ISSA

Information Systems Security Association International

www.issa.org

ISSA Thought Leadership Series: A Cure for the Common SOC

February 14, 2008

Today's web conference is generously sponsored by:

JASK

www.jask.ai

A Cure for the Common SOC

Moderator

Candy Alexander, CISSP CISM

Candy has 30 years of information security experience working for various high-tech companies. She has held several positions as CISO (Chief Information Security Officer) for which she developed and managed Corporate Security Programs. She is now working as a Virtual CISO and Executive Cyber Security consultant assisting companies large and small to improve their potential risks through effective security initiatives.

Candy was the chief architect for the Cyber Security Career Lifecycle for the ISSA (Information Systems Security Association) and is a long-standing Director on the International Board. She is also the inaugural President and past Board Member of the ISSA Education and Research Foundation. Candy has also served as Vice President of Education and Vice President of International Relations for the ISSA. She remains a loyal member at the local level with the New England Chapter and the ISSA - New Hampshire Chapter.

Candy has received numerous awards and recognition, including that of Distinguished Fellow of the ISSA, ranking her as one of the top 1% in the association, and she was inducted into the ISSA Hall of Fame in 2014. She also had the opportunity to be a featured speaker for the IT Security Symposium at the United Nations, and received an invitation to the Offices of the White House to speak on the importance of security awareness to the President's "Cyber-Czar" staff.

A Cure for the Common SOC

Speaker

Rocky DeStefano, JASK

Rocky DeStefano serves as VP Product at JASK and is an IANS faculty member. Previously he acted as Cloudera's subject matter expert on cybersecurity. Mr. DeStefano was a member of the USAF and subsequently supported AFCERT as part of the Incident Response Team. Rocky founded and led the Global Security Operations Center for EDS and has supported cybersecurity advancement in notable companies such as ArcSight, NetWitness, RSA and Visible Risk. At every step in his career, Rocky's focus has been to continually enhance visibility and detection solutions to defend the enterprise.

A Cure for Common SOC

Speaker

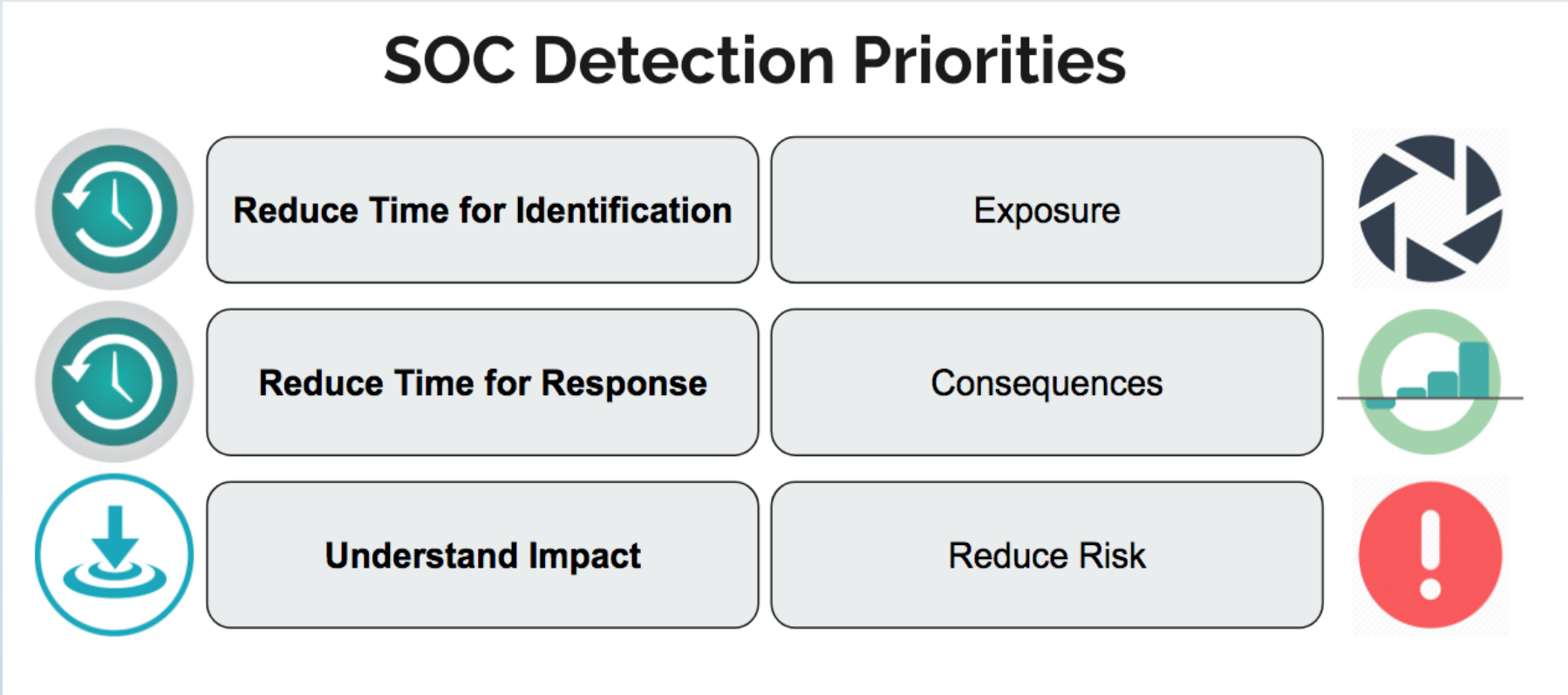
Vince Campitelli II

Vince has extensive experience in the converged fields of information technology and risk management. As a Regional Partner with Coopers & Lybrand (now PWC) he was a member of a small team of partners who led the adaptation of technology into the traditional fields of accounting and auditing.
Post public accounting, he applied his mastery of risk management and technology with leading Wall Street and Healthcare organizations including Salomon Smith Barney, Goldman Sachs and McKesson Corporation. He developed and designed risk-based continuous improvement processes to monitor IT business systems and applications that resulted in improvements in operational performance and the reduction in outages and control deficiencies. Most recently, Vince has been consulting with the Office of the CEO of the Cloud Security Alliance (CSA) in supporting enter- prise members apply CSA Security Guidance and Research results into their Cloud adoption and implementation programs.

Vince is an active participant in numerous conferences on Information Security and Risk Management. He also serves on the Advisory Boards of several security advisory and educational organizations.

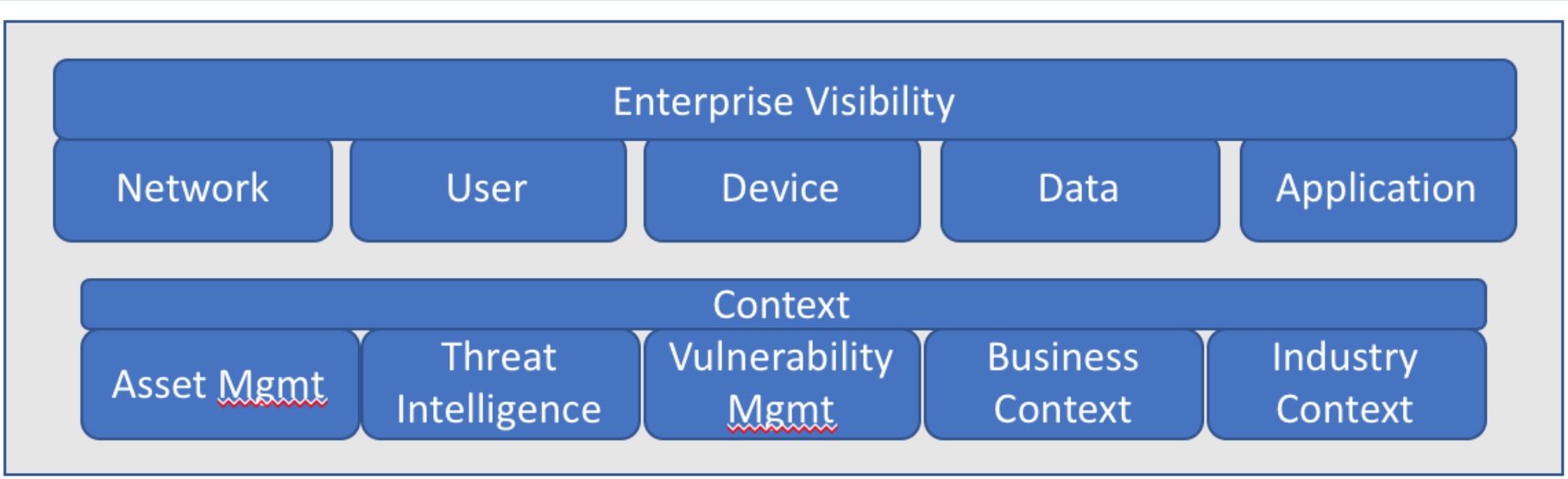
SOC Execution

- What are the core issues that hinder SOC teams ability to execute?



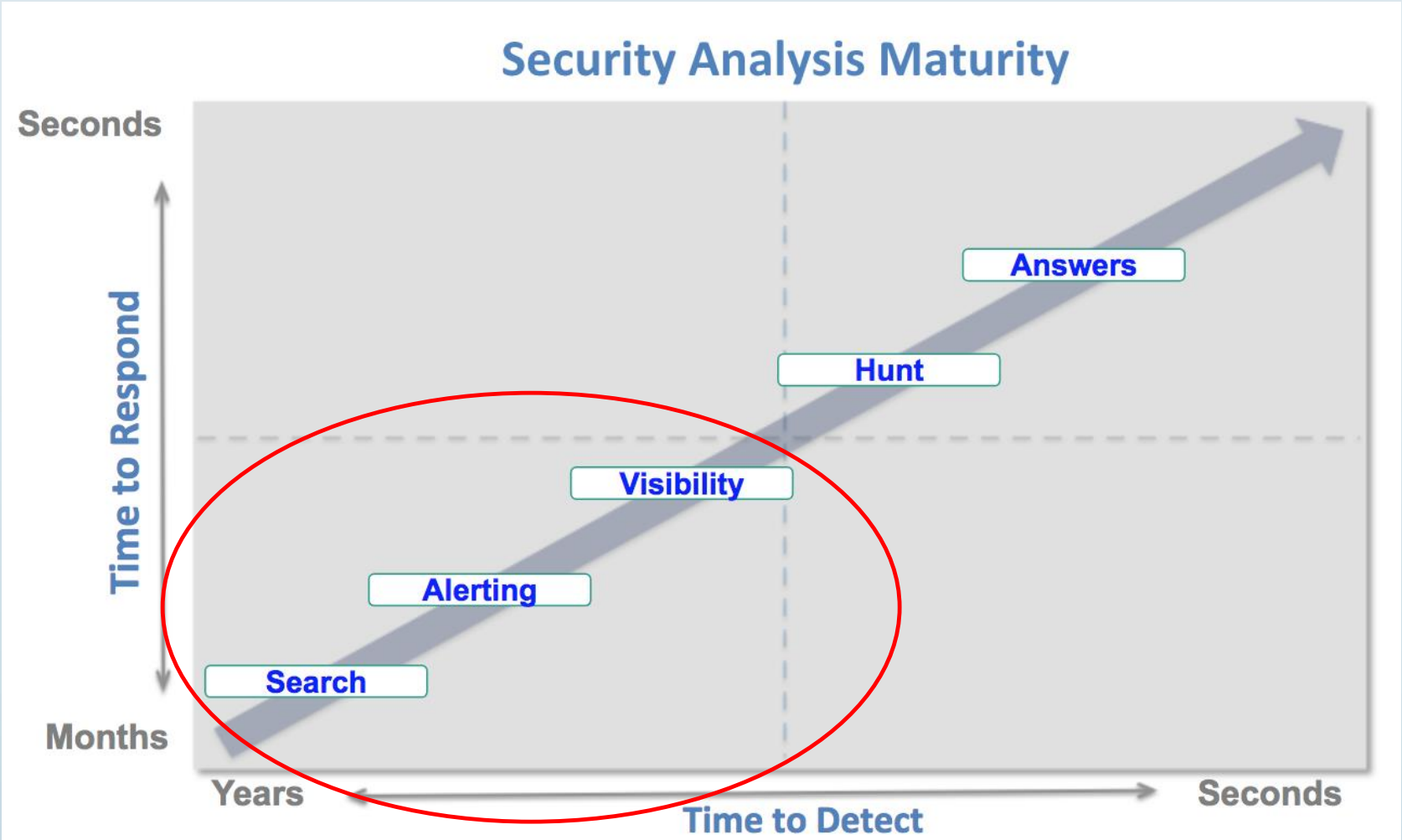
Visibility & Context

- How big of a role do context and visibility play in the success of the SOC team?



Scavenging vs. Hunting

- Instead of validation activities what should SOC analysts focus on accomplishing?



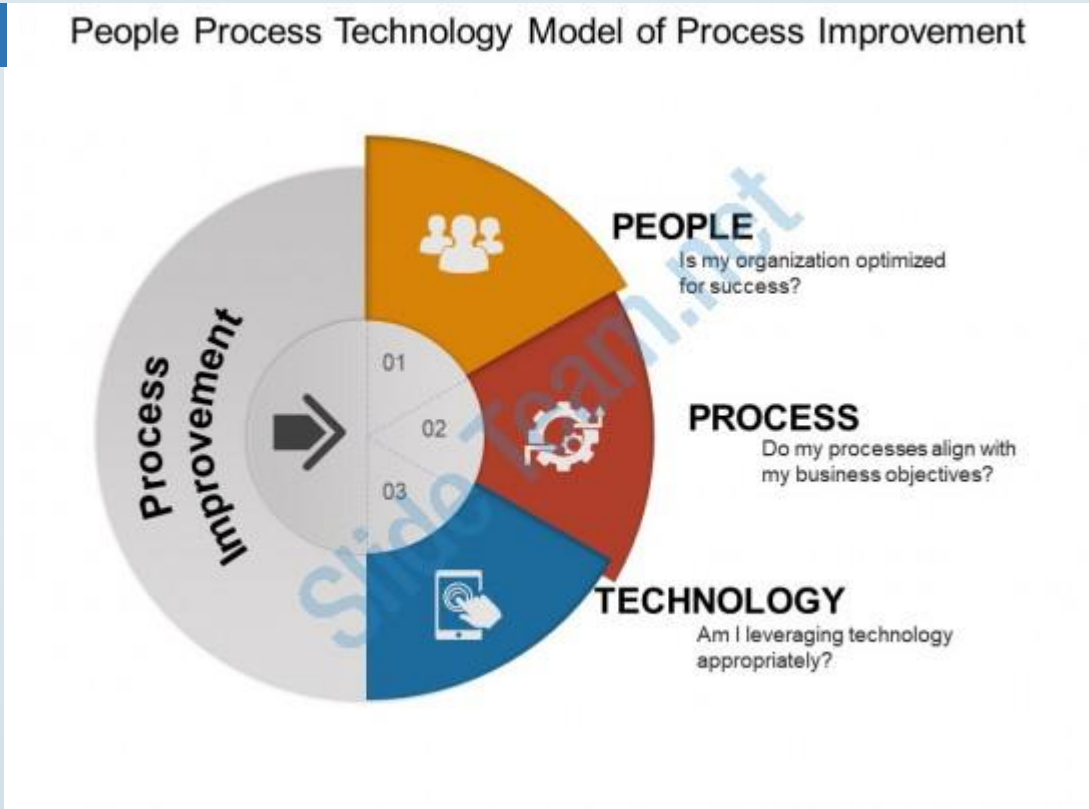
Ideal State of SOC

- Regroup and Rebuild: What would be different?

Enterprise Visibility	Logs, Users, Systems, Networks, Applications, Artifacts, Threat Intelligence, Business Context
Context	Asset, Threat, Vulnerability, Function, Owner, Criticality, Why does this matter to the business or mission?
Speed	Adversaries adjust in seconds, Enterprises weeks/months
Flexibility	Authority to change tools, tactics, visibility and to instrument as needed.
Expertise	Security Analysis, System/Network/Memory Forensics, Malware Reversing, Enterprise Architecture.
Process	Standardized, communicated, trained and robust enough to flex when necessary.

People

1. Shortage of experts
2. Retention/career development
3. Turnover
4. Role enhancement
5. global considerations



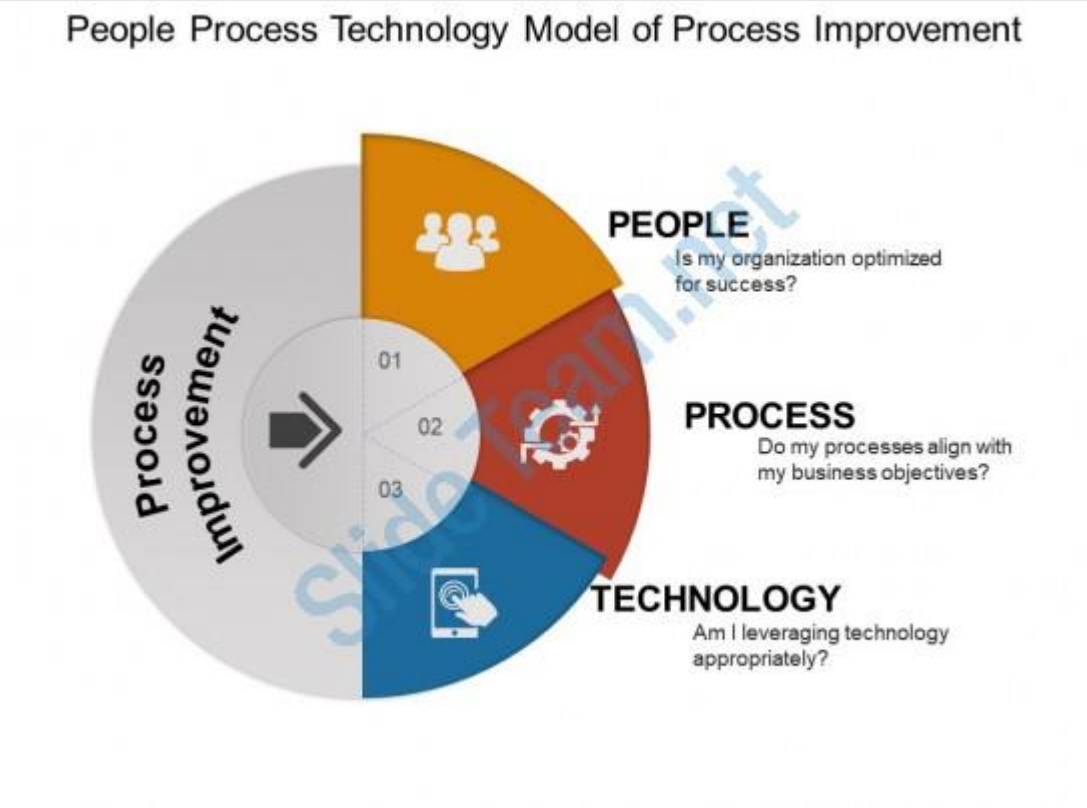
Process

1. Process Complexity

   Architectural
   approach
   scope of processes
   SOC / NOC relationship
   variation in coverage

2. Variation in capabilities

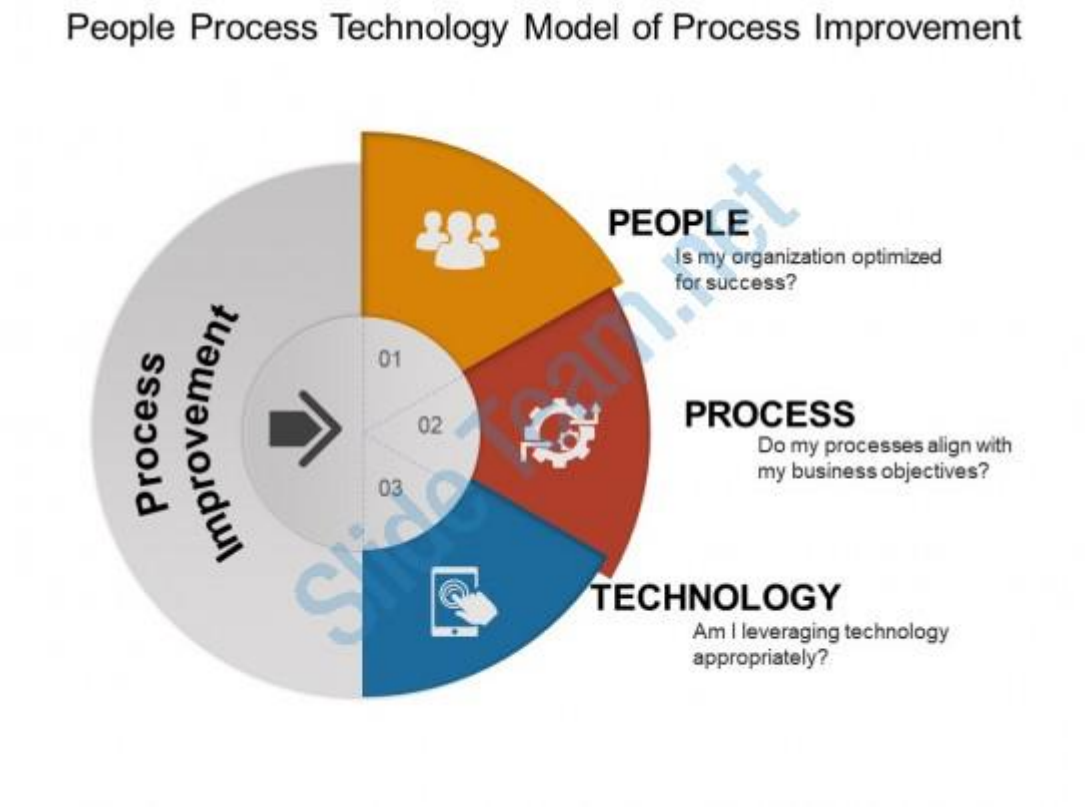
   Prevention
   Detection
   Response
   Logging
   Monitoring
   Analysis
   Intelligence
   Metrics/Performance



Technology

1. **Discipline over technology selection, implementation integration and configuration:**

Standards
Naming conventions
Data validation
Maintenance
User training
Business alignment
Interoperability



ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?