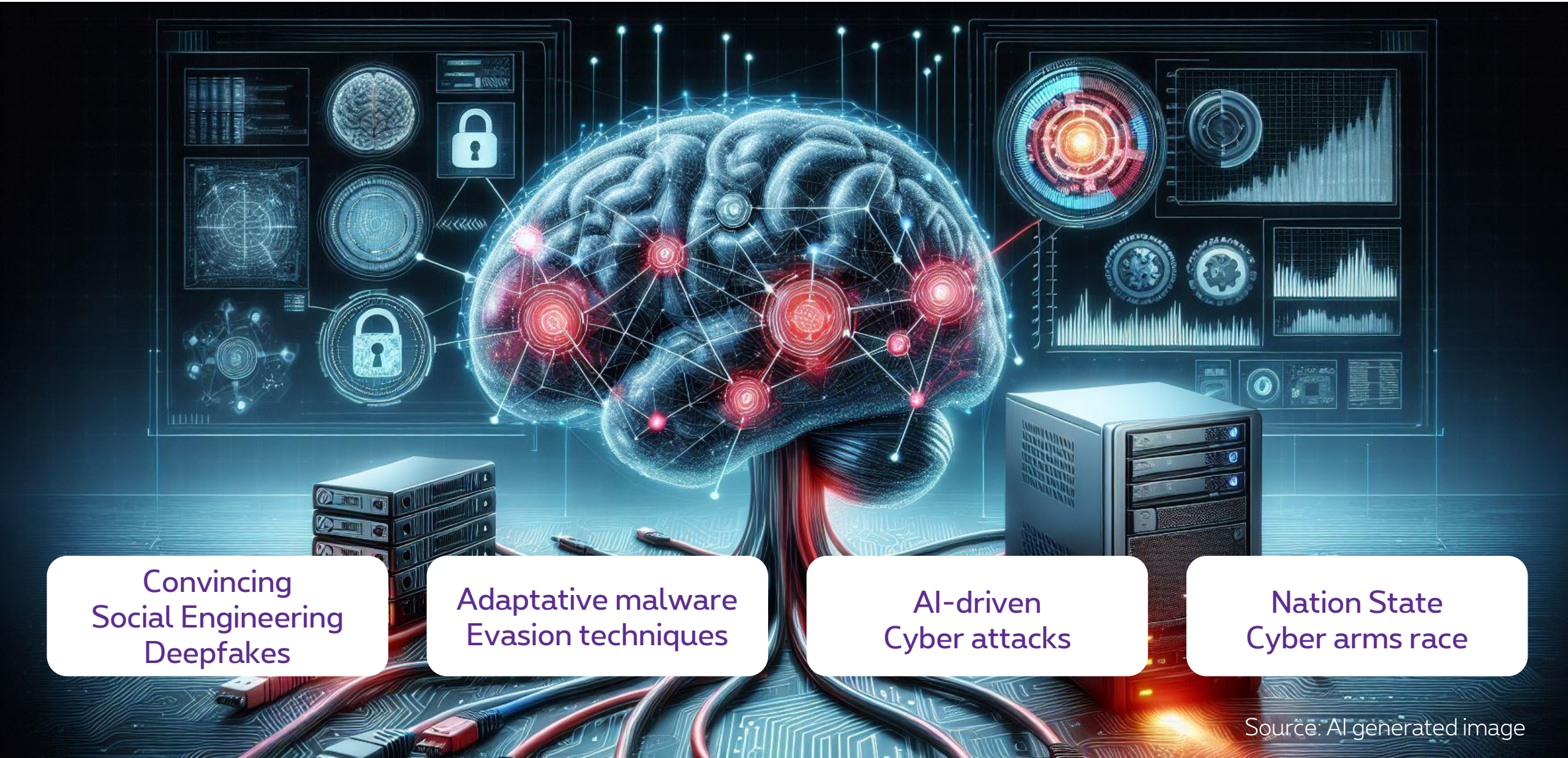
How AI will boost our Cyber Security

A proximus vision

Fabrice Clément, Group CISO

proximus

AI, the ultimate cyber threat ?



Convincing
Social Engineering
Deepfakes

Adaptative malware
Evasion techniques

AI-driven
Cyber attacks

Nation State
Cyber arms race

Source: AI generated image

AI, the brain of cyber defence ?

Source: AI generated image

We need something disruptive...

proximus

Artificial Intelligence

Cybersecurity

proximus

proximus ada

The center of excellence providing Artificial Intelligence and Cybersecurity solutions to the Proximus Group and Belgian Society

Proximus Ada is named after Ada Lovelace, born in 1815 and considered the world's first computer programmer.

proximus ada

A proximus daughter company

Launched April 1st 2022

AI & CS Talent

At launch: 50
Now: 100
Next year: 130-150

Start-up culture

Guilds
Ecosystem
Modern Employer

Modern Employer

Inter-personal &
Technical skills
Recognition

proximus ada

1.

Leverage our Artificial Intelligence and Cybersecurity talents and expertise within the broader Proximus Group

3.

Use our digital, AI and cybersecurity competencies to do good for Belgian society

2.

Be recognized as the reference center of excellence in Belgium for these domains, attract local talents and build strong collaborations and partnerships with local universities and research institutes

proximus ada

Our AIxCS vision

1.

We strive to protect our company and customers by detecting and countering the most advanced cyber attacks

2.

We empower our security professionals to focus on the most critical tasks, by automating basic tasks and enhancing efficiency through context-based guidance

3.

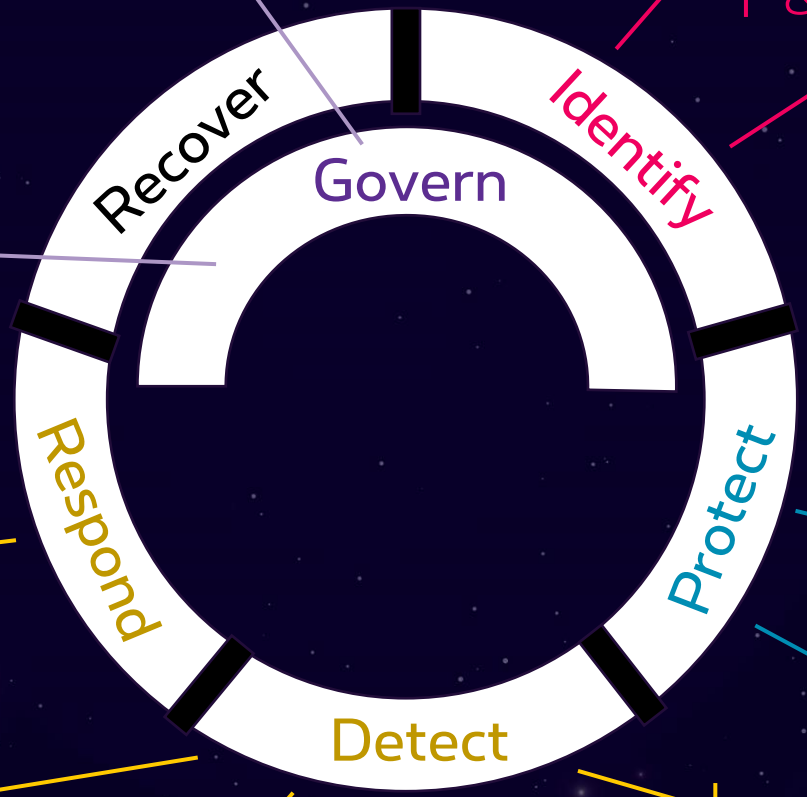
We ensure customer trust by countering fraud, leveraging AI and automation.

4.

We aim to enhance our compliance by conducting a thorough analysis of the regulations and adhering to international standards

proximus ada

We have identified a set of AIxCS use cases



Regulations and International Standards Compliance

Customer Questionnaires

Copilot

SOAR

Actionable & Predictive Intelligence

Intrusion Detection System

Attack Path Discovery

Log Analysis

Anti-fraud Platforms

Role-based Access Control

Security Coach

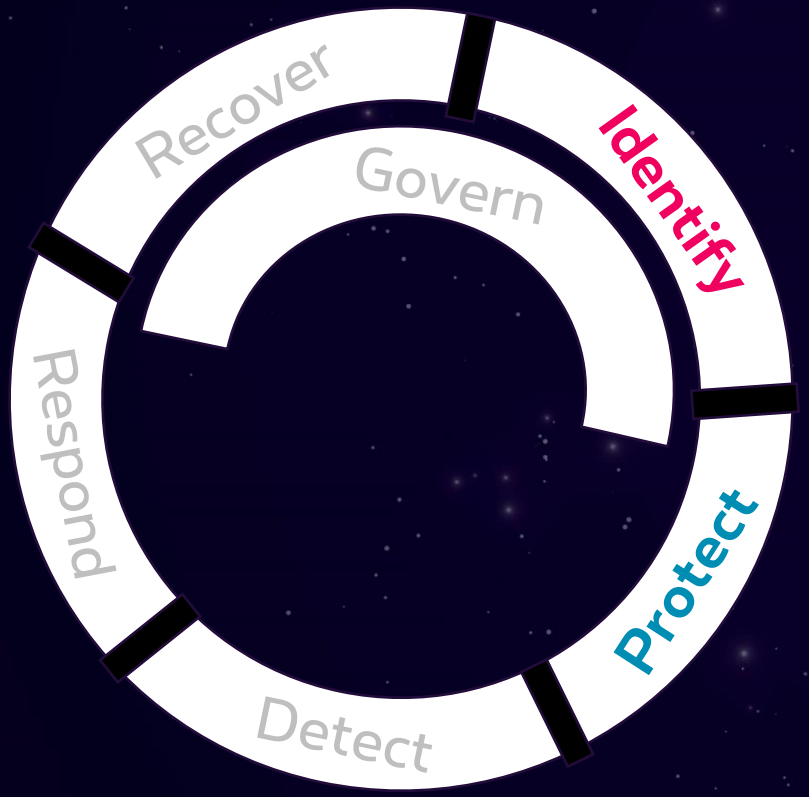
Security Control Validation

PEN testing

Vulnerability Scanning & Prioritisation

proximus ada

Identify & Protect



Vulnerability Scanning & Prioritisation

Scan platforms, enrich with context-based information, prioritise vulnerability remediations and create remediation workflows.

PEN testing

Build and execute advanced attack scenarios based on given context, threat landscape and attack techniques.

Security Control Validation

Assess the overall security posture of a system, by correlating the threat, vulnerabilities, and applied security measures.

Security Coach

Provide guidance to security analysts based on internal knowledge base (policies, guidelines, architecture blueprints, etc.)

Role-based Access Control

Define automatically business roles and assign them to end-users.
Detect deviations and ensure maintenance.

Anti-fraud Platforms

Detect & block phishing, malware spread and fraud attempts.

proximus ada

SAFE

Language

English

Number of search results used to answer

15

5 20

proximus ada

Chat History

- PDP-32.pdf

What security measures do I need to expose my API to Internet ?

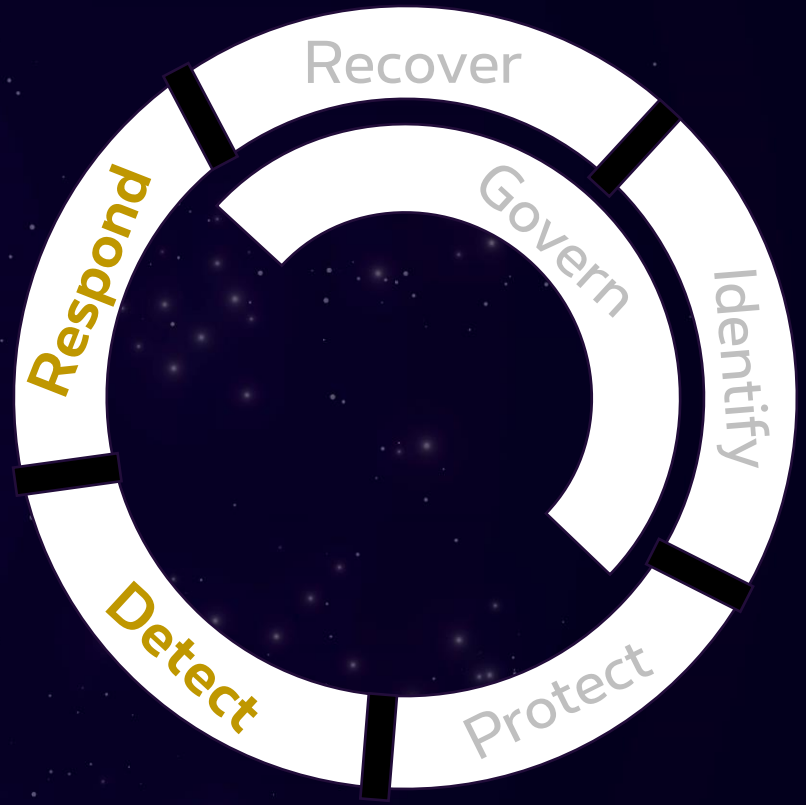
To expose an API to the internet, the following security measures must be considered:

- A Perimeter Gateway MUST be used when API integrations cross the security zones corresponding to the different network fabrics (i.e. Cumulus fabrics, Telco fabrics, legacy network zones) (PCS-04.01.04.02)
- An API consumer on the Internet accessing an API via a Perimeter Gateway MUST be authenticated using strong authentication, which SHOULD be done using mutual TLS. The Perimeter Gateway accepting connections from the Internet MUST be located in a DMZ (PCS-04.01.04.02)
- When an API provider exposes an API via an API gateway, it MUST NOT accept direct API invocations and ensure all API invocations are coming from the API gateway, for example, using mutual TLS. The API provider MAY delegate authentication and authorization to the API gateway and SHOULD implement further fine-grained access control (PCS-04.01.04.02)
- An API provider MUST authenticate the Perimeter Gateway, which SHOULD be done using mutual TLS. The API provider SHOULD perform fine-grained access control based on the information about the actual API consumer provided by the Perimeter Gateway (PCS-04.01.04.02)
- All API invocations MUST go over TLS and the caller MUST authenticate the destination endpoint. HTTP connections MUST be rejected and not redirected to HTTPS. An API consumer SHOULD use a certificate store with CA certificates explicitly approved by Proximus instead of system-wide trust store which contains generally trusted CA certificates. An API consumer MAY pin the API provider endpoint certificate or public key, and subsequently not establish connections with endpoints that offer a different certificate or key, even if

Type your question here

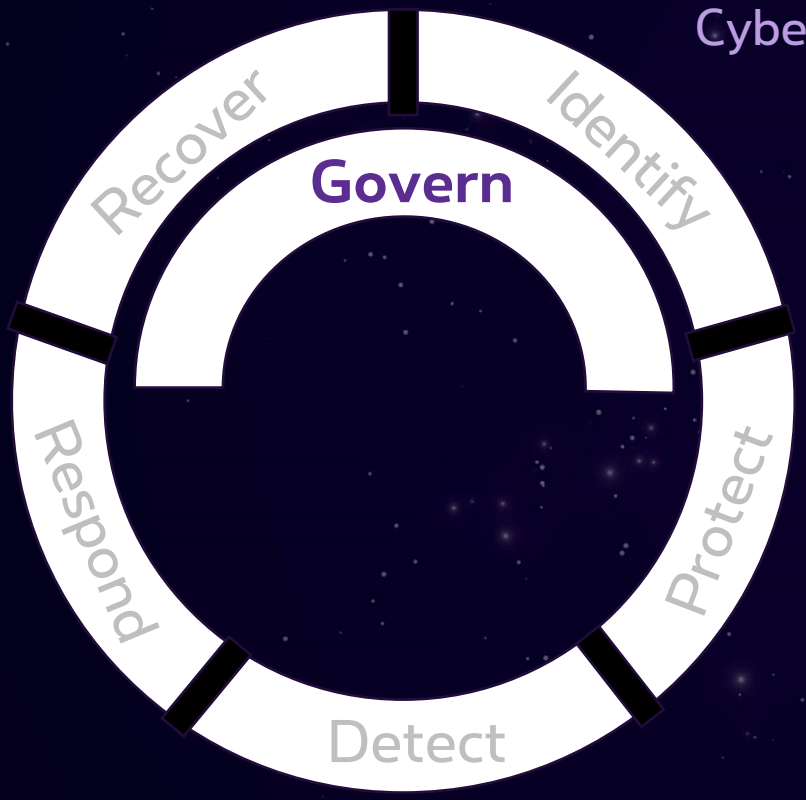
Detect & Respond

Provide guidance Automate the assessment, monitoring & remediation.	Copilot
Automate time-consuming, repetitive, and complicated incident response workflows.	SOAR
Analyse large set of intelligence sources. Summarize & classify information into MITRE ATT&CK categories.	Actionable & Predictive Intelligence
Monitor network traffic, detect anomalies and suspicious activities.	Intrusion Detection System
Collect & format heterogeneous logs into standardized information. Detect anomalies & suspicious behaviours.	Log Analysis
Search across the network, firewalls, servers and end-points to detect potential attack paths.	Attack Path Discovery



proximus ada

Governance



AI-assisted Compliance for Cyber Security Regulations and International Standards

- Get a comprehensive view on cyber security regulations and standards.
- Address a specific requirement across multiple regulations and international standards and map them with Proximus policies.
- Provide recommendations and best practices on how to comply.
- Generate compliance statements.

Customer questionnaires

- Generate answer to customer's questionnaires based on past answers and security knowledge base.

proximus ada

Some take-aways

- AI is a game changer for cyber security, from a threat but also from a defence perspective
- AI will bring value in all aspects of the end-to-end cyber security value chain
- Proximus Ada is uniquely positioned at the intersection of AI and CS
- We started from our vision, and we are now developing the first AIxCS use cases which are very promising

Thank you!

proximus