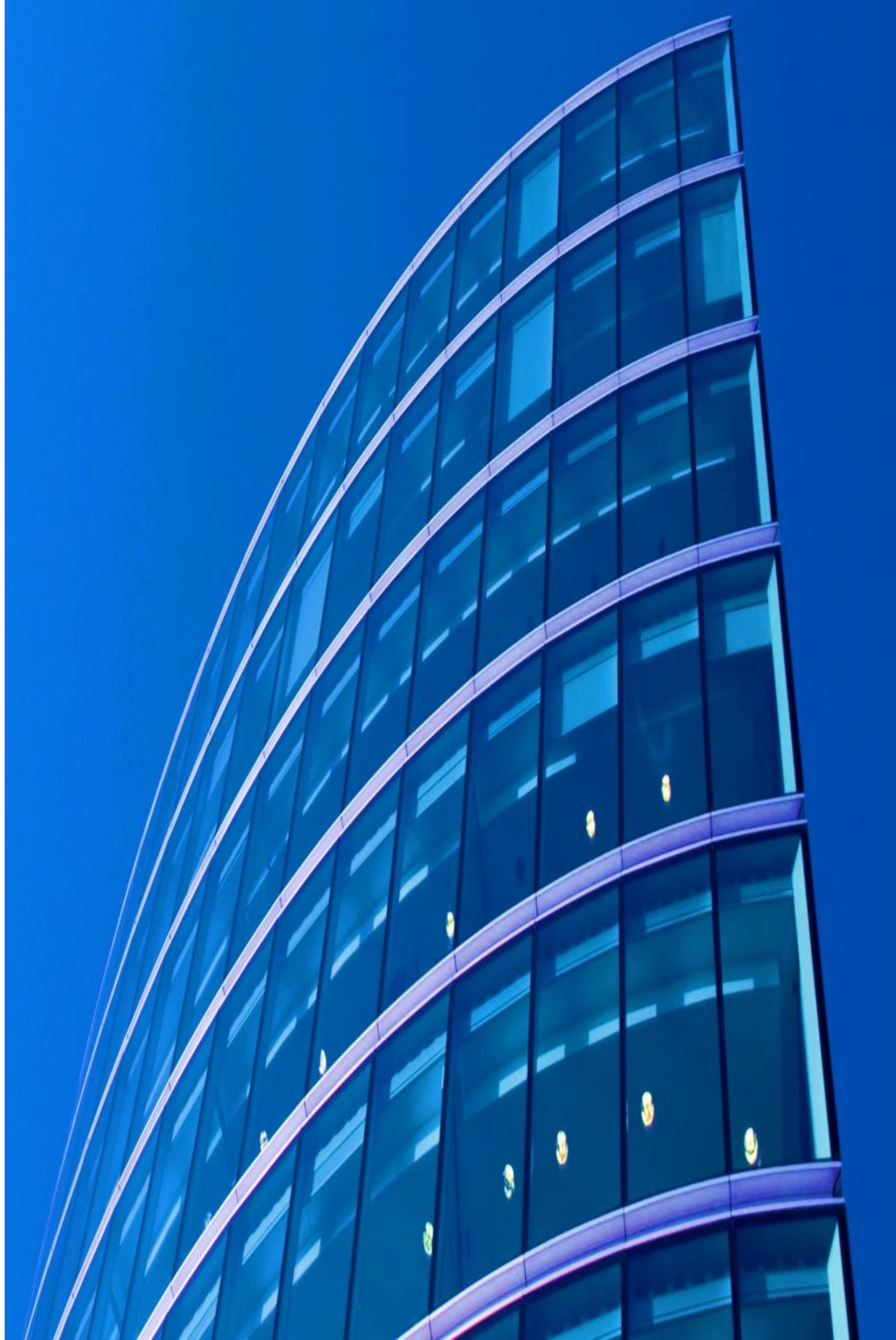
Symantec

Deploying a CSIRT/CERT for Critical Infrastructure.

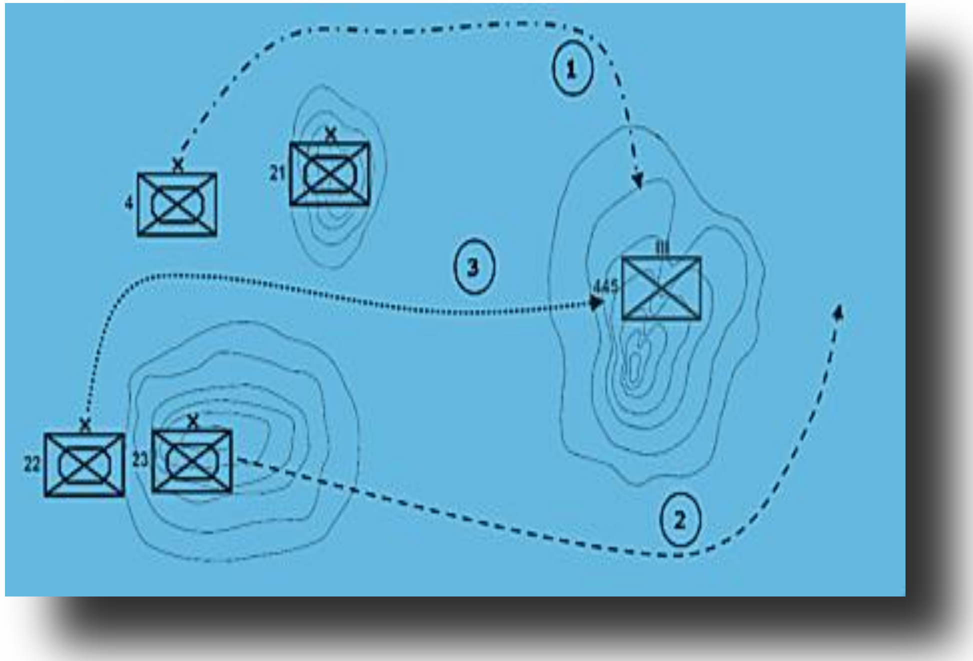
Objectives, policies, responsibilities, and modus operandi.

Giampiero Nanni
Government Affairs EMEA
Symantec Corporation



How is strategy evolving?

- Known unknowns
  - Will be attacked
  - Don’t know when, where, how, who
  - Accept the inevitable
  - Not just about technology
  - Unique features of cyber
- Acquisition of intelligence for situation awareness and early warning
- Focus on capabilities
- Focus on collaboration with trusted parties



Prepare to defend. Situation awareness

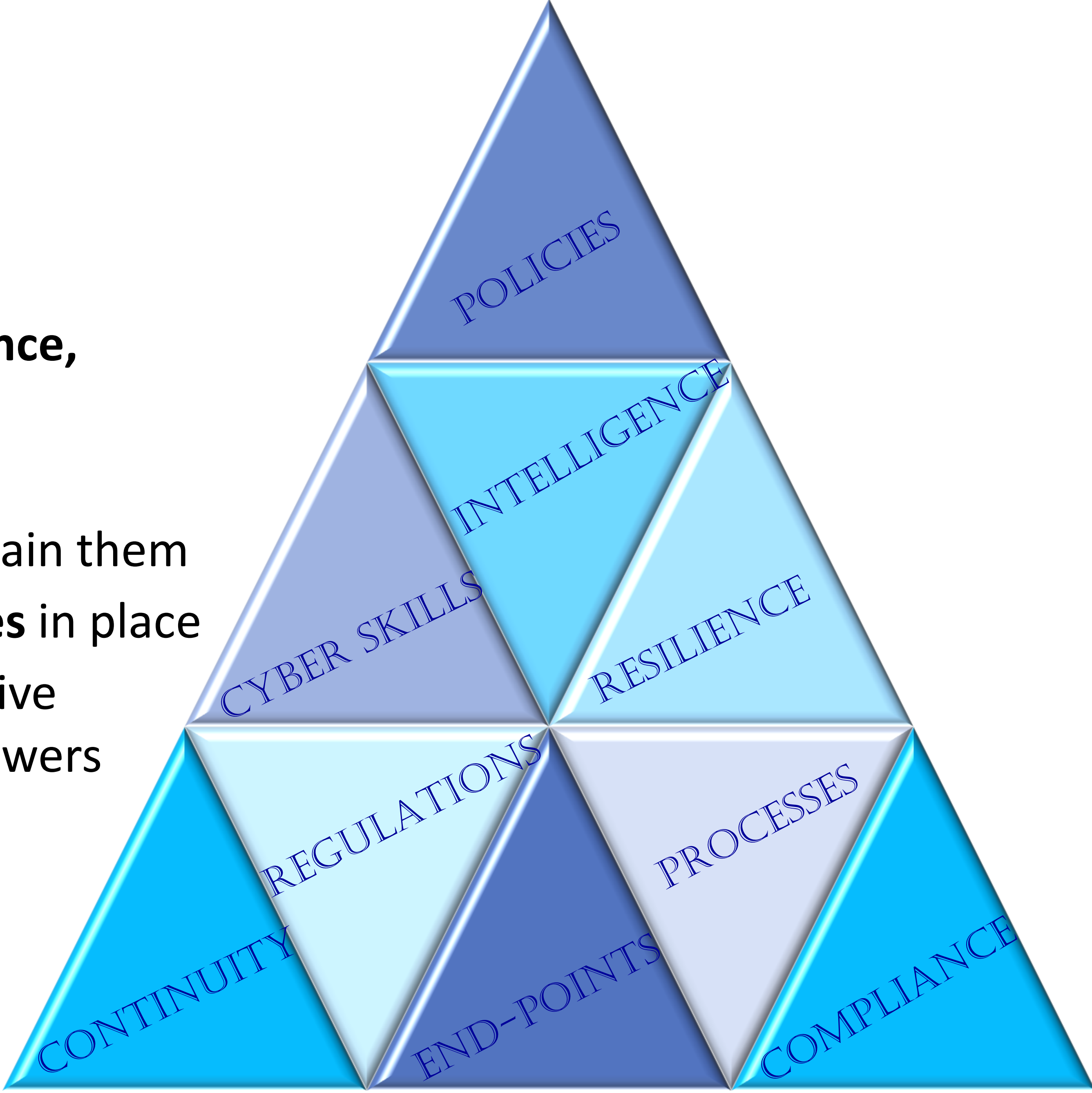
- Identify infrastructures and key government systems that need to be defended
- Develop a level of resilience for those key assets
- Accept the possibility of a successful attack and focus on containment and mitigation
- Cooperate with the private sector
- Build information sharing platforms
- Intelligence-centric approach is key
- Information collection is the default posture but is that enough?
- Actionable data that are categorized, classified and prioritized

Technological/process requirements

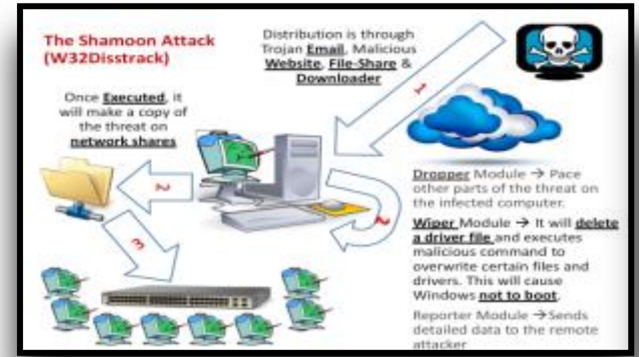
- Build the CERT and…..
- Protect information and identities not just the hardware endpoints
- Address data leakage
- Look at mobile and emerging threats
- Build a comprehensive redundancy and disaster recovery capability
- Risk based approach
- Manage cloud and outsourcing
- You can’t defend everything

Actually defend

- Prioritize
- Defend in depth on multiple points
- Focus on **containment, mitigation, resilience, continuity** of critical systems
- Monitor and protect real-time
- Develop the necessary **cyber skills** and retain them
- Compliance with **laws/regulations/policies** in place
- Have the **process** in place to deliver effective incident response and decision-making powers
- Collect **intelligence** on the attacker
- To the extend possible, attribute



High-profile Critical Information Infrastructure attacks



The Shamoon Attack (W32Disstrack)

Distribution is through Trojan **Email**, Malicious **Website**, **File-Share** & **Downloader**

Once **Executed**, it will make a copy of the threat on **network shares**

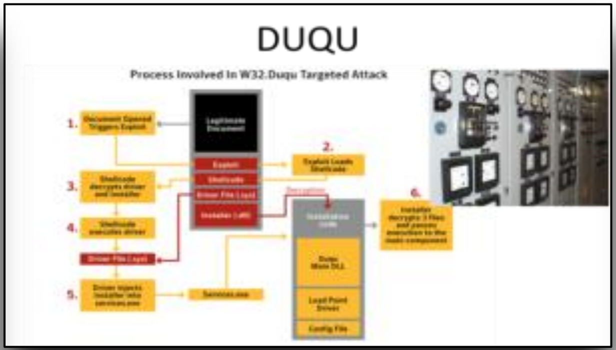
Dropper Module → Pace other parts of the threat on the infected computer.

Wiper Module → It will **delete a driver file** and executes malicious command to overwrite certain files and drivers. This will cause Windows **not to boot**.

Reporter Module → Sends detailed data to the remote attacker

Dragonfly

Attack Investigations Team



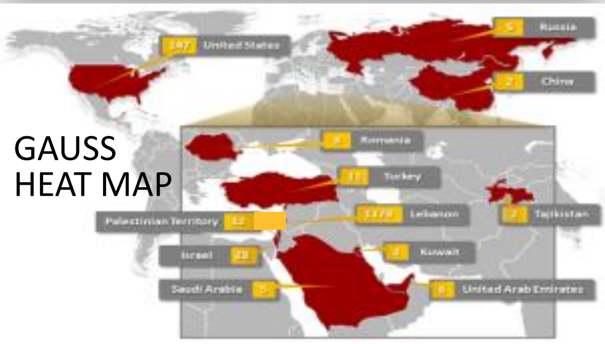
DUQU

Process Involved In W32.Duqu Targeted Attack

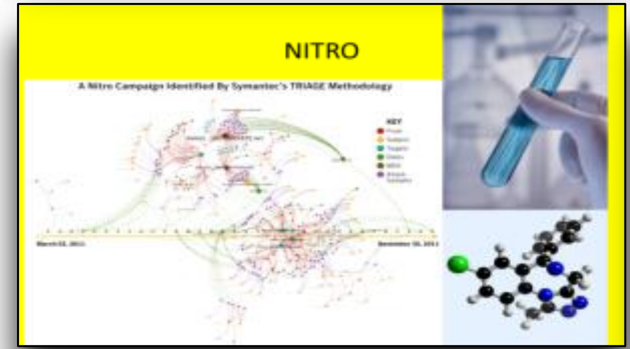
1. Document Opened Triggers Exploit
Legitimate Document
Exploit
Shellcode
Driver File Load
Installer DLL
2. Exploit Loads Shellcode
3. Shellcode decrypts driver and installer
4. Shellcode executes driver
Driver File Load
5. Driver injects installer into services.exe
Services.exe
Decryption
Installation code
Duqu Main DLL
Load Point Driver
Config File
6. Installer decrypts 3 files and passes execution to the main component

© Foto Guido Coolens

FLAMER

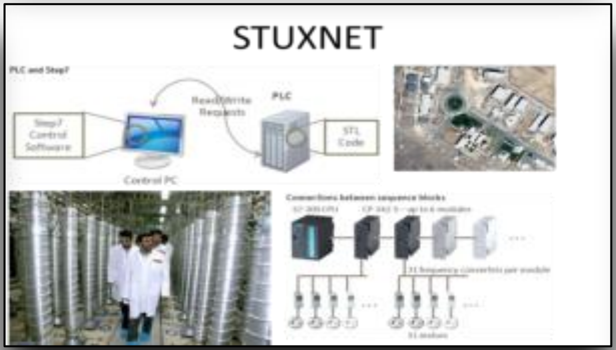


GAUSS HEAT MAP



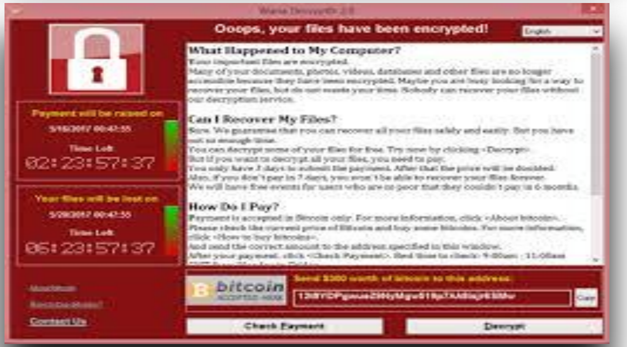
NITRO

A Nitro Campaign Identified By Symantec's TRIAGE Methodology



STUXNET

PLC and Step7
Step7 Control Software
Read/Write Requests
PLC
STL Code
Control PC
Connections between sequence blocks
S7-300 CPU
CP 342-5 – up to 6 modules
31 frequency converters per module



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

NIS Directive - Key mandates to Member States

- Ensure a high level of NIS in Country
- National Cybersecurity Strategies
- Crate/equip Computer Security Incident Response Teams (**CSIRTs**)
- Designate one or more national competent authority
- Define, implement, enforce security & **notification** requirements
- Implement organisational and technological measures
- Promote a culture of **risk management**
- Designate a national single point of contact responsible for coordination
- Report and publish serious incidents
- Need to **exchange** information
- Emphasis on cross-border implications

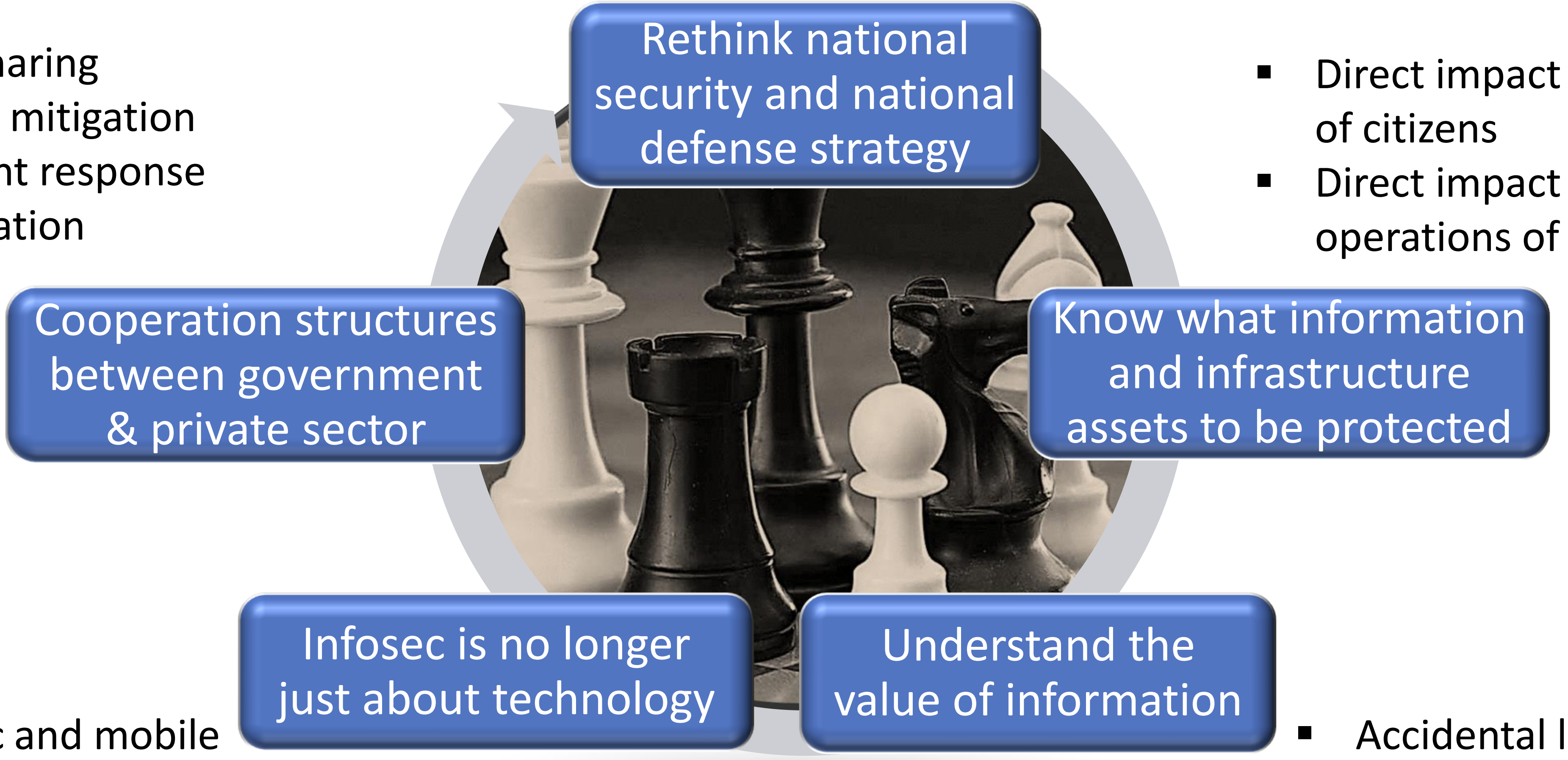
Operators of Critical infrastructure

- Need to develop a risk management approach
- Are subject to audit and supervision by national authorities
- Need to report security incidents
- Need to exchange information

Symantec.

Key elements of cyber strategies

- Info-sharing
- Threat mitigation
- Incident response
- Notification



Rethink national security and national defense strategy

Know what information and infrastructure assets to be protected

Understand the value of information

Infosec is no longer just about technology

Cooperation structures between government & private sector

- Direct impact on the lives of citizens
- Direct impact on the operations of government

- Dynamic and mobile
- Intelligence and risk-driven
- Process and people-driven
- Educate the users to cyber discipline

- Accidental loss and Open Source Intelligence
- Resilience and service continuity

What is a CERT/CSIRT

Computer Emergency Response Team/ Computer Security Incident Response Team

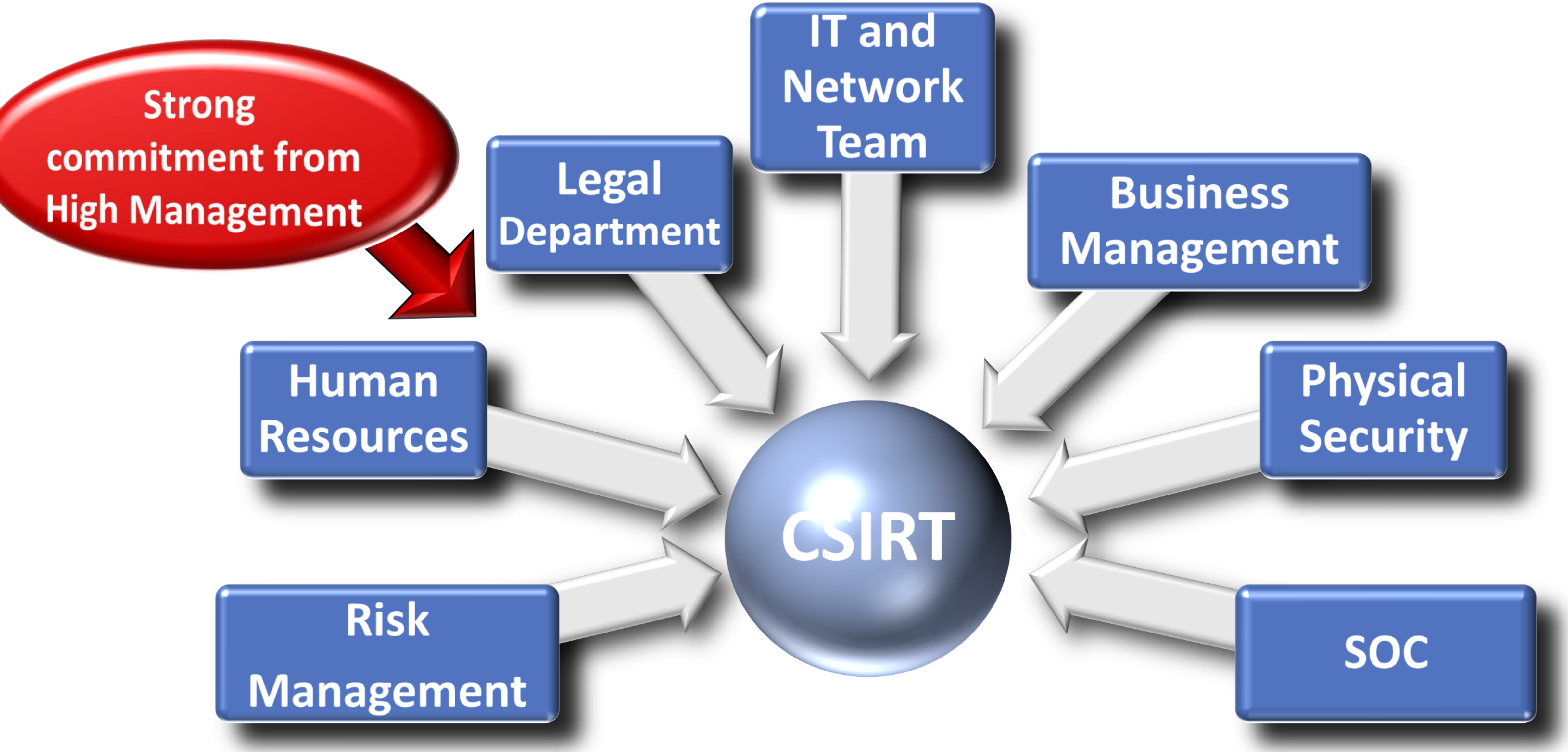
- A CERT/CSIRT is:
  - ✓ an organization or team
  - ✓ that provides services and support
  - ✓ to a defined constituency
  - ✓ for preventing
  - ✓ handling and
  - ✓ responding to
  - ✓ computer security incidents.

CERT/CSIRT – Objectives of the implementations

- Enhance information security awareness
- Build (national) expertise in information security, incident management and computer forensics
- Provide a central trusted point of contact for
  - Cyber security incident reporting
  - For general contact for security issues
- Establish a (national) center to disseminate information about threats, vulnerabilities, and cyber security incidents
- Coordinate with other domestic and international CERT/CSIRTs and related organizations
- Share information and lesson learned with other CERT/CSIRT/response teams and appropriate organizations and sites.

- Protect mission-critical data and assets
- Prepare for and respond to security threats
- Help provide continuity and efficient recovery
- Fortify business infrastructure
- Monitor, Analyze, Correlate & Escalate Intrusion Events
- Develop Appropriate Responses; Protect, Detect, Respond
- Conduct Incident Management and Forensic Investigation
- Assist in Crisis Operations

CERT/CSIRT – Who Need to be involved



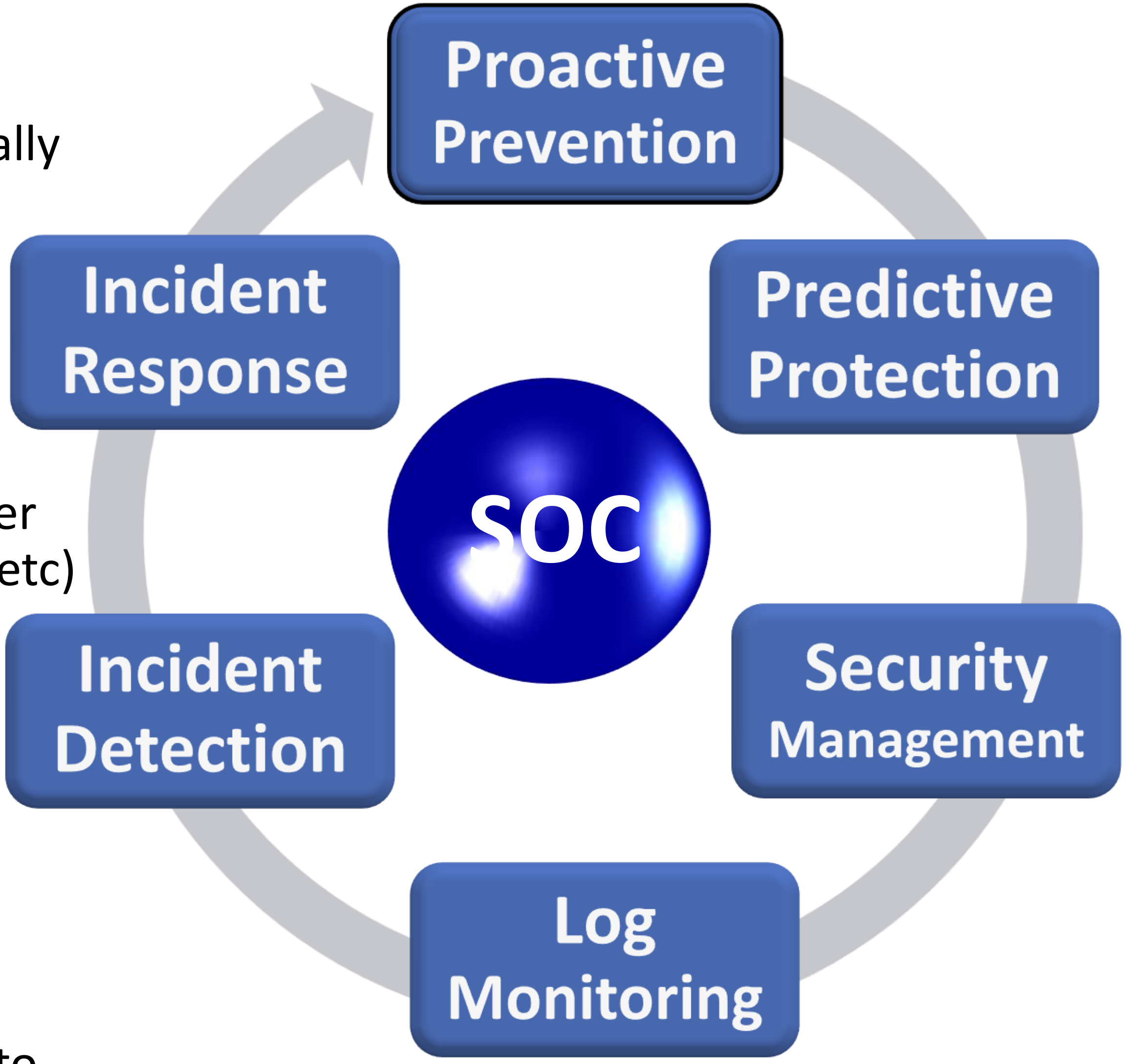
Copyright © 2018 Symantec

What is a SOC

- A **Security Operations Center** ("**SOC**") is a facility where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are **monitored, assessed, and defended.**
- A SOC is related with the **people, processes and technologies** involved in providing situational awareness through the **detection, containment, and remediation** of IT threats.
- A SOC **manages incidents** for the enterprise, ensuring they are properly identified, analyzed, communicated, actioned/defended, investigated and reported.
- The SOC also **monitors applications** to identify a possible cyber-attack or intrusion (event) and determine if it is a real, malicious threat (incident), and if it could have a business impact.
- **Maturity level**: Outsourcing → Co-Sourcing → Insourcing

Challenges of any SOC

- **Threat Evolution**
  - ➢ Complexity of managing a SOC has increased exponentially
  - ➢ Inside and outside threats
  - ➢ Requires having global visibility and superior knowledge detect
- **Complex Monitoring**
  - ➢ Monitoring operations are no longer just about perimeter protection (Firewalls, IPS, IDS, Proxy, Applications, IAM, etc)
  - ➢ Onslaught of security data from disparate systems, platforms and applications
  - ➢ Very huge amount of daily logs that must be monitored, analyzed and correlated.
- **Staffing**
  - ➢ Quality staff is hard to find, retain.. Don't Settle
  - ➢ 24/7 Shifts difficult to achieve - Good people don't like to work on Shifts for long period
  - ➢ Hard to develop a career plan for the resources



Symantec.

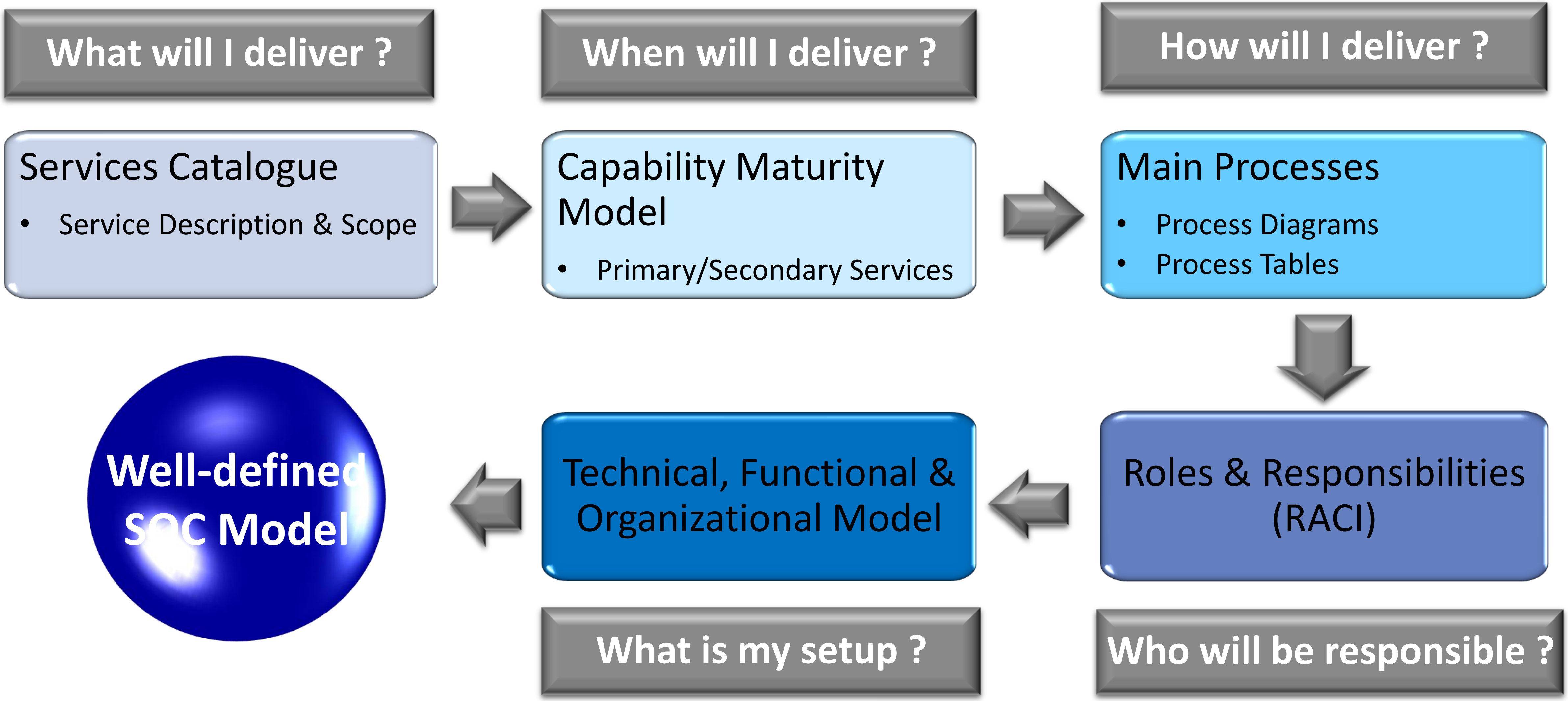
SOC Focus Area

Not every SOC has the same role. There are three different focus areas in which a SOC may be active, however combined:

- **Monitoring**: focusing on events and the response with log monitoring, SIEM administration, and incident response
- **Operational**: focusing on the operational security administration such as identity & access management, key management, firewall administration, etc.
- **Control**: focusing on the state of the security with compliancy testing, penetration testing, vulnerability testing, etc.

Bulding a SOC

The journey toward a well-defined SOC



What will I deliver ?

Services Catalogue

- Service Description & Scope

When will I deliver ?

Capability Maturity Model

- Primary/Secondary Services

How will I deliver ?

Main Processes

- Process Diagrams
- Process Tables

Roles & Responsibilities (RACI)

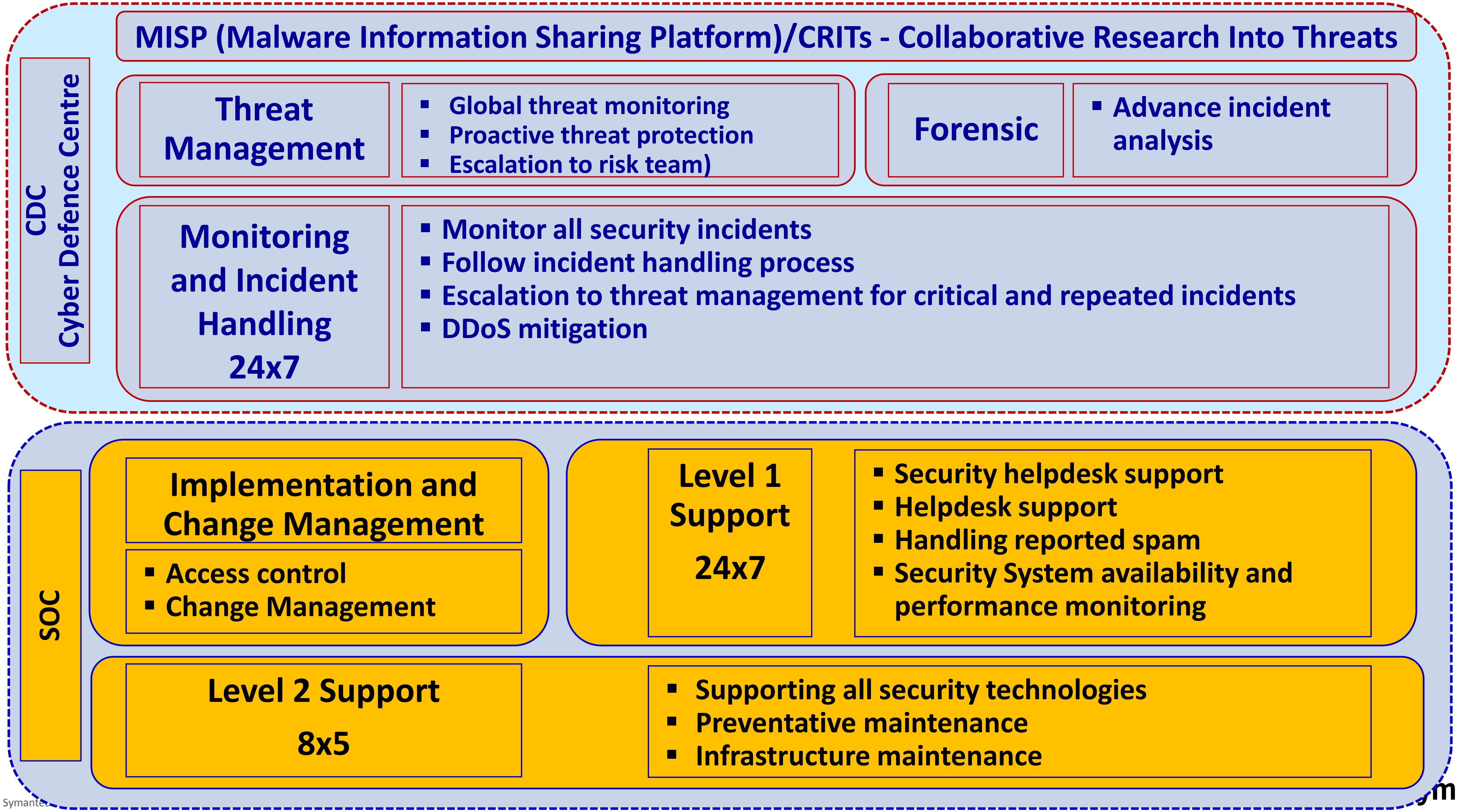
Who will be responsible ?

Technical, Functional & Organizational Model

What is my setup ?

Well-defined SOC Model

C-SOC Functions (Cyber Defence Centre + SOC)



CDC
Cyber Defence Centre

MISP (Malware Information Sharing Platform)/CRITs - Collaborative Research Into Threats

Threat Management

- Global threat monitoring
- Proactive threat protection
- Escalation to risk team)

Forensic

- Advance incident analysis

Monitoring and Incident Handling 24x7

- Monitor all security incidents
- Follow incident handling process
- Escalation to threat management for critical and repeated incidents
- DDoS mitigation

SOC

Implementation and Change Management

- Access control
- Change Management

Level 1 Support 24x7

- Security helpdesk support
- Helpdesk support
- Handling reported spam
- Security System availability and performance monitoring

Level 2 Support 8x5

- Supporting all security technologies
- Preventative maintenance
- Infrastructure maintenance

Cyber Defence Center Service Catalog

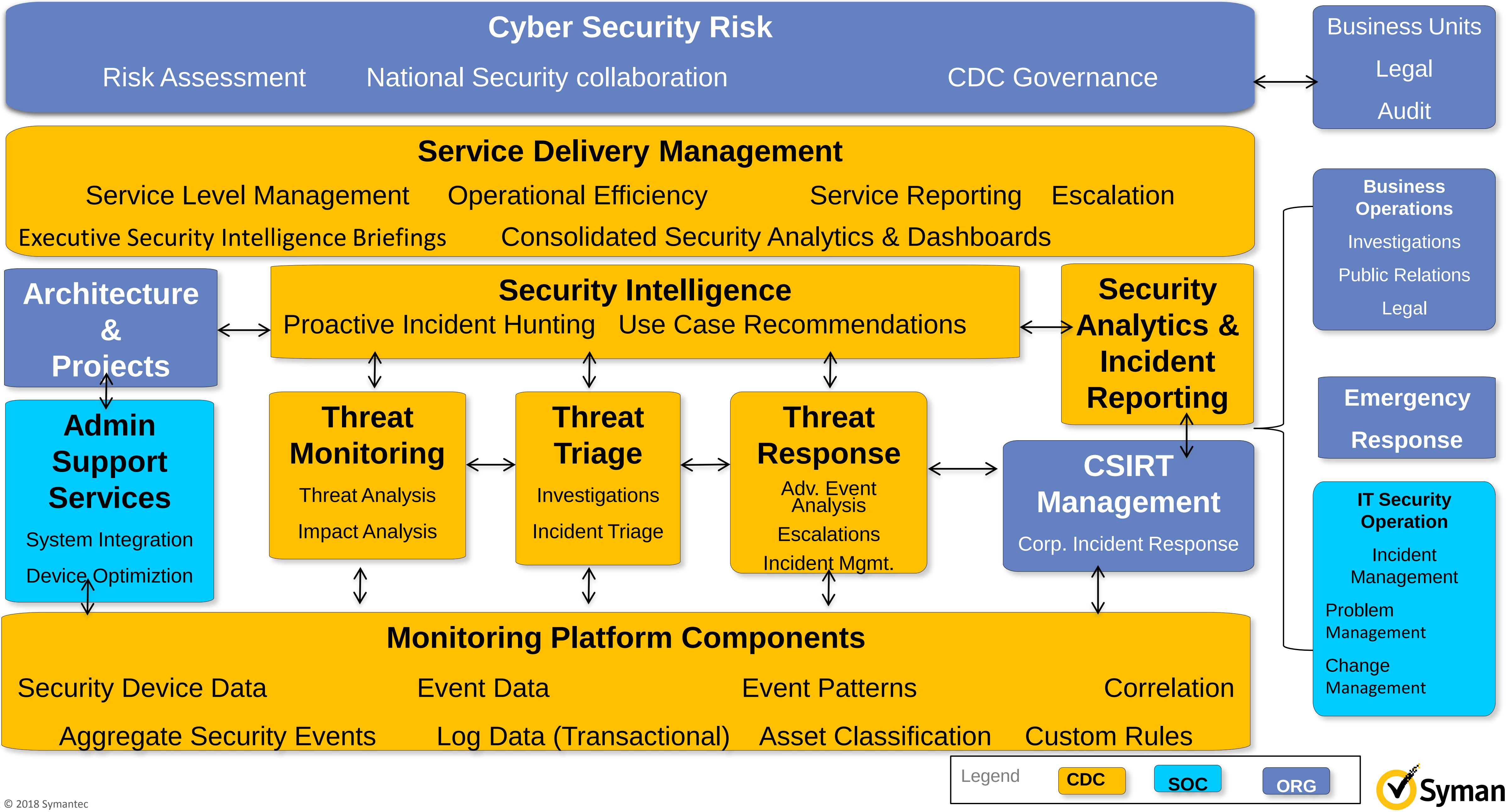
“Define your security services menu”

	Proactive Services	Reactive Services	Security Management
Monitoring	▪ Real Time Device Monitor ▪ Vulnerability Assessment ▪ Penetration Test ▪ Security & Compliance Audit ▪ Cyber Security Intelligence ▪ Performance and Fault Monitoring ▪ Policy Compliance ▪ Hunting / Honeypotting	▪ Incident Identification ▪ Incident Classification	▪ Business Impact Analysis ▪ Risk Assessment ▪ Threat Assessment ▪ Technology Watch
Advisoring	▪ Alerting & Warning ▪ Trending ▪ Technical Reporting ▪ Security Hotline	▪ Incident Notification	▪ Executive Reporting ▪ Security Consulting ▪ Awareness ▪ Countermeasures Selection
Managing	▪ Secure Device Configuration ▪ Secure Device Maintenance ▪ Policy Management ▪ Policy Enforcement ▪ Patch Management ▪ Events Data Retention ▪ Endpoint Management ▪ Hardening	▪ Incident Response ▪ Incident Recovery ▪ Forensics Evidence Collection ▪ Malware Analysis ▪ Forensics Analysis ▪ Tracking & Tracing ▪ Post Mortem Analysis	▪ Business Continuity ▪ Asset Inventory ▪ Policy Planning ▪ Risk Management ▪ Education/Training ▪ Certification

SOC Services - Capability Maturity Model

	Initial >>	Aware >>	Defined >>	Managed >>	Optimised
Security Management		▪ Security Awareness ▪ Executive Security Reporting	▪ Business Impact Analysis ▪ Risk Assessment ▪ Asset Inventory	▪ Technology Watch ▪ Security Consulting ▪ Countermeasures selection ▪ Risk Management	▪ Business Continuity ▪ Policy Planning ▪ Education ▪ Training ▪ Certification
Incident Handling	▪ Incident Identification ▪ Incident Notification ▪ Incident Response	▪ Incident Classification ▪ Tracking & Tracing	▪ Incident Recovery	▪ Forensics Evidence Collection ▪ Post-mortem Analysis	▪ Forensics Analysis
Proactive Security	▪ RT Device Monitoring ▪ Alerting & Warning ▪ Policy Management ▪ Policy Enforcement	▪ Vulnerability Assessment ▪ Penetration Test ▪ Security Intelligence ▪ Technical Reporting ▪ Event Data Retention	▪ Security Device Config. ▪ Security Device Maintenance	▪ Fault Monitoring ▪ Patch Management ▪ End Point Security ▪ Hardening	▪ Security Audit ▪ Performance Monitoring ▪ Policy Compliance ▪ Security Hotline

Cyber Defence Functional Model



Cyber Security Risk

Risk Assessment
National Security collaboration
CDC Governance

Business Units
Legal
Audit

Service Delivery Management

Service Level Management
Operational Efficiency
Service Reporting
Escalation
Executive Security Intelligence Briefings
Consolidated Security Analytics & Dashboards

Architecture & Projects

Security Intelligence

Proactive Incident Hunting
Use Case Recommendations

Security Analytics & Incident Reporting

Business Operations

Investigations
Public Relations
Legal

Admin Support Services

System Integration
Device Optimiztion

Threat Monitoring

Threat Analysis
Impact Analysis

Threat Triage

Investigations
Incident Triage

Threat Response

Adv. Event Analysis
Escalations
Incident Mgmt.

CSIRT Management

Corp. Incident Response

Emergency Response

IT Security Operation

Incident Management
Problem Management
Change Management

Monitoring Platform Components

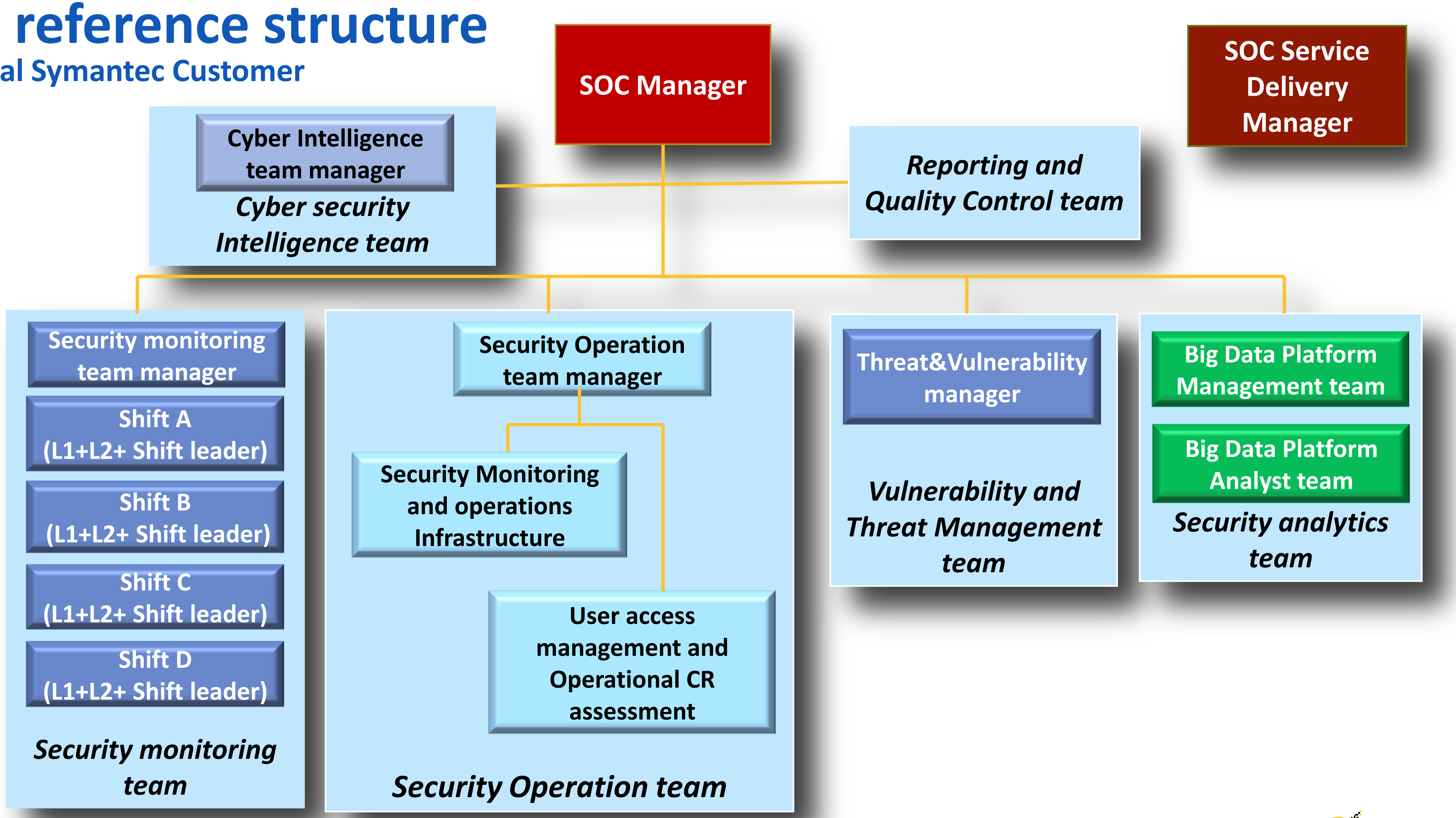
Security Device Data
Event Data
Event Patterns
Correlation
Aggregate Security Events
Log Data (Transactional)
Asset Classification
Custom Rules

Legend
CDC
SOC
ORG

Symantec

A reference structure

Real Symantec Customer

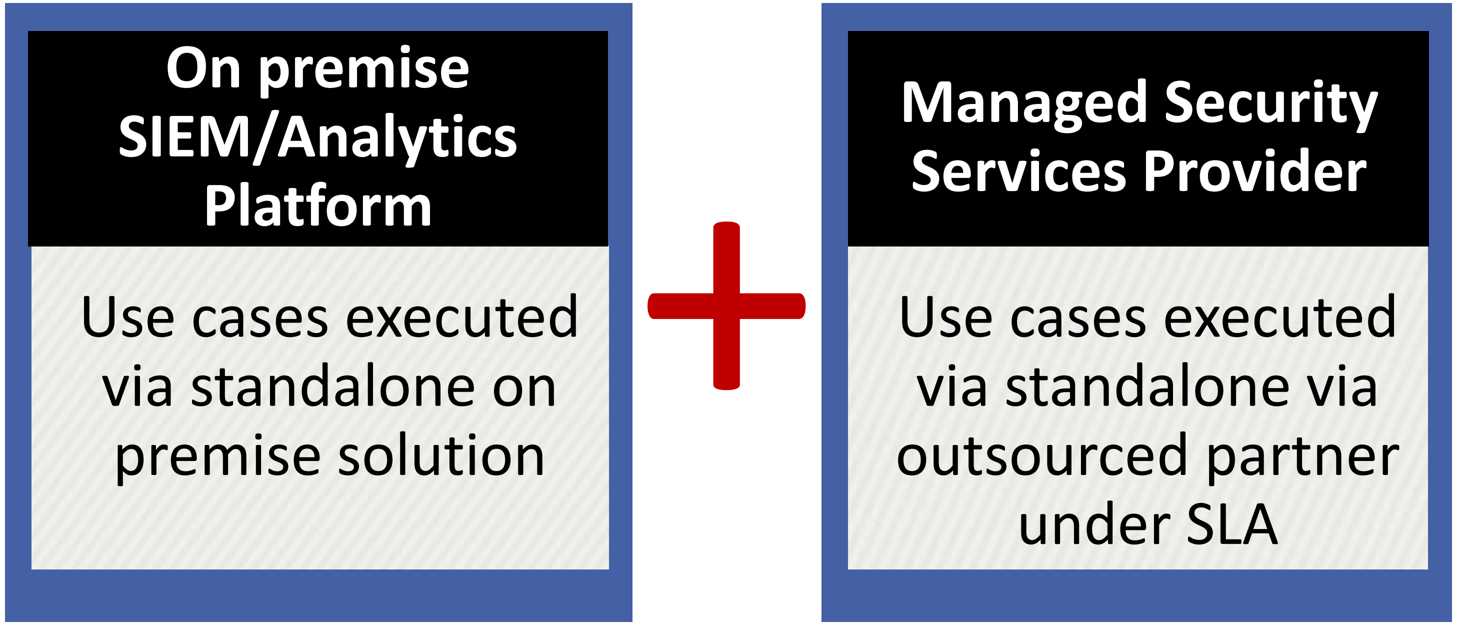

SOC Manager
SOC Service Delivery Manager
Cyber Intelligence team manager
Cyber security Intelligence team
Reporting and Quality Control team
Security monitoring team manager
Shift A (L1+L2+ Shift leader)
Shift B (L1+L2+ Shift leader)
Shift C (L1+L2+ Shift leader)
Shift D (L1+L2+ Shift leader)
Security 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

What are we seeing?

“Best Practice being re-defined through blended approaches”

“The optimum balance of cost, risk, time & performance”

- Managed Service Providers:
  - Real time threat alerting & remediation guidance
  - Provide global threat intelligence & industry comparison
  - Extend customer’s team (& address industry skill shortage) with 24x7x365 coverage by skilled threat analysts
- On premise solutions:
  - Provide historical investigative analysis & compliance capability
  - Onsite team remains embedded in the business with flexible ad hoc query capability
- Together, supports a flexible, employee engaged and agile business solution



On premise SIEM/Analytics Platform

Use cases executed via standalone on premise solution

+

Managed Security Services Provider

Use cases executed via standalone via outsourced partner under SLA

ευχαριστώ

Giampiero Nanni
Government Affairs EMEA

giampiero_nanni@symantec.com

+44 780 8248100

@Giampieronanni

Ilias Chantzos
Senior Director
Government Affairs EMEA-APJ

Ilias_Chantzos@symantec.com