Deloitte.

Cybersecurity Operations Center: Cyber Preparedness and Lesson Learned

AITRI SEMINAR ON
NEW TECHNOLOGY RISKS AND CYBER SECURITY, KUALA LUMPUR

14 Feb 2017

Cyber

Contents

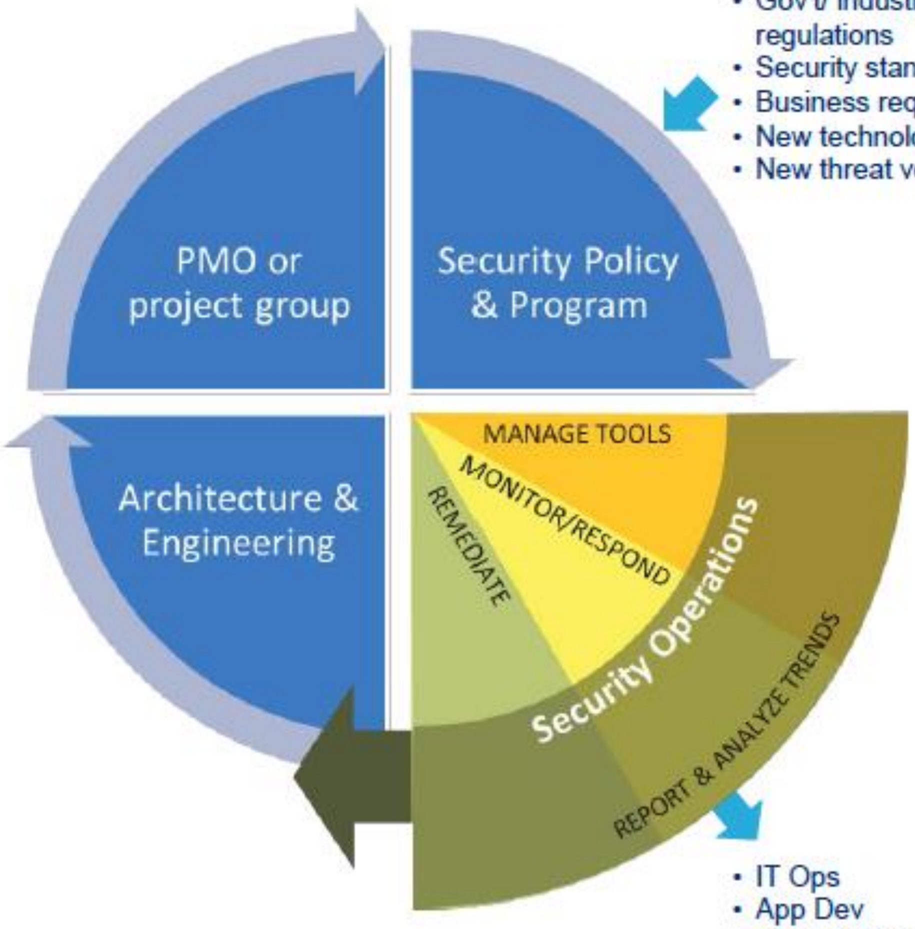
Learning Objectives
You will learn about…

Cybersecurity Operations

o What a Cybersecurity Operations Center (CSOC) is and the primary capabilities a CSOC may have

o Typical CSOC organizational structure and Governance aspects of a CSOC, including the core scope and services of a CSOC

Cybersecurity Operations Functions are Changing



- Gov't/ industry regulations
- Security standards
- Business requirements
- New technologies
- New threat vectors

- IT Ops
- App Dev
- Lines of Business
- CISO/CTO
- Audit & Risk

TRADITIONAL ROLE:

- Actualize security policy
- Monitor and respond to incidents
- Manage tools
- Assimilate new policies and requirements

NEW PRESSURES:

- Facilitate business growth and demonstrate value
- Ensure protection against high-impact threats

Requires a change in focus from compliance and investigation to a threat-based model

Monitoring must be Risk-Aware & Threat-Centric

- Security teams are under-resourced relative to potential impact of targeted threats.
- Business leaders need assurance that key assets are protected.
- The starting point for effective monitoring:
  - *What are my key assets, information and processes?*
  - *Who would be motivated to steal, manipulate, or disrupt them?*
  - *What tactics might they use?*

DIFFERENT INDUSTRIES FACE DIFFERENT THREATS…

◢ FINANCIAL SERVICES
- Attempts to disrupt economic infrastructure
- Organized crime to steal money through ATMs or account manipulation

◢ PUBLIC UTILITIES
- Take-down of grid systems
- Manipulation of meters and billing systems

◢ MANUFACTURING OR BIOTECH
- Theft of trade secrets and IP

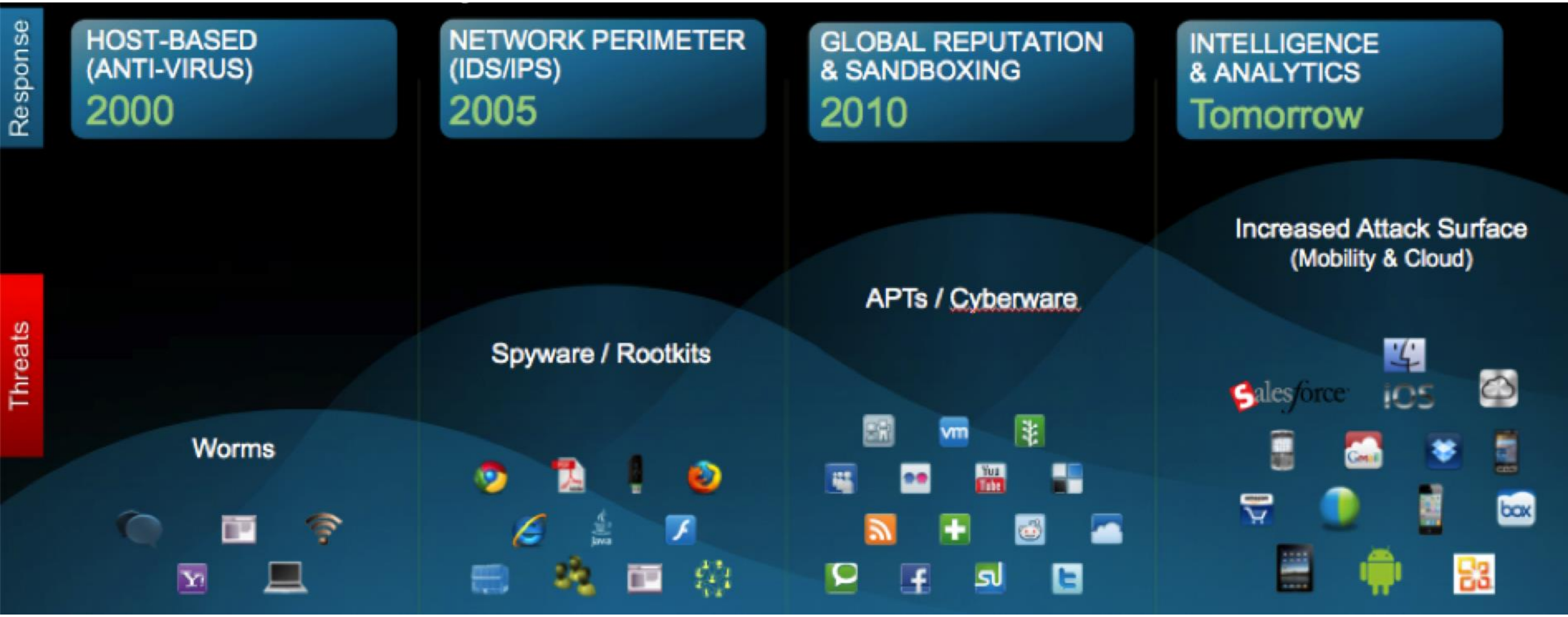
◢ RETAIL
- Theft of credit card databases
- Theft of inventory

◢ TELECOM
- Theft of account credentials for resale
- Disruption to critical communication systems

… in which malicious actors use various tools, tactics, and procedures.

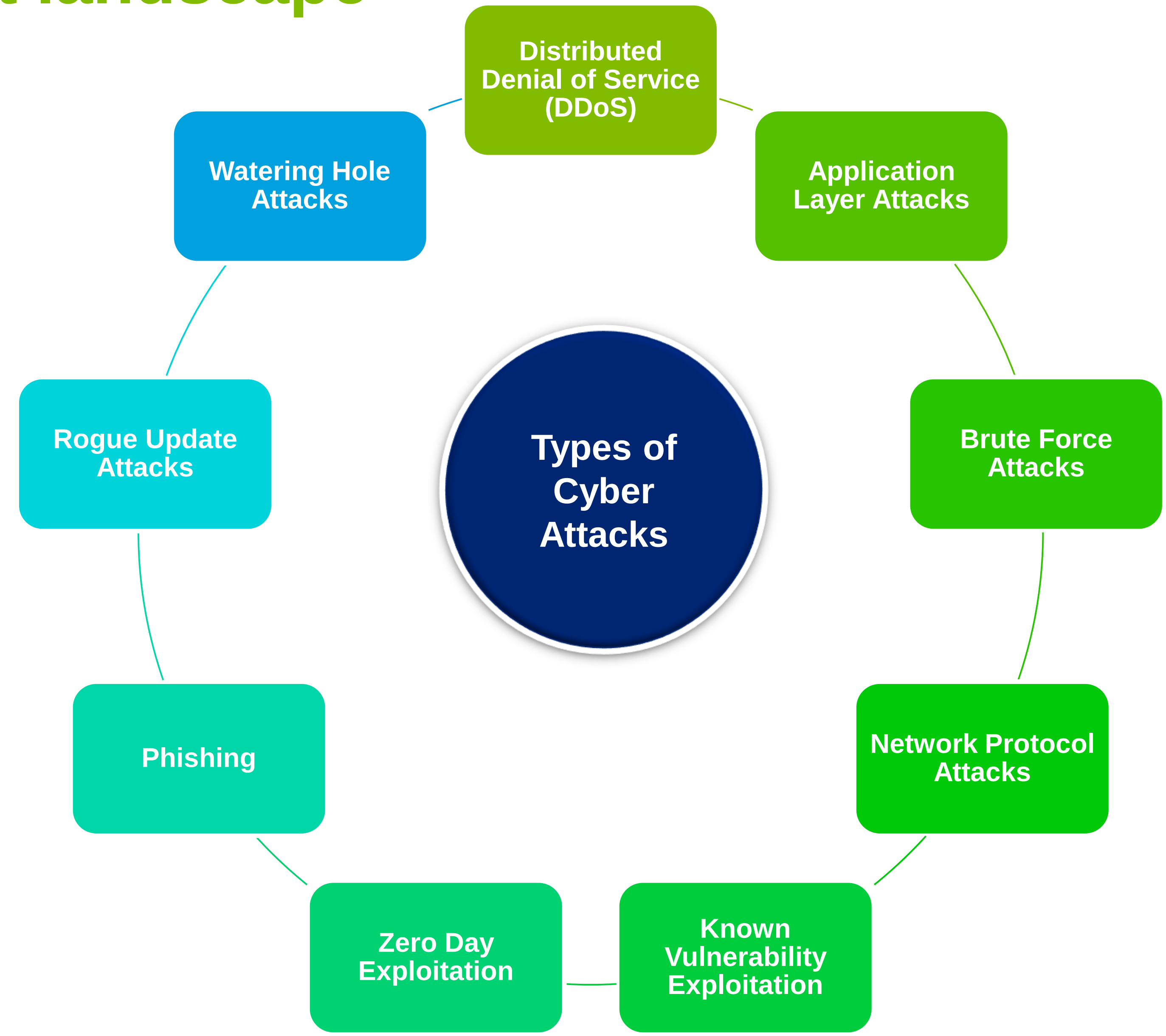
Threat Landscape

The cyber threat landscape will continue to deteriorate as the attack surface expands with advances through digital innovation via IoT, consumerisation of enterprise mobility and cloud.



Source: http://blogs.cisco.com/ciscoit/cisco-security-intelligence-operations-defense-in-depth

Threat landscape



What Is a CyberSOC (CSOC)?

Cyber Security Operations Center (CSOC)

A CSOC is a highly skilled *team* primarily composed of security analysts hierarchically organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents.

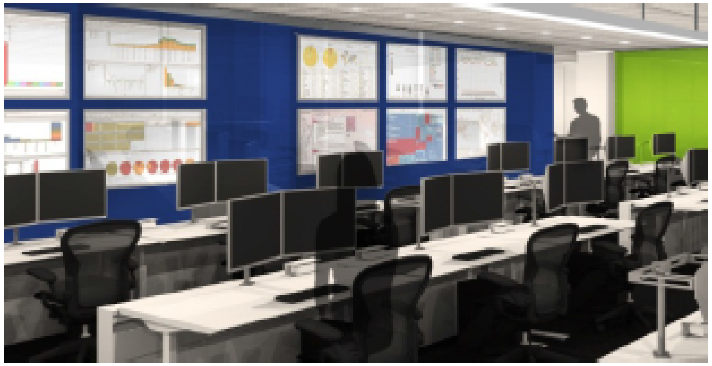
Under the **authorities** specified by a **charter**, and through the judicious use of technologies and processes, this team delivers a set of **services** that usually include the management of the attack, vulnerability, and threat lifecycles:

- **Attack** – An attempt (successful or not) to damage, disrupt, or gain unauthorized access to a computing system, a network, or data, or certain classes of policy violations.
- **Vulnerability** – A weakness in a computing system, such as a flaw in software code or weak configuration settings, that may allow an attacker to compromise that system.
- **Threat** – The potential for an actor or agent (external or internal) to exploit a vulnerability or otherwise leverage some technique to cause an incident.

These services and their underlying **capabilities** support the **information assurance** of a bounded set of users, computers, networks, and other assets known as the **constituency**.

The CSOC leverages situational awareness – obtained partially through cyber intelligence – to guide its daily activities, and provides the same to its constituency.

These activities commonly include monitoring and managing the output of a fleet of sensors, scanners, and other analytic tools, and usually take place on an operations floor.

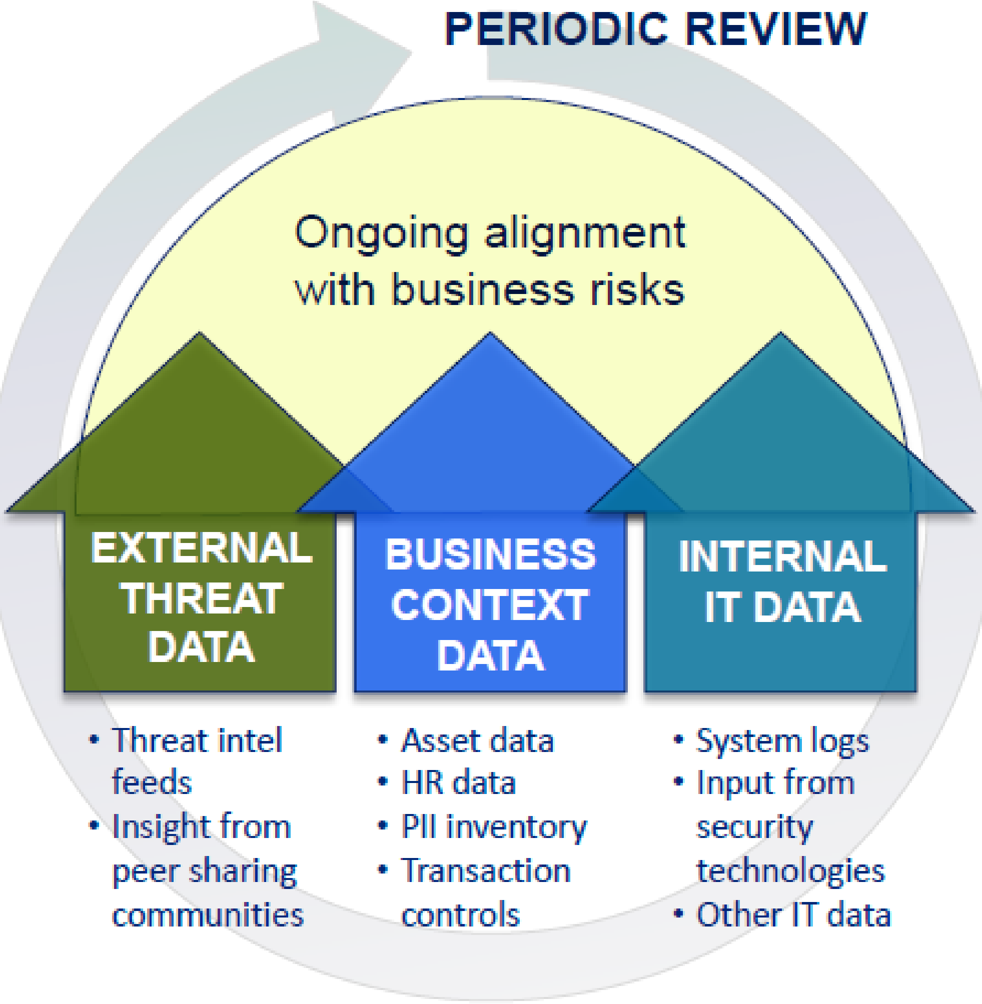


An Effective CSOC must be Dynamic and Agile

- The business continually expands use of technology
- Many kinds of rapidly changing data sources must be incorporated
- Change management and risk review processes must be integral to every day operations

Few organizations leverage business context data

Few centrally correlate threat intelligence effectively



PERIODIC REVIEW

Ongoing alignment with business risks

EXTERNAL THREAT DATA

- Threat intel feeds
- Insight from peer sharing communities

BUSINESS CONTEXT DATA

- Asset data
- HR data
- PII inventory
- Transaction controls

INTERNAL IT DATA

- System logs
- Input from security technologies
- Other IT data

CSOC should take a Service Management Approach

Become an internal MSSP

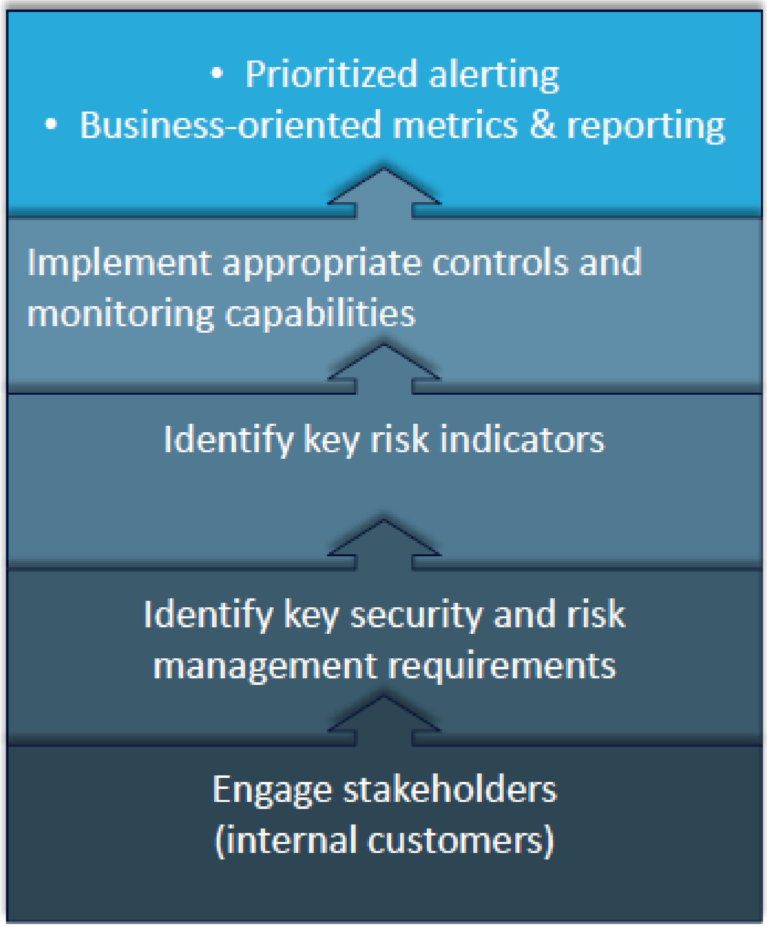
- Compliance & audit support
- Basic security device management
- Encryption services
- Critical application monitoring
- Fraud prevention support

Offer a range of operational capabilities

- From monitoring of basic controls…
- To advanced ability to detect exceptions to "normal" business processes

A service-driven CSOC:

- Ensures business alignment
- Demonstrates value
- Can more effectively interface with the CXO to secure future funding


- Prioritized alerting
- Business-oriented metrics & reporting

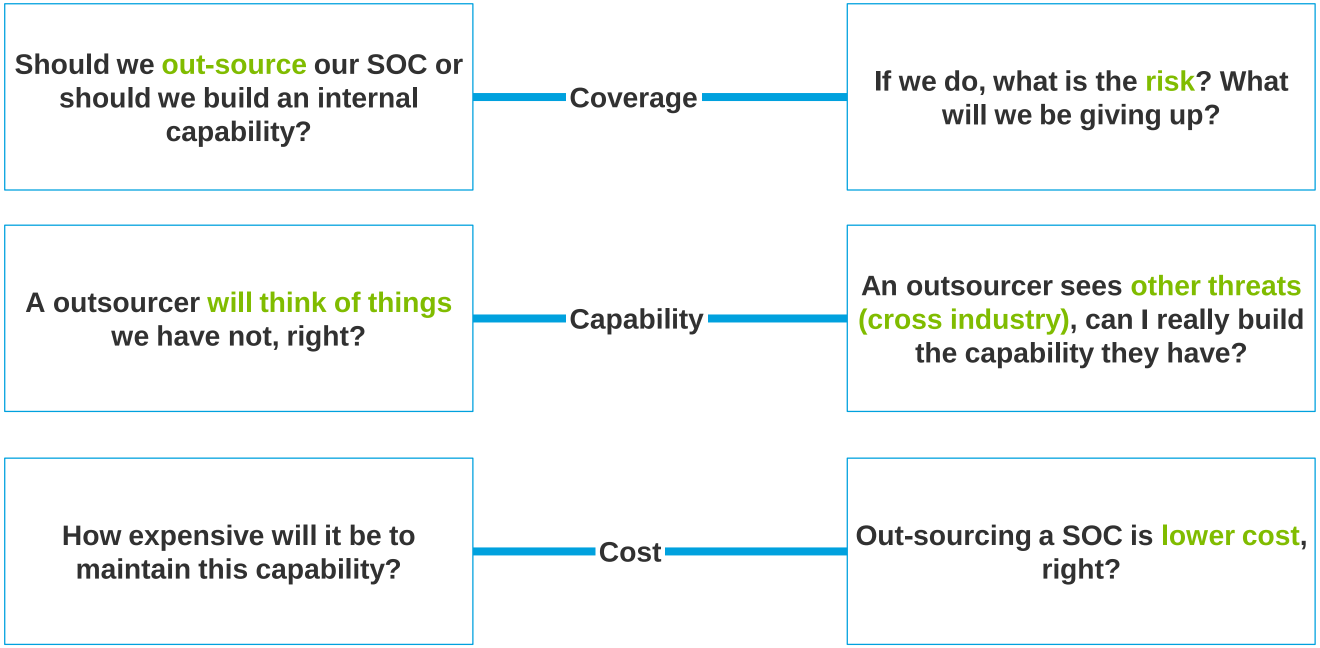
Implement appropriate controls and monitoring capabilities

Identify key risk indicators

Identify key security and risk management requirements

Engage stakeholders (internal customers)

Determine the best CSOC Model for YOU



Should we out-source our SOC or should we build an internal capability?

Coverage

If we do, what is the risk? What will we be giving up?

A outsourcer will think of things we have not, right?

Capability

An outsourcer sees other threats (cross industry), can I really build the capability they have?

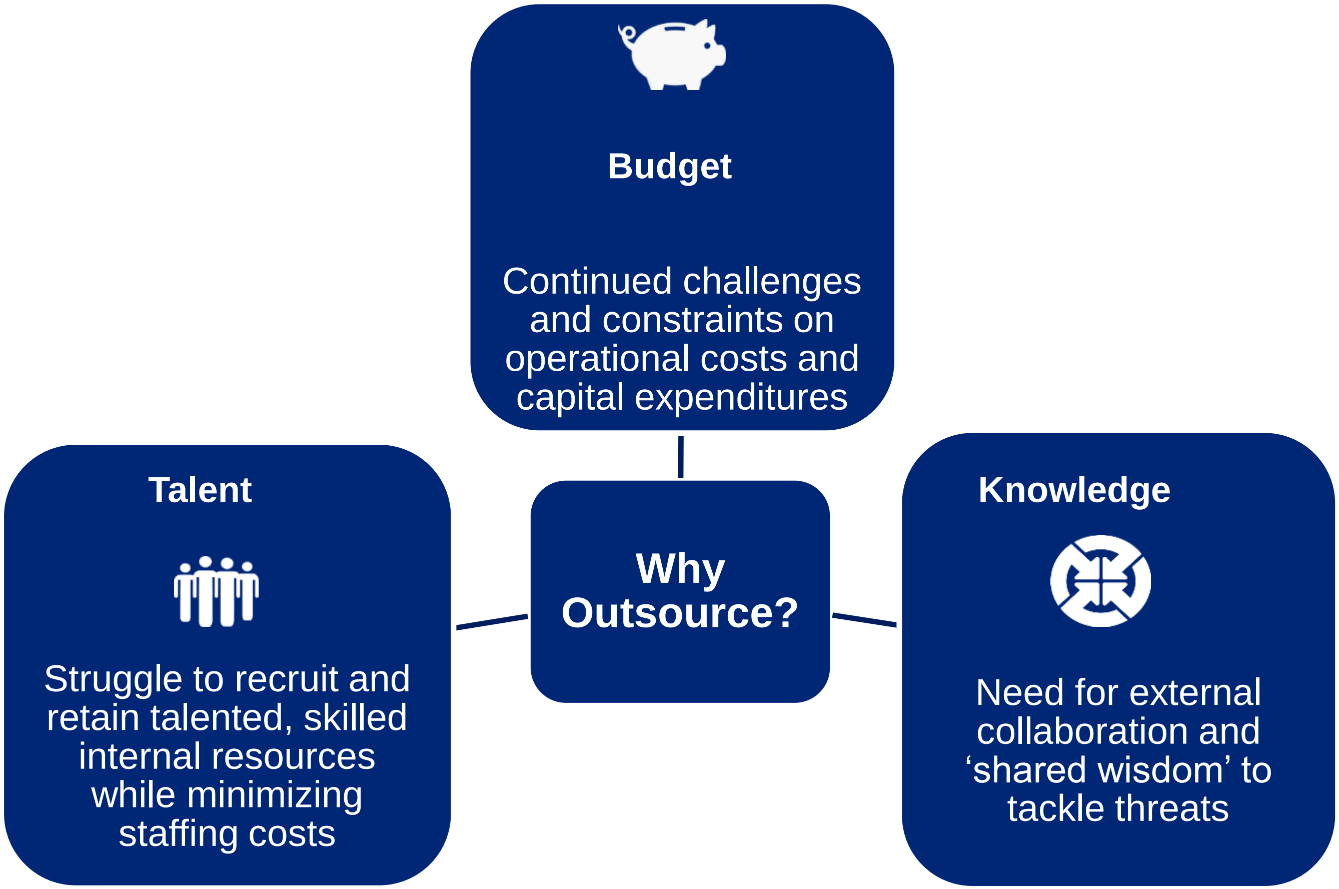
How expensive will it be to maintain this capability?

Cost

Out-sourcing a SOC is lower cost, right?

Why outsourcing

There are a number of key drivers that lead businesses to look to managed security services.



Budget

Continued challenges and constraints on operational costs and capital expenditures

Talent

Struggle to recruit and retain talented, skilled internal resources while minimizing staffing costs

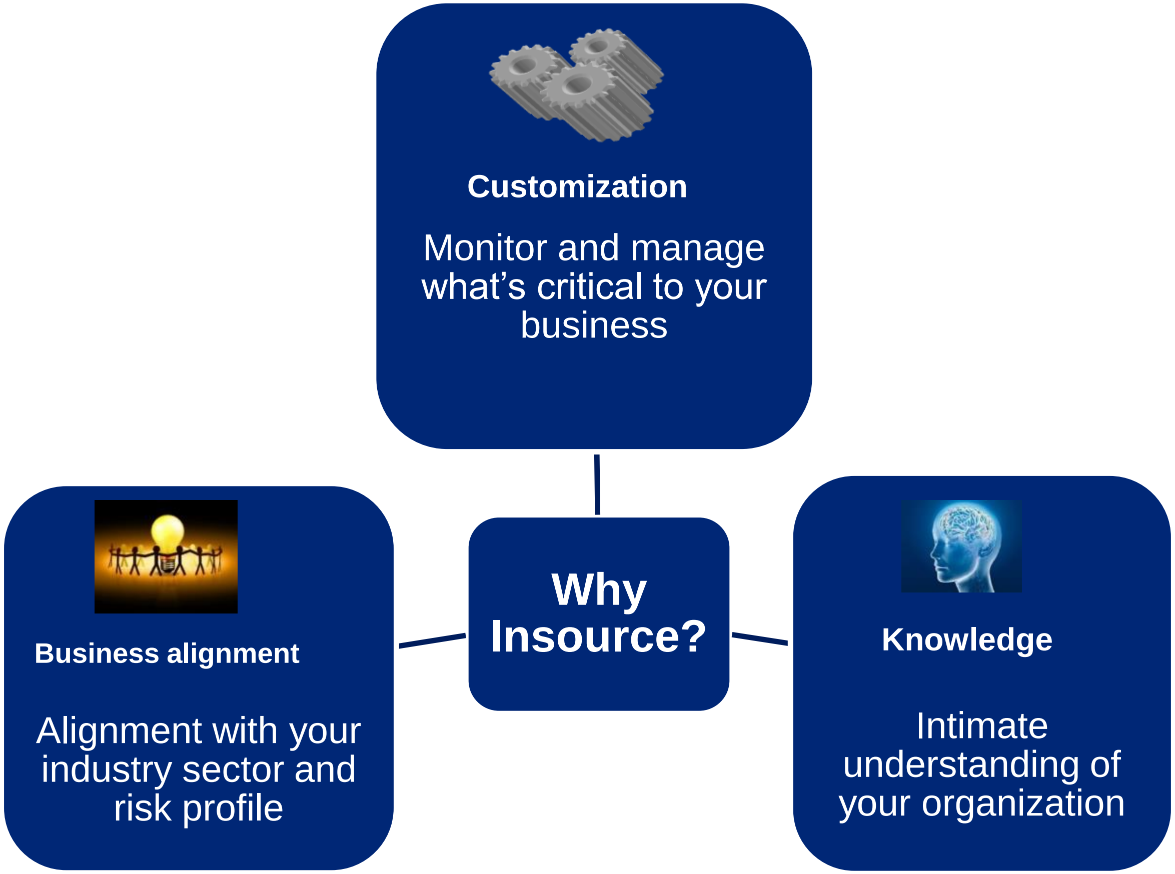
Why Outsource?

Knowledge

Need for external collaboration and ‘shared wisdom’ to tackle threats

Why in-sourcing

Drivers for in-sourcing security operations



Customization

Monitor and manage what’s critical to your business

Why Insource?

Business alignment

Alignment with your industry sector and risk profile

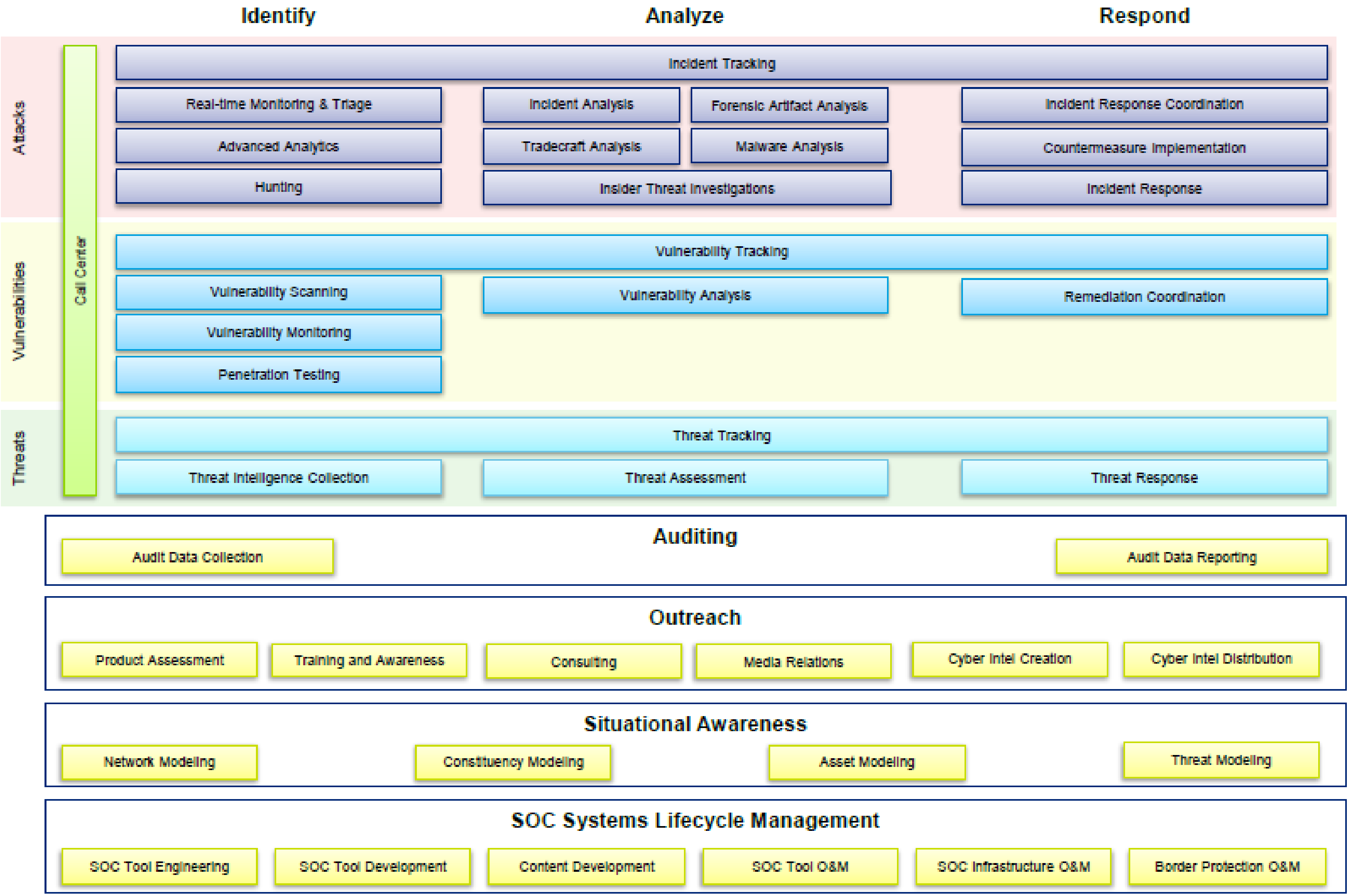
Knowledge

Intimate understanding of your organization

CSOC Model: insourcing, outsourcing, hybrid

1: Insource	2: Outsource	3: Hybrid
Industry and business alignment	Industry and risk profile alignment	Business, industry and risk profile alignment
Level one monitoring and management	Level one, two and three monitoring and management	Level one, two and three monitoring and management
Maintain and enhance existing use cases	Alignment of use cases to evolving threat landscape	Alignment of use cases to evolving threat landscape
Limited threat intelligence gathering	Proactive Cyber Threat Intelligence	Proactive Cyber Threat Intelligence
Resourcing required to operate three shifts	Round the clock monitoring, management and incident response	Round the clock monitoring, management and incident response
Hardware, build, run and maintain costs	Cloud based service – utility based costing	Hardware, build, run and maintain costs
Capex	Opex	Capex and Opex

CSOC Capability Model



Identify

Analyze

Respond

Attacks

Vulnerabilities

Threats

Call Center

Incident Tracking

Real-time Monitoring & Triage

Advanced Analytics

Hunting

Incident Analysis

Forensic Artifact Analysis

Tradecraft Analysis

Malware Analysis

Insider Threat Investigations

Incident Response Coordination

Countermeasure Implementation

Incident Response

Vulnerability Tracking

Vulnerability Scanning

Vulnerability Monitoring

Penetration Testing

Vulnerability Analysis

Remediation Coordination

Threat Tracking

Threat Intelligence Collection

Threat Assessment

Threat Response

Auditing

Audit Data Collection

Audit Data Reporting

Outreach

Product Assessment

Training and Awareness

Consulting

Media Relations

Cyber Intel Creation

Cyber Intel Distribution

Situational Awareness

Network Modeling

Constituency Modeling

Asset Modeling

Threat Modeling

SOC Systems Lifecycle Management

SOC Tool Engineering

SOC Tool Development

Content Development

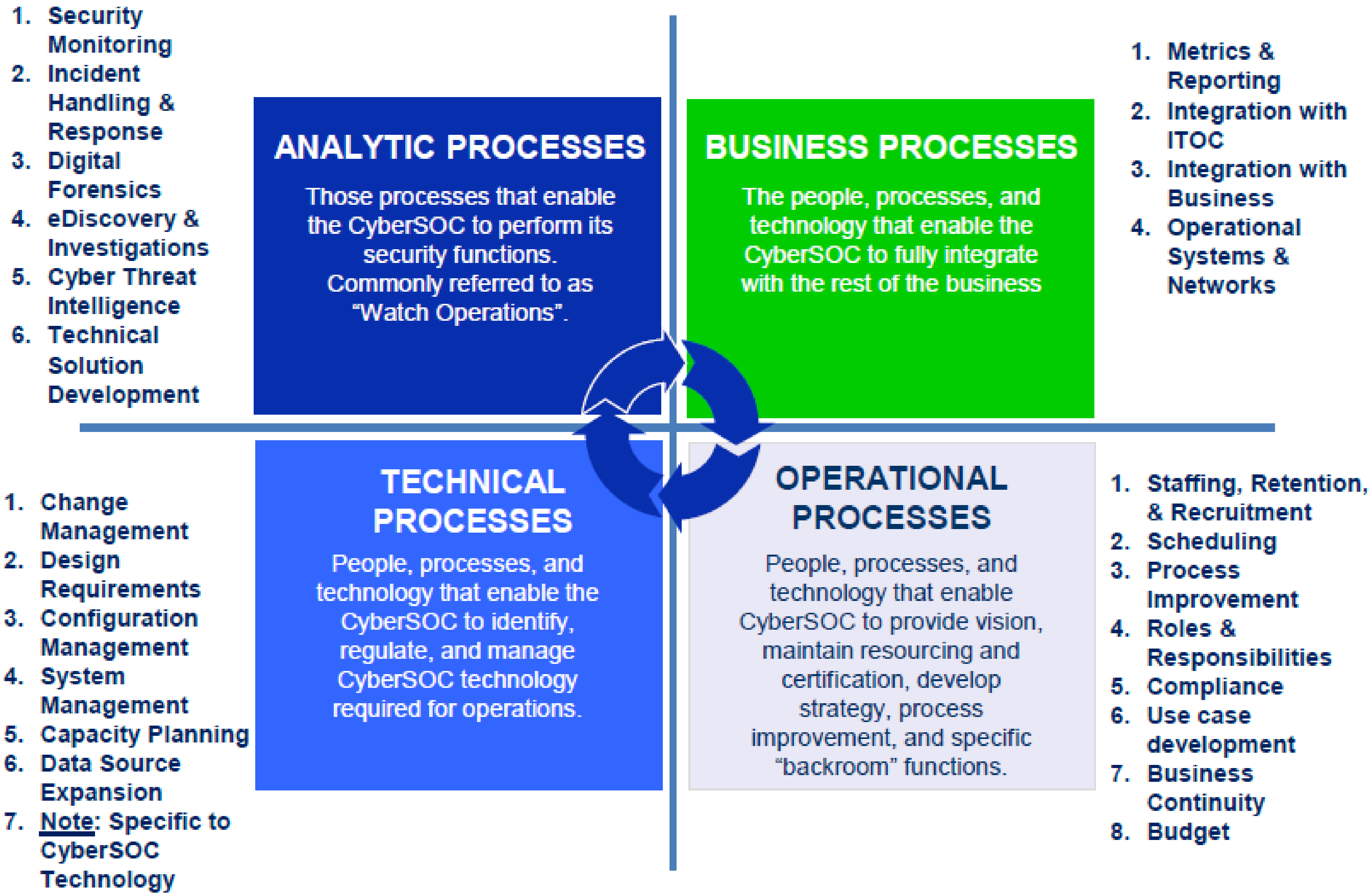
SOC Tool O&M

SOC Infrastructure O&M

Border Protection O&M

CSOC: Structure and Governance Model

CSOC: Integrated Process Model



1. Security Monitoring
2. Incident Handling & Response
3. Digital Forensics
4. eDiscovery & Investigations
5. Cyber Threat Intelligence
6. Technical Solution Development

ANALYTIC PROCESSES

Those processes that enable the CyberSOC to perform its security functions. Commonly referred to as “Watch Operations”.

BUSINESS PROCESSES

The people, processes, and technology that enable the CyberSOC to fully integrate with the rest of the business

1. Metrics & Reporting
2. Integration with ITOC
3. Integration with Business
4. Operational Systems & Networks

1. Change Management
2. Design Requirements
3. Configuration Management
4. System Management
5. Capacity Planning
6. Data Source Expansion
7. Note: Specific to CyberSOC Technology

TECHNICAL PROCESSES

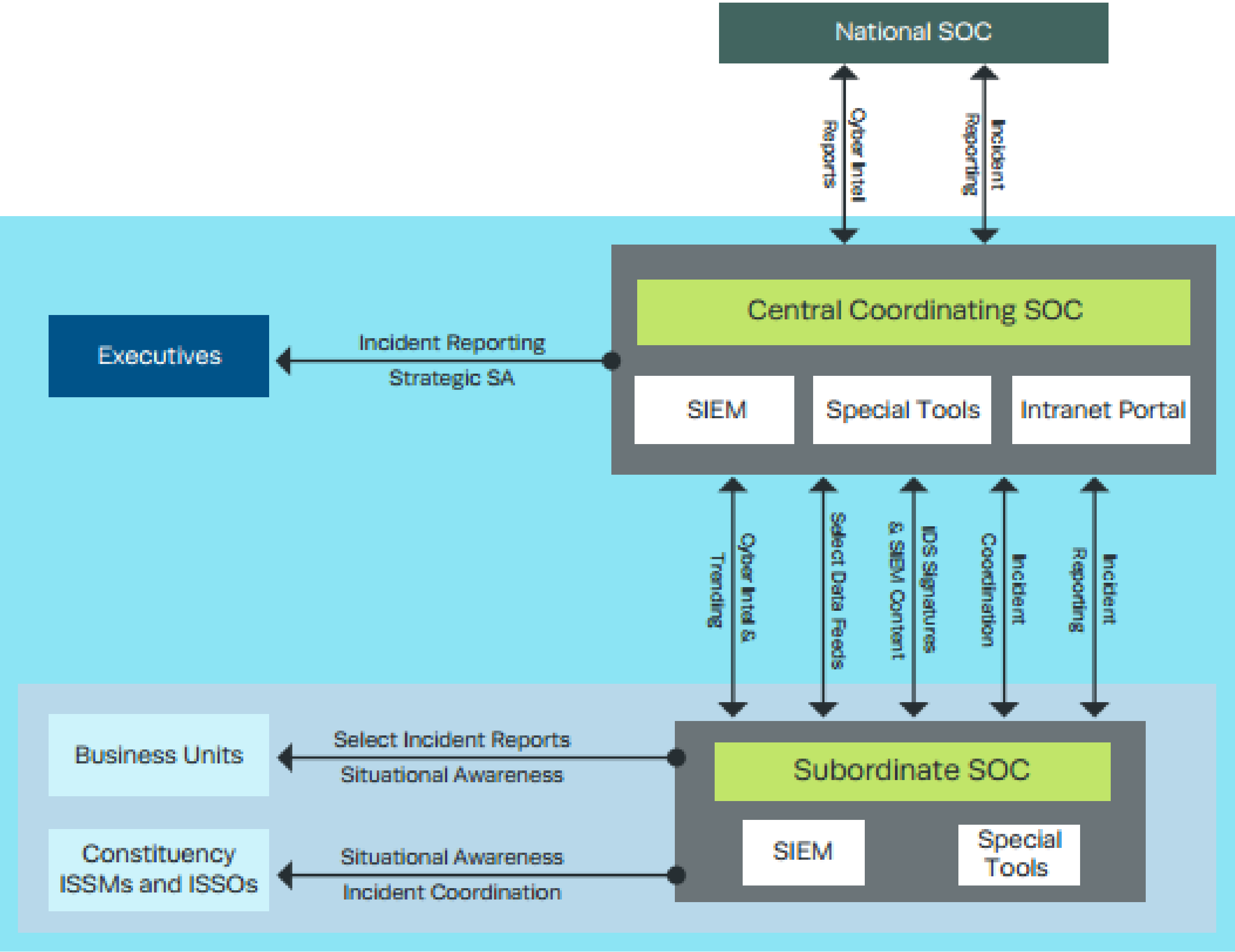
People, processes, and technology that enable the CyberSOC to identify, regulate, and manage CyberSOC technology required for operations.

OPERATIONAL PROCESSES

People, processes, and technology that enable CyberSOC to provide vision, maintain resourcing and certification, develop strategy, process improvement, and specific “backroom” functions.

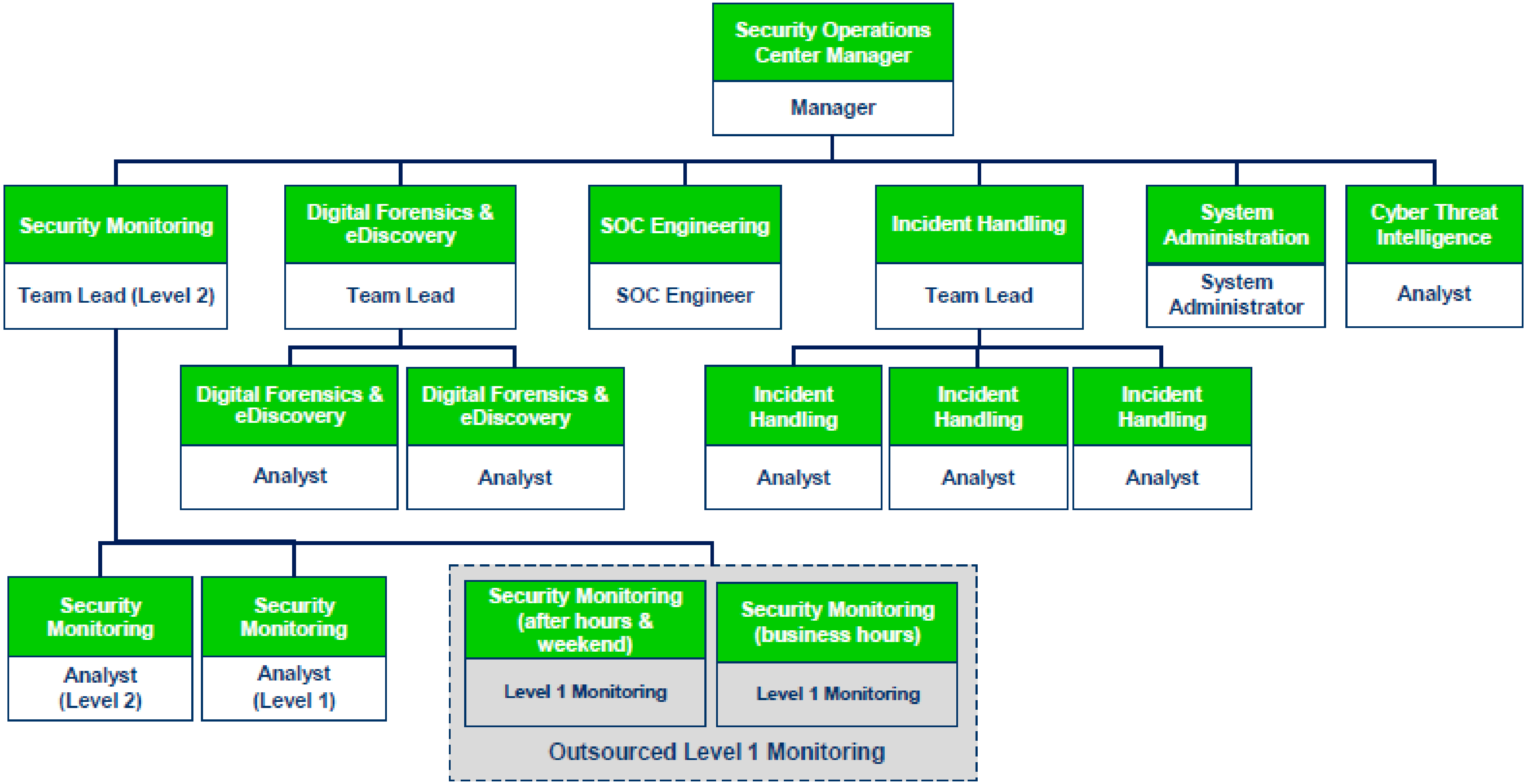
1. Staffing, Retention, & Recruitment
2. Scheduling
3. Process Improvement
4. Roles & Responsibilities
5. Compliance
6. Use case development
7. Business Continuity
8. Budget

CSOC: Sample Data Flow



https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

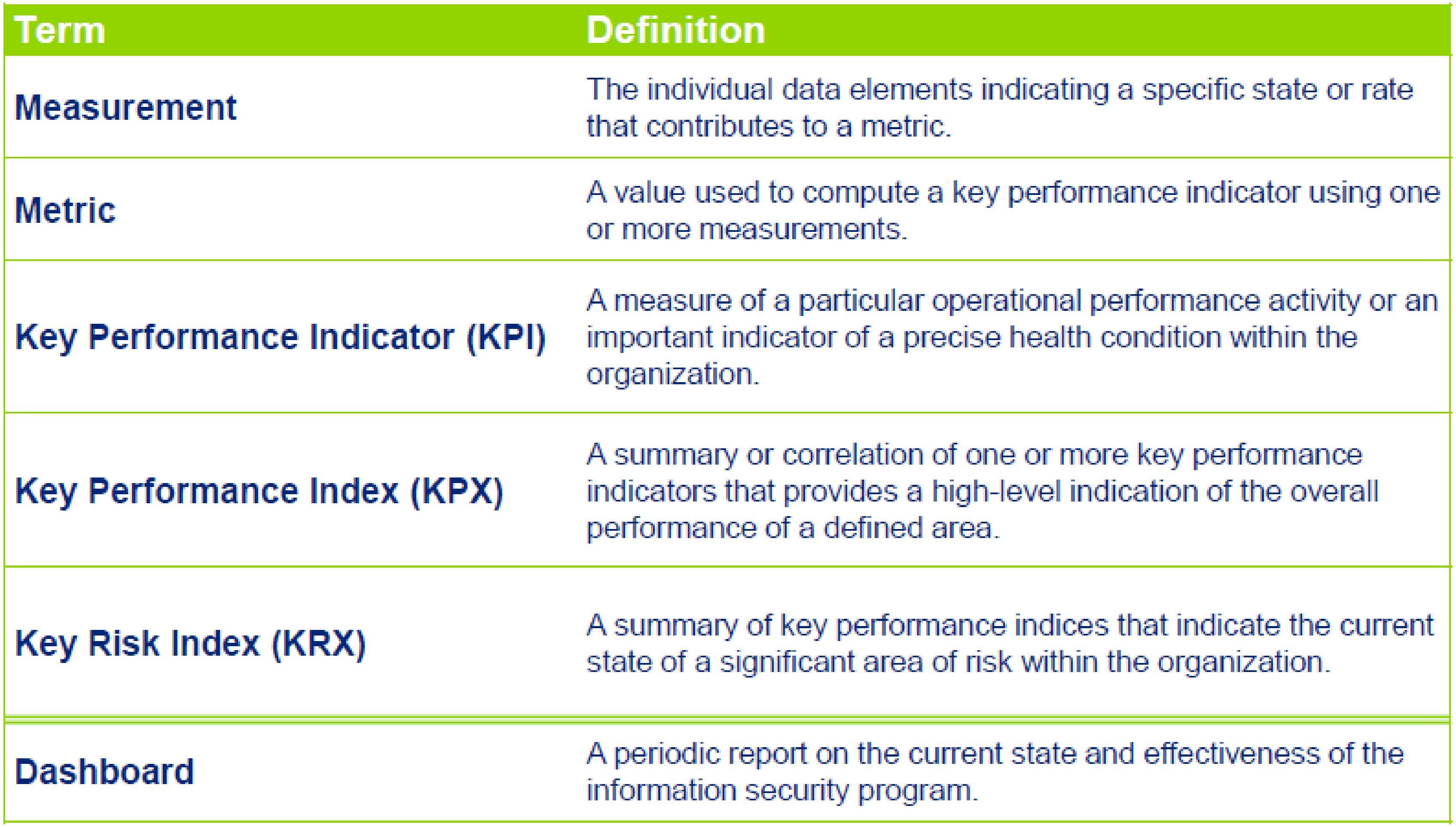
CSOC: Sample Org Chart



CSOC: Operations Metrics

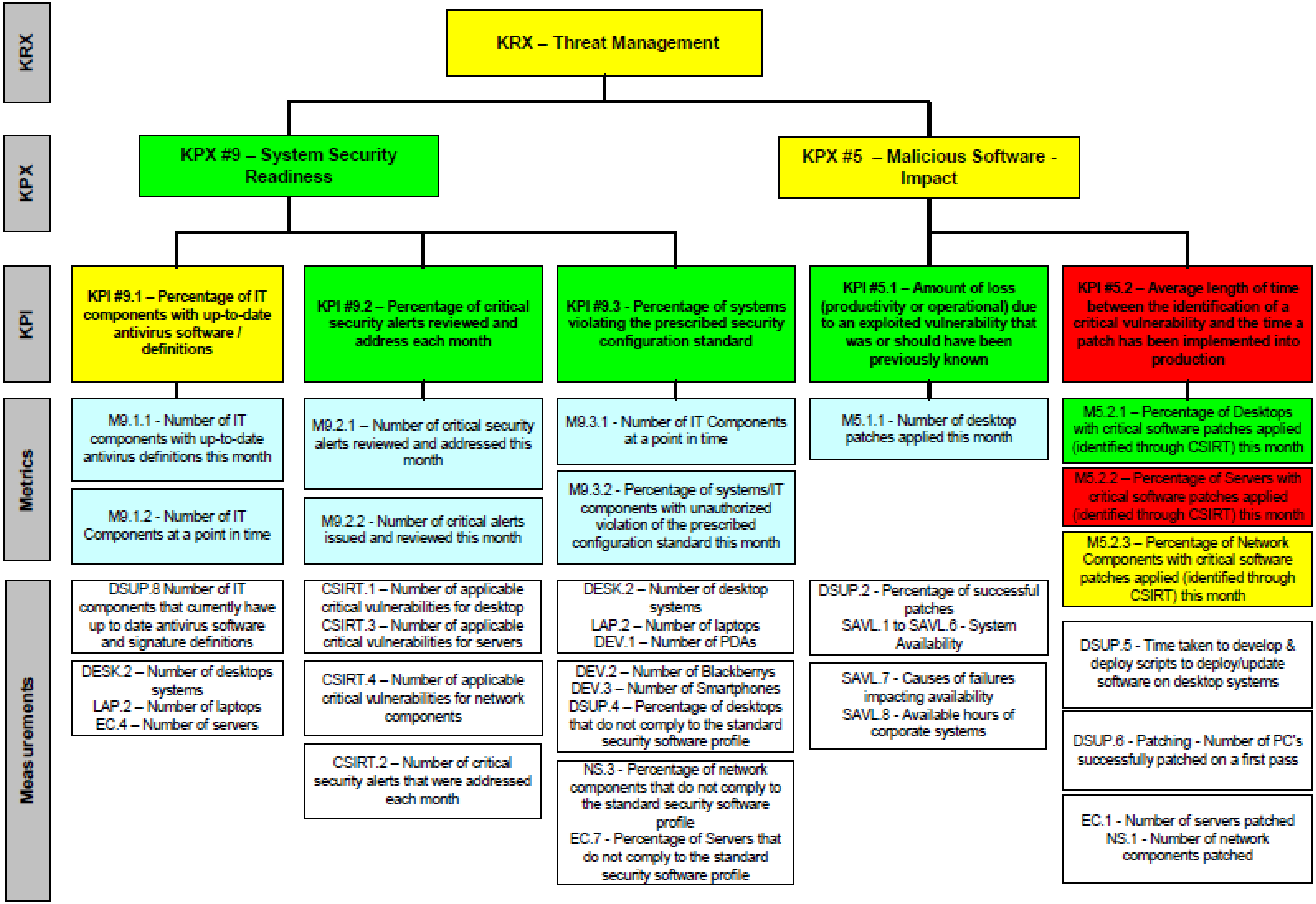
Information Security Measurement and Reporting

The following key definitions are used in an information security measurement and reporting program.



Term	Definition
Measurement	The individual data elements indicating a specific state or rate that contributes to a metric.
Metric	A value used to compute a key performance indicator using one or more measurements.
Key Performance Indicator (KPI)	A measure of a particular operational performance activity or an important indicator of a precise health condition within the organization.
Key Performance Index (KPX)	A summary or correlation of one or more key performance indicators that provides a high-level indication of the overall performance of a defined area.
Key Risk Index (KRX)	A summary of key performance indices that indicate the current state of a significant area of risk within the organization.
Dashboard	A periodic report on the current state and effectiveness of the information security program.

Example Relationship of KRX, KPXs, KPIs and Supporting Metrics



KRX

KPX

KPI

Metrics

Measurements

KRX – Threat Management

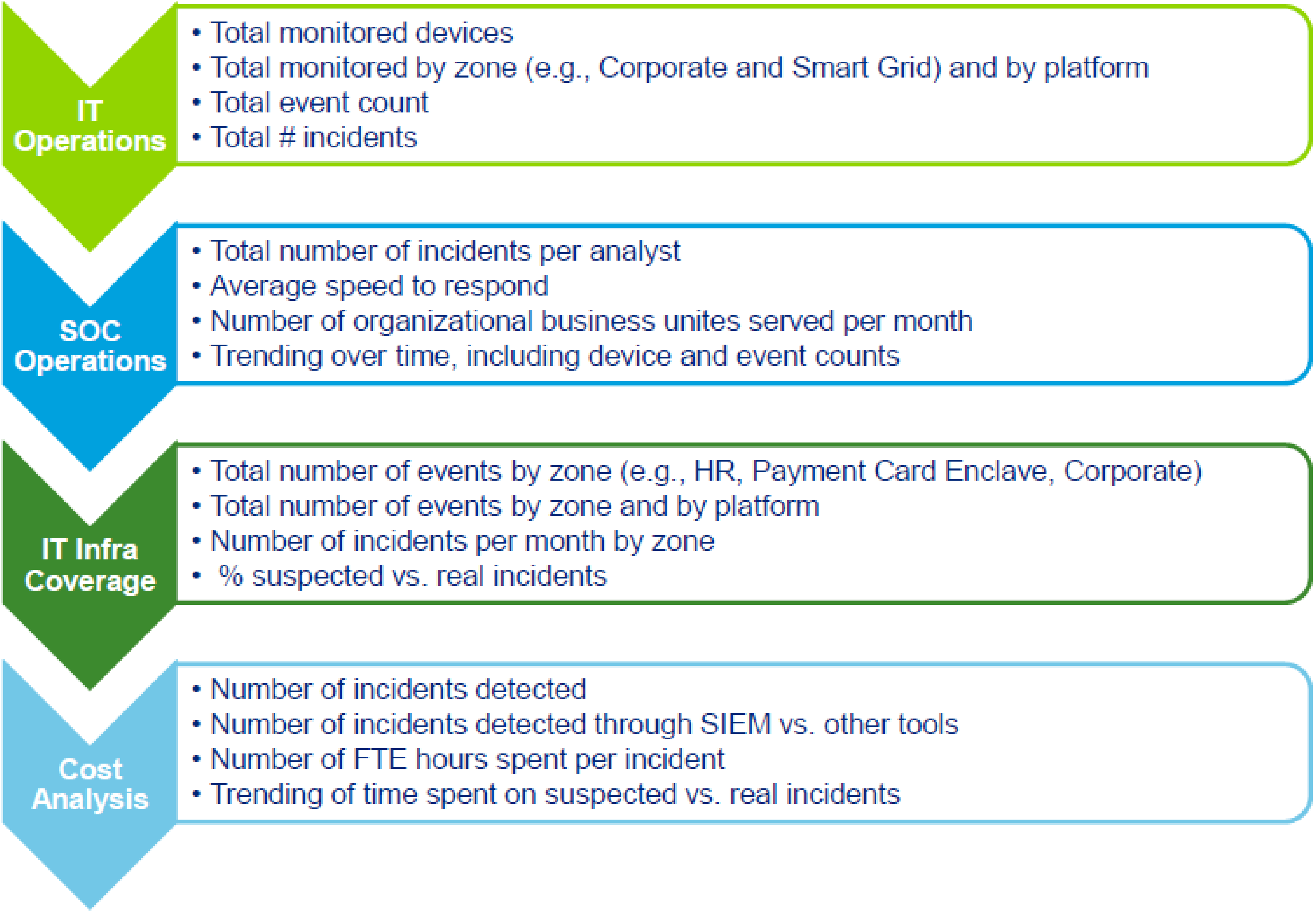
KPX #9 – System Security Readiness

- KPI #9.1 – Percentage of IT components with up-to-date antivirus software / definitions
  - M9.1.1 - Number of IT components with up-to-date antivirus definitions this month
  - M9.1.2 - Number of IT Components at a point in time
  - DSUP.8 Number of IT components that currently have up to date antivirus software and signature definitions
  - DESK.2 – Number of desktops systems
LAP.2 – Number of laptops
EC.4 – Number of servers
- KPI #9.2 – Percentage of critical security alerts reviewed and address each month
  - M9.2.1 – Number of critical security alerts reviewed and addressed this month
  - M9.2.2 - Number of critical alerts issued and reviewed this month
  - CSIRT.1 – Number of applicable critical vulnerabilities for desktop
  - CSIRT.3 – Number of applicable critical vulnerabilities for servers
  - CSIRT.4 – Number of applicable critical vulnerabilities for network components
  - CSIRT.2 – Number of critical security alerts that were addressed each month
- KPI #9.3 - Percentage of systems violating the prescribed security configuration standard
  - M9.3.1 - Number of IT Components at a point in time
  - M9.3.2 - Percentage of systems/IT components with unauthorized violation of the prescribed configuration standard this month
  - DESK.2 – Number of desktop systems
  - LAP.2 – Number of laptops
  - DEV.1 – Number of PDAs
  - DEV.2 – Number of Blackberrys
  - DEV.3 – Number of Smartphones
  - DSUP.4 – Percentage of desktops that do not comply to the standard security software profile
  - NS.3 - Percentage of network components that do not comply to the standard security software profile
  - EC.7 - Percentage of Servers that do not comply to the standard security software profile

KPX #5 – Malicious Software - Impact

- KPI #5.1 – Amount of loss (productivity or operational) due to an exploited vulnerability that was or should have been previously known
  - M5.1.1 - Number of desktop patches applied this month
  - DSUP.2 - Percentage of successful patches
  - SAVL.1 to SAVL.6 - System Availability
  - SAVL.7 - Causes of failures impacting availability
  - SAVL.8 - Available hours of corporate systems
- KPI #5.2 – Average length of time between the identification of a critical vulnerability and the time a patch has been implemented into production
  - M5.2.1 – Percentage of Desktops with critical software patches applied (identified through CSIRT) this month
  - M5.2.2 – Percentage of Servers with critical software patches applied (identified through CSIRT) this month
  - M5.2.3 – Percentage of Network Components with critical software patches applied (identified through CSIRT) this month
  - DSUP.5 - Time taken to develop & deploy scripts to deploy/update software on desktop systems
  - DSUP.6 - Patching - Number of PC's successfully patched on a first pass
  - EC.1 - Number of servers patched
  - NS.1 - Number of network components patched

Example Operational Metrics



IT Operations

- Total monitored devices
- Total monitored by zone (e.g., Corporate and Smart Grid) and by platform
- Total event count
- Total # incidents

SOC Operations

- Total number of incidents per analyst
- Average speed to respond
- Number of organizational business unites served per month
- Trending over time, including device and event counts

IT Infra Coverage

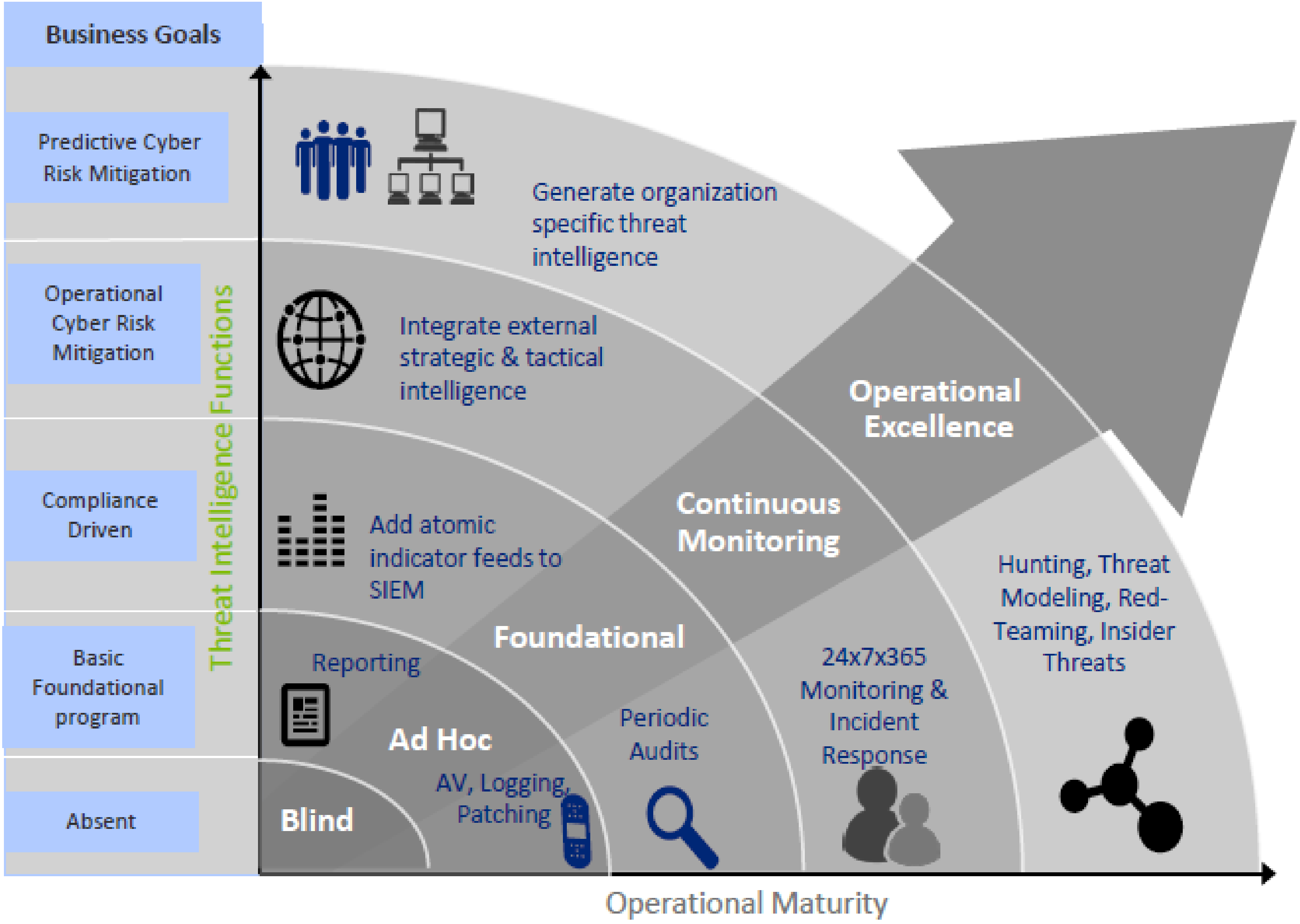
- Total number of events by zone (e.g., HR, Payment Card Enclave, Corporate)
- Total number of events by zone and by platform
- Number of incidents per month by zone
- % suspected vs. real incidents

Cost Analysis

- Number of incidents detected
- Number of incidents detected through SIEM vs. other tools
- Number of FTE hours spent per incident
- Trending of time spent on suspected vs. real incidents

CSOC: Maturity and Conclusion

Maturation Process of a Successful CSOC


Business Goals
Predictive Cyber Risk Mitigation
Operational Cyber Risk Mitigation
Compliance Driven
Basic Foundational program
Absent
Threat Intelligence Functions
Generate organization specific threat intelligence
Integrate external strategic & tactical intelligence
Add atomic indicator feeds to SIEM
Reporting
Operational Excellence
Continuous Monitoring
Foundational
Ad Hoc
Blind
AV, Logging, Patching
Periodic Audits
24x7x365 Monitoring & Incident Response
Hunting, Threat Modeling, Red-Teaming, Insider Threats
Operational Maturity

Business Value of an Advanced Cyber Threat Program

An advanced program that has been designed to protect your business against the threats specific to your organization and industry will allow you to:

Protect value and brand, not "compliance"

- Align your cyber threat program to your business risks
- Protect what matters most from advanced threats
- Realize greater value and risk mitigation on dollars invested
- Demonstrate compliance via superior protection, not checklists and spreadsheets

Disrupt attacks as they happen

- Leverage internal and external intelligence to identify threats in real time
- Leverage automation to speed analysis
- Generate analytics that provide transparency into the *real* state of security
- Disrupt campaigns before they turn into a breach

Clean up quickly and adapt for the next round

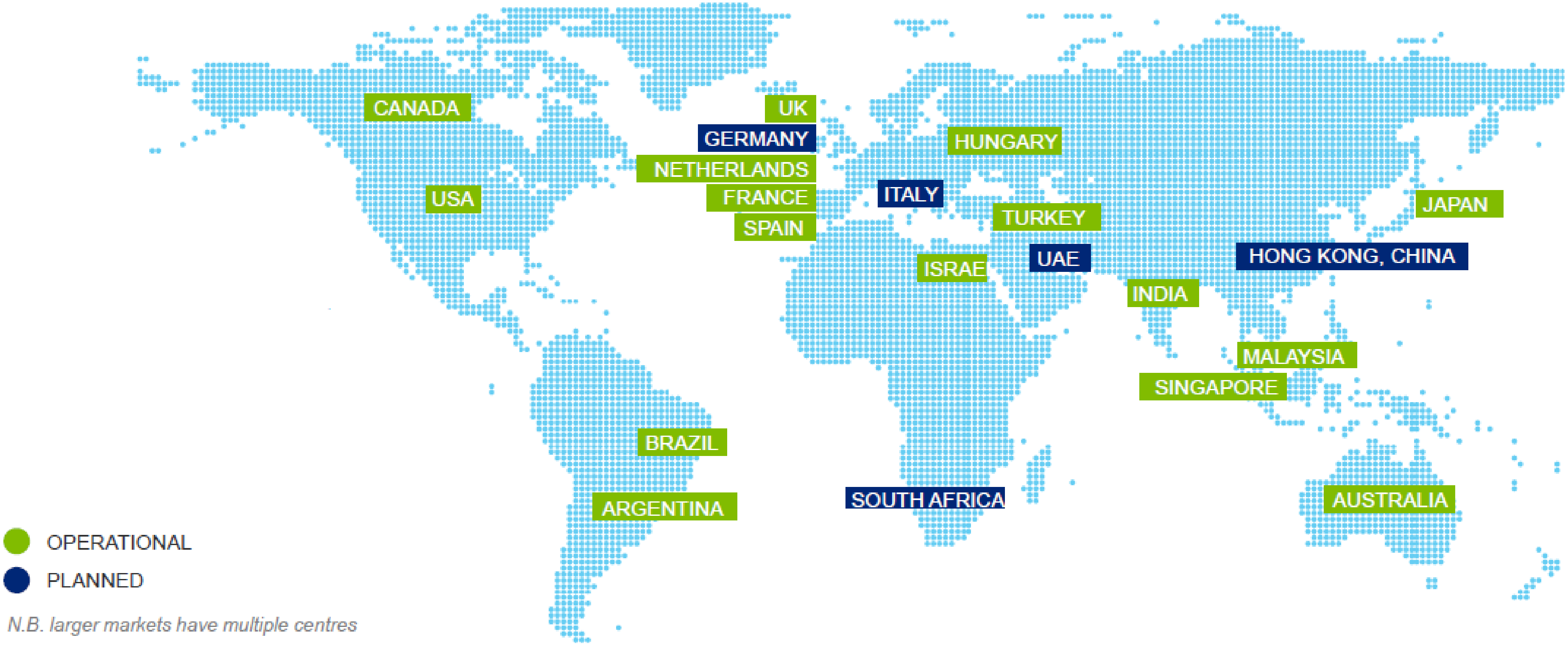
- Reduce timeframe to and cost of recovery
- Reduce disruption to the business
- Improve your security posture, adapt tactics and techniques in an agile fashion
- Prevent similar attacks in the future

Eliminate the threat

- Automate control updates and forensic response
- Reduce investigation timeframes
- Contain the threat more quickly
- Limit exposure and loss

Deloitte.

Deloitte’s global cyber threat intelligence centres offer local context and tailored business understanding



N.B. larger markets have multiple centres

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 225,000 professionals, all committed to becoming the standard of excellence.

About Deloitte Southeast Asia
Deloitte Southeast Asia Ltd – a member firm of Deloitte Touche Tohmatsu Limited comprising Deloitte practices operating in Brunei, Cambodia, Guam, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam – was established to deliver measurable value to the particular demands of increasingly intra-regional and fast growing companies and enterprises.

Comprising over 270 partners and 7,300 professionals in 25 office locations, the subsidiaries and affiliates of Deloitte Southeast Asia Ltd combine their technical expertise and deep industry knowledge to deliver consistent high quality services to companies in the region.

All services are provided through the individual country practices, their subsidiaries and affiliates which are separate and independent legal entities.

About Deloitte Malaysia

In Malaysia, services are provided by Deloitte Enterprise Risk Services Sdn Bhd and its affiliates.