ISACA

NIS2 and IAM

ISACA NL chapter roundtable
15 mei 2024 Eindhoven

André Koot

NIS2 and IAM

● Introduction

● Reasoning behind NIS2

● NIS2 and IAM

● Q & A

SonicBee

Whoami

- Co-founder SonicBee 1-12-20220
- InfoSec since 1995
- IAM since 1999
  Member BoK committee IDPro
- Member PvIB
- Ex-member ISACA / Norea

SonicBee in short

Our vision:
Independent IAM advisory services from a business perspective

30+

IAM business experts & growing fast

Locations:

Utrecht (NL)
Regensburg (DE)

International (EU) growth ambitions

Unique business oriented IAM Advisory Services and portfolio

ISO 27001 Certified

Our drive:
Help organisations to use data to be better equipped to take decisions, enhance the customer experience and lower costs in a secure an compliant way of working

Founded **2020**

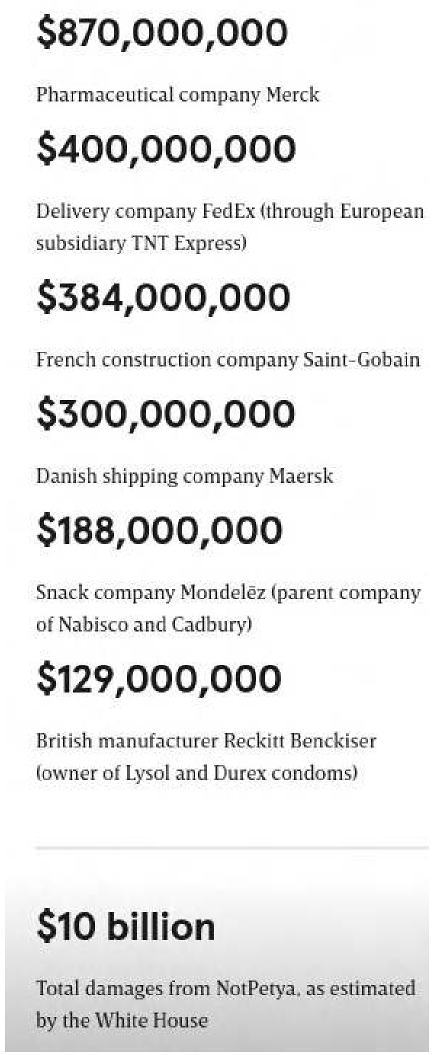
By Patrick, André & Anne

MSP developments:

NEXIS PlatinumPartner

economic
rights
repeal
cooperation
authorities
confidentiality
control
appropriate
mechanism
non-discrimination
party
infrastructure
sharing
law
function
effectiveness
state
fundamental
efficiency
Member
continuity
actor
application
implementing
financial
provider
data
directive
practices
authentication
good
coherence
integrity
assessment
attack
competent
consumer
investigate
exchange
team
freedom
act
platform
processing
measures
measure
obligation
review
States
business
report
third
management
penalty
access
response
non-repudiation
national
best
essential
critical
entry
society
personal
body
reporting
regulatory
notify
system
public
plan
administrative
Union
breach
organizational
impact
international
risk
authority
harmonization
coordination
force
technical

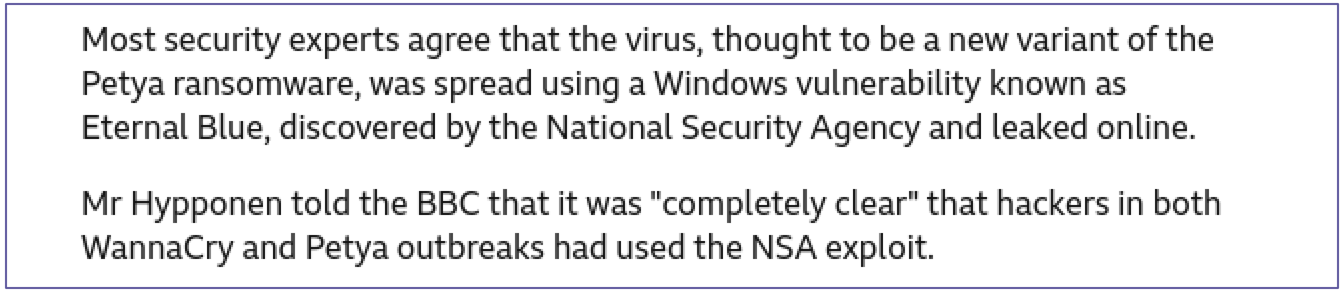
Third-party Code Repository Compromise



$870,000,000	Pharmaceutical company Merck
$400,000,000	Delivery company FedEx (through European subsidiary TNT Express)
$384,000,000	French construction company Saint-Gobain
$300,000,000	Danish shipping company Maersk
$188,000,000	Snack company Mondelēz (parent company of Nabisco and Cadbury)
$129,000,000	British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)

$10 billion

Total damages from NotPetya, as estimated by the White House



Most security experts agree that the virus, thought to be a new variant of the Petya ransomware, was spread using a Windows vulnerability known as Eternal Blue, discovered by the National Security Agency and leaked online.

Mr Hypponen told the BBC that it was "completely clear" that hackers in both WannaCry and Petya outbreaks had used the NSA exploit.

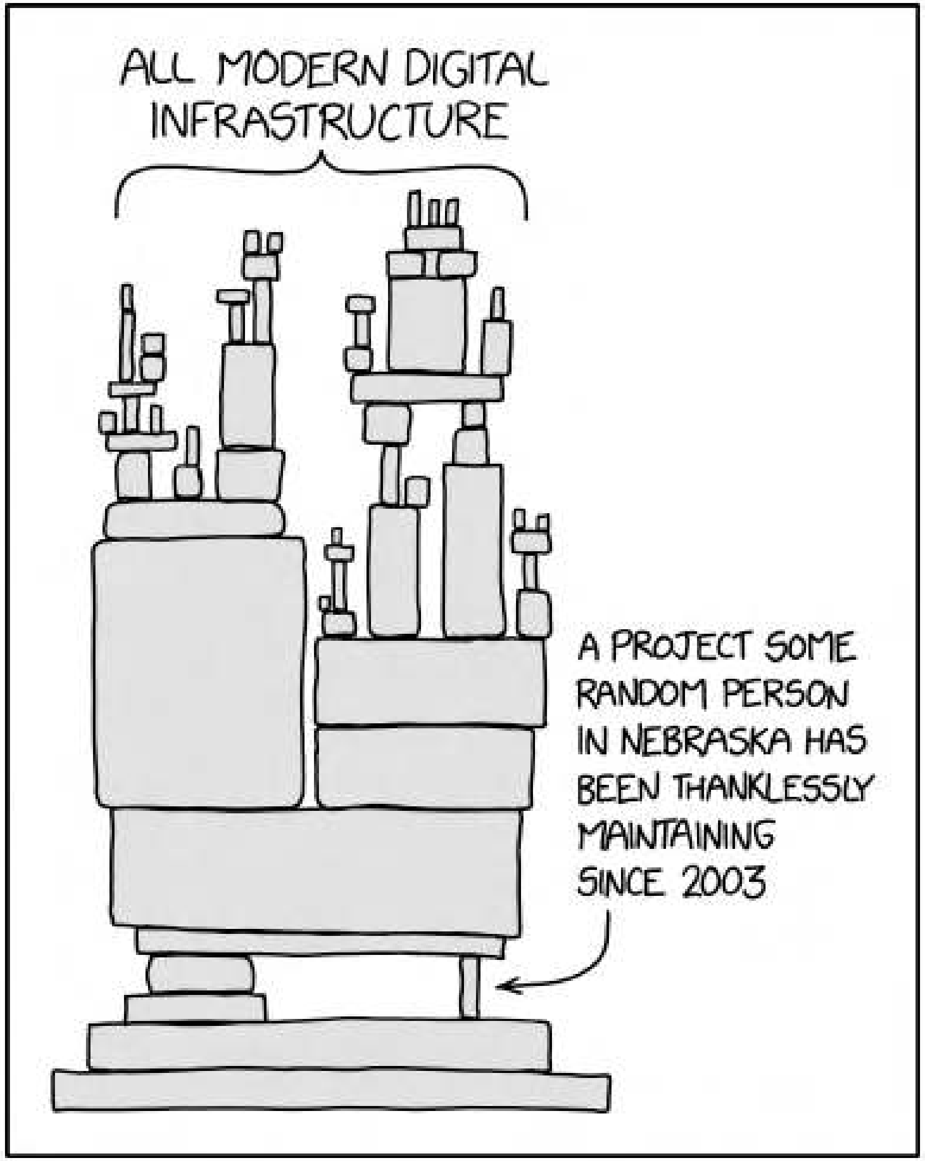
SolarWinds (2020)

SonicBee

Third-party Code Repository Compromise

open source

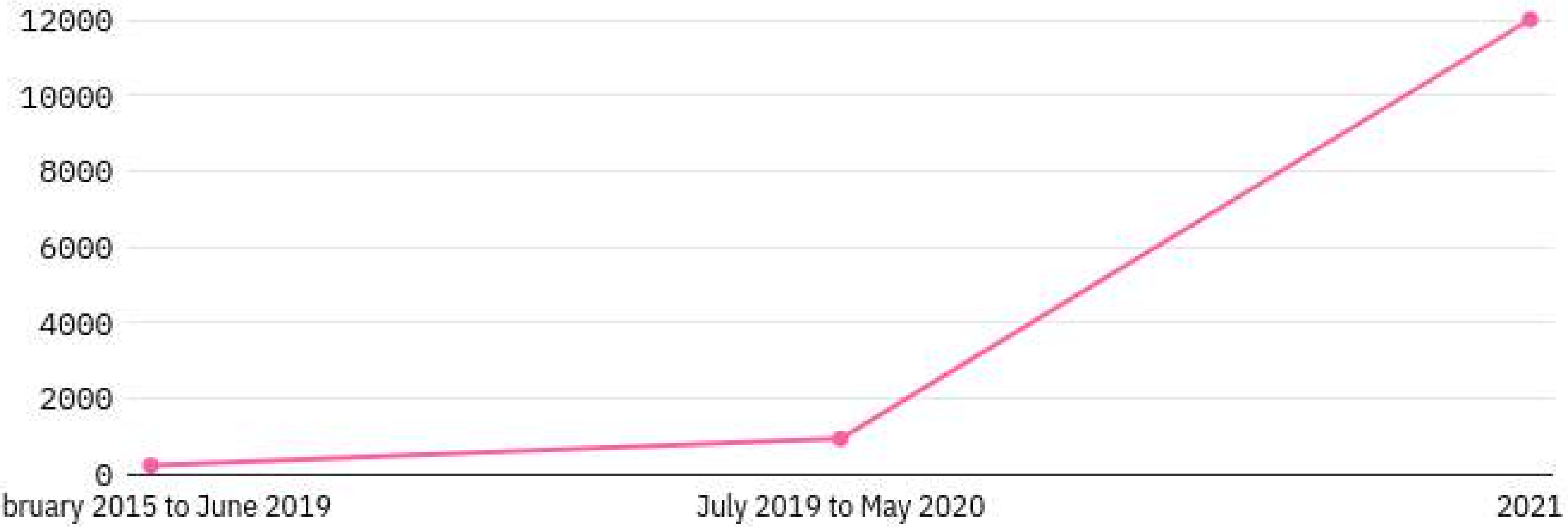
- Drupalgeddon
- Apache Struts
- PHPMyAdmin
- ...


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Third-party Code Repository Compromise

Supply chain attacks on open source software packages increased by 650% in 2021

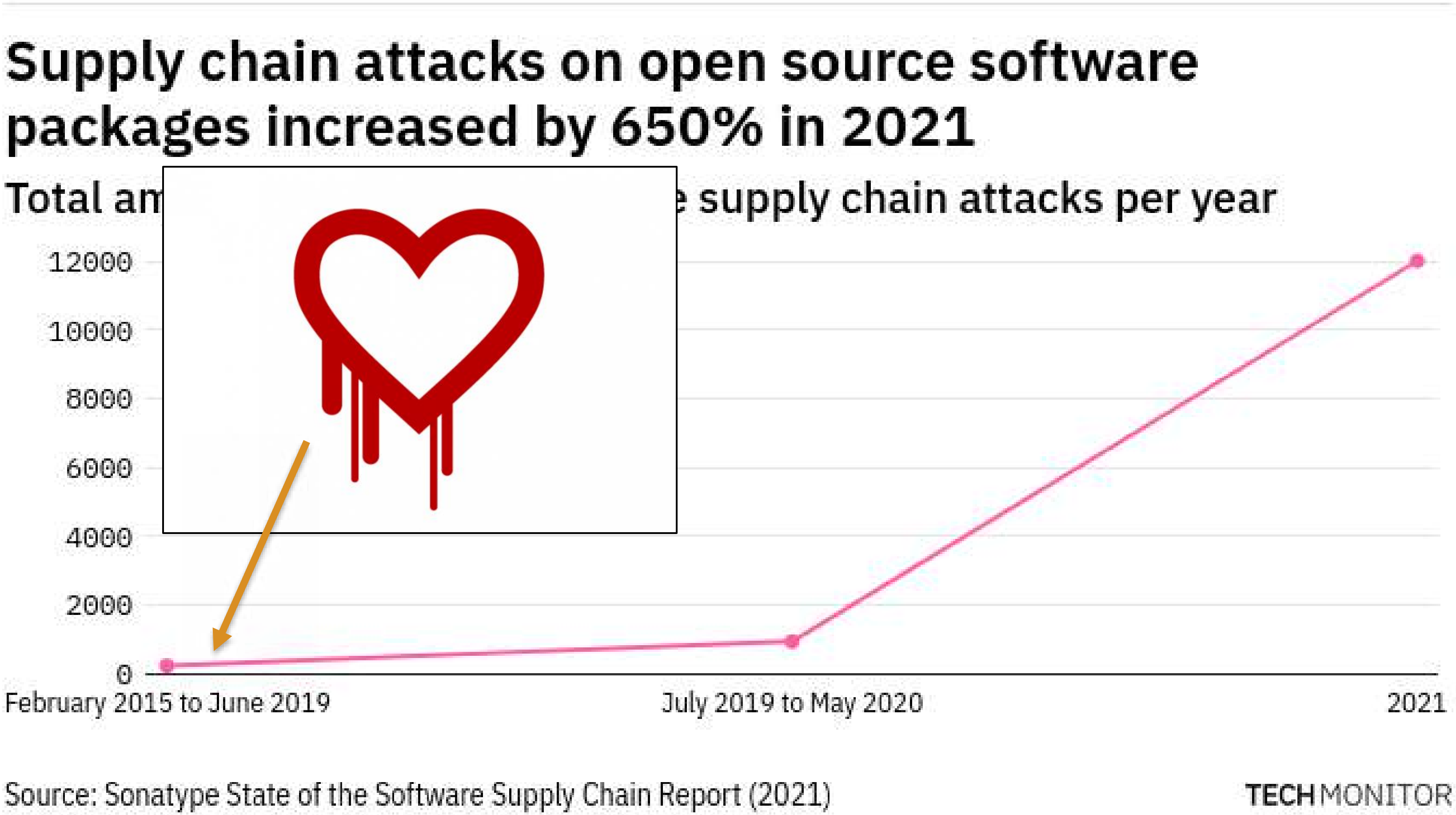
Total amount of recorded software supply chain attacks per year



Source: Sonatype State of the Software Supply Chain Report (2021)

TECH MONITOR

Third-party Code Repository Compromise



Supply chain attacks on open source software packages increased by 650% in 2021

Total am e supply chain attacks per year

Source: Sonatype State of the Software Supply Chain Report (2021)

TECH MONITOR

SonicBee

Lack of controls: NIS2

Why NIS2?

We already have...

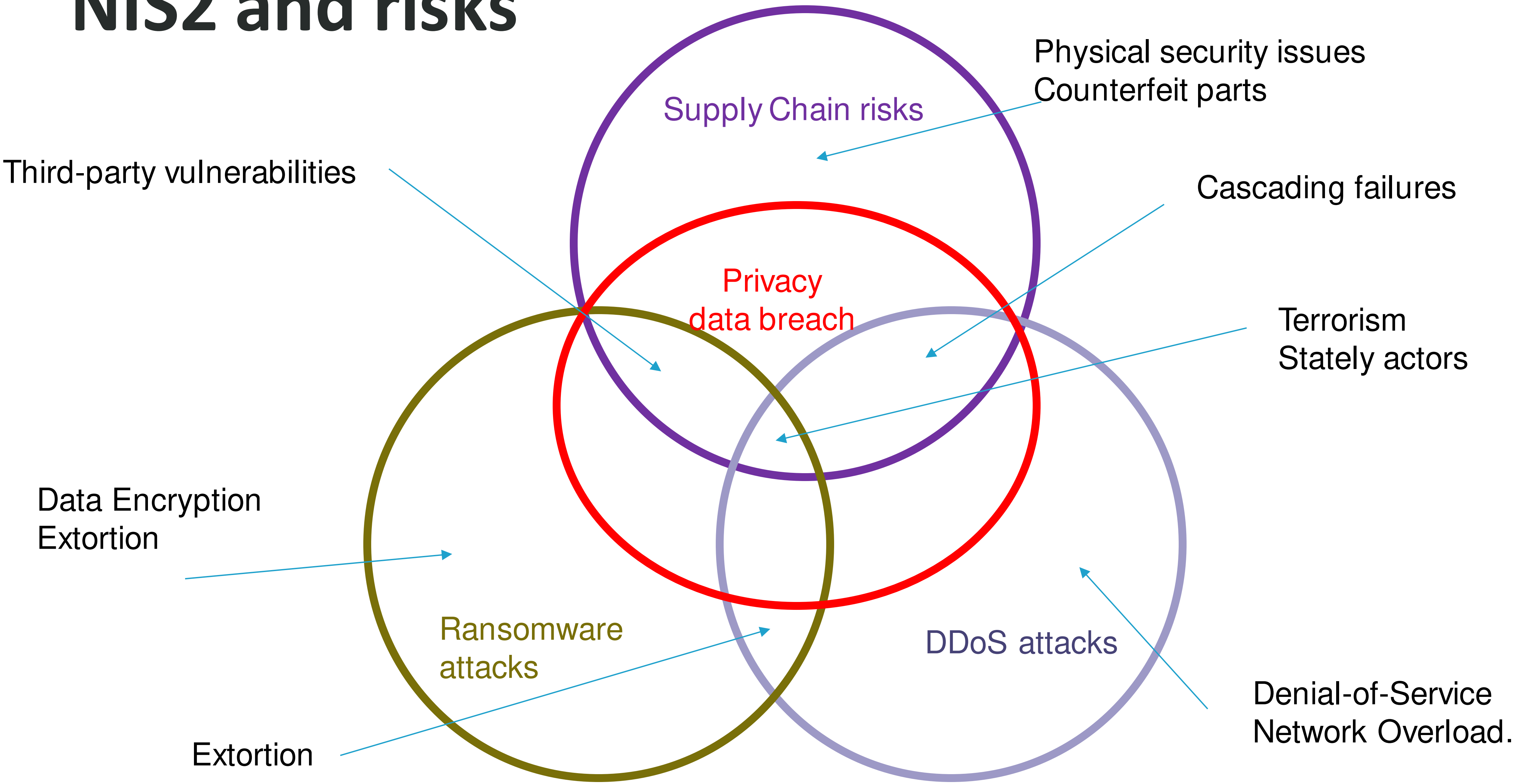
- NIS
- ISO27K
- GDPR
- NIST

NIS2

The EU's new cybersecurity legislation

- Aims to **improve** cyber resilience of essential entities
- **Broadens** the scope to include more sectors
- Introduces **stricter** reporting requirements

NIS2 and risks



NIS2 and IAM

While NIS2, ISO27002, NIST and GDPR all touch upon Identity and Access Management (IAM) from different perspectives, they share a common goal: securing access to critical information. Here's a breakdown of how each one approaches IAM:

NIS2: NIS2 has a specific set of requirements focused on access governance to mitigate cybersecurity risks for essential entities. It mandates enforcing least privilege, encourages the use of MFA, and emphasizes the need for robust IAM solutions.

NIS2 and the others

NIS2 versus ISO / NIST

1. Focus:

- NIS2 is a **regulatory framework**
- ISO27000 and NIST are **voluntary** families of international standards providing **best practices** for information security management.

NIS2 versus ISO / NIST

2. Prescriptiveness:

- NIS2 takes a **prescriptive** approach
- ISO / NIST is **recommending best practices**

NIS2 versus ISO / NIST

3. Enforcement:

- NIS2 is **enforced by member states** of the European Union.
- ISO27000 / NIST are a **voluntarily** framework and organizations can **seek certification**

NIS2 versus ISO / NIST

4. Scope:

- NIS2 applies to a specific set of **essential entities**
- ISO27000 / NIST is applicable to **any organization**

NIS2 versus ISO / NIST

5. Cost:

- Compliance with NIS2 may require **significant investments**

- The cost of implementing NIST / ISO27000 **can vary,** based on scope and risk appetite and (for ISO) need for certification

NIS2 versus ISO / NIST

Relationship:

- NIS2 **complements** ISO / NIST by providing a more specific set of requirements for essential entities.
- Organizations can use the ISO / NIST to implement controls and practices that **align** with NIS2 requirements

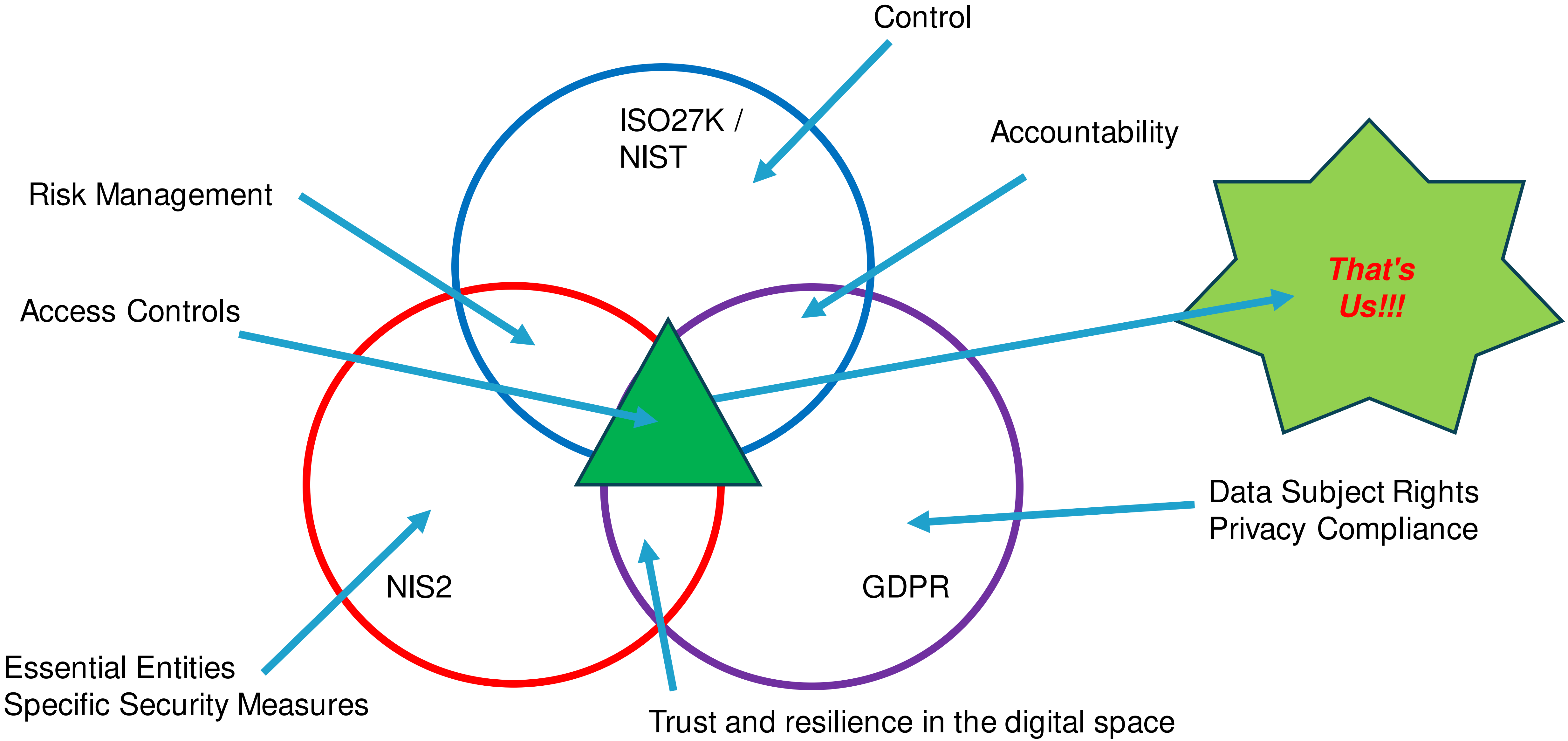
NIS2 versus the World

No real global equivalence, but there are:

- US: The Cybersecurity Act of 2015 (SCA):
  encourages the development of voluntary cybersecurity frameworks within critical infrastructure sectors.
- UK
  The Network and Information Systems Regulations 2018, based on the original EU NIS Directive
- Australia
  The Essential Eight Maturity Framework
- Singapore
  The Cybersecurity Act 2018
- Japan
  The Act on the Protection of Information Technology Infrastructure (2014)

SonicBee

NIS2 and the others



SonicBee

NIST, ISO and IAM

ISO 27K

- ISO 27001 doesn't explicitly define IAM, but it incorporates relevant access control requirements.
- Annex A.9 of ISO 27001 specifically addresses access control, including:
  - User provisioning and de-provisioning
  - Password complexity and management
  - Access rights review and authorization
  - Managing special access rights

NIST SP800-63

NIST SP 800-63 is a comprehensive guide to digital identity management, covering topics such as enrollment, authentication, and lifecycle management.

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST IAM roadmap

Identifies key objectives NIST aims to achieve in the coming years. These include:

- Accelerating the adoption of mobile driver's licenses and user-controlled digital identities.
- Expanding and improving biometric and identity measurement programs.
- Promoting technologies for secure and privacy-preserving attribute verification.
- Enhancing fraud mitigation and secure identity proofing methods.
- Modernizing Multi-Factor Authentication (MFA) practices.
- Updating federal guidelines and infrastructure for Personal Identity Verification (PIV).

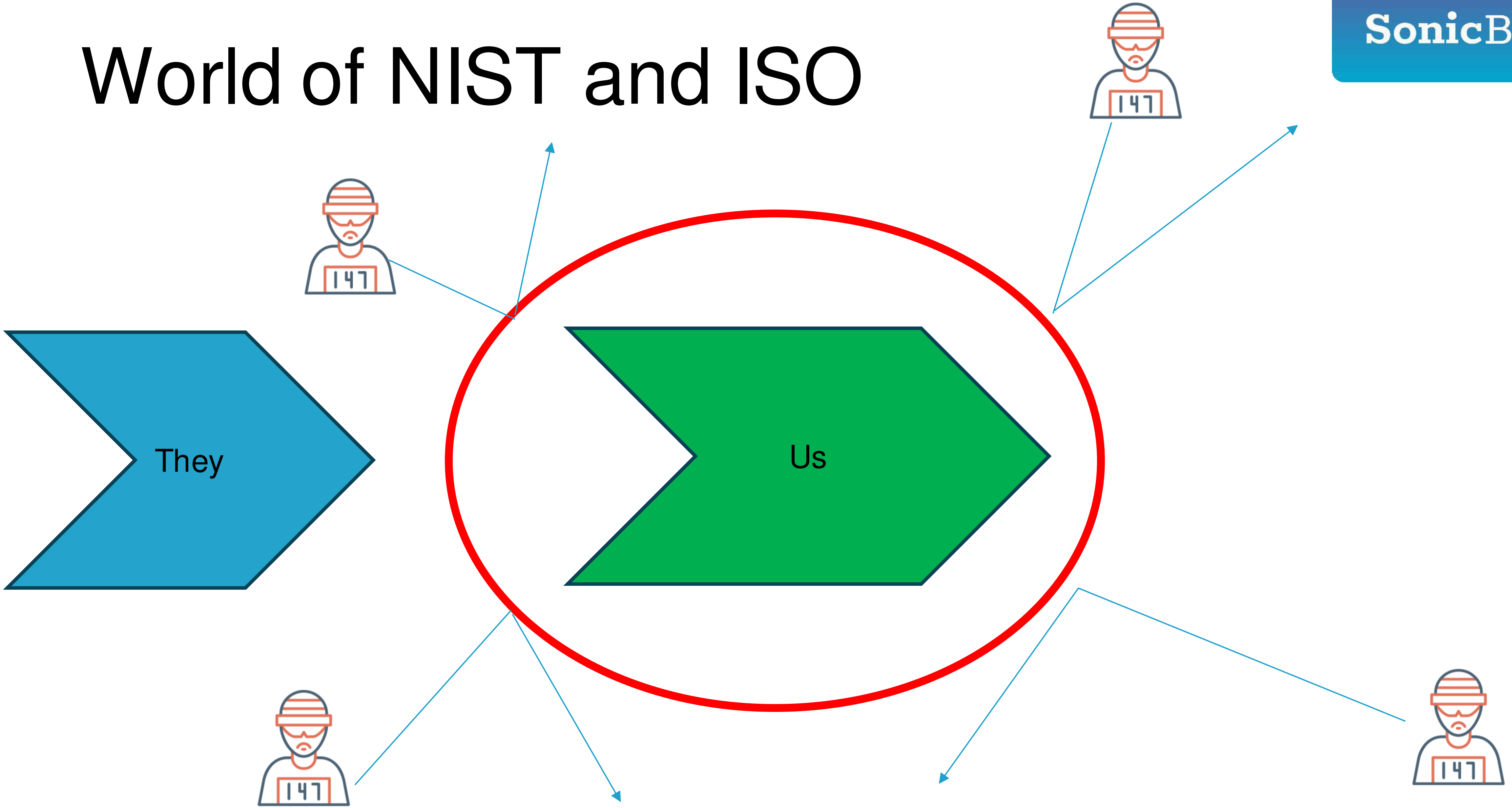
ISO and NIST

Both ISO and NIST emphasize core IAM principles:

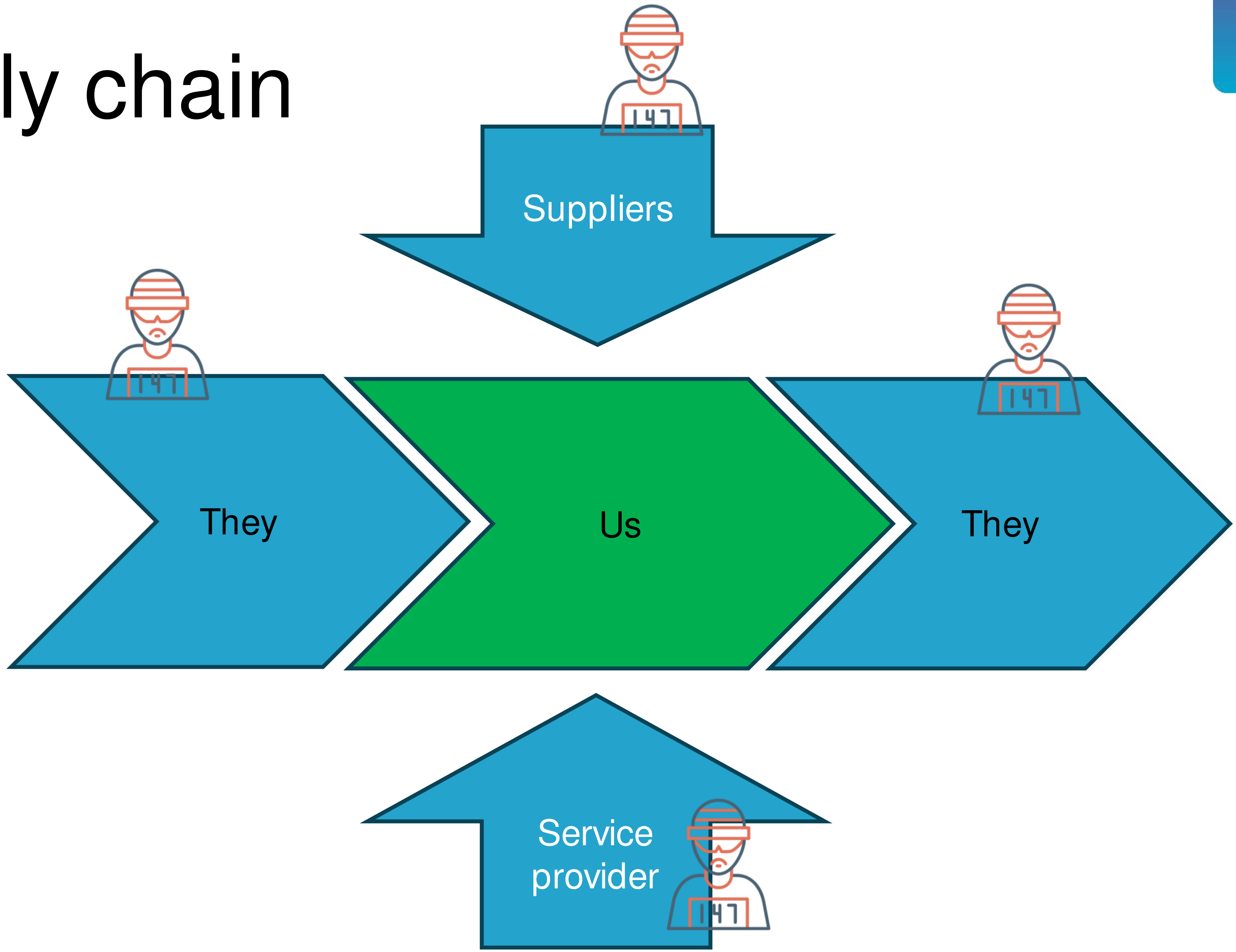
- Accountability: Holding users responsible for their access and actions.
- Least privilege: Granting only the minimum access rights necessary for a user's role.
- Separation of duties: Distributing critical tasks among multiple users to reduce risk.

World of NIST and ISO

SonicBee



Supply chain



SonicBee

NIS2 and IAM

SonicBee

The directive and Access

Consideration 49: Administrator accounts and Privileged Access Management
Consideration 79: Personnel security and a fitting access control policy
Consideration 85: Chain partners, more specific service providers
Consideration 89: Zero trust … and IAM...

- ISP's, DNS, Consideration 98, 99 en 100

Art 21, measures
Par 2:The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following::
...

- ❖ d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- ❖ i) human resources security, access control policies and asset management

...

SonicBee

Privileged Access Control

Consideration 49

...Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application security, and business or end-user data upon which entities rely. Cyber hygiene policies comprising a common baseline set of practices, including software and hardware updates, password changes, the management of new installs, ***the limitation of administrator-level access accounts***...

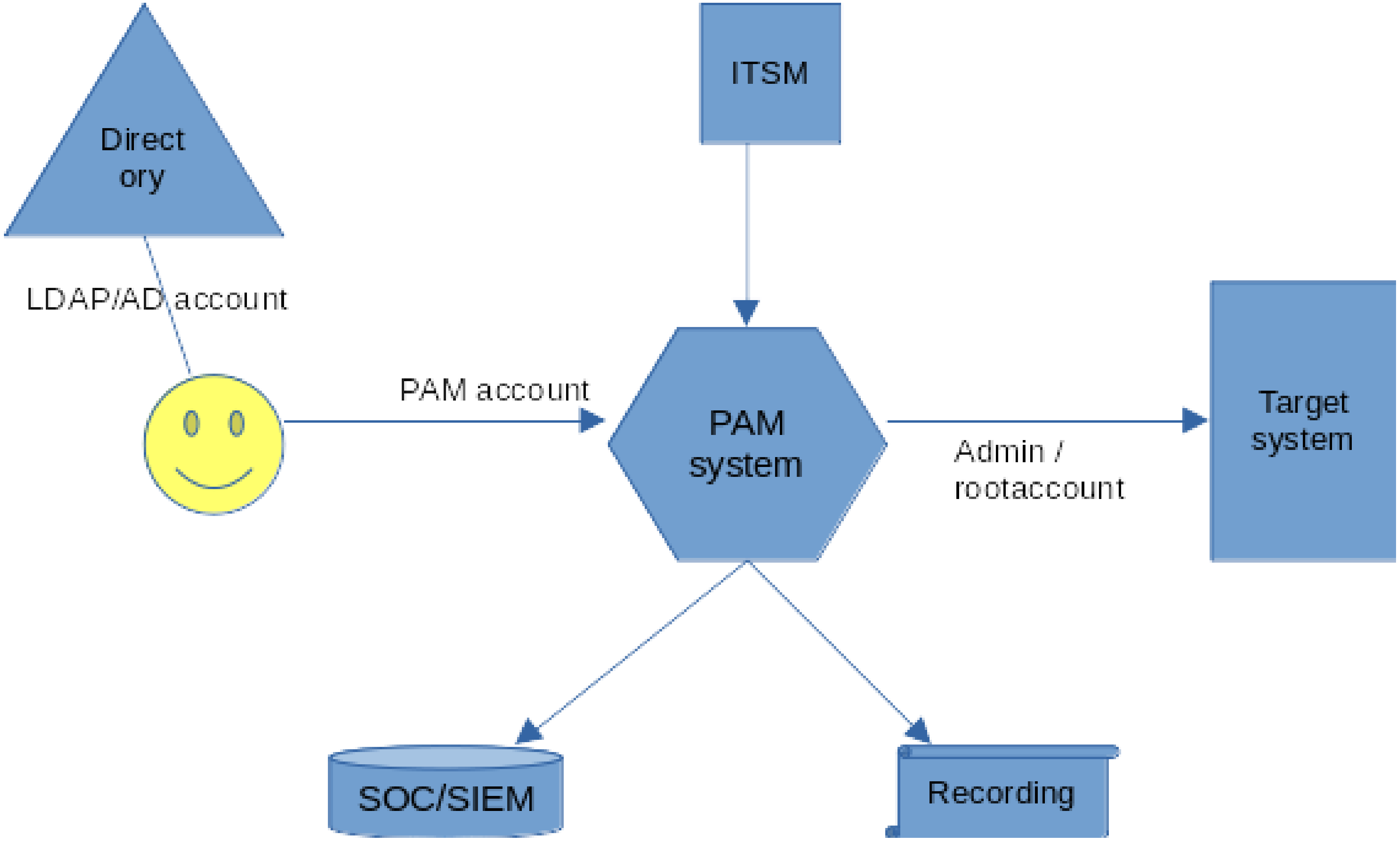
PAM: NIS2 and the others

- **NIS2**: While NIS2 doesn't explicitly mandate PAM, it strongly encourages robust access governance practices. Considering that many cyberattacks target privileged accounts, implementing PAM to safeguard these accounts aligns well with NIS2's objectives.

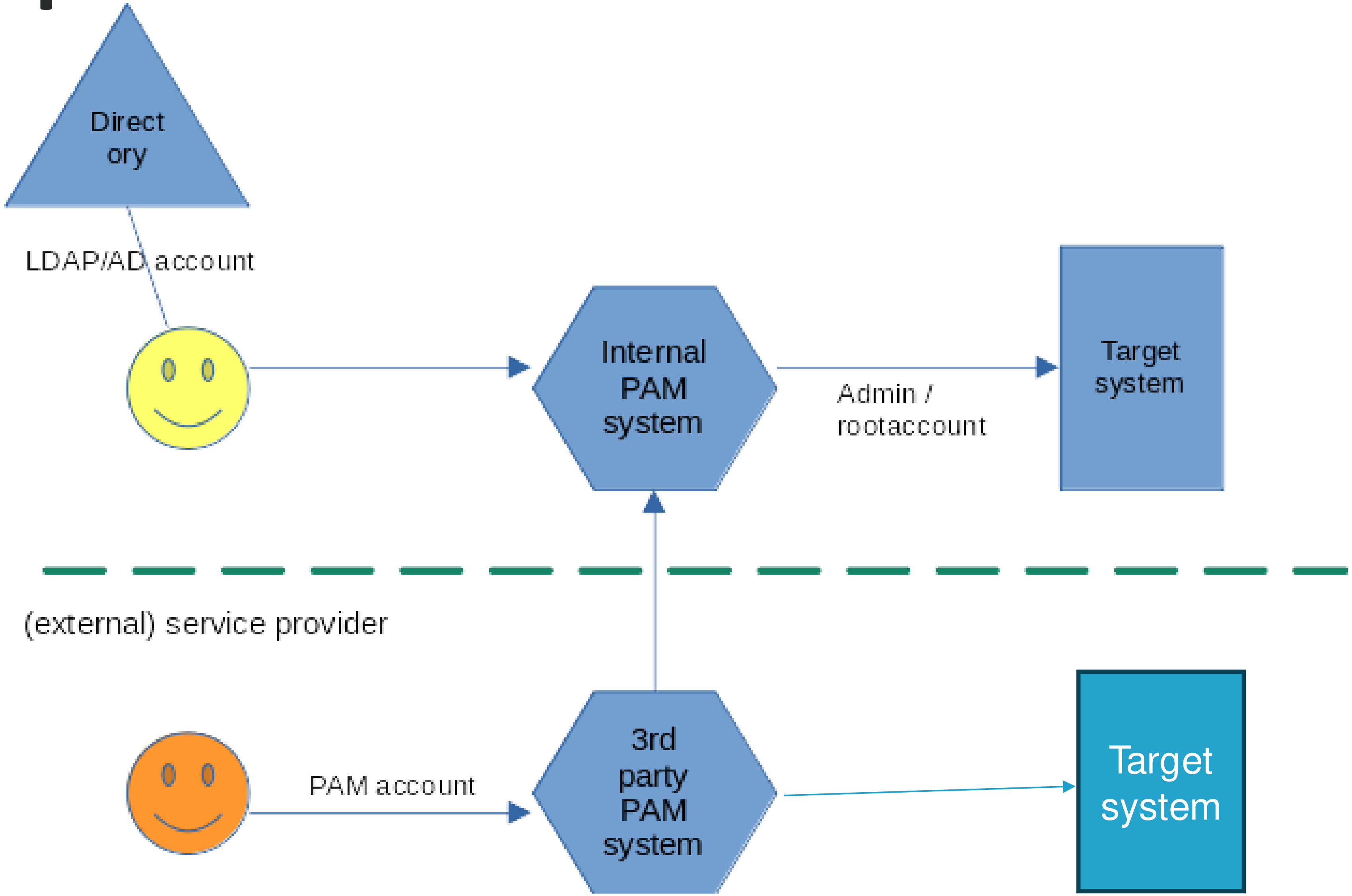
- **ISO27002**: Similar to NIS2, ISO27002 focuses on access control for all user accounts but emphasizes the importance of stricter controls for privileged accounts. PAM solutions directly address this by providing features like least privilege enforcement, session monitoring, and privileged password vaulting.

- **GDPR**: The GDPR doesn't directly regulate PAM, but since PAM can help secure access to personal data, it indirectly contributes to GDPR compliance. By implementing PAM to control and monitor privileged access to personal data, organizations can minimize the risk of data breaches and unauthorized access.

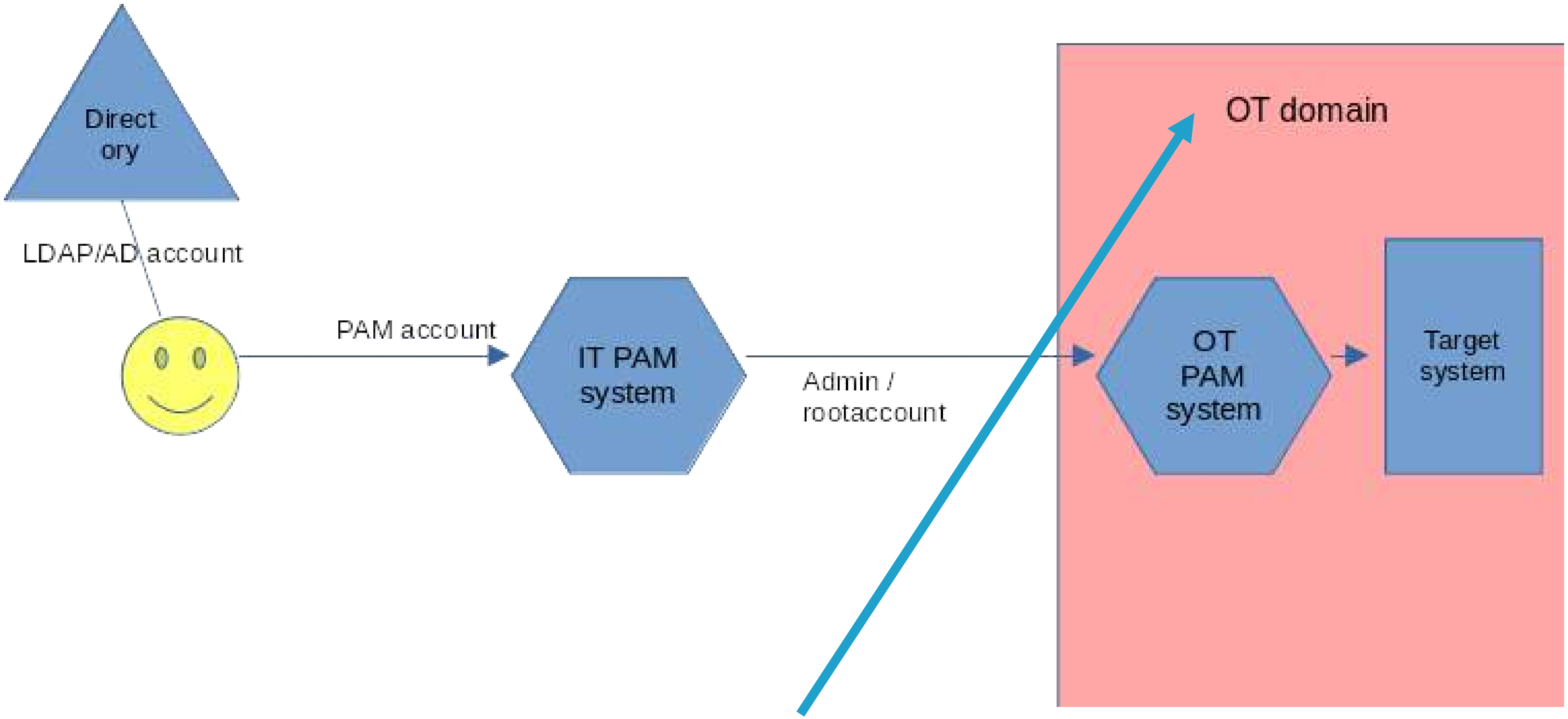
PAM


ITSM
Direct
ory
LDAP/AD account
PAM account
PAM
system
Target
system
Admin /
rootaccount
SOC/SIEM
Recording

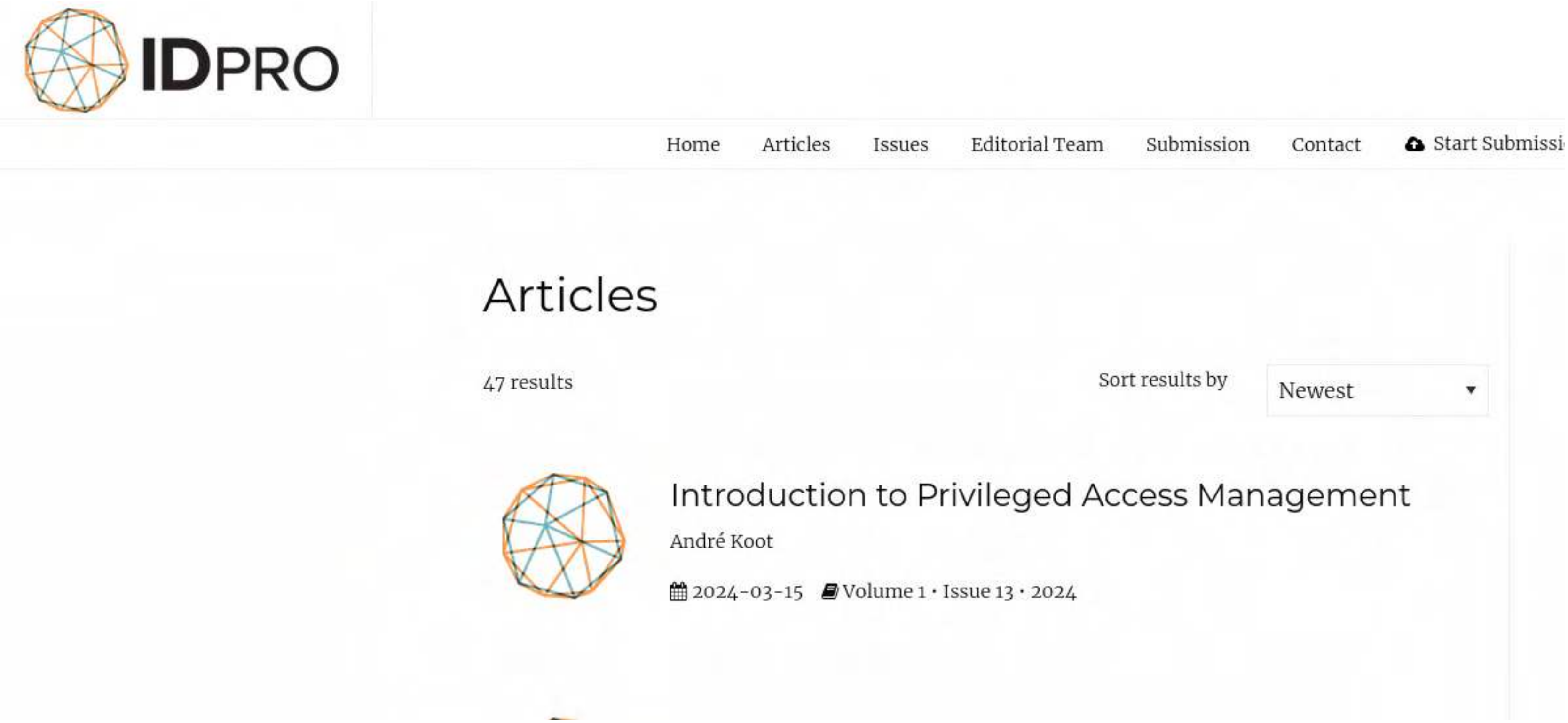
PAM 3rd parties



PAM-PAM



Essential Entities



Articles

47 results

Introduction to Privileged Access Management

André Koot

2024-03-15 Volume 1 · Issue 13 · 2024

https://bok.idpro.org/article/id/101/

Identity and Access Management

Consideration 89

Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, ***identity and access management*** or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques...

Consideration 89

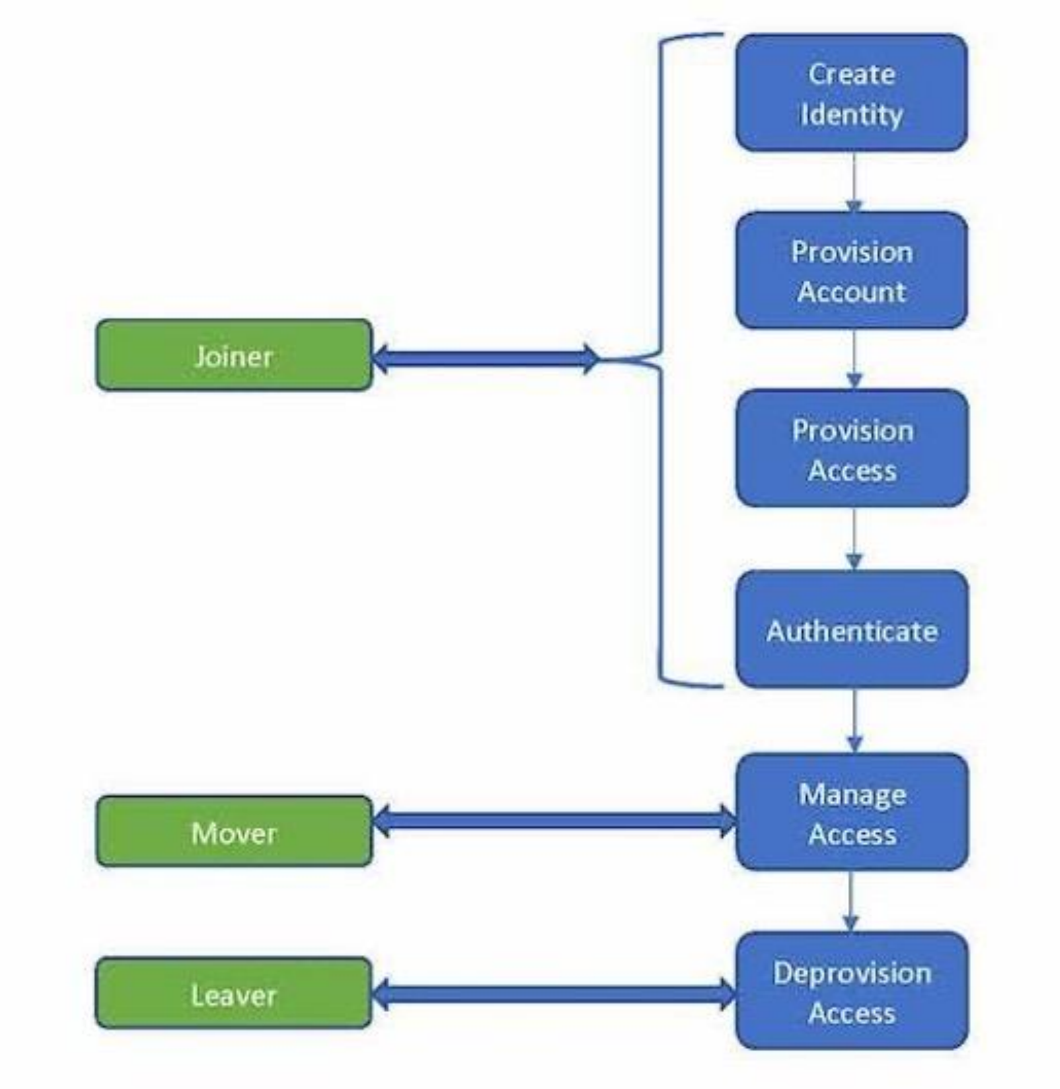
Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management ***or user awareness***, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques...

Identity and Access Management

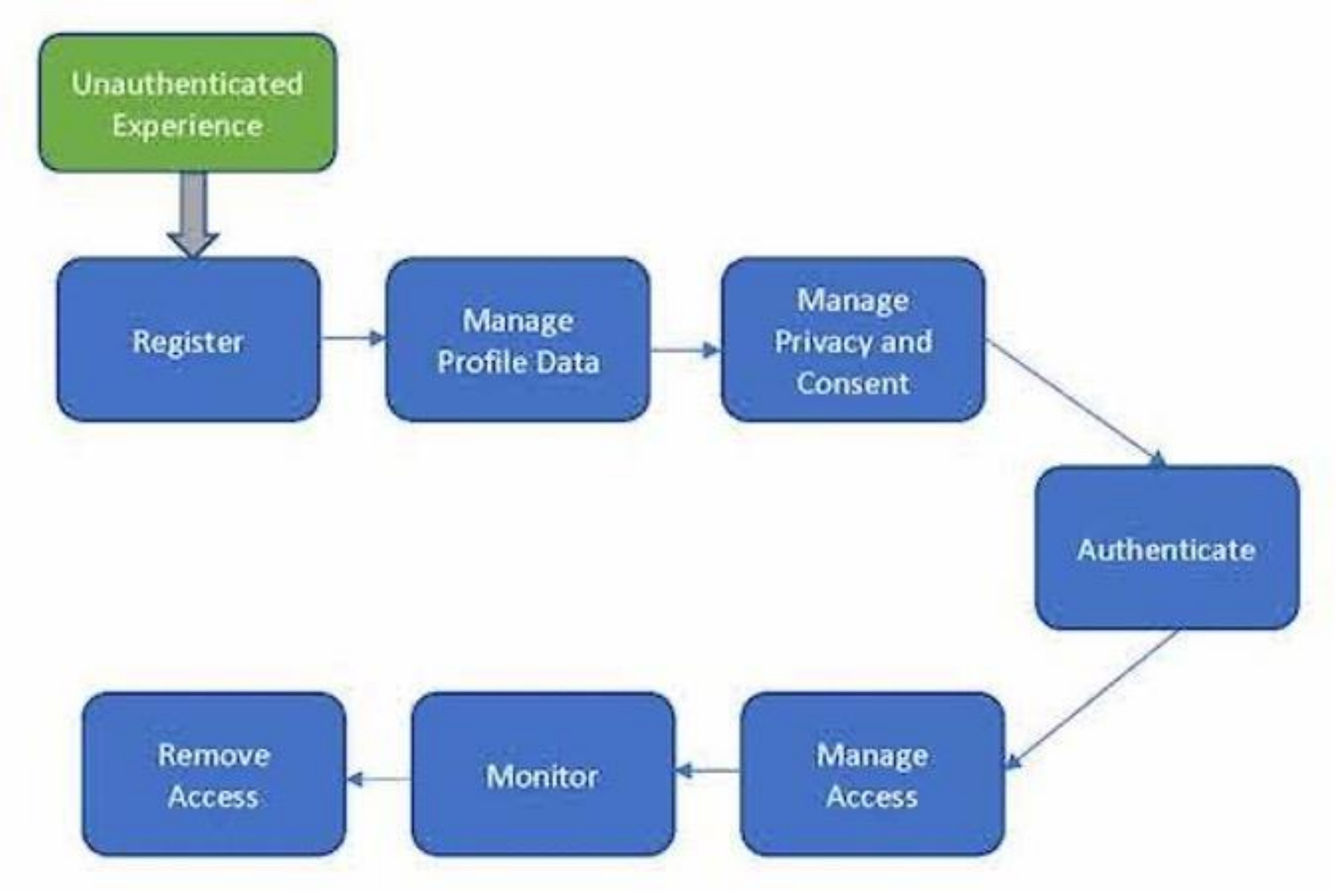
All about:

- Identity lifecycle management: joiner, mover and leaver workflows
  - Own employees, extenals
  - Third parties, vendors/suppliers, chainpartners, customers, devices...
- Authorization management
  - RBAC, role based access control
  - Dynamic access control
    - ABAC, PBAC, xBAC
    - >>> zero trust architecture
- Governance and compliance
  - Rapporting, logging and monitoring

Workforce IAM

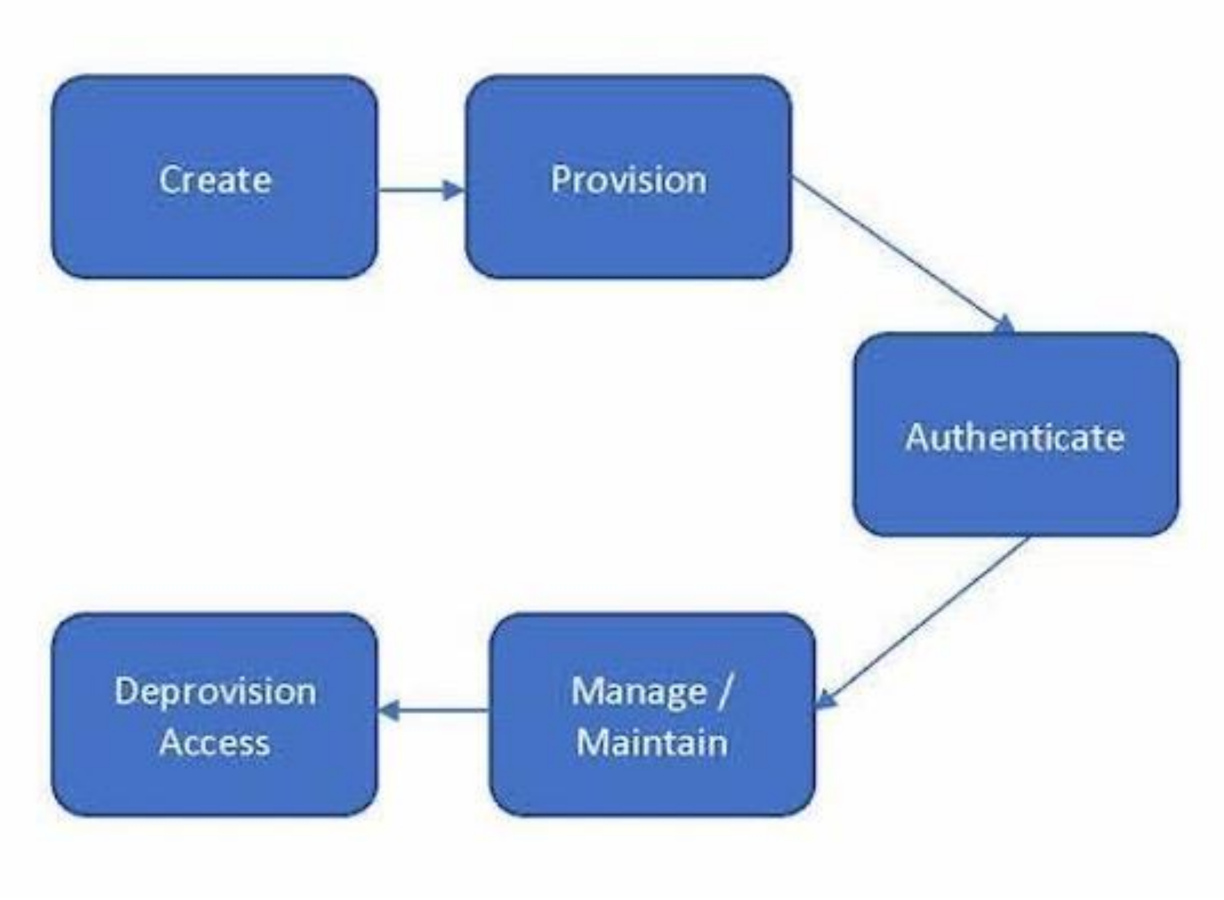


CIAM


Unauthenticated Experience
Register
Manage Profile Data
Manage Privacy and Consent
Authenticate
Manage Access
Monitor
Remove Access

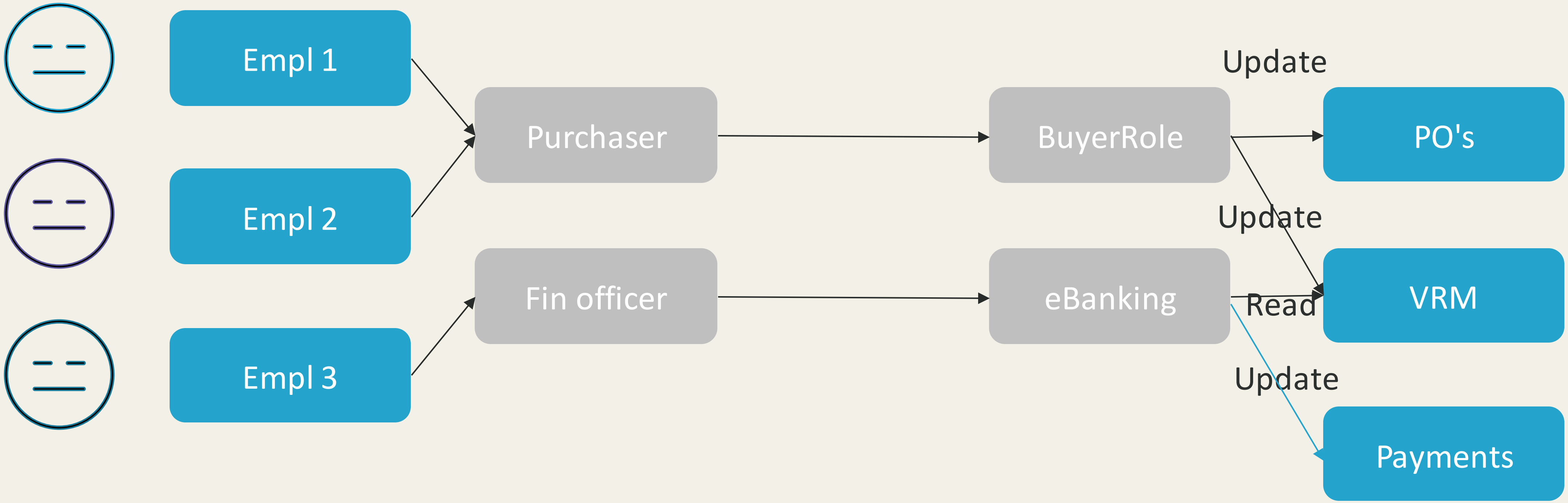
22-5-2024

IoT IAM



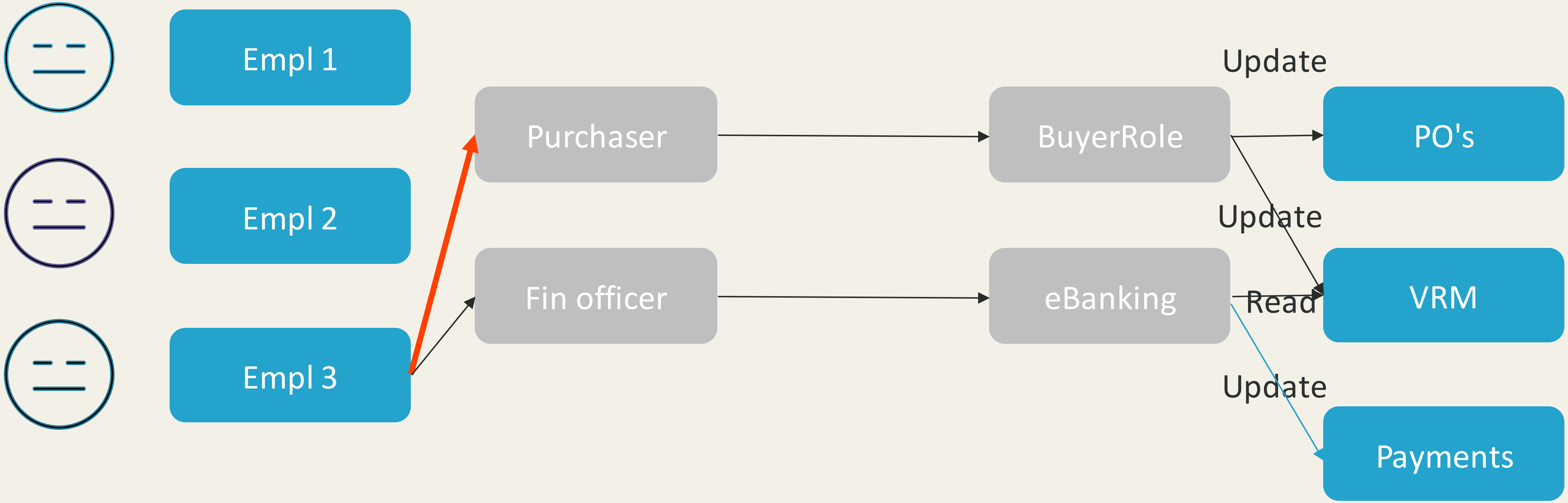
Access Control models

- Role Based Access Control



Access Control models

- Role Based Access Control



RBAC – role hierarchy

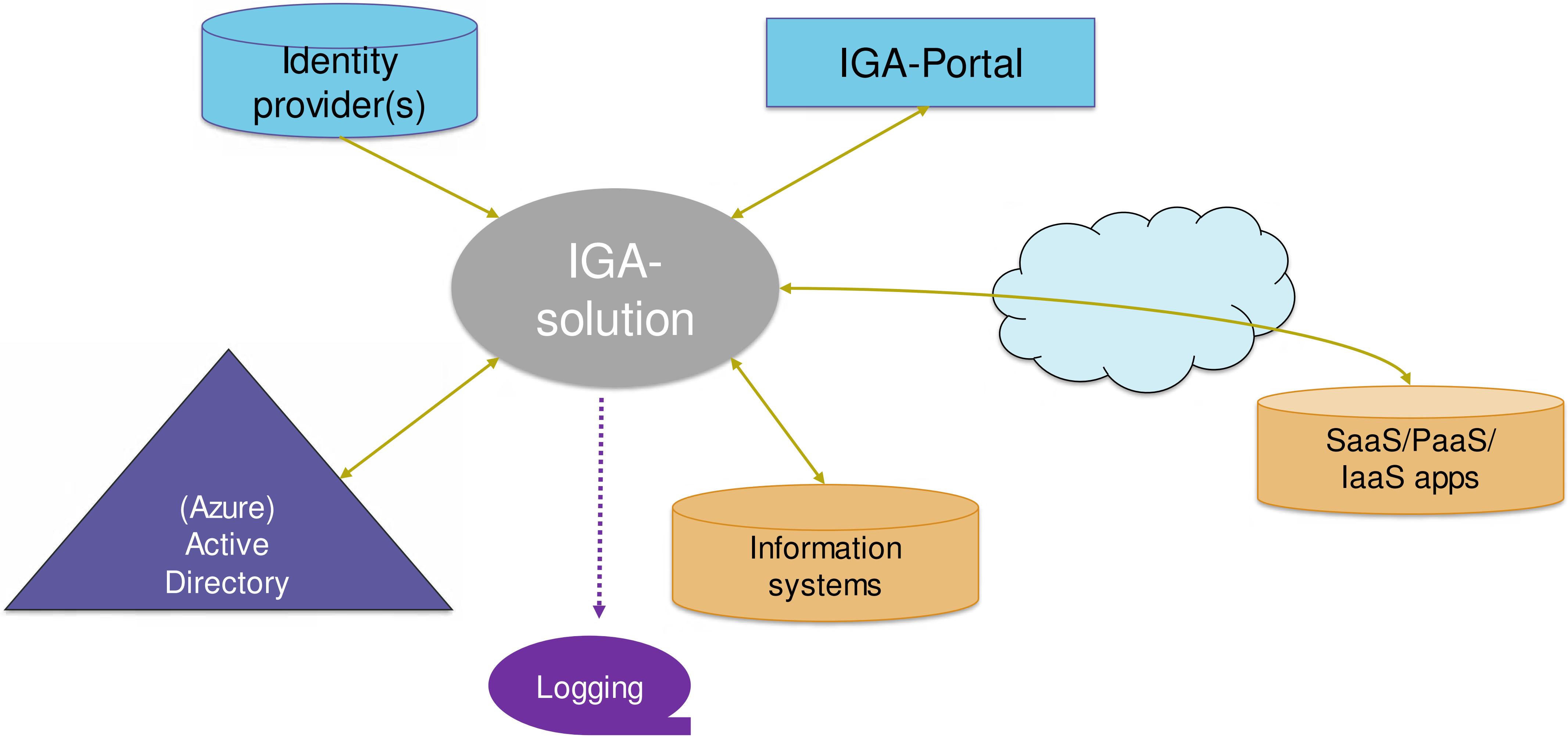
1. Global, or company role
2. Employee type role
3. (potentially) Location role
4. Department role
5. Position, function or process role
6. Specific role (e.g., employee counsel)
7. Specifically assigned authorizations

Birthright roles or authz

Requested or assigned roles or authz

SonicBee

IGA Reference Architecture



Zero Trust

Consideration 89

Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as ***zero-trust principles***, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques...

Why Zero Trust?

Implementing zero trust architecture principles can significantly contribute to achieving the goals of NIS2 by:

- Reducing the attack surface and making it harder for attackers to gain unauthorized access.
- Enhancing the security of privileged accounts.
- Facilitating faster detection and response to security incidents.
- Providing greater visibility and control over the IT environment.

While NIS2 doesn't explicitly mandate zero trust, it strongly encourages robust access control practices that align with zero trust principles.

Why Zero Trust?

1. Reducing Attack Surface:

- Zero Trust Principle: Zero trust assumes all users and devices are potentially untrusted and continuously verifies their access requests. This reduces the attack surface by limiting access to only authorized users and resources, regardless of their location or device.
- NIS2 Relevance: This principle aligns with NIS2's emphasis on stricter access controls and the principle of least privilege. By implementing zero trust, organizations can minimize the potential impact of a successful cyberattack by limiting the attacker's ability to move laterally within the system.

Why Zero Trust?

2. Enhanced Security for Privileged Access:

- Zero Trust Principle: Zero trust requires continuous verification, even for privileged accounts. This prevents attackers from leveraging stolen credentials to gain unauthorized access to critical systems and data.
- NIS2 Relevance: NIS2 places a strong emphasis on protecting privileged accounts, as they pose a significant risk if compromised. Zero trust helps address this concern by requiring additional verification steps even for privileged users.

Why Zero Trust?

3. Improved Incident Response:

- Zero Trust Principle: By continuously monitoring and verifying access, zero trust can help detect suspicious activity faster, allowing organizations to respond to incidents more effectively.
- NIS2 Relevance: NIS2 mandates reporting of certain cybersecurity incidents. Faster detection through zero trust can lead to faster reporting and mitigation of incidents, minimizing their impact.

Why Zero Trust?

4. Increased Visibility and Control:

- Zero Trust Principle: Zero trust provides organizations with a more comprehensive view of user and device access attempts, allowing for better monitoring and control of their IT environment.
- NIS2 Relevance: NIS2 requires organizations to have a clear understanding of their cybersecurity risks and implement appropriate controls. Zero trust can assist in achieving this by providing valuable insights into access patterns and potential vulnerabilities.

Zero trust concept

NIST SP800-207

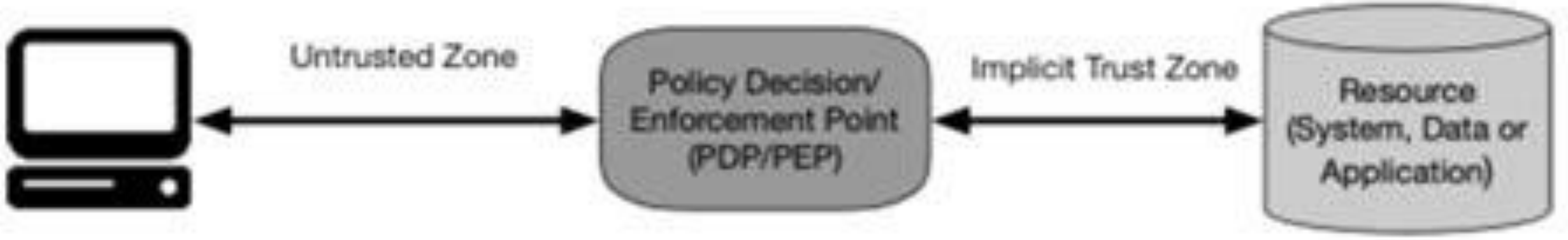

Untrusted Zone
Policy Decision/ Enforcement Point (PDP/PEP)
Implicit Trust Zone
Resource (System, Data or Application)

Figure 1: Zero Trust Access

NIST SP800-207

Decomposition of Access

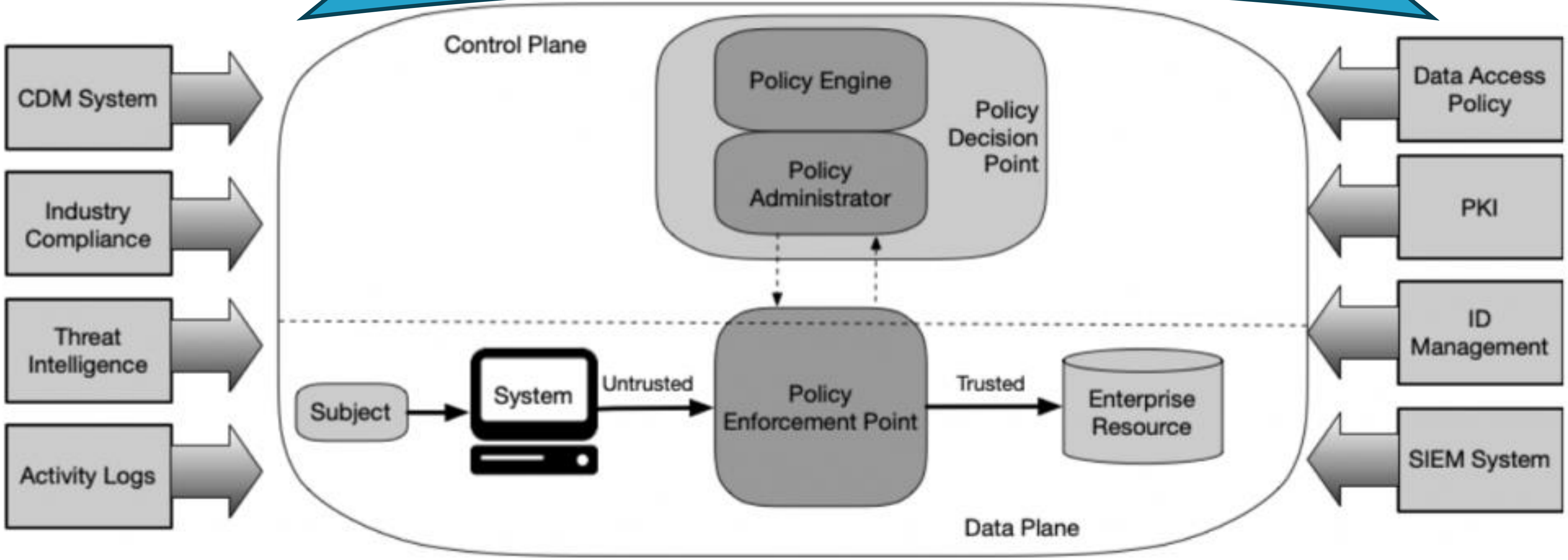
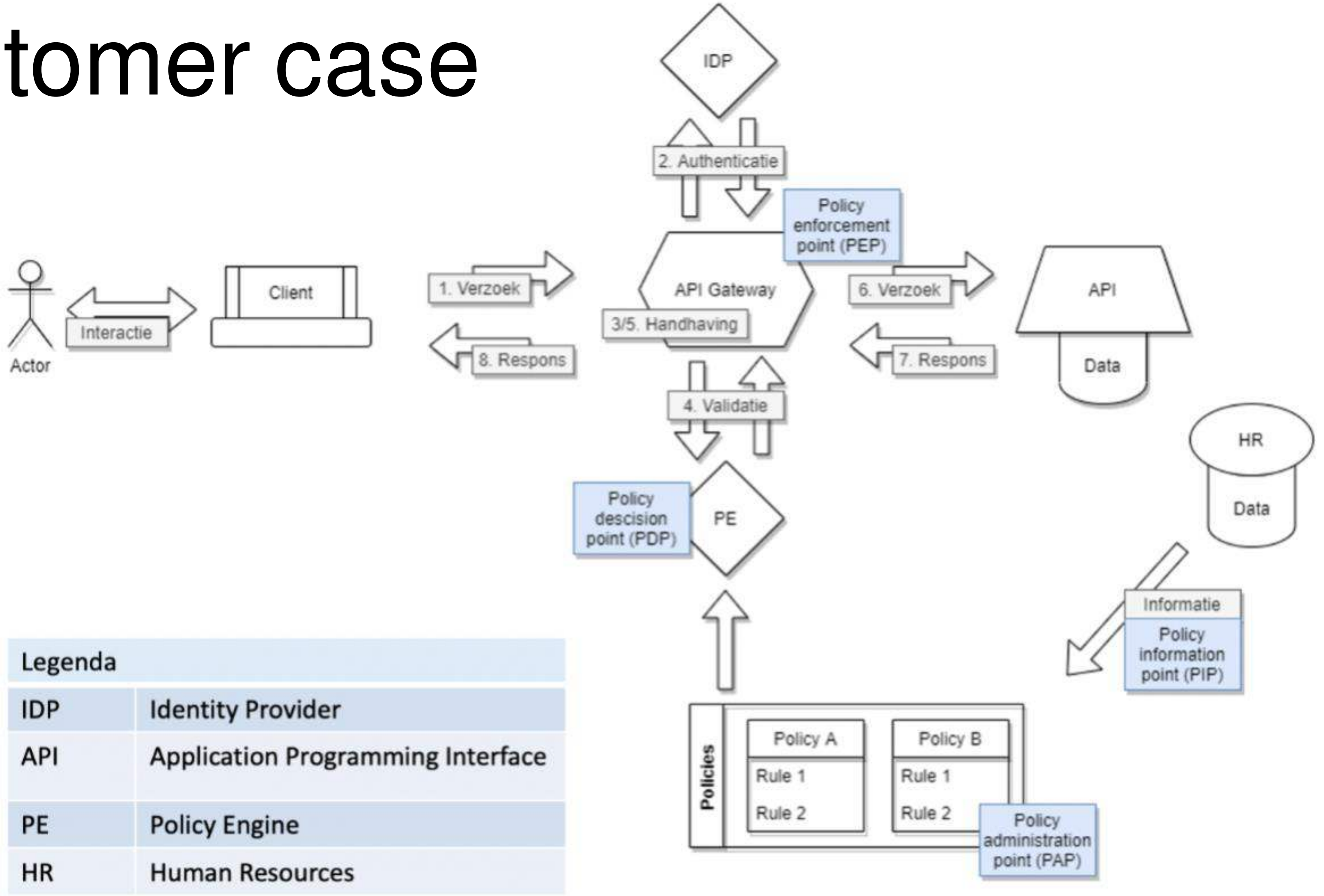


Figure 2: Core Zero Trust Logical Components

Customer case



Legenda	
IDP	Identity Provider
API	Application Programming Interface
PE	Policy Engine
HR	Human Resources

SonicBee

Access Governance

The directive and Access

Consideration 49: Administrator accounts and Privileged Access Management
Consideration 79: Personnel security and a fitting access control policy
Consideration 85: Chain partners, more specific service providers
Consideration 89: Zero trust … and IAM...

- ISP's, DNS, Consideration 98, 99 en 100

Art 21, measures

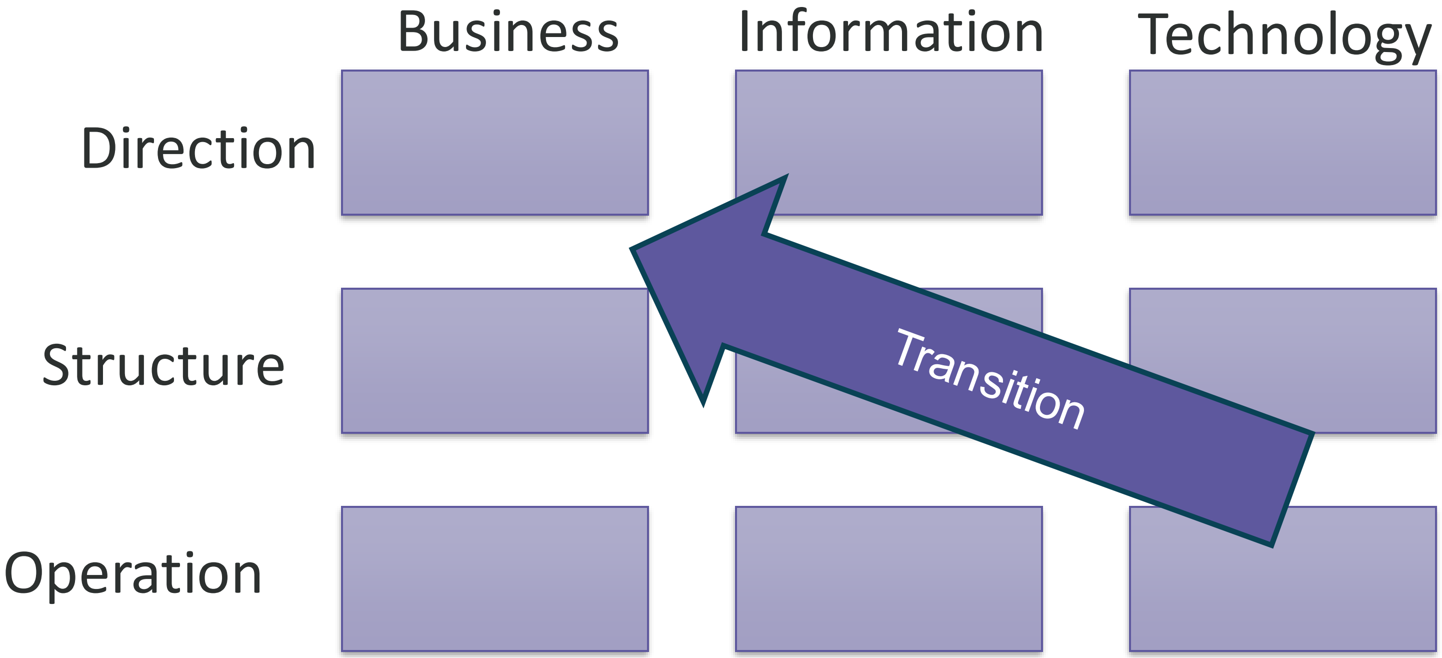
Par 2:The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following::

...

- d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- i) human resources security, access control policies and asset management

...

Amsterdam information model



Business

Information

Technology

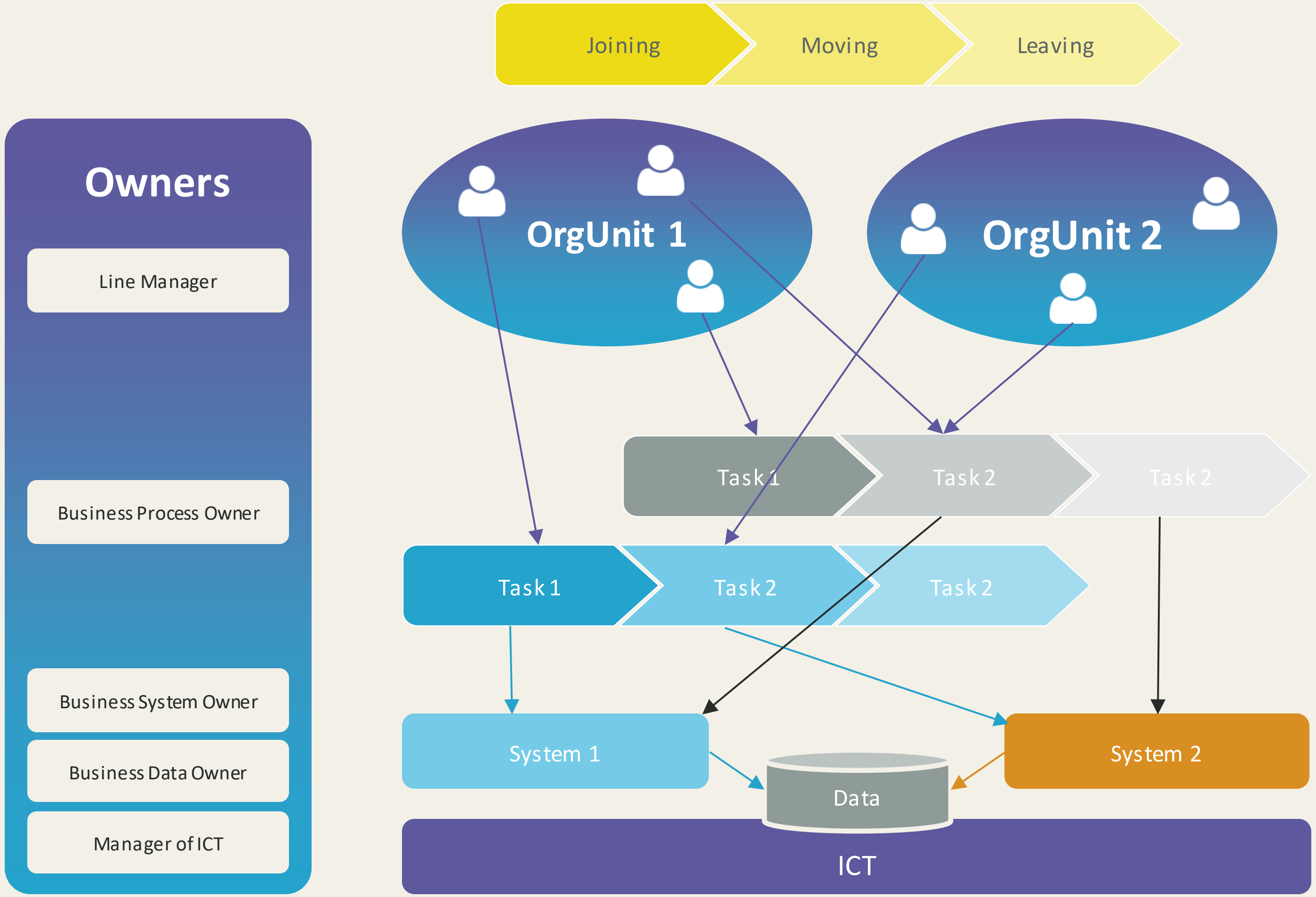
Direction

Structure

Operation

Transition

Stakeholders in Access Governance



SonicBee

Impact of NIS2

NIS2 and IAM

- NIS2 mandates **stricter access governance** practices
- Focus on **least privilege**, MFA, and IAM
- Organizations **need to act now** to ensure compliance
- Improved access governance strengthens overall security posture

NIS2 and IAM

NIS2 **does not explicitly mandate** the implementation of IAM. However:

- NIS2 emphasizes **risk management** for essential entities. Strong IAM is a critical component of effective risk management, as it mitigates unauthorized access risks.
- NIS2 requires entities to take **appropriate technical and organizational measures** to manage security risks. IAM plays a vital role here by ensuring only authorized users have access to sensitive information and systems.

NIS2 and IAM

- NIS2 mandates reporting of cybersecurity incidents. Effective IAM helps identify and respond to incidents faster, as it provides an audit trail of user activity.

While NIS2 doesn't explicitly dictate IAM, fulfilling its requirements **heavily relies on strong IAM practices**.

Any questions?

André Koot
andre.koot@sonicbee.nl
Tel: +31 6 24512021

Han Pieterse
han.pieterse@outlook.com
Tel: +31 6 23759964

Refs

Sources and refs

- https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555&qid=169676906212
- NIST documentatie Zero Trust, SP800-207
- https://github.com/VNG-Realisatie/RAWA
- Amsterdams 9-vlaks model van Rik Maes
- Whitepaper 'identifying stakeholders in access governance'

SonicBee

Thank you for your attention