CISO Alliance Southern Africa

The Inevitable Cyber Attack: *From Observation to Remedial Action and Minimizing Dwell Time" In-between*

Presenter

Jon Hamlet – *Senior Country Manager*

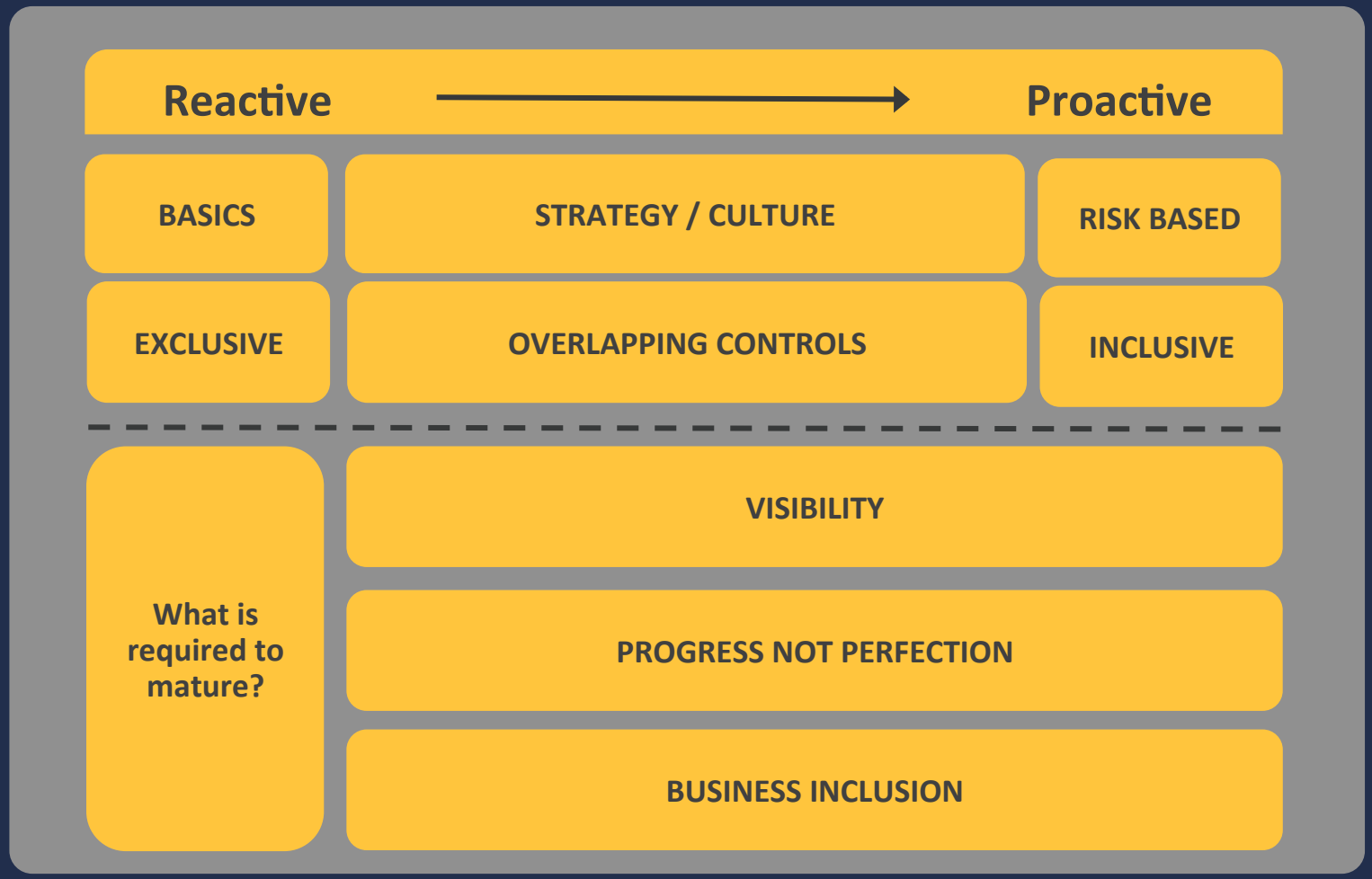
Gareth Hawkins – *Pre-Sales Manager*

Symantec

Date

22 September 2017

Organizational Security Maturity



Insights


Symantec
“Dwell Time”
The amount of time between initial compromise and final remediation”


Symantec
A Security Operations Center is a Highly Skilled team following Well-Defined Definitions and Processes to Manage Threats and Reduce Security Risk
Haider Pasha, CISSP, CIEH
Chief Technology Officer
Emerging Markets

Key Security Challenges

Security Operations Center

CONCERNS

- Scaling for Growth
- Data Protection & Compliance
- Limited Cyber Security Threat Intelligence & Analytics
- SOC Implementation Methodology

REQUIREMENTS

- Outsource vs. Co-Source of Security Operations
- Enhancing Visibility
- Governance & Control
- Proactive Threat Detection, Prevention, & Response

SOC FOCUS

- Threat Protection
- Threat Monitoring and Operations
- Intelligence & Incident Response
- Security Analytics

SOC Vision

Symantec

Managed Security Service

SIEM

Big Data Analytics

IT-GRC

Threat Intelligence

Vulnerability Assessments

Simulation Services

Network Protection

Intelligence

Threat Protection

Cyber Security Services

People

Technology

Processes

SOC

Security Monitoring Services

Cyber Security Services

SOC Maturity

DEFENSE

Proactive Protection

Incident Response

Incident Management

Enhanced Visibility

Security Advisory

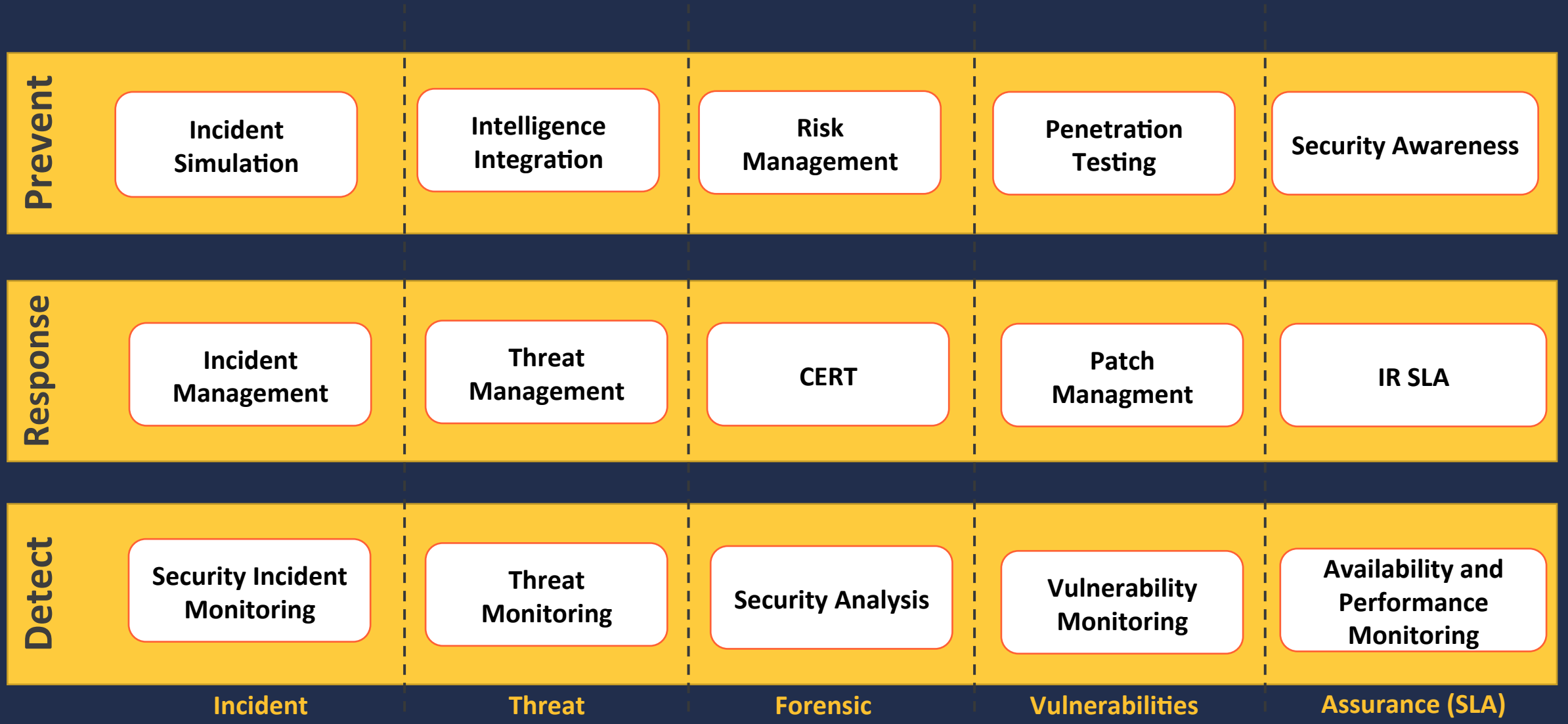
Reporting and SLAs

Security Management Consideration

Insourcing	Outsourcing	Co-sourcing
Cost High CAPEX Variable OPEX	**Cost** Low CAPEX Predictive OPEX	**Cost** Moderate CAPEX Predictive OPEX
Control Internal Team Knows Environment Potentially Most Efficient Complex to Manage	**Control** Lack of Environment Knowledge by 3rd Party SLA Based Services Difficult to Terminate / Change	**Control** Benefits of Local Knowledge and 3rd Party Expertise Partial SLA Service Flexible Future Change
Time People Recruitment, Tools Procurement & Configuration	**Time** Handover, Service Definition and SLA Measurement	**Time** Blended Approach
Staff Hard to Acquire, Retain, Train	**Staff** 3rd Party Responsibility	**Staff** Staff Augmentation
Risk High Risk – Mitigated with Augmentation Assigned to End-User	**Risk** Medium Risk Assigned to the Provider	**Risk** Lowest Risk; Shared Between Companies

Process

SOC Framework Best Practice



SOC Methodology

Conduct health-check and preventive maintenance for all security systems

Analyze Security Systems logs for any security threats and take proper action accordingly

Implement new Security Policy on the managed devices following the agreed process

Provide 1st & 2nd level of support for the security incidents

Perform Change & Configuration Management through RFC&MDT process

Supporting other Security departments during the incident handling process

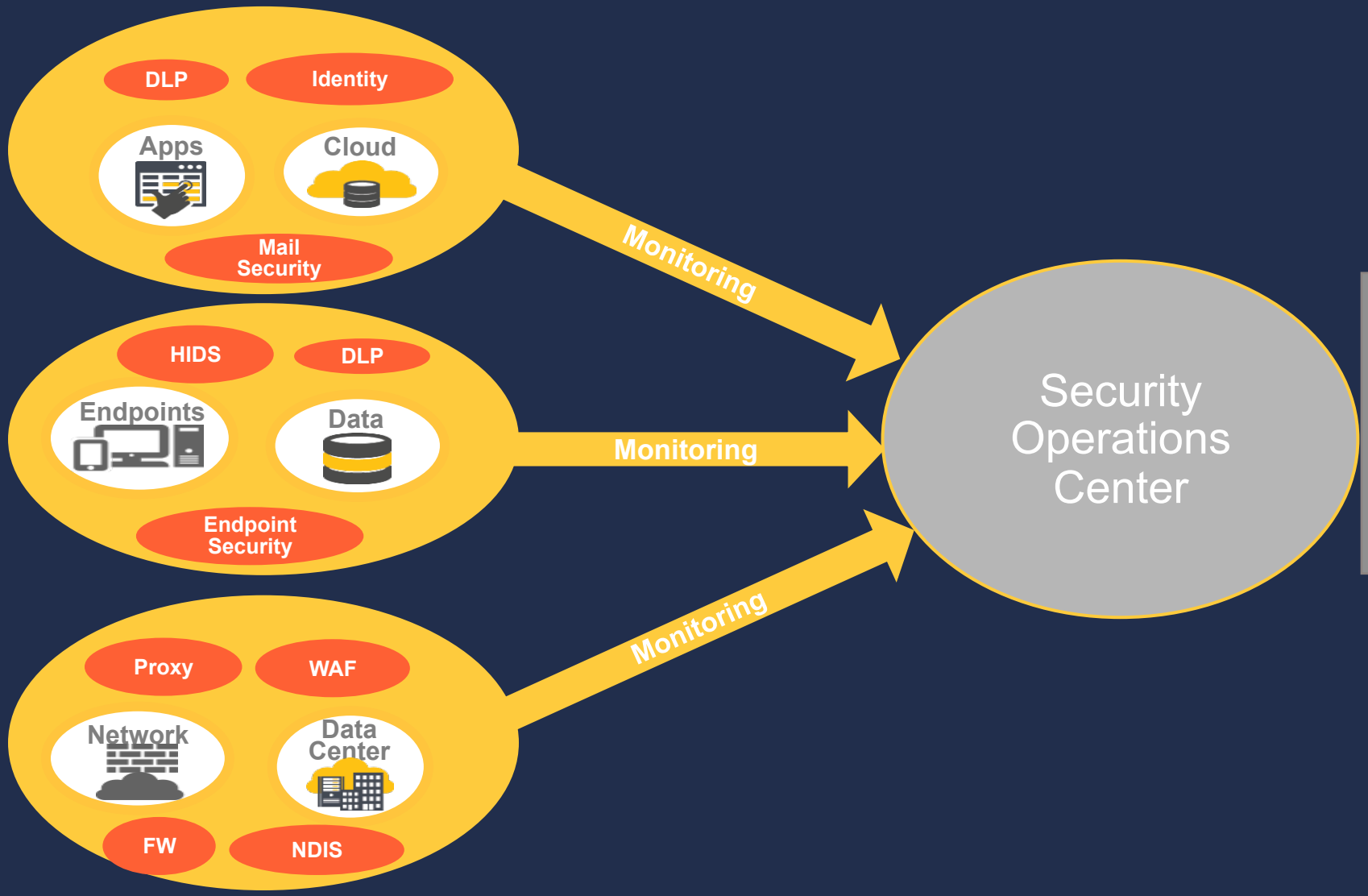
SOC Service Catalog

"Define your security services menu"

Symantec

	Reactive Services	Proactive Services	Security Management
Monitoring	**Security Monitoring** • Event Monitoring • Event Correlation • Incident Management	**Vulnerability Management** • Real-Time Device Monitoring • VA/PT & Threat Model Simulations • Security & Compliance Audit **Cyber Threat Intelligence** • Threat Hunting & Analysis • Honey potting • Performance & Fault Monitoring	**Business Impact Analysis** • Risk Assessment • Threat Assessment • Technology Watch **Inventory Scanning**
Advisory	**Incident Notification**	**Reporting** • Alerting & Warning • Trending • Technical Reports **Security Hotline** **Operational & Strategic Threat Reports**	**Security Consulting** • Awareness • Countermeasure Selection • Executive Reporting **Patch & Vulnerability Governance**
Managing	**Incident Response** • Incident Triage • Malware & Forensics Analysis • Incident Recovery & Post Mortem **Threat & Vulnerability Triage**	**Policy & Device Management** • Secure Device Configuration • Policy Enforcement • Patch Management **Security Governance** • Personnel & Supplier Management • Hardening • Events Data Retention	**Risk Management** • Business Continuity • Asset Inventory • Policy Planning **Education & Training** **Certification**

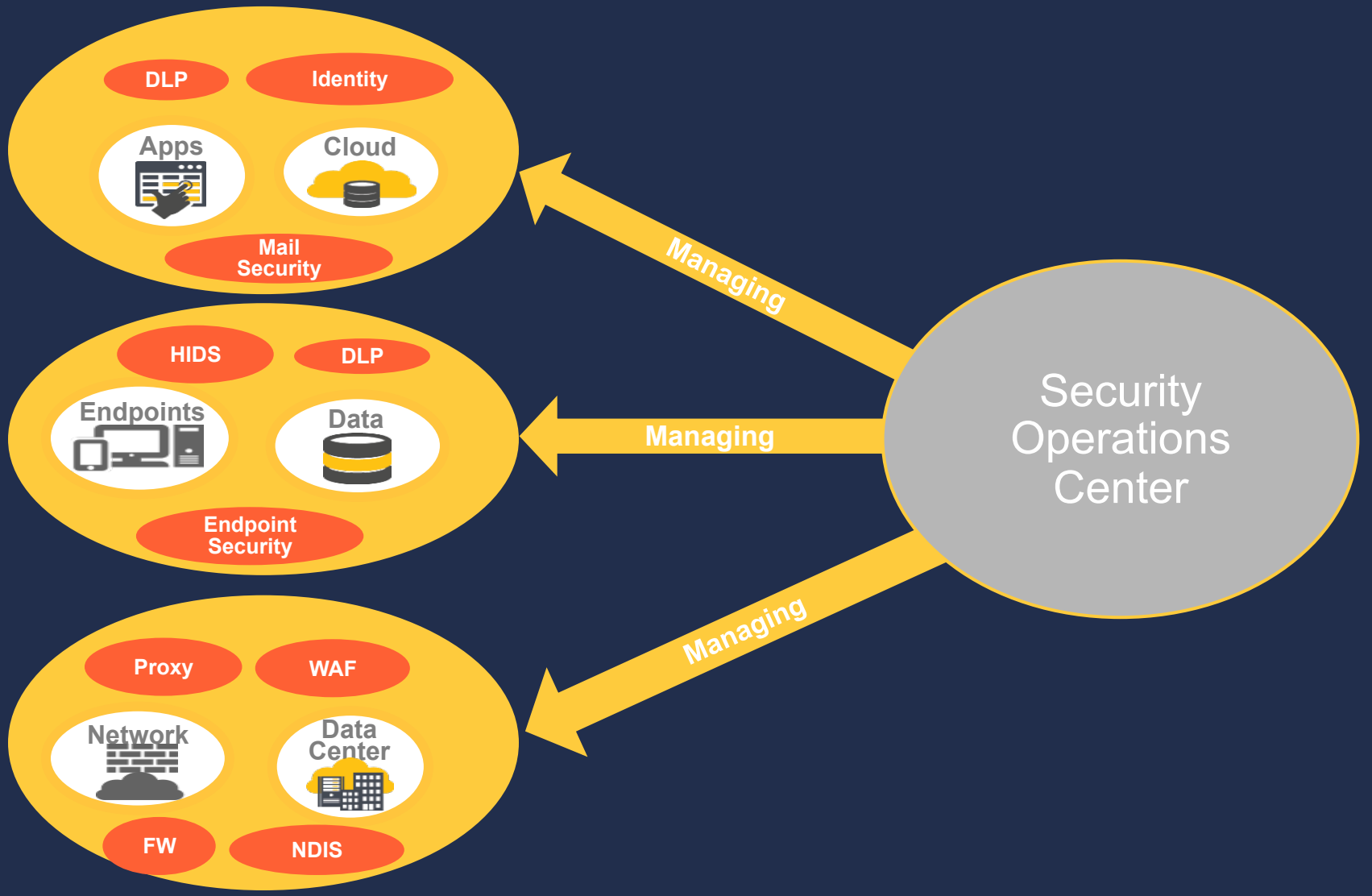
A Simplified View



First SOC function: Monitoring

Bring visibility to current security issues
Real-time Device Monitoring
Incident Detection
Incident Classification

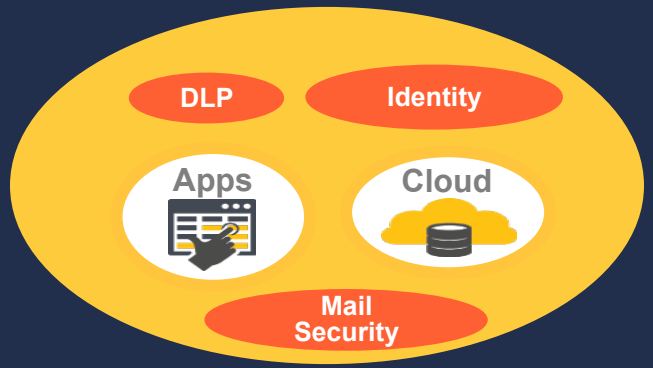
A Simplified View

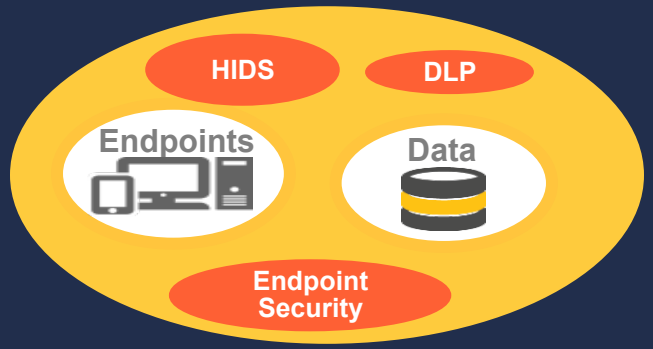


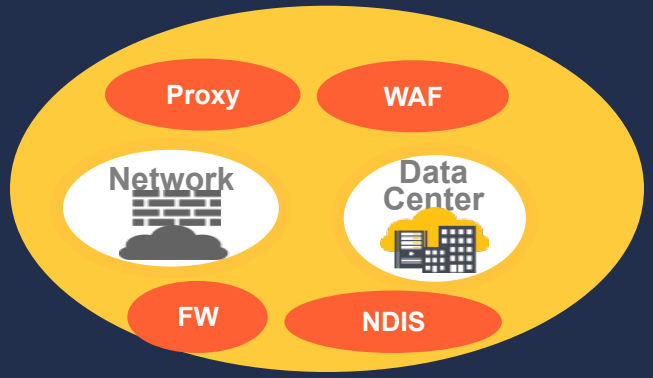
Second SOC function: Managing

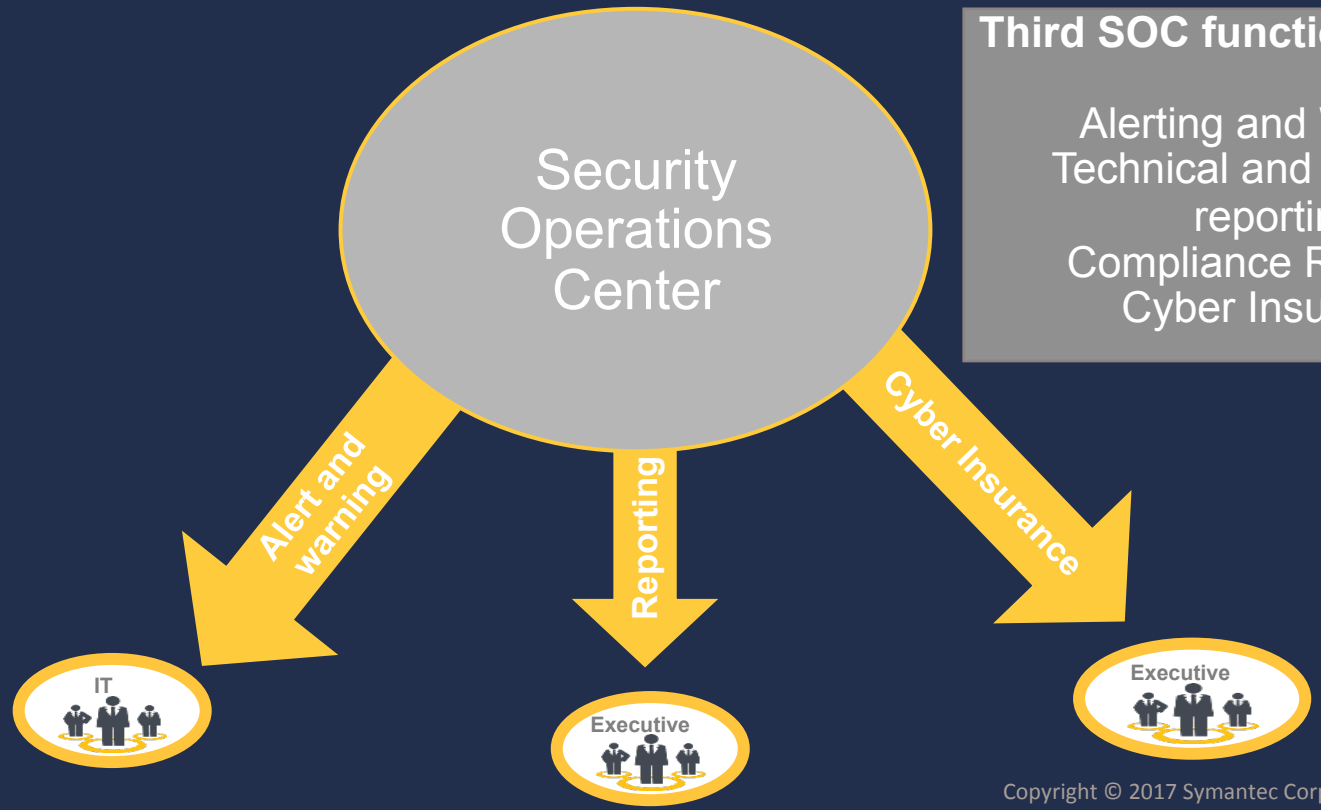
Policy Management
Policy Enforcement
Incident Remediation
Managed Network Security
Managed Endpoint
Managed Messaging
Advanced Threat Protection
Risk Management
Cyber Resilience

A Simplified View







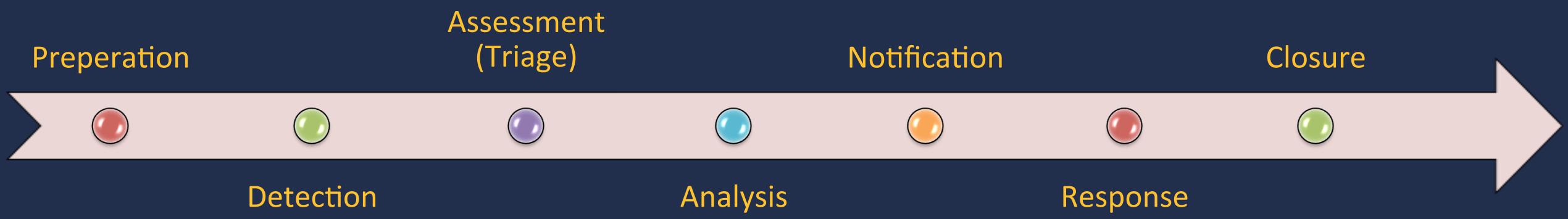


Third SOC function: Advisory

Alerting and Warning
Technical and executive reporting
Compliance Reporting
Cyber Insurance

Incident Handling Methodology

REDUCING DWELL TIME?



Threats | Events | Infrastructure | **VISIBILITY** | Response Efficacy | Audit | GRC

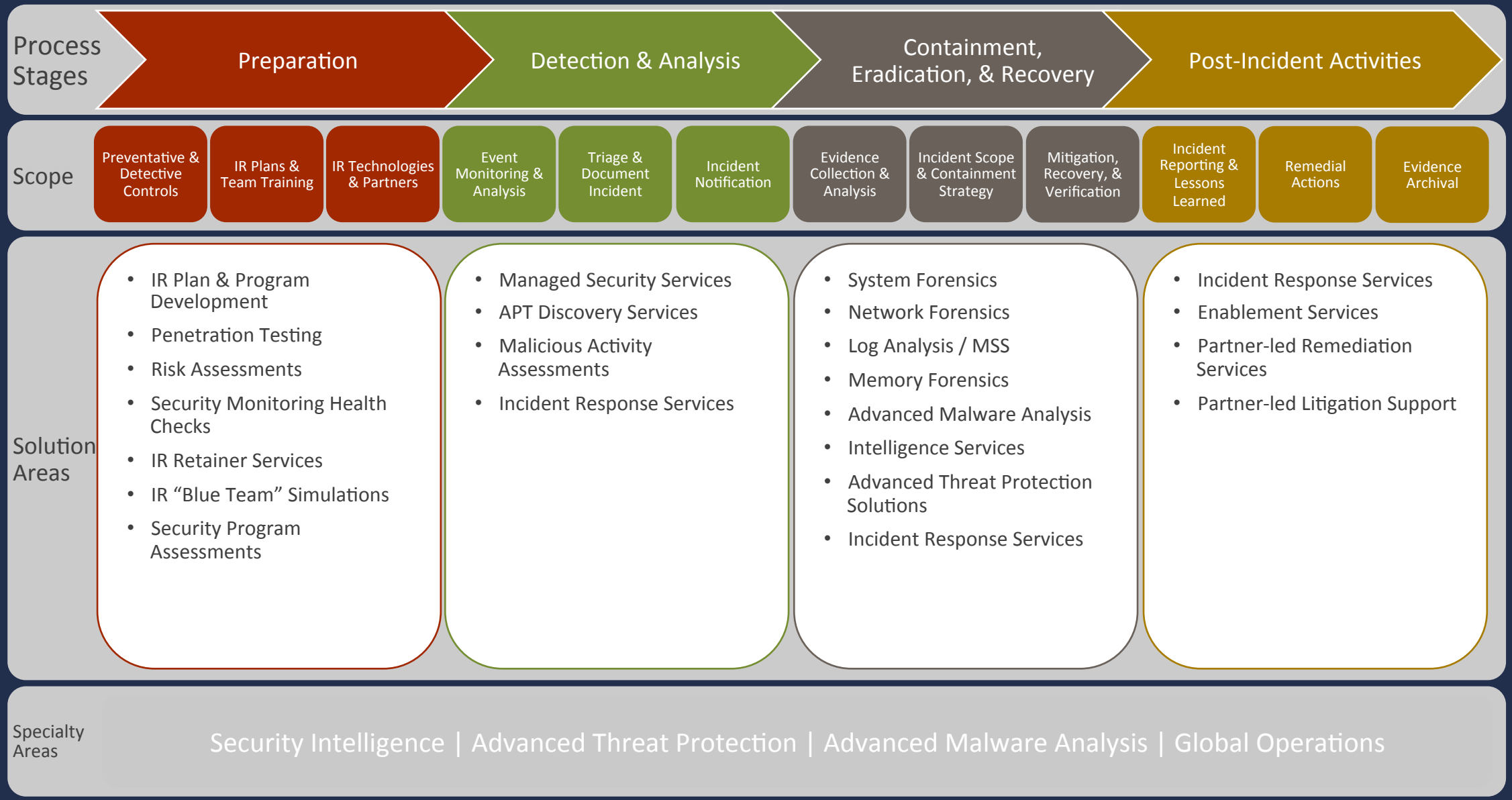
Vulnerabilities | Cloud | Changes | Workbench | Closed Loop | Remediation | Repositioning

WELL DEFINED PROCESS – RESPONSES ACROSS THE BOARD

Reduced Noise | **INTEGRATED TECHNOLOGY (OPEN SYSTEMS)** | GLOBAL

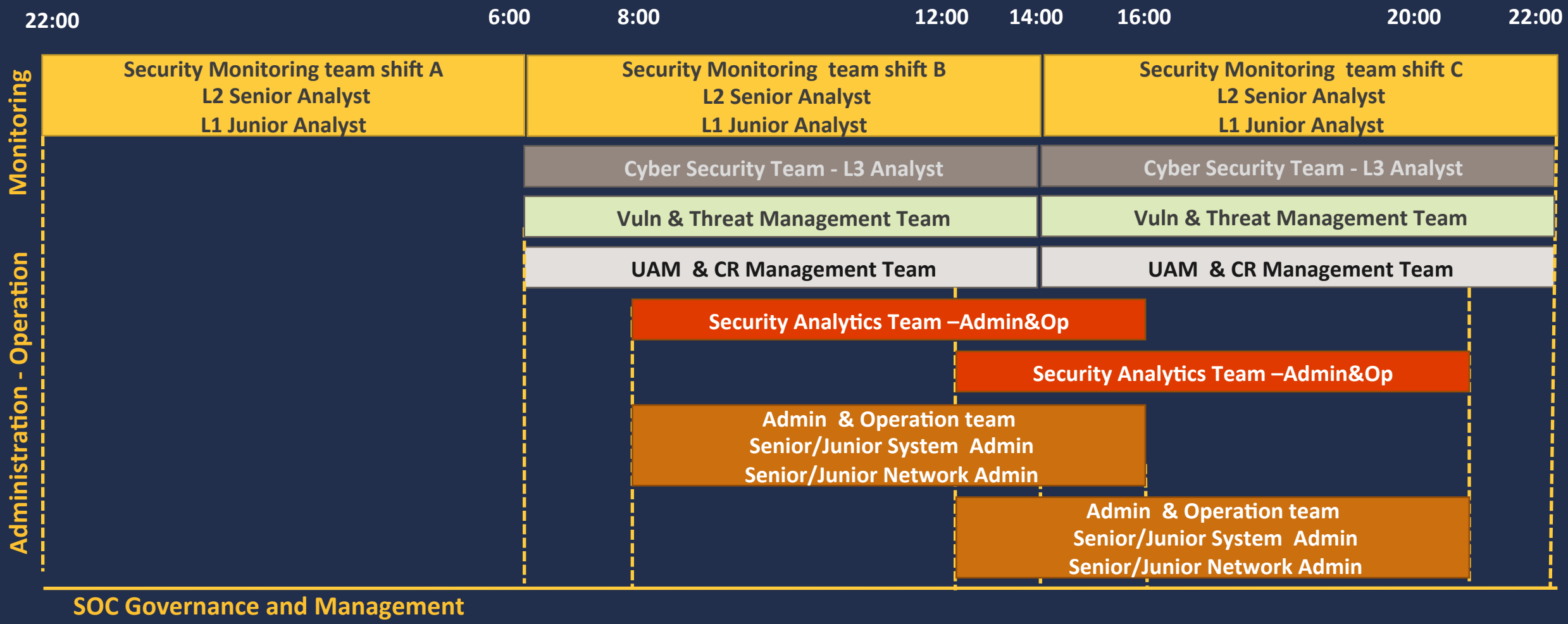
Shared Threat Intelligence | Orchestration | Automated Remediation | Bidirectional | Closed Loop

Incident Response Process Framework



People

PEOPLE: 24/7 SOC Shift Example

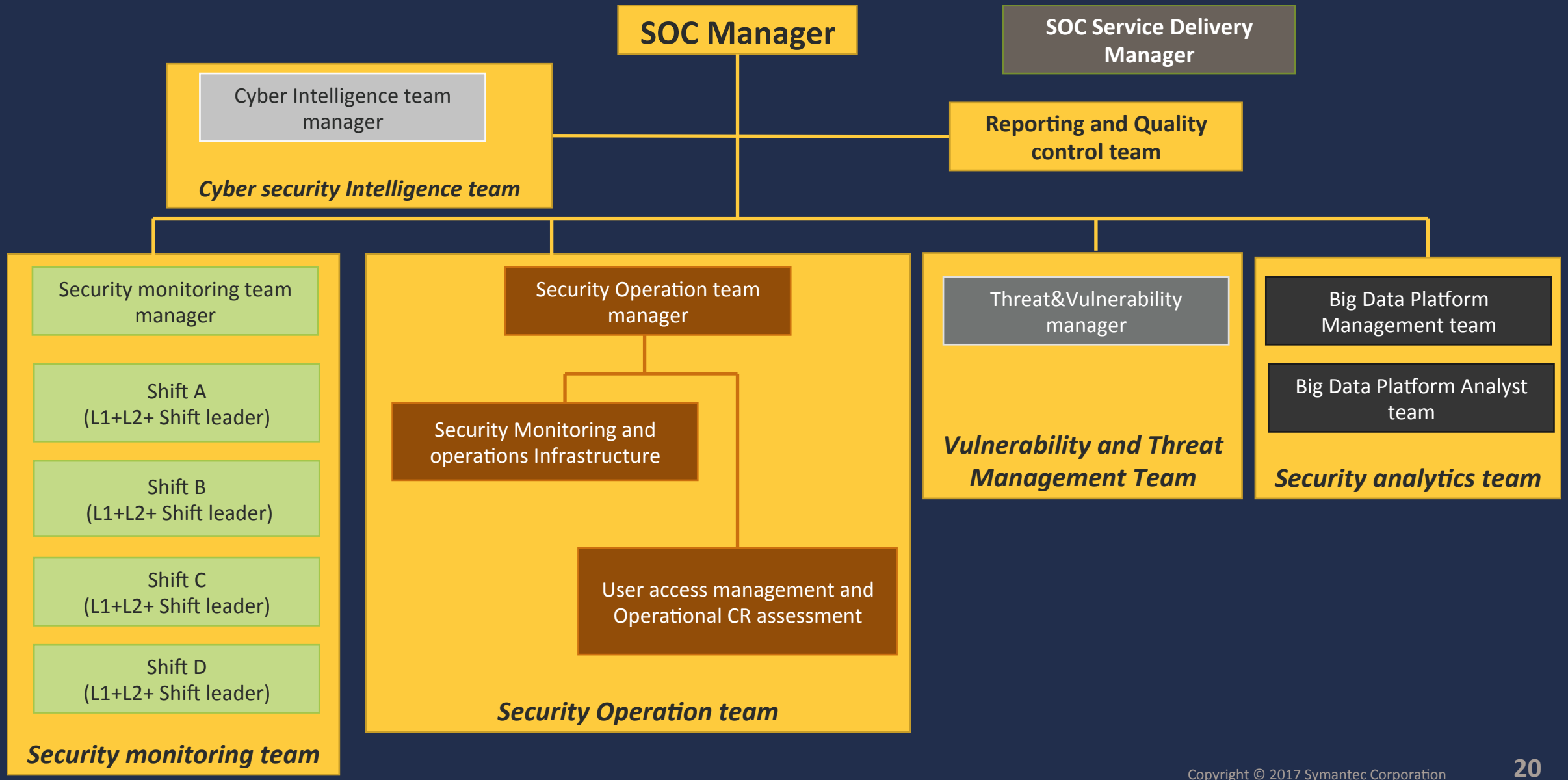


SOC Service Delivery Manager
SOC Manager
SOC Quality Control Team

Shift team in rest

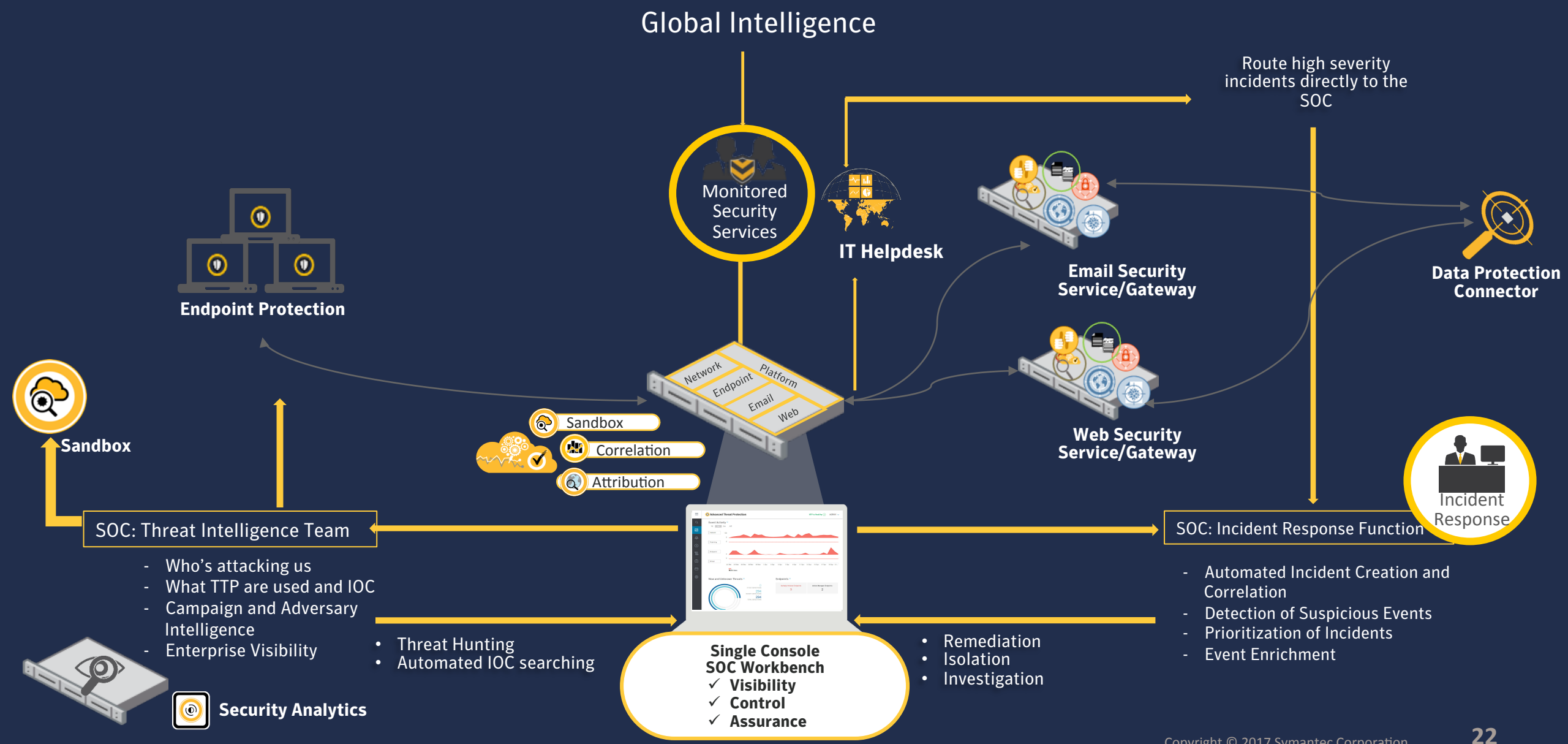
Security Monitoring team shift D
L2 Senior Analyst
L1 Junior Analyst

Typical SOC Team Structure

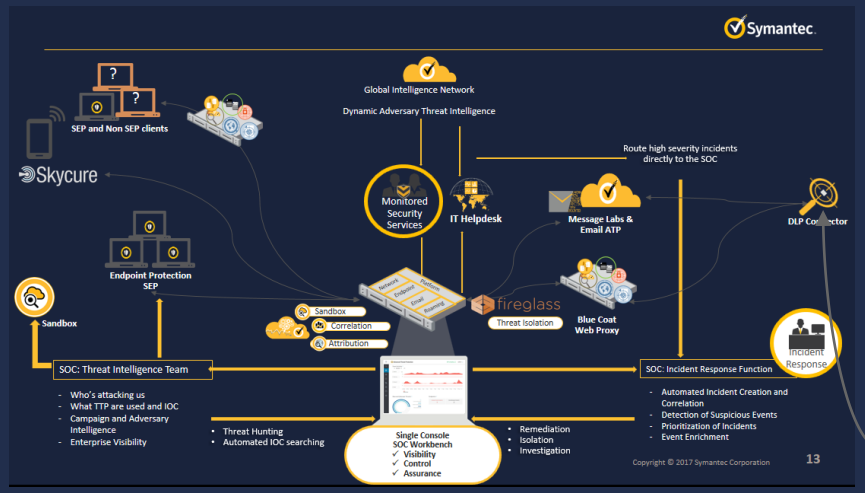


Technology

Integrated Threat Protection: SOC Workbench



Integrated Information Protection: SOC Workbench



Integrated Information Protection Controls

Shadow IT Visibility & Control

Tagging & Encryption

Identity & Authentication

Data Protection: Incident Response Function

- Automated Incident Creation
- Universal policy deployment
- Single enforce platform

- Remediation
- Investigation

Corporate SaaS Apps

Email

Email Security Service (SMTP)

CASB

IT Helpdesk

Web & Internet

Web Proxy

Data Protection Connector

Email
Endpoint
Web
Platform
Storage

Data at Rest

Endpoint

Single Data Protection Console
✓ Visibility
✓ Control
✓ Assurance

Few takeaways

- Each SOC project is a journey. Get the required buy in.
  - *Projects require a considerable amount of time and money.*
- Hybrid approach can massively speed up the time to service delivery.
  - *Consider adopting an MSSP even as a temporary solution*
- Define Service Catalog Carefully.
- Implement baby steps: do few things well.
  - *Do not oversell SOC mission and implement the basics right.*
- Do not ingest any data: clearly define your use cases.
- Get the right staff in place.
  - *Motivate them, motivate them, motivate them.*