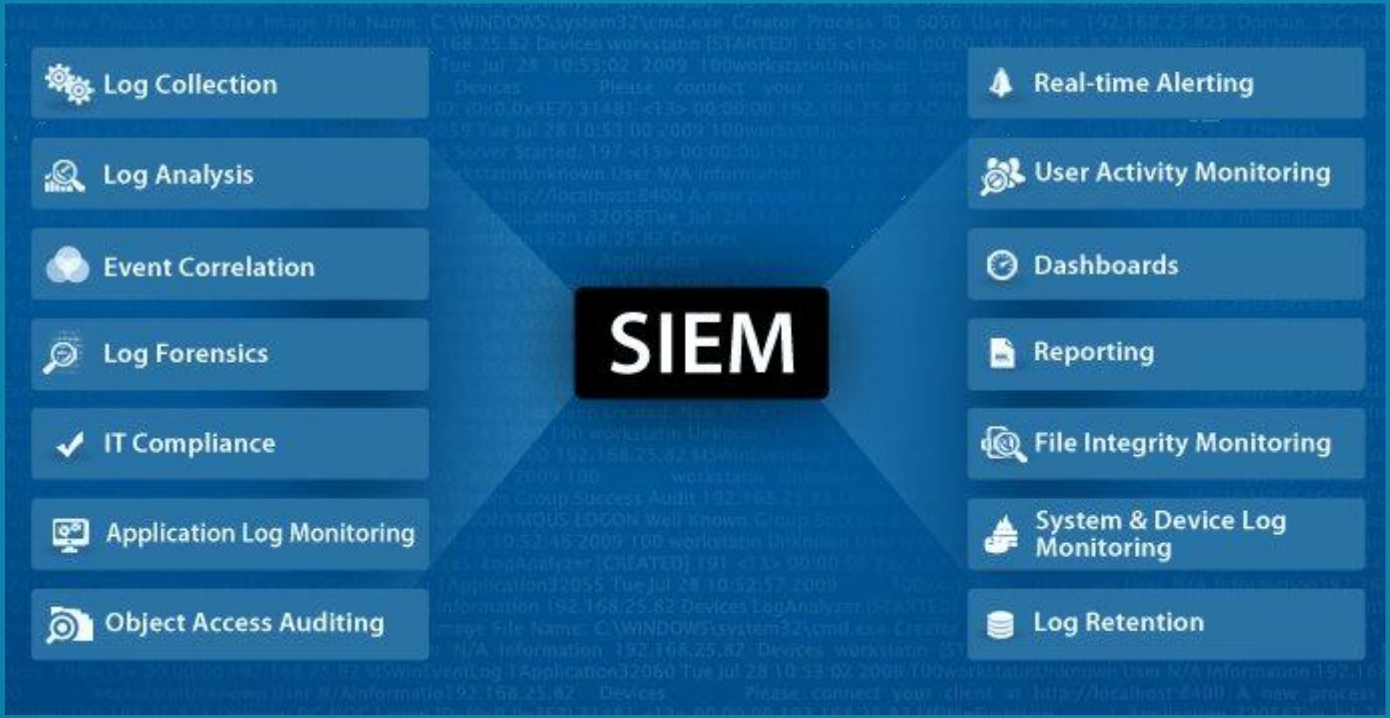
This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

SIEM SOLUTIONS



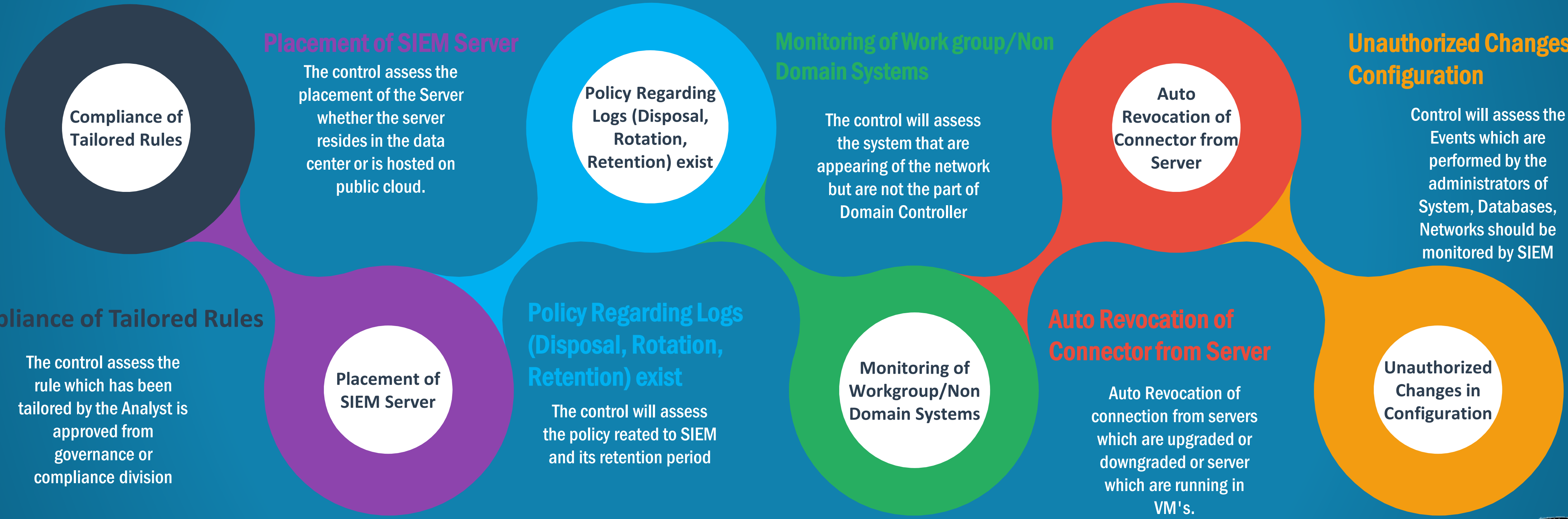
SIEM

- Log Collection
- Log Analysis
- Event Correlation
- Log Forensics
- IT Compliance
- Application Log Monitoring
- Object Access Auditing
- Real-time Alerting
- User Activity Monitoring
- Dashboards
- Reporting
- File Integrity Monitoring
- System & Device Log Monitoring
- Log Retention

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

Ubaid Jafri

SIEM SOLUTION SECURITY ASSESSMENT CHECKLIST


Compliance of Tailored Rules
Placement of SIEM Server
Policy Regarding Logs (Disposal, Rotation, Retention) exist
Monitoring of Workgroup/Non Domain Systems
Auto Revocation of Connector from Server
Unauthorized Changes in Configuration

Compliance of Tailored Rules

The control assess the rule which has been tailored by the Analyst is approved from governance or compliance division

Placement of SIEM Server

The control assess the placement of the Server whether the server resides in the data center or is hosted on public cloud.

Policy Regarding Logs (Disposal, Rotation, Retention) exist

The control will assess the policy reated to SIEM and its retention period

Monitoring of Work group/Non Domain Systems

The control will assess the system that are appearing of the network but are not the part of Domain Controller

Auto Revocation of Connector from Server

Auto Revocation of connection from servers which are upgraded or downgraded or server which are running in VM's.

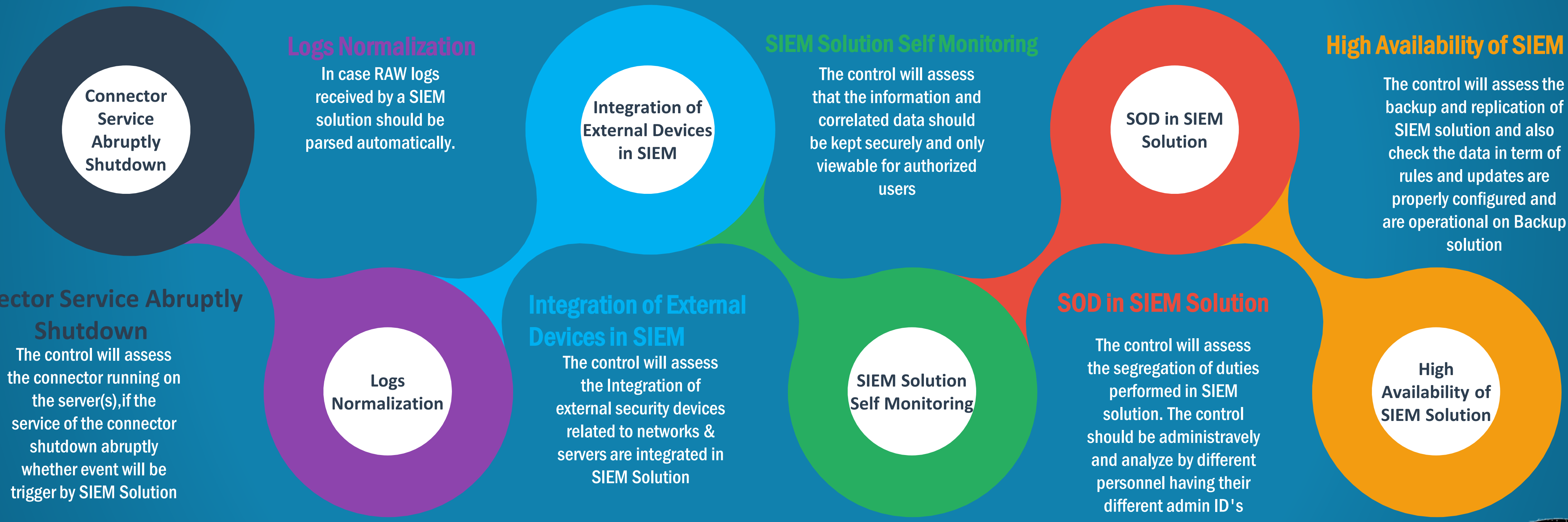
Unauthorized Changes in Configuration

Control will assess the Events which are performed by the administrators of System, Databases, Networks should be monitored by SIEM

ALL RIGHTS RESERVED

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

SIEM SOLUTION SECURITY ASSESSMENT CHECKLIST(CONT'D)


Connector Service Abruptly Shutdown
Logs Normalization
Integration of External Devices in SIEM
SIEM Solution Self Monitoring
SOD in SIEM Solution
High Availability of SIEM Solution

Connector Service Abruptly Shutdown

The control will assess the connector running on the server(s),if the service of the connector shutdown abruptly whether event will be trigger by SIEM Solution

Logs Normalization

In case RAW logs received by a SIEM solution should be parsed automatically.

Integration of External Devices in SIEM

The control will assess the Integration of external security devices related to networks & servers are integrated in SIEM Solution

SIEM Solution Self Monitoring

The control will assess that the information and correlated data should be kept securely and only viewable for authorized users

SOD in SIEM Solution

The control will assess the segregation of duties performed in SIEM solution. The control should be administravely and analyze by different personnel having their different admin ID's

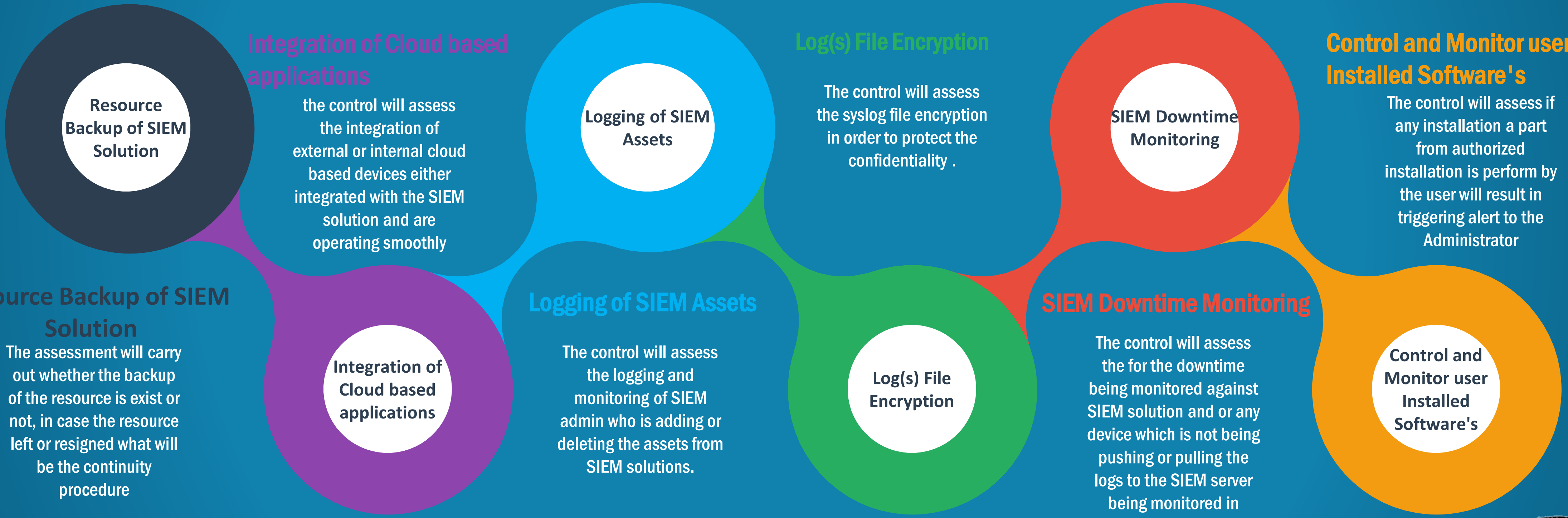
High Availability of SIEM Solution

The control will assess the backup and replication of SIEM solution and also check the data in term of rules and updates are properly configured and are operational on Backup solution

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

Ubaid Jafri

SIEM SOLUTION SECURITY ASSESSMENT CHECKLIST(CONT'D)


Resource Backup of SIEM Solution
Integration of Cloud based applications
Logging of SIEM Assets
Log(s) File Encryption
SIEM Downtime Monitoring
Control and Monitor user Installed Software's

Resource Backup of SIEM Solution

The assessment will carry out whether the backup of the resource is exist or not, in case the resource left or resigned what will be the continuity procedure

Integration of Cloud based applications

the control will assess the integration of external or internal cloud based devices either integrated with the SIEM solution and are operating smoothly

Logging of SIEM Assets

The control will assess the logging and monitoring of SIEM admin who is adding or deleting the assets from SIEM solutions.

Log(s) File Encryption

The control will assess the syslog file encryption in order to protect the confidentiality .

SIEM Downtime Monitoring

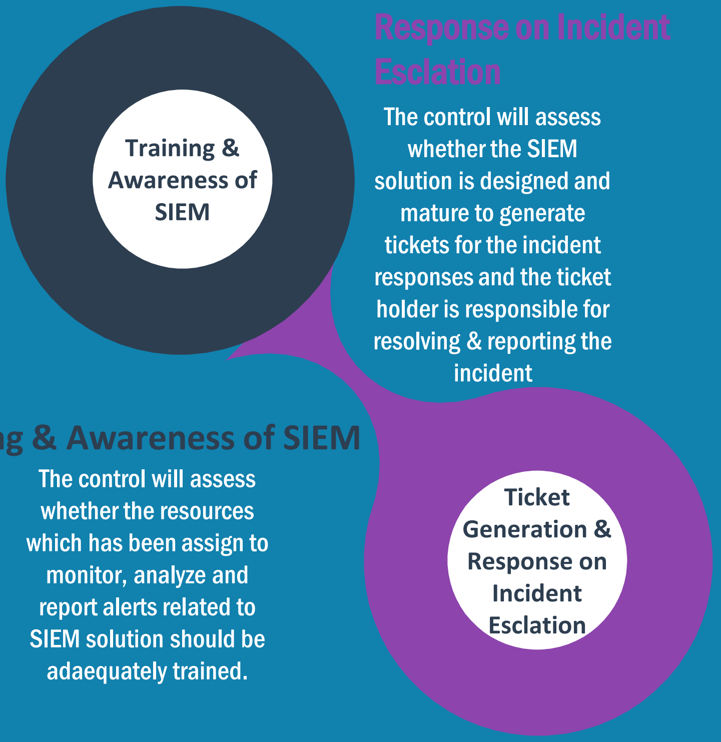
The control will assess the for the downtime being monitored against SIEM solution and or any device which is not being pushing or pulling the logs to the SIEM server being monitored in downtime event or not?

Control and Monitor user Installed Software's

The control will assess if any installation a part from authorized installation is perform by the user will result in triggering alert to the Administrator

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

SIEM SOLUTION SECURITY ASSESSMENT CHECKLIST(CONT’D)



Training & Awareness of SIEM

Ticket Generation & Response on Incident Esclation

Ticket Generation & Response on Incident Esclation

The control will assess whether the SIEM solution is designed and mature to generate tickets for the incident responses and the ticket holder is responsible for resolving & reporting the incident

Training & Awareness of SIEM

The control will assess whether the resources which has been assign to monitor, analyze and report alerts related to SIEM solution should be adaequately trained.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

THANK YOU

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.