SIMPLIFIED
CYBERSECURITY MANAGEMENT

SWIPE

Pro CISO® announces CA/CR™, its unique approach to Cybersecurity Management

Pro CISO®

Contact use here, or visit our website!

+31202117467

1

WHAT IS CA/CR™ ?

We are excited to announce our innovative service concept that we called **Continuous Assessment and Continuous Remediation (CA/CR™)**.

This approach is designed to simplify how organizations manage their cybersecurity, inspired by the principles of Continuous Integration and Continuous Deployment (CI/CD) in DevOps.

This pragmatic methodology can be adopted by both mature enterprises and by smaller companies that don't have a structured cybersecurity team.

2

TRADITIONAL ASSESSMENTS

The traditional approach to cybersecurity management involves periodical assessments, followed by often disconnected remediation efforts.

This method is costly, inefficient, and typically results in reactive measures that do not align with long-term security strategies.

Organizations spend significant resources on assessments and then additional funds on implementing remediation actions through various suppliers, leading to fragmented and short-term fixes.

3

THE CA/CR™ APPROACH

At **Pro CISO®**, we introduced a unique approach to cybersecurity management. **CA/CR™** ensures continuous assessment and continuous remediation. Leveraging international security standards like ISO 27001, NIST CSF 2.0, PCI-DSS, etc., and regulations such as GDPR and NIS2, we continuously evaluate the presence and effectiveness of each control, identify coverage gaps, and determine both current and target risk levels after remediation.

- **Continual Process: CA/CR™** adopts the principles of seamless and continuous integration from DevOps and Agile, applying them to cybersecurity management.

- **Low Overhead and Efficient** : Our **CA/CR™** approach simplifies the cybersecurity management of organizations by allowing continuous assessments to flow directly into remediation actions. Governance is ensured through the use of either custom toolkits, or lean IRM tools that integrate with Slack or Microsoft Teams.

- **Flexible to the Changing Threats:** The effectiveness of cybersecurity measures are reviewed and improved continuously, in function of the evolving threats that the organization is exposed to. Threat modelling is performed both in the Assessment phase and the Remediation phase, to ensure that the risk exposure is timely identified and analysed for pragmatic mitigation.

4 CA/CR™ WORKFLOW

Define Scope: Determine the area of intervention. It can be a system, a department or an entire organization

Reference Standards: Identify the benchmark standards, frameworks, regulatory requirements

Identify Assets: Identify infra, systems, applications, data that is involved

Threat Model: Analyse the risk exposure, the data flows, the entry points and the threats

Assess Controls: Verify the presence and effectiveness of existing controls

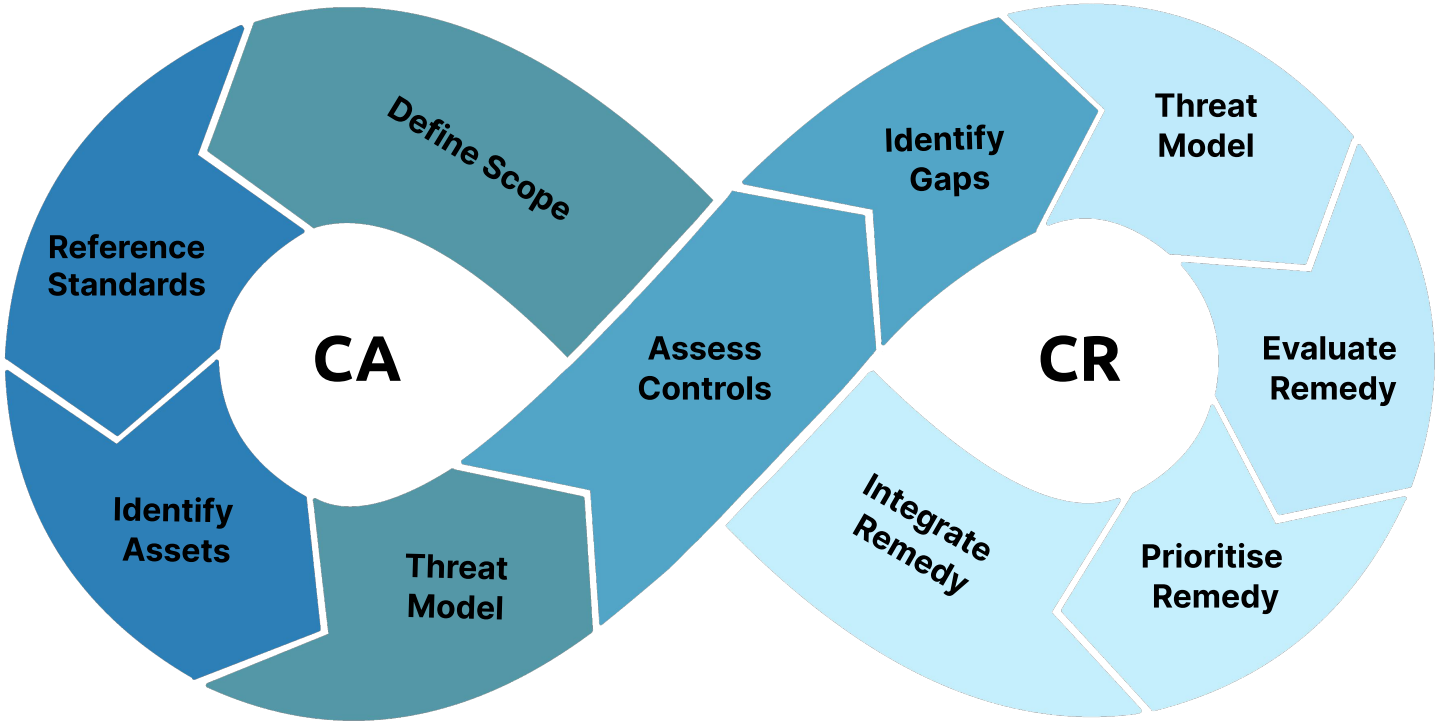
Identify Gaps: Determine the absence or ineffectiveness of present controls

Threat Model: Map the identified gaps with present and emerging threats and perform a to-be risk reduction simulation

Evaluate Remedy: Perform a cost/ benefit analysis of the identified additional controls, ensure coherence with the Cybersecurity strategy

Prioritize Remedy: Identify the remedies for high risks that require funding and priority

Integrate Remedy: Harmonize implementation plans with involved Stakeholders (IT, HR, Finance, etc.) and monitor their progress



WHY CHOOSE CA/CR™? 5

Cost Efficiency:
By integrating assessment and remediation processes, we significantly reduce costs.

Sized to Fit:
The program can be optimized for any size company, focused on a the entire organization, or initially a limited scope of departments and systems including on only the relevant controls.

Contextual Remediations:
Our solutions are tailored to the specific business context, addressing multiple controls simultaneously.

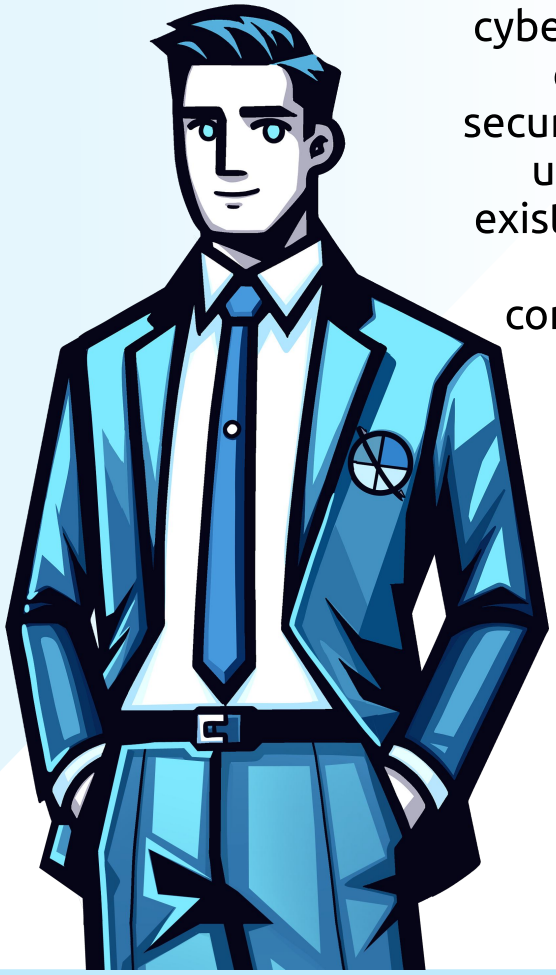
Strategic Alignment:
CA/CR™ ensures that remediation actions align with long-term business strategies, rather than being isolated initiatives.

Progressive Risk Reduction:
With each iteration, the scope is extended, more risks are identified and mitigated more effectively, leading to a progressively lower risk profile.

6

TRADEMARK AND INNOVATION

We are proud to announce that **CA/CR™** is a registered trademark, highlighting its innovative and disruptive nature in the field of cybersecurity! Just as CI/CD has transformed DevOps, **CA/CR™** is set to revolutionize cybersecurity management, providing continuous, integrated protection and improvement.



At **Pro CISO®**, our expertise lies in enabling organizations to methodically develop and enhance cybersecurity measures. With our holistic approach to cybersecurity we support companies to develop a secure culture throughout the organization by making use of available resources and integrating with the existing culture. We listen to our customers and tailor security awareness projects to the needs of the company, the people and the relevant threat actors.

Additionally, we provide tactical advice for immediate impact, addressing clear risks while aligning with broader strategic objectives.

Reach out to learn more about how we can help you!