eu-LISA

NTT DaTa

Active threat management: A holistic approach to ensure cyber-resilience against emerging threats

Industry Roundtable – Cybersecurity for EU Large-Scale IT Systems

Presented by: Notis Iliopoulos, Senior Manager Head of Cyber Security in Benelux

Date: 02/06/2023

Agenda

1. Effectiveness - the missing element of Cyber Security

2. Holistic approach for active threat management

3. The future is now

4. Q&A

Cyber Security @ NTT Group at a glance

4.000 +

Security Specialists, Architects and Engineers across the globe

12 SOCs

And 7 R&D Centers

10.000 +

Clients spanning six continents

40 %

Of internet traffic through NTT's Global Threat Detection Platform

6.2 Billion

Attacks detected and defended against each year

3.5 Trillion +

Logs analyzed annually

Cyber Security Experts

NTT DATA's security expertise is underpinned by NTT Group.

NTT Data is one of only a handful of 'pure play' information security providers and strategic security advisors around the world.

Consistently recognized by the analyst community as providing excellent customer satisfaction, based on the depth of experience and expertise.

NTT DaTa

NTT Group at a glance

$108 billion
Global Revenue

Fortune Global
#83

330,000+
Employees Worldwide

A
S&P Rating

150+ years
Heritage

Top 5
Global IT
Services Provider

Presence in
80+
Countries & Regions

75%
Of Fortune Global
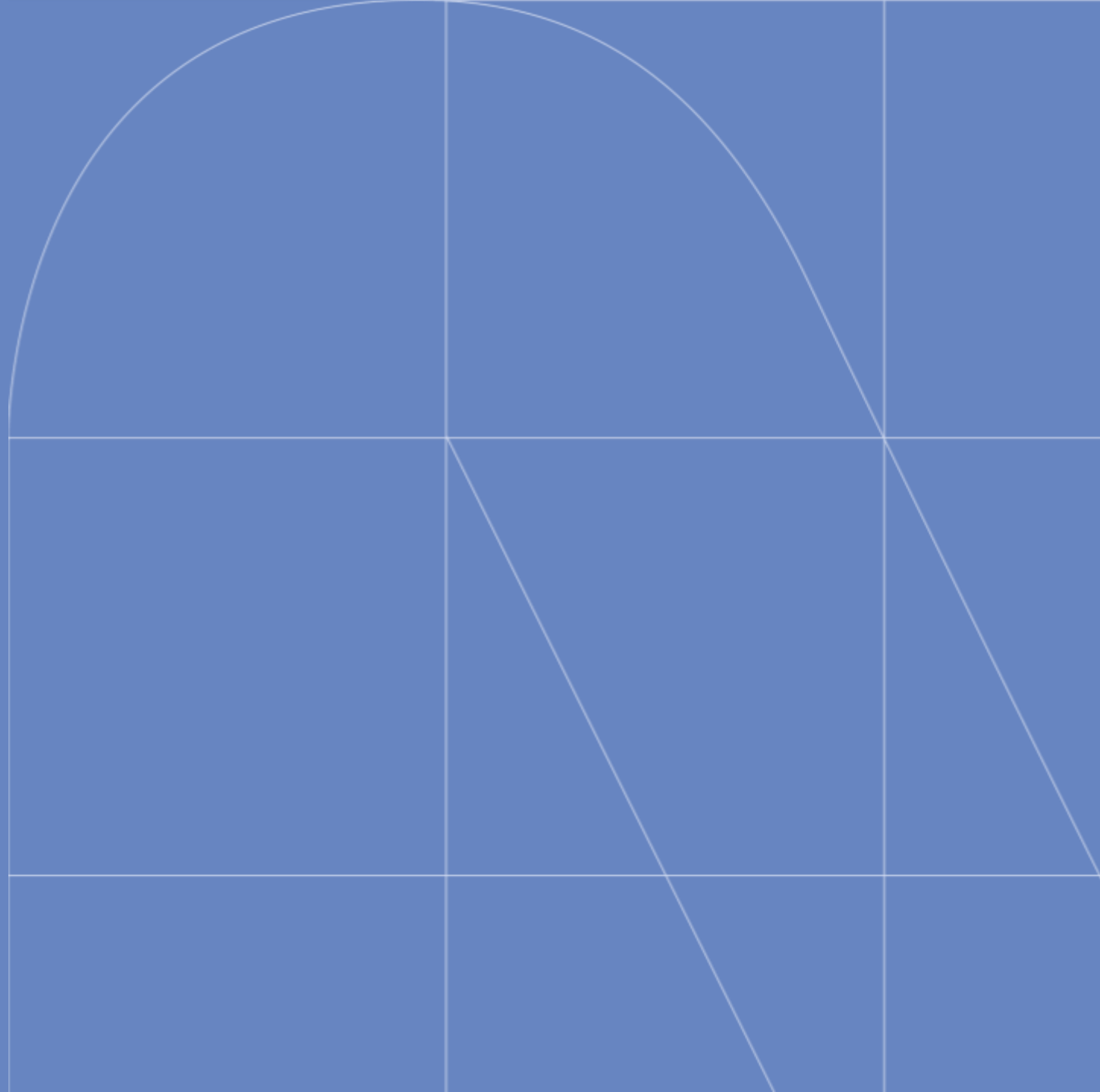100 Are Clients

Global Brand
#41
Brand Finance

As of May 2022
Fortune & Brand Finance ranking: as of January 2023

01

Effectiveness

The missing element of Cyber Security

Cyber security challenges

Convergence of virtual, physical, and digital corporate environments

Digital transformation, automation and transition to the cloud

Adoption of the hybrid working model

Growing regulatory framework

# The awareness has been raised, but we still lack effectiveness

- Overconfident about the level of information security

- Supply chain risk management

- Ineffective cyber security risk management

- Zero Trust Architecture, is not a single product or action, is a philosophy

- The biggest percentage of the cyber security budget is allocated to cyber security solutions ust Architecture

02

Active threat management

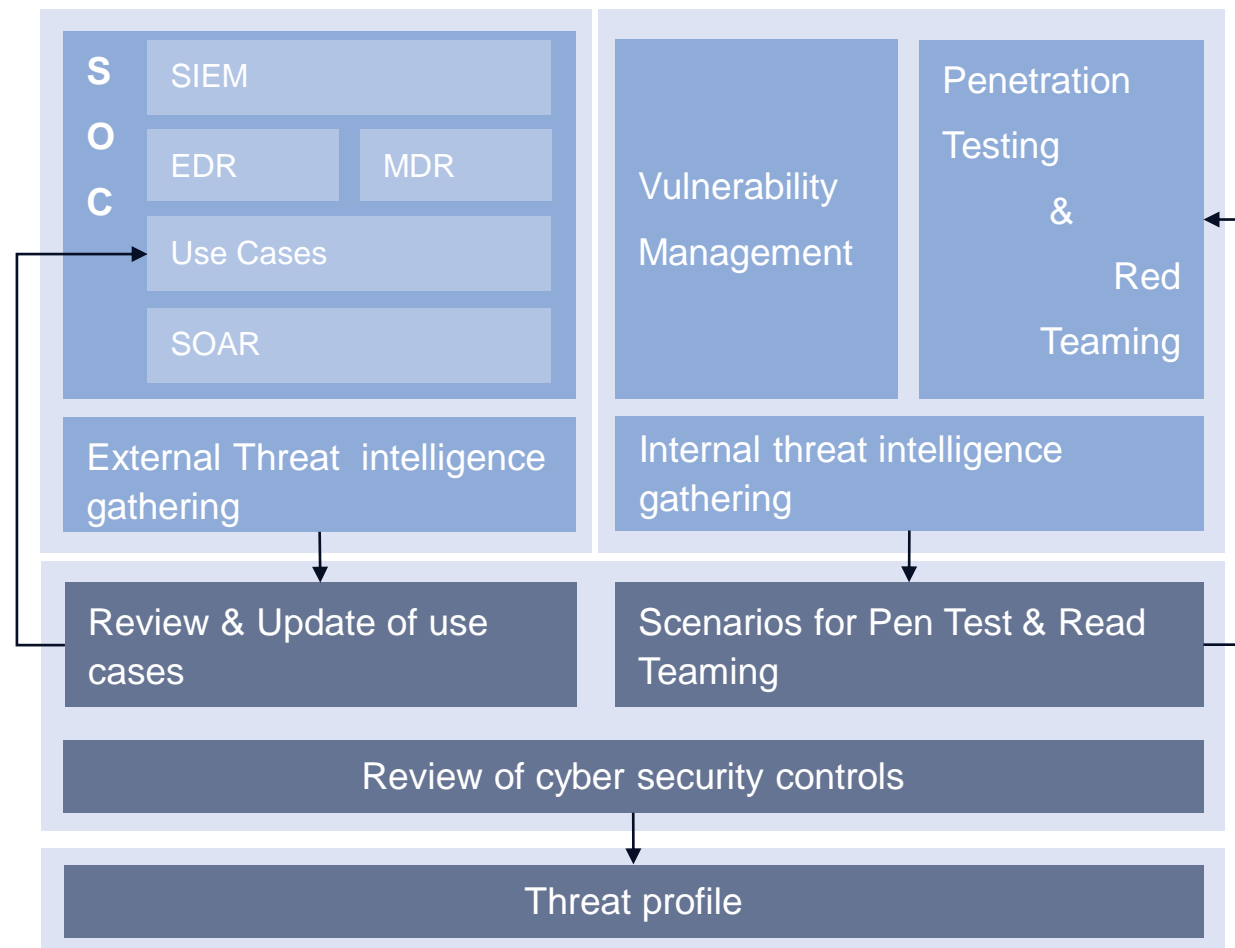Holistic approach for threat management
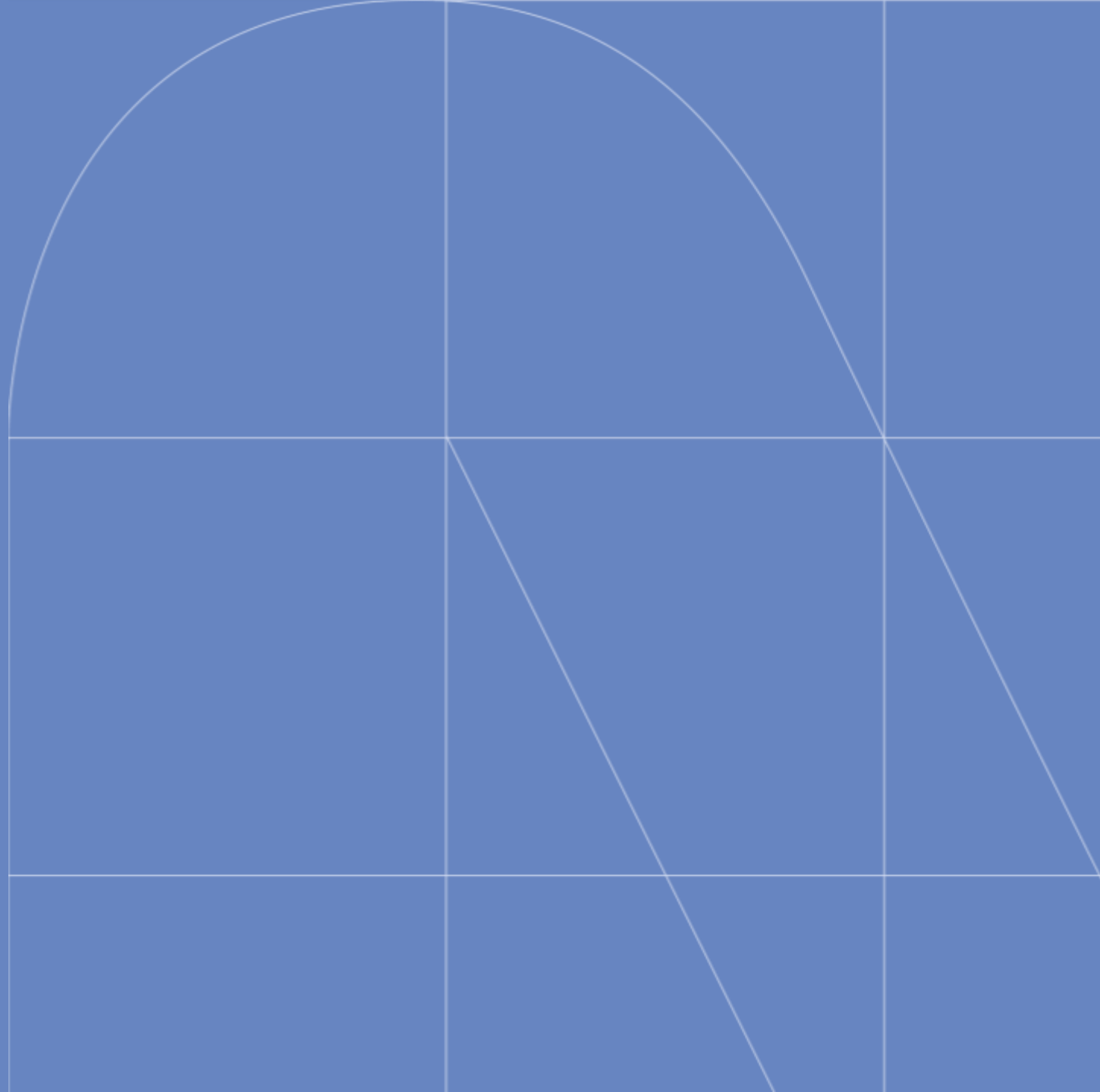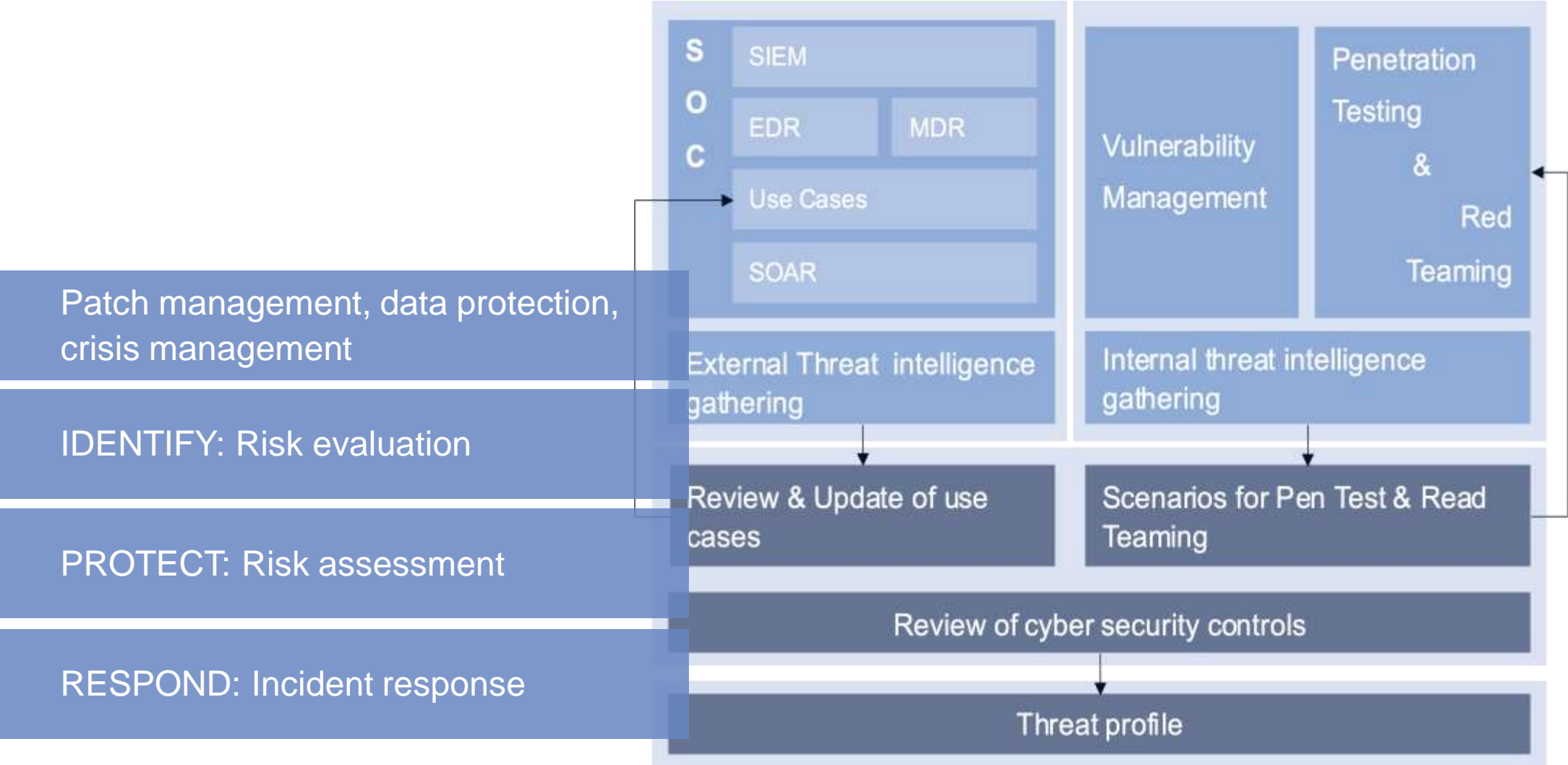
Active Threat Management Components

Holistic active threat management approach

Continuous process to manage cyber security related threats that is comprised by two sub processes:
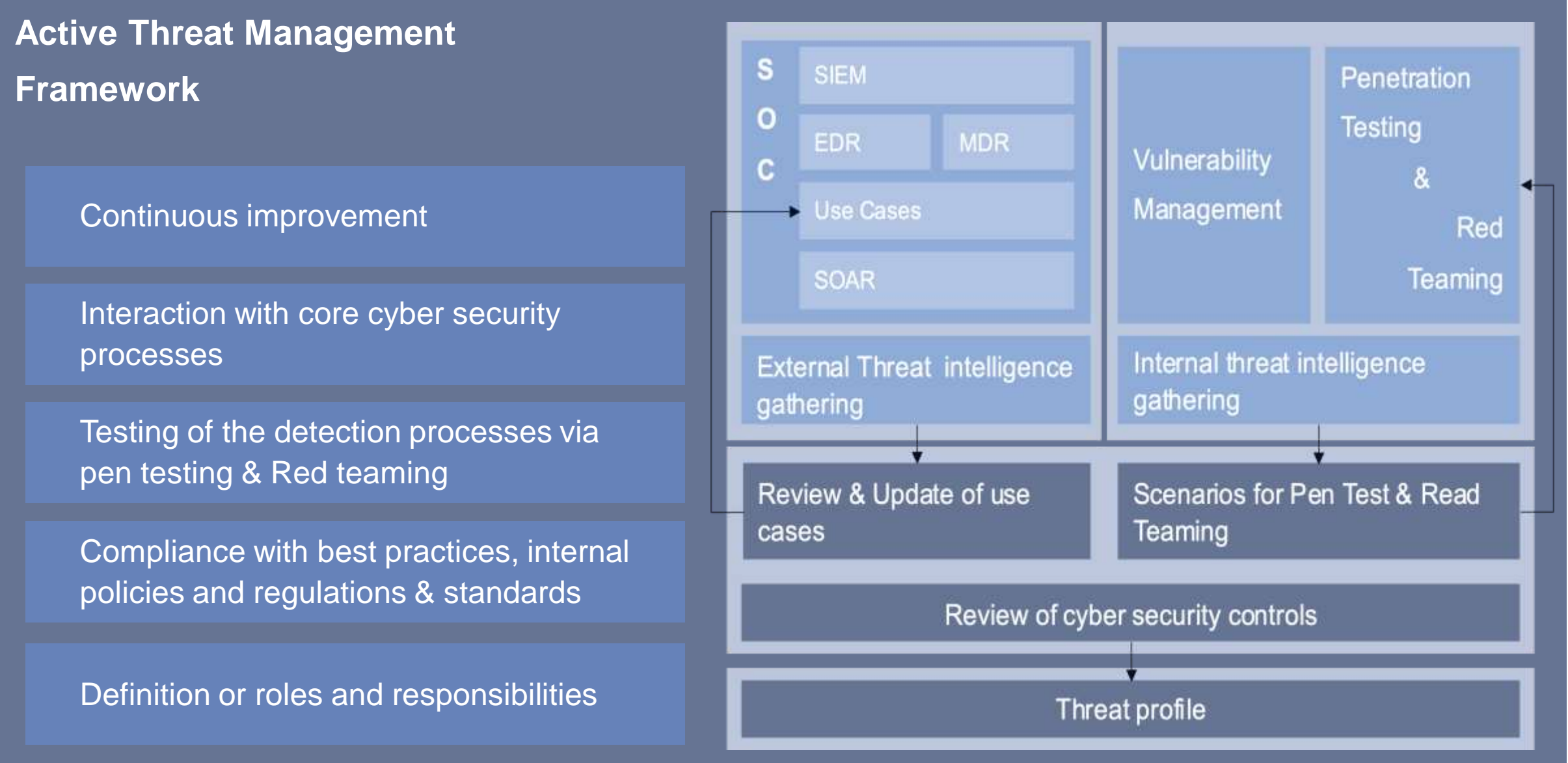
a) Active definition and continuous update the threat profile of the organization

b) Active detection of cyber security threats

Interaction with core cyber security processes

Patch management, data protection, crisis management

IDENTIFY: Risk evaluation

PROTECT: Risk assessment

RESPOND: Incident response

SOC
- SIEM
- EDR
- MDR
- Use Cases
- SOAR

Vulnerability Management

Penetration Testing & Red Teaming

External Threat intelligence gathering

Internal threat intelligence gathering

Review & Update of use cases

Scenarios for Pen Test & Read Teaming

Review of cyber security controls

Threat profile

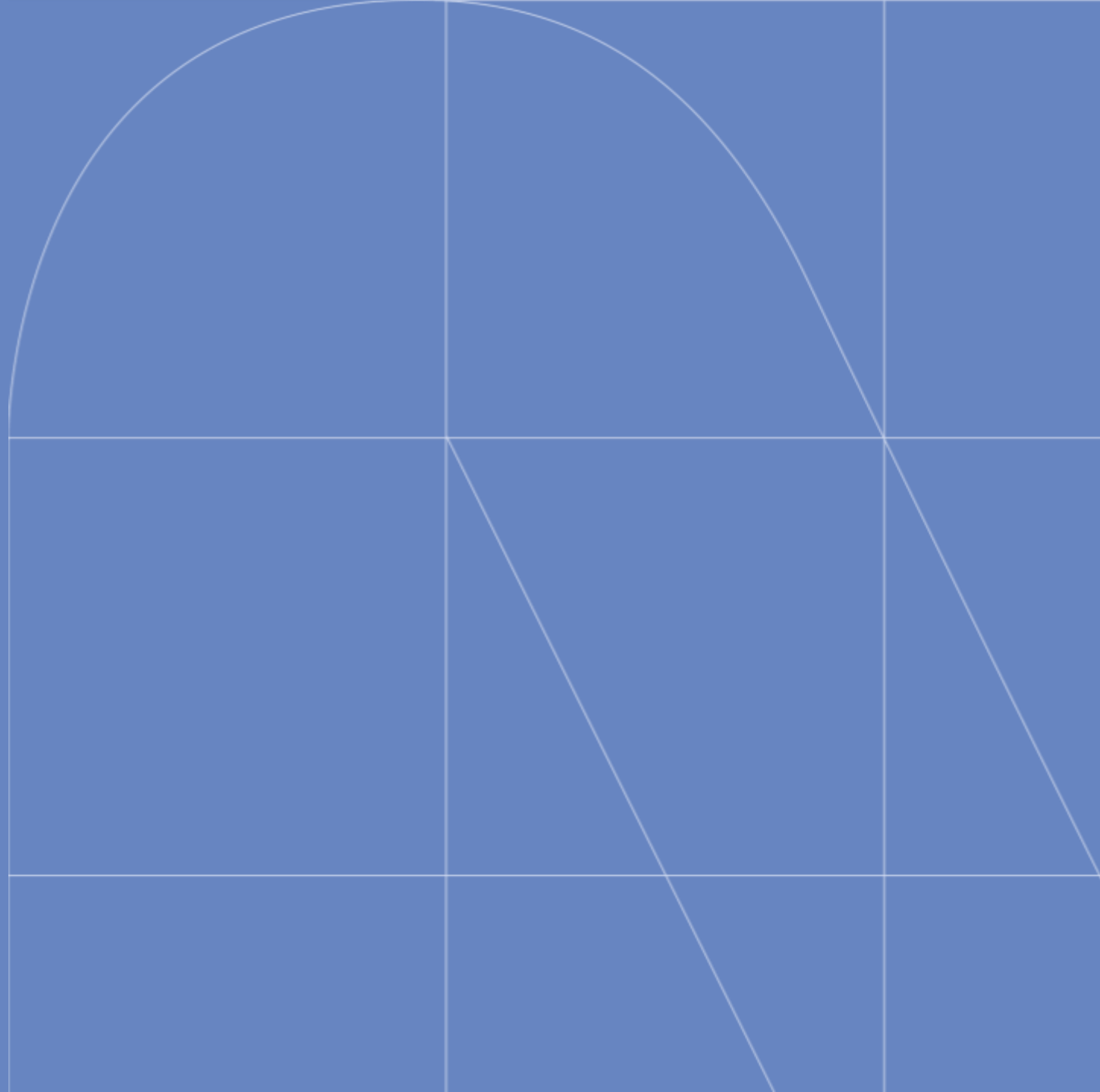# Active Threat Management Governance Framework

03

The future is now

Focus areas and next steps

Next is now

Mixture of coercive & subversive activity, conventional and un-conventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives

Integrated security across the entire organization, connects a wide range of security processes. Centralized visibility & incident response. Effectiveness & economies of scale, adoption of controls and unification of operations. Convergence of CSO, and CISO roles
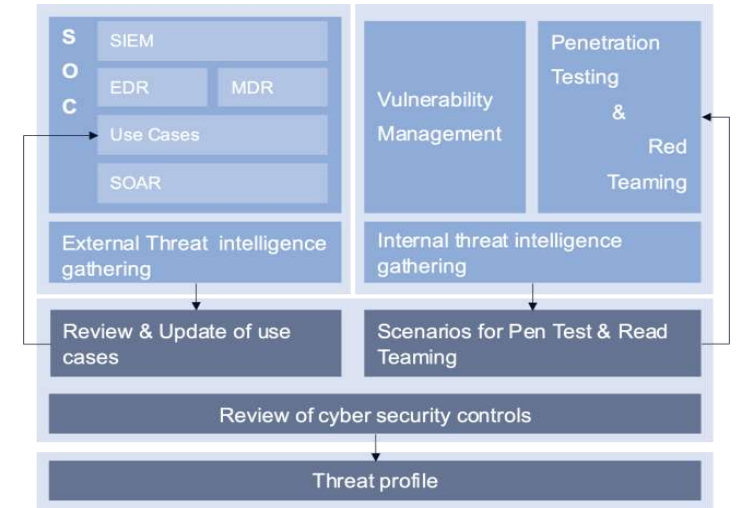
Working proactively to defend networks, applications, and all kinds of digital systems against active threats, while at the same time risks and vulnerabilities that may lead to threats are identified.

Hybrid threats

Security convergence

Active threat management

The way forward

Holistic strategy for information security

Active threat management and response to all events affecting the required level of security

Integration of information security responsibilities to all business and technology roles

Focus on effectiveness and prioritize based on risk

NTT DaTa

The changing face of corporate security

Information Assurance

Continuity of operations & resilience

Confidentiality	Integrity
Availability	Safety
Authenticity	Resilience

Security Governance & Risk Management

Monitor, Response & Improvement

Thank you.

Panagiotis.iliopoulos@emeal.nttdata.com

NTT DaTa