# Building Blocks of a Cyber Resilience Program

Monika Josi

monika.josi@safis.ch

CyAN Cybersecurity Advisors Network

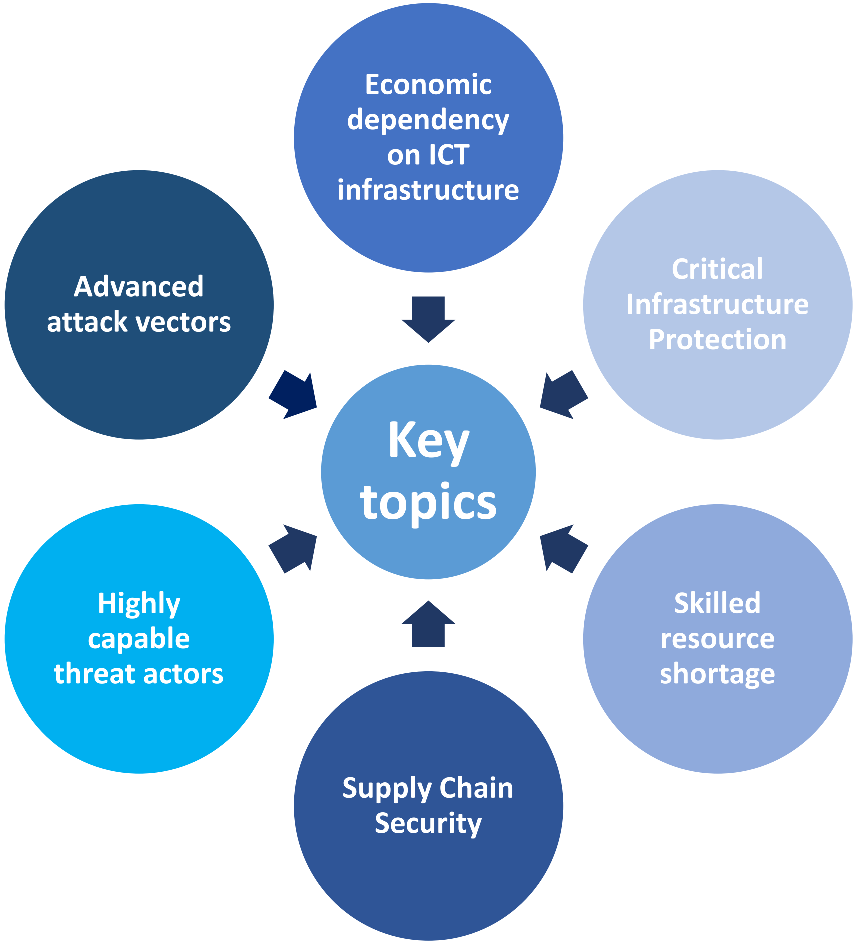
Safis Consulting

# About me

- Chief Security Advisor for Microsoft Europe, Middle East and Africa providing support to Governments and CIIP until 2014
- Since May 2014, Founder and Principal Consultant of Safis Consulting
    - Cyber security consulting for public and private sector
    - Vice President for International Development for CyAN, an association with the ambition to strengthen cybersecurity and fighting against cybercrime through a multi-disciplinary approach
    - Lead expert on EU-funded project for an Identification and Formulation Study for a Project on Cybersecurity Capacity Building outside the EU

# The world we live in

# The challenge


Economic dependency on ICT infrastructure
Critical Infrastructure Protection
Skilled resource shortage
Supply Chain Security
Highly capable threat actors
Advanced attack vectors
Key topics

- New supply chain dependencies transcending boundaries

- Advances in technology, i.e. tablets, smart phones, cloud services and social communication, have fundamentally changed the way people work and increase the demand on ICT reliance

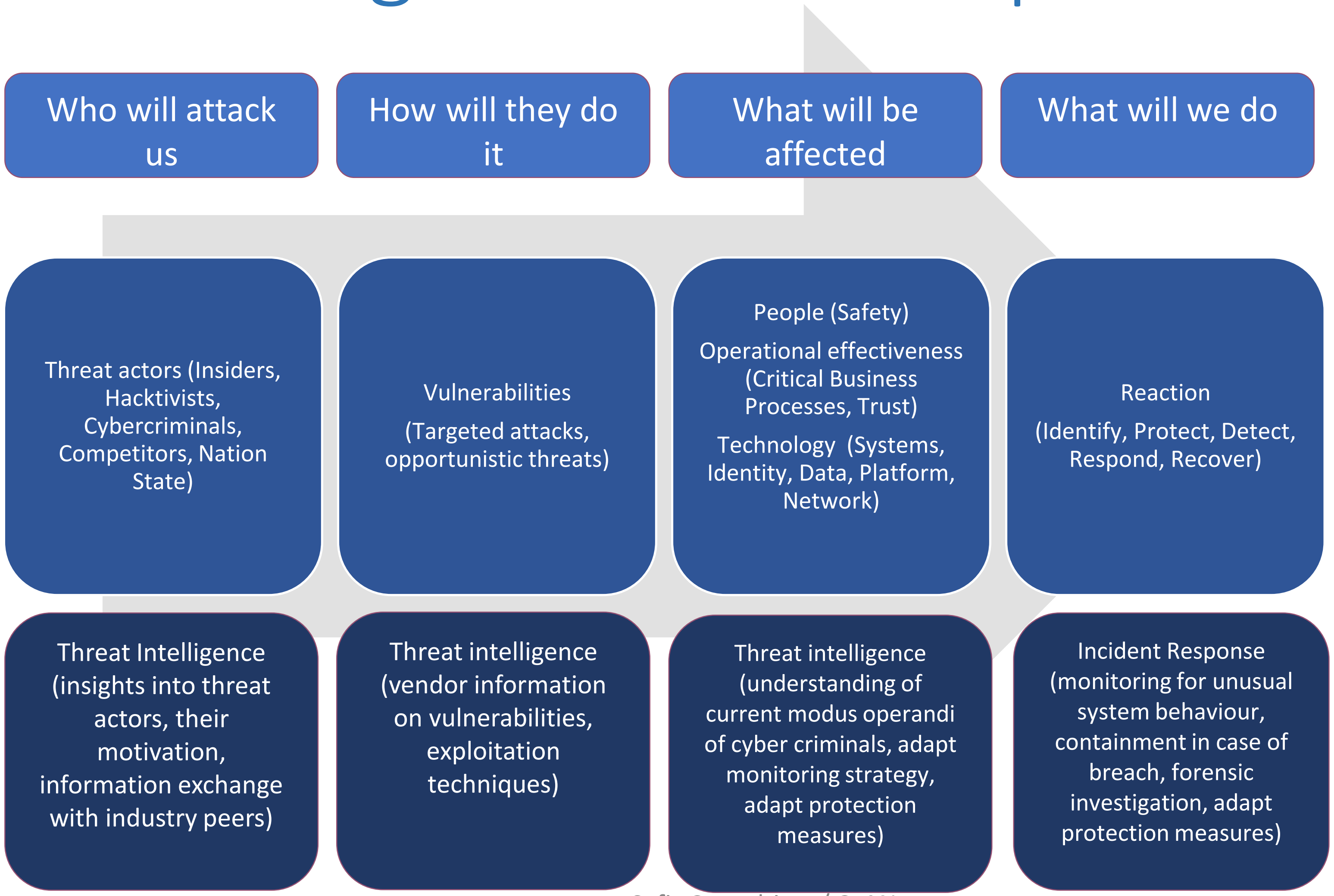
- The cyber threat landscape has changed substantially in the past few years bringing significant advances in attack methods and making them readily available

- This has rendered traditional (perimeter) security measures insufficient in mitigating security risks

# A map doesn’t help if you don’t know where you are

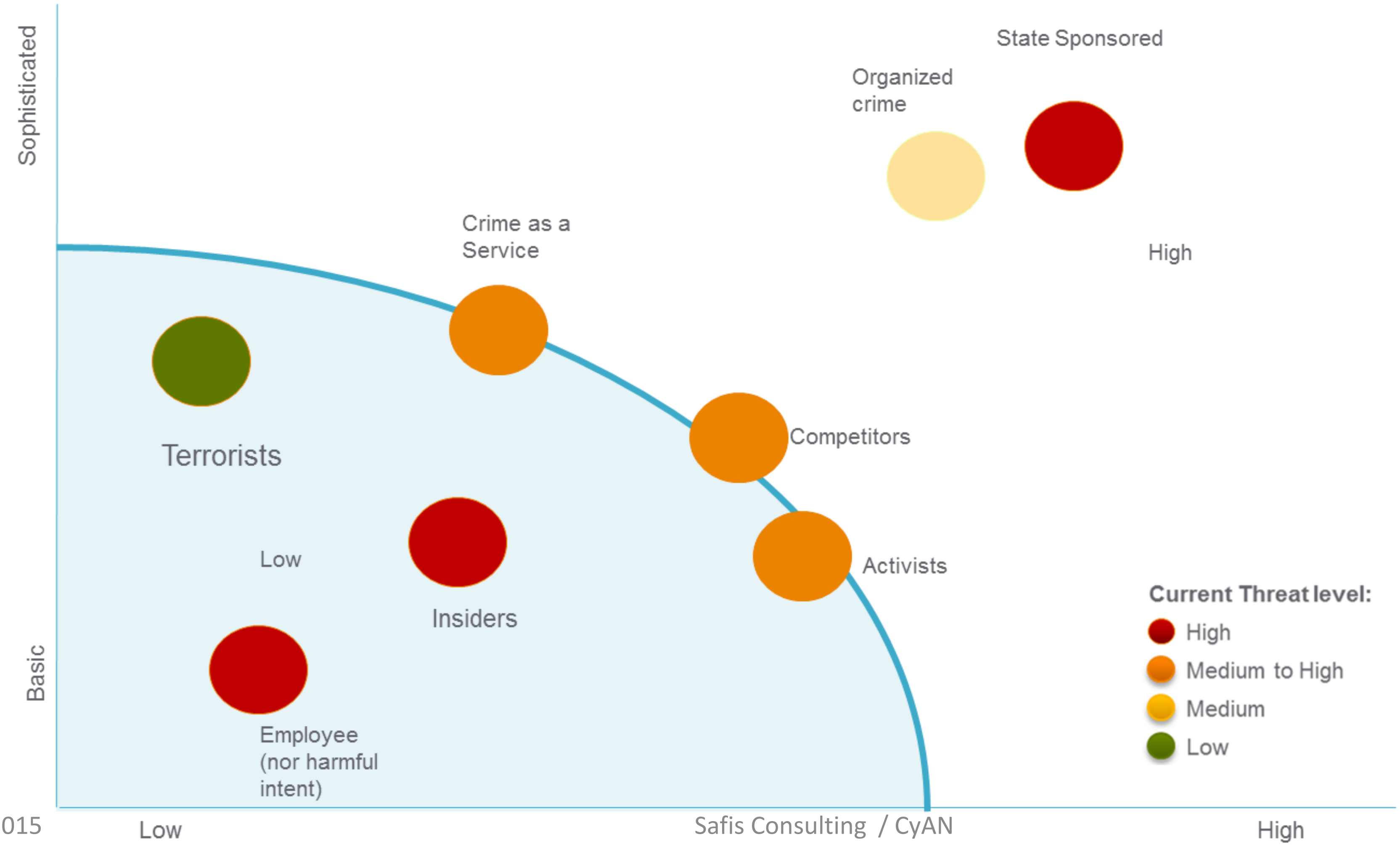
| The steps | Supporting information |
|---|---|
| Assessing the current landscape regarding threat actors, method used, target and response | • Intelligence feeds<br>• Twitter feeds<br>• Hacktivist webpages<br>• Information from peers<br>• Vendor information (e.g. Security Bulletins) |
| Assessing the needs and capabilities | • Maturity models<br>  • Often bespoke in private sector based on consultant used<br>  • For governments: Global Cyber Security Capacity Centre (University of Oxford, CMM model) |
| Developing the cybersecurity strategy | Private Sector: often bespoke based on consultants, ISO standards<br>Governments: ENISA offers a wide range of studies regarding national cyber security strategies and assessments |

# Setting the scene – getting an understanding of the landscape

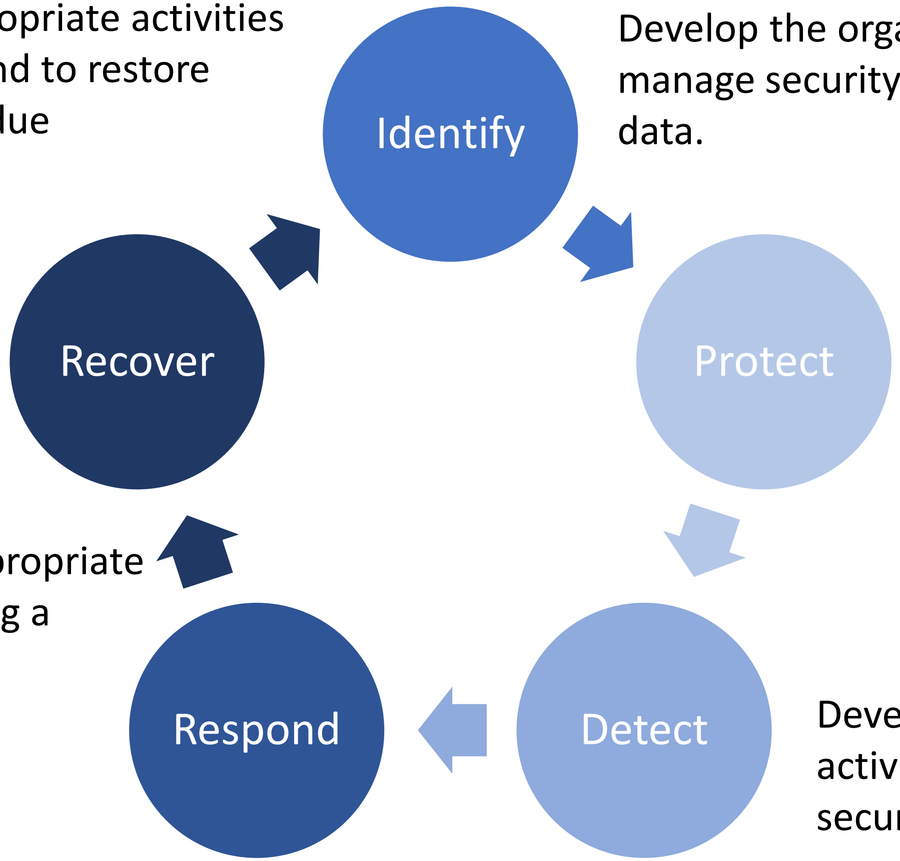


| Who will attack us | How will they do it | What will be affected | What will we do |
|---|---|---|---|
| Threat actors (Insiders, Hacktivists, Cybercriminals, Competitors, Nation State) | Vulnerabilities<br>(Targeted attacks, opportunistic threats) | People (Safety)<br>Operational effectiveness (Critical Business Processes, Trust)<br>Technology (Systems, Identity, Data, Platform, Network) | Reaction<br>(Identify, Protect, Detect, Respond, Recover) |
| Threat Intelligence (insights into threat actors, their motivation, information exchange with industry peers) | Threat intelligence (vendor information on vulnerabilities, exploitation techniques) | Threat intelligence (understanding of current modus operandi of cyber criminals, adapt monitoring strategy, adapt protection measures) | Incident Response (monitoring for unusual system behaviour, containment in case of breach, forensic investigation, adapt protection measures) |

# Setting the scene – getting an understanding of the actors



# The NIST cycle – focusing on resilience



Develop the organizational understanding to manage security risk to systems, assets, data.

Develop and implement the appropriate safeguards to ensure delivery of IT services.

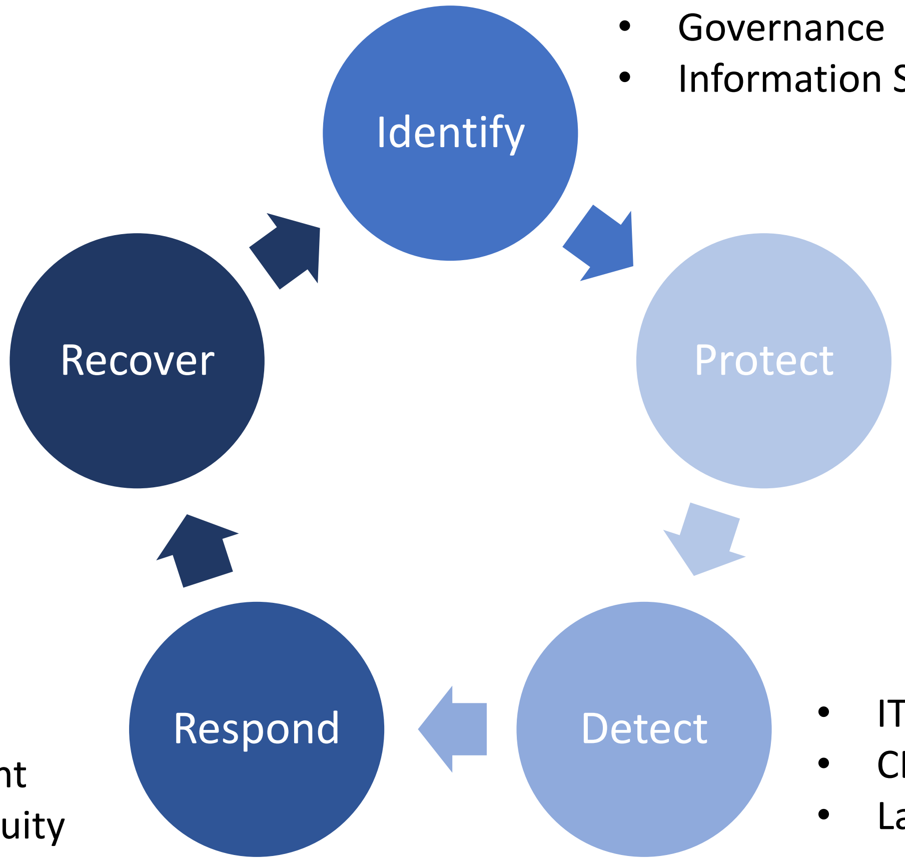
Develop and implement the appropriate activities to identify the occurrence of a security event.

Develop and implement the appropriate activities to take action regarding a detected security event.

Develop and implement the appropriate activities to maintain plans for resilience and to restore any services that were impaired due to a security event.

Source: National Institute of Standards and Technology (NIST): Cybersecurity Framework for Critical Infrastructure

# The NIST cycle – focusing on resilience



- Governance
- Information Security

- Governance
- Information Security
- IT Security

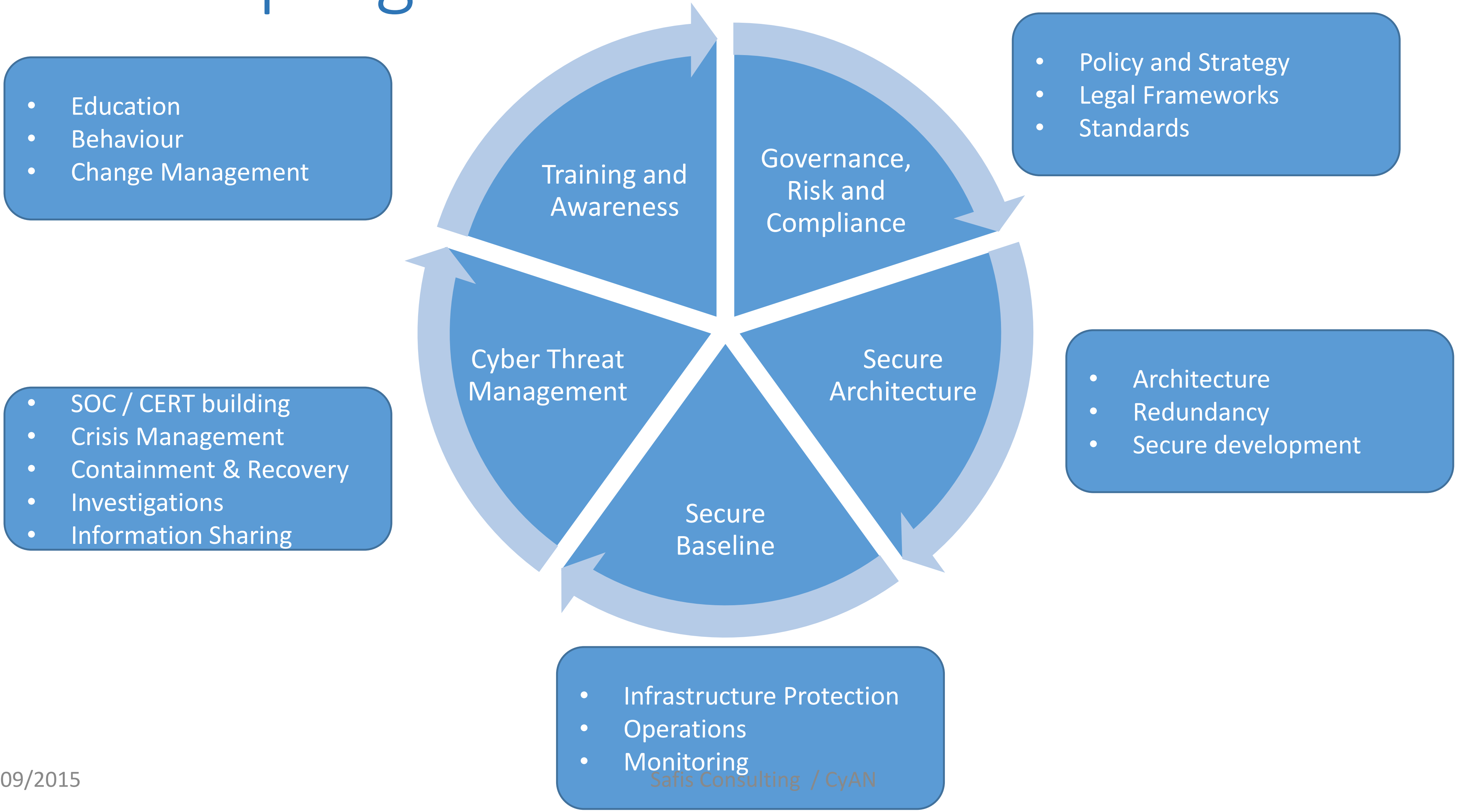
- IT Security
- CERT’s
- Law Enforcement

- IT Security
- CERT’s
- Law Enforcement
- Business Continuity

- Business Continuity
- IT Security
- Information Security

Source: National Institute of Standards and Technology (NIST): Cybersecurity Framework for Critical Infrastructure

# Mapping the NIST – cycle to a resilience-focused program



Training and Awareness

- Education
- Behaviour
- Change Management

Governance, Risk and Compliance

- Policy and Strategy
- Legal Frameworks
- Standards

Secure Architecture

- Architecture
- Redundancy
- Secure development

Secure Baseline

- Infrastructure Protection
- Operations
- Monitoring

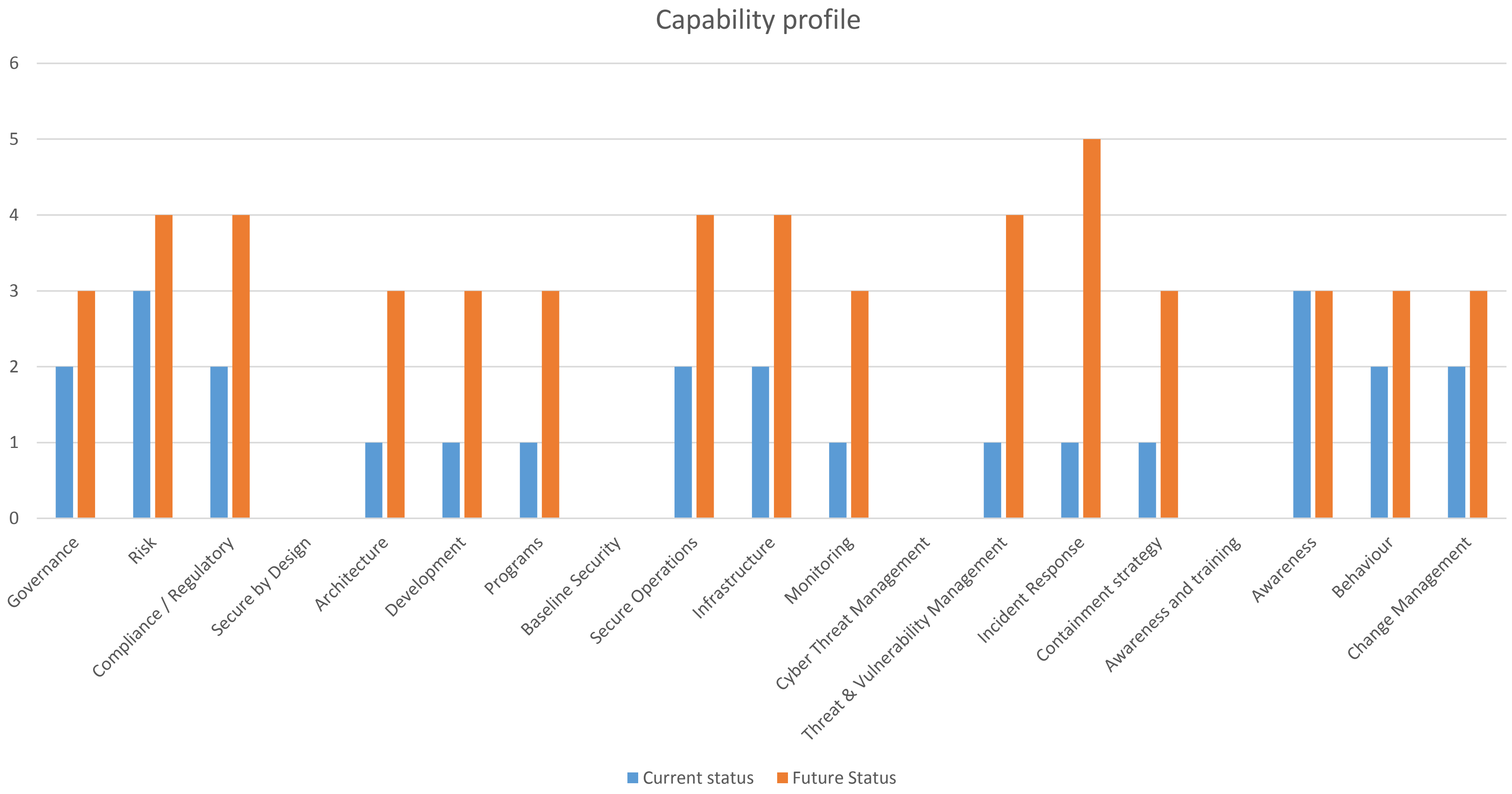
Cyber Threat Management

- SOC / CERT building
- Crisis Management
- Containment & Recovery
- Investigations
- Information Sharing

# Maturity assessment based on Oxford model

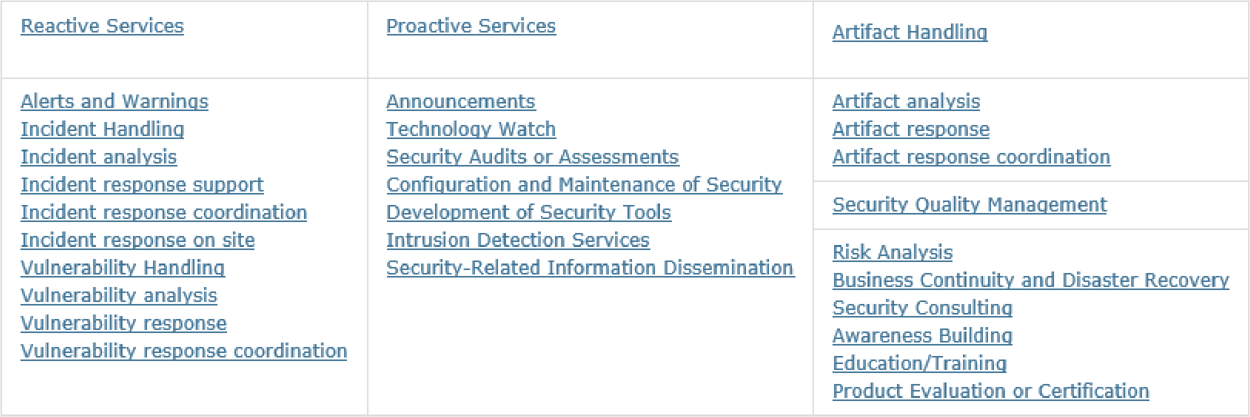
- Start-up: embryonic
- Formative: ‘new’
- Established: indicators are functional and defined
- Strategic: choices have been made about what to prioritize
- Dynamic: rapid decision- making, reallocation of resources and constantly changing environment

# Organizational profile


Capability profile

# Putting the strategy into action – example Threat Management Stream

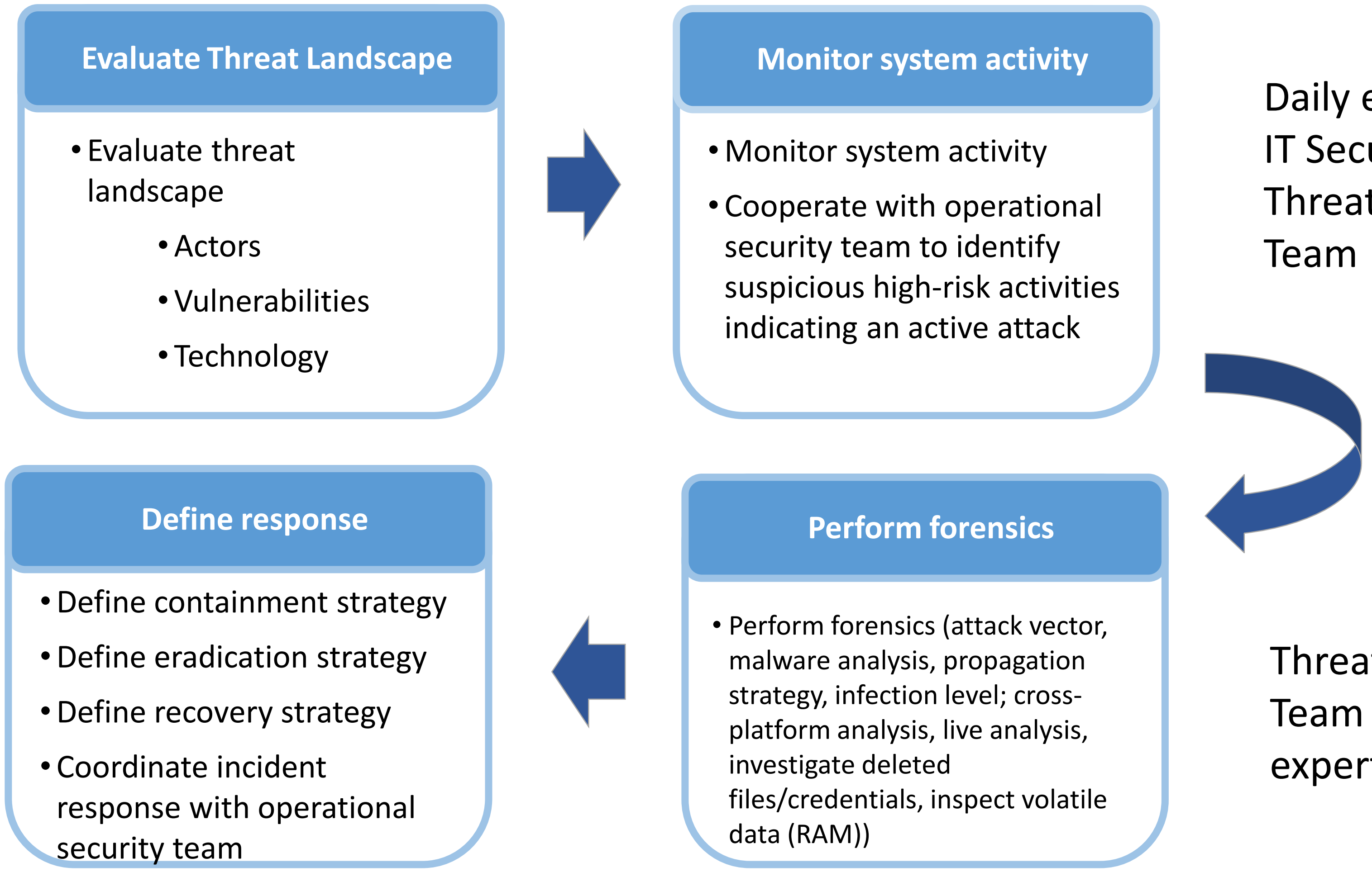
- Decisions to be made
  - Which services
  - Interfaces with other work streams
  - Sourcing of information and expertise
  - Skills / people needed
  - Communication strategy
  - Information sharing strategy



| Reactive Services | Proactive Services | Artifact Handling |
|---|---|---|
| Alerts and Warnings<br>Incident Handling<br>Incident analysis<br>Incident response support<br>Incident response coordination<br>Incident response on site<br>Vulnerability Handling<br>Vulnerability analysis<br>Vulnerability response<br>Vulnerability response coordination | Announcements<br>Technology Watch<br>Security Audits or Assessments<br>Configuration and Maintenance of Security<br>Development of Security Tools<br>Intrusion Detection Services<br>Security-Related Information Dissemination | Artifact analysis<br>Artifact response<br>Artifact response coordination |
| | | Security Quality Management |
| | | Risk Analysis<br>Business Continuity and Disaster Recovery<br>Security Consulting<br>Awareness Building<br>Education/Training<br>Product Evaluation or Certification |

Source: ENISA & CERT/CC

# Process and roles



Threat Management Team

## Evaluate Threat Landscape

- Evaluate threat landscape
  - Actors
  - Vulnerabilities
  - Technology

## Monitor system activity

- Monitor system activity
- Cooperate with operational security team to identify suspicious high-risk activities indicating an active attack

Daily exchange between IT Security Team and Threat Management Team

## Perform forensics

- Perform forensics (attack vector, malware analysis, propagation strategy, infection level; cross-platform analysis, live analysis, investigate deleted files/credentials, inspect volatile data (RAM))

Threat Management Team and external experts

## Define response

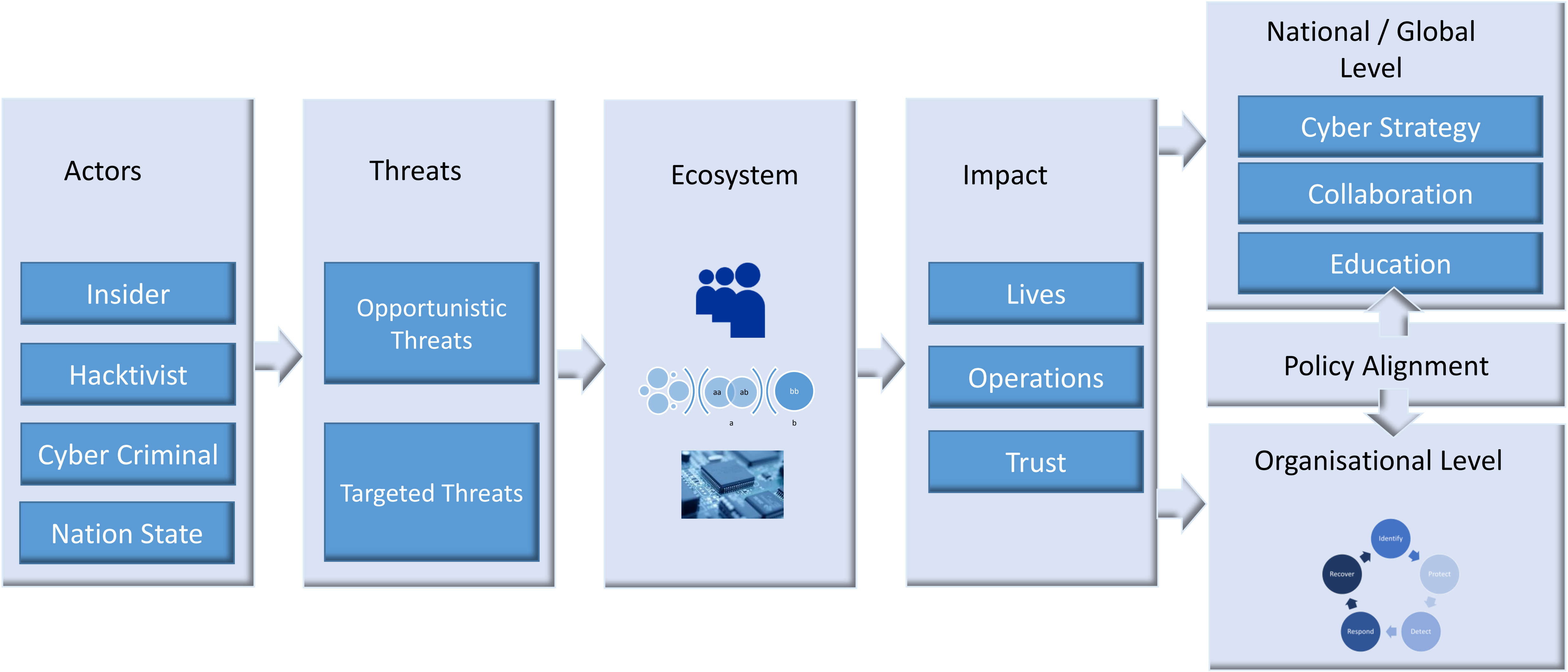
- Define containment strategy
- Define eradication strategy
- Define recovery strategy
- Coordinate incident response with operational security team

Threat Management Team with input of other work streams

# Future work

- On-going projects with budget in all work stream areas
- Roles and responsibilities, accountability, authority, budget, implementation plan, measuring progress and success, periodic reporting in all work streams
- Implementation timeline 2015 - 2019

# Summary



Actors

- Insider
- Hacktivist
- Cyber Criminal
- Nation State

Threats

- Opportunistic Threats
- Targeted Threats

Ecosystem

Impact

- Lives
- Operations
- Trust

National / Global Level

- Cyber Strategy
- Collaboration
- Education

Policy Alignment

Organisational Level

# Learnings

- Invest time in assessing your needs and capabilities
- There is a lot of good information available but a copy-paste approach does not work: it needs to fit your specific case
- No single organization can solve the challenge: multi-disciplinary approach needed (legal, policy, technical, organizational, educational)
- Communication / information sharing is key to learning and improving
- Put the strategy into action soon: Roles and responsibilities, accountability, authority, budget, implementation plan, measuring progress and success, periodic reporting
- Resources are scarce but not an excuse to do nothing: find different approaches to tackle the shortage

# Learnings

- Resilience assessments should be function-based (rather than asset-based), and should encompass both physical and cyber terrain.
- Include external providers in your consideration
- Implementing resilience is a long-term project: plan to cater for changes and look for partners that stay with you long-term

Monika Josi

monika.josi@safis.ch

CyAN Cybersecurity Advisors Network

Safis Consulting