nviso

SHIELD vzw

Introduction to NVISO

Overview of our services & use cases for Shield VZW "GRC"

www.nviso.eu

About NVISO

Our Company

NVISO is a pure play **Cyber Security services firm** of 300+ specialized security experts and founded in 2013.

Initially founded in **Belgium**, we've been in **Germany** since 2019, and **Greece** & **Austria** since 2022.

Our mission is to **safeguard the foundations of European society from cyber attacks**.

Our DNA

We are proud: we are proud of who we are and what we do.

We care: we care about our customers and people.

We break barriers: We challenge the status quo by continuous innovation.

No BS: We keep our promises and don't fool around.

Our Research

We invest 10% of our annual revenue in research of new security techniques and the development of new solutions.

Follow us on:

@NVISO_security and @NVISO_Labs

blog.nviso.eu/

Brussels
Frankfurt
Munich
Vienna
Athens

© GeoNames, Microsoft, Open Places,

CYBER
SECURITY

CHALLENGE
BELGIUM

CYBER
SECURITY

RUMBLE
GERMANY

AN INITIATIVE FROM nviso

Our expertise

We lead the way and actively teach others, a testament to this are the SANS courses we (co-)author and instruct:

SEC575

Mobile Pen. Testing

Since 2019, NVISO experts are the lead authors of the SANS SEC575 course "Mobile Penetration Testing & Ethical Hacking".

NVISO experts maintain 6 days of courseware of this 6-day course.

SEC598

Security Automation

Over the course of 2021 and 2022, NVISO has developed a new SANS course focused on Security Automation. Released in 2023.

NVISO experts maintain and develop 6 days of courseware of this 6-day course.

SEC599

Purple Team Tactics

In 2018, NVISO experts were lead authors of one of the first purple teaming courses, "SEC599 – Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses".

NVISO experts maintain 5 days of courseware of this 6-day course. We also actively teach it worldwide.

SEC699

Advanced Purple Team

In 2020, NVISO experts developed a follow-up course to SEC599, labelled SEC699, which focuses more on automated adversary emulation using CALDERA.

NVISO experts maintain 5 days of courseware of this 6-day course. We also actively teach it worldwide.

Our expertise

We share our know-how with the community

Public Conferences

Our research results have been **presented at well-respected security events** and conferences including Black Hat, BruCON, OWASP, FIRST, and many more.

Knowledge Sharing Sessions

Our **brown bag sessions** are **free-of-charge lunch talks** in which our experts pass on their knowledge to colleagues and customers.

Our team does not only have the knowledge required to teach, but also the expertise to **convey complex material to their audience in an understandable, engaging and fun way** without being too overwhelming.

Curious to join a session, or have us organize a private session for your team? Let your NVISO contact know!

Our Blog & Open Source

NVISO Labs

Cyber security research, straight from the lab!

We love to write about the things we are most passionate about! Our blog features innovative content from each of our different services lines: https://blog.nviso.eu.

We strongly believe in **sharing our work** with the community & **giving back**. We continuously **release & maintain security tools** for use by other professionals, write & share our **detection rules**, develop **new technology integrations**. Our work is freely available on GitHub: https://github.com/NVISOSecurity

Disclaimer: General Intro on NVISO – not all of the below are eligble under Shield (yet)

Market trends

What our clients are asking us and what we're investing in.

Incident Readiness

CSIRT Service
24/7 on-call support

Incident & Crisis Governance

DRP / BCP

Backup Readiness
Strategy, Assessment

Ransomware resilience package
Playbooks, BCP & DRP update

Attack Surface Management

Managed Detection & Response
Incl. Managed Vuln Mgt

Third-Party Risk Management
optimization and automation

Security Automation

Cloud engineering & automation
(mostly Azure, AWS)

SOC Automation
Our NITRO service runs on Cortex XSOAR

Adversary Emulation

Scenario-based penetration test

Red Teaming

Automated Purple Teaming

Regulation

NIS2 Implementation
ISO27001, BSI (DE), Cyber Fundamentals (BE)

DORA Implementation

ISO27001 Certification Support

SWIFT CSP Support

Executive Briefings

AppSec

Threat Modelling

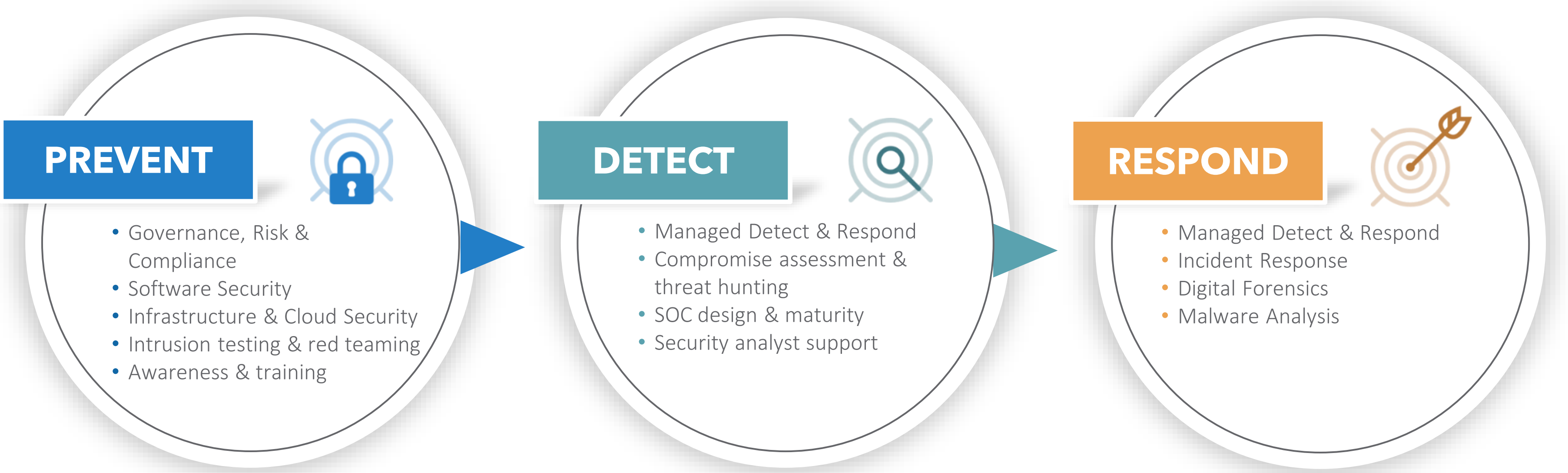
SSDLC Implementation

SSDLC as a Service

We Support You Throughout the Entire Cyber Security Incident Lifecycle

Define & deliver your cyber strategy

Disclaimer: General Intro on NVISO – not all of the below are eligble under Shield (yet)



PREVENT

- Governance, Risk & Compliance
- Software Security
- Infrastructure & Cloud Security
- Intrusion testing & red teaming
- Awareness & training

DETECT

- Managed Detect & Respond
- Compromise assessment & threat hunting
- SOC design & maturity
- Security analyst support

RESPOND

- Managed Detect & Respond
- Incident Response
- Digital Forensics
- Malware Analysis

NITRO is NVISO's Managed Services platform. Leverage NVISO's expertise at scale, combined with best-of-breed technology.

Our Research & Development cell fosters innovation and manages technology development projects that empower our services.

Cyber Strategic Advisory & GRC Ops

Possible under Shield GRC

Define & Deliver a Cyber Strategy

Small & Medium Bus.

Enterprise

Your Cyber Security Roadmap

Light or extended, based on NVISO Rapid Assessment, ISO27k, CIS20, NIST CSF…

CISO as a Service

- A SPOC complemented by our pool of experts
- Accelerators (ISO27k-compliant docs, awareness enablers, incident response playbooks, …)
- Packaged Solutions (Vuln. Mgt as a Service, Azure Sec. Monitoring as a Service, SOC-as-a-Service, Awareness as a Service, …)

ISO27k & Compliance Support

We help you achieve certification e.g. ISO27k, CyFun, ETSI319401/eIDAS, ISA62443, SWIFT CSP, …

Governance

- Define Cyber Security Strategy framework
- Implement, diagnose & improve cyber governance

Risk

- Vendor Risk Management (TPRM)
- Compliance Risk Assessments
- Security Audits
- On-demand risk assessments based on ref. models

Compliance

- Expertise in regulation (NIS2),
- fin. regulation (EBA, PCI, …) & trust services (eIDAS)
- Product security compliance (CRA)
- Extensive experience with leading standards

Possible under Shield GRC

SHIELD vzw nviso

Our approach

Defining your strategy and help you implement it

DEFINE

IMPLEMENT

1 Risk / Gap Assessment
Based on NVISO Rapid Assessment method
for ISO27k, CyFun, CIS18, NIST CSF…

2 Cyber Security Roadmap
3 years planned & budgeted

3 Validation & Governance Kick Start

Pool of Experts

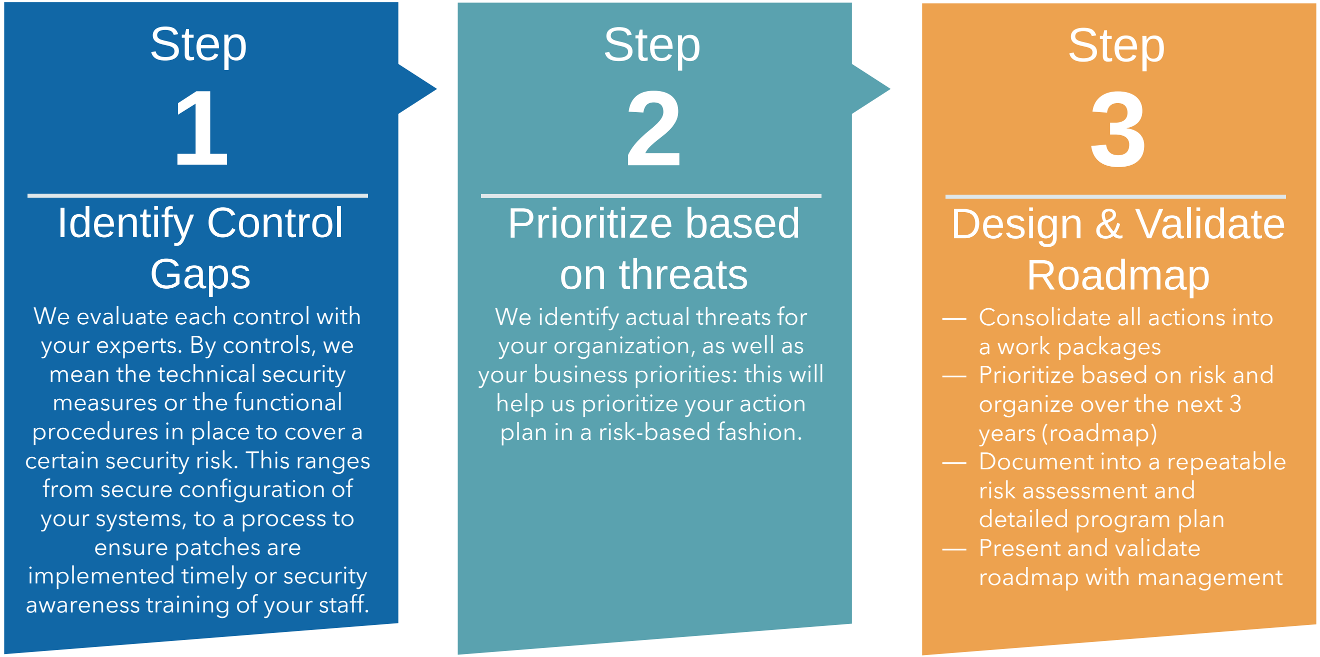
Accelerators

Packaged Solutions

Possible under Shield GRC

Our Approach

We propose to develop a Cyber Security Roadmap based on the following set of activities:



Step 1

Identify Control Gaps

We evaluate each control with your experts. By controls, we mean the technical security measures or the functional procedures in place to cover a certain security risk. This ranges from secure configuration of your systems, to a process to ensure patches are implemented timely or security awareness training of your staff.

Step 2

Prioritize based on threats

We identify actual threats for your organization, as well as your business priorities: this will help us prioritize your action plan in a risk-based fashion.

Step 3

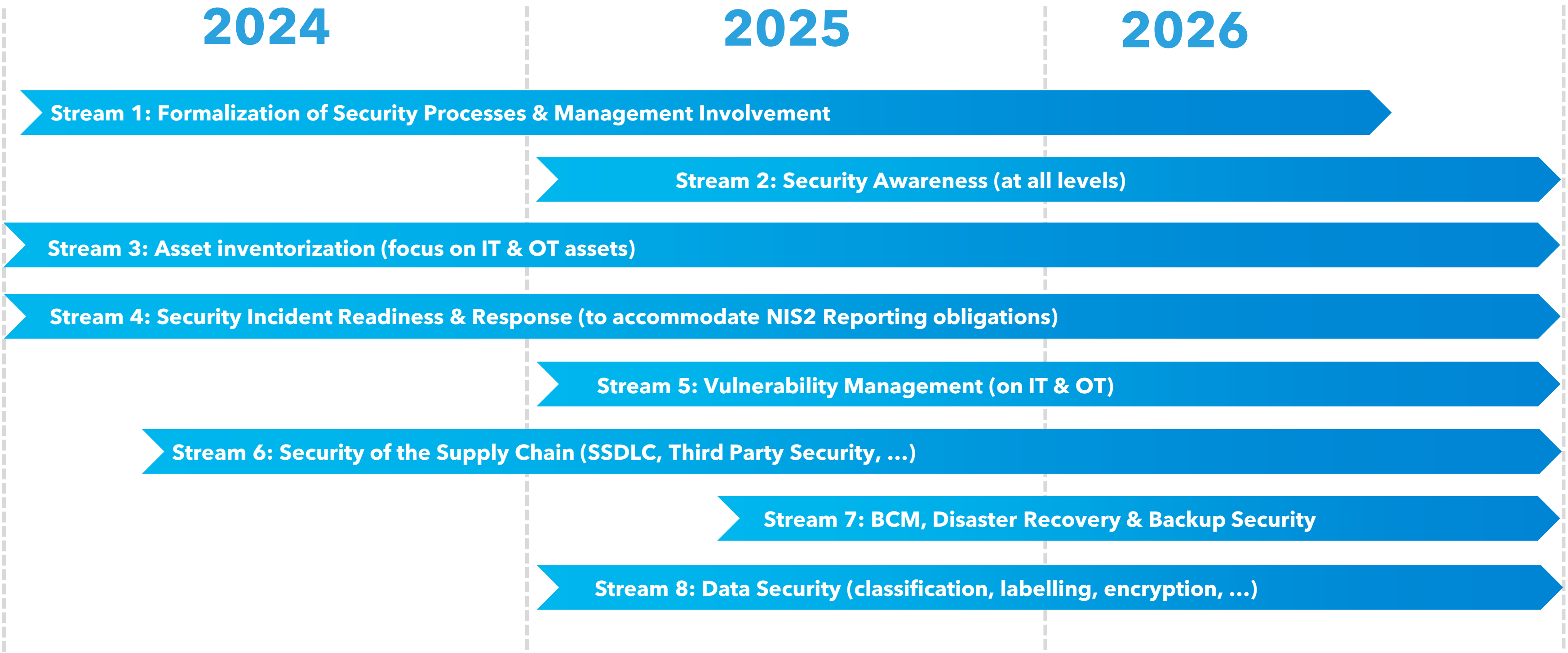
Design & Validate Roadmap

- Consolidate all actions into a work packages
- Prioritize based on risk and organize over the next 3 years (roadmap)
- Document into a repeatable risk assessment and detailed program plan
- Present and validate roadmap with management

Possible under Shield GRC

Define & Deliver a Cyber Strategy

Illustrative Example – Threat-Based NIS2 Compliance



2024

2025

2026

Stream 1: Formalization of Security Processes & Management Involvement

Stream 2: Security Awareness (at all levels)

Stream 3: Asset inventorization (focus on IT & OT assets)

Stream 4: Security Incident Readiness & Response (to accommodate NIS2 Reporting obligations)

Stream 5: Vulnerability Management (on IT & OT)

Stream 6: Security of the Supply Chain (SSDLC, Third Party Security, …)

Stream 7: BCM, Disaster Recovery & Backup Security

Stream 8: Data Security (classification, labelling, encryption, …)

Possible under Shield GRC

IMPLEMENT

We assist you with…

ROADMAP EXECUTION

Implement or monitor defined actions

DAY TO DAY QUESTIONS

Handle incoming security & privacy questions

SPARRING PARTNER

Acting as a sounding board for security projects

We balance budget & flexibility

We operate in a fixed capacity mode – We want you to know what to expect in terms of presence and of budget: this is why we usually offer a fixed capacity of the CISO per week. We are present on fixed days, and we have fixed status meetings together, to keep you in control.

We ensure contractual agility – You may also need extra capacity at certain moments: we ensure sufficient agility through a contractual agreement where we can increase our presence or mobilize experts (within 4 to 6 weeks) based on your simple written request / approval, based on a rate card and discount model agreed in advance.

IMPLEMENT

Possible under Shield GRC

SHIELD vzw nviso

Our team features world-class security experts that supports the implementation of the program

Pool of Experts

Our people speak at some of the world’s most prestigious security conferences
And regularly speak on security for the Belgian cyber and business community.

SANS BRUCON OWASP Open Web Application Security Project CYBER SECURITY COALITION black hat

.AGORIA CYBERSEC EUROPE FIRST Improving Security Together WORLD Conference and Exhibition FIC HITB RSA Conference

Disclaimer: only for illustrative purposes – not all of this is possible under shield (yet).

IMPLEMENT

We have built a set of accelerators and services that enable us to rapidly deliver at an affordable cost.

Basic Security Framework

Policy, Code of Conduct, Risk Assessment kit

Architecture Check

Light and Advanced Security Architecture Review Method

Incident Response Readiness Check

Cloud Reference Architectures

And many others

Policies, procedures, and much more.

MDR (Managed Detect & Respond)

Vulnerability Management as a Service

Awareness as a Service

3rd party risk mgt as a Service

Incident Response Retainer

Technical Preventive Security

Possible under Shield GRC

Preventing Incidents

Security Architecture reviews on multiple levels

Within NVISO we have experts on multiple levels, **our standard security architecture review includes multiple levels** to so we can apply the **defense-in-depth approach**. Fully understanding your environments starts with understanding the architectural model implemented and the design decisions that were made, this includes mapping data flows, account management and overall architecture. Based on the **selected services we will perform an in-depth GAP assessment** on network configuration and/or system level according to best practices and industry standard such as the CIS top 20.

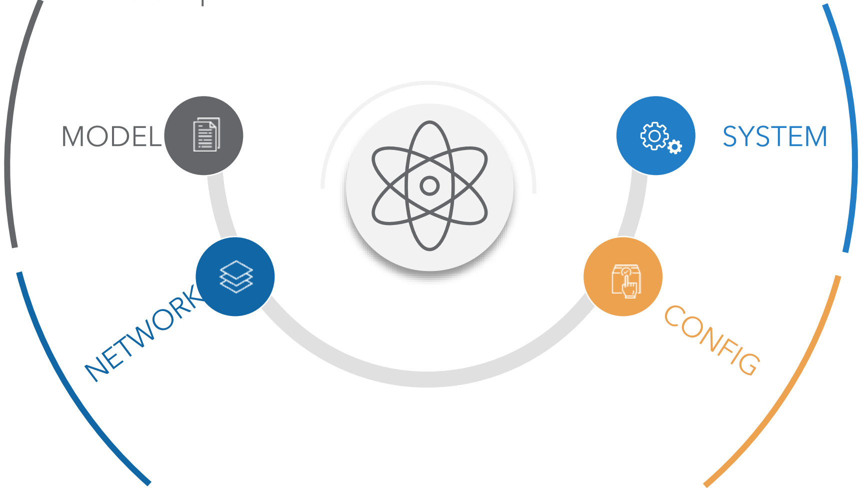
Architectural Model

An assessment and review will be performed based on the current state of the network and maturity related to security architecture.

Network Architecture

Reviewing the level 3 design and focus on perimeter and internal network controls to identify potential single point of failures or misconfigurations.

- Firewall rule-set review (option)
- DDoS Resiliency (option)



System Reviews

Proven guidelines will enable you to safeguard operating systems, software and networks that are most vulnerable to cyber attacks.

Configuration reviews

Every customer has specific security technology in place. Our configuration review is a more in-dept analysis per technology to find security misconfigurations.

These services are part of our standard model, but ad-hoc and more specialized reviews can also custom scoped and requested!

Possible under Shield GRC

SHIELD vzw nviso

Preventing Incidents

Cloud Security Projects

Microsoft Azure amazon web services Office 365

In case you are thinking about **moving towards the cloud** or you are **already in the cloud** NVISO can assist you in both cases. Our cloud security services can range from an integrated security design in your new environment to reviewing your current infrastructure via our standardized security assessment.

Cloud Security Assessment

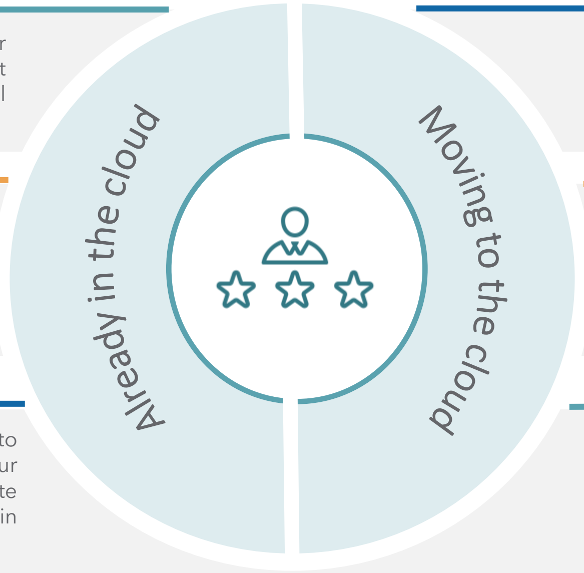
How secure your current environment is? Our assessment provides you an overview about your current exposure, missing security controls or typical misconfigurations within cloud environments.

Cloud Security Assurance

As your cloud environment is changing, you will need to review and adapt your security requirements continuously. After **an intake of the current setup** our security architects will **review changes and support your operational teams.**

Cloud Security Compliance

As new cloud resources are deployed, you will need to ensure that **compliance** of each cloud resource to your **corporate security standard**. NVISO can help you create automated compliance checks and reporting to gain visibility and additional compliance rules .



Cloud Security Design

NVISO can assist **you within the design process to integrate security in your design** based on your requirements, industry best practices and our technology expertise.

Cloud Security Assurance

Continuously integrate our security expertise in your cloud environment. During the design phase we will **define and review the security controls**, in a later stage our security architects review **ongoing changes and support your operational teams.**

Cloud Security Roadmap

Define the security roadmap for the cloud services used withing your organization through workshops and setup cloud infrastructure for your organization defining **quick wins and structural recommendations**.

Preventing Incidents

Preventing Incidents

At NVISO, we have a dedicated team that is specialized in both giving security advice and performing assessments on both applications and infrastructure. As a **world-class provider of security assessment services**, we ensure our methodology meets the highest quality standards and thus ensure it is based on several internal and external sources.

Methodology

- The SANS **security assessment** & **penetration testing courses**,
- The community driven **Penetration Testing Execution Standard (PTES).**
- The **OWASP Testing & Code Review guides.**
- The results of **our own Research & Development activities.**

NVISO Security Assessment Methodology

Portfolio

Standard assessments

- Web application assessments
- Mobile application assessments
- Infrastructure assessments
- Wireless & WiFi assessments

Advanced assessments

- Social engineering
- Physical security
- Internet of Things assessments
- Red / Purple teaming

Possible under Shield GRC

SHIELD vzw nviso

Technical Preventive Security

Illustrative Examples

Medical Device Product Security

1. Pentesting and threat modeling of Medical Printers
2. Pentesting and threat modeling of Medical Telemetry & Monitoring system
3. Pentesting and threat modeling of Medical Implants

Hospital Security Assessments

1. Several pentesting and Red Teaming exercises for hospitals
2. Specific technical assessments/reviews, such as Ransomware Readiness assessments, for hospitals.

We understand your technological complexities (on device as well as within the wider healthcare environment) and how to secure these.

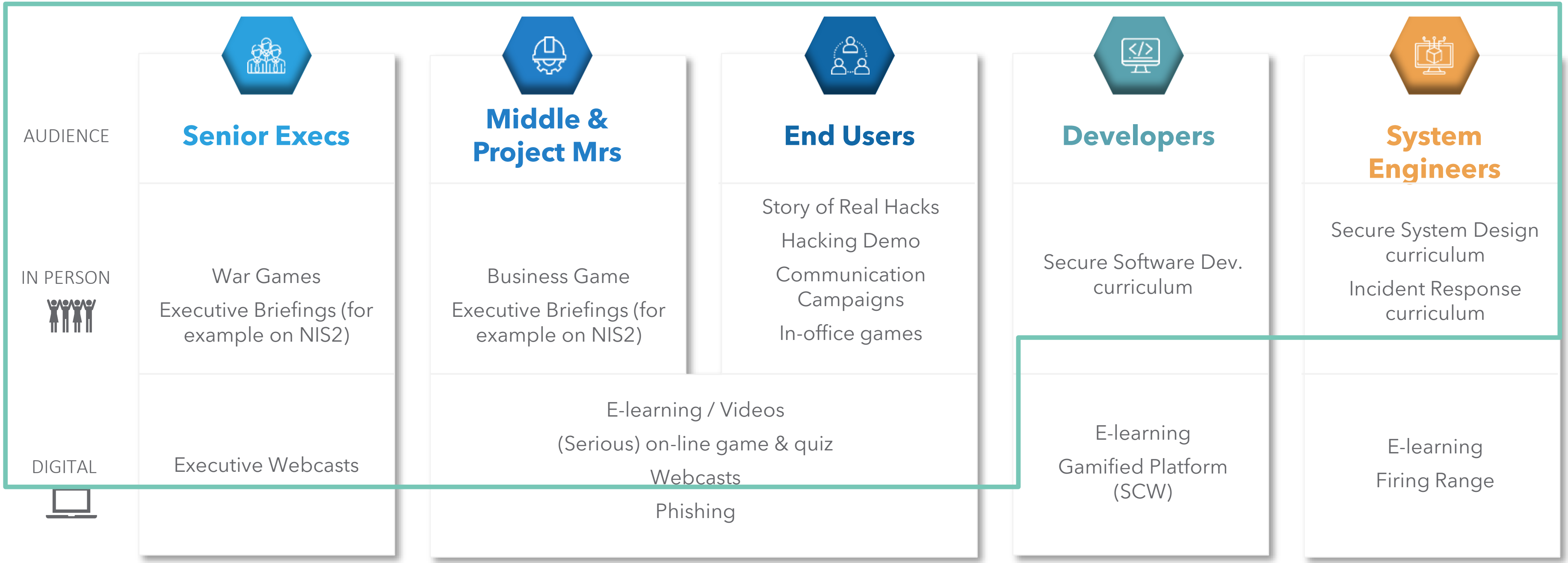
The Human Factor

Possible under Shield GRC

Preventing Incidents

Security Awareness

We assist organizations of all size in creating a **cyber culture** at all levels, mixing **proven communication techniques** with **original in-person and digital solutions**.

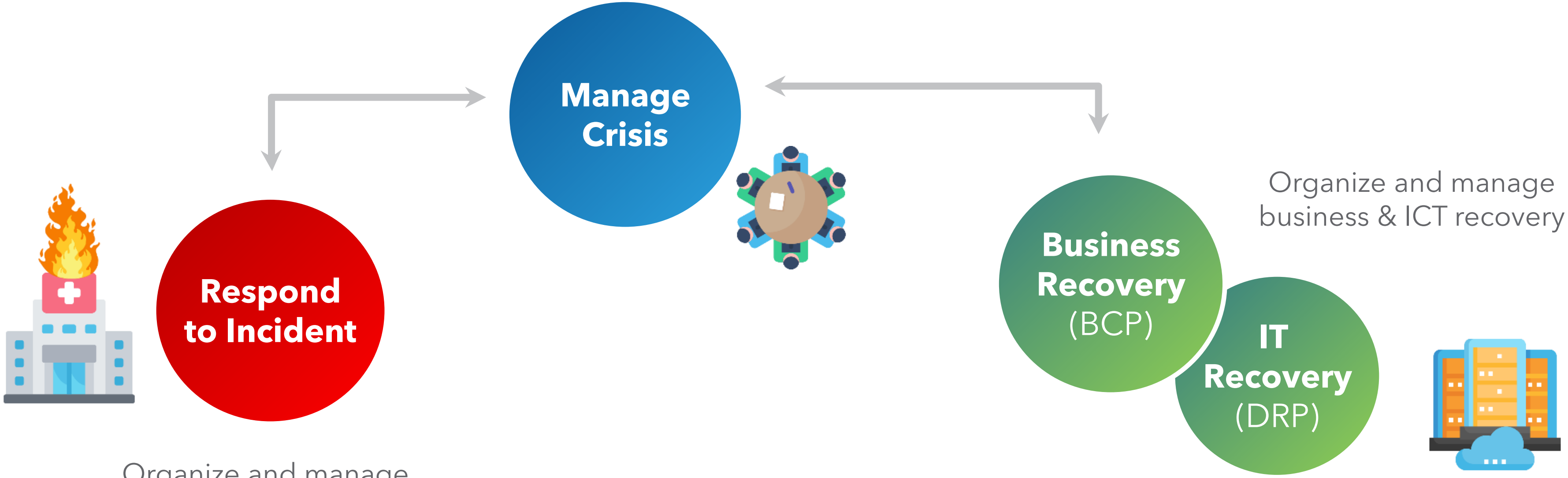


AUDIENCE	Senior Execs	Middle & Project Mrs	End Users	Developers	System Engineers
IN PERSON	War Games Executive Briefings (for example on NIS2)	Business Game Executive Briefings (for example on NIS2)	Story of Real Hacks Hacking Demo Communication Campaigns In-office games	Secure Software Dev. curriculum	Secure System Design curriculum Incident Response curriculum
DIGITAL	Executive Webcasts	E-learning / Videos (Serious) on-line game & quiz Webcasts Phishing		E-learning Gamified Platform (SCW)	E-learning Firing Range

Incident Readiness

Responding to an incident : a threefold approach

Make key business decisions to ensure **Business Continuity**
Steer External & Internal **Communication**



Organize and manage business & ICT recovery

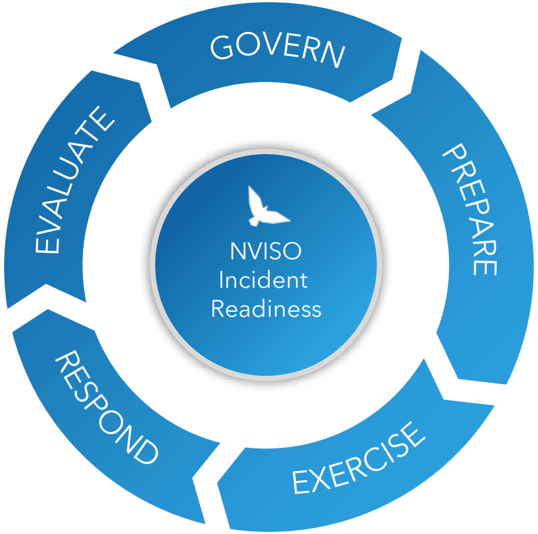
Organize and manage (ICT) operational response

Identify source - Contain attack - Eradicate source

Our Incident Readiness offering

Possible under Shield GRC

We help you be incident ready. Ready to respond efficiently to an incident, to reduce its impact. We work on **incident response** (operational handling of the incident) and **crisis management** (management handling of the communication and strategic business decisions).



GOVERN *Crisis & incident response governance; and briefing & training of roleholders*

- Crisis Management
- Incident Management
- BC & DR Governance integration

PREPARE *Operational response procedures, and key controls to enhance resilience*

- Standard Operating Procedures / Playbooks
- Readiness Checks
- Quick remediations (AD, backups, forensic readiness)

EXERCISE *Train and test plans & people*

- Tabletop Exercises (crisis, incident)
- Recovery Tests
- Attack Simulations & Red Teaming

RESPOND *Help you face a cyber attack*

- NVISO CSIRT - Incident Response
- NVISO CSIRT - Crisis Support
- NVISO CSIRT - Forensics

EVALUATE *Evaluate effectiveness and completeness of response measures*

- Red Teaming
- Audits
- Remediation projects

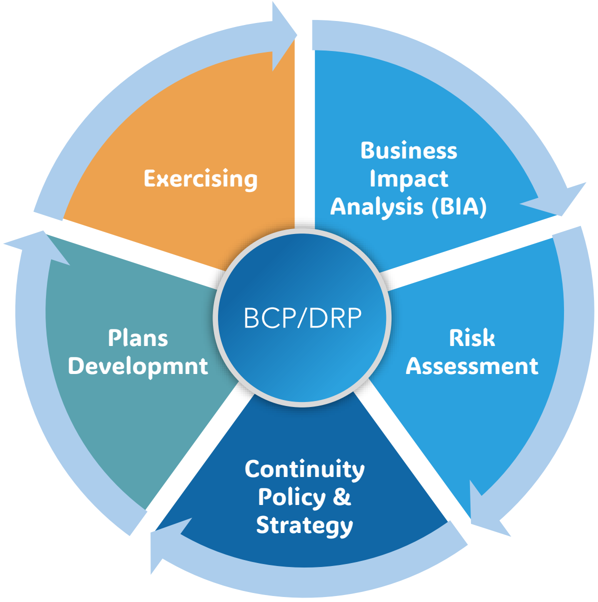
Crisis Management

Incident Management

Possible under Shield GRC

Our Business Continuity Management (BCM) Methodology

We leverage the ISO22301 BCM standard and ISO27031 DRP standard, which has founded our own hands-on methodology.



International Organization for Standardization ISO 22301

International Organization for Standardization ISO 27031

Part 1 – Prioritize Activities

- Business Impact Analysis: define priorities based on RTO (recovery time objective)
- Risk Assessment: identify continuity risks, to reduce them

Part 2 - Prepare Continuity & Recovery

- Business Continuity Strategy: define needs in terms of People, Facilities, ICT Infrastructure, ICT end-user equipment, and third parties.
- Business Continuity Policy: defining your BCM methodology and obligations
- Plan Development:
  - Activity Recovery Plans: Develop operational recovery plans for highly-critical activities
  - Business Continuity Master Plan: your central plan. Defines how to activate and manage BCM mechanisms when a disaster strikes. Includes definition of supporting governance mechanisms, roles & responsibilities.

Part 3: Exercise

- Define test plan
- Execute tests: BCM Test, DRP Test and Crisis Mgt / Incident Mgt test

SHIELD vzw

Possible under Shield GRC

Incident Readiness

Illustrative Examples – Business Continuity & Incident Readiness

Business Continuity & Disaster Recovery Planning

1. Development of a BCP & DRP for one of the largest hospitals in Belgium. Focus on "Minimum Viable IT".

2. Creation of a disaster recovery plan for a hospital.

Incident & Crisis Management

1. Creation of incident response plans, tailored to the needs and dependencies of a hospital.

2. Simulation of table-top exercises with hospitals to verify the organizational & stakeholder readiness to deal with incidents.

We understand the impact of an incident, or crisis on your activities. It's not only about the financial impact…. We're talking about the lives of people.

Conclusion: Why NVISO?

Wrap-up – Why NVISO?

1. Our focus is cybersecurity and our mission is ***to safeguard the European society from cyberattacks. The Healthcare sector is a critical sector within this society*** and we are extremely eager to help the Shield community to better prepare against cyber attacks.

2. We can advise your ***strategically***, but are ***pragmatic*** and think ***threat-based*** to advise you on ***compliance***. We can help you define and implement your roadmap and help you to manage & reduce cyber risk & to achieve NIS2 compliance (ISO27001 or CyFun).

3. We ***understand threats the healthcare sector is facing*** and ***technical expertise*** is deep-rooted in our organization and based on our relevant experience in the healthcare industry.

4. We're committed to ***increase awareness***, in the Shield community and its members and to ***prepare you better detect and respond to security incidents.***

HACKED ?

CALL

+32 (0) 2 588 43 80
+43 (0) 720 228337
+49 69 8088 3829

NVISO • Security. Research. Risk.

www.nviso.eu

nviso