Risk treatment methods of cyber attacks

János Ivanyos, MEKH

ERRA WORKSHOP

CYBERSECURITY OF ENERGY INFRASTRUCTURE

February 20 – 21, 2025

Hungarian Energy and Public Utility Regulatory Authority

Clean energy, sustainable environment

The Hungarian Energy and Public Utility Regulatory Authority (MEKH)

MEKH

REGULATION OF THE ELECTRICITY MARKET

REGULATION OF THE NATURAL GAS MARKET

REGULATION OF THE DISTRICT HEATING MARKET

Established in 1994 by law

Independent regulatory authority since 2013

REGULATION OF WATER UTILITY SERVICES

IMPROVE ENERGY EFFICIENCY, AND SUPPORT THE USE OF RENEWABLE ENERGY SOURCES

PREPARATION OF THE WASTE MANAGEMENT PUBLIC SERVICE FEE

Budget
~20 million
EUR

331
Current
staff

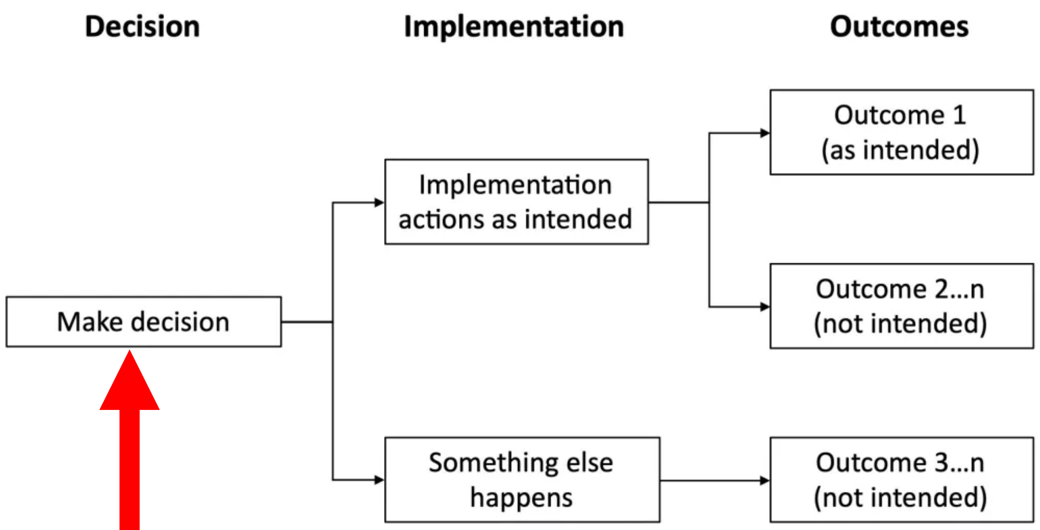
NCCS
NCA

Competences: licensing, supervision, price regulation, national energy-statistics related tasks, supporting competition and renewable integration, market monitoring, customer protection and ensure rTPA to the networks and system services.

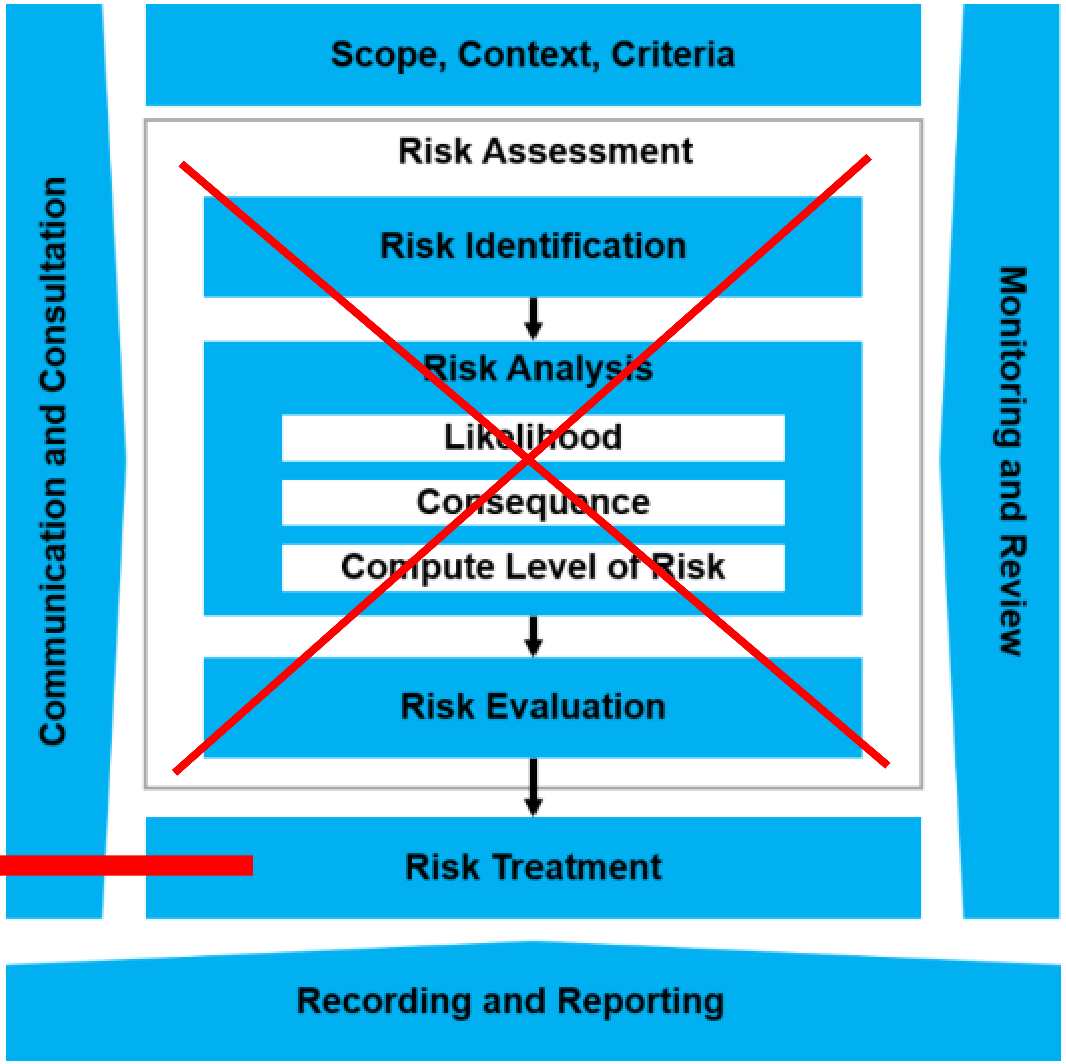
Why „Risk Management” is NOT in the title?

- The term of ***„Risk Management”*** refers to an independent function within the organisation.
- In real (personal and business) life this term could be simply replaced by ***„making decisions”***.
- There are no generic rules, **each decision (type) is unique** and depens on the circumstances, the stakeholders and the information available.
- The literature and science of „Risk Management" is mainly the invention of consultants, auditors, academics, etc. to create **business opportunities.**
- Governments and Regulators „outsource” their social and economic responsibilities by setting **compliance requirements** because they lack the capacity to deal with uncertainty.
- Evidence of „compliance” with risk management (e.g. statutory risk assessment reports, risk maps, risk registers, risk mitigation plans, audit reports, certificates, etc.) are merely **static documents or data sets**.

Risk treatment by Regulators

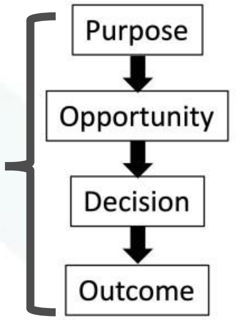

Decision
Implementation
Outcomes
Make decision
Implementation actions as intended
Something else happens
Outcome 1 (as intended)
Outcome 2...n (not intended)
Outcome 3...n (not intended)

Source: https://sufficientcertainty.com/topics/decisions/



Source: ISO 31000:2018 Risk management process

- Cognition
- Regulation
- Support
- Supervision
- Enforcement
- Review



Content overview

Risk treatment methods from the **regulators**' perspective

- **Hybrid defence** and the energy regulators
- **Risk treatment regulatory exercise:** Identifying high impact and critical impact entities under the temporary provisions of the NCCS regulation
- **Information Sharing and Analysis Center (ISAC)**
- Assessment of the **effectiveness of cybersecurity investments** (based on NCCS benchmarking requirements)
- **Cybersecurity Capability Maturity Model** (C2M2)
- **MITRE D3FEND™**

NOTE: This presentation is not a technical level review of risk treatment methods!

Why energy regulators should treat risks?

MEKH

- Systematic cyber attacks in the energy sector against **critical infrastructure**
- In-depth sector (risk impact) **knowledge and empowerment** (market, technology, participants, etc.)
- Relations **between stakeholders** (authorities, consumers, system operators, producers, suppliers, traders, etc.)
- Sectoral and state level **risk preparedness functions** (supervison & exercises)
- **Duty to cooperate** with other competent authorities
- **Independence** from the government (trust issue in information sharing)

What should energy regulators take into account?

- National **development objectives** established by strategy documents

  like supply and operational security; climate neutrality, decarbonisation; affordable energy; etc.

- **Stakeholders' (often contradictory) expectations**

  e.g. economic and environmental sustainability; profitability and consumer prices; increase of renewables and maintaining grid operational security, etc.

- **Sources of uncertainties**

  e.g. climate change, geopolitical situations, technologies, availability of resources, supply chain distruptions, cyber threats, etc.

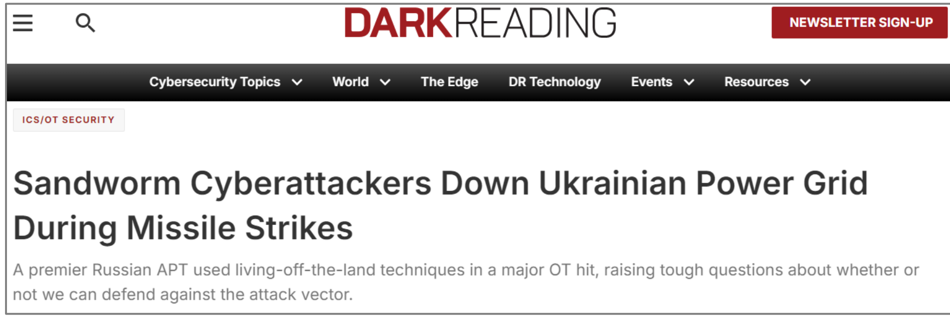
- **Threats to critical infrastructure**

  Hybrid attacks on critical infrastructures, threat actors and their motivations, challenges of hybrid defence, etc.

Hybrid attacks on critical infrastructure

Use of cyber-attack as a tool in geopolitical conflicts

- Increased cyber activities targeting critical infrastructure, including energy and transportation sectors (Ukraine-Russia 2015-)

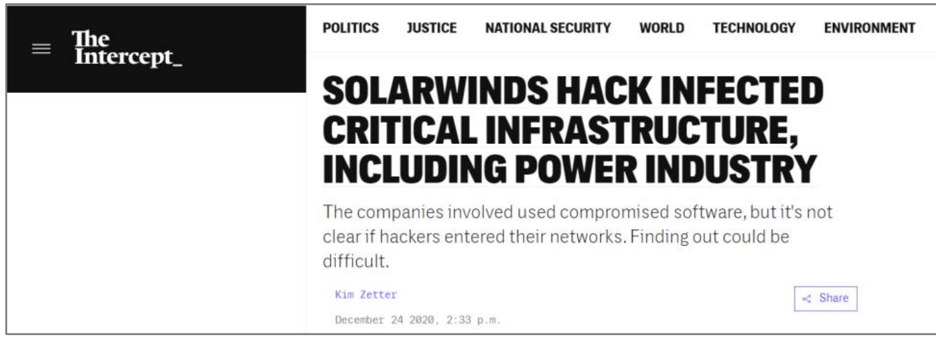


Sandworm Cyberattackers Down Ukrainian Power Grid During Missile Strikes

A premier Russian APT used living-off-the-land techniques in a major OT hit, raising tough questions about whether or not we can defend against the attack vector.

Risks associated with supply chain vulnerabilities

- Compromised SolarWinds' Orion software, affecting numerous organizations in various sectors including government and critical infrastructure (2020).



SOLARWINDS HACK INFECTED CRITICAL INFRASTRUCTURE, INCLUDING POWER INDUSTRY

The companies involved used compromised software, but it's not clear if hackers entered their networks. Finding out could be difficult.

Kim Zetter

December 24 2020, 2:33 p.m.

Large scale simultanious cyber attacks

MEKH

- **Many companies targeted at the same time**, avoiding that impacted infrastructure could have shared information on the attack with peers.
- **State-sponsored** planning and resources.
- **Coordinated attacks** on Danish critical infrastructure (2023)

SEKTOR CERT

The attack against Danish, critical infrastructure

Published: November 2023

TLP:CLEAR

https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

Threat actors

Categories:

- Cybercriminal 50%
- State-sponsored 40%
- Hacktivist 10%

Origin:

- China (17%)
- Russia (9%)
- Iran (5%)

Targeted countries (T10):

- US
- Germany, India, Australia
- UK
- France, Italy, China, Japan, Canada

Targeted industries (T10):

- Government
- Financial services
- Technology, Telecommunication
- Media, Education, Healthcare, **Energy**
- Manufacturing, Retail

<) FORESCOUT RESEARCH | VEDERE LABS

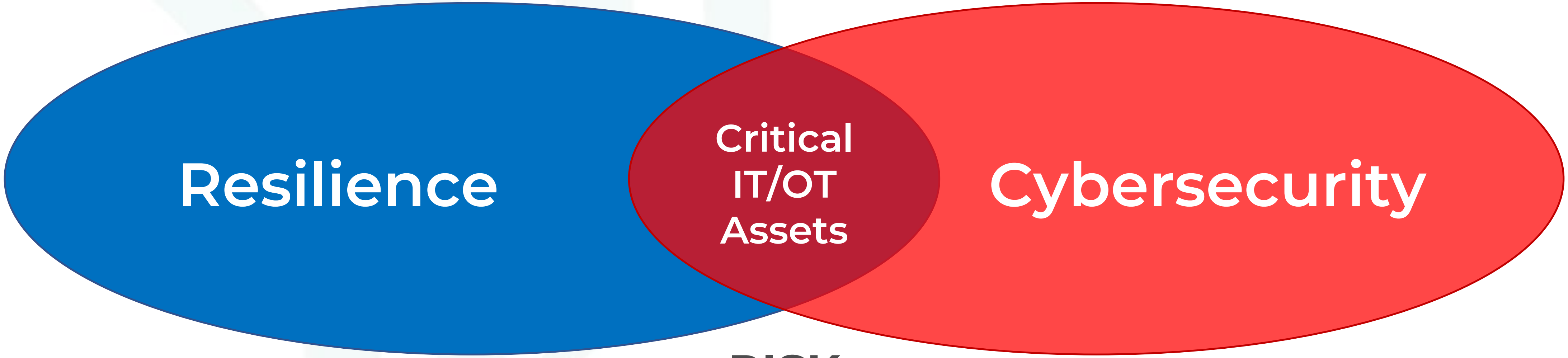
PERILS IN THE PERIPHERY: A 2024H1 THREAT REVIEW

Vulnerabilities, Threat Actors and Ransomware in the Unmanaged Perimeter

August 29, 2024

Hybrid defence aspects for regulators

MEKH



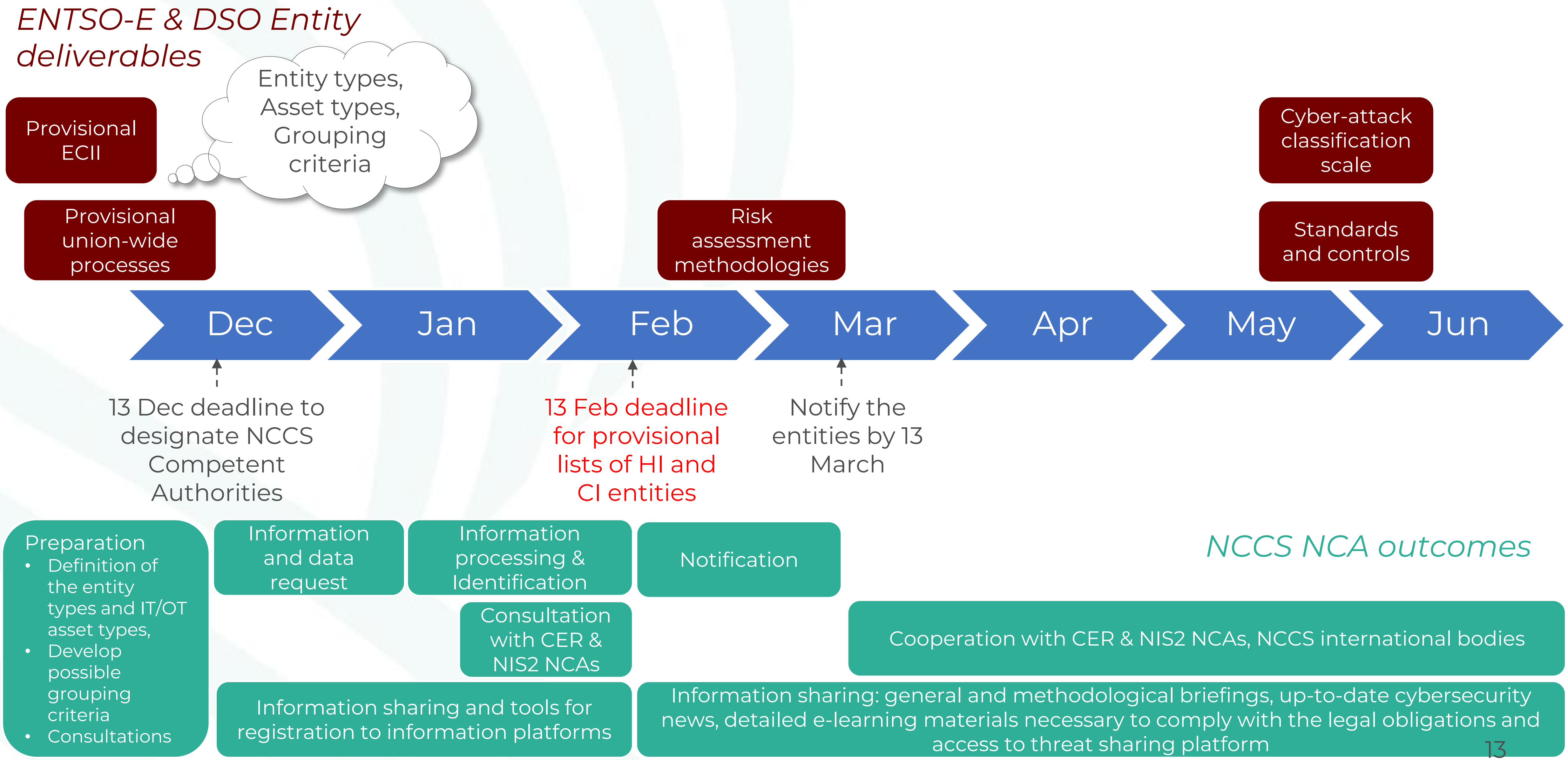
RISK PREPAREDNESS & MITIGATION

- Similar **risk impact** on society, economy, military, environment, etc. -> same impact metrics
- Different **occurance** types (vulnerability, threat, attack) -> likelihood vs severity (metrics)

Risk treatment challenges in cyber defence

• Dependence from supply chain	✓ Controls of (ICT) products & services, supplier contracts
• Simultaneous attacks and cross-border impact	✓ Knowledge & information sharing
• Enhanced cybersecurity control requirements	✓ Cybersecurity maturity development
• Real time detection and reaction	✓ Exploiting artificial intelligence
• Crisis management	✓ Planning & testing (exercises)

NCCS implementation - as a regulatory risk treatment exercise



ENTSO-E & DSO Entity deliverables

Provisional ECII

Entity types, Asset types, Grouping criteria

Provisional union-wide processes

Risk assessment methodologies

Cyber-attack classification scale

Standards and controls

Dec → Jan → Feb → Mar → Apr → May → Jun

13 Dec deadline to designate NCCS Competent Authorities

13 Feb deadline for provisional lists of HI and CI entities

Notify the entities by 13 March

NCCS NCA outcomes

Preparation
- Definition of the entity types and IT/OT asset types,
- Develop possible grouping criteria
- Consultations

Information and data request

Information processing & Identification

Consultation with CER & NIS2 NCAs

Notification

Cooperation with CER & NIS2 NCAs, NCCS international bodies

Information sharing and tools for registration to information platforms

Information sharing: general and methodological briefings, up-to-date cybersecurity news, detailed e-learning materials necessary to comply with the legal obligations and access to threat sharing platform

NCCS implementation: Preparation

Taking into account:

- Provisional **ECII indicators and the thresholds**
- The **Union-wide high impact and critical impact processes** published by ENTSO-E
  - roles in the implementation of the processes -> **entity types**
  - **list of assets** necessary to implement the processes per entity types
- **Information requests** from all entities (per entity types)
  - **volume indicator** (max. load/capacity/trade/etc. of last year)
  - **power of disposal** (control) over the listed assets
  - **ICT service providers** relevant to IT/OT assets
  - **connections** to external data or communication networks or systems
- **Providing information** to entities about
  - the identification process,
  - the relevant legislative environment,
  - the data requests, and
  - the obligations and opportunities of being identified.

NCCS implementation: Grouping

- The competent authority may identify additional entities as high-impact or critical-impact entities if the following criteria are met:
  a) the **entity is part of a group** of entities for which there is a significant risk that they will be **affected simultaneously by a cyber-attack**;
  b) the **ECII aggregated over the group** of entities is above the high-impact or critical-impact threshold.
- The **significant risk of a simultaneous cyber-attack** exists (not exclusively)

  when the assets at the disposal of the members of the group are **connected to the same network or system** for the purpose of exchanging data or communication.

  [E.g. connections to a network or system of a company group, a TSO, a DSO, a NEMO, an ICT service provider, etc.]

NCCS implementation: Identification process

- **Information collection** and processing, setting **grouping criteria**
- **Decision**
  - Calculated **ECII value** is over the provisional high impact and critical impact tresholds
  - Disposal over any **asset** necessary to implement a union-wide process
- Establishing the **provisional list** of high impact and critical impact entities
- **Notify** the decision on identification to the relevant entity within 30 days
- **Consulting** with the competent authorities under the CER and NIS2 Directives on the designation status
- Providing access to **information sharing platforms**

  provision of general and methodological briefings, up-to-date cybersecurity news, detailed e-learning materials necessary to comply with the legal obligations and access to threat sharing platform

NCCS implementation: Information sharing

- Provision of general and methodological briefings, up-to-date cybersecurity news, detailed e-learning materials necessary to comply with the legal obligations and access to threat sharing platform.
- **Information Sharing and Analysis Center (ISAC)**
  - Central resource for gathering **information on cyber threats** (in many cases to critical infrastructure)
  - **Two-way sharing of information** between the private and the public sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis.
  - **Models:** Country focused; Sector specific; International
  - **Capabilities:** Information sharing; Analysis; Trust building; Capacity building

Source: Information Sharing and Analysis Center (ISACs) - Cooperative Models, ENISA, 2018

ISAC: Types of information to be shared 1.

- **Incidents** - details of attempted and successful attacks
  - that may include a description of information lost, techniques used, intent, and impact.
  - The severity of an incident could range from a successfully blocked attack to a serious national security situation.
- **Threats** - yet-to-be-understood issues
  - with potentially serious implications; indicators of compromise, such as malicious files, stolen email addresses, impacted IP addresses, or malware samples; or information about threat actors.
  - Threat information can help operators detect or deter incidents, learn from attacks, and create solutions that can better protect their own systems and those of others.
- **Vulnerabilities** - in software, hardware, or business processes that can be exploited for malicious purposes
- **Mitigations** - methods for remedying vulnerabilities, containing or blocking threats, and responding to and recovering from incidents

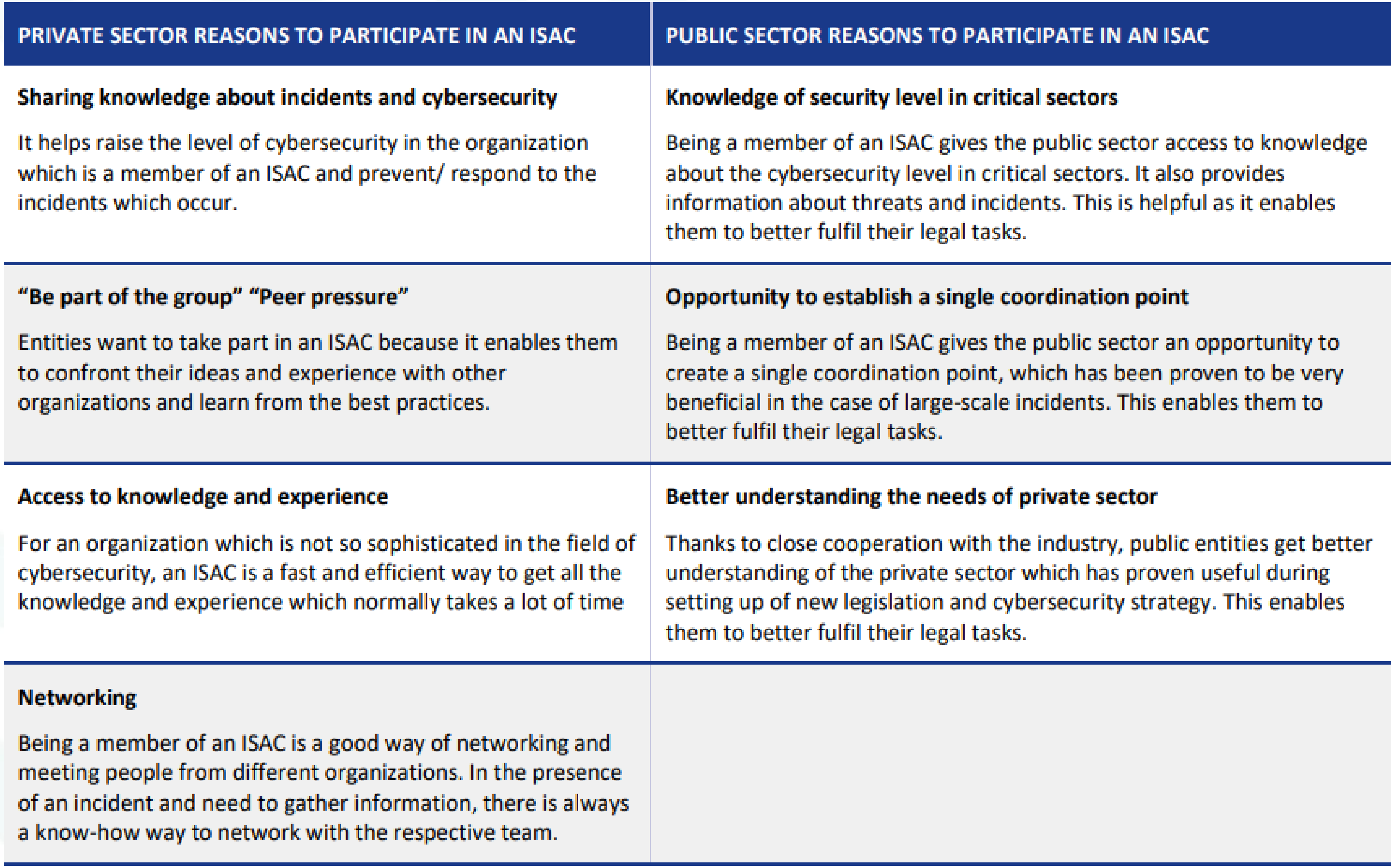
Source: Information Sharing and Analysis Center (ISACs) - Cooperative Models, ENISA, 2018

ISAC: Types of information to be shared 2.

- **Situational awareness** - information that enables decision-makers to respond to an incident
  - and that may require real-time telemetry of exploited vulnerabilities, active threats, and attacks.
  - It could also contain information about the targets of attacks and the state of critical public or private networks.
- **Best practices** - information related to how software and services are developed and delivered
  - such as security controls, development and incident response practices, and software patching or effectiveness metrics;
- **Strategic analysis** - gathering, distilling, and analyzing many types of information to build metrics, trends, and projections.
  - It is often blended with projections of potential scenarios to prepare government or private sector decision-makers for future risks.

Source: Information Sharing and Analysis Center (ISACs) - Cooperative Models, ENISA, 2018

ISAC: Private and public sector motivations



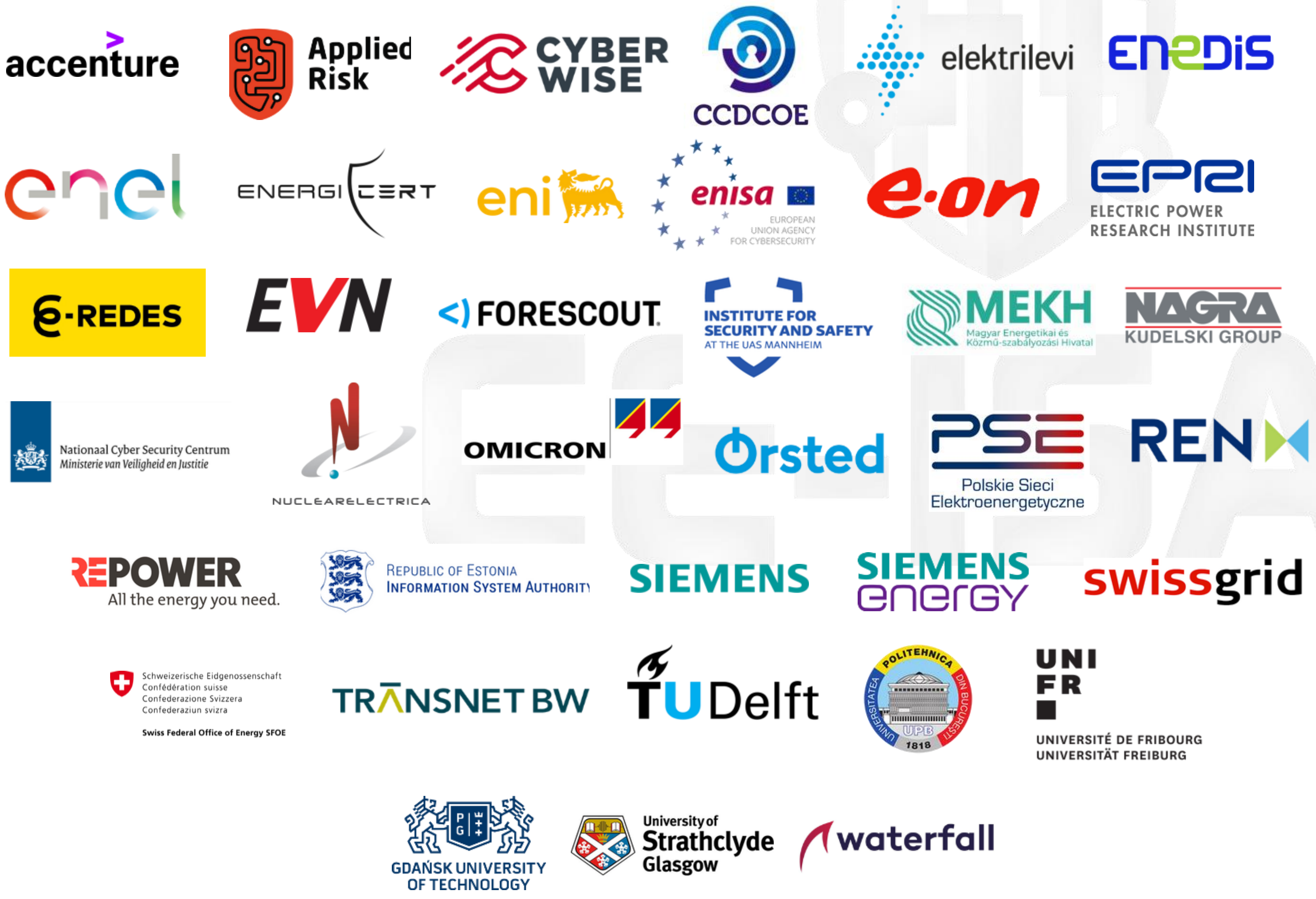
PRIVATE SECTOR REASONS TO PARTICIPATE IN AN ISAC	PUBLIC SECTOR REASONS TO PARTICIPATE IN AN ISAC
Sharing knowledge about incidents and cybersecurity It helps raise the level of cybersecurity in the organization which is a member of an ISAC and prevent/ respond to the incidents which occur.	**Knowledge of security level in critical sectors** Being a member of an ISAC gives the public sector access to knowledge about the cybersecurity level in critical sectors. It also provides information about threats and incidents. This is helpful as it enables them to better fulfil their legal tasks.
"Be part of the group" "Peer pressure" Entities want to take part in an ISAC because it enables them to confront their ideas and experience with other organizations and learn from the best practices.	**Opportunity to establish a single coordination point** Being a member of an ISAC gives the public sector an opportunity to create a single coordination point, which has been proven to be very beneficial in the case of large-scale incidents. This enables them to better fulfil their legal tasks.
Access to knowledge and experience For an organization which is not so sophisticated in the field of cybersecurity, an ISAC is a fast and efficient way to get all the knowledge and experience which normally takes a lot of time	**Better understanding the needs of private sector** Thanks to close cooperation with the industry, public entities get better understanding of the private sector which has proven useful during setting up of new legislation and cybersecurity strategy. This enables them to better fulfil their legal tasks.
Networking Being a member of an ISAC is a good way of networking and meeting people from different organizations. In the presence of an incident and need to gather information, there is always a know-how way to network with the respective team.	

Source: Information Sharing and Analysis Center (ISACs) - Cooperative Models, ENISA, 2018

EE-ISAC

Information Sharing in Network of Trust

MEKH


accenture
Applied Risk
CYBER WISE
CCDCOE
elektrilevi
ENEDIS
enel
ENERGICERT
eni
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
e·on
EPRI
ELECTRIC POWER RESEARCH INSTITUTE
E-REDES
EVN
FORESCOUT
INSTITUTE FOR SECURITY AND SAFETY
AT THE UAS MANNHEIM
MEKH
Magyar Energetikai és Közmű-szabályozási Hivatal
NAGRA
KUDELSKI GROUP
Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie
NUCLEARELECTRICA
OMICRON
Ørsted
PSE
Polskie Sieci Elektroenergetyczne
REN
REPOWER
All the energy you need.
REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY
SIEMENS
SIEMENS energy
swissgrid
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Federal Office of Energy SFOE
TRANSNET BW
TU Delft
POLITEHNICA DIN BUCUREŞTI
UNIVERSITATEA
UPB
1818
UNI FR
UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG
GDAŃSK UNIVERSITY OF TECHNOLOGY
University of Strathclyde Glasgow
waterfall

Operators	14
Solution Providers	9
Academia	6
Governmental - NFP	7
Research	1

MEMBERS #37

TLP GREEN

EE-ISAC

Information Sharing in Network of Trust

MEKH

MoU Partners (12)

Cynergy ISAC

EASE Energy Analytic Security Exchange

E.DSO

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

A DIVISION OF NERC

ENCS

DSO ENTITY DSOs FOR EUROPE

EUROCONTROL

EUTC

FS-ISAC

JE-ISAC

kraftCERT

OT-ISAC OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

Institutions (2)

European Commission

European Parliament

MOU in process (2)

IT ISAC

KEPCO

Collaboration: #12 Partners & EU Institutions

TLP GREEN

MISP and TASK FORCES

Malware Information Sharing Platform (MISP)

MISP is a threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attack, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.

Info sharing platforms & Threat Inteligence

Forescout elaborates a monthly report that summarizes the main vulnerabilities, incidents and malwares detected, along with some statistics related to the MISP platform. Any organization can send relevant cyber threats/attacks to collect on the report.

Threat Landscape

The EE-ISAC, in collaboration with ENISA's team, is working on the establishment of a threat modelling standard to be disseminated among Members as the guidelines and best practices of threat intelligence and incident management.

Advocacy

Acts to solidify EE-ISAC as the unified voice for cybersecurity in the European energy industry by monitoring EU policy developments, EU funding opportunities and engaging with European institutions.

Communications

In charge of coordinating the marketing initiatives of the Association, specifically the ones related to promotional activities, webinars, events and the EE-ISAC presence in international and European conferences on cybersecurity and digitalization.

Physical Security

Composed by 16 representatives of the EE-ISAC members, this task force supports utilities in enhancing physical security capabilities and ensuring compliance by sharing international best practices and use cases from the energy and other critical sectors.

Assessment of the effectiveness of cybersecurity investments (NCCS Benchmarking)

Practical approach keeping the assessment workload manageable for the entities and the regulators

Quantitative performance indicators If they are too detailed, then will go beyond what most entities would be able to furnish within the timeframes (e.g. 3 years)

Qualitative self-assessment questionnaires could be based on existing ‘cybersecurity maturity’ self-evaluation tools or questionnaires (e.g. C2M2, ENISA’s cybersecurity maturity self-assessment tool for SMEs, etc.)

Simple ‘maturity-type’ questions based on

- the cost items (should be identical in general ledger data);
- the costs of these items reported by entities;
- the transformation of the legislative assessment criteria to specific questions; and
- the comparability of the cybersecurity costs and functions

Very effective	Mostly effective	Mostly ineffective	Ineffective

NCCS Art. 13(2) NRAs assess whether **current investments** in cybersecurity:

(a) **mitigate risks** having an impact on cross-border electricity flows;

(b) **provide the desired results and engender efficiency gains** for the development of the electricity systems; and

(c) are **efficient and integrated into the overall procurement** of assets and services.

Comparability of cybersecurity costs and functions (NCCS Benchmarking)

MEKH

Comparability of costs

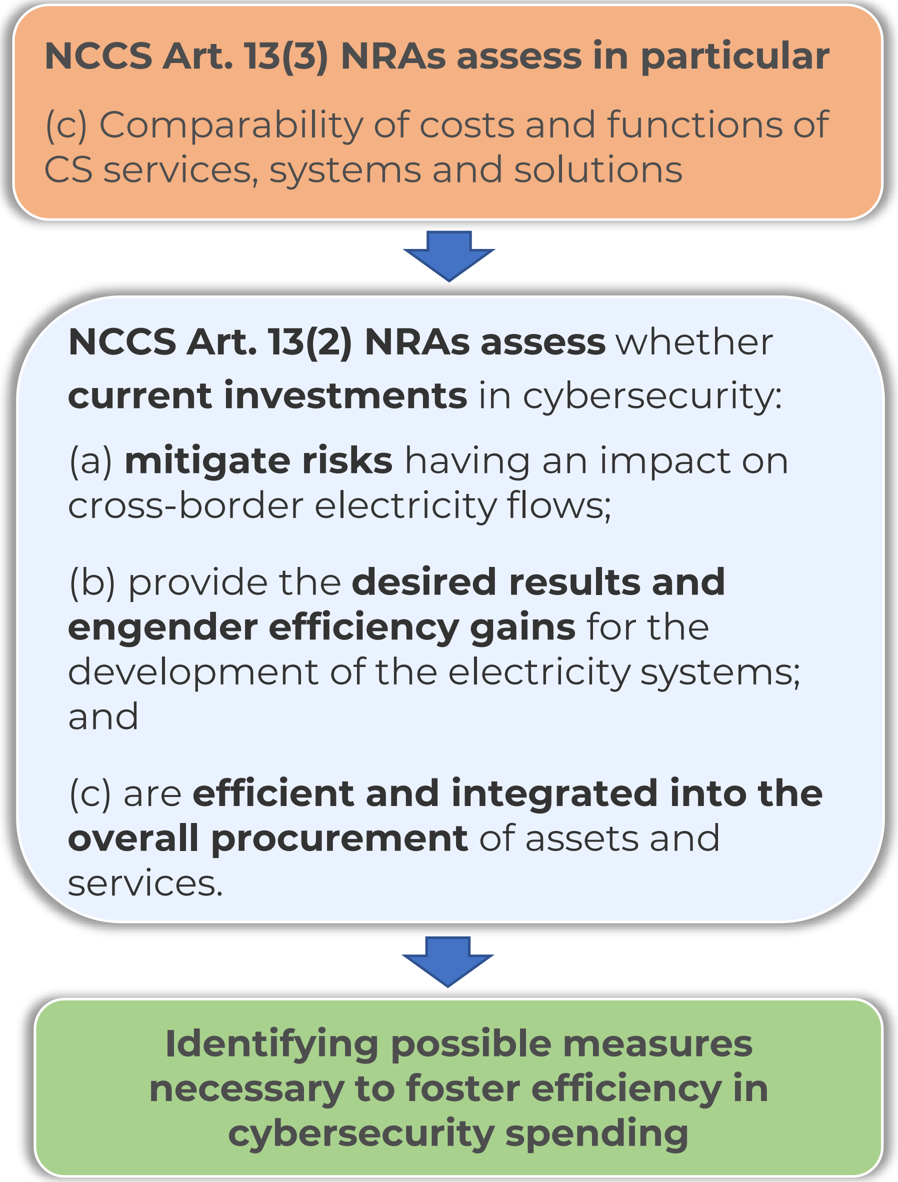
Should be based on cost items, asset types and entity types (normalisation)

Comparability of functions

Comparability of functions by reference to types of mitigations, e.g.:
MITRE ATT&CK® ICS Mitigations;
MITRE D3FEND™ cybersecurity countermeasures;
ISO/IEC 27002:2022 operational capabilities (merged):

- **Governance, including risk management activities, assurance (e.g. audit), legal and compliance**
- **Asset management, secure configuration, threat and vulnerability management**
- **Information protection, system and network security and application security**
- **Physical security**
- **Human resource security (screening policy)**
- **Identity and access management**
- **Information security event management**
- **Continuity**
- **Supplier relationships security**

Based on ISO/IEC 27002:2022



NCCS Art. 13(3) NRAs assess in particular

(c) Comparability of costs and functions of CS services, systems and solutions

NCCS Art. 13(2) NRAs assess whether **current investments** in cybersecurity:

(a) **mitigate risks** having an impact on cross-border electricity flows;

(b) provide the **desired results and engender efficiency gains** for the development of the electricity systems; and

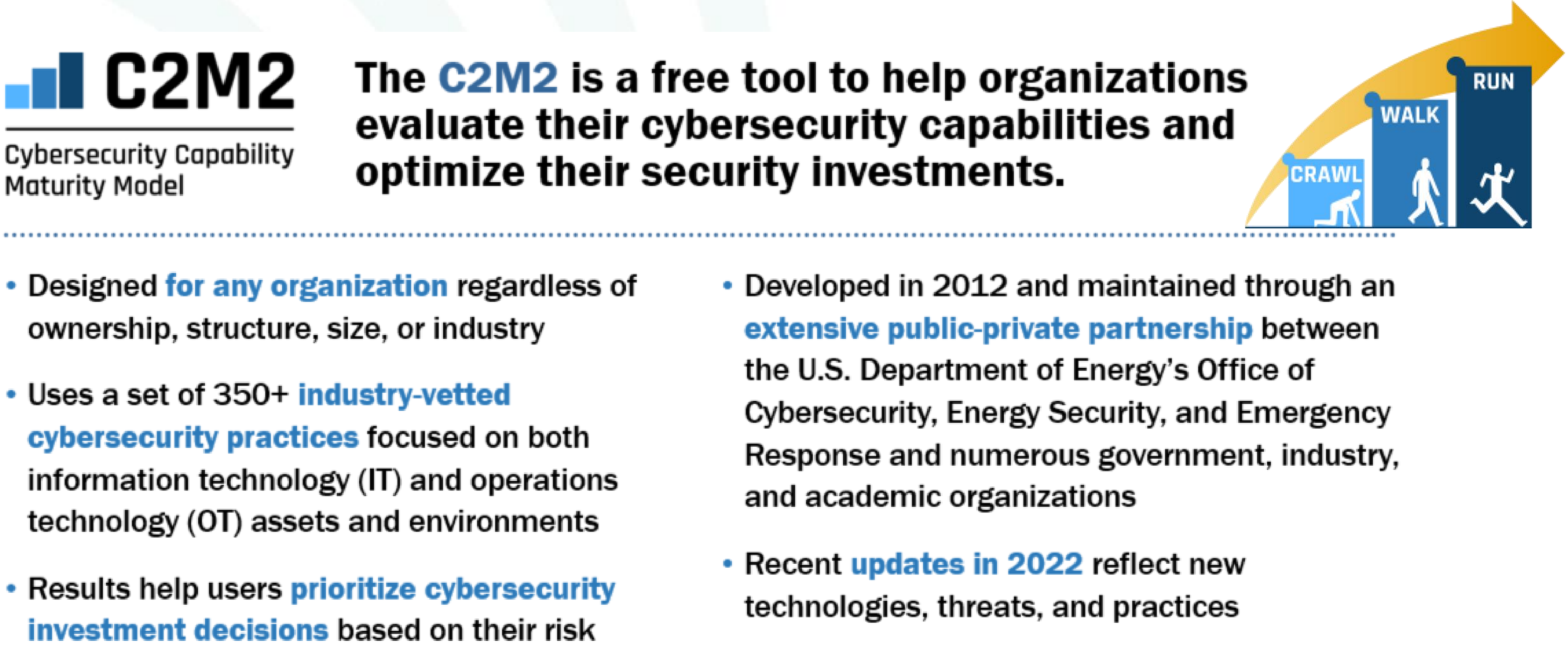
(c) are **efficient and integrated into the overall procurement** of assets and services.

Identifying possible measures necessary to foster efficiency in cybersecurity spending

enisa

ACER
European Union Agency for the Cooperation of Energy Regulators

Cybersecurity Maturity Assessment (Supporting methodology)



CRAWL
WALK
RUN

C2M2

Cybersecurity Capability Maturity Model

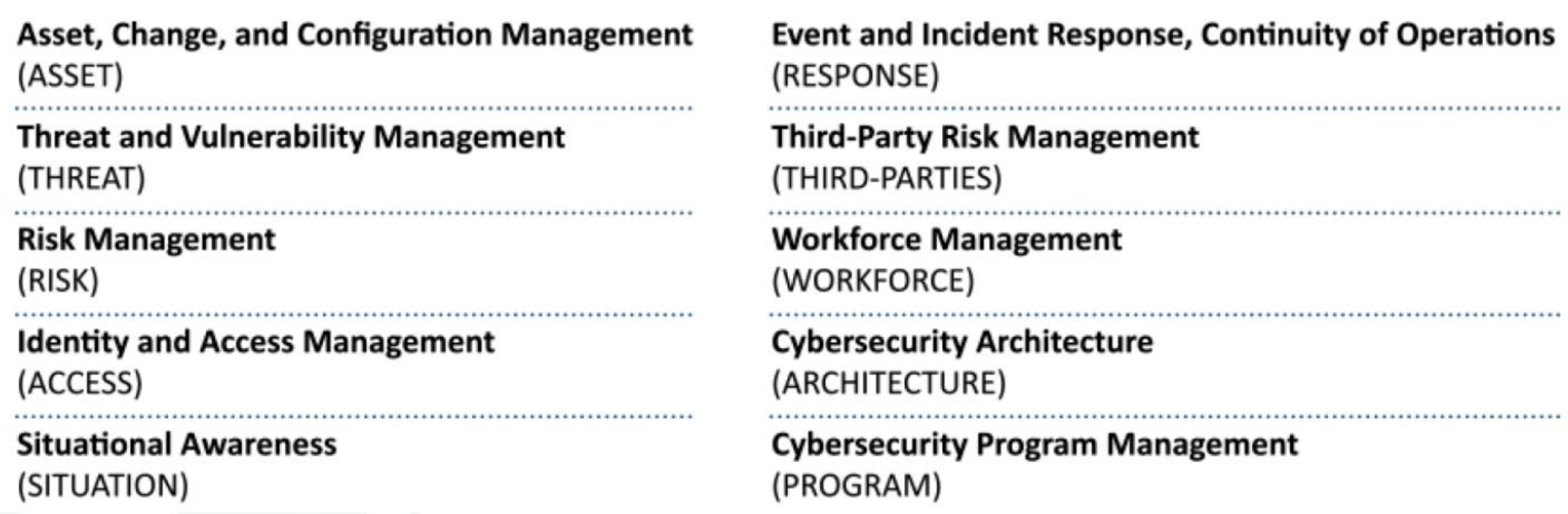
The C2M2 is a free tool to help organizations evaluate their cybersecurity capabilities and optimize their security investments.

- Designed **for any organization** regardless of ownership, structure, size, or industry
- Uses a set of 350+ **industry-vetted cybersecurity practices** focused on both information technology (IT) and operations technology (OT) assets and environments
- Results help users **prioritize cybersecurity investment decisions** based on their risk
- Developed in 2012 and maintained through an **extensive public-private partnership** between the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response and numerous government, industry, and academic organizations
- Recent **updates in 2022** reflect new technologies, threats, and practices

https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

U.S. DEPARTMENT of ENERGY

C2M2 Domains (Supervision areas)



Asset, Change, and Configuration Management
(ASSET)

Threat and Vulnerability Management
(THREAT)

Risk Management
(RISK)

Identity and Access Management
(ACCESS)

Situational Awareness
(SITUATION)

Event and Incident Response, Continuity of Operations
(RESPONSE)

Third-Party Risk Management
(THIRD-PARTIES)

Workforce Management
(WORKFORCE)

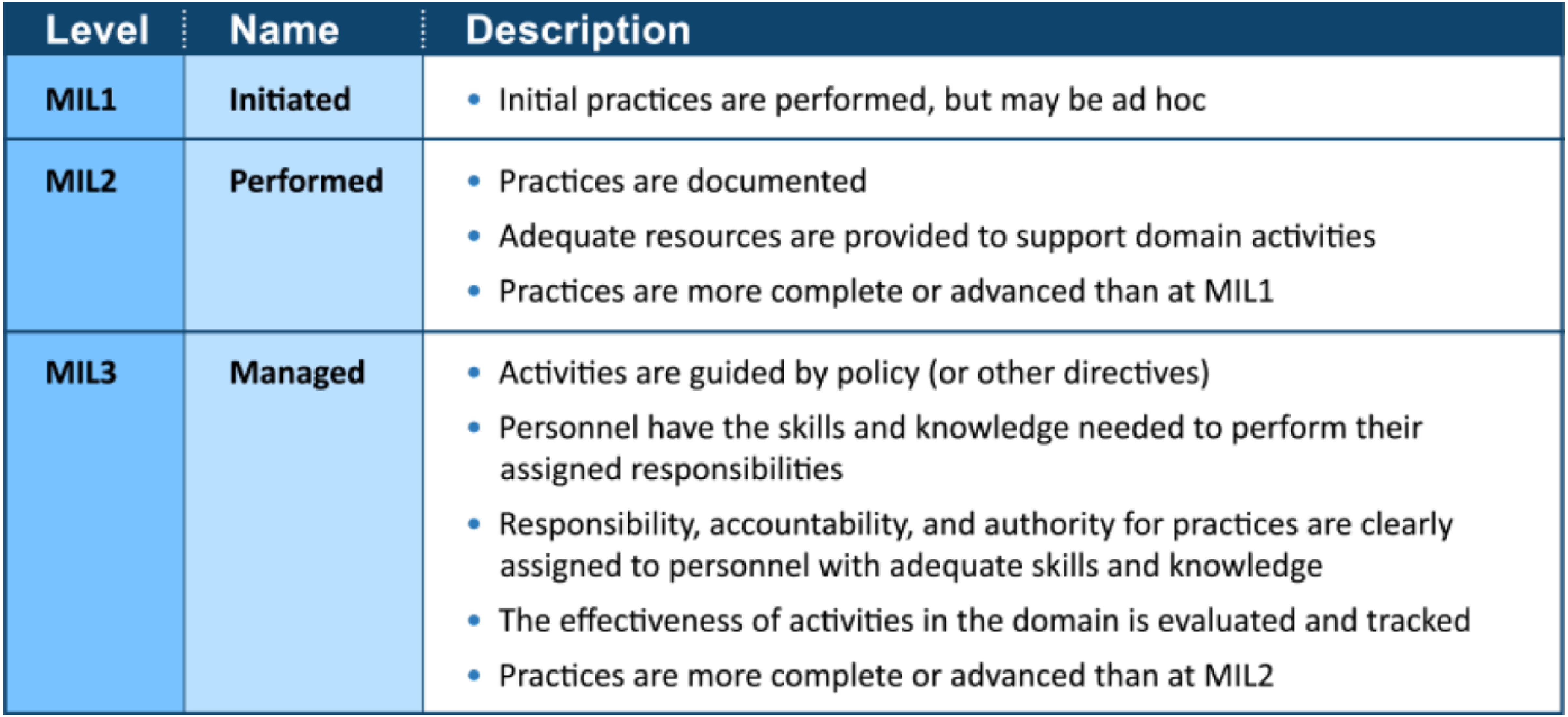
Cybersecurity Architecture
(ARCHITECTURE)

Cybersecurity Program Management
(PROGRAM)

https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

Targeting Maturity Indicator Levels (MILs)
Decision based on costs, benefits and obligations

MEKH



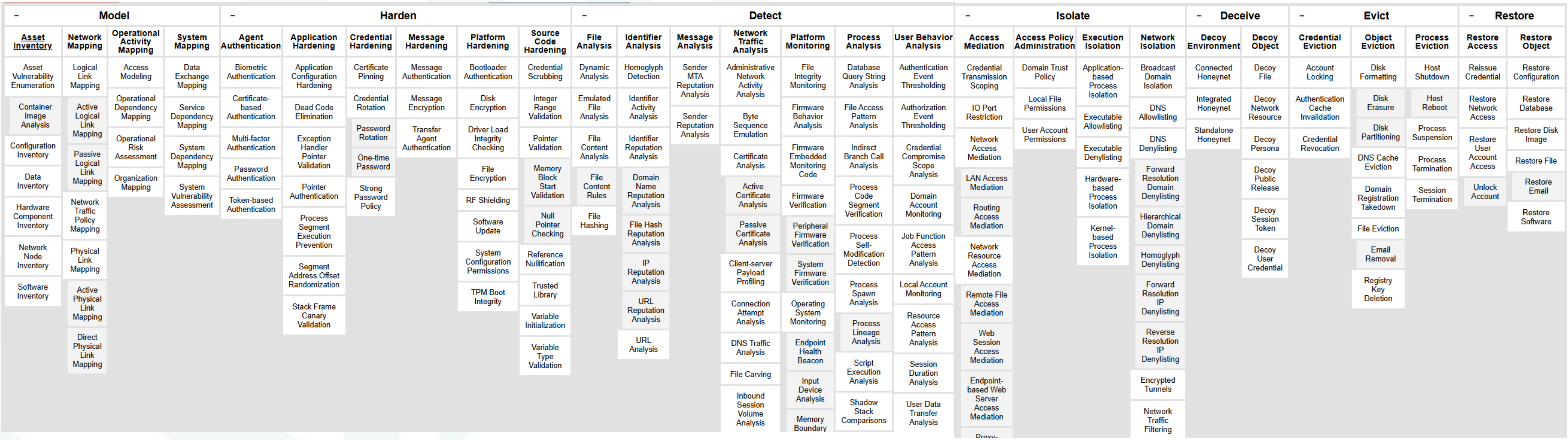
Level	Name	Description
MIL1	**Initiated**	• Initial practices are performed, but may be ad hoc
MIL2	**Performed**	• Practices are documented • Adequate resources are provided to support domain activities • Practices are more complete or advanced than at MIL1
MIL3	**Managed**	• Activities are guided by policy (or other directives) • Personnel have the skills and knowledge needed to perform their assigned responsibilities • Responsibility, accountability, and authority for practices are clearly assigned to personnel with adequate skills and knowledge • The effectiveness of activities in the domain is evaluated and tracked • Practices are more complete or advanced than at MIL2

https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

U.S. DEPARTMENT of ENERGY

MITRE D3FEND™ (Support)

Knowledge Graph and website of cybersecurity countermeasures



- Model

Asset Inventory
- Asset Vulnerability Enumeration
- Container Image Analysis
- Configuration Inventory
- Data Inventory
- Hardware Component Inventory
- Network Node Inventory
- Software Inventory

Network Mapping
- Logical Link Mapping
- Active Logical Link Mapping
- Passive Logical Link Mapping
- Network Traffic Policy Mapping
- Physical Link Mapping
- Active Physical Link Mapping
- Direct Physical Link Mapping

Operational Activity Mapping
- Access Modeling
- Operational Dependency Mapping
- Operational Risk Assessment
- Organization Mapping

System Mapping
- Data Exchange Mapping
- Service Dependency Mapping
- System Dependency Mapping
- System Vulnerability Assessment

- Harden

Agent Authentication
- Biometric Authentication
- Certificate-based Authentication
- Multi-factor Authentication
- Password Authentication
- Token-based Authentication

Application Hardening
- Application Configuration Hardening
- Dead Code Elimination
- Exception Handler Pointer Validation
- Pointer Authentication
- Process Segment Execution Prevention
- Segment Address Offset Randomization
- Stack Frame Canary Validation

Credential Hardening
- Certificate Pinning
- Credential Rotation
- Password Rotation
- One-time Password
- Strong Password Policy

Message Hardening
- Message Authentication
- Message Encryption
- Transfer Agent Authentication

Platform Hardening
- Bootloader Authentication
- Disk Encryption
- Driver Load Integrity Checking
- File Encryption
- RF Shielding
- Software Update
- System Configuration Permissions
- TPM Boot Integrity

Source Code Hardening
- Credential Scrubbing
- Integer Range Validation
- Pointer Validation
- Memory Block Start Validation
- Null Pointer Checking
- Reference Nullification
- Trusted Library
- Variable Initialization
- Variable Type Validation

- Detect

File Analysis
- Dynamic Analysis
- Emulated File Analysis
- File Content Analysis
- File Content Rules
- File Hashing

Identifier Analysis
- Homoglyph Detection
- Identifier Activity Analysis
- Identifier Reputation Analysis
- Domain Name Reputation Analysis
- File Hash Reputation Analysis
- IP Reputation Analysis
- URL Reputation Analysis
- URL Analysis

Message Analysis
- Sender MTA Reputation Analysis
- Sender Reputation Analysis

Network Traffic Analysis
- Administrative Network Activity Analysis
- Byte Sequence Emulation
- Certificate Analysis
- Active Certificate Analysis
- Passive Certificate Analysis
- Client-server Payload Profiling
- Connection Attempt Analysis
- DNS Traffic Analysis
- File Carving
- Inbound Session Volume Analysis

Platform Monitoring
- File Integrity Monitoring
- Firmware Behavior Analysis
- Firmware Embedded Monitoring Code
- Firmware Verification
- Peripheral Firmware Verification
- System Firmware Verification
- Operating System Monitoring
- Endpoint Health Beacon
- Input Device Analysis
- Memory Boundary

Process Analysis
- Database Query String Analysis
- File Access Pattern Analysis
- Indirect Branch Call Analysis
- Process Code Segment Verification
- Process Self-Modification Detection
- Process Spawn Analysis
- Process Lineage Analysis
- Script Execution Analysis
- Shadow Stack Comparisons

User Behavior Analysis
- Authentication Event Thresholding
- Authorization Event Thresholding
- Credential Compromise Scope Analysis
- Domain Account Monitoring
- Job Function Access Pattern Analysis
- Local Account Monitoring
- Resource Access Pattern Analysis
- Session Duration Analysis
- User Data Transfer Analysis

- Isolate

Access Mediation
- Credential Transmission Scoping
- IO Port Restriction
- Network Access Mediation
- LAN Access Mediation
- Routing Access Mediation
- Network Resource Access Mediation
- Remote File Access Mediation
- Web Session Access Mediation
- Endpoint-based Web Server Access Mediation
- Proxy-

Access Policy Administration
- Domain Trust Policy
- Local File Permissions
- User Account Permissions

Execution Isolation
- Application-based Process Isolation
- Executable Allowlisting
- Executable Denylisting
- Hardware-based Process Isolation
- Kernel-based Process Isolation

Network Isolation
- Broadcast Domain Isolation
- DNS Allowlisting
- DNS Denylisting
- Forward Resolution Domain Denylisting
- Hierarchical Domain Denylisting
- Homoglyph Denylisting
- Forward Resolution IP Denylisting
- Reverse Resolution IP Denylisting
- Encrypted Tunnels
- Network Traffic Filtering

- Deceive

Decoy Environment
- Connected Honeynet
- Integrated Honeynet
- Standalone Honeynet

Decoy Object
- Decoy File
- Decoy Network Resource
- Decoy Persona
- Decoy Public Release
- Decoy Session Token
- Decoy User Credential

- Evict

Credential Eviction
- Account Locking
- Authentication Cache Invalidation
- Credential Revocation

Object Eviction
- Disk Formatting
- Disk Erasure
- Disk Partitioning
- DNS Cache Eviction
- Domain Registration Takedown
- File Eviction
- Email Removal
- Registry Key Deletion

Process Eviction
- Host Shutdown
- Host Reboot
- Process Suspension
- Process Termination
- Session Termination

- Restore

Restore Access
- Reissue Credential
- Restore Network Access
- Restore User Account Access
- Unlock Account

Restore Object
- Restore Configuration
- Restore Database
- Restore Disk Image
- Restore File
- Restore Email
- Restore Software

https://d3fend.mitre.org/

Thank you for your attention!

Hungarian Energy and Public Utility Regulatory Authority

Clean energy, sustainable environment