



GRC Be Connected

Cybersecurity Activities & Knowledge

26 January 2021



Programme

Time	Topic	Speaker
1:00 pm - 1:05 pm	Welcome	Mrs. Giselle Vercauteren President ISACA Belgium
1:05 pm - 1:35 pm	Cybersecurity expertise essential for all professions	Mr. Karel De Kneef Chief Security Officer SWIFT
1:35 pm - 2:15 pm	Cybersecurity steps based on the NIST cybersecurity framework	Mr. Umut Inetas Manager Security Architecture Ahold Delhaize
2:15 pm - 2:55 pm	Be successful in IT governance	Mr. Vilius Benetis CEO NRD Cyber Security
2:55 pm - 3:00 pm	Wrap-up & closure of the meeting	Mrs. Giselle Vercauteren President ISACA Belgium



**How can security and risk management
leaders optimize their talent challenges.**

Karel De Kneef, Chief Security Officer, SWIFT

Belgian Cybersecurity Coalition – 26 January 2021



The global
provider of secure
financial
messaging
services



SWIFT
in figures

36.7 million

FIN messages peak day (2019)

8.5 billion

FIN messages per year (2019)

7.3%

Increase in FIN traffic (2019)

11,000+

SWIFT users

200+

Countries and territories

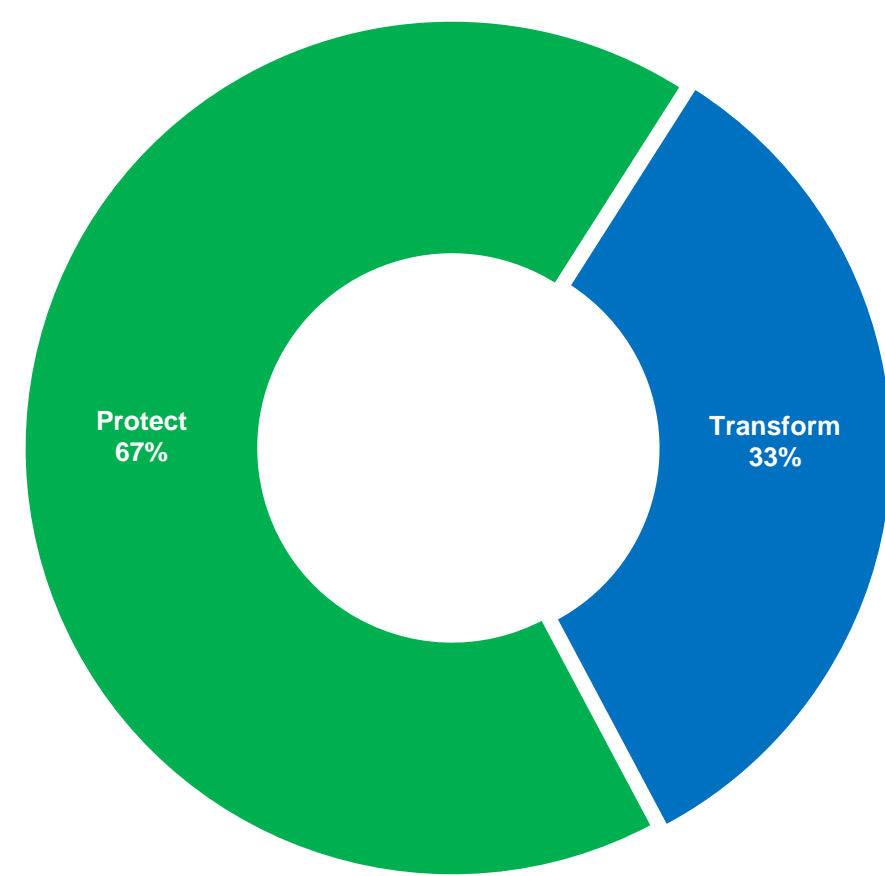


Cyber threat landscape is shifting and the attack surface is always changing

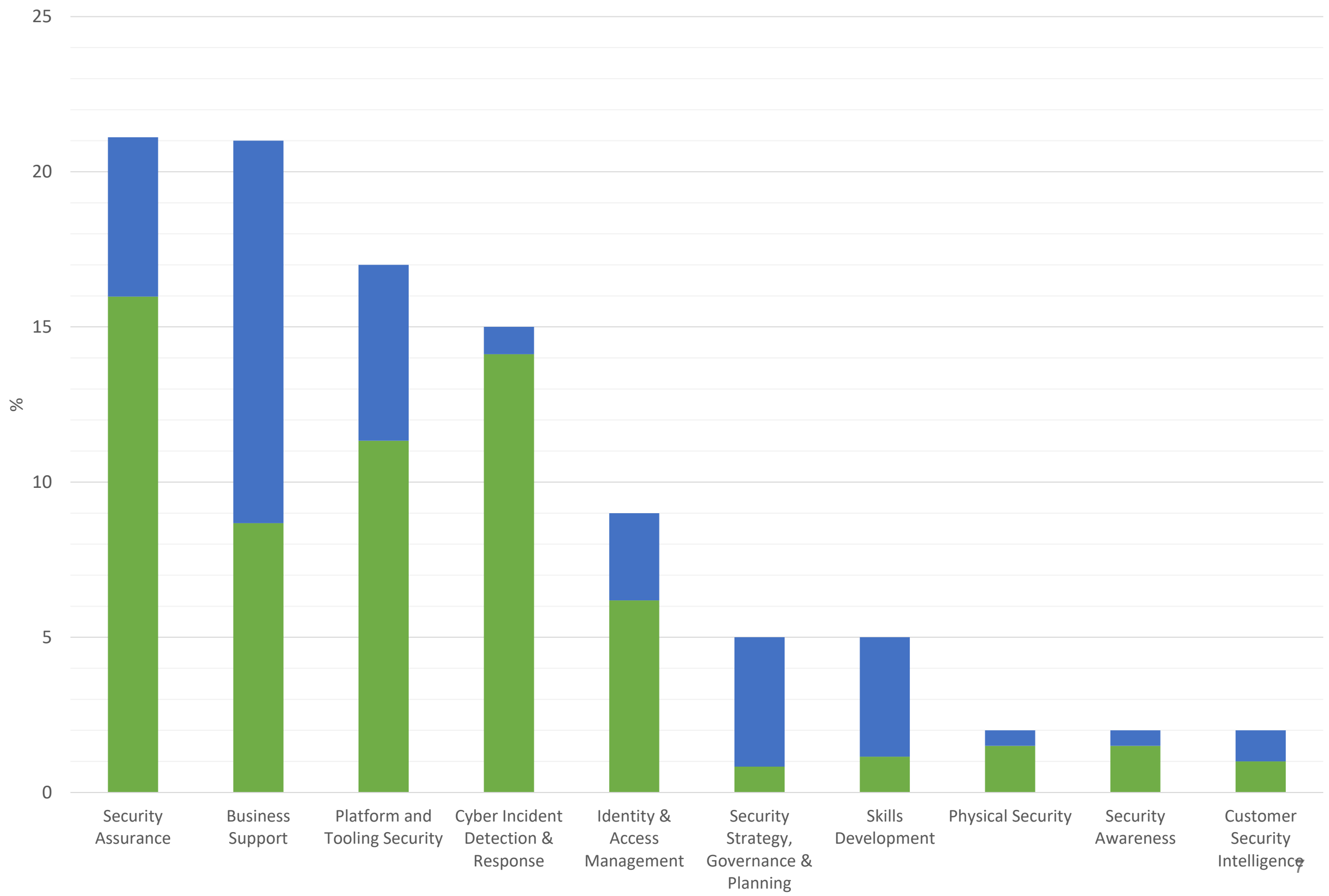


Cybersecurity activities

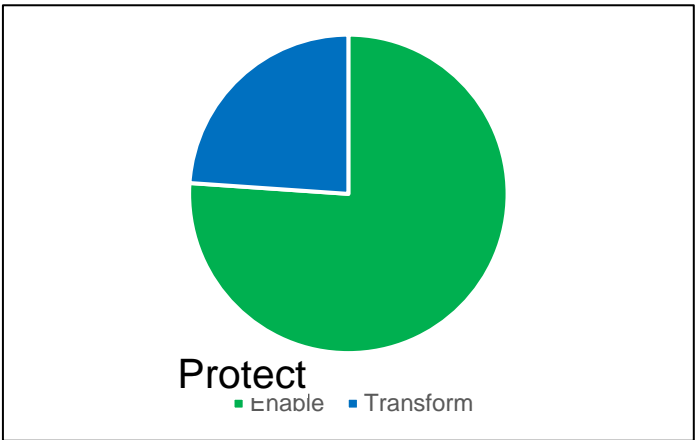
Effort split : Protect vs Transform



- ❖ **Protect = daily operations of key security functions**
- ❖ **Transform = initiatives to improve security functions and/or support new business initiatives**

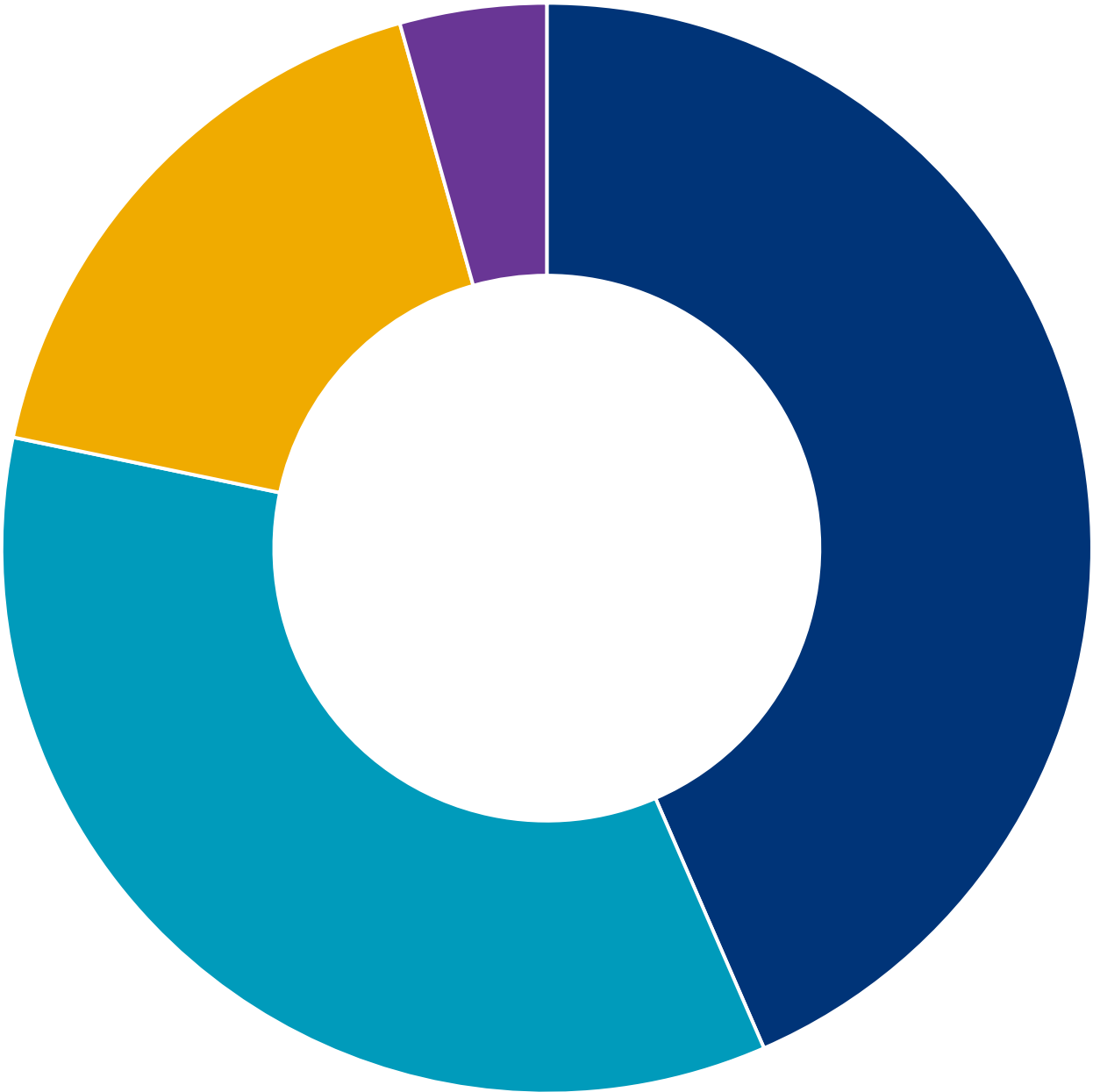
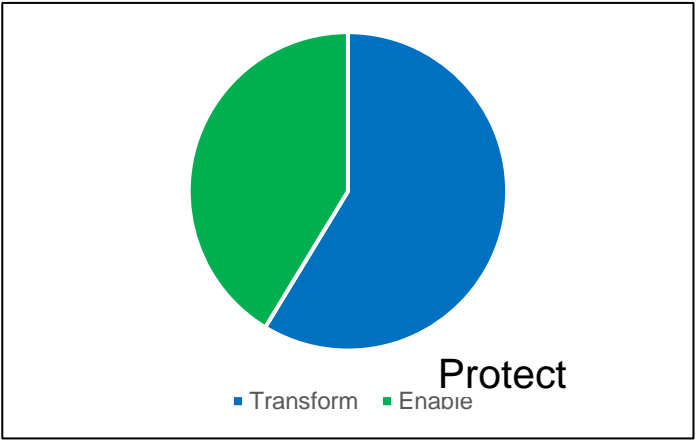


Zoom on Security Assurance activity



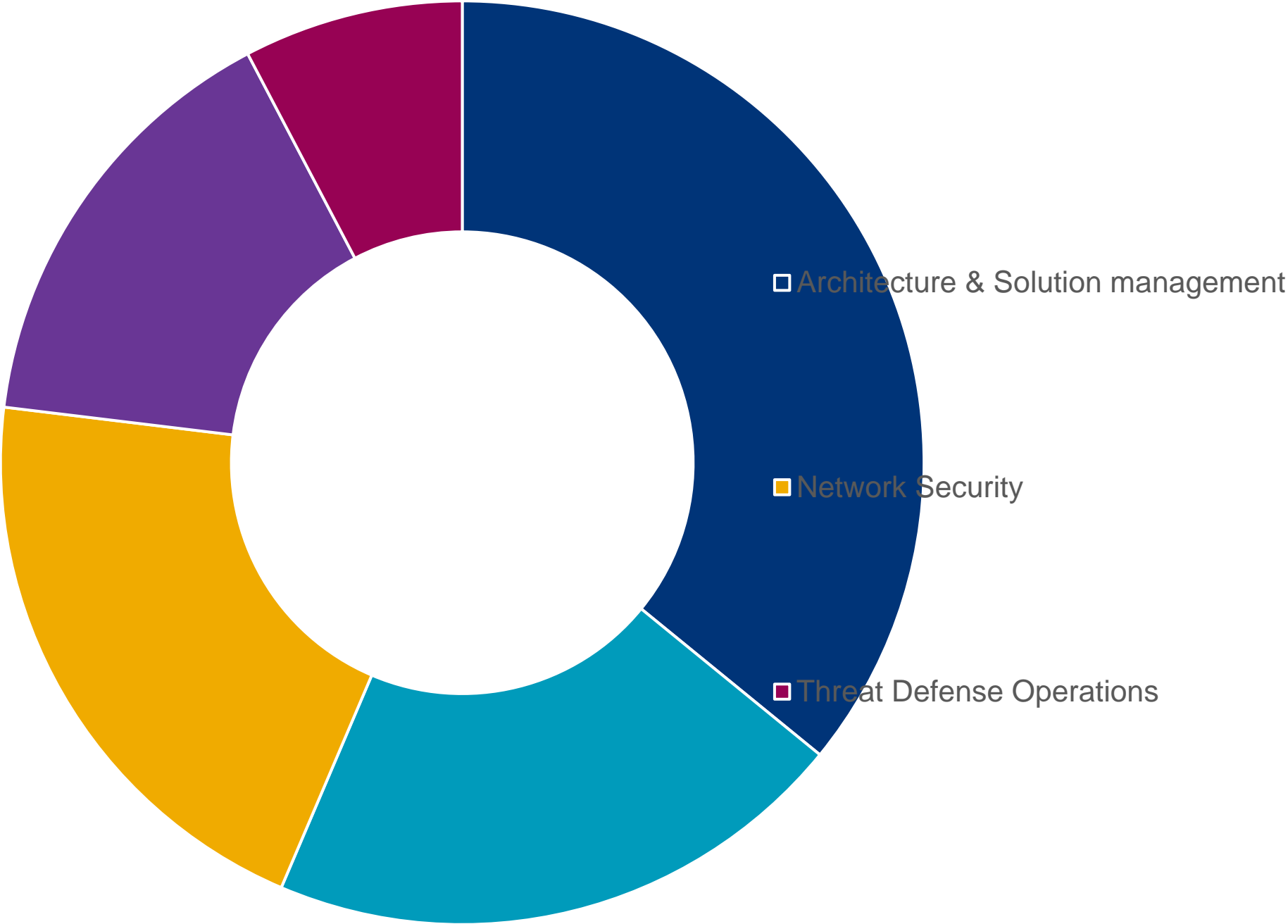
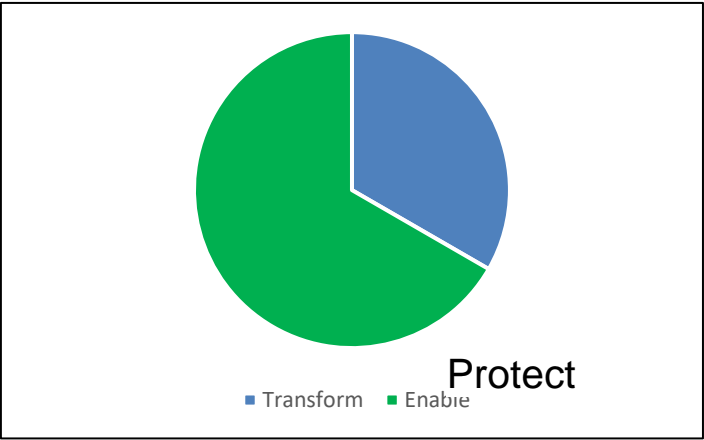
- Security validation (pen test, cyber exercises,..)
- Baseline checking (MSB,..)
- Risk assessments(Vendor, CROSS,Business risk,..)
- Security posture reporting
- Policies&standards maintenance
- Audit follow up
- Secuity management tools maintenance

Zoom on Business Support activity



- Business projects support
- Tribe support
- Cloud initiatives
- Audit/Control framework (ISO 27K, PCI DSS,eIDAS,..)

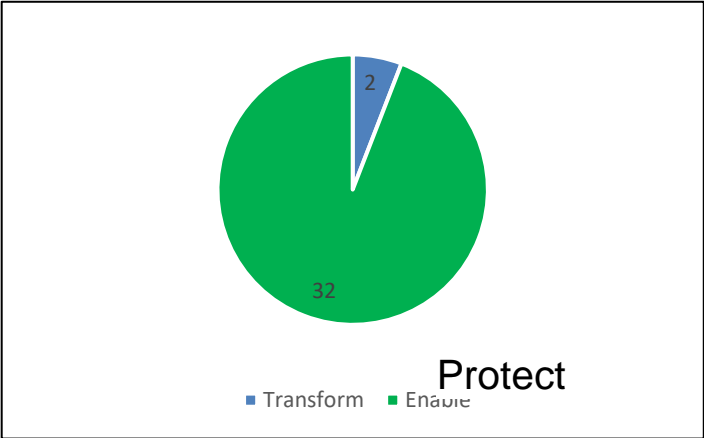
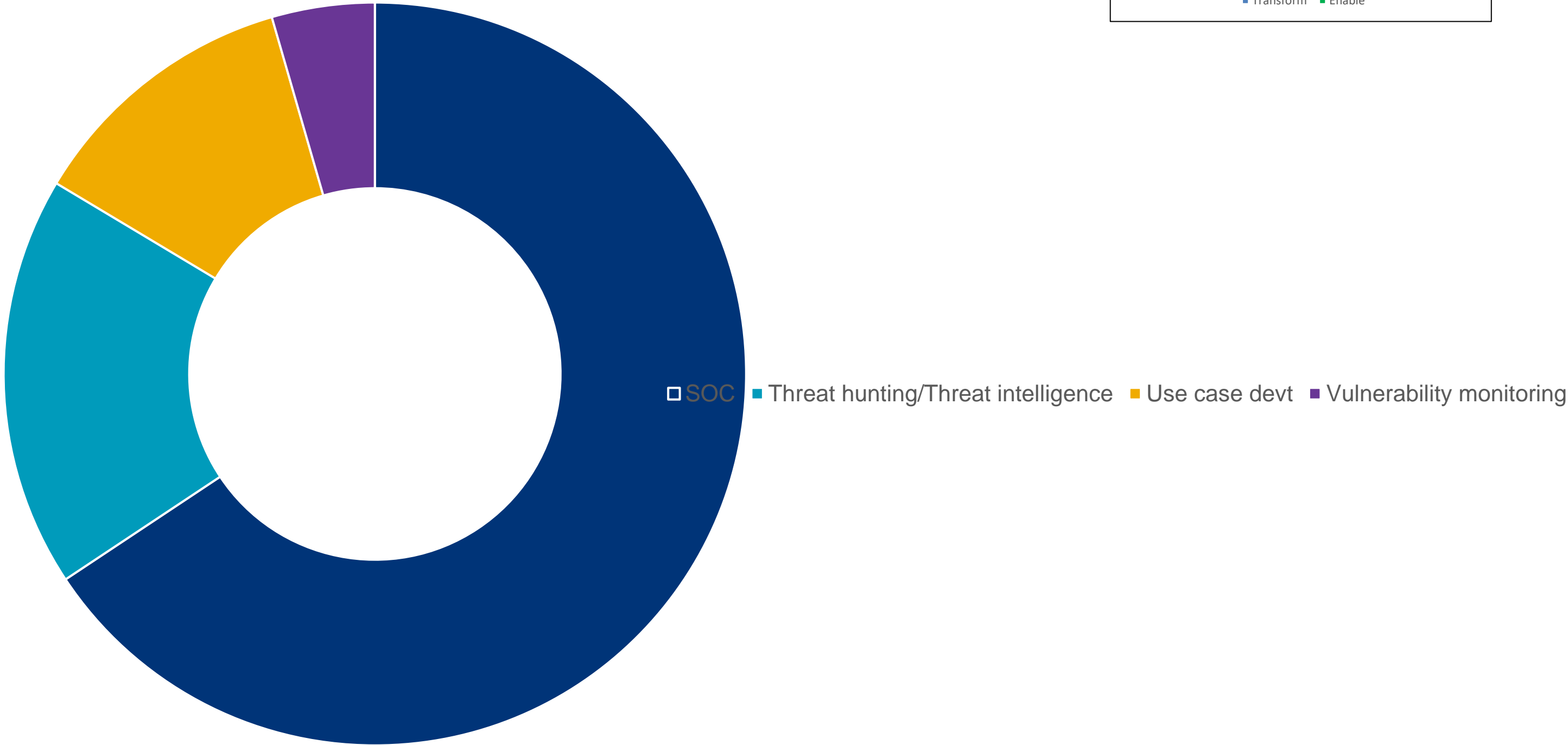
Zoom on Platform & Tooling security activity



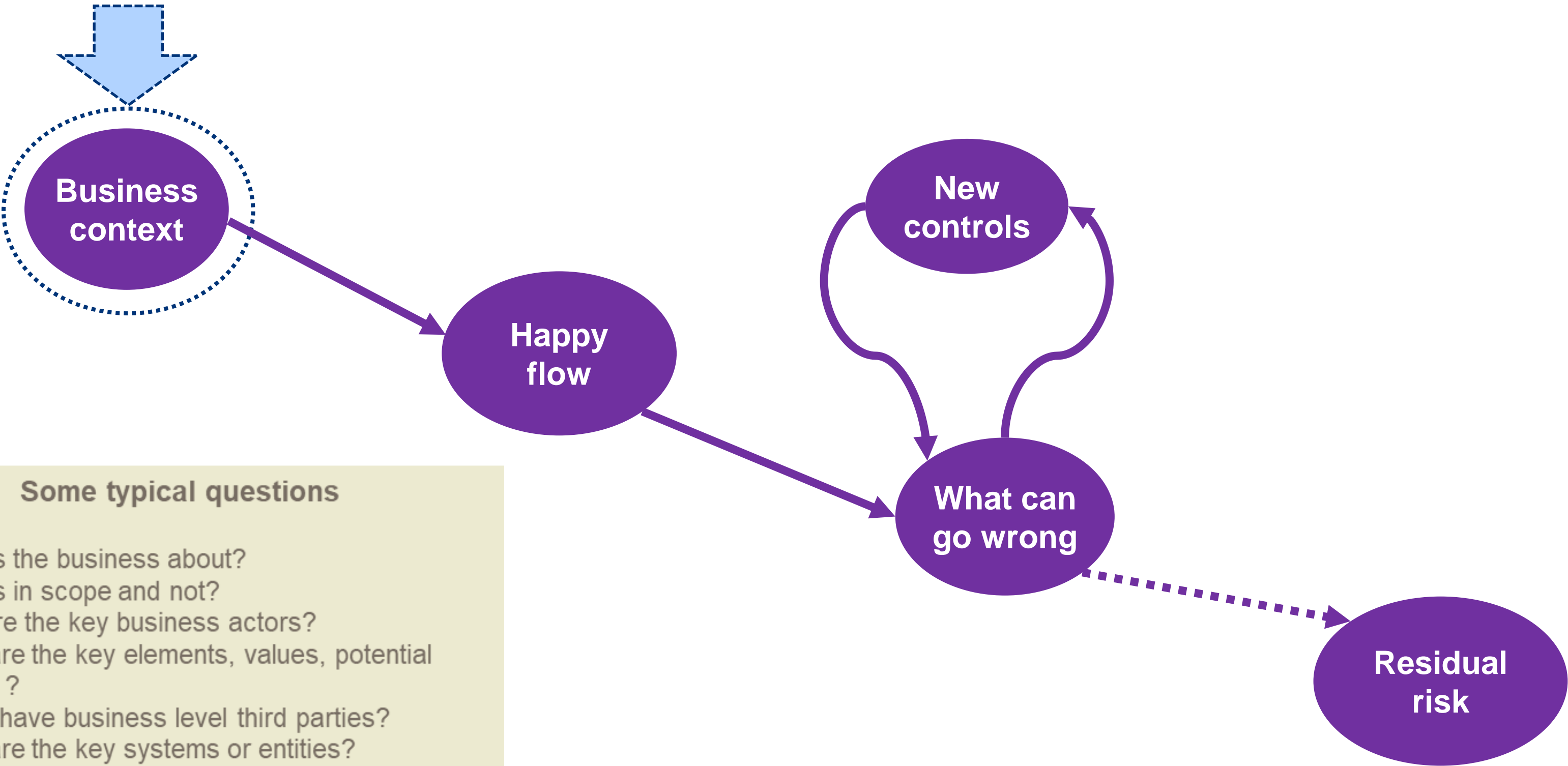
- Endpoint Security
- Security Logging & Automation



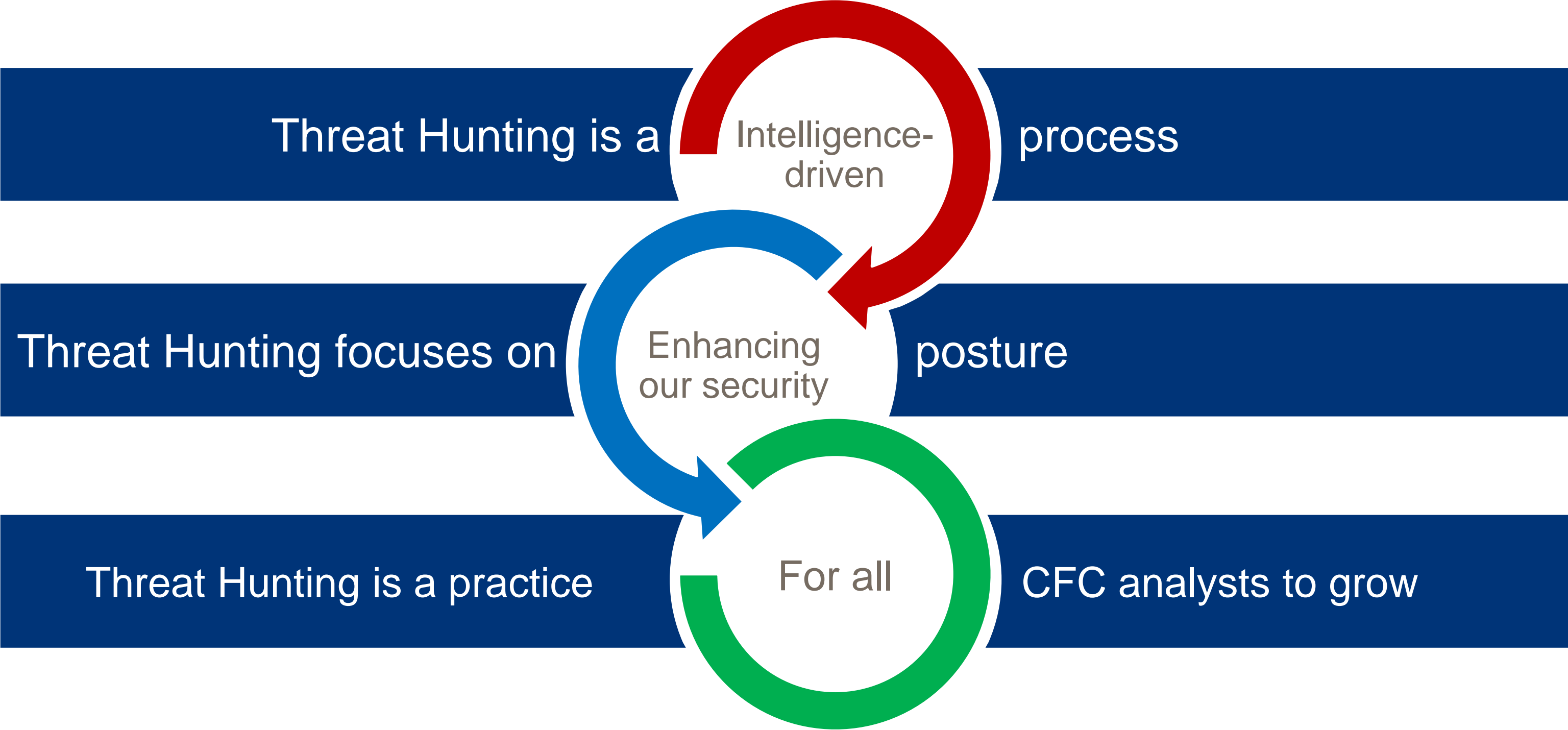
Zoom on Cyber Incident Detection & Response activity



Example: Business Security Assessment



Example: Threat Hunting



Example: Key competencies for all with learning maps tracking

3 Proficiency levels

4 Focus areas

Learning map	Basic	Intermediate	Advanced
Cloud Security			
SWIFT Business			
Agile			
Risk Management			

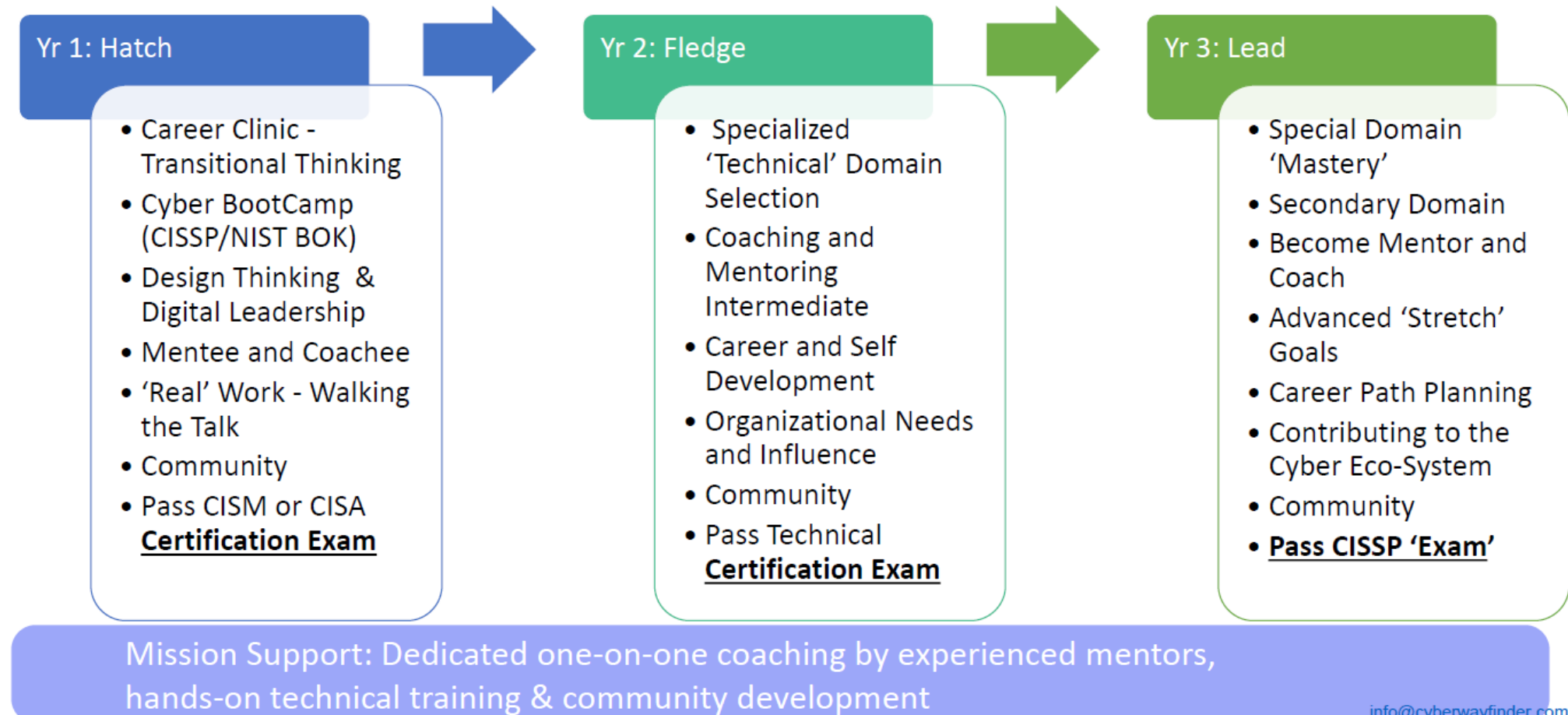
- Library
 - References to relevant documentation
- E-learning
 - References to platforms and courses name
- Classroom
 - References to vendors and courses name



Example: bringing diversity through “Women In Cyber” programme

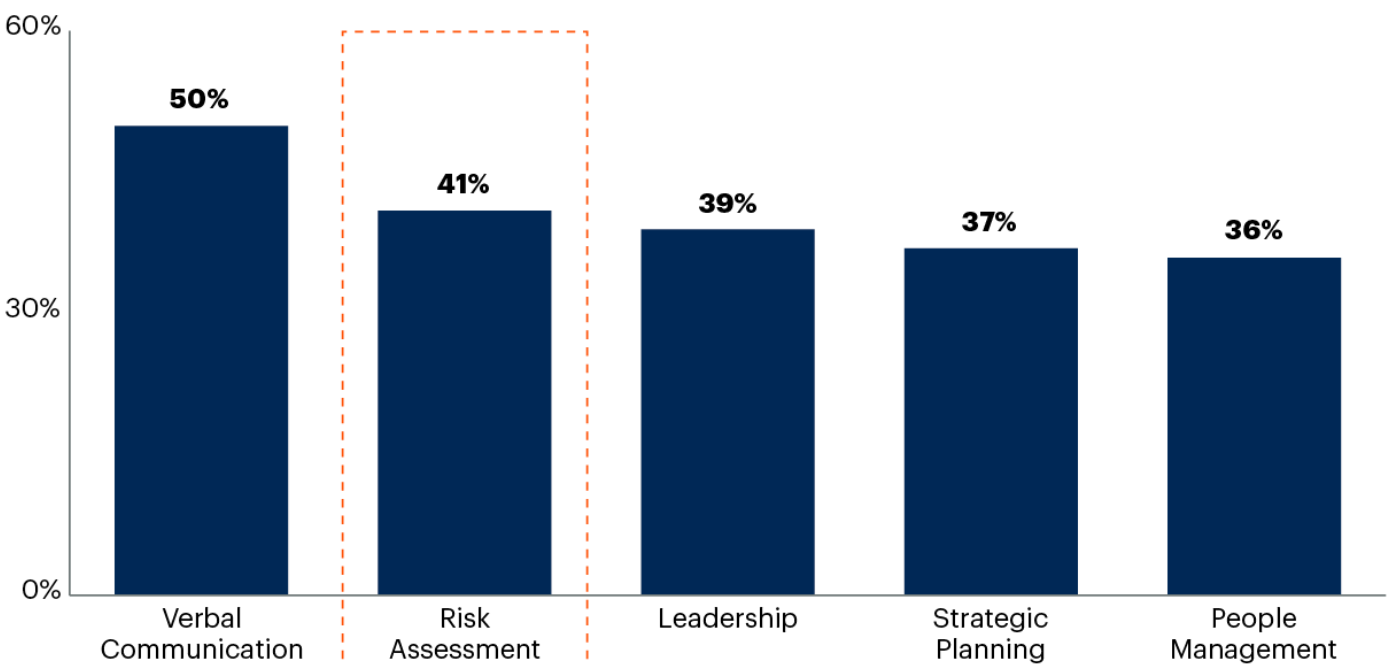
- **Hire women into existing cyber teams**
- Provide **academic and structured industry knowledge** via evening and weekend classes for **3 years** having them pass industry recognized certification exams
- Engage with **senior cyber security mentors**
- Challenge with **real-life and real-world problems in the workplace**

Timeline: Three Stages to **SUCCESS**



Let's not forget about leadership

Top Five Skills Hiring Organizations Seek
Percentage of Sample



n = 70
Source: Gartner
716225_C

MANAGEMENT PRINCIPLES

LEAD

- Set direction & drive for results
- Inspire your team to innovate & bring ideas
- Foster collaboration within & across groups
- Be a role model: Walk the talk

COMMUNICATE

- Listen
- Invite regular multidirectional feedback
- Share information
- Provide honest, constructive, & timely feedback

DEVELOP

- Develop your team & yourself
- Engage & empower diverse individuals
- Energize people to bring out their best
- Recognize & reward achievements

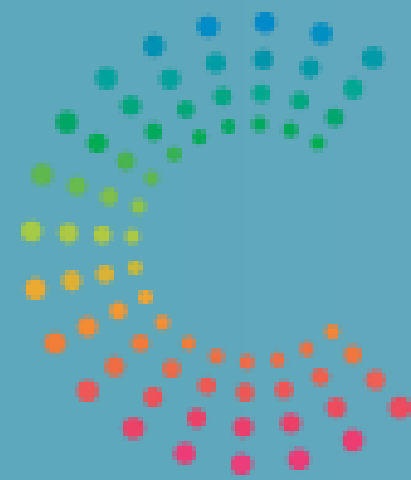
TRUST

- Act with integrity, respect, & fairness
- Show genuine interest in people
- Explain the rationale behind decisions





www.swift.com



CYBER SECURITY
COALITION.be

VIRTUAL GRC EXPERIENCE
SHARING EVENT
26 JANUARY 2021

CYBERSECURITY STEPS BASED ON THE NIST CYBERSECURITY FRAMEWORK

UMUT INETAS



Solvay Brussels School
Executive Education

AGENDA

- NIST Cyber Security Framework: History, Structure, Overview
- NIST CSF Implementation Tiers
- NIST CSF Profiles
- 5 Pillars of NIST Core Function
- Why NIST ?
- Other Frameworks and Future of NIST

ABOUT ME



UMUT INETAS

Current: Manager Security Architecture @Ahold Delhaize

S3 Cybersecurity Topic Leader @Solvay Business School - IT & Information Security Management Education

Previously: Head of CDC @ING BE

- Info Sec Team Manager
- Information Risk Manager
- IT Sec Architect
- IT Sec Engineering

Worked at Istanbul, Vienna, Moscow, Amsterdam and Brussels for different financial institutions

<https://be.linkedin.com/in/umutin>

NIST FRAMEWORK HISTORY

- Released in 2014
 - 2013 - Executive Order 13636: “Improving Critical Infrastructure security”
 - May 2017 - Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- Version 1.1 (April 2018)
 - A new section titled “Self-Assessing Cybersecurity Risk with the Framework.”
 - More detailed IAM and vulnerability management

“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”



Executive Order 13636
February 12, 2013

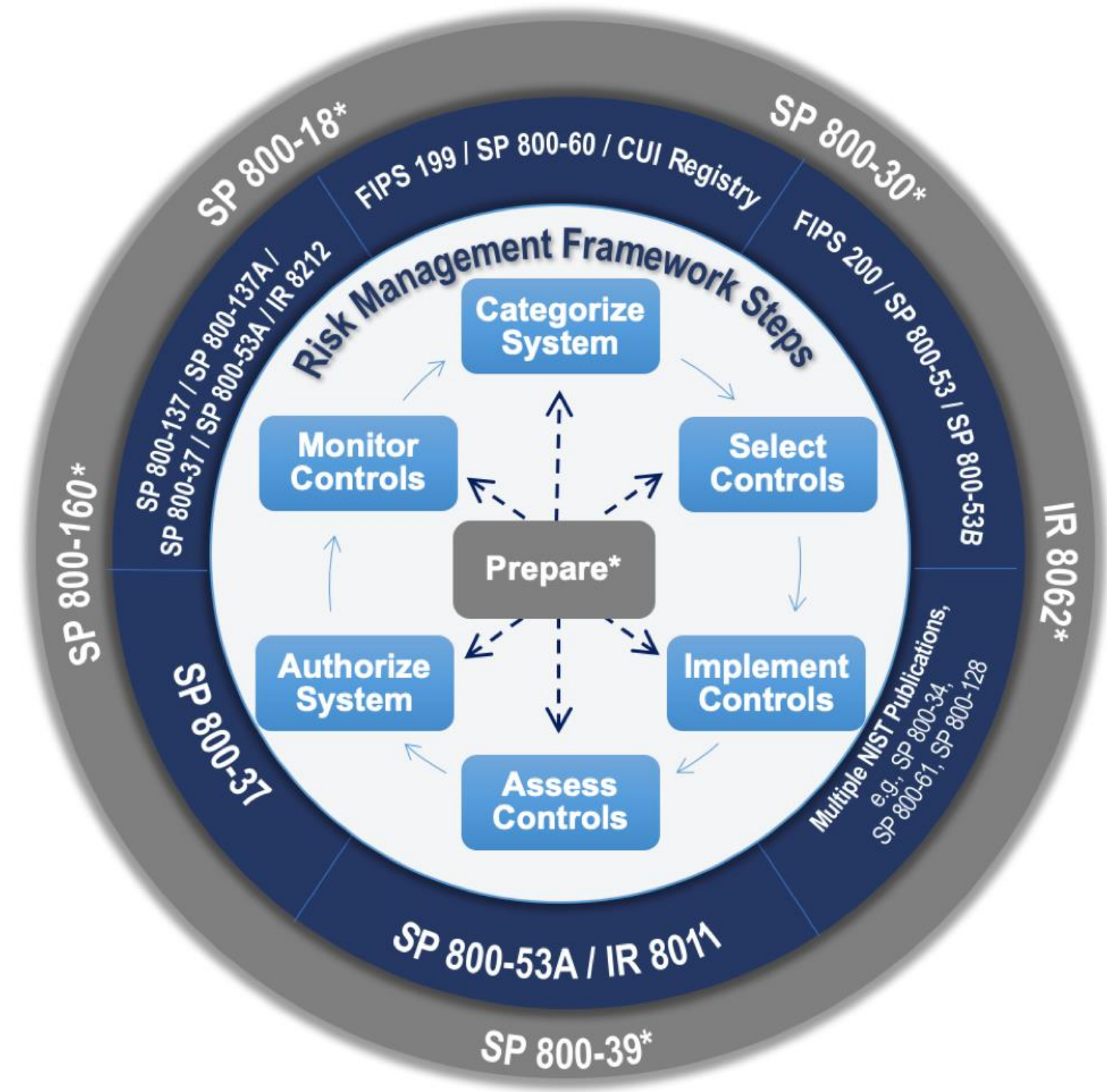
2

Source: crsr.nist.gov

- Cost effective, business centric, risk-based cybersecurity framework
- Attempt to help critical organizations defend against growing tide of cyber security attacks

NIST FRAMEWORK STRUCTURE

- A Framework of Frameworks
- Lots of Standards & Specifications
 - NIST SP 800-137 Information Security Continuous Monitoring (ISCM)
 - NIST SP 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
 - NIST SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government
 - NIST SP 1800-23 Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry
 - And many other...



Source: csrc.nist.gov

NIST FRAMEWORK OVERVIEW

3 MAIN COMPONENTS OF NIST CSF



IMPLEMENTATION TIERs

- Link to the risk management frameworks
- How cybersecurity risks and processes are viewed and measured

PROFILE

- Where you are and where you want to go
- Defines (measures) current state and projects (measures) desired state

CORE

- What NIST tries to achieve
- Alignment of cybersecurity strategy in a structured way and link to more detailed guidance and controls

NIST CSF – IMPLEMENTATION TIERS

IMPLEMENTATION TIERS

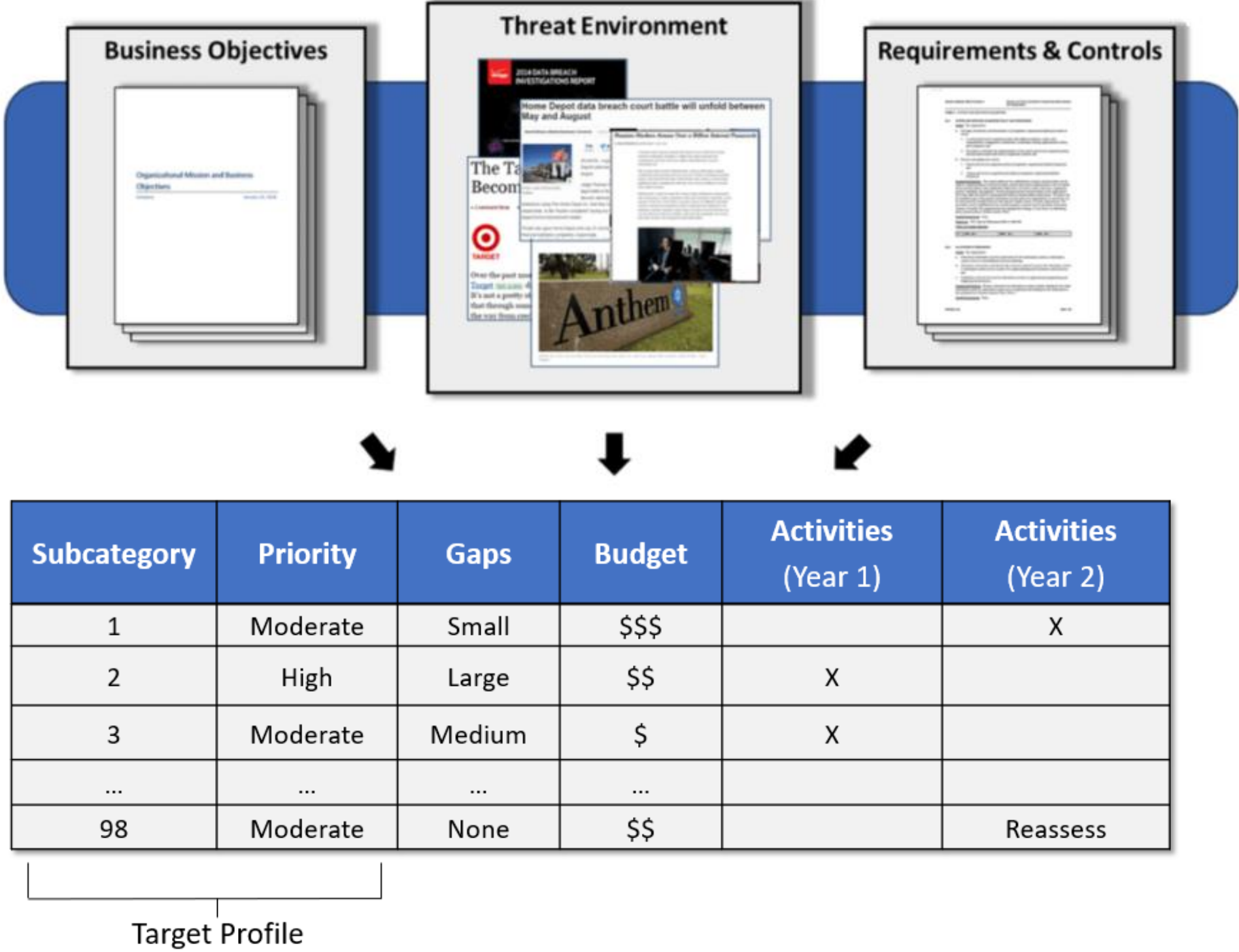
	1	2	3	4
	Partial	Risk Informed	Repeatable	Adaptive
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: <ul style="list-style-type: none">• monitors and manages supply chain risk^{1.1}• benefits my sharing or receiving information from outside parties			

- The degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined.
- Ranges from Partial (Tier 1) to Adaptive (Tier 4) to degree of rigor, and how well integrated cybersecurity risk decisions are into broader risk decisions
- 3rd party involvement which organization shares and receives cybersecurity info from external parties.

NIST CSF - PROFILES

CSF PROFILE

- Presents overview of present and future cybersecurity posture
 - Business Requirements
 - Risk Tolerance
 - Resources
- Used to define current state and desired state and measure progress



NIST CORE FUNCTIONS - IDENTIFY

IDENTIFY

Business goals

Who We Are

Vision Statement:
Become the leader in our market by enhancing the wonder, joy and happiness of our customers

Our Ability to Achieve These



Business risk focus information security

The Risks We Face

**If We Don't Manage These Risks
We Have a Problem**

- Loss of Intellectual Property
- Regulatory and Compliance
- Lack of Resiliency in Critical Systems
- Inability to Keep Up With Digital Business Projects
- Third-Party Risk
- Reputational Risk
- Emerging Technology Risk

Information security principles

How We Address Them



- Know your business
- Know your people, process and technology
- Link business goals to information security principles
- Build Information security strategy & roadmap
- Adapt the information security strategy to changing business environment

You can't protect what you don't know about. Know your assets.

NIST CORE FUNCTIONS - PROTECT

PROTECT

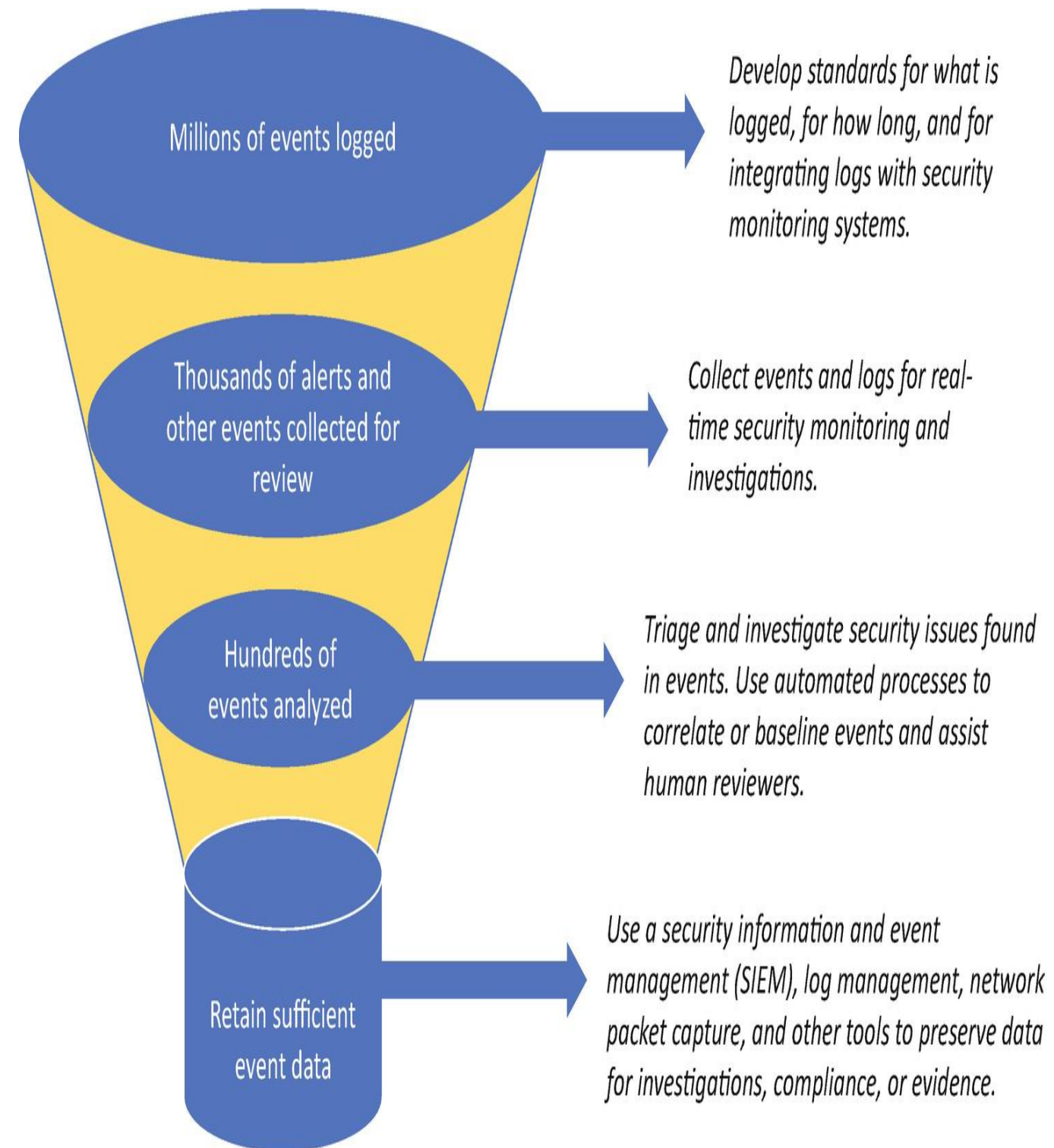
- Access control: Secure access for authorized users
- Awareness and Training: Awareness and training of the personnel against information security risks
- Data Security: Manage data with the business risk strategy and support the confidentiality and integrity of information while also ensuring its availability.
- Information Protection Processes and Procedures: Maintaining and leveraging security policies, processes and procedures



- Maintenance: Ensure that maintenance takes place in a structured manner
- Protective Technology: Technical security solutions with the documentation, implementation and review

NIST CORE FUNCTIONS - DETECT

DETECT



- Logging & Monitoring
- Anomaly Detection
- SIEM & UEBA
- Building a SOC
- Continuous Monitoring
- Threat Hunting

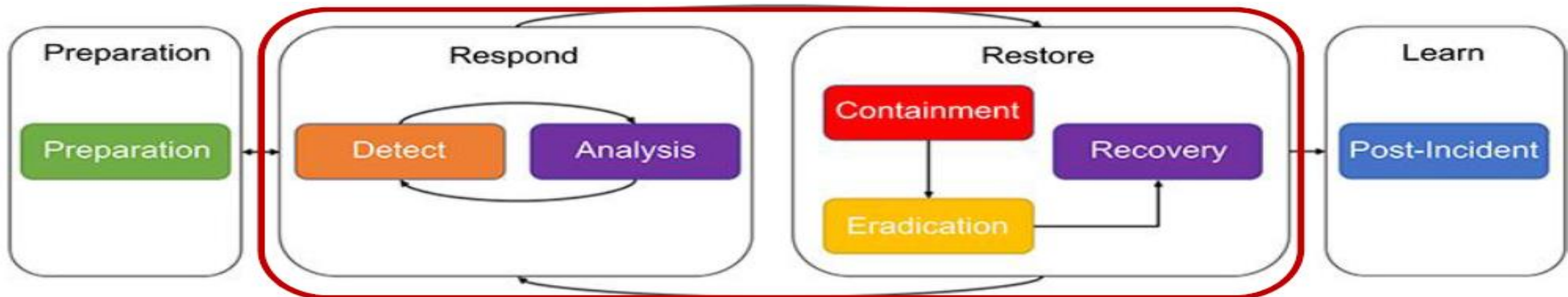


Figure 1. Building Blocks of a SOC

NIST CORE FUNCTIONS - RESPONSE

RESPONSE

- Response Planning: It is all about planning and preparedness
- Analysis: Examine and investigate detections to analyze the impact of the event, as well as the adequacy of the enterprise's response with forensics
- Mitigations: Contain the incident and mitigate the potential damage of the threat
- Communications : Coordination of internal and external stakeholders for response activities
- Improvements : The lessons learned from responding to the threat, and work to incorporate these findings into future response strategies



NIST CORE FUNCTIONS - RECOVER

RECOVERY

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

- Part of Business Continuity Planning
- Ultimate Goal: Timely recover to normal and minimize the business impact

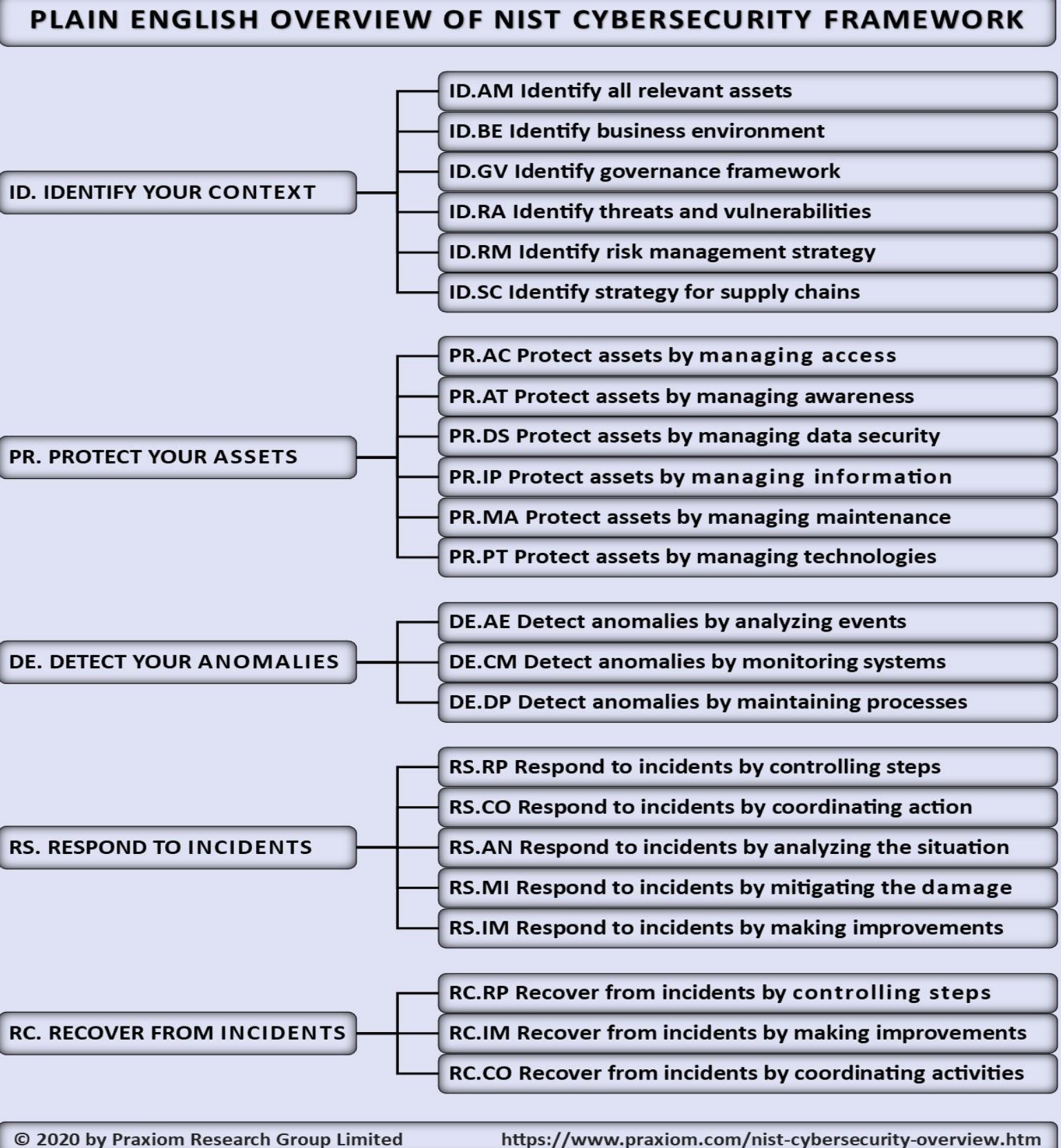
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	<ul style="list-style-type: none">- CCS CSC 8- COBIT 5 DSS02.05, DSS03.04- ISO/IEC 27001:2013 A.16.1.5- NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	<ul style="list-style-type: none">- COBIT 5 BAI05.07- ISA 62443-2-1 4.4.3.4- NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	<ul style="list-style-type: none">- COBIT 5 BAI07.08- NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	<ul style="list-style-type: none">- COBIT 5 EDM03.02
		RC.CO-2: Reputation after an event is repaired	<ul style="list-style-type: none">- COBIT 5 MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	<ul style="list-style-type: none">- NIST SP 800-53 Rev. 4 CP-2, IR-4

NIST CORE – MAPPING TO ACTIVITIES

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	COBIT 5 DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

<https://nist.gov/document/Framework-improving-critical-infrastructure-cybersecurity-corexlsx>



WHY NIST CSF ?

- Risk-based, common and accessible language
- Adaptable to many technologies, lifecycle phases and use cases in private sector, academia, public sector
- Right level of security for business needs with resource planning
- Measurement of cybersecurity effectiveness

COMMON PITFALLS OF NIST IMPLEMENTATION

- Lack of senior management alignment and support
- NIST Framework \neq Risk assessment & Audit Guideline
- Roles & Responsibilities (Cloud Service Providers or outsourcing in general)
- Wrongful assumptions and company culture

“The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes...”

“... NOT achieve every Core outcome but consider their business requirements and material risks, and then make reasonable and informed cybersecurity decisions using the Framework”

WHY NIST CSF ?

Works with other Frameworks

- Mappings of the NIST 800–53 to MITRE ATT&CK Techniques by MITRE Engenuity

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Control Integration	Account Manipulation	Abuse Remote Control Mechanism	Abuse Remote Control Mechanism	Brute Force	Account Discovery	Execution of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Exploit Public Facing Application	Exploitation of Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credential Theft	Application Window Discovery	Internal Spearphishing	Audio Capture	Communications Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Web Process Communication	Boot or Logon Assistant Execution	Boot or Logon Assistant Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Ingress
Hardware Additions	Native API	Boot or Logon Assistant Execution	Boot or Logon Assistant Execution	Direct Volume Access	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over Cloud Channel	Data Manipulation
Phishing	Scheduled Task/job	Browser Extensions	Event Triggered Execution	Guardrails	Input Capture	File and Directory Discovery	Remote Services	Data from Local System	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Registration Through Removable Media	Shared Modules	Clipboard Client Software Binary	Event Triggered Execution	Guardrails	Input Capture	Network Service Scanning	Real-time Through Removable Media	Data from Network Shared Drive	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Supply Chain Compromise	Software Deployment Tools	Create Account	Registration for Software Execution	Registration for Software Execution	Input Capture	Network Share Discovery	Software Deployment Tools	Data from Network Shared Drive	Failback Channels	Exfiltration Over Web Service	System Denial of Service
Trusted Relationship	System Services	Online or Ready System Access	Group Policy Modification	Group Policy Modification	Network Sniffing	Network Sniffing	Text Shared Content	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts	User Execution	Event Triggered Execution	Hijack Execution Flow	Group Policy Modification	On-Credential Dumping	File and Directory Discovery	Use Remote Authentication Protocol	Data Staged	Multi-Stage Channels		Initial System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection	Hide Artifacts	On-Credential Dumping	File and Directory Discovery		Email Collection	Non-Application Layer Protocol		Network Denial of Service
		Hijack Execution Flow	Scheduled Task/job	Hijack Execution Flow	On-Credential Dumping	File and Directory Discovery		Input Capture	Non-Standard Port		Resource Hijacking
		Pre-OS Boot	Valid Accounts	Impair Defenses	On-Credential Dumping	File and Directory Discovery		Man in the Browser	Protocol Tunneling		Service Stop
		Network Local		Remove Removal on Host (Initial)	Unsecured Credentials	Query Registry		Network Media	Proxy		System Shutdown/Reboot

<https://mitre-engenuity.org/blog/2020/12/15/ctid-releases-security-control-mappings-to-attck/>



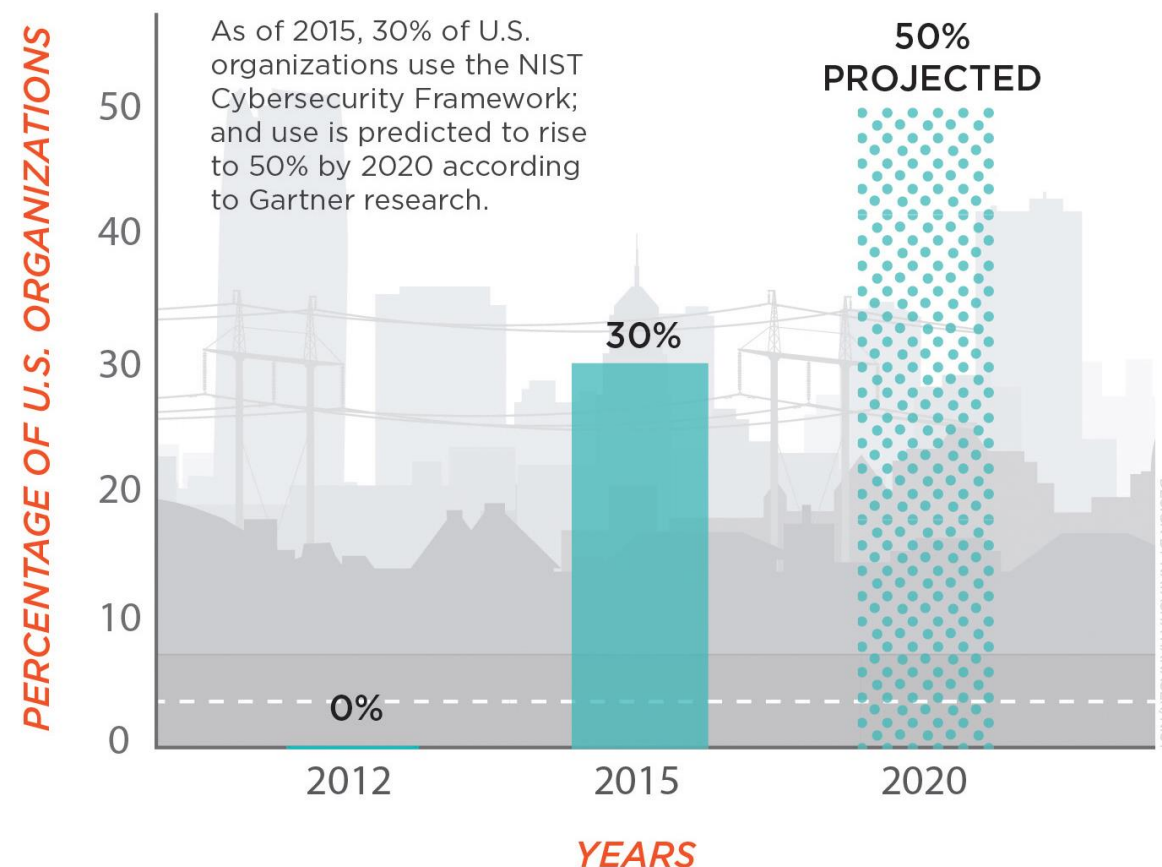
Function	Category	CIS Control
Identify	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management	CIS Control #1, 2 CIS Control #3
Protect	Identity Management and Access Control Awareness and Training Data Security Information Protection Processes & Procedures Maintenance Protective Technology	CIS Control #4, 9, 11, 12, 13, 14, 16 CIS Control #4, 17 CIS Control #1, 2, 13, 14, 18 CIS Control #3, 5, 7, 10, 11 CIS Control #4, 12 CIS Control #4, 6, 8, 11, 13, 14, 16
Detect	Anomalies and Events Security Continuous Monitoring Detection Processes	CIS Control #6, 9, 12, 19 CIS Control #3, 8, 19 CIS Control #6
Respond	Response Planning Communications Analysis Mitigation Improvements	CIS Control #19 CIS Control #19 CIS Control #3, 19 CIS Control #3, 19 CIS Control #19
Recover	Recovery Planning Improvements Communications	CIS Control #19 CIS Control #19 CIS Control #19

<https://www.cisecurity.org/white-papers/cis-controls-v7-1-mapping-to-nist-csf/>

FUTURE OF NIST CSF

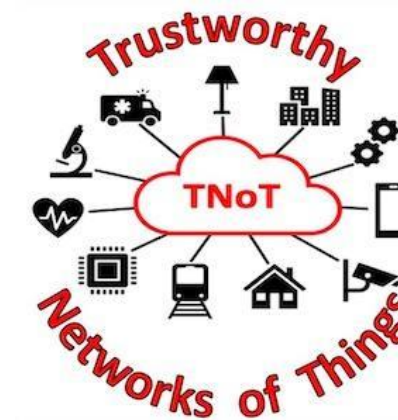
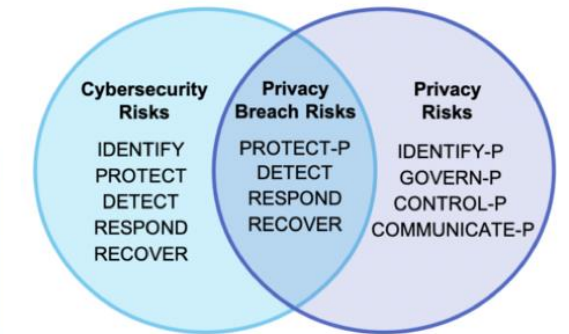
- NIST CSF is here to stay
- Becoming a standard for Cyber Security field
- More adaptations & versions

CYBERSECURITY FRAMEWORK USAGE



“16 Critical Infrastructure sectors and more than 20 States use the NIST Cybersecurity Framework”

<https://nist.gov/industry-impacts/cybersecurity-framework>





THANKS
DREAM. LEARN. LEAD.



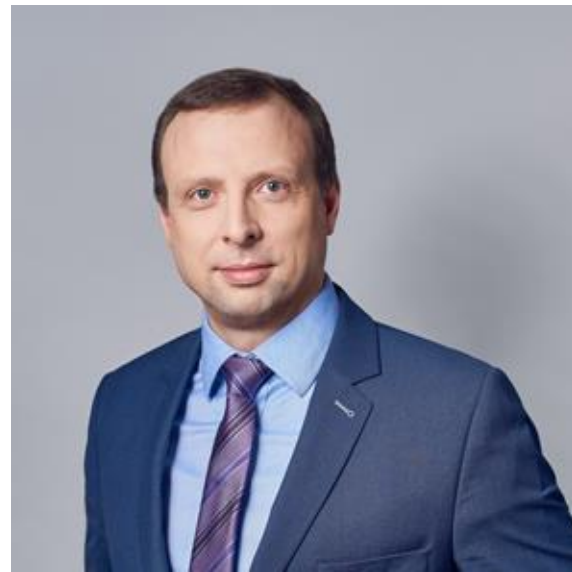
Solvay Brussels School
Economics & Management

Applied Cybersecurity Research from ISACA and FIRST.org

Vilius Benetis



ABOUT SPEAKER



DR. VILIUS BENETIS

**NRD Cyber Security
Director**

ABOUT DR. **VILIUS BENETIS**

Dr. Vilius Benetis specializes in security operations build-out:

- CSIRT/SOCs incident response capability establishment or modernization for nations, regions, sectors and organizations;
- Law enforcement e-crime optimization platforms and security automation.

Dr. Benetis is also a researcher and contributor to FIRST.Org's CSIRT Services Framework and CIS's Critical Security Controls. He advocates SIM3 and SOC-CMM models for CSIRT/SOC modernization and Oxford's CMM model for national cybersecurity capacity building.

Vilius Benetis graduated from Kaunas University of Technology (KTU), with BSc in Computer Science as well as MSc and PhD in Teletraffic Engineering from Danish Technical University, and currently serves as a cybersecurity industry professor at KTU.

AREAS OF EXPERTISE

- CSIRT/SOC establishment / modernization (LT, CY, BD, BT, ZA, EG, TZ, KE, PE, ..)
- Cybersecurity resilience and governance
- CII methodologies establishment

CREDENTIALS AND MEMBERSHIPS IN PROFESSIONAL ASSOCIATIONS

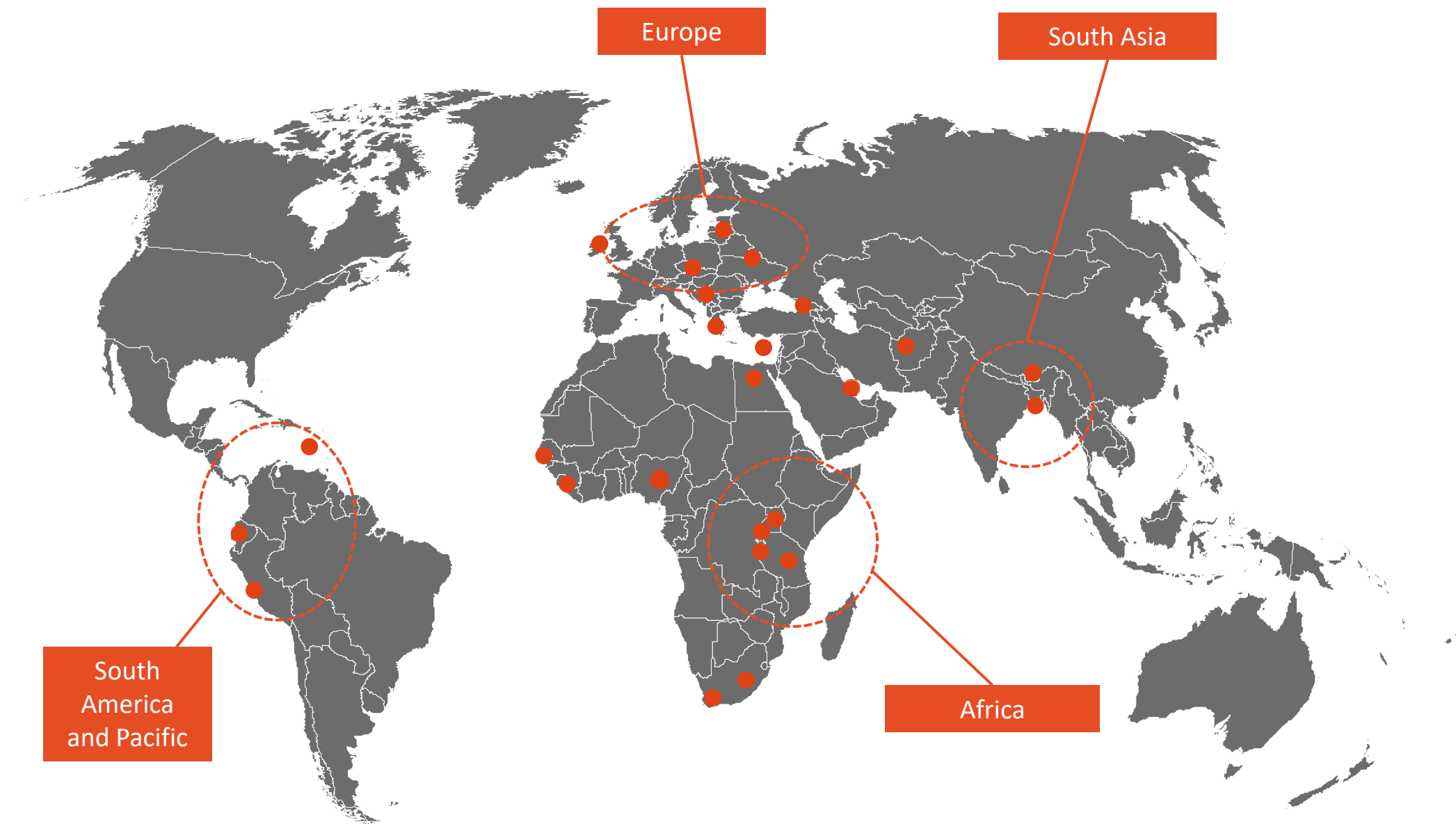
- CISA, CRISC, ..
- Chairman of ISACA Lithuania Chapter
- ITU-D SG2Q3, GFCE group B, CIS Controls

FOCUS: CSIRTs and SOCs

Cybersecurity operations build-out, incident detection and handling, establishment and support of Computer Security Incident Response Teams and cyber capacity enhancement at organizational and national levels

CUSTOMERS

Governments, public and private sector organizations



Today I will talk about:

ISACA's Cybersecurity Value Proposition

- ISACA's Governance and Audit Frameworks
- ISACA's Certifications and Certificates
- CSX Certificates
- Technical enablement Courses
- Cybersecurity Enterprise Solutions (CMMI)

FIRST.org' and friends value proposition:

- As home of CVSS, TLP, CSIRT framework
- Value of CSIRTs and SOCs
- CSIRT and SOCs Buildout Guidance


ISACA's Cybersecurity Value Proposition

ISACA's Governance and Audit Frameworks

AUDIT PROGRAMS AND TOOLS

Results 1-16 of 61

RELEVANCY DATE




Audit Program

VMware Server Virtualization Audit Program

Objective—The VMware server virtualization audit review will provide management with an independent assessment of the...

FREE to ISACA Members
Not a Member? Join Now




Audit Program

UNIX/LINUX Operating System Security Audit Program

Objective—The objective of the UNIX/LINUX Audit program is to provide management with an independent assessment relating...

FREE to ISACA Members
Not a Member? Join Now




Audit Program

Microsoft SQL Server Database Audit Program

The Microsoft® SQL Server® Database Audit Program is designed to provide a relatively complete guide to the audit of SQ...

FREE to ISACA Members
Not a Member? Join Now




Audit Program

IPv6 Security Audit Program

The major objectives of the IPv6 networking audit review are to: Provide management with an independent assessment of the...

FREE to ISACA Members
Not a Member? Join Now




Audit Program

Microsoft Internet Information Services (IIS) 7 Web Services Server Audit...

Objective—The Microsoft IIS 7.x Audit review provides management with an independent assessment of the effectiveness...

FREE to ISACA Members
Not a Member? Join Now




Audit Program

Microsoft SQL Server 2016 Audit Program

With GDPR and data privacy initiatives currently the focus of many enterprises, now might be a good time to take a new look at...

FREE to ISACA Members
Not a Member? Join Now




Audit Program

Microsoft Windows File Server Audit Program

The File Server Audit review provides management with an independent assessment of the effectiveness of the configuratio...

FREE to ISACA Members
Not a Member? Join Now



Audit Program

HIPAA Audit Program

The Health Insurance Portability and Accountability Act (HIPAA) was created to provide privacy and security for protected health...

FREE to ISACA Members
Not a Member? Join Now




Audit Program

Voice Over Internet Protocol (VoIP) Audit Program

A typical VoIP network comprises a complex series of cooperating protocols, networks (wireless and wired), servers, security...

FREE to ISACA Members
Not a Member? Join Now




Audit Program

Microsoft SharePoint 2010 Audit Program

SharePoint is a group of Microsoft architectures with a common purpose—to provide sharing and retention of data in various forms...

FREE to ISACA Members
Not a Member? Join Now




Audit Program

Microsoft Exchange Server 2010 Audit Program

Exchange Server 2010 is comprised of a series of cooperating processes that communicate with one another o...

FREE to ISACA Members
Not a Member? Join Now




Audit Program

Lotus Domino Server Audit Program

Domino server comprises a series of cooperating processes that communicate with one another on multiple servers and connect to...


FREE to ISACA Members
Not a Member? Join Now



Book

COBIT Focus Area: Information Security


COBIT Focus Area: Information Security provides guidance related to information security and how to apply COBIT to specific...



Book

ITAF, 4th Edition


Get the guidance and techniques that will lend consistency and effectiveness to your audits. The new 4th edition of ITAF outlines...



Book

ITAF™ Companion Performance Guidelines 2208

ISACA created the Information Technology Audit Sampling guidelines (Guidelines 2208) as a companion to its Information...




Book

Risk IT Framework, 2nd Edition

The Risk IT Framework is designed to assist in developing, implementing or enhancing the practice of risk management by...

18 June 2020



Audit Program

Azure Audit Program


In a cloud provider market comprised of solid frontrunners such as Amazon Web Services (AWS) and Microsoft Azure...



Audit Program

California Consumer Privacy Act (CCPA) Audit Program

One of the challenges that auditors face with compliance initiatives is providing assurance as expectations change. Data...




Audit Program

Amazon Web Services (AWS) Audit Program

The primary purpose of the Amazon Web Services (AWS) Audit Program is to provide a means for organizations to...

FREE to ISACA Members
Not a Member? Join Now



ISACA's Cybersecurity Value Proposition

- Certifications:



- Certificates:



ISACA's Cybersecurity Value Proposition

Certificate:

Proof of passing though cybersecurity technical practice.



Obtain a globally acknowledged credential from ISACA's Cybersecurity Nexus (CSX)

Affirm your cyber knowledge and real-world cybersecurity skills. Learn about both training and exam options below.



Certificate
CSX Advanced Exploitation Certificate

Prove that you have the skills to crack the hardest systems.



Certificate
CSX Advanced Forensics Certificate

Prove you have the skills and techniques to accomplish advanced forensics tasks.



Certificate
CSX Forensics Analysis Certificate

Affirm your skills in forensic documentation and data recovery methods.



Certificate
CSX Cybersecurity Fundamentals Certificate

Show You Know Cybersecurity's Concepts, Principles and Language



Certificate
CSX Linux Application and Configuration Certificate

Demonstrate your mastery in Linux operating systems, commands and capabilities.



Certificate
CSX Network Application and Configuration Certificate

Prove your understanding of network establishment and configuration.



Certificate
CSX Packet Analysis Certificate

Confirm your skills and understanding in packet and protocol analysis.



Certificate
CSX Penetration Testing Overview Certificate

Demonstrate your ability to conduct a penetration test.



Certificate
CSX Technical Foundations Certificate

Pass the CSX Packet Analysis, CSX Linux Application and Configuration and CSX Network...



Certificate
CSX Vulnerability and Exploitation Certificate

Prove you can exploit vulnerabilities and gain access to key systems.

ISACA's Cybersecurity Value Proposition

CSX cybersecurity online technical enablement courses

Bundle: CSX Technical Foundations Course Series

Contains three courses covering packet analysis, Linux, and network application. Certificate exams sold separately.

BEGINNER

ALL DOMAINS

CLICK FOR DETAILS

Bundle: CDPSE Hands-On Privacy Lab Package

Enhance your in-demand privacy skills and earn CPEs with ISACA's Technical Privacy Hands-on training bundle.

MULTILEVEL

ALL DOMAINS

CLICK FOR DETAILS

Bundle: CSX Emerging Technology Specialist Pathway

Covering blockchain basics as well as the topics of the Internet of Things (IoT) and prevalent attacks.

MULTILEVEL

ALL DOMAINS

CLICK FOR DETAILS

Bundle: CSX Forensic Examiner Pathway

Students will gain an understanding of forensic documentation and data recovery methods.

MULTILEVEL

ALL DOMAINS

CLICK FOR DETAILS

Bundle: CSX Linux System Administrator Pathway

Students get an understanding of Linux operating systems, commands, and capabilities.

MULTILEVEL

ALL DOMAINS

CLICK FOR DETAILS

Bundle: CSX Penetration Testing Overview

An hands-on introduction to penetration testing.

BEGINNER

DETECT

CLICK FOR DETAILS

Bundle: CSX Web Application Security Engineer Pathway

OWASP gives students an understanding on how each of these vulnerabilities that puts organizations at risk.

MULTILEVEL

ALL DOMAINS

CLICK FOR DETAILS

CSX Advanced Forensics Course

Learn advanced forensics techniques.

ADVANCED

RESPOND

CLICK FOR DETAILS

CSX Blockchain Basics Course

Learn how to practically apply blockchain basics.

ADVANCED

PROTECT

CLICK FOR DETAILS

CSX Cybersecurity Analyst Pathway

Learn to track and hunt cyber threats through cybersecurity forensics and threat hunting.

MULTILEVEL

ALL DOMAINS

CLICK FOR DETAILS

CSX Cybersecurity Hands-On Basics Labs

Apply fundamental cybersecurity concepts in a live environment.

BEGINNER

ALL DOMAINS

CLICK FOR DETAILS

CSX Cybersecurity Specialist Pathway

Enhance your cybersecurity foundational skill set to prepare for a specialized career in cybersecurity.

MULTILEVEL

ALL DOMAINS

CLICK FOR DETAILS

CSX Immersion: The OWASP Top 10

Train and sharpen your skills related to the OWASP Top 10 web application security vulnerabilities.

MULTILEVEL

ALL DOMAINS

CLICK FOR DETAILS

CSX Linux Application and Configuration

Learn Linux commands, create objects, and establish network connections.

BEGINNER

IDENTIFY

CLICK FOR DETAILS

CSX Network Application and Configuration

Establish and secure networks from scratch.

BEGINNER

PROTECT

CLICK FOR DETAILS

CSX Packet Analysis Course

Leverage packets to characterize networks, devices, and people.

BEGINNER

IDENTIFY

CLICK FOR DETAILS

CSX Penetration & Vulnerability Tester Pathway

Learn, test, and earn three of ISACA's most prestigious certificates in less than 6 months.

MULTILEVEL

ALL DOMAINS

CLICK FOR DETAILS

CSX Technical Foundations Certificate Package

Earn certificates in packet analysis, Linux, and network application. Includes 3 courses and 3 certificate exams.

BEGINNER

ALL DOMAINS

CLICK FOR DETAILS

CSX Threat Hunting

Learn to identify threats before they impact your system.

ADVANCED

DETECT

CLICK FOR DETAILS

CSX Vulnerability and Exploitation Course

Learn how to gain access and maintain access to a system.

INTERMEDIATE

DETECT

CLICK FOR DETAILS

ISACA's Cybersecurity Value Proposition

Cybersecurity Enterprise Solutions



Limited Time Offer

**SAVE
10%**

Enterprise Cybermaturity

Purchase ISACA's CMMI Cybermaturity Platform by 31 March 2021: Receive 10% off your full-year subscription—including implementation, set up and full tech support.*

ISACA's CMMI® Cybermaturity Platform

Cybersecurity is High Stakes from Wall Street to C-Suite: Avoid Catastrophic Business Disruption and Reputational Damage

Mitigate enterprise cybersecurity threats with a risk-based approach. Use our globally-accepted industry standards to strategically measure, assess and report on the capabilities of your cyber controls. CISOs, CIOs and boards can confidently lead cybersecurity initiatives to build cyber resilience for the threats most relevant to your organization.

Solves for Your Biggest Enterprise Cybersecurity Challenges

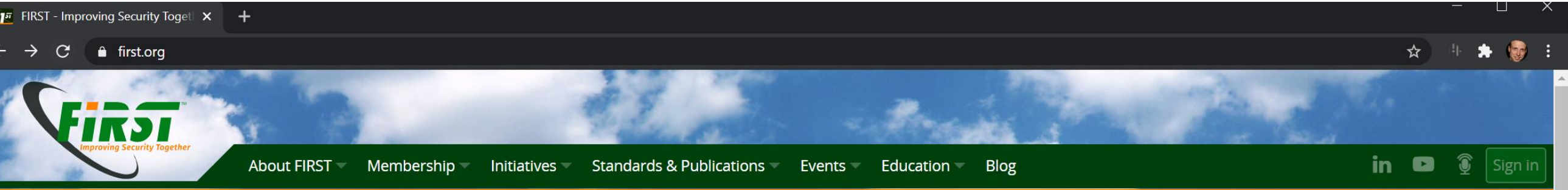
- **Compliance Alignment** – demonstrate compliance alignment to leading security frameworks and standards including NIST CSF, NIST 800-171, FFIEC, CMMC, and the Threat Kill Cycle.
- **Calibrated Maturity** – use globally recognized CMMI methodology and industry standards to quantify risks. Demonstrate standardized maturity, framework alignment, track progress towards cybersecurity goals.
- **Scalable Continuity** – perform continuous assessments across individual business units, with unlimited users and automatic updates.
- **Roadmap Prioritization** – leverage a risk-prioritized roadmap for remediation and risk mitigation, develop evidence-based board-ready reporting, and allocate budget and resources to close

[Learn More](#)

[Schedule a Demo](#)

*Limited-time offer for new ISACA CMMI Cybermaturity Platform customers only. Cannot be combined with any other offers. Subject to change at any time.

FIRST.org Value Proposition: Knowledge and working groups



Current FIRST SIGs
Academic Security SIG Space for discussion in order to reflect on our collective experiences, focus on current challenges and envision strategies on how we could work together to improve security in academic environments.
Big Data SIG Incident Detection and Response at Scale.
CSIRT Framework Development SIG The SIG will seek to involve experts interested in that work and provide a community to discuss improvements in need, existing gaps and (potential) new developments.
CVSS SIG: Common Vulnerability Scoring System For a global approach towards scoring metrics for vulnerabilities.
Cyber Insurance SIG To coordinate cyber insurance actuarial and modelling work with professional incident response and digital forensic teams.
Cyber Threat Intelligence SIG To define Threat Intelligence in the commercial space.

Events at spotlight

FIRST is the global Forum of Incident Response and Security Teams

FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

- Apart from the trust network that FIRST forms in the global incident response community, FIRST also provides value added services. Some of these are:
- access to up-to-date [best practice documents](#)
 - [technical colloquia](#) for security experts
 - hands-on classes
 - [annual incident response conference](#)
 - [publications and web services](#)
 - [special interest groups](#)
- Currently FIRST has [more than 500 members](#), spread over Africa, the Americas, Asia, Europe and Oceania.

What's New

Preparing for Post-Intrusion Ransomware

This evolving and brutally effective threat can have a significant impact on an organization's resources, finances, and reputation, but it can be stopped

(Mon, 11 Jan 2021 17:00 +0000)

Using similarity to expand context and map out threat campaigns

Cyber Threat Intelligence (CTI) practitioners can gain insight into adversary operations by tracking conflicts or geopolitical tensions. Similar to a "follow the money" approach in criminal investigations, looking at conflict zones can reveal cyber capabilities deployed as part of events —either by the parties to the conflict itself, or third parties interested in monitoring events for their own purposes.

(Mon, 04 Jan 2021 17:00 +0000)

Forecasting: All for One and One for All in Cybersecurity

(Mon, 21 Dec 2020 17:00 +0000)







What is FIRST to you?


DNS Abuse SIG Understanding the international customary norms applicable for detecting and mitigating DNS abuse from the perspective of the global incident response community is critical for the open Internet's stability, security and resiliency.	Metrics SIG To improve CSIRT incident management practices within the FIRST community.
Ethics SIG The Ethics SIG seeks to further the professionalization of the FIRST Community and improve the global understanding of SIRTs through the development of an ethical code for FIRST Members.	Passive DNS Exchange Develops and maintains a standard for exchanging passive DNS information between organizations.
Exploit Prediction Scoring System (EPSS) The Exploit Prediction Scoring System (EPSS) is an open, data-driven effort for predicting when software vulnerabilities will be exploited.	PSIRT SIG Drive the evolution of PSIRT practices by developing and maturing product response.
ICS SIG: Industrial Control Systems In ICS-SIG we bring together expertise from several sectors to create processes, best practices and incident response support recommendations and package useful open source tools for the ICS environments.	Red Team SIG The Red Team SIG provides a forum for practitioners to discuss the state of the art for tools, technologies, processes and methodologies for red team activities and to share experiences and best practices.
IEP SIG: Information Exchange Policy The initial goals of this SIG are to collaboratively develop an extensible framework for defining information exchange policy and a set of standard definitions for most common aspects.	Security Lounge SIG Designs, develops, and conducts security challenge and competition exercises for the FIRST.org community.
Information Sharing SIG The core mission is to support existing and new FIRST members to practice information sharing and acquire feedback from the members to improve the information sharing practices.	TLP SIG: Traffic Light Protocol The TLP SIG governs the standard definition of TLP for the benefit of the worldwide CSIRT community and its operational partners.
Malware Analysis This SIG will advocate and promote the sharing of malware analysis tools and techniques to enable CSIRTs to combat and analyze malicious code.	Vulnerability Coordination SIG Develop and execute a strategy for improving vulnerability coordination globally.
	Vulnerability Reporting and Data Exchange SIG Primarily chartered to research and recommend ways to identify and exchange vulnerability information across disparate vulnerability databases.

FIRST.org Value Proposition: Membership of CSIRTs/SOCs/ISACs/..


FIRST Members around the world


country:BE
There are 6 Teams in 553 for your query.

Team	Official Team Name	Country
BELNET CERT	BELNET CERT	 BE
CERT.be	Belgian Federal Cyber Emergency Team	 BE
KBC Group CERT	KBC Group CERT	 BE
NCIRC CC	NATO Computer Incident Response Capability - Coordination Center	 BE
NVISO CSIRT	NVISO CSIRT	 BE
PXS-CSIRT	Proximus Cyber Security Incident Response Team	 BE




TF-CSIRT
Trusted Introducer

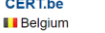



BELNET CERT
 Belgium

Last updated on 04 Oct 2020




Accredited
since 14 Sep 2004





CERT.be
 Belgium

Last updated on 12 Oct 2020




Accredited
since 22 Jan 2010





EATM-CERT
 Belgium

Last updated on 07 Dec 2020




Accredited
since 19 Mar 2020





KBC Group CERT
 Belgium

Last updated on 04 Jan 2021




Accredited
since 22 Feb 2016

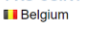



NVISO-CSIRT
 Belgium

Last updated on 18 Dec 2020




Accredited
since 09 Apr 2018

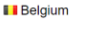



PXS-CSIRT
 Belgium

Last updated on 12 Jan 2021



Certified
since 08 Jul 2016



Xameco-CSIRT
 Belgium

Last updated on 06 Jan 2021

Listed
since 22 Mar 2018

Who should have CSIRT/SOC?



When organization is substantially digital, i.e.:

1. Processes a lot of data
Especially sensitive: personal, financial, etc.
2. Automates processes heavily
3. Is part of critical infrastructure
4. Is highly susceptible to the cyber threats

Defining CSIRT/SOC/CERT/ISAC/

IT Security Teams mature into:

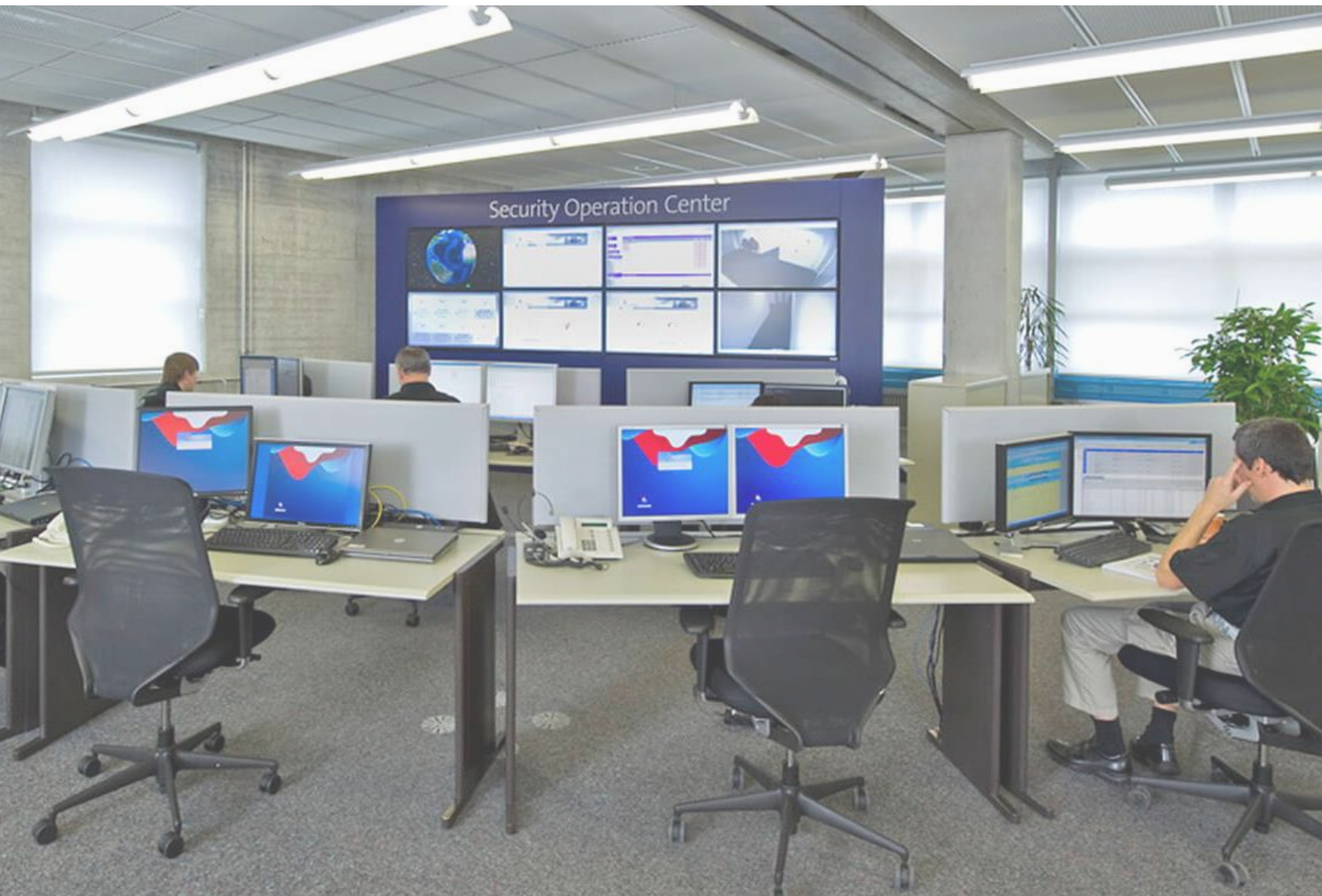
Computer Security Incident Response Teams (CSIRT), is (almost) synonymous to:



Security Operations Center (SOC, Global SOC, Joint Operation Center) is:

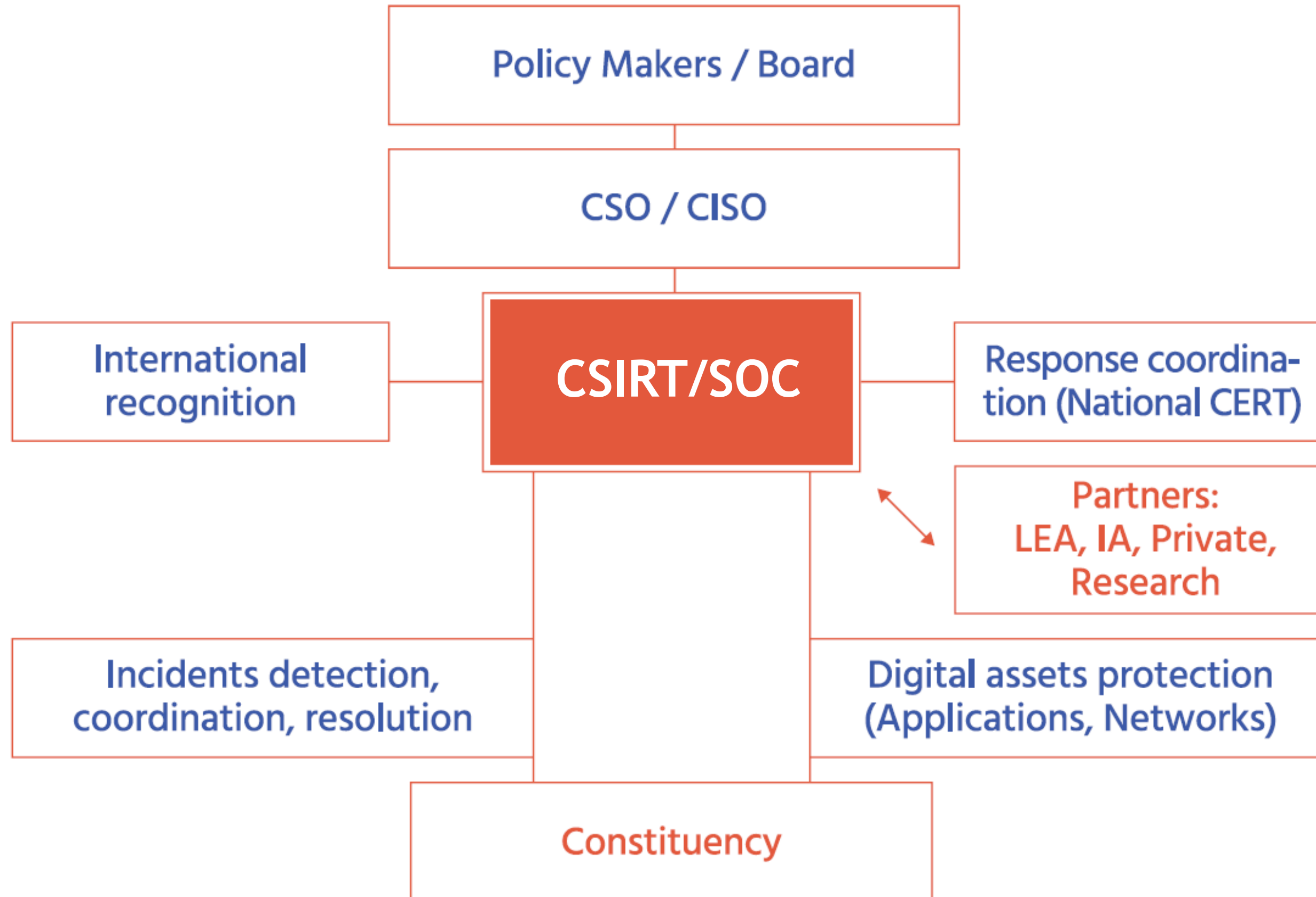
A partial operations of CSIRT model, primarily focused on internal monitoring, detection and triage

True needs for CSIRT/SOC



1. When attack hits:
is there a skilled team ready to respond and handle cyber-incidents using well known and internationally accepted Incident Response method?
2. Cyber crime is international:
is your team trusted by international community to provide support during your investigations?

CSIRT/SOCs model



FIRST.org Services Model Framework



Services typical sets

CSIRT



SOC



Different CSIRT/SOC stacks

	Mini	Basic	Effective	Full Scale
Governance 	<ul style="list-style-type: none"> • Mandate definition • FIRST.org membership • Roadmap & Strategy 	<ul style="list-style-type: none"> • Mandate definition • FIRST.org membership • Roadmap & Strategy 	<ul style="list-style-type: none"> • Mandate definition • FIRST.org membership • Roadmap & Strategy • Orgchart buildout 	<ul style="list-style-type: none"> • Mandate definition • FIRST.org membership • Roadmap & Strategy • Orgchart buildout
People 	<ul style="list-style-type: none"> • Featured CSIRT training • Limited remote support 	<ul style="list-style-type: none"> • Relevant CSIRT training • Remote support • SOPs • Study mission tours 	<ul style="list-style-type: none"> • Relevant CSIRT training • Remote support • SOPs • Study mission tours 	<ul style="list-style-type: none"> • Relevant CSIRT training • On-site and remote support • SOPs • Study mission tours
Processes and services 	<ul style="list-style-type: none"> • Incident handling service • Incident handling process 	<ul style="list-style-type: none"> • Incident handling and outreach • Infrastructure support • Standard reporting 	<ul style="list-style-type: none"> • Incident handling, outreach, digital forensics, vulnerability management • Process automation • Infrastructure support • Standard reporting 	<ul style="list-style-type: none"> • Full scale CSIRT/SOC services • Process automation • Automated custom reporting • Maturity progress assessment • Infrastructure support
Measurements 	<ul style="list-style-type: none"> • A few KPIs • No SLAs 	<ul style="list-style-type: none"> • Basic KPIs • SLAs for processes 	<ul style="list-style-type: none"> • KPIs system • SLAs for processes • SIM3 successful audit 	<ul style="list-style-type: none"> • KPIs system • SLAs for services and automation • Annual reviews, SOC-CMM L3 C1.5
Technological Capability 	<ul style="list-style-type: none"> • Incident registration and handling • PGP 	<ul style="list-style-type: none"> • Incident registration and handling • Outreach and visualization portal • Internal support, PGP • Simple vulnerability assessment 	<ul style="list-style-type: none"> • Incident detection and handling • Outreach and visualization portal • Internal support, PGP • Simple vulnerability assessment • Simple video wall • Simple threat intelligence • Simple digital forensics • Simple integration with ex. tooling • Situational awareness 	<ul style="list-style-type: none"> • Incident detection and handling • Outreach and visualization portal • Internal support, PGP • Vulnerability assessment • Video wall • Threat intelligence • Digital Forensics • Integration with existing tooling • Situational awareness and EWS • Multi-site sensing at CII
Local resources 	2-5 people	5-10 people	7-15 people	15-45 people
Duration 	9 months	12 months	12-24 months	24-36 months

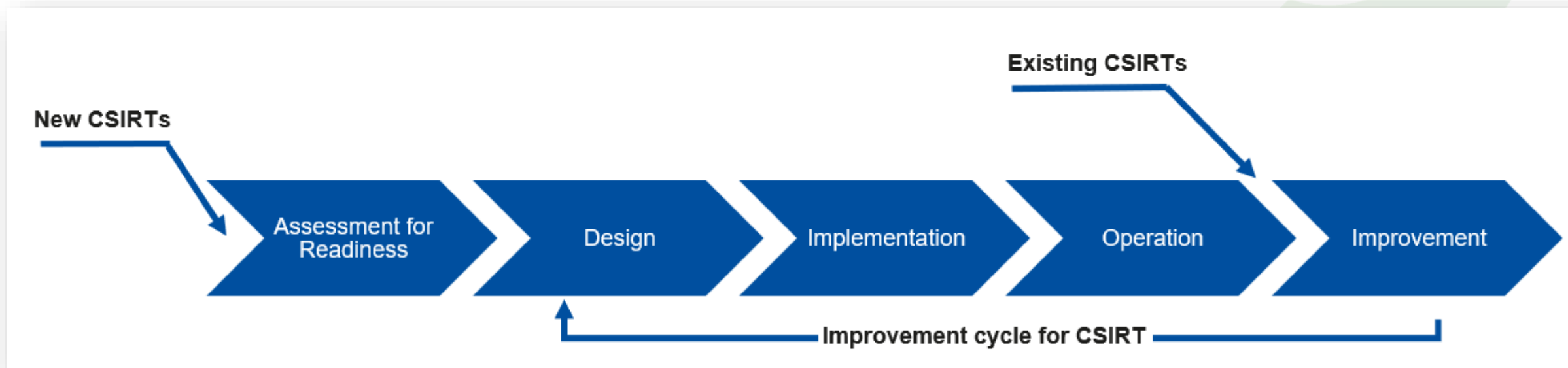
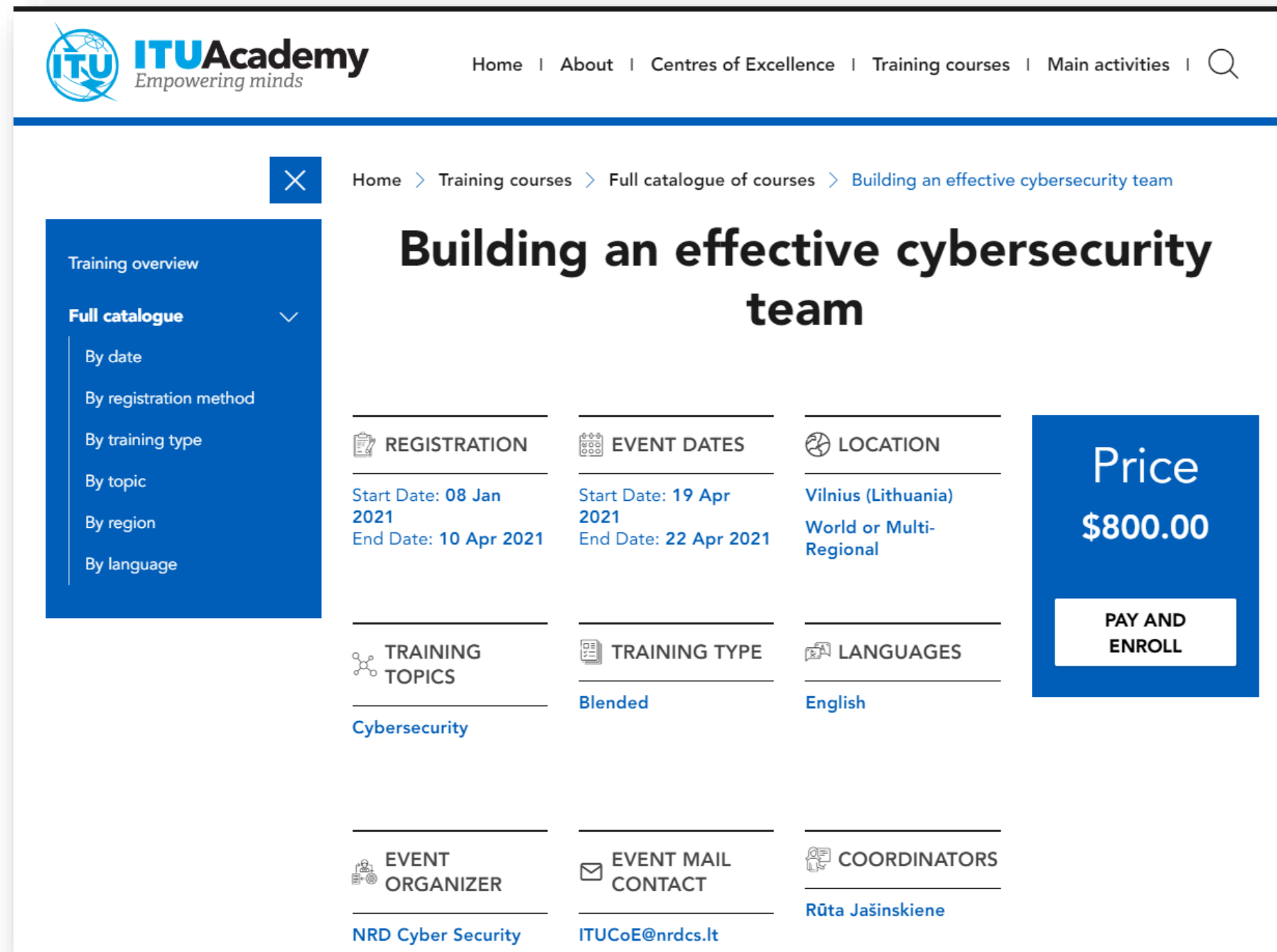


Figure 2 Summary of CSIRT Establishment Outcomes

Assessment for Readiness	Design	Implementation	Operations	Improvement
<input type="checkbox"/> Preliminary Mandate <input type="checkbox"/> Governance Structure <input type="checkbox"/> CSIRT hosting organisation <input type="checkbox"/> Budget for 1-3 years <input type="checkbox"/> Detailed Requirements for Design Stage	<input type="checkbox"/> Approved Detailed Mandate <input type="checkbox"/> CSIRT Services Plan <input type="checkbox"/> CSIRT Processes and Workflows Plan <input type="checkbox"/> CSIRT Organisation, Skills and Training Structure Plan <input type="checkbox"/> CSIRT Facilities Plan <input type="checkbox"/> CSIRT Technologies and Processes Automation Plan <input type="checkbox"/> CSIRT Cooperation Plan <input type="checkbox"/> CSIRT IT and Information Security Management Plan <input type="checkbox"/> Detailed Requirements for Implementation Stage	<input type="checkbox"/> Approved and implemented organisational structure <input type="checkbox"/> Hired and appointed people <input type="checkbox"/> Executed training plan for the staff roles <input type="checkbox"/> Prepared facilities <input type="checkbox"/> Developed and Implemented detailed processes and procedures <input type="checkbox"/> Implemented technology for automation of processes <input type="checkbox"/> Implemented IT and information security management procedures <input type="checkbox"/> Trained people for CSIRT Operations <input type="checkbox"/> Signed relevant agreements with constituency, stakeholders and partners <input type="checkbox"/> CSIRT Services Test Run and Tuning Results <input type="checkbox"/> CSIRT Launch Communication and Celebrations	<input type="checkbox"/> Measured KPIs <input type="checkbox"/> Annual Operations Performance Review <input type="checkbox"/> Annual Stakeholder Needs Review <input type="checkbox"/> Approved Annual Budget <input type="checkbox"/> Collected Requirements for Improvement	<input type="checkbox"/> List of chosen Initiatives for improvement <input type="checkbox"/> Detailed Requirements for Improvement for Design Stage <input type="checkbox"/> Preliminary Budget for Improvement



If interested to dive deeper – Training: Building CSIRTs and SOC



Home | About | Centres of Excellence | Training courses | Main activities | 🔍

Home > Training courses > Full catalogue of courses > Building an effective cybersecurity team

Building an effective cybersecurity team

Training overview

Full catalogue

- By date
- By registration method
- By training type
- By topic
- By region
- By language

<p>REGISTRATION</p> <p>Start Date: 08 Jan 2021 End Date: 10 Apr 2021</p>	<p>EVENT DATES</p> <p>Start Date: 19 Apr 2021 End Date: 22 Apr 2021</p>	<p>LOCATION</p> <p>Vilnius (Lithuania) World or Multi-Regional</p>	<p>Price</p> <p>\$800.00</p> <p>PAY AND ENROLL</p>
<p>TRAINING TOPICS</p> <p>Cybersecurity</p>	<p>TRAINING TYPE</p> <p>Blended</p>	<p>LANGUAGES</p> <p>English</p>	
<p>EVENT ORGANIZER</p> <p>NRD Cyber Security</p>	<p>EVENT MAIL CONTACT</p> <p>ITUCoE@nracs.lt</p>	<p>COORDINATORS</p> <p>Rūta Jašinskiene</p>	

Day I:

- Intro, greetings, expectations
- Cybersecurity Monitoring & Incident Response Teams
- Process of building the CSIRT or SOC team
- Mandate

Day II:

- CSIRT Services
- Incident Management
- Automation of CSIRTs and SOC
- Applied Threat Intelligence

Day III:

- Reporting
- Maturity models of CSIRTs
- Upskilling of people
- Partnering

Day IV:

- Test

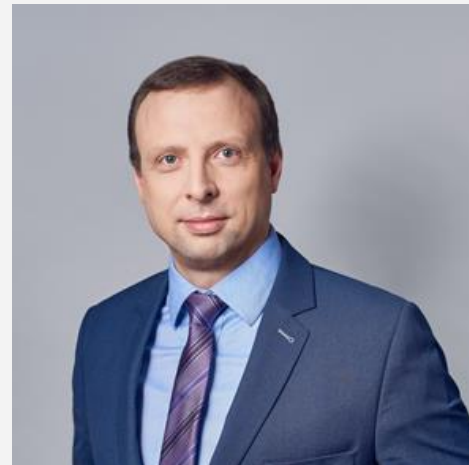


<https://academy.itu.int/training-courses/full-catalogue/building-effective-cybersecurity-team-0>

Any Questions?

Vilius Benetis
NRD Cyber Security

VB@NRDCS.LT
linkedin.com/in/viliusbenetis





ISACA[®]
Belgium Chapter



「Thank you」