مـــــرافـــــق
MARAFIQ

SOC

Security Operations Center Challenges And Implementation

Tariq Al-Walah
IT Security Supervisor , CISMP , BCCPP,BCCPA , Security +

مـــرافـــق
MARAFIQ

SOC

Security Operations Center Challenges And Implementation

Agenda

- Necessity to Monitor
- Challenges
- Approach
- Triad of Security Monitoring
- Focus Areas
- SOC Service catalog
- SOC as Project
- Manpower Selection
- Modes Of Operation

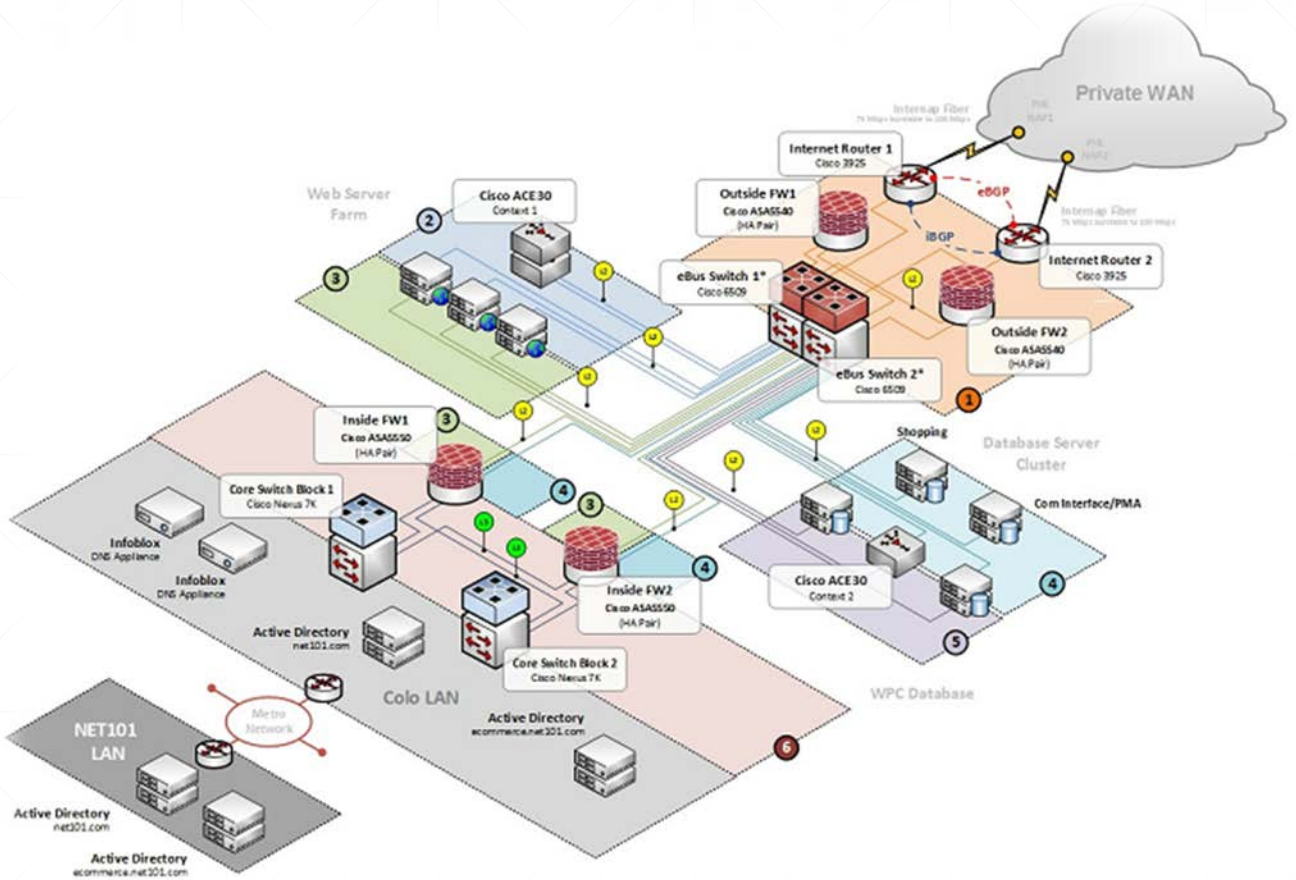
مرافق MARAFIQ

SOC

Security Operations Center Challenges And Implementation

Necessity to Monitor

- Nation Scale Attacks
- Huge amount of logs
- Versatile technologies
- Slow Incident Response
- Distributed security Silos
- Compliance needs



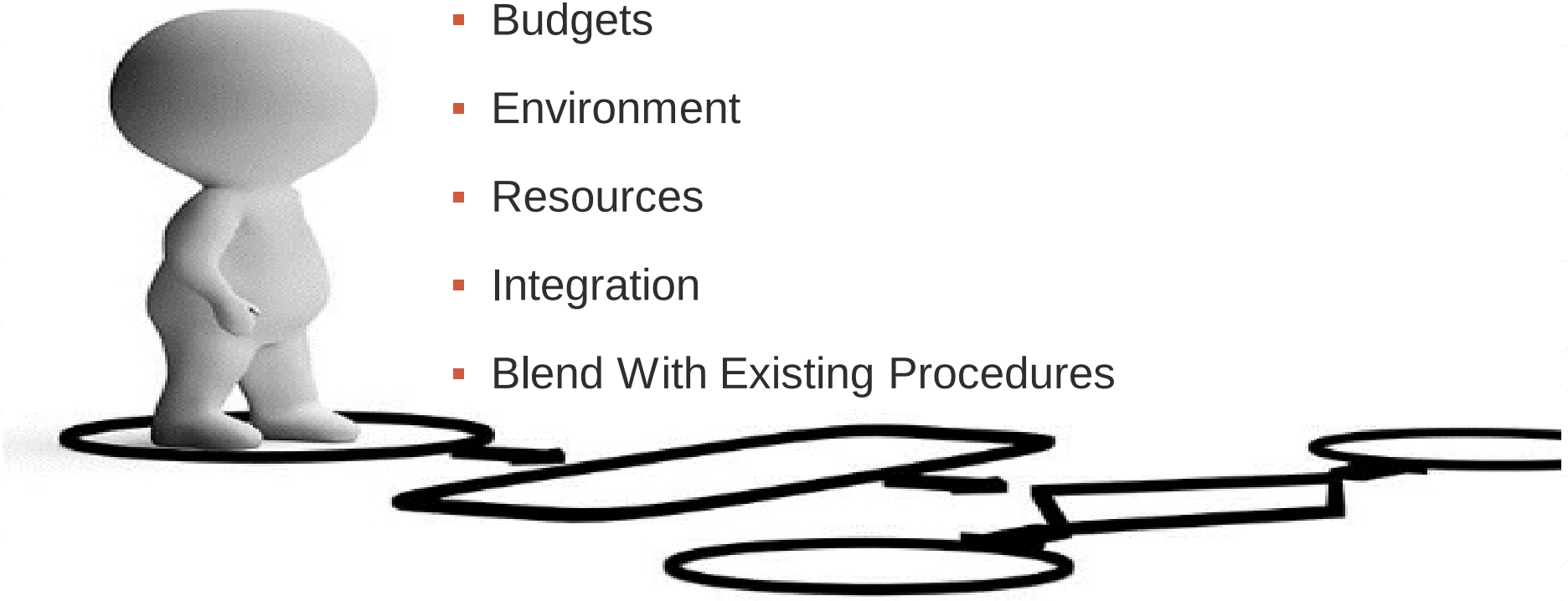
مـــرافـــق
MARAFIQ

SOC

Security Operations Center Challenges And Implementation

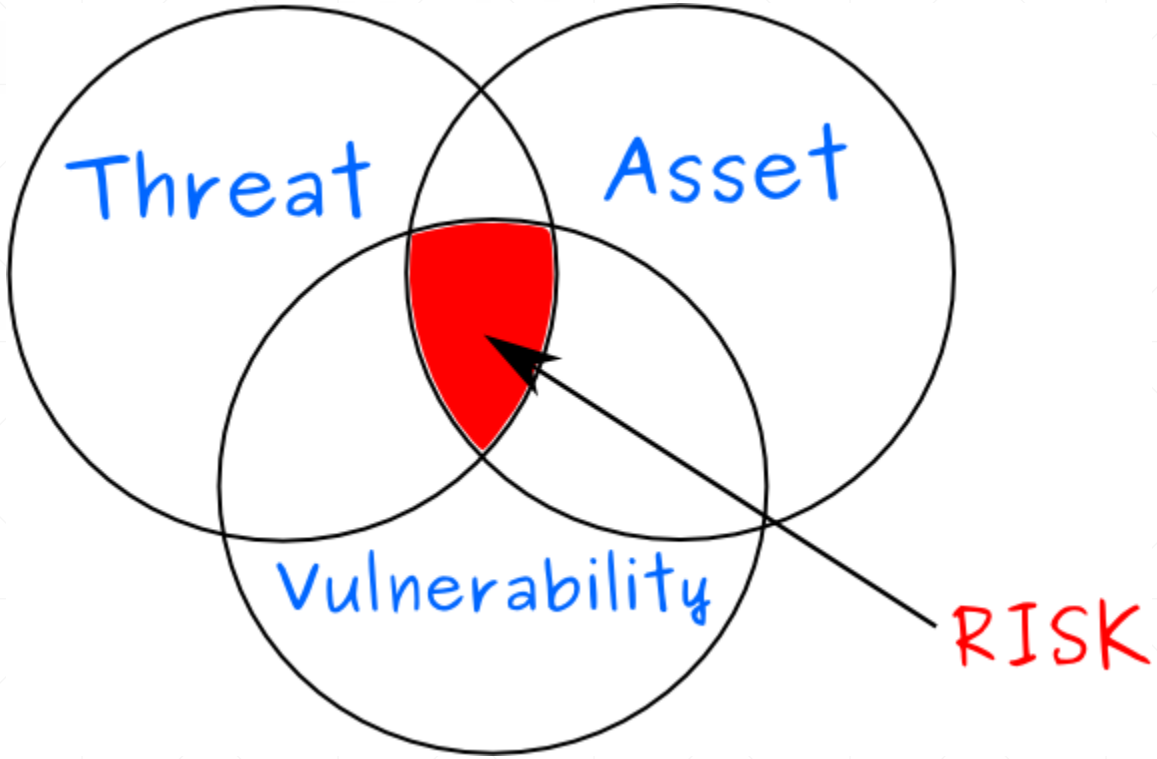
Challenges

- Management Support
- Budgets
- Environment
- Resources
- Integration
- Blend With Existing Procedures



Approach

- Risk Assessment.
- External Security Audit.
- Cybersecurity Steering Committee.
- Site visits.
- Develop SOW.
- Bidding.
- Awarding.



مـــرافـــق
MARAFIQ

SOC

Security Operations Center Challenges And Implementation

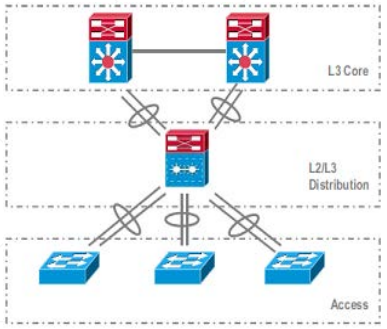
Triad Of Security Monitoring

مـــرافـــق
MARAFIQ

SOC

Security Operations Center Challenges And Implementation

Focus Areas



Network Infrastructure

SIEM

ERP Servers

IT Infrastructure Servers

Security Appliances

مـــرافـــق
MARAFIQ

SOC

Security Operations Center Challenges And Implementation

Service Catalog

مـــرافـــق
MARAFIQ

SOC

Security Operations Center Challenges And Implementation

Building SOC As a Project

- Planning and Design
- SIEM Implementation
- SOC Security Framework Development
- Man power deployment
- Live Operations
- Tuning And Continuous Development

مـــرافـــق
MARAFIQ

SOC

Security Operations Center Challenges And Implementation

Manpower Selection

مـــرافـــق
MARAFIQ

SOC

Security Operations Center Challenges And Implementation

Modes Of Operation

Outsourcing

Co-sourcing

Insourcing

Thank you