RSA Conference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: SDS1-R02

Building and Sustaining an Effective Incident Response Center

Sunil Varkey

Chief Information Security Officer
Wipro

@sunilvarkey

#RSAC

Drivers

- Compliance / Regulatory requirements
- Centralized monitoring & responding to IT - availability incidents
- Monitor the effectiveness of the security controls and recommend improvement, move from reactive response to proactive mitigation
- Build infrastructure to retain centralized event logs for analysis, investigation purpose – Isolated / Integrated
- User - IT activity monitoring / Threat intelligence / visibility / Real time alerts
- Part of institutionalized, formal detection and response capability – Incident management and Real-time decision support system
- Peer pressure / status symbol

WIPRO
Applying Thought

Mission & Vision

- CERT - Computer Emergency Response Team
- CSIRT - Computer Security Incident Response Team
- IRT - Incident Response Team / IRC – Incident Response Centre
- CIRT - Computer Incident Response Team
- SOC / CSOC – Security Operations Centre / Cyber Security Operations Center
- CIRC - Computer Incident Response Capability or Center
- SIRT / SERT - Security Incident / Emergency Response Team
- SNOC - Security & Network Operations Center

Align with business objectives, priorities and risk posture

WIPRO Applying Thought

Constituents & Success factors

Constituents

- Business
- Technical Teams
- Audit / HR / Legal / Privacy
- Compliance & Regulatory
- Physical and Crisis Management
- CIO / CRO / CMO / COO

Success factors

- Define expectations
- Determine the right services
- Consistent quality of service
- Communication / Reporting
- Right Metrics & Feedback
  Build the trust

Timely Information and Intelligence in Context & Perspectives

WIPRO
Applying Thought

Threat Actors & Targets

Prioritization

- Typology of threat actors
- Strategic intent
- Motive
- Capabilities
- Targets

Motive

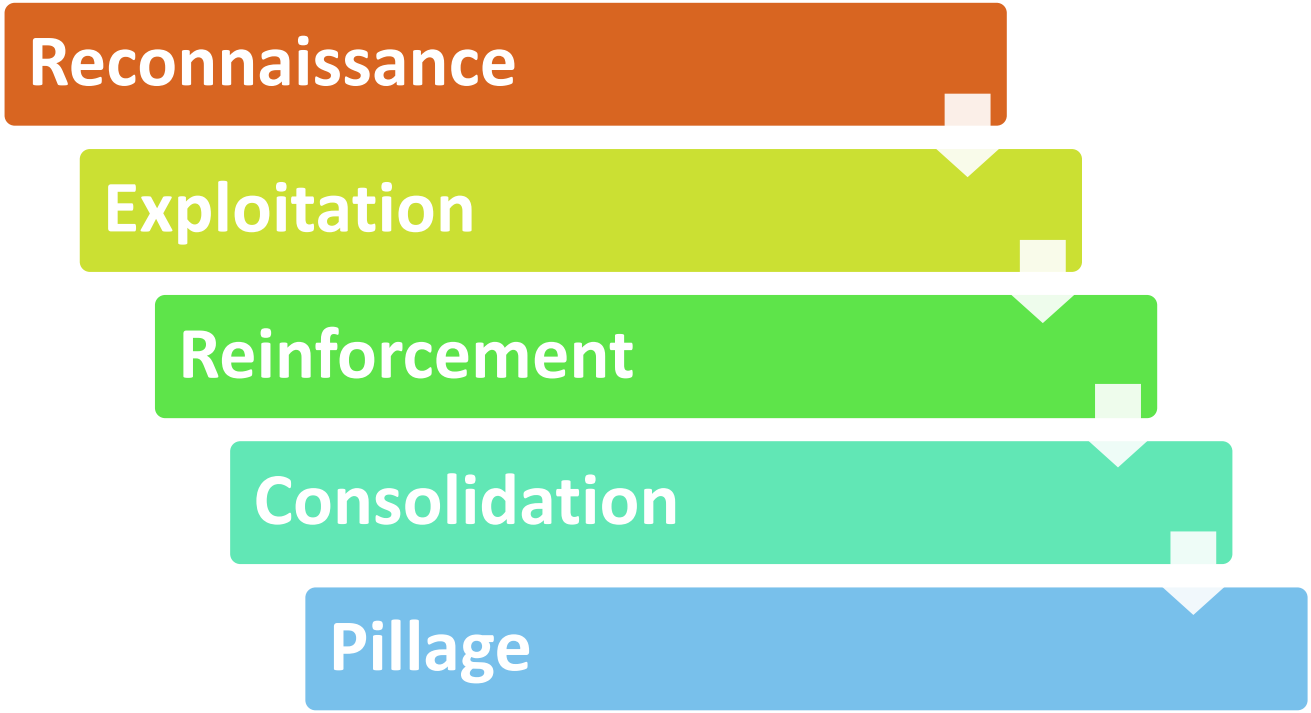
- Financial damage
- Disruption or control
- Espionage
- Fraud / Corruption
- Blackmail / Sabotage
- Access to data

Actors

- Cybercriminals
- Terrorist / Insurgents
- Hacktivism / Patriotism
- Script kiddies
- Cyber-researchers
- Advanced / Rogue States
- Competition

Varies between Industry, service and Geo locations

Incident & Defense Lifecycle



Preparation

Detection

Analysis

Containment

Eradication

Recovery

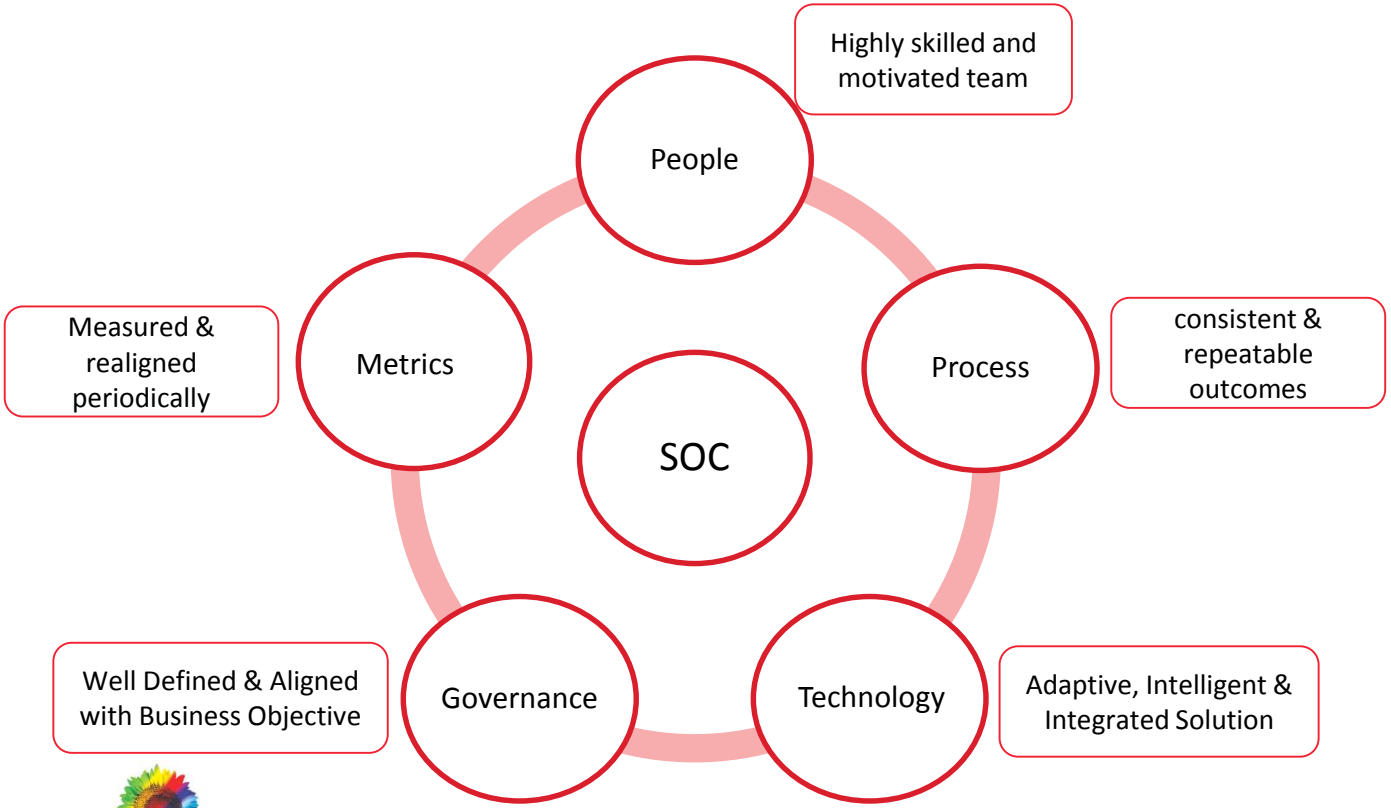
RCCA

Key Challenges

- Availability of the right people with right skills and spirit
- False positives resulting in flooding of Security irrelevant alerts
- Tool limitation in handling large data pool, advance queries and analytics capabilities to provide required context and situational awareness
- Insufficient & irrelevant event collection – Cloud, Legacy, Applications
- Highly sophisticated, coordinated and zero day attacks which are mostly unpredictable
- Complicit users, misaligned policies, lack of adequate logs, business support …

Challenges from every direction and is dynamic

Sustenance & Innovation



- People
- Process
- Technology
- Governance
- Metrics

WIPRO
Applying Thought

SOC Governance

- Foundation Process
- SOC Operations
- Incident Response
- Framework: The high level framework which defines the various elements, their objectives and the operating policies of the SOC
- Processes: Detailed description of the processes, their objectives, inputs, outputs, users, recipients, consumption, metrics etc.
- Procedures & Work Instructions: Detailed templates & documents

Strong Governance for operational excellence, effectiveness & Sustenance

WIPRO
Applying Thought

Foundation Process

- Log Management
- Change Management
- Release Management
- Configuration & Capacity Management
- Resource Management / Vendor Management
- Continues Improvement / Quality / SLA Management
- Business Continuity Management
- Legal & Compliance

WIPRO
Applying Thought

SOC Operations

- SOC Security Policy / Security Organization
- Service Catalog
- Service Desk & Work Flow / Service Delivery Platform Management
- Physical Security
- Service Induction / Termination
- Access Management & Segregation of duties
- Constituent Communication Management / Escalation Process
- Human Resource, Risk Assessment, Auditing & Reporting

Incident Response

- Event Monitoring & Analysis
- Threat intelligence collection, Analysis and consumption
- Use case development and Optimization
- Incident Communication, Follow ups & Response framework
- Incident Life cycle management & Root Cause Analysis
- Asset, Data & Incident Categorization and Classification
- Generic & Specific Incident Handling / Management

Use case development

- Business case, scope and purpose
- Threat modelling
- Top down vs Bottom up
- Data sources and event of interests
- Reports and Metrics
- Thresholds and response plan

Goal..

- Was the attack credible?
- What was the attack?
- Who was the attacker?
- Was the attack success / failure?
- What was the motive?
- Was there any data extrusion?
- Was the asset vulnerable?
- Was the attack unique?
- Where did attack originate from?
- Which is the target?
- Potential Root cause

Team - varied skills

Roles	Structure	Accountability
• Infrastructure support • SIEM & Tool Specialists • Automation SME's • Security Analysts • **Incident Handlers** • Researchers / Hunters • Forensics / Reverse engineers • Shift Leads	• Internal Distributed • Internal Centralized • Distributed & Centralized • Coordinating • Partially / Fully outsourced • Virtual	• Full Authority • Shared Authority • No Authority

Right people on board with the right attitude and spirit

Incident Handler

- Play book director
- POC for Events of Interest reported both internally and externally through its lifecycle
- Excellent technical and communication and soft skills to articulate and coordinate with varied constituents across the globe
- Passion and persistence
- Continues leaner and leader, matured from Incident responder to Handler

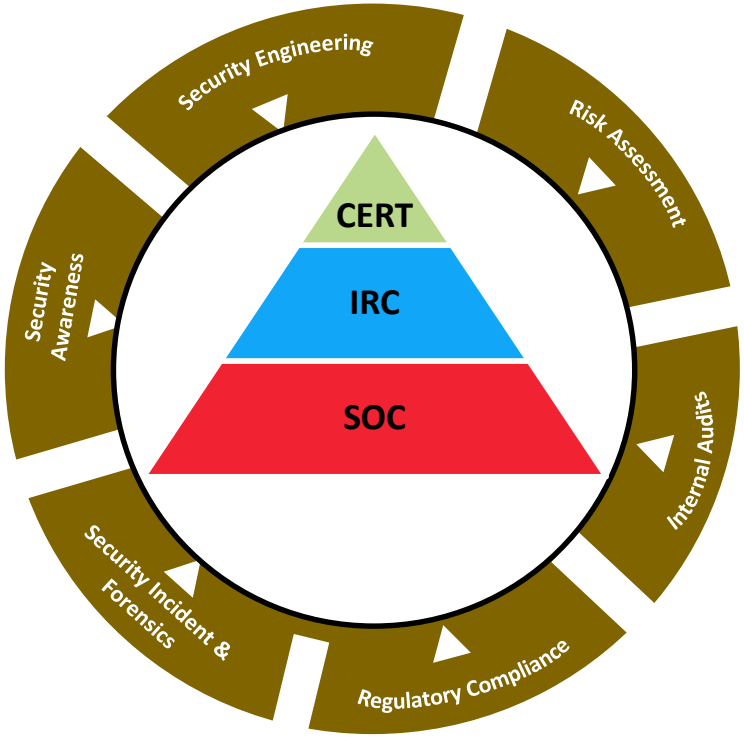
Tools

- Enterprise Device, application and log format coverage & support
- Ease of use, Integration and deployment
- Correlation, Query and Reporting capability and flexibility
- External threat and vulnerability feed integration
- OEM - Continues Innovation, support and roadmap
- TCO - Licensing models, scale, storage compression, Hardware

Tool strategy should be based on defined Business objectives

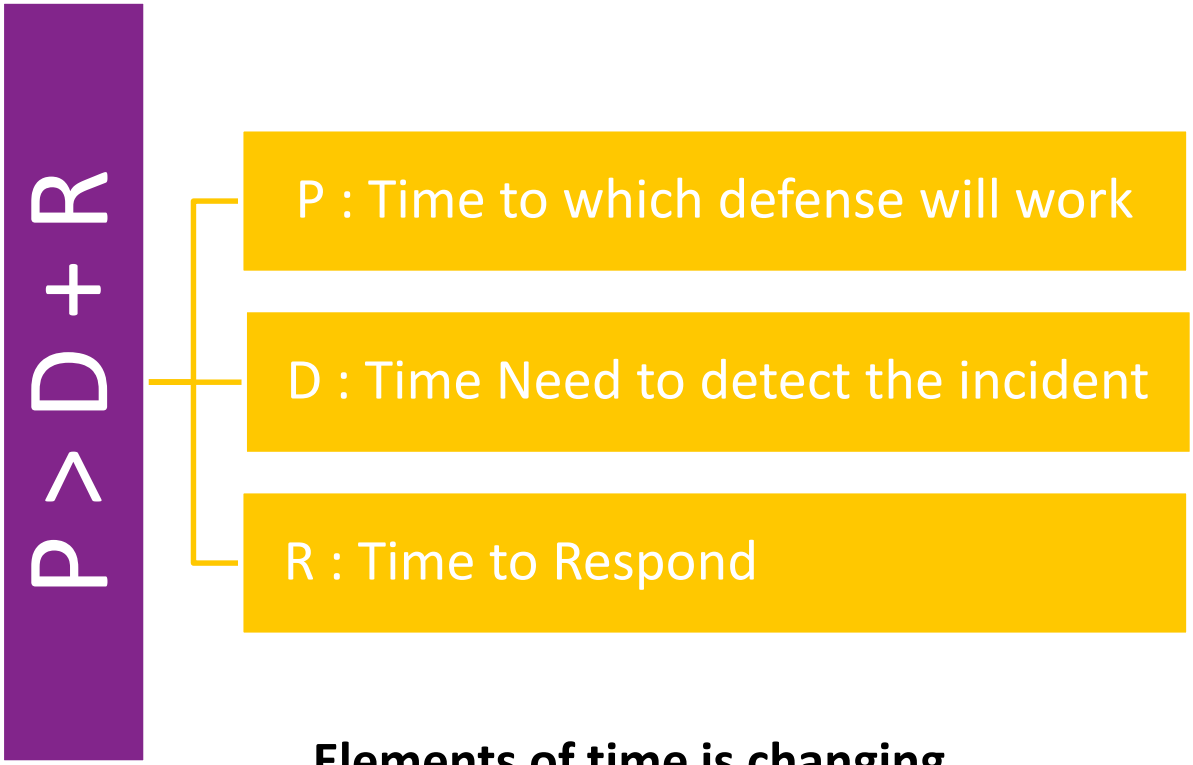
Incident Response Center Framework

Cyber Defense	Tiered Function R&R
Computer Emergency Response Center (CERT)	Cyber Intel Collection and Analysis, Threat Assessment , Threat Actor / Vector analysis, Advanced Forensic Analysis
Incident Response Center (IRC)	Real-Time Monitoring & Triage, Event Analysis, Trending & correlation, Incident coordination & Response, Root Cause Analysis and Mitigation, Situational Awareness, Custom signature creation, Scripting & automation
Security Operations Center (SOC)	Availability, Configuration, Change and Release Management, Sustenance of Security Devices, Emergency alerts & warnings, Call center



Continues Incident monitoring, analysis, Response & Reinforcement

Time based Security Incident Defense



Elements of time is changing

Models

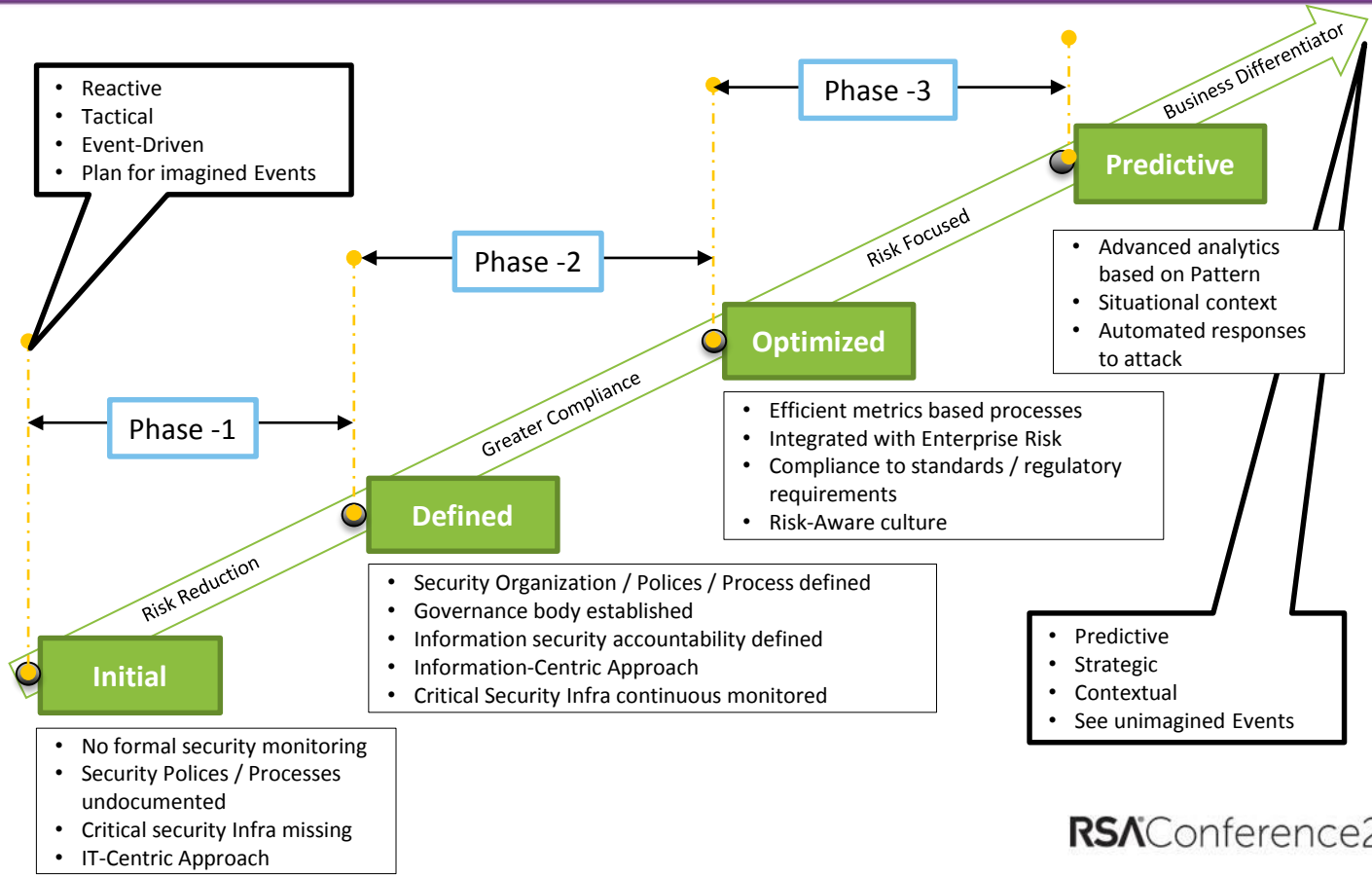
Structure	Availability	Deliverables
• Centralized • Federated • Remote • Alert based	• 24x7 • Follow the Sun • On Demand • Consultative	• Free • Membership • Basic + Value added service • Research / Advisories / News Letters • Ad Hoc Service • Professional Services

Defensible Network

- Persistent organizational commitment
- Inventories, mapped & Documented
- Claimed
- Controlled, Minimized & Baselined
- Assessed, Mitigated & Current
- Monitored & Measured

Pre-requisite for an effective Incident Response Centre

Incident Response Maturity Model

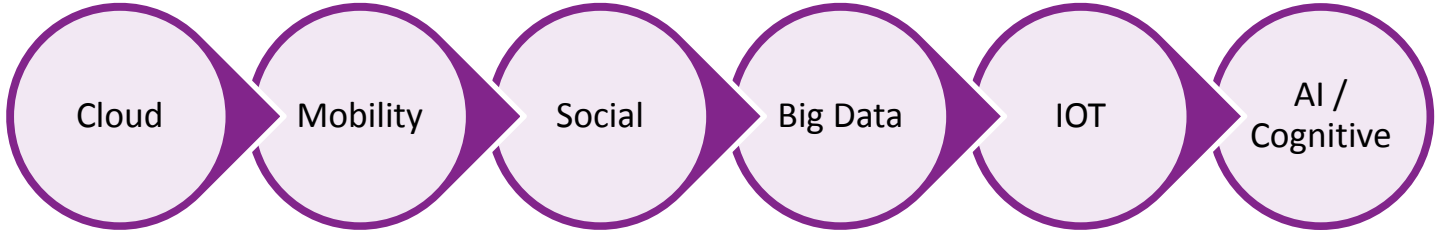


Optimized & Effective IRC

- Should be able to differentiate between normal to abnormal to suspicious with right baselines
- Should know yourself and enemy – SWOT
- Should be supporting a defensive network
- Sensible time to identify and respond to all incidents covering when, who, what, how, where and why
- Well defined and tested playbook and incident response strategy
- Passionate and skilled resources
- Management and Business should be part of IRC along with IT

Central point for Incident response with full visibility across enterprise

NEW BUSINESS IMPERATIVE..



Evolving Regulations
Sophisticated & Targeted attacks
Connected partner / Platform echo systems
Blurred perimeters, Encrypted traffics
New business models & expectations

Share
Everything
Everywhere

Information
Intelligence
Insights
Opinions

Incident response will become a priority for the security program &
Budget allocation for incident response will go higher over the years

Wrap up – Key takeaways

- Revisit Short term and long term vision and stakeholders expectations
- Initiate project for a defensible network
  - Noise reduction
  - Malware eradication
  - Improving patching and hardening compliance
- Analysis of
  - logging levels
  - SIEM Rules,
  - Reports and Dashboards

Acknowledge the great work, blogs, publications

- MITRE
- SANS
- CERT
- Richard Bejtlich
- Anton A. Chuvakin
- Bruce Schneier
- Gartner

Thank You

Sunil Varkey

CISSP, CIPP/US, GSNA, CISA, CGEIT, CRISC, ABCP, *ITIL- V2 (Red Badge) & Six Sigma GB certified*

Twitter: @sunilvarkey