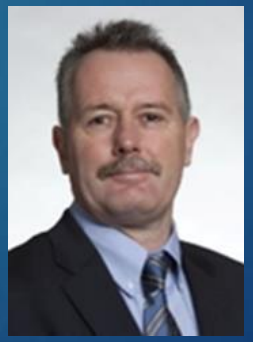
“Supply Chain Cyber Security Resiliency

‘It’s more than Tech!’

Executive Director, Sustainable Resilient Value Chains, EPFL



Former VP Procter & Gamble Globla Cyber Security

What is Supply Chain Resiliency
2-3 slides

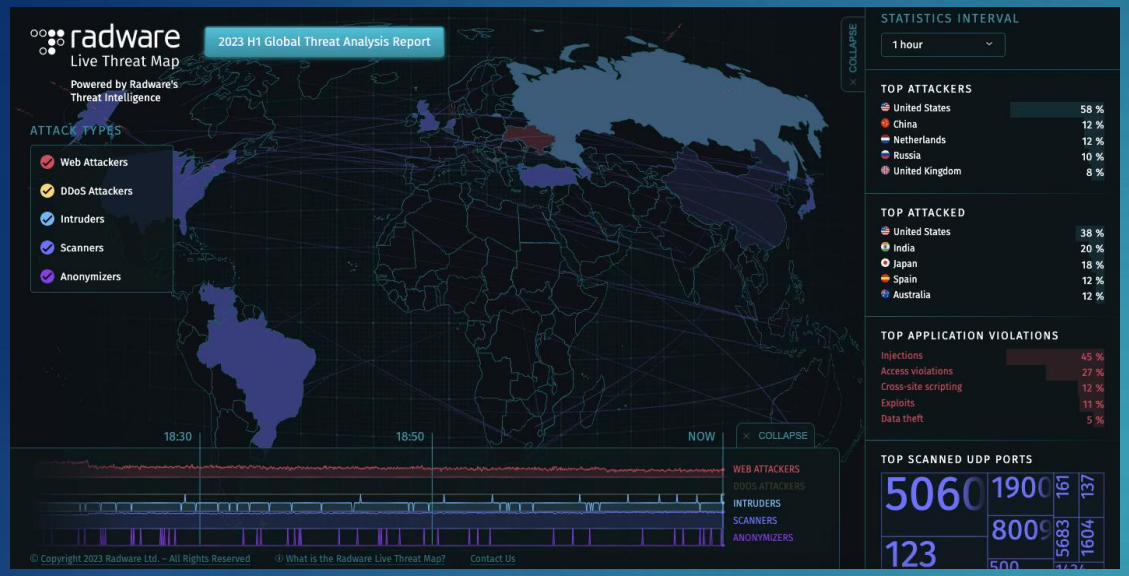
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

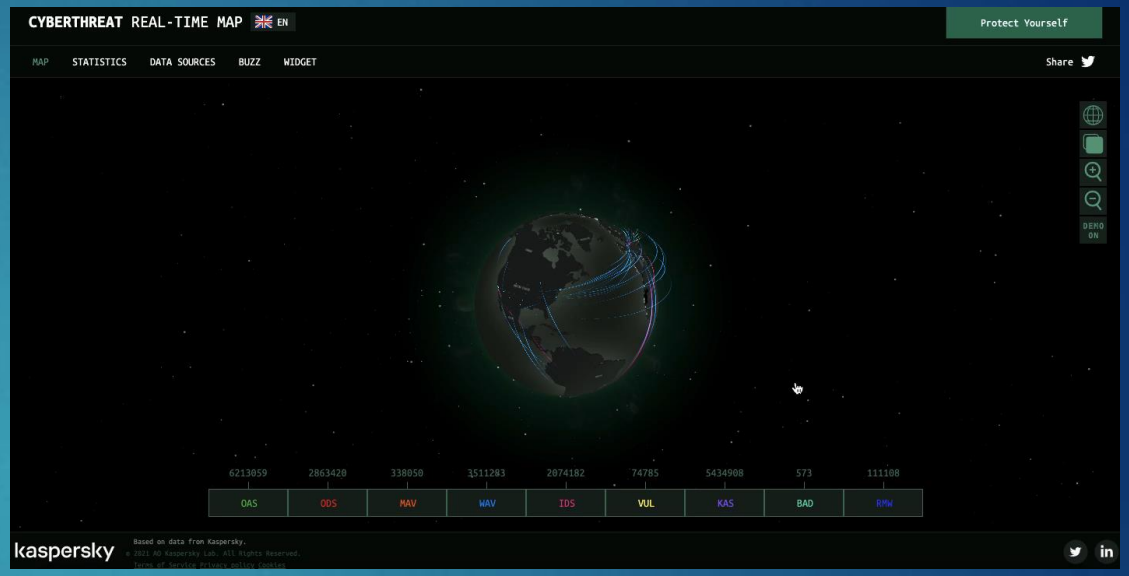
Cyber Security Resiliency

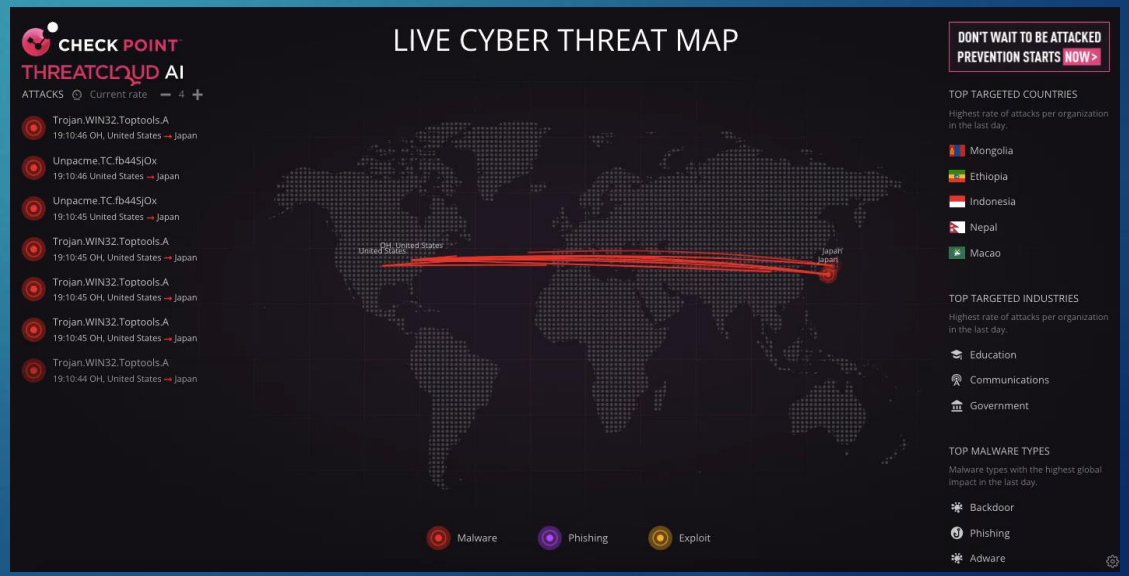
What are the resiliency challenges?
1-2 slides
(including cyber security risks)

Reality

It's not IF you are attacked – it's when you knew about it







WHY DO COMPANIES & ORGANIZATIONS GET BREACHED?

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Cyber Security Resiliency

CMA Shipping – Sept 2021

Transport for London – Sept 2024

Molson Coors – March 2021

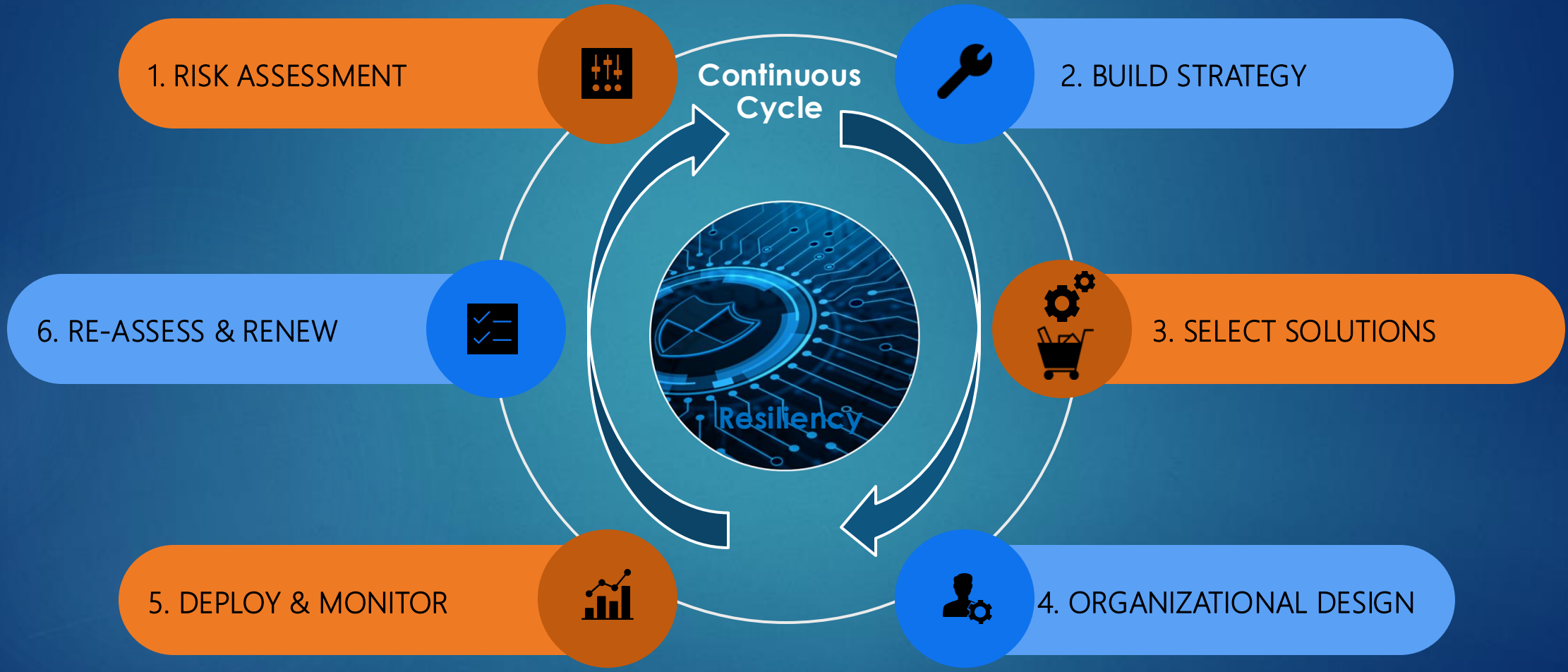
MGM – Caesars – Sept 2023

Duvel Moortgat brewery - *March 2024*

Colonial Pipeline – May 2021

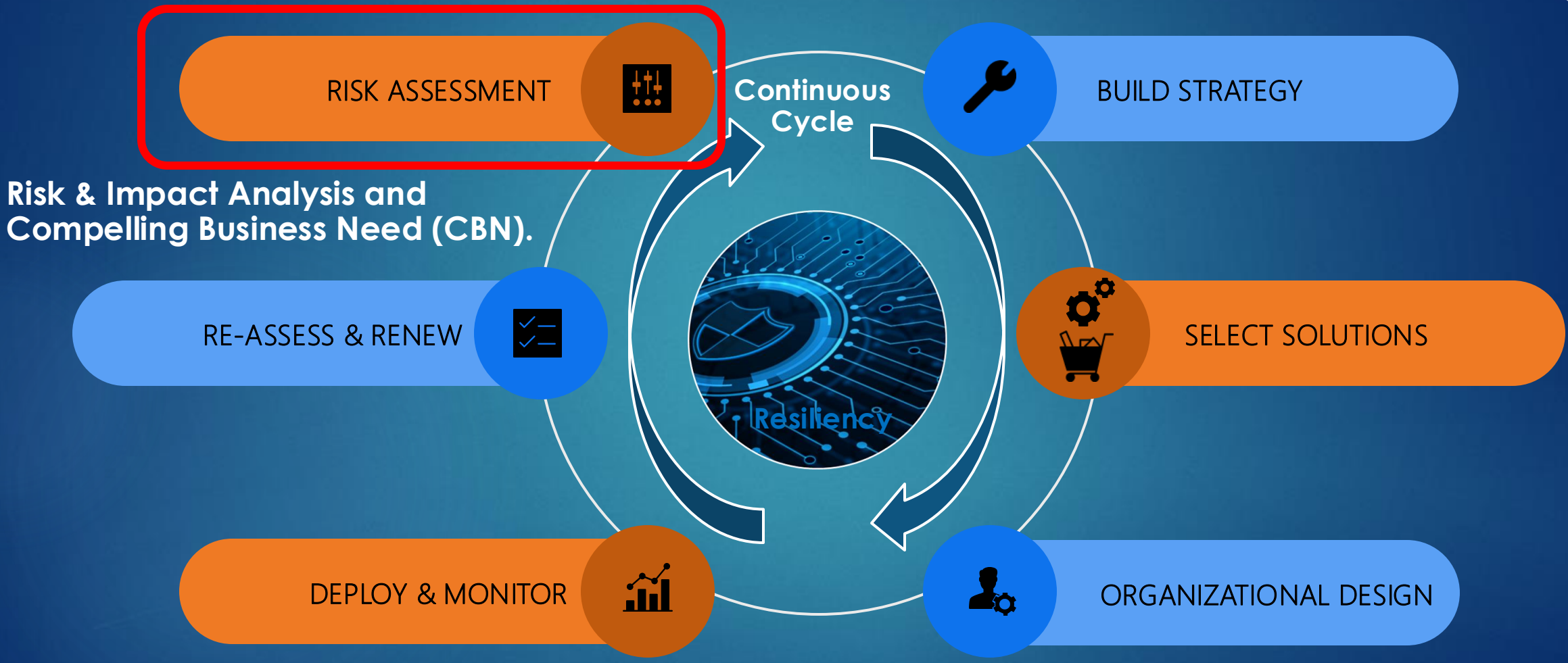
Cyber Resiliency

How to improve



Cyber Resiliency

The roadmap to cyber security resiliency



Cybersecurity risk

Cybersecurity risk is the potential for exposure or loss resulting from a cyberattack or data breach within an organization.

WHAT'S THE INFORMATION SECURITY RISK?

The cyber threat landscape is becoming increasingly complex as we see threat actors blend methods and motivations of other threat actors

Hacktivists

Cybercriminals

Nation-state sponsored attacks & advanced persistent threat[1] (APT)

Attacker sophistication

"Apple Pay has numerous protections for users' own credit cards. But researchers claims it's easy to add stolen cards to the app, helping fraudsters circumvent protections designed to prevent cloned cards." - *Forbes,* March 1, 2016

Could potentially bypass biometric solutions by targeting authentic data stored on a customer's mobile device

Typically operate with a high degree of persistence and stealth against high profile corporations and foreign governments, but are also capable of highly disruptive attacks

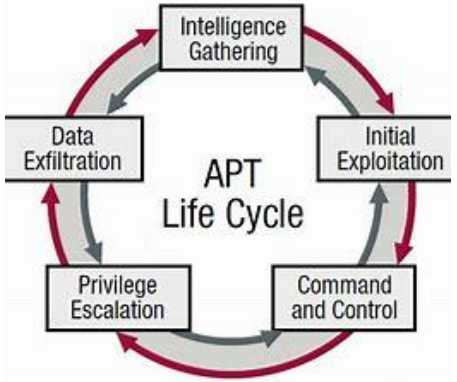
State Sponsored Espionage (Stuxnet)
Market Manipulation (M&A)
Competitive Advantage (contract negotiations, trade secrets)
Military / Political objectives

Uses commoditized exploit kits along with botnets and other automated attack vectors to maximize financial returns while minimizing hands-on effort

Anonymous' Operation Icarus has attempted to initiate DDoS attacks against a variety of global financial institutions.

Disrupt operations through DDoS attacks, website defacements, and/or negative social media postings

"FireEye researchers Tao Wei and Yulong Zhang outlined new ways to attack Android devices to extract user fingerprints."
-*ZDNet*, August 5, 2015

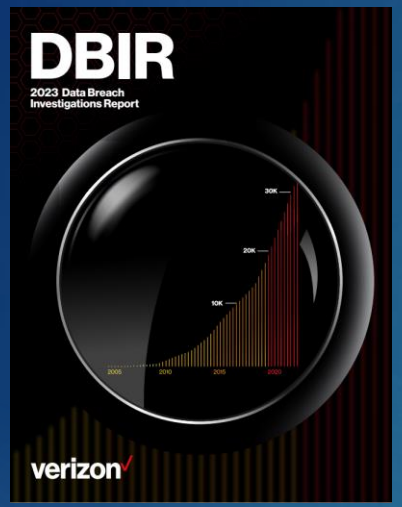


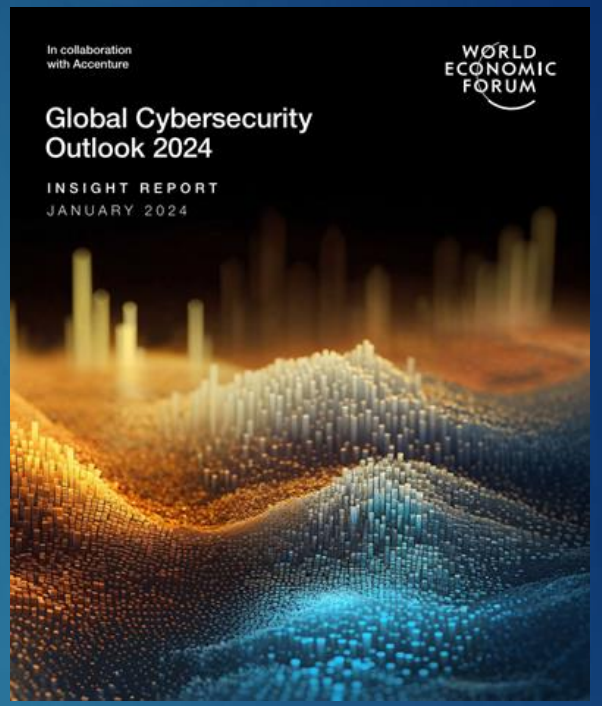
Attacker resources and risk level

[1] An advanced persistent threat (APT) is a set of sophisticated, stealthy and continuous computer attacks often targeting a specific entity with business or political motives. The processes used involve a high degree of covertness over a long period of time using sophisticated techniques to exploit vulnerabilities in systems.

RISK ASSESSMENT

Sources for Risk Insights





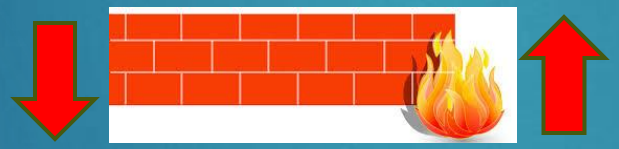
Colonial Pipeline

- Discovered Aug 2020
- Apolitical group (focus $)
- Highly-targeted attacks
- Based in Eastern Europe
- Ransomware developer
- RaaS Provider

Industrial Controls Systems

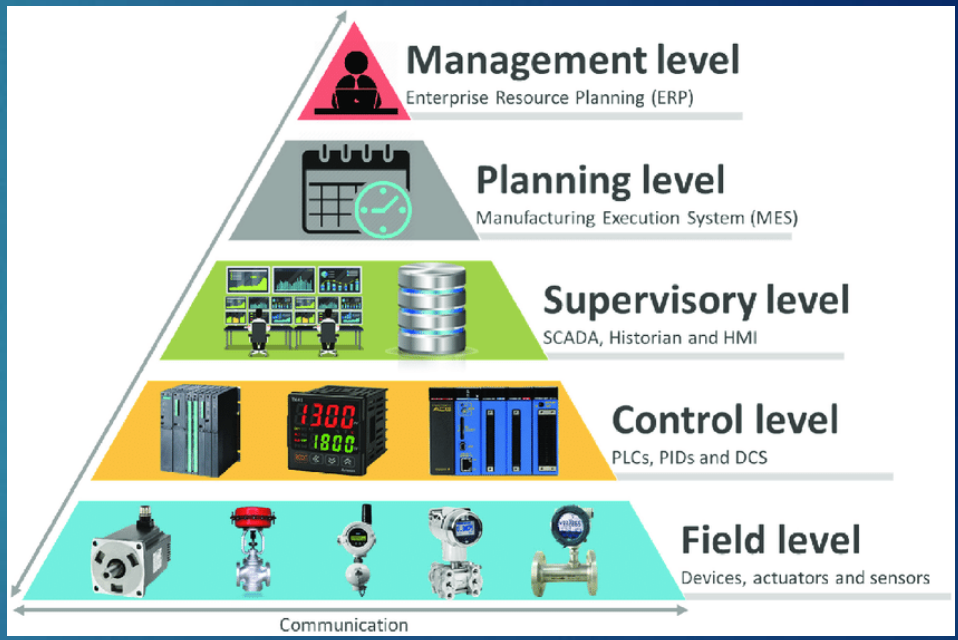
Operating Technology (OT) Domain

IT Domain
Typical Focus



OT Domain
100x microprocessors versus IT Domain

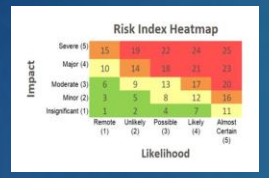
Purdue Model



Risk Assessment Models

1. **Quantitative** - Assets and risks receive $ values

2. **Qualitative** - Categorize risks on rough scales



3. **Semi-quantitative** - Numerical scale, such as 1-10 or 1-25

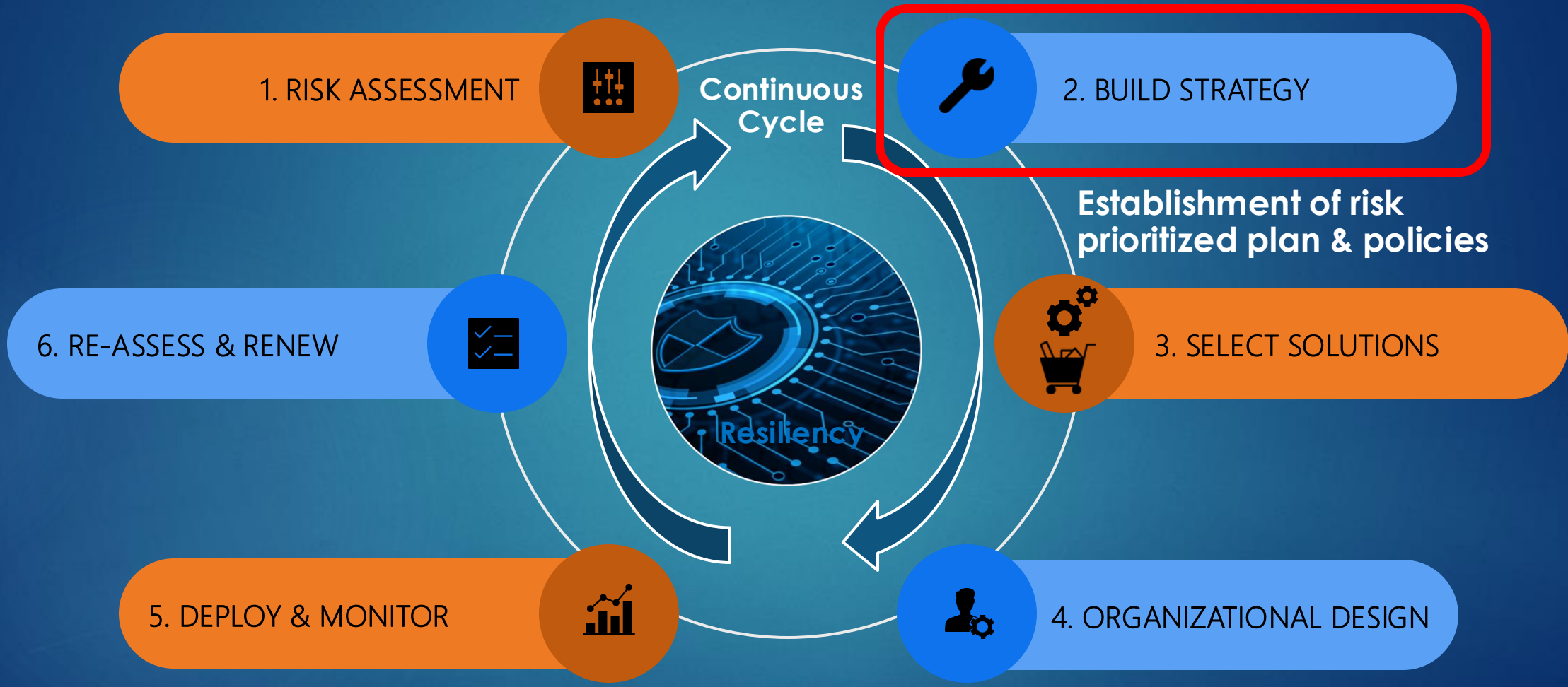
4. **Asset-based** - Hardware, software, and networks that handle data.

5. **Vulnerability-based** - Examination of the known weaknesses, deficiencies & threats

6. **Threat-based** - Evaluate the conditions that create risk across enterprise including people

Cyber Resiliency

The roadmap to cyber security resiliency

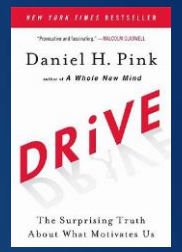


05/05/2025

BUILD STRATEGY

Compelling Business Need

Provide a collective sense of **purpose**

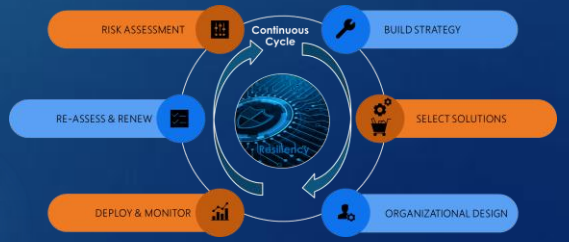


YouTube

MISSION STATEMENT

To **protect** the company and its stakeholders, including employees, from a business and reputational loss due to a **security breach** incurring loss of **critical information** or an impact to **operations**.

Protect, Detect & Respond to Cyber Threats that could **impact** Product Supply Manufacturing & Distribution



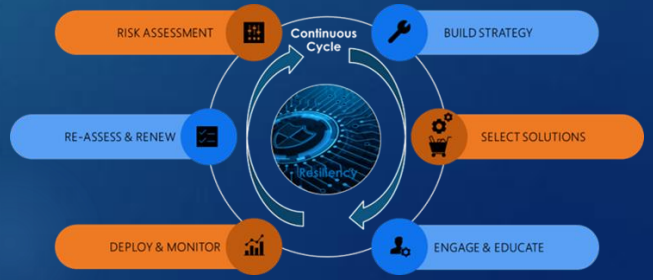
BUILD ON INDUSTRY FRAMEWORKS

Protection is IDEAL – **Detection** is a MUST (but needs an operational **Response** Capability).

Three most implemented frameworks.

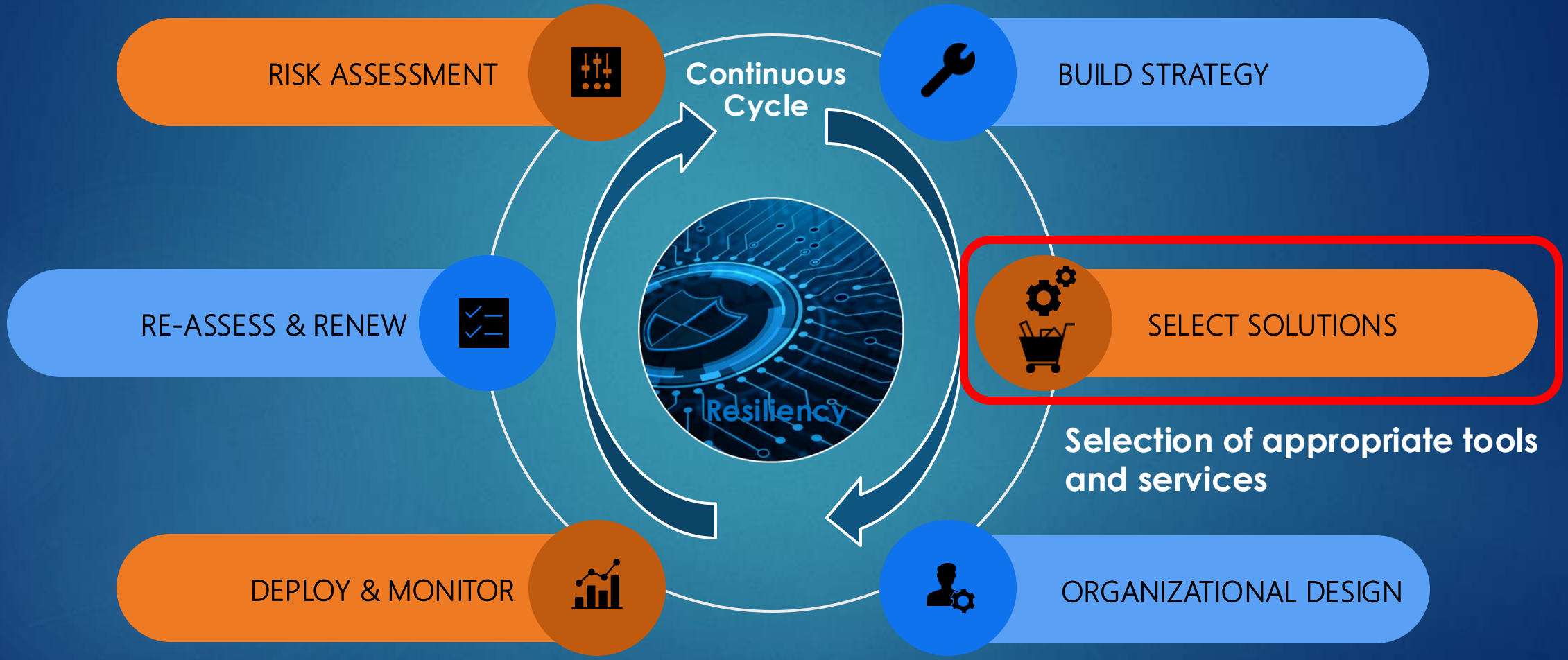
1. NIST (National Institute Standards & Technology) Cyber Security Framework ***(P&G adopted)***
2. ISA / IEC 62443 ***(P&G added for additional OT perspectives)***
3. ISO 27001

Capability	Description
Identify	What processes and assets need protection?
Protect	Implement appropriate safeguards to ensure protection of the enterprise's assets
Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
Respond	Develop techniques to contain the impacts of cybersecurity events
Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events



Cyber Resiliency

The roadmap to cyber security resiliency

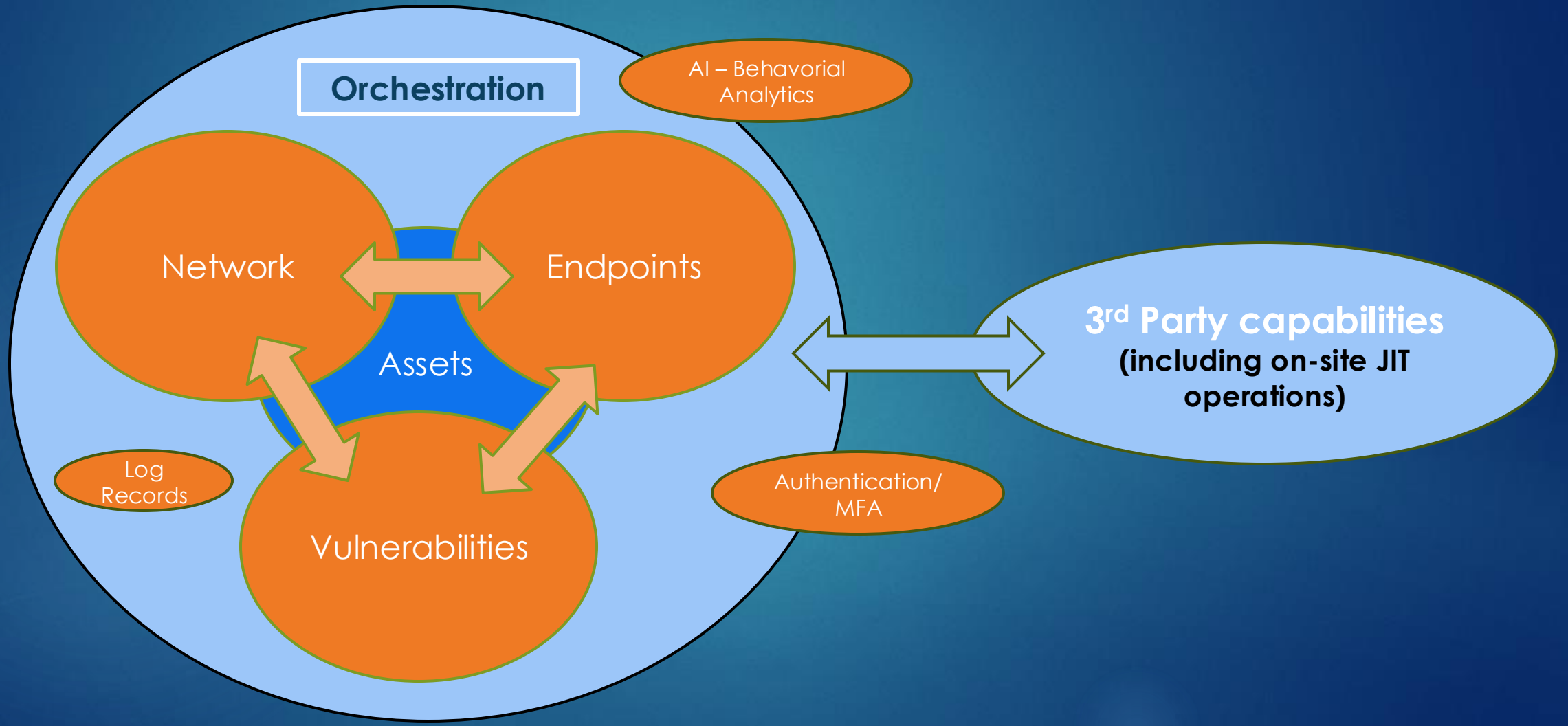


Selection of appropriate tools and services

SELECT SOLUTIONS

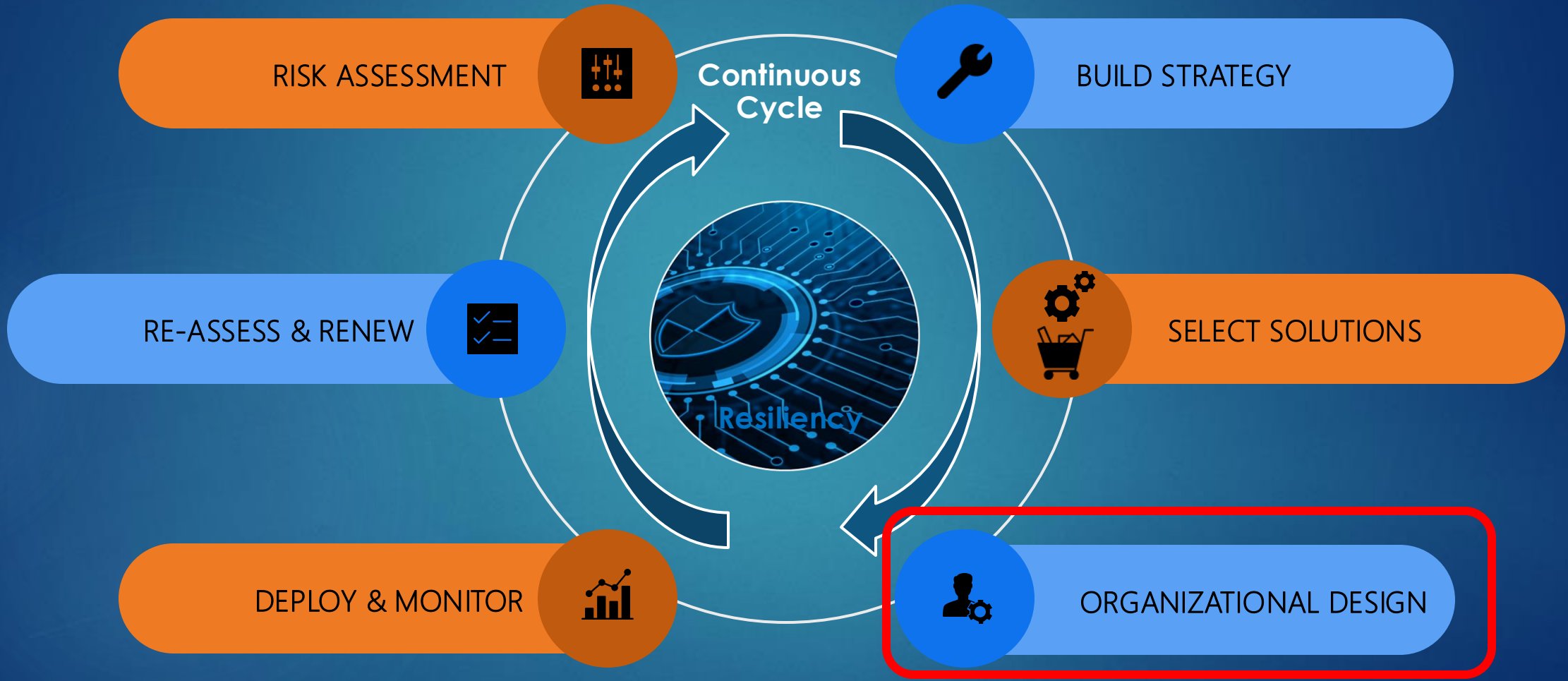
Cyber Security Solutions

A constantly changing complex environment



Cyber Resiliency

The roadmap to cyber security resiliency



Organizational design and train employees & partners

ORGANIZATIONAL DESIGN

Organization Design

"All organizations are perfectly designed to get the results they get"

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Cyber Security Resiliency

Design Elements

Structure
Does the structure permit the right people to work together on the tasks?

Rewards
Are the desired behaviors rewarded or punished? Are undesired behaviors rewarded or punished?

Tasks
Are specific tasks clearly identified which will lead to achieving the strategy and goals?

Decision Making
Do decisions reflect knowledge, experience and a 'bias for action'

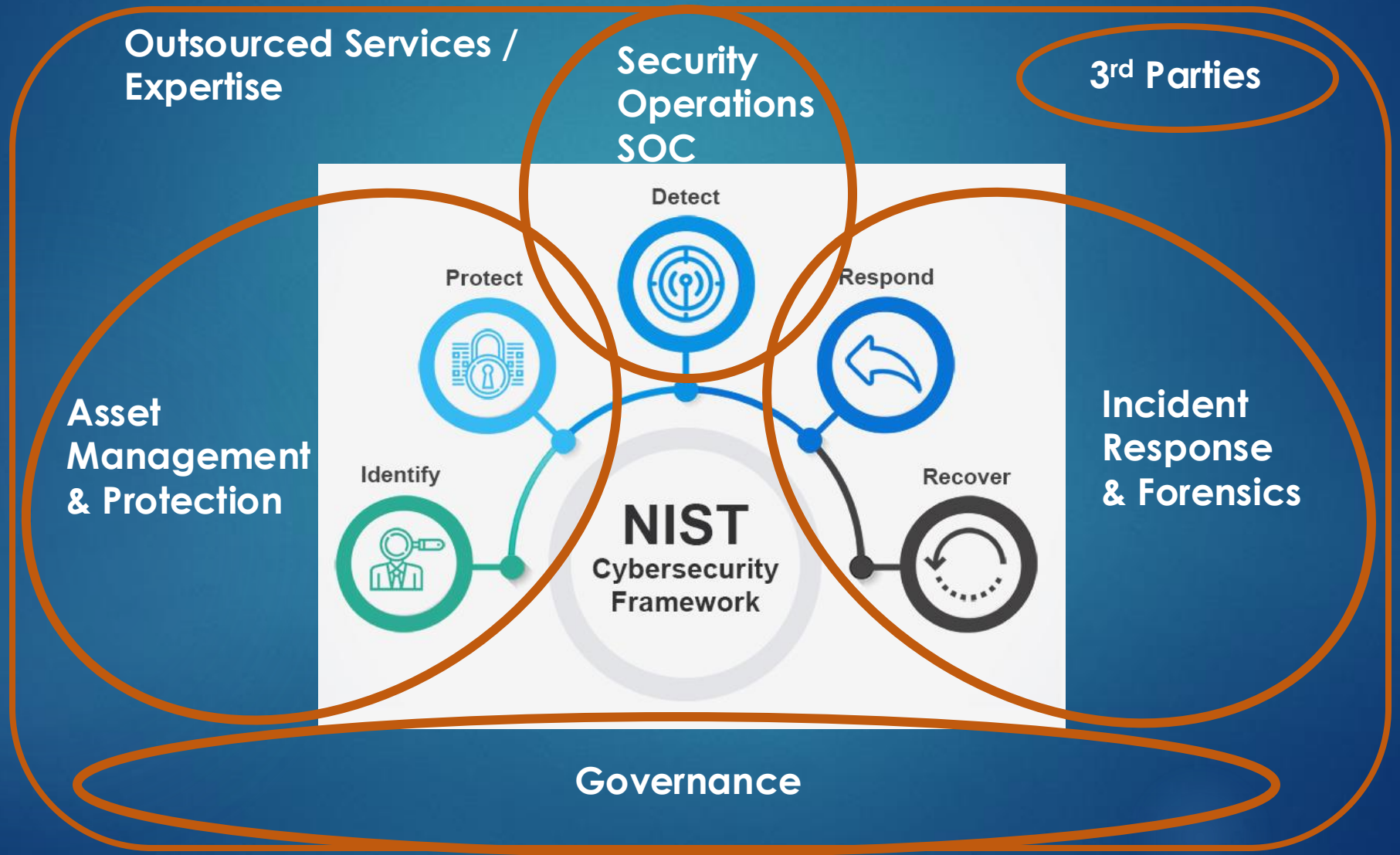
People
Do people have the skills to do the job?

Information
Is the information available?

ORGANIZATIONAL DESIGN

Organization Design

What needs to be true to enable the strategy & actions to be successfully applied



Common Cybersecurity Tabletop Exercise Scenarios

Scenario 1: Insider Threats

Scenario 2: Malware Infection

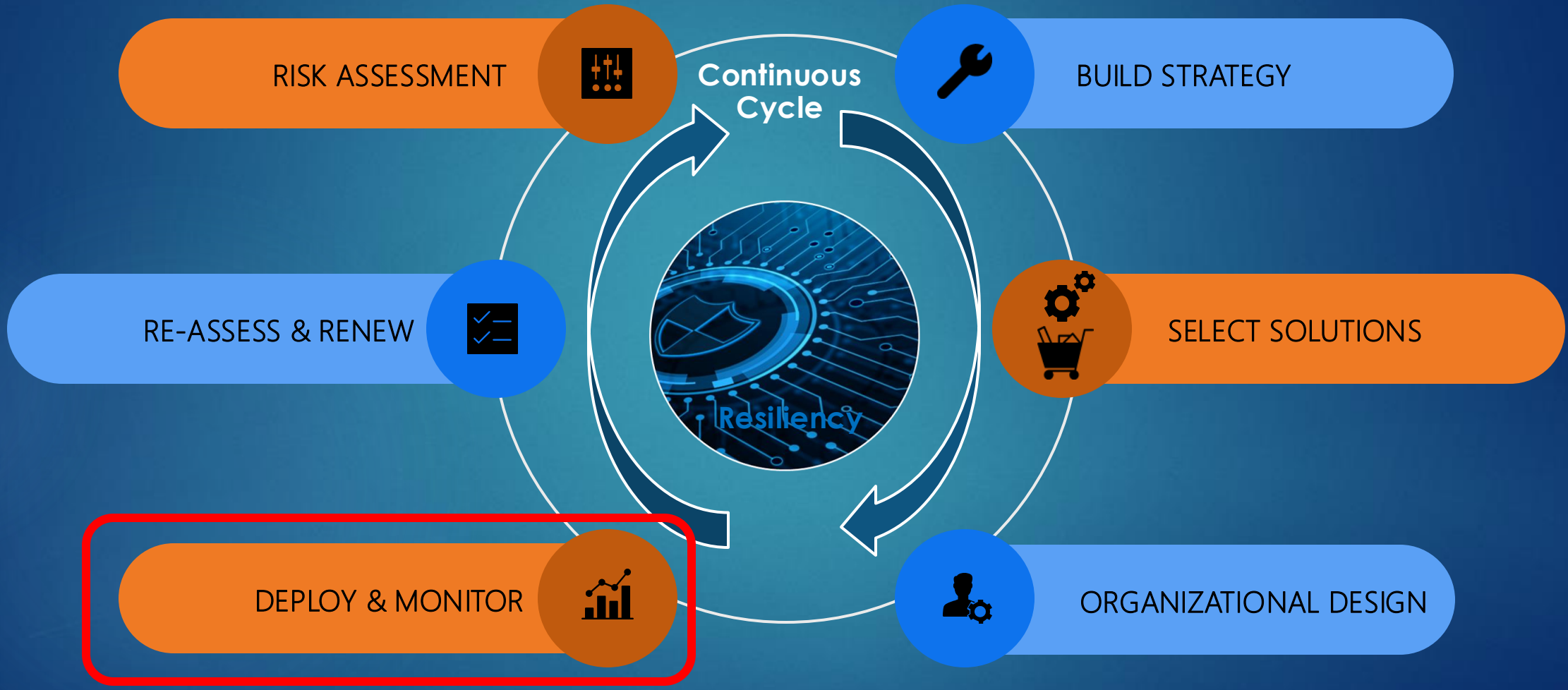
Scenario 3: Nation State Attack

Scenario 4: Accidental Compromise

Scenario 5: Social Engineering Attack

Cyber Resiliency

The roadmap to cyber security resiliency

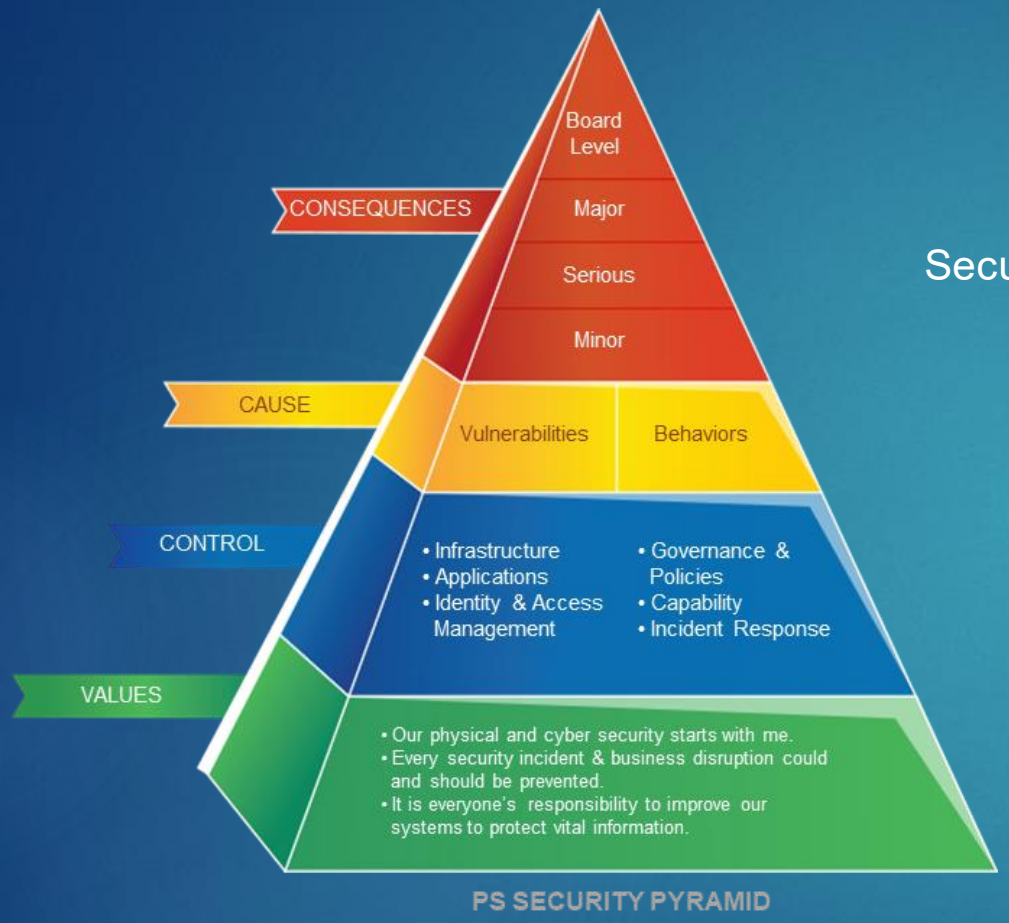


Engage Organization and implement solutions with governance, controls & continuous monitoring

DEPLOY & MONITOR

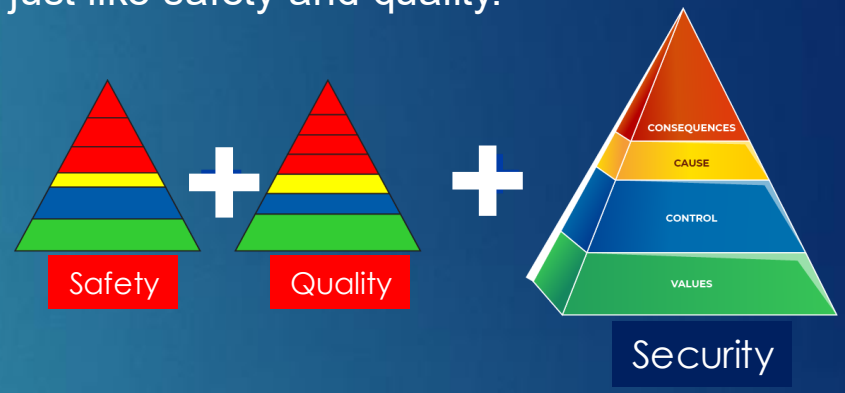
COMMUNICATION

Engage the organization's heart & mind



PS SECURITY PYRAMID

Security must be foundational, just like safety and quality.



DEPLOY & MONITOR

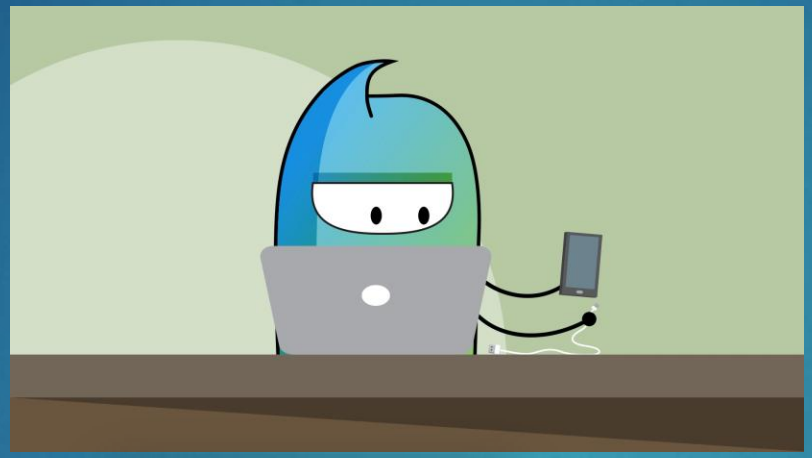
COMMUNICATION

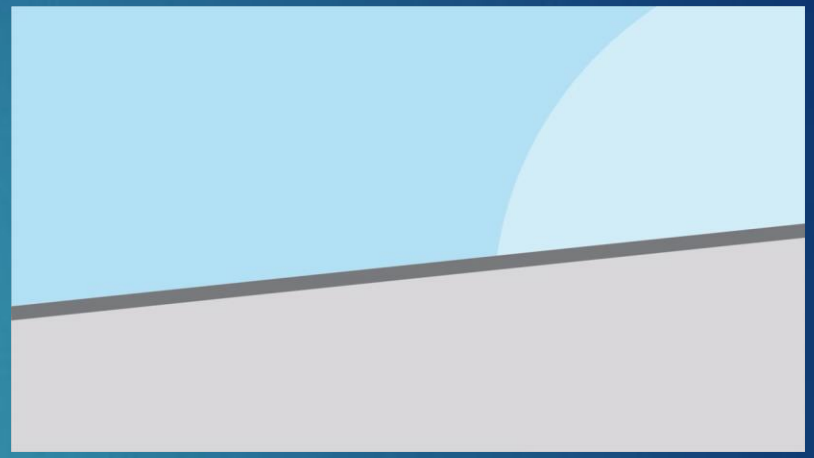
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

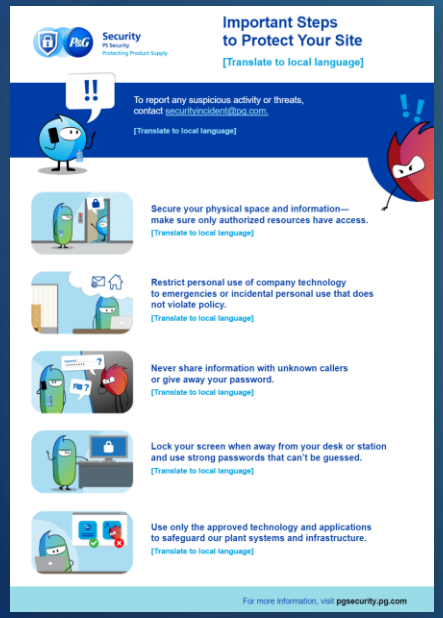
Cyber Security Resiliency

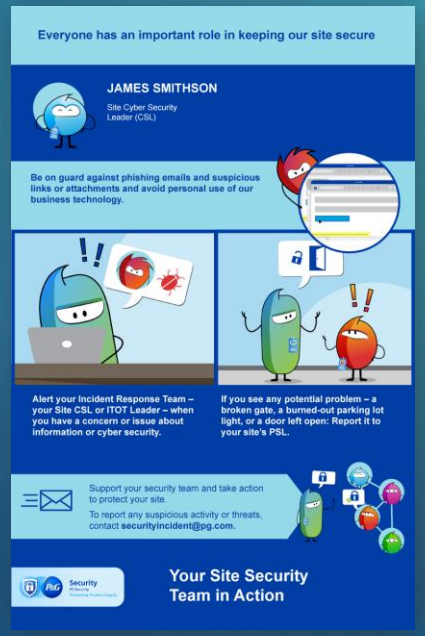
CREATING AWARENESS THAT CHANGES EMPLOYEE BEHAVIOR including THIRD-PARTIES

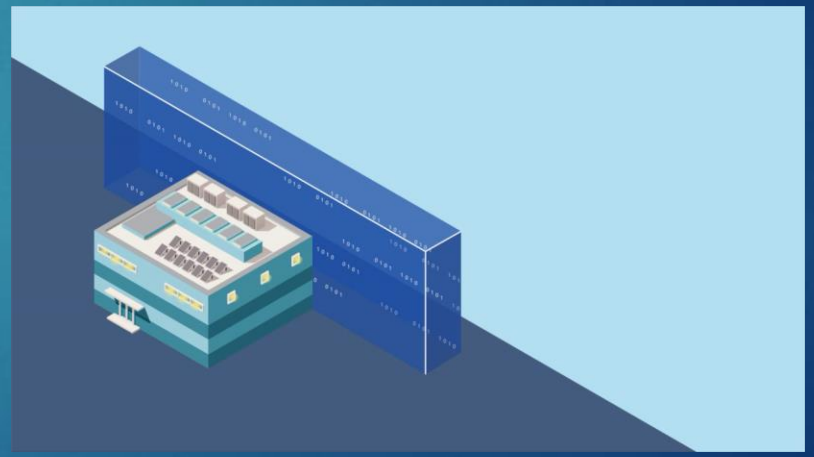
Security threat | Security learner | Security champion





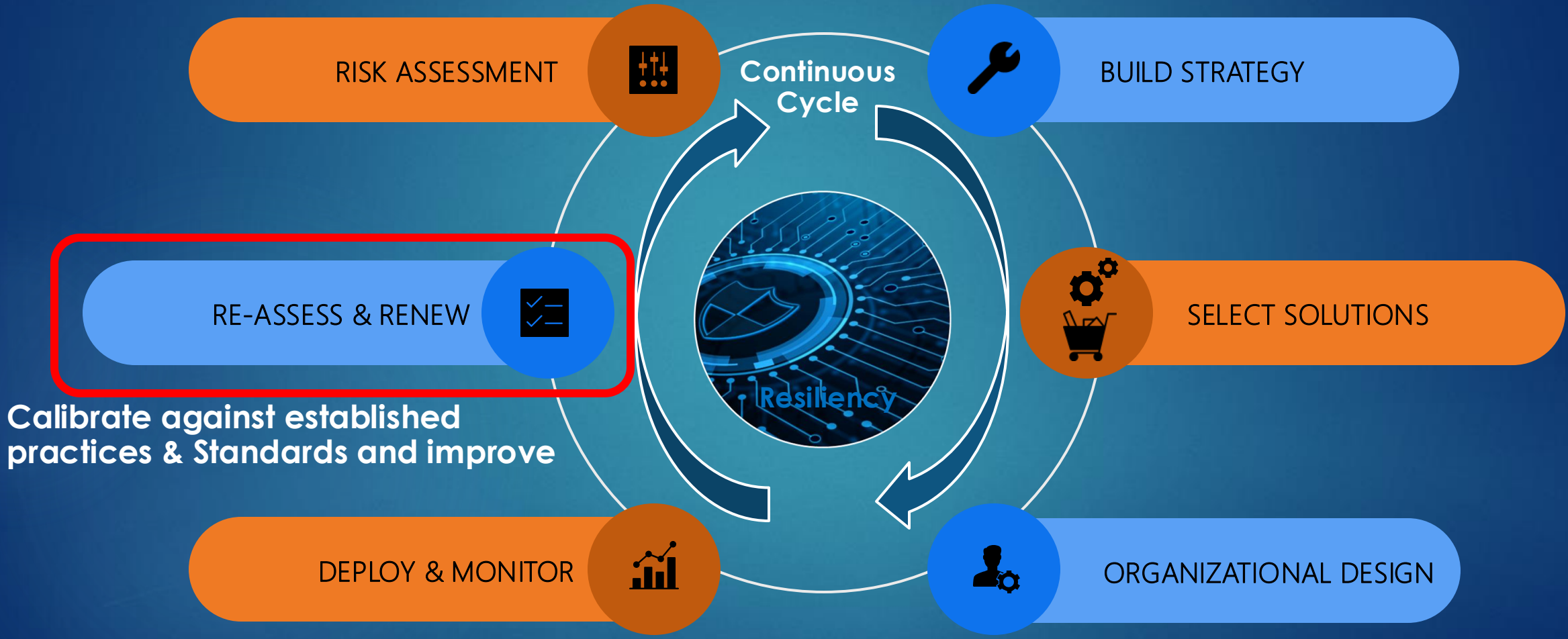






Cyber Resiliency

The roadmap to cyber security resiliency



Calibrate against established practices & Standards and improve

RE-ASSESS & RENEW

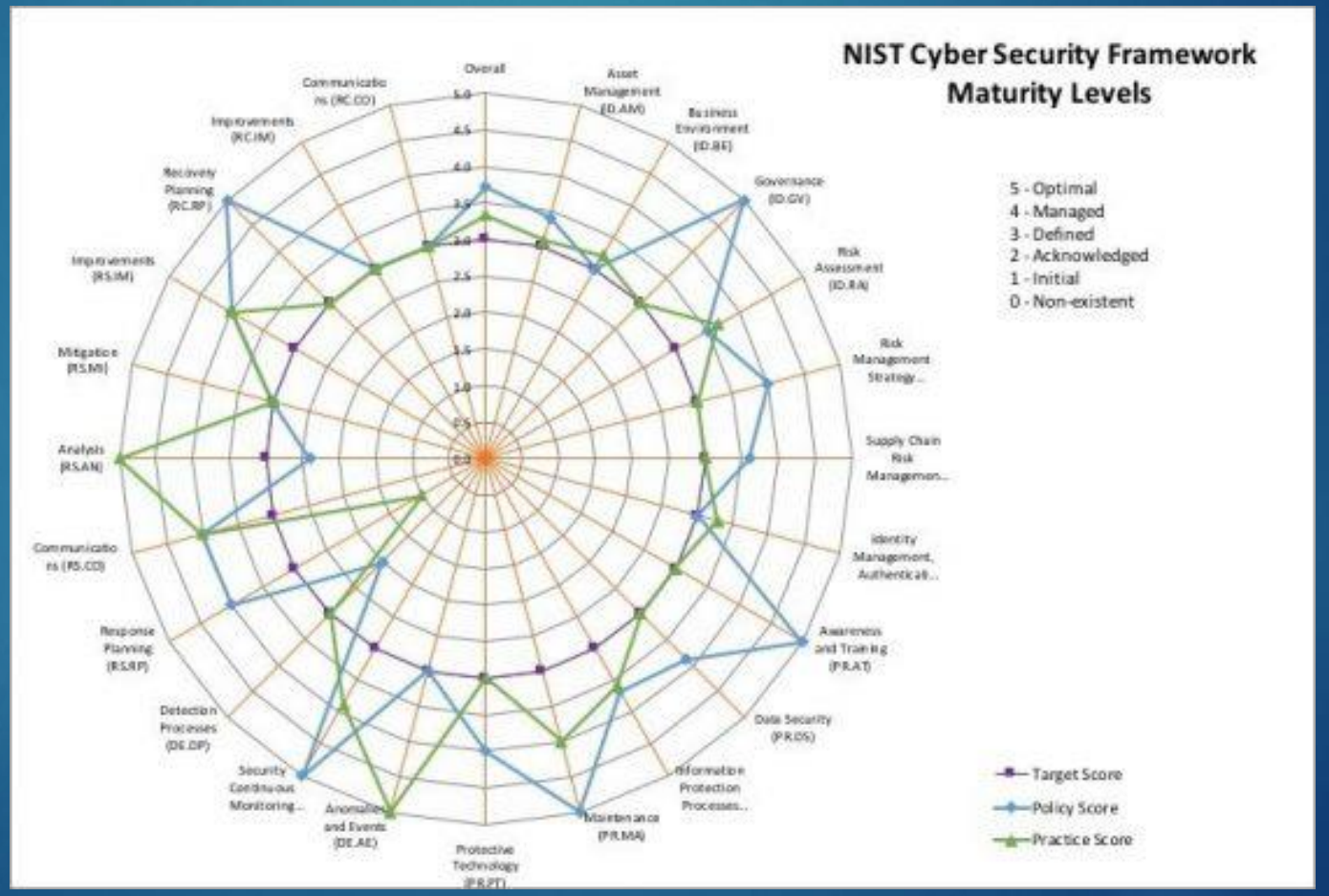
Achieve the desired Outcome

External cyber security maturity assessment and benchmarking

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Cyber Security Resiliency

IT and OT Domains



ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Cyber Security Resiliency

“Supply Chain Cyber Security Resiliency

‘It’s more than Tech!’