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*

Symantec.

Date

27 June 2018

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, C|EH*
Chief Technology Officer
Emerging Markets

Key Security Challenges

Security Operations Center

CONCERNS	REQUIREMENTS	SOC FOCUS
Scaling for Growth	Outsource vs. Co-Source of Security Operations	Threat Protection
Data Protection & Compliance	Enhancing Visibility	Threat Monitoring and Operations
Limited Cyber Security Threat Intelligence & Analytics	Governance & Control	Intelligence & Incident Response
SOC Implementation Methodology	Proactive Threat Detection, Prevention, & Response	Security Analytics

SOC Vision

Managed Security Service

SIEM

Big Data Analytics

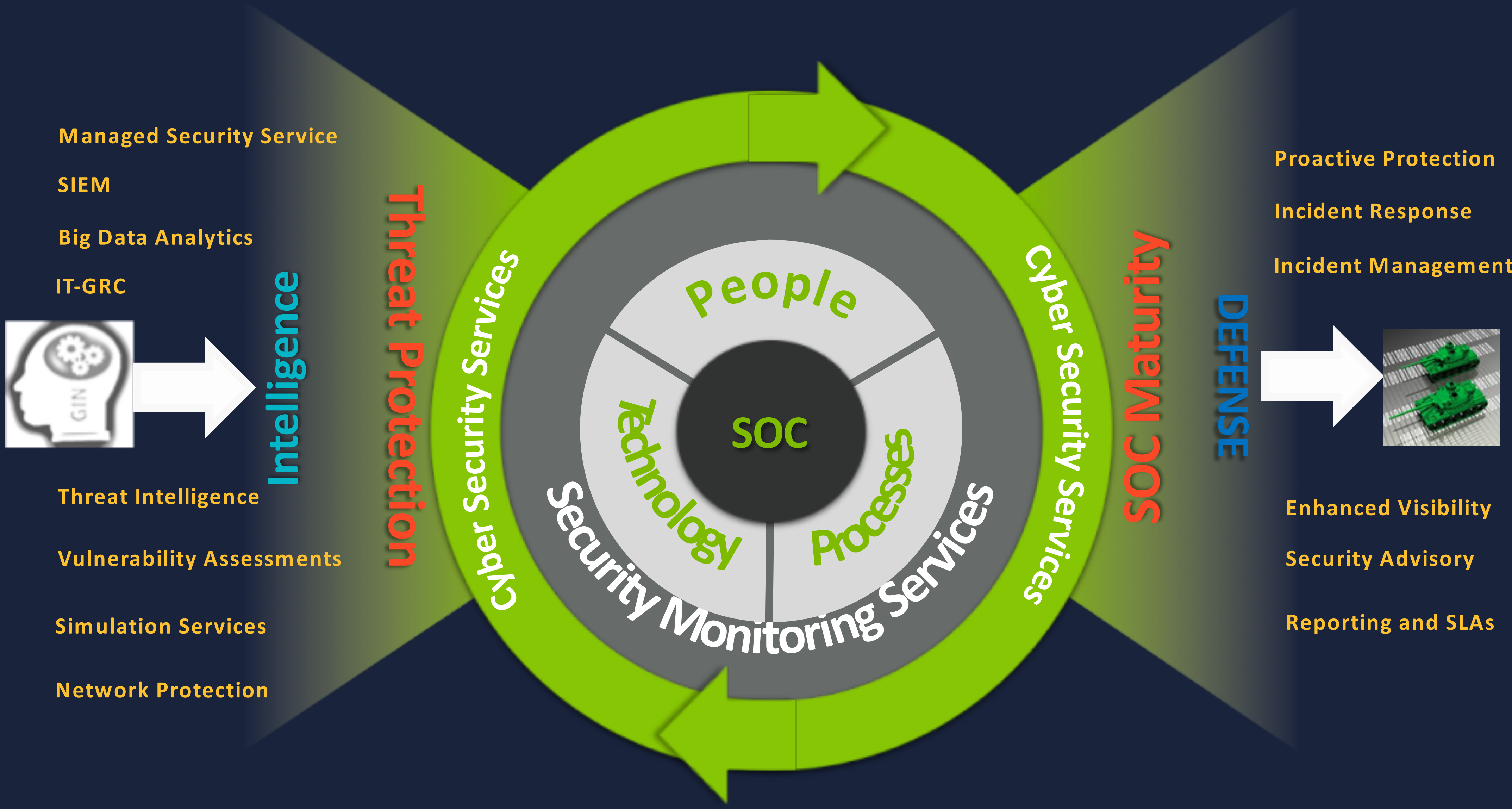
IT-GRC

Threat Intelligence

Vulnerability Assessments

Simulation Services

Network Protection



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

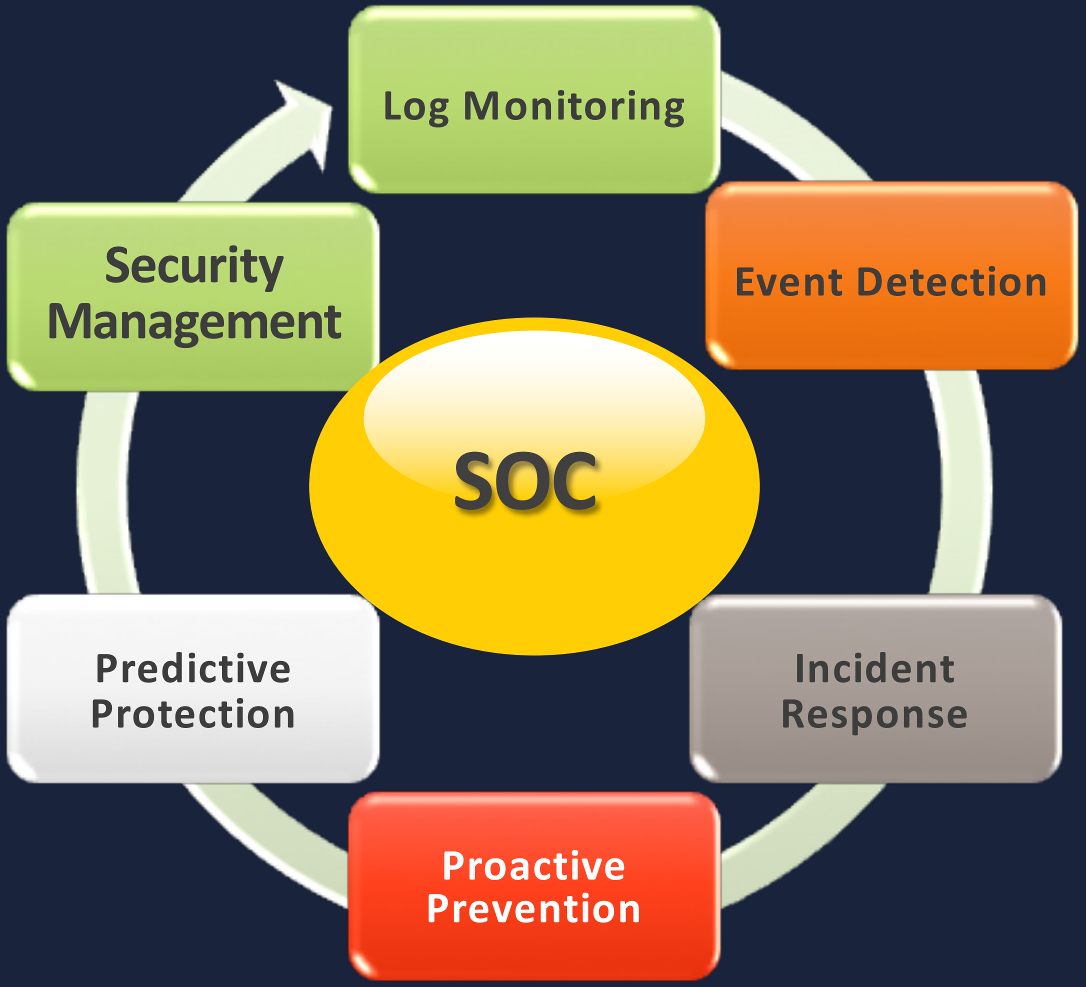
SOC Framework Best Practice

	Incident	Threat	Forensic	Vulnerabilities	Assurance (SLA)
Prevent	Incident Simulation	Intelligence Integration	Risk Management	Penetration Testing	Security Awareness
Response	Incident Management	Threat Management	CERT	Patch Managment	IR SLA
Detect	Security Incident Monitoring	Threat Monitoring	Security Analysis	Vulnerability Monitoring	Availability and Performance Monitoring

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

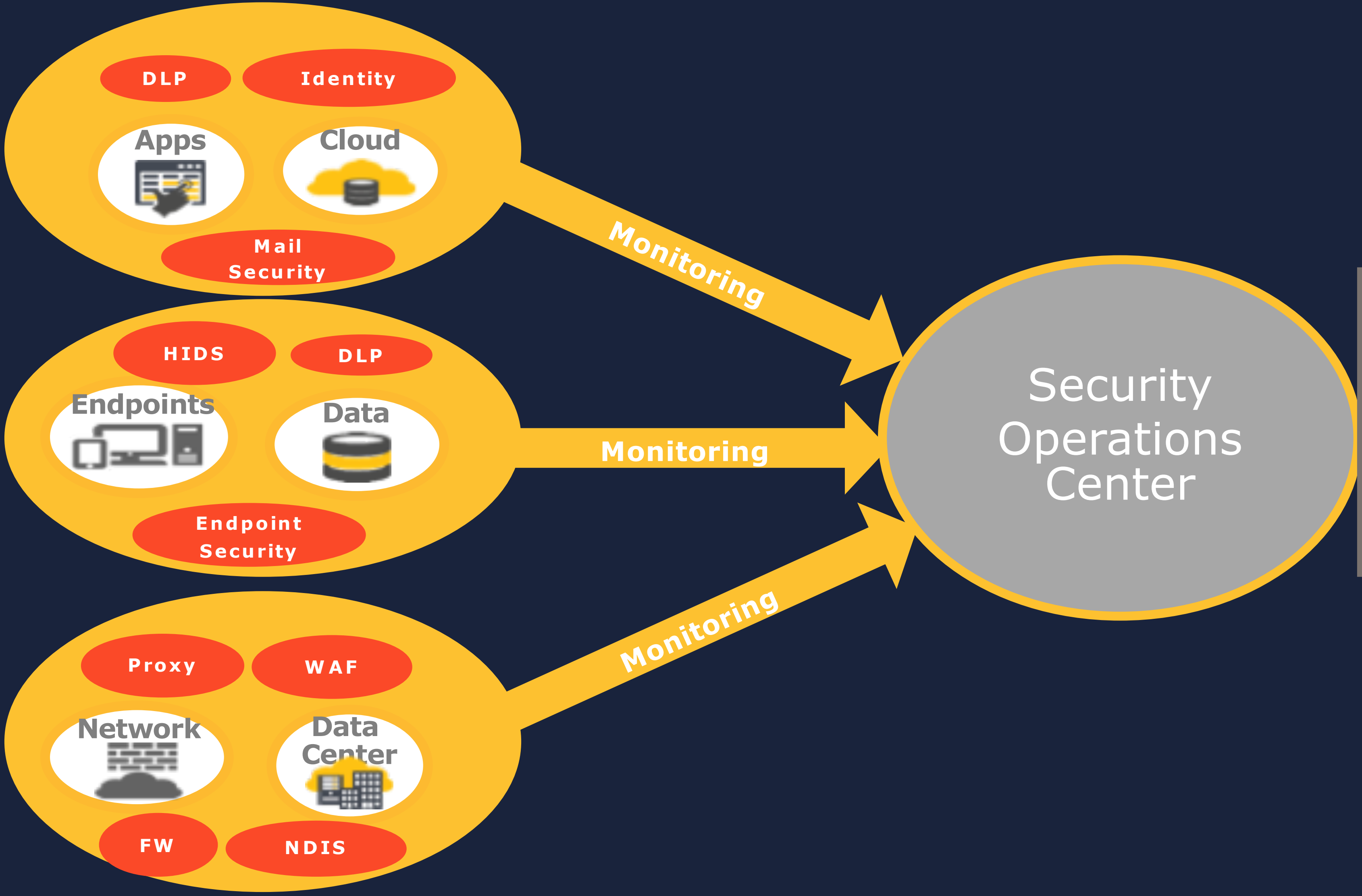
Supporting other Security departments during the incident handling process

SOC Service Catalog

"Define your security services menu"

	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

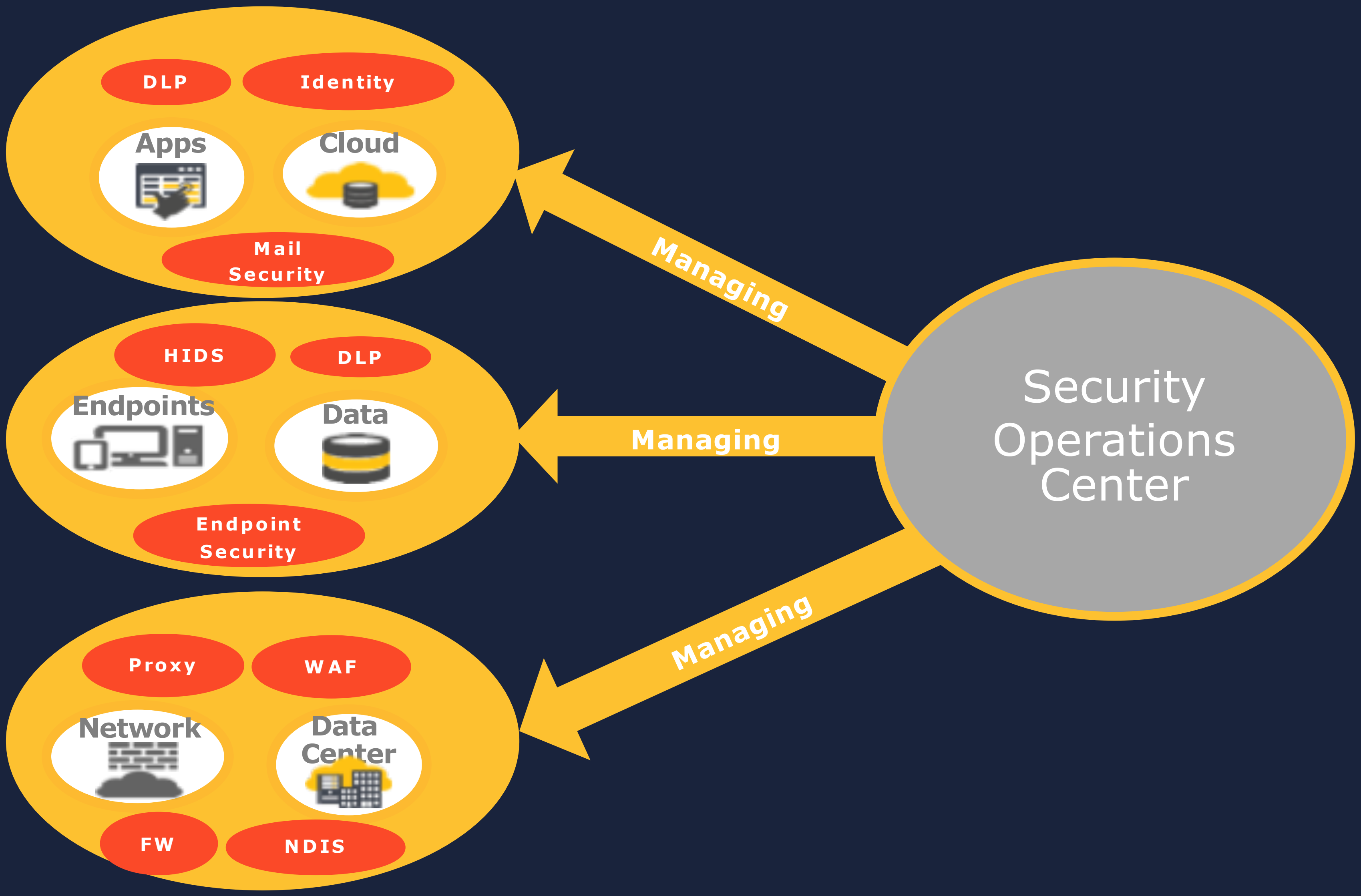
A Simplified View



First SOC function: Monitoring

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

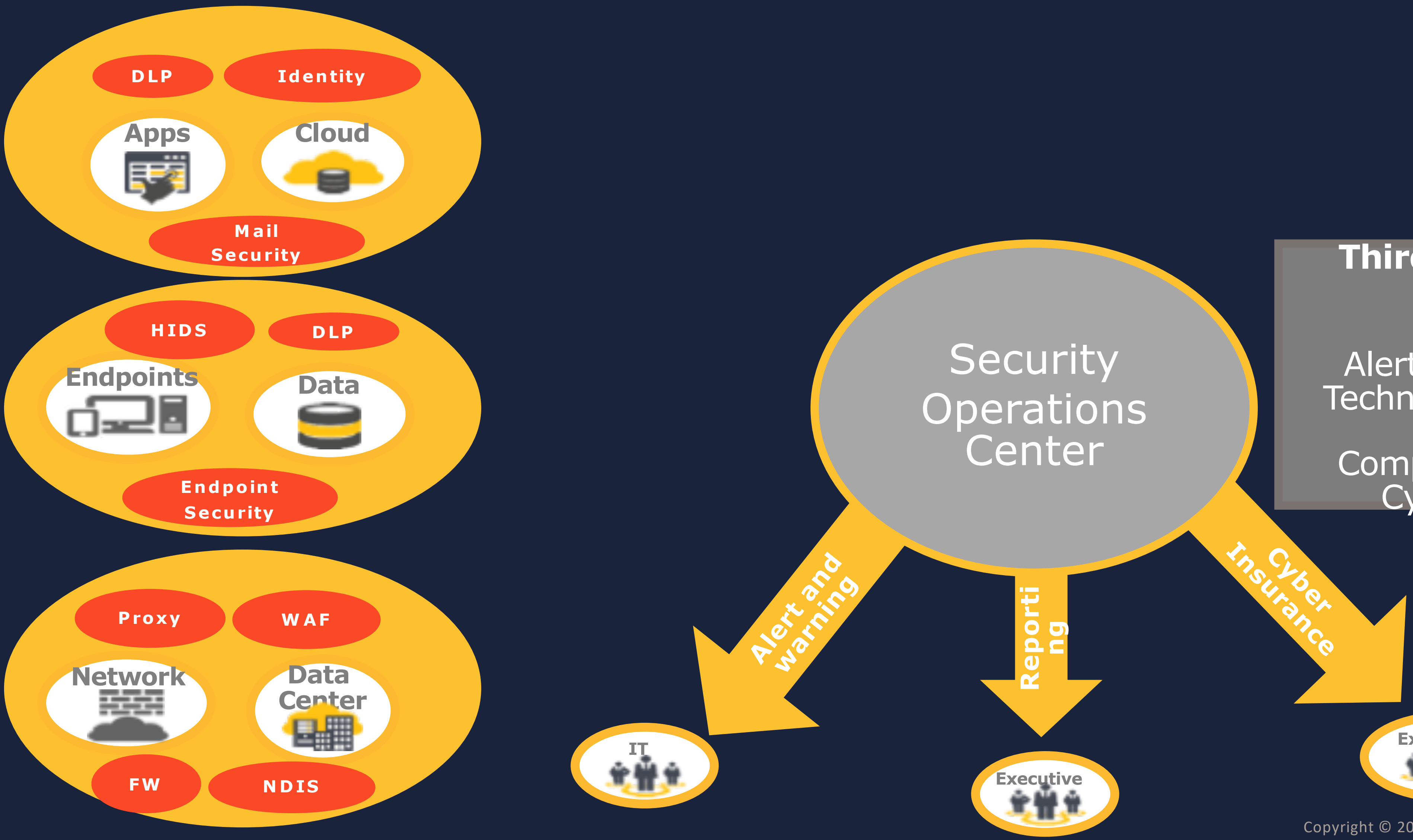
A Simplified View



Second SOC function: Managing

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

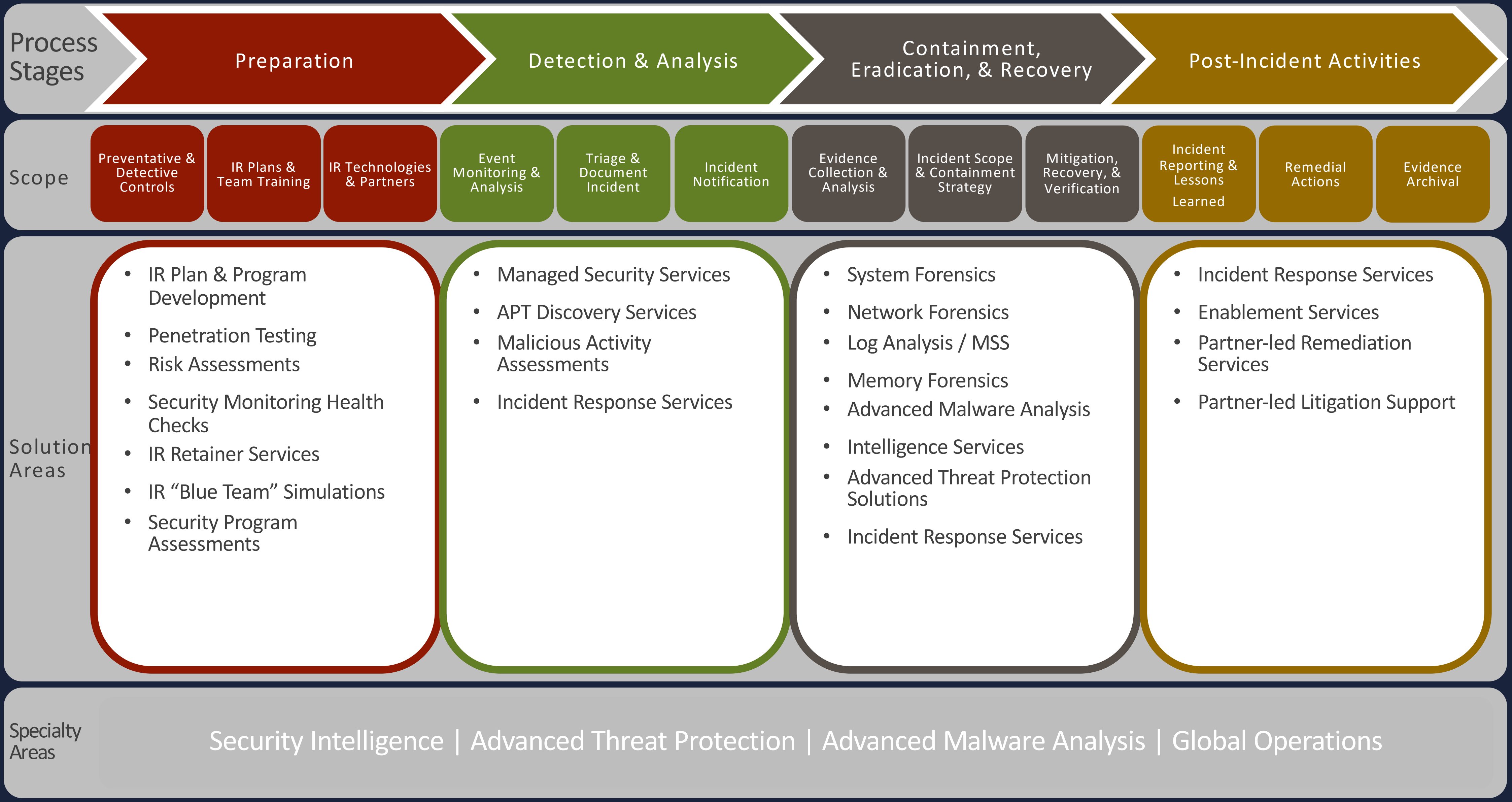
A Simplified View



Third SOC function: <u>Advisory</u>

Alerting and Warning
Technical and executive reporting
Compliance Reporting
Cyber Insurance

Incident Response Process Framework

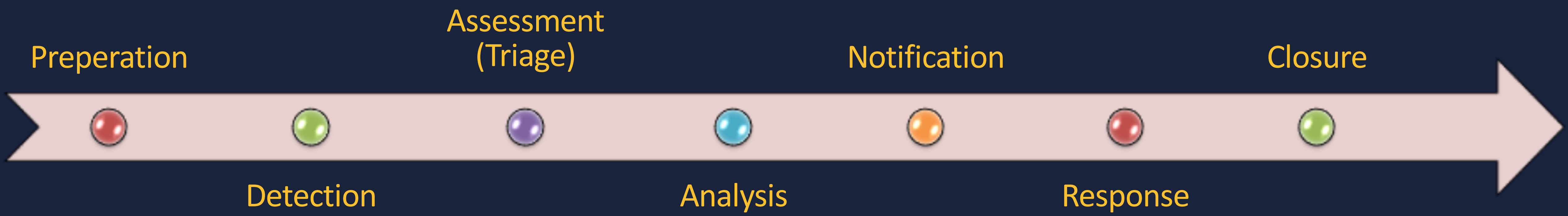


Process Stages	Preparation	Detection & Analysis	Containment, Eradication, & Recovery	Post-Incident Activities
Scope	Preventative & Detective Controls IR Plans & Team Training IR Technologies & Partners	Event Monitoring & Analysis Triage & Document Incident Incident Notification	Evidence Collection & Analysis Incident Scope & Containment Strategy Mitigation, Recovery, & Verification	Incident Reporting & Lessons Learned Remedial Actions Evidence Archival
Solution Areas	• IR Plan & Program Development • Penetration Testing • Risk Assessments • Security Monitoring Health Checks • IR Retainer Services • IR “Blue Team” Simulations • Security Program Assessments	• Managed Security Services • APT Discovery Services • Malicious Activity Assessments • Incident Response Services	• System Forensics • Network Forensics • Log Analysis / MSS • Memory Forensics • Advanced Malware Analysis • Intelligence Services • Advanced Threat Protection Solutions • Incident Response Services	• Incident Response Services • Enablement Services • Partner-led Remediation Services • Partner-led Litigation Support

Specialty Areas

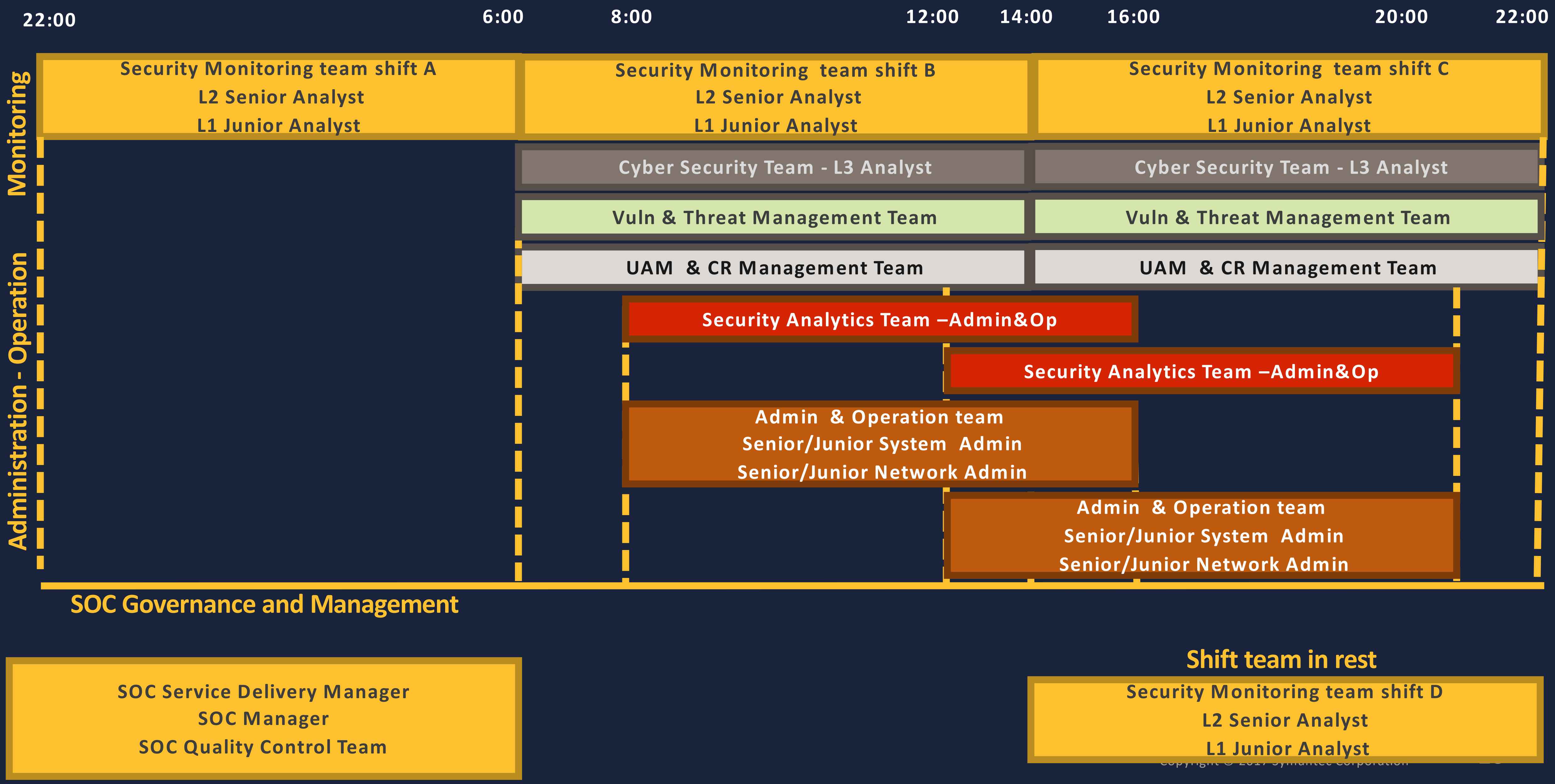
Security Intelligence | Advanced Threat Protection | Advanced Malware Analysis | Global Operations

Incident Handling Methodology



People

PEOPLE: 24/7 SOC Shift Example



22:00 | 6:00 | 8:00 | 12:00 | 14:00 | 16:00 | 20:00 | 22:00

Monitoring

Security Monitoring team shift A
L2 Senior Analyst
L1 Junior Analyst

Security Monitoring team shift B
L2 Senior Analyst
L1 Junior Analyst

Security Monitoring team shift C
L2 Senior Analyst
L1 Junior Analyst

Administration - Operation

Cyber Security Team - L3 Analyst

Cyber Security Team - L3 Analyst

Vuln & Threat Management Team

Vuln & Threat Management Team

UAM & CR Management Team

UAM & CR Management Team

Security Analytics Team –Admin&Op

Security Analytics Team –Admin&Op

Admin & Operation team
Senior/Junior System Admin
Senior/Junior Network Admin

Admin & Operation team
Senior/Junior System Admin
Senior/Junior Network Admin

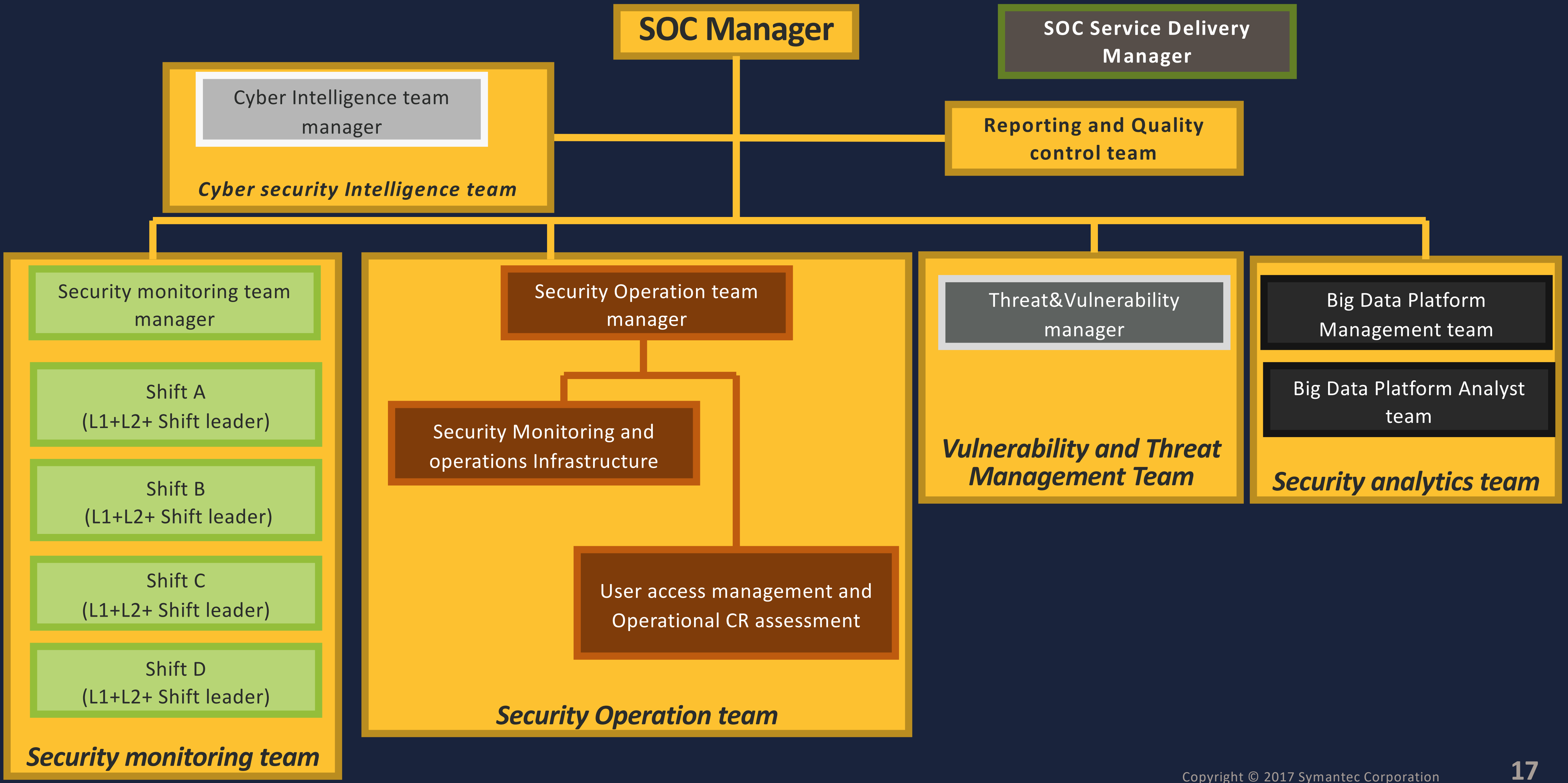
SOC Governance and Management

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



SOC Manager

SOC Service Delivery Manager

Cyber Intelligence team manager

Cyber security Intelligence team

Reporting and Quality control team

Security monitoring team manager

Shift A (L1+L2+ Shift leader)

Shift B (L1+L2+ Shift leader)

Shift C (L1+L2+ Shift leader)

Shift D (L1+L2+ Shift leader)

Security monitoring team

Security Operation team manager

Security Monitoring and operations Infrastructure

User access management and Operational CR assessment

Security Operation team

Threat&Vulnerability manager

Vulnerability and Threat Management Team

Big Data Platform Management team

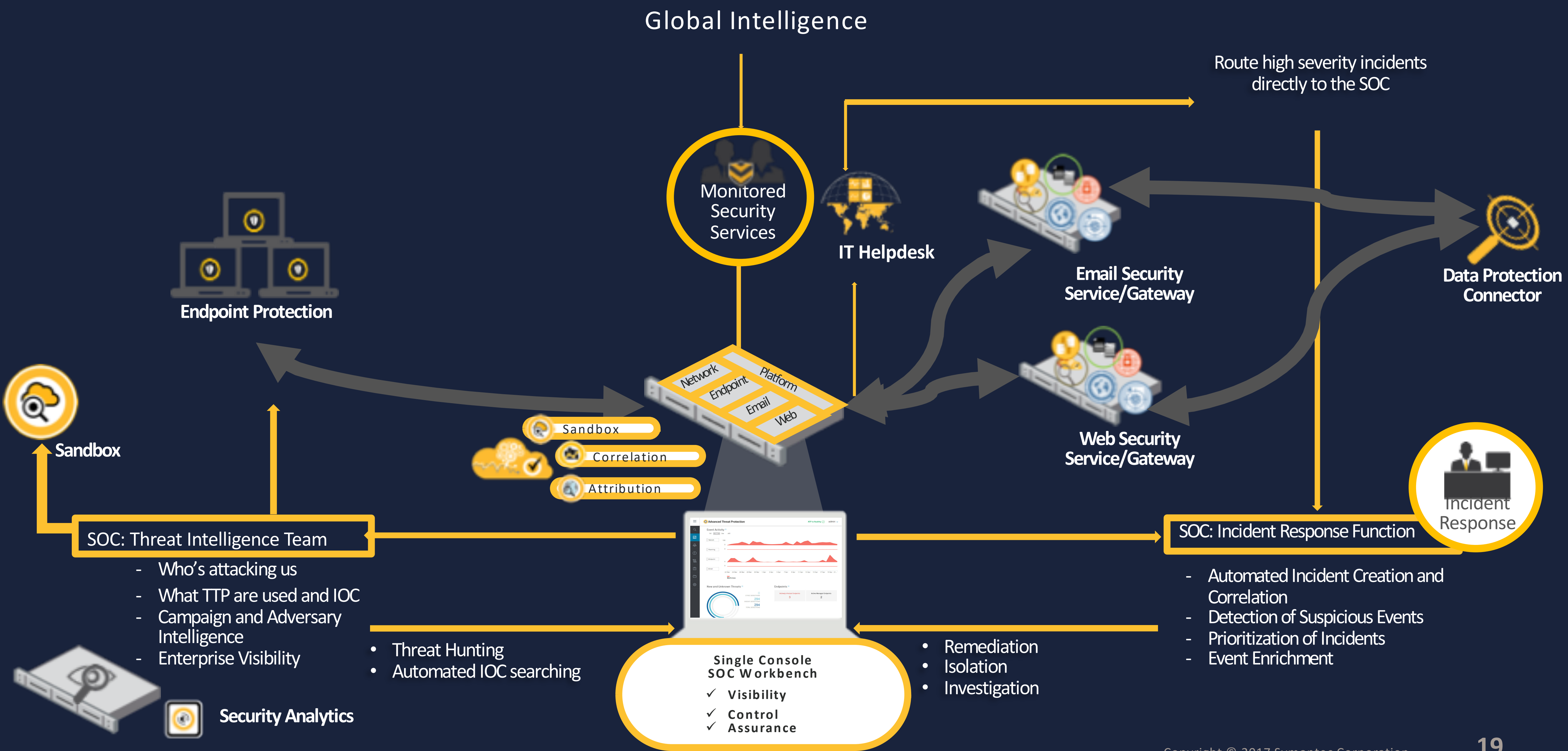
Big Data Platform Analyst team

Security analytics team

Technology

Integrated Threat Protection: SOC Workbench

Symantec.



Global Intelligence

Route high severity incidents directly to the SOC

Monitored Security Services

IT Helpdesk

Endpoint Protection

Email Security Service/Gateway

Data Protection Connector

Web Security Service/Gateway

Sandbox

SOC: Threat Intelligence Team

- Who's attacking us
- What TTP are used and IOC
- Campaign and Adversary Intelligence
- Enterprise Visibility

- Threat Hunting
- Automated IOC searching

Security Analytics

Single Console
SOC Workbench

- ✓ Visibility
- ✓ Control
- ✓ Assurance

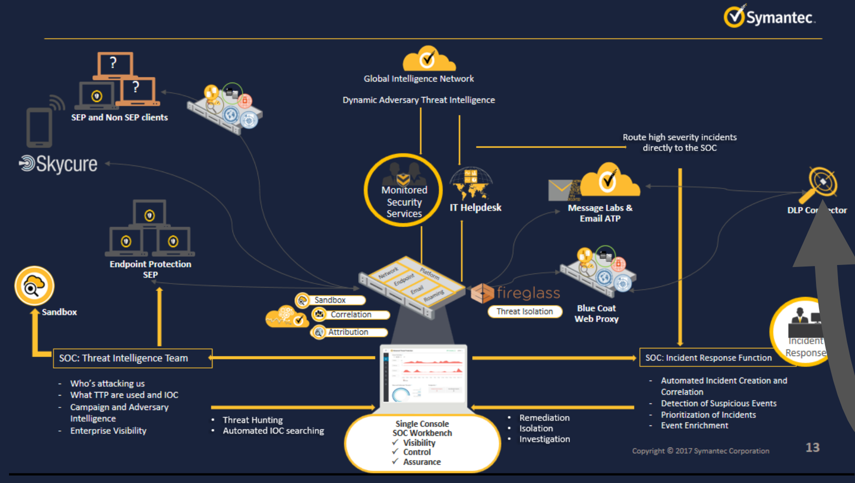
- Remediation
- Isolation
- Investigation

SOC: Incident Response Function

- Automated Incident Creation and Correlation
- Detection of Suspicious Events
- Prioritization of Incidents
- Event Enrichment

Integrated Information Protection: SOC Workbench

Symantec.



SOC: Threat Intelligence Team

- Who's attacking us
- What TTP are used and IOC
- Campaign and Adversary Intelligence
- Enterprise Visibility

- Threat Hunting
- Automated IOC searching

Single Console
SOC Workbench
✓ Visibility
✓ Control
✓ Assurance

- Remediation
- Isolation
- Investigation

SOC: Incident Response Function

- Automated Incident Creation and Correlation
- Detection of Suspicious Events
- Prioritization of Incidents
- Event Enrichment

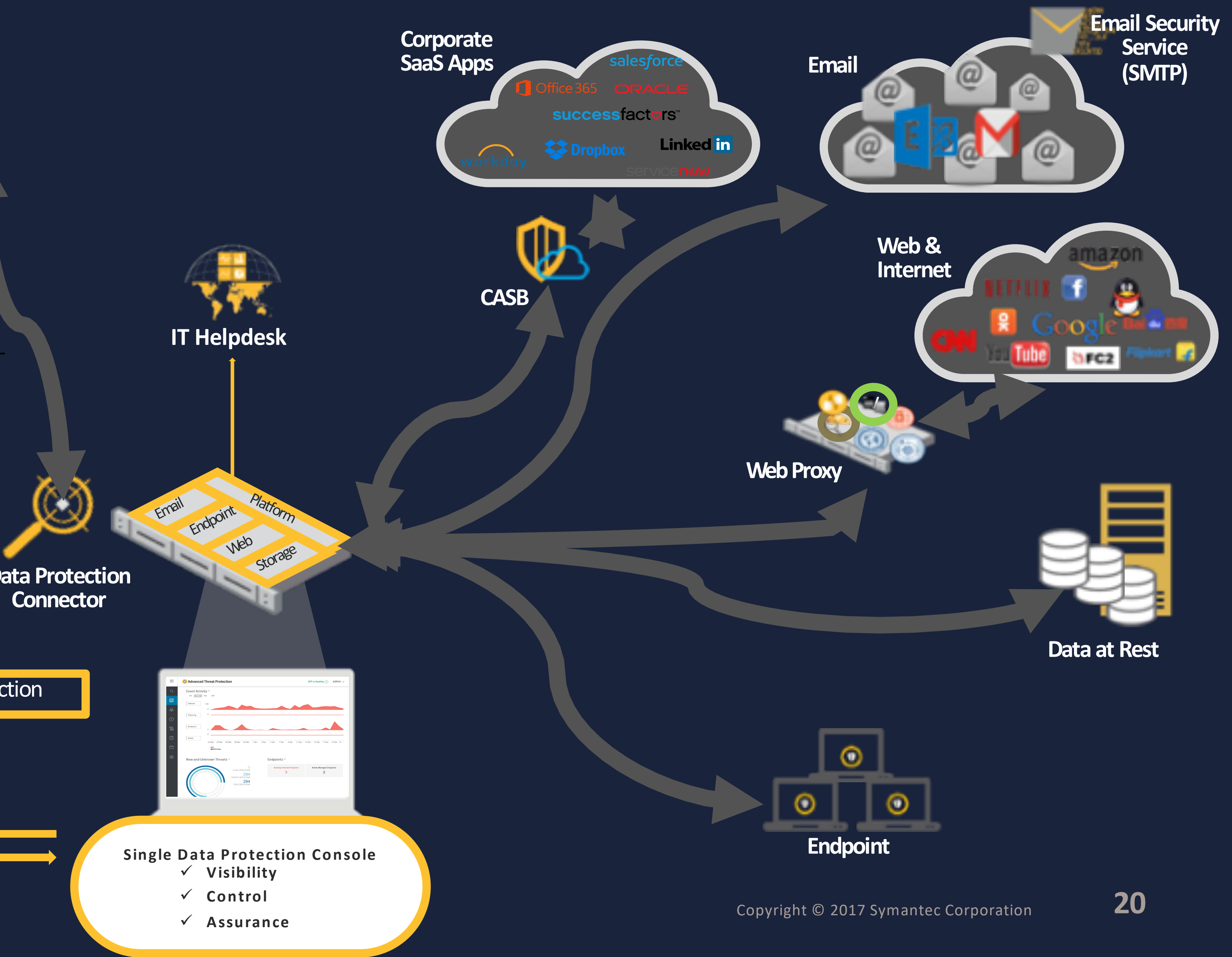
Copyright © 2017 Symantec Corporation 13

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

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.*