



# MANAGED THREAT FOR OT NETWORKS

Sean Tufts, Aug 2020



# Who We Are

**\$2.4+B**

2019 sales



**7,000+**

Clients served in more than 65 countries



**KKR Owned**

2017

**38**

Offices, SOC's and training centers



**1,900+**

Employees



**OPTIV**

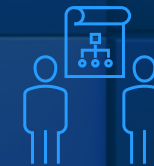
**400+**

Technology partners



**800+**

Field staff dedicated to client success



**~1,600**

Cybersecurity experts



# WHO WE SERVE

**7K+** Clients in  
**65** Countries

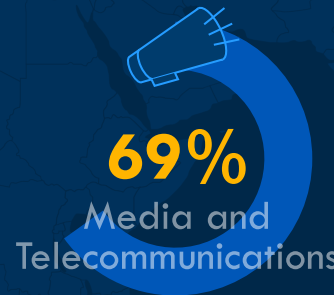
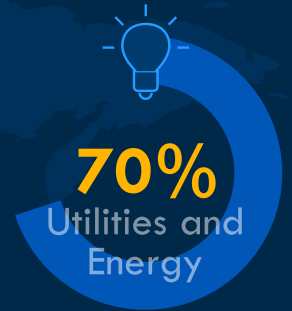
ME, AF, NA, SA, EU, APAC, LATAM

**570+**  
Educational  
Institutions

**830+**  
Government  
Agencies and  
Departments



■ **71%** of Fortune 1000  
■ **77%** of Fortune 500  
■ **81%** of Fortune 100



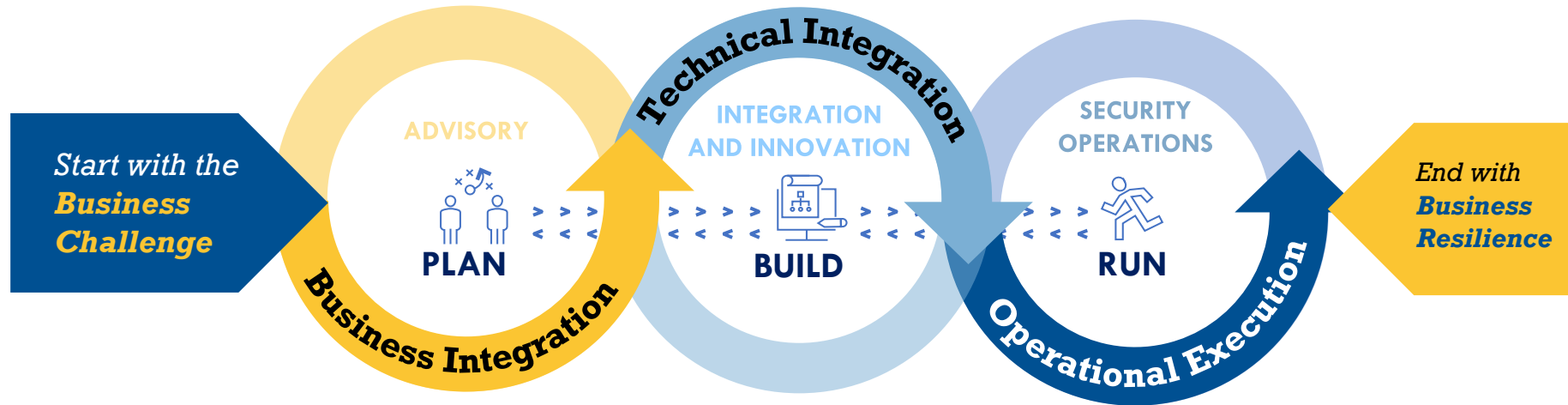
**Fortune 500**  
Industry Client Share



# PLAN, BUILD, RUN



# Outcome



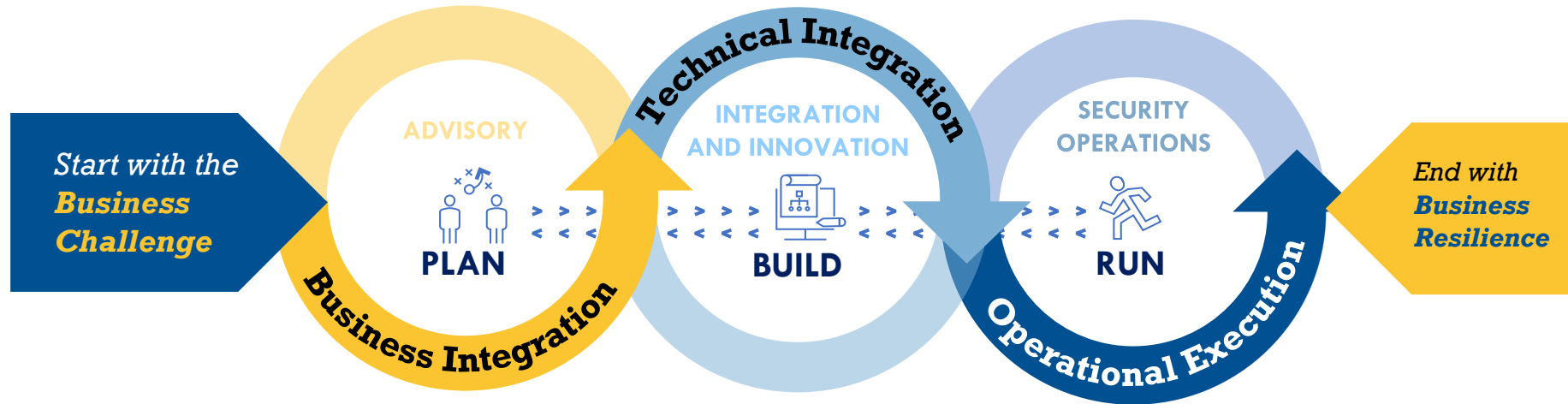
**Challenge:** Building resiliency against cyber disruptions by actively monitoring the environment for threat actors and disruptions from internal operational inefficiencies. Overall, the goal is to shrink the attack surface and reduce the dwell time of malicious actors.

Professional  
install and  
tuning

## **Business Resilience**

- Reduce Cyber risk exposure
- Shrink attack service
- Better alerts with less fatigue
- Reduce dwell time
- Reduce management burden

# Outcome



## Architecture & Planning

*Architecture*  
*Runbook Services*

## Deployment

*On-site*  
*Quick-Start*  
*Silver*  
*Gold*

## Managed

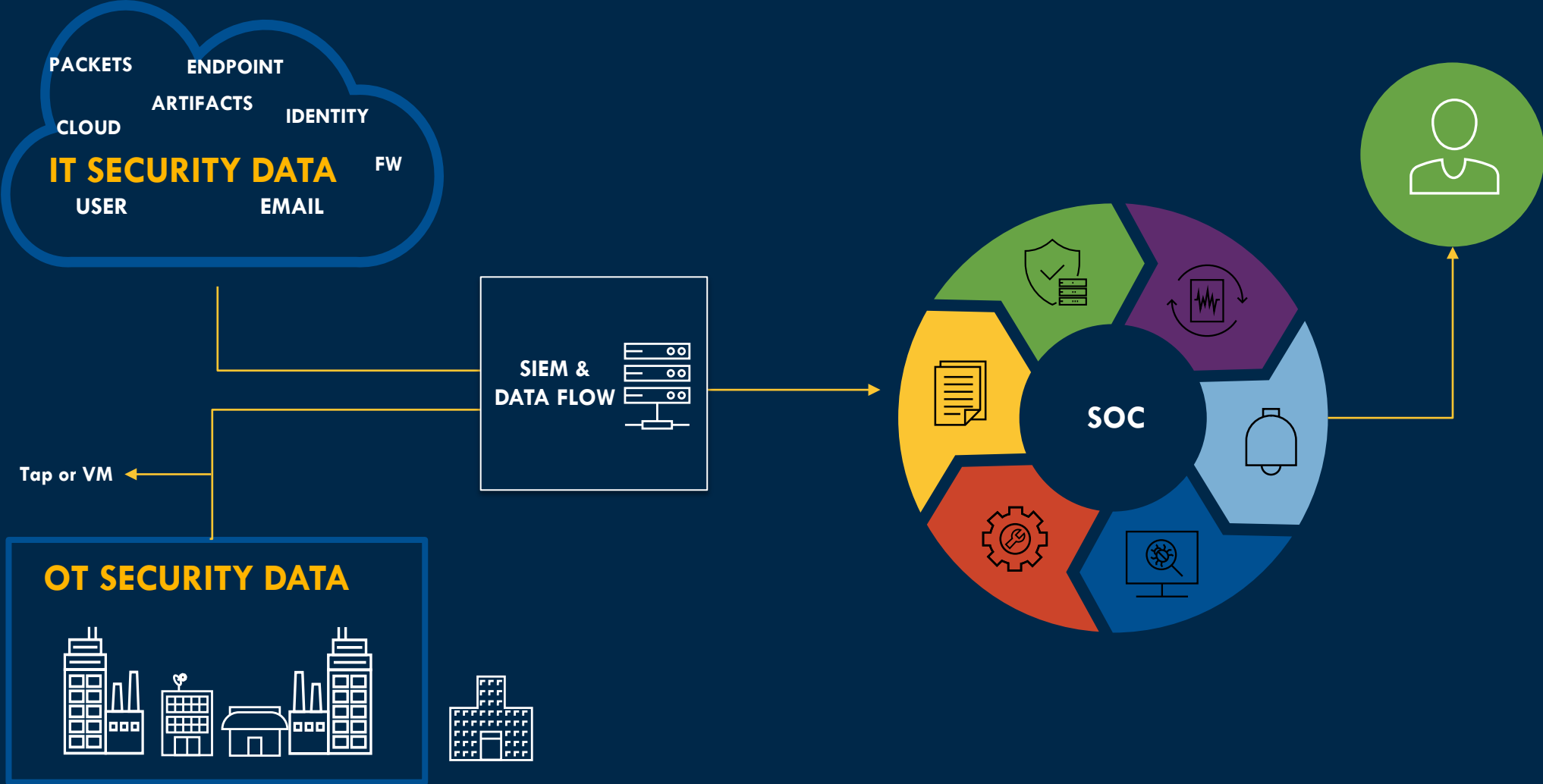
*Threat Management*  
*Platform Support*

# WHAT WE DO



# Deployment Model #1

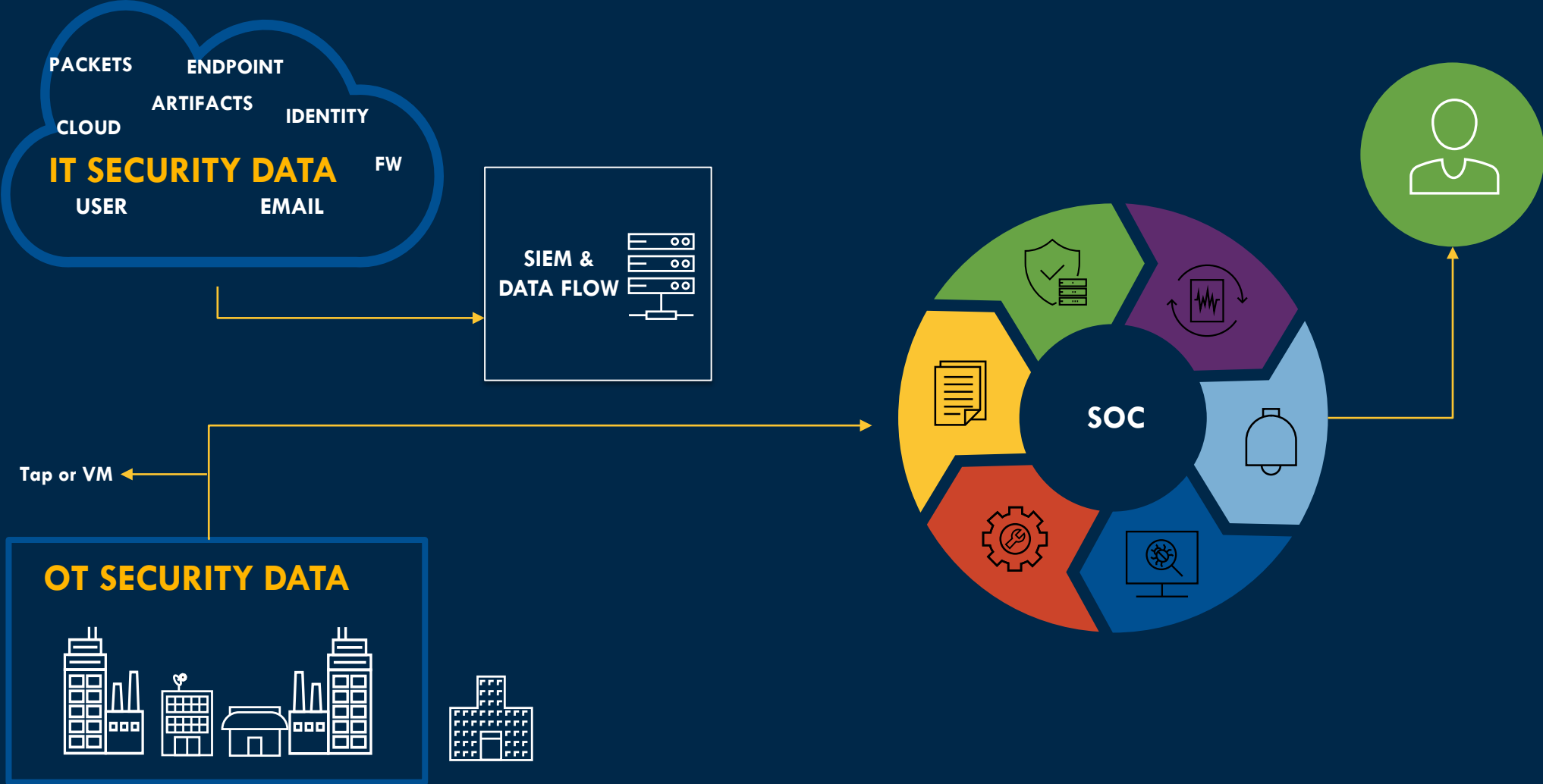
## Integration with existing security tools









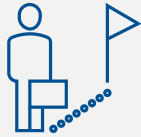
# Deployment Model #2

## Stand-alone OT Monitoring



# HOW WE DO IT

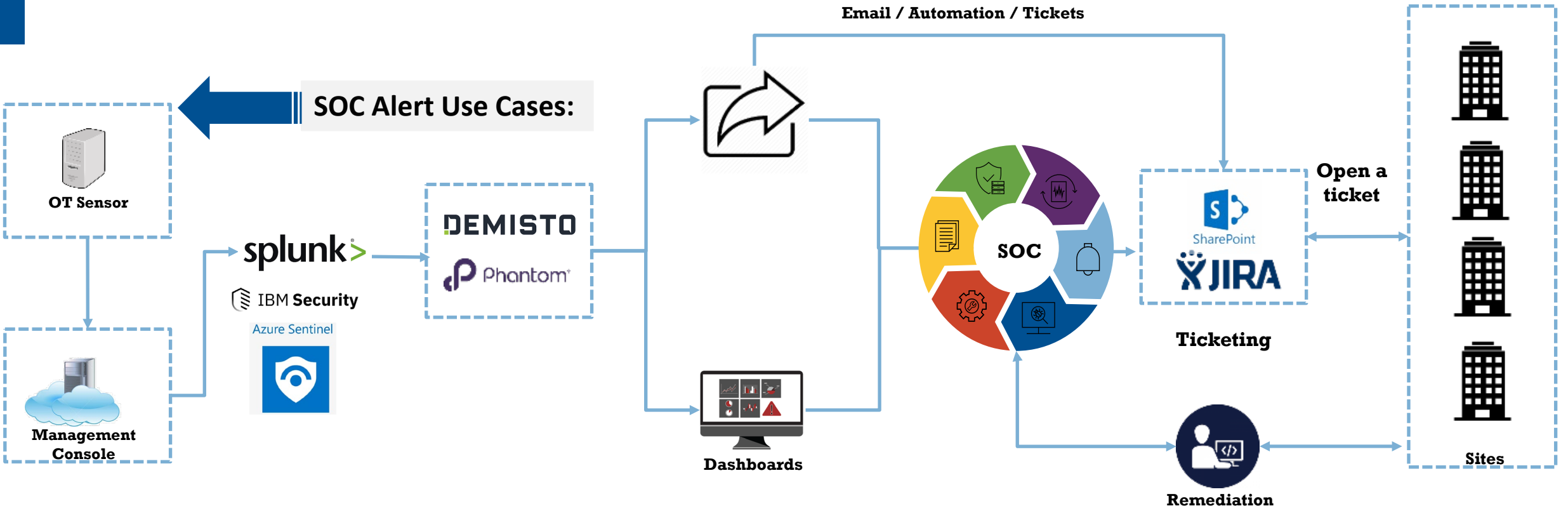


Architecture & Planning		Deployment	Managed	
				
<b>Architecture</b>	<b>Runbook Workshop</b>	<b>Deployment</b>	<b>Managed</b>	<b>Scale at speed</b>
<ul style="list-style-type: none"> <li>• Integrations</li> <li>• Architectures &amp; Sensor location</li> <li>• <b>KPIs</b></li> <li>• Creation of Gold Image</li> <li>• Stake holder identification</li> <li>• Site rollout plan</li> <li>• 2 to 4-week engagement</li> </ul>	<ul style="list-style-type: none"> <li>• Define required use cases</li> <li>• Define alerts and incidents</li> <li>• Identify business requirements</li> <li>• Identify critical processes</li> <li>• Create criteria scoring</li> <li>• <b>Create runbooks for key alerts</b></li> <li>• 4 to 8-week engagement</li> </ul>	<ul style="list-style-type: none"> <li>• On site support</li> <li>• <b>Sensor tuning</b></li> <li>• <b>Alert tuning</b></li> <li>• 3 tiers               <ul style="list-style-type: none"> <li>Quick start</li> <li>Silver</li> <li>Gold</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>24/7/365 alerting and triage</b></li> <li>• Platform support and reporting</li> <li>• Settings and configurations</li> <li>• System health</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Confirm KPIs are met.</b></li> <li>• Identify items for improvement</li> <li>• Expand stakeholders population</li> <li>• Develop Executive Dashboards</li> <li>• Define Phase II</li> </ul>
<b>DEFINE SUCCESS FIRST</b>	<b>RELEVANT CONTENT FOR RELEVANT PARTIES</b>	<b>BUILT IT</b>	<b>24/7/365 ALERTS</b>	<b>MEET GOALS MAKE NEW GOALS</b>

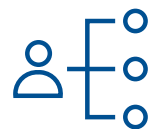
# Runbook Creation



SOC Alert Use Cases:



# DEPLOYMENT OPTIONS



## QUICK START

### Focused on – Standing up the environment

- Fundamentally ensures that the sensor is installed with core elements of related network accounted for
- Remedial initial review of alerting to show sensor is functioning – no depth in investigation
- Listing of alerts provided to client for investigation and resolution
- **Outcomes**
  - Sensors are installed and are ‘working’
  - Lowest cost of the three

## SILVER

### Focused on – Refining Alerts

- Significantly higher touch on installation
  - Enhanced time on asset map analysis
  - Vetting of subnets, external connections, etc.
  - Packet capture and review to validate architecture
- Higher touch on analysis and investigation of alerts – investigation driven by Optiv team with client support
  - Tickets created and comments entered for the Optiv SOC analysts
- Creation of threat reporting, KRI and other collateral
- **Outcomes**
  - Sensors prepared with alert intelligence available for MSS
  - Potential issues addressed that would likely not be identified in Base mode

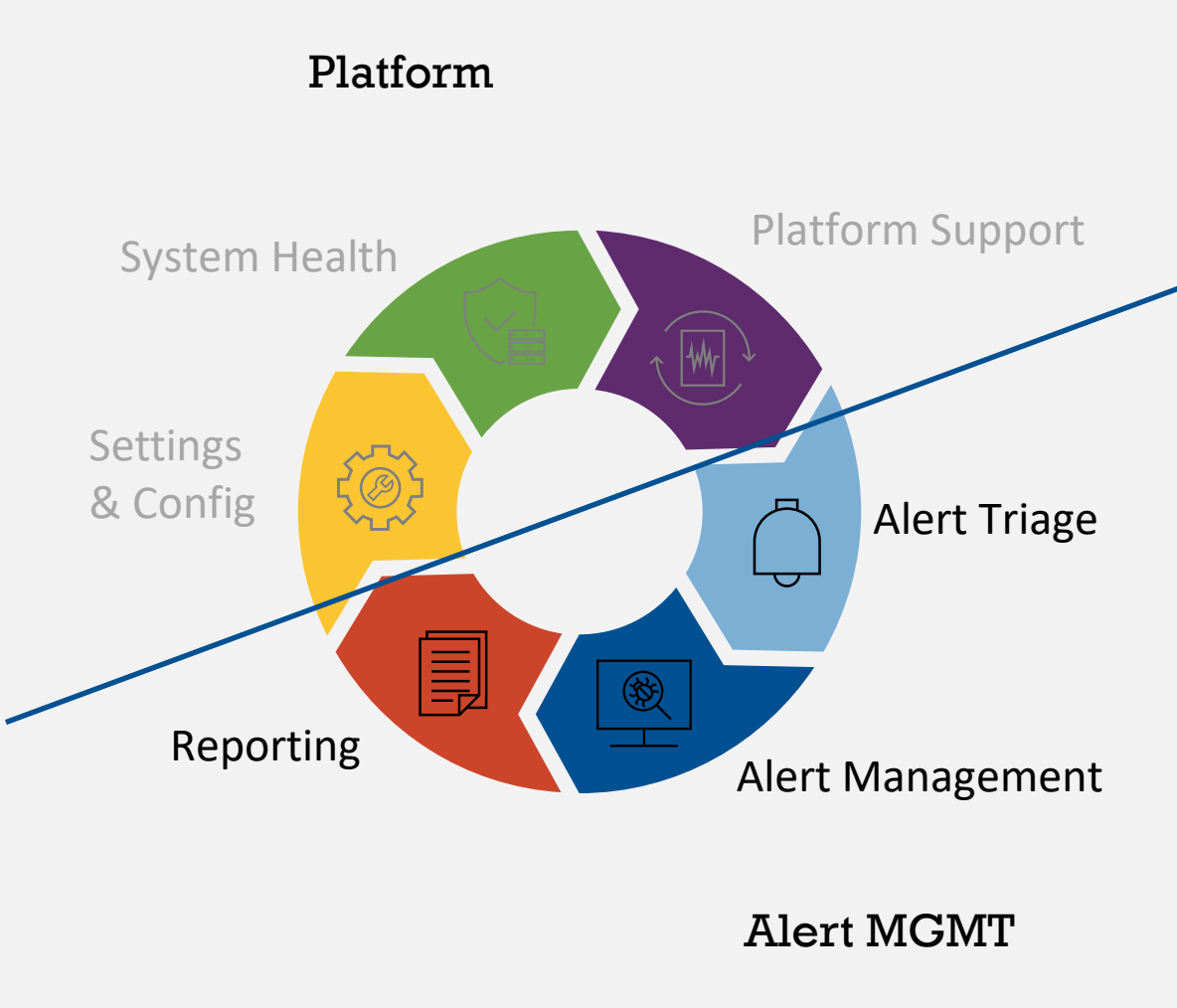
## GOLD

### Focused on – Improving Operations







- Build out of reference architecture
- Increased depth in Sensor tuning
  - Review of firewall integration/config
  - Segmentation recommendations
  - Custom reporting
- Identification of critical asset listing for incorporation into the monitoring process
- **Outcomes**
  - Global deployment that is fully tuned with threat intelligence provided



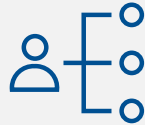

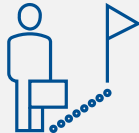
**ON SITE SET UP ALSO AVAILABLE**

# Use Case to Playbook Mapping

Use Case	24/7/365 Monitoring
1. Illegal Function Codes for ICS Traffic 2. Unauthorized PLC Changes 3. PLC Stop	 <p data-bbox="1421 354 1607 396"><b>Platform</b></p> <p data-bbox="1230 539 1513 582">System Health</p> <p data-bbox="1862 511 2201 554">Platform Support</p> <p data-bbox="1200 729 1370 829">Settings &amp; Config</p> <p data-bbox="1982 801 2211 843">Alert Triage</p> <p data-bbox="1281 1029 1472 1072">Reporting</p> <p data-bbox="1849 1058 2219 1100">Alert Management</p> <p data-bbox="1854 1210 2130 1253"><b>Alert MGMT</b></p>
4. Malware Found in Network	
5. Multiple Scans in the Network	
6. Internet Connectivity	
7. Unauthorized device in DCS network	
8. Unauthorized DHCP Configurations	
9. Excessive Login Attempts	
10. High Bandwidth in network	
11. Denial of Service	
12. Unauthorized remote access	

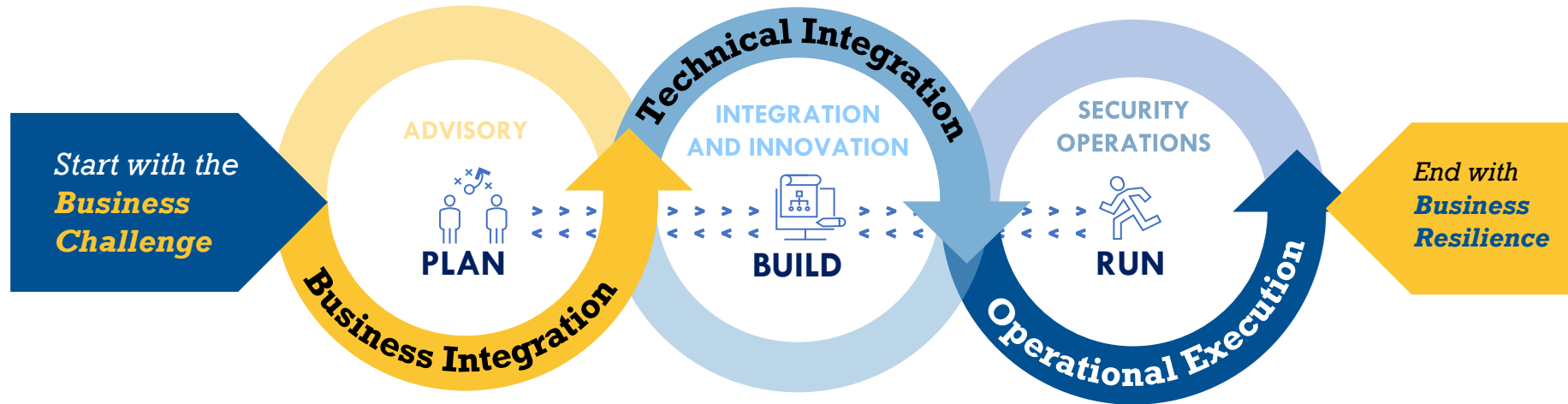
# Use Case to Playbook Mapping

Use Case	Playbooks
1. Illegal Function Codes for ICS Traffic 2. Unauthorized PLC Changes 3. PLC Stop	 A. Unauthorized Changes to ICS Equipment
4. Malware Found in Network	 B. Malware Found in Network
5. Multiple Scans in the Network	 C. Reconnaissance Tool in Network
6. Internet Connectivity	 D. Internet Connectivity
7. Unauthorized device in DCS network 8. Unauthorized DHCP Configurations	 E. Unauthorized / Malicious Activity in Network Performed by a newly discovered Device
9. Excessive Login Attempts 10. High Bandwidth in network 11. Denial of Service 12. Unauthorized remote access	 F. ICS equipment is inaccessible

Architecture & Planning		Deployment	Managed		
					
<b>Architecture</b>	<b>Runbook Workshop</b>	<b>Deployment</b>	<b>Managed</b>	<b>Scale at speed</b>	
<ul style="list-style-type: none"> <li>• Integrations</li> <li>• Architectures &amp; Sensor location</li> <li>• <b>KPIs</b></li> <li>• Creation of Gold Image</li> <li>• Stake holder identification</li> <li>• Site rollout plan</li> <li>• 2 to 4-week engagement</li> </ul>	<ul style="list-style-type: none"> <li>• Define required use cases</li> <li>• Define alerts and incidents</li> <li>• Identify business requirements</li> <li>• Identify critical processes</li> <li>• Create criteria scoring</li> <li>• <b>Create runbooks for key alerts</b></li> <li>• 4 to 8-week engagement</li> </ul>	<ul style="list-style-type: none"> <li>• On site support</li> <li>• <b>Sensor tuning</b></li> <li>• <b>Alert tuning</b></li> <li>• 3 tiers               <ul style="list-style-type: none"> <li>Quick start</li> <li>Silver</li> <li>Gold</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>24/7/365 alerting and triage</b></li> <li>• Platform support and reporting</li> <li>• Settings and configurations</li> <li>• System health</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Confirm KPIs are met.</b></li> <li>• Identify items for improvement</li> <li>• Expand stakeholders population</li> <li>• Develop Executive Dashboards</li> <li>• Define Phase II</li> </ul>	
<b>DEFINE SUCCESS FIRST</b>	<b>RELEVANT CONTENT FOR RELEVANT PARTIES</b>	<b>BUILT IT</b>	<b>24/7/365 ALERTS</b>	<b>MEET GOALS MAKE NEW GOALS</b>	



# Outcome



## Architecture & Planning

*Architecture  
Runbook Services*

## Deployment

*On-site  
Quick-Start  
Silver  
Gold*

## Managed

