WORLD BANK GROUP
Information and Technology Solutions

Building a 24x7 Incident Response Operation – Our Journey

Clay Lin
WBG CISO
June 14, 2016

Agenda

- About the World Bank Group
- WBG Office of Information Security
- Business Case and Considerations
- WBG Information Security Operations Center – Our Journey
  - Goals and Services
  - Timeline - A Phased Approach
  - Shift Operations
  - People, Process, Technology
- Lessons Learned
- Next Generation Cyber Security


ENDING
POVERTY
building shared prosperity

Sustainable Development Goals

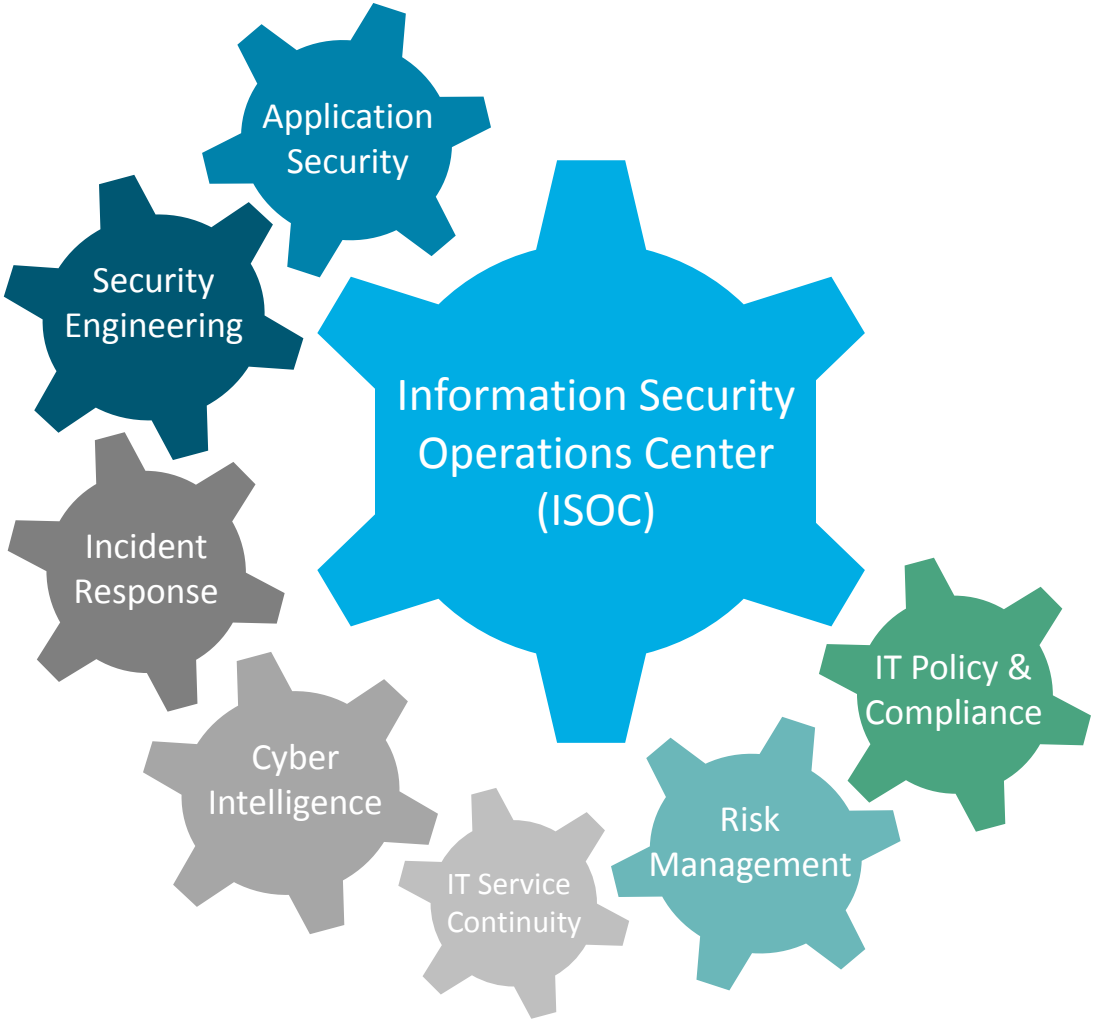
WBG Today

16,000
staff

150
country offices

170
nationalities

WBG Office of Information Security



The Business Case for 24x7 Information Security Operations Center

Breaches are often not detected until months later

Effective incident response requires strong business context

IR is a tactical, as well as a strategic element of information security

100% prevention is not possible. More emphasis on detection and response

Emerging and rapidly evolving threats demand a dedicated team

Critical Considerations for an ISOC

Sourcing Options	In house, outsourced or hybrid? Staff vs. contractors
Budget	Cost considerations
Resources	Scheduling for 24x7 operations Quality talent is hard to find and hard to retain Training and development for higher level skills
Location	Onsite, onshore, vs. offshore?
Existing Posture	Controls maturity

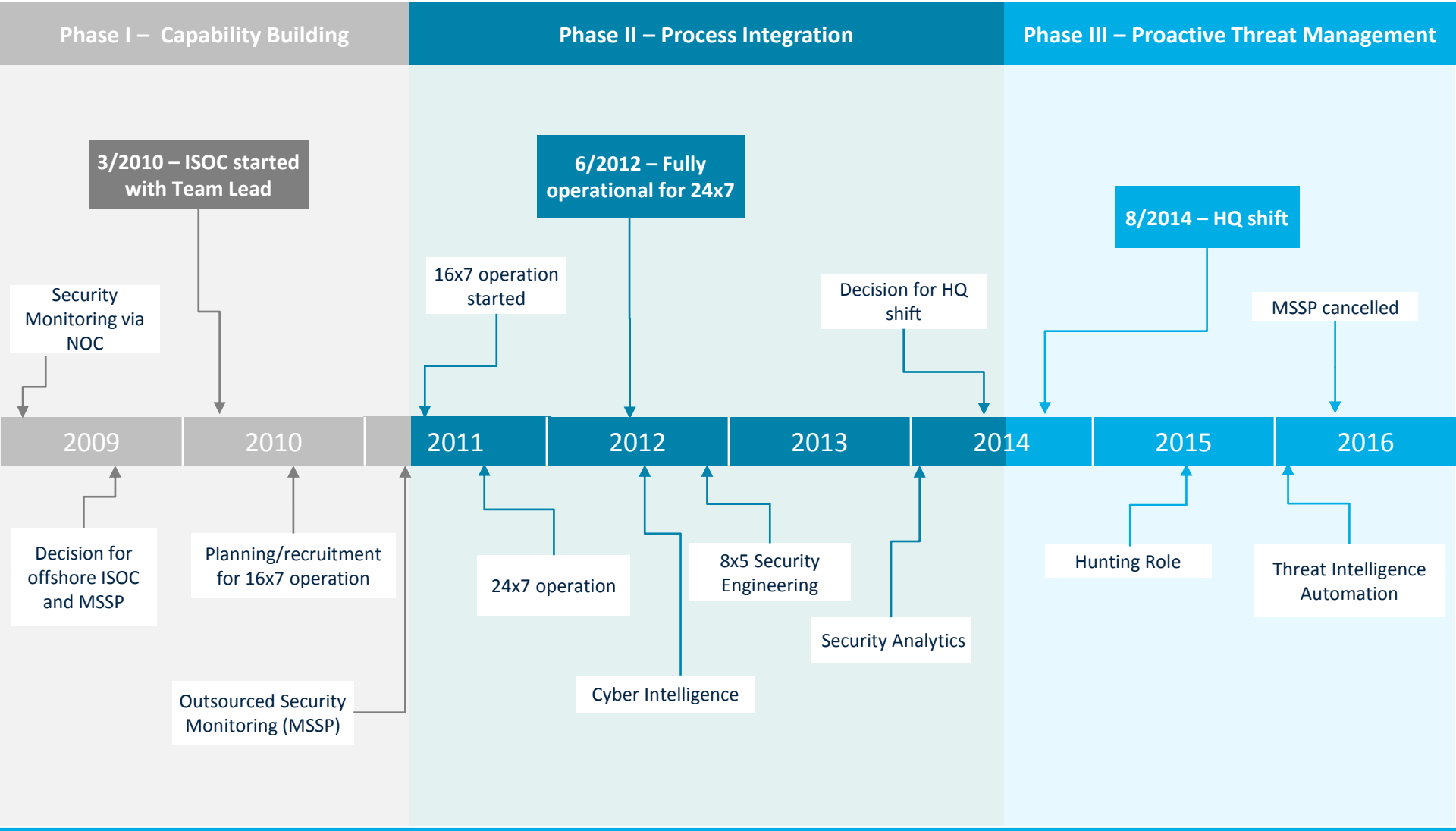
ISOC Goals

- Facilitate 24 x 7 World Bank Group **incident detection and response** capabilities
- Minimize damage from security incidents through **well-coordinated response**
- Improve information security practices from incident **lessons learned**

Our Services

- Consistent incident detection and response
- Event monitoring, analysis, correlation, and resolution
- Alerts and notifications on information security threats
- Incident identification, analysis, and handling
- Coordination and escalation
- Maintenance of database of security events
- Improved communication and reporting

WBG Security Event Management – Our Journey



NOC – Network Operations Center
ISOC - Information Security Operations Center

Security Incident Response – A Phased Approach

Phase I - Capability Building: Security Monitoring and Escalation

Sourcing Approach: Hybrid

In house: Network Operations Center

- Security monitoring from multiple sources
- Security event triage and initial impact analysis
- Incident identification and escalation
- Reporting and follow up

Outsourced: MSSP

Complement in-house capabilities with monitoring and alerting of:

- Peripheral Devices
- Internet ingress/egress points
- Firewalls/IPS/IDS

Objectives

- Establish 24/7 security monitoring, alerting, escalation
- Leverage existing resources for Tier 2 and Tier 3 support

Capabilities

- Real-time security monitoring, triage, alerting, and escalation to Tier II support
- Log management platforms, IDS, IPS, vulnerability scanners
- Documented processes and procedures
- Team structure with clear roles and responsibilities

Security Incident Response – A Phased Approach

Phase II – Process Integration: ISOC

Sourcing Approach: In-house and Offshore - ISOC

- Virus and malware remediation
- Resolution of Medium/Low severity incidents
- Log analysis and follow-up on critical events
- Identifying hostile information from dynamic malware analysis
- SIEM maintenance
- Integration with Cyber intelligence, threat and vulnerability management, log management, compliance

Objectives

- Build dedicated Tier 1 and Tier 2 support in offshore ISOC to offload operational tasks, achieve process excellence and cost efficiency

Capabilities

- 24x7 real-time monitoring and triage
- Incident detection, analysis, notification, and containment
- Malware analysis
- Cyber intelligence collection and analysis
- Consistent incident management process with well defined critical incident response procedure and planning exercises
- Metrics Reporting
- Incident management tool, analytics tool, advanced endpoint threat protection
- ISOC organization with skilled resources performing Tiers 1 and 2 support

Security Incident Response – A Phased Approach

Phase III - Proactive Threat Management

Sourcing Approach: In house, Onsite and Offshore - ISOC and Chennai Operations Center

- HQ shift during HQ business hours
- Chennai: weekend coverage and 2 shifts on weekdays
- Additional security functions in Chennai

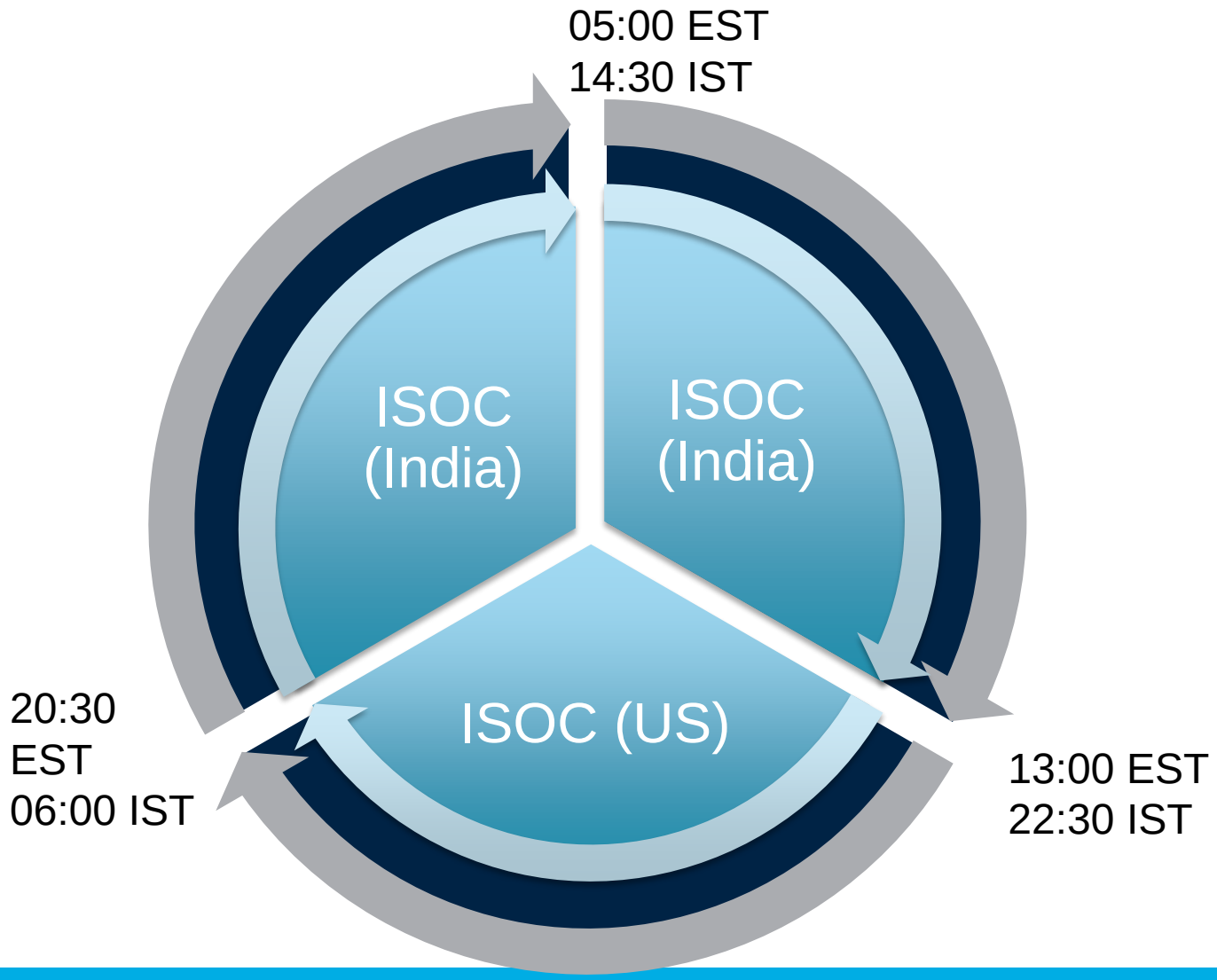
Objectives

- Establish data-driven security to increase detection and defend against advanced threats
- Continuous improvement to drive effectiveness and efficiency

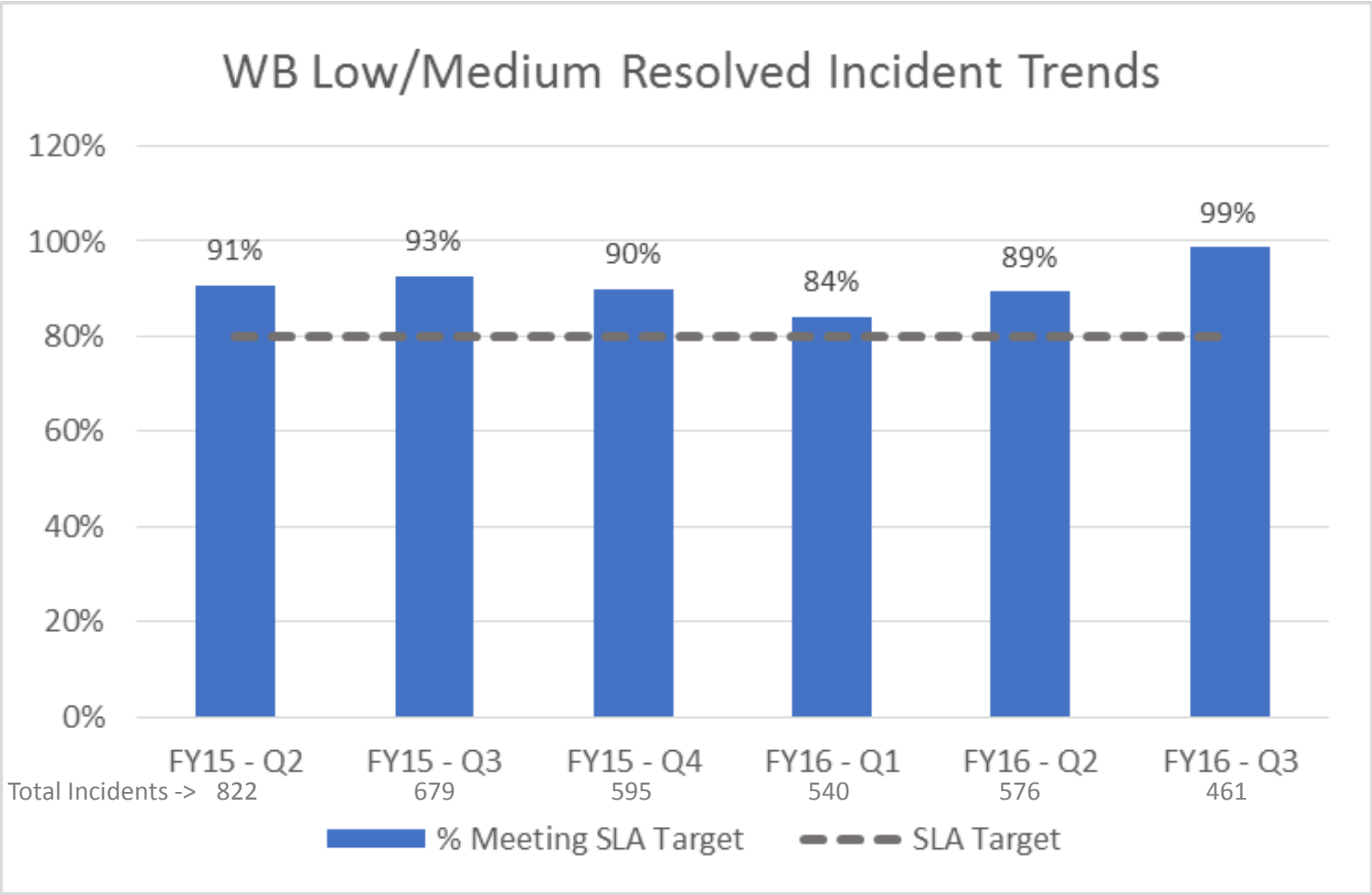
Capabilities

- Continuous monitoring
- Fusion of cyber threat intelligence with security analytics and hunting to proactively identify threats and implement defenses
- Effective linkage with the WBG-wide Emergency Management process
- Advanced analytics tools, automated threat intelligence tool
- Intrusion hunting
- Skilled security staff

ISOC Shift Operations



Incident Management SLA Trend



SLA Target: Low/Medium incidents contained by ISOC in categories (Hacking, Malware, and Social Engineering) within 3 days

Security Incident Response – Tiered Support

Tier I (ISOC) – 24x7 Security Monitoring

- Security monitoring from multiple sources
- Event correlation and analysis
- Triage and initial impact analysis
- Incident identification and escalation
- Incident data entry
- Reporting and follow up
- Quarantine Release

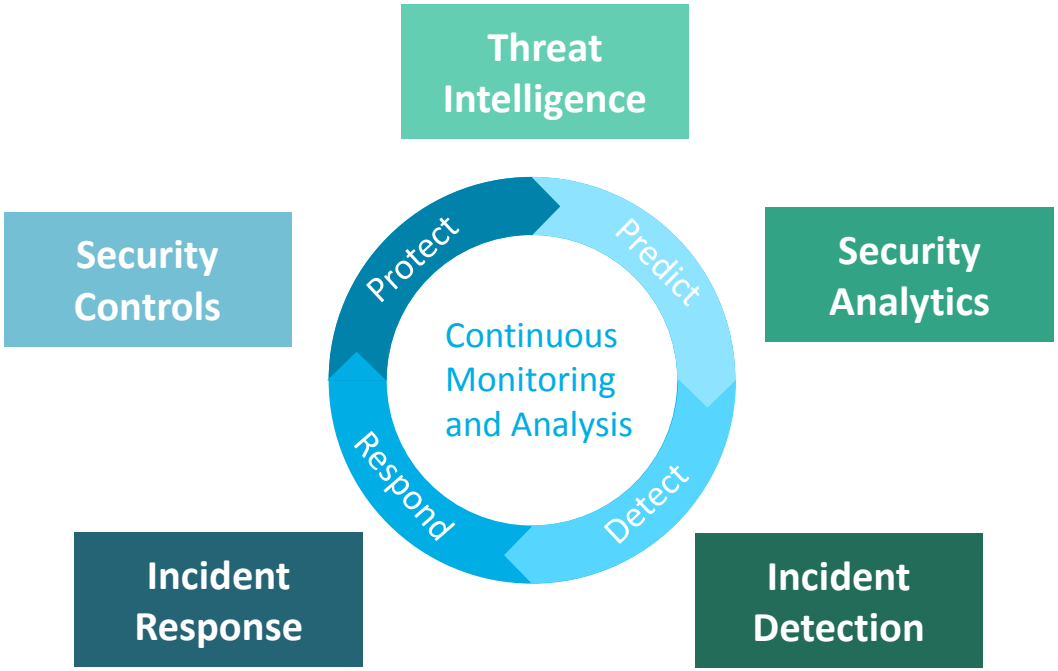
Tier II (ISOC and HQ On-Call Incident Handler)

- Virus and malware remediation
- Resolution of Medium/Low severity incidents
- Log analysis and follow-up on critical events
- Limited IR
- Incident coordination and management
- Identifying hostile information from dynamic malware analysis
- SIEM maintenance
- Vulnerability scanning
- Cyber threat intelligence: collect threat information; organize, correlate, and analyze; provide alerts & notifications
- Take action on threat intelligence information

Tier III (Critical Incident Response and Remediation and Security Engineering in HQ)

- Critical Incident Response Team
- Vulnerability management and remediation
- Resolution of high severity and complex incidents
- requiring changes to controls, i.e. log management or IDS rule changes
- Forensics

Putting it Together - People, Process, Technology



Lessons Learnt

- Outsourcing security monitoring to MSSP still requires onsite resources for analysis and coordination
- Running 24x7, 3 shifts on weekdays and weekends
- Retention and career development of security talent
- Executive support and communications
- Incident response cannot be effectively transferred or outsourced to vendors

- Business continuity (HQ shift)
- Process integration
- Security incident response needs to be integrated with corporate emergency response
- Take a phased approach
- Share cyber threat knowledge with and across industries, and collaborate with your peers
- Metrics and Key Performance Indicators

- Leverage available market capabilities
- Log management and advanced analytics

WBG Cybersecurity Strategy and Key Initiatives

Next Generation Cybersecurity Strategy (NGCS)

From…	To…
• Just protect the perimeter	• Protect critical information
• Risk avoidance approach	• Risk management approach
• Reactive security against emerging threats	• Proactive defense against emerging threats
• Security is IT's responsibility	• Security is a shared responsibility
• Security is the bottleneck	• Security is a business enabler

Continuous improvement of our Defense-in-Depth capabilities through **people**, **process**, and **technology**

WBG Focus Areas

- Strengthen foundational preventative controls and threat management and incident response capabilities
- Engage with the business to strike balance between being secure while remaining business-driven
- People, process and technology
- Invest in adaptive security and analytics
- Retention and development of skilled security and IT risk professionals

Key Initiatives

- ITS Policies and Procedures Revamp
- Ongoing Security Awareness and Training (i.e. Phishing Exercises)
- WB and IFC information governance initiatives

- Cyber Threat Preparedness
- Data Breach Notification Framework
- Third Party Vendor Risk Management

- Cloud First Strategy & Adoption
- Data Loss Prevention (DLP) and access control
- Threat Analytics