National System Integrator

TACTICS FOR SUCCESSFULLY MANAGING A SECURITY OPERATIONS CENTER

Simeon Kartselyanski

Team Lead Security Operation Center

Security Operation Center

86.63

Million PPS

600GB

Most Massive DDOS Attack in Bulgaria
(information is based on ledaer in DDoS Proteciton)
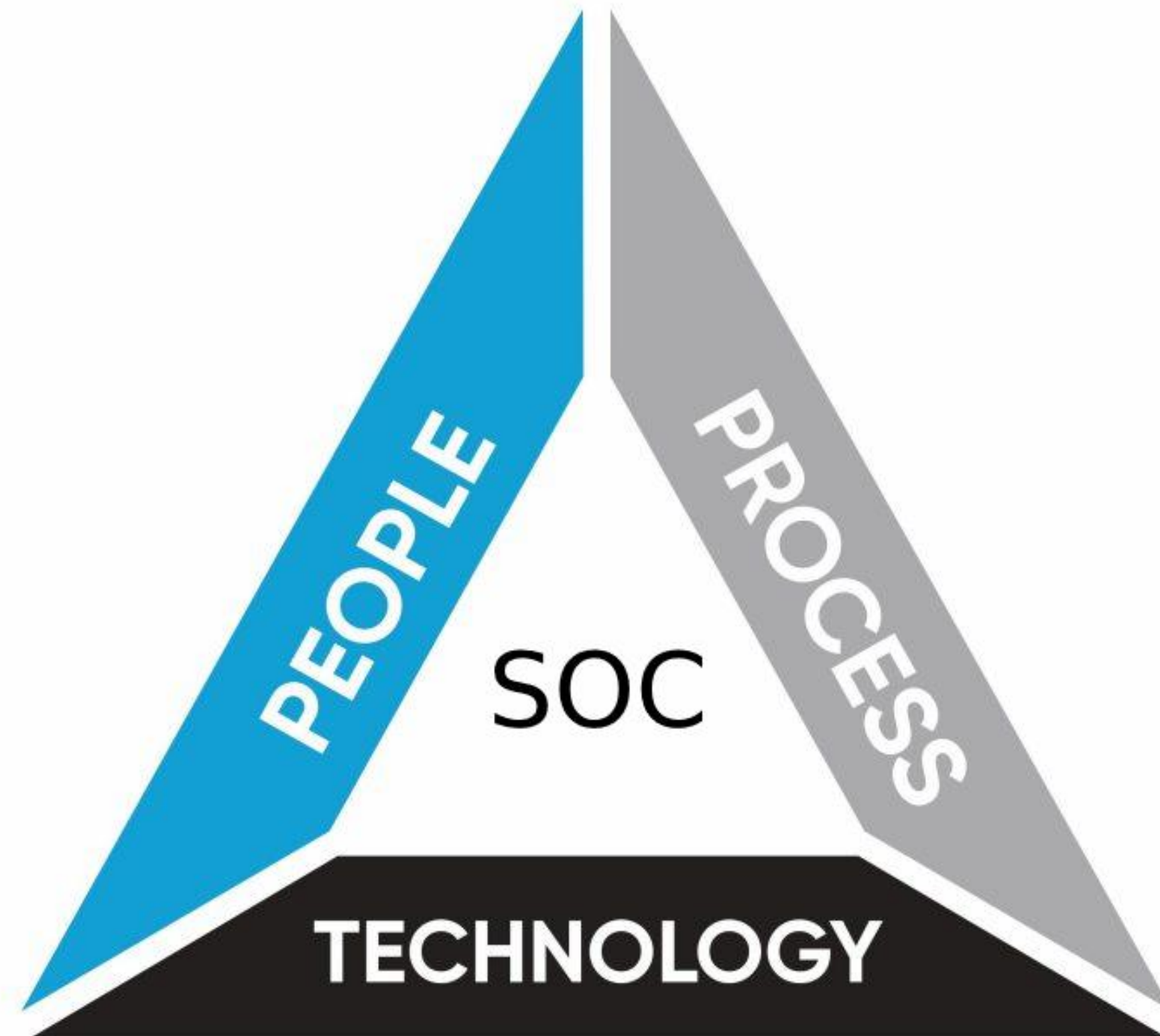
20

Security Experts

15+

Best Security Technology Platform by Vector

15000+

Protected Endpoints

50

Years a leader in the delivery of ICT services in the public sector.

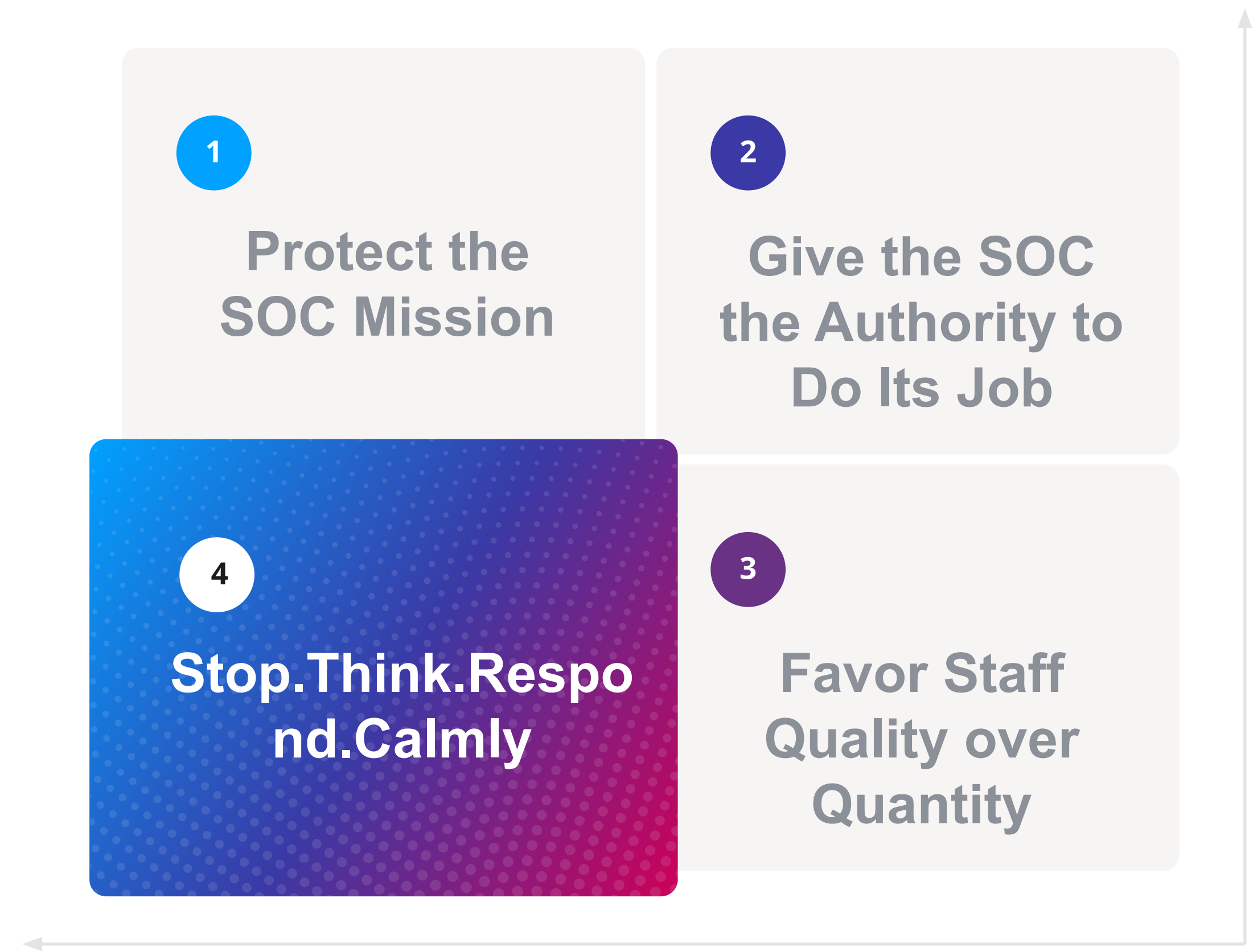# SOC - PYRAMID OF PAIN-YES OR NO?

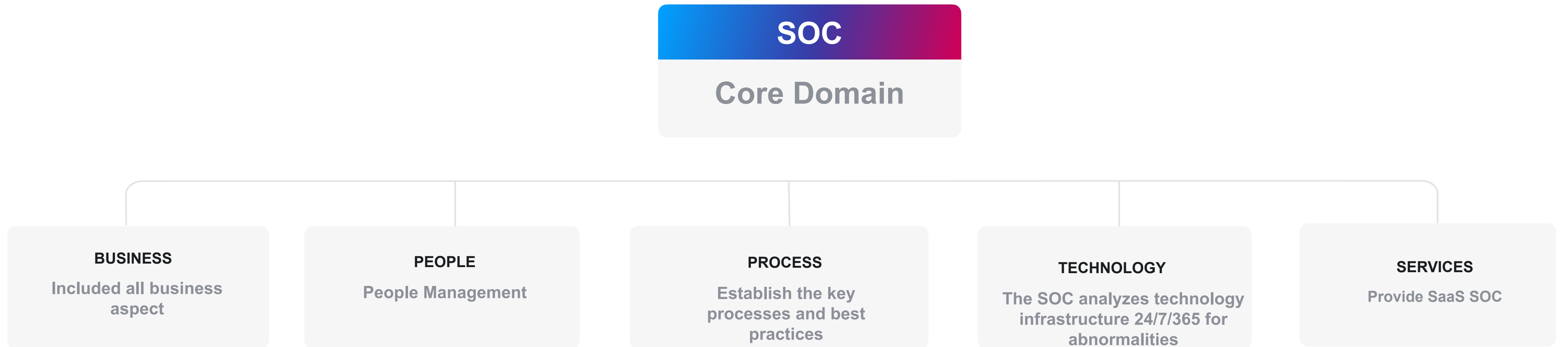**Key Success Factors in SOC**

1.People

2.Technology

3.Process

TACTICS FOR SUCCSESS SOC

Creating a SOC can be a daunting task. After all, it is meant to be the first and last point of call when it comes to system security. However, you can build an effective SOC team that meets the unique needs of your organization. It takes time, effort and careful evaluation, but the reward is a reliably secure infrastructure.

1 **Protect the SOC Mission**

2 **Give the SOC the Authority to Do Its Job**

4 **Stop.Think.Respond.Calmly**

3 **Favor Staff Quality over Quantity**

Assessment Model for Security Operation Center

SOC

Core Domain

BUSINESS

Included all business aspect

PEOPLE

People Management

PROCESS

Establish the key processes and best practices

TECHNOLOGY

The SOC analyzes technology infrastructure 24/7/365 for abnormalities

SERVICES

Provide SaaS SOC

Thank you

for your
attention