# NNIT Cybersecurity

## A new threat landscape requires a new approach

“

Effective cybersecurity is not about spending more money.

It’s about aligning your security initiatives with the threats and priorities for your business in order to protect it from financial and reputational damage.

**NNIT**

# NNIT Cybersecurity

## A comprehensive cybersecurity portfolio

In today's business climate, companies face three security challenges: finding the right level of IT security; managing changing risk scenarios arising from trends such as Internet of Things (IoT), mobility and cloud; and combating increasingly sophisticated cyber threats. In addition, rigorous new legislations, such as EU General Data Protection Regulation, continually drives the need for dedicated cybersecurity initiatives.

NNIT is a full range cybersecurity provider with a long and proven record of accomplishment. With deep roots in the pharmaceutical industry, we are highly experienced in delivering compliance management, servicing heavily regulated industries, and providing comprehensive business continuity management.

One of our key focus areas is to identify and secure critical customer data and infrastructure. As both supply chains and intellectual property become digital, the need to protect critical systems and data is imperative to ensure the reputation and continuity of the business. Our specialized teams leverage their extensive experience and expertise to help your business address its unique cybersecurity risks.

Read on to learn how our cybersecurity services can help your business stay compliant, secure, and future-ready.

# NNIT Cybersecurity Core Principles

1

**NNIT IS A FULL RANGE CYBERSECURITY PROVIDER**

We provide end to end security services suited to all customers.

2

**COST EFFECTIVE SECURITY**

We take pride in ensuring that we deliver the right level of security, tailored to each customer.

3

**PROTECTING BUSINESS CRITICAL SYSTEMS**

We specialize in protecting our customers' business critical systems, and safeguarding business operations.

NNIT CYBERSECURITY

SECURITY CONSULTING

REGULATORY COMPLIANCE

APPLICATION SECURITY

CYBER DEFENSE CENTER

CLOUD SECURITY

IDENTITY & ACCESS MGMT

MANAGED SECURITY

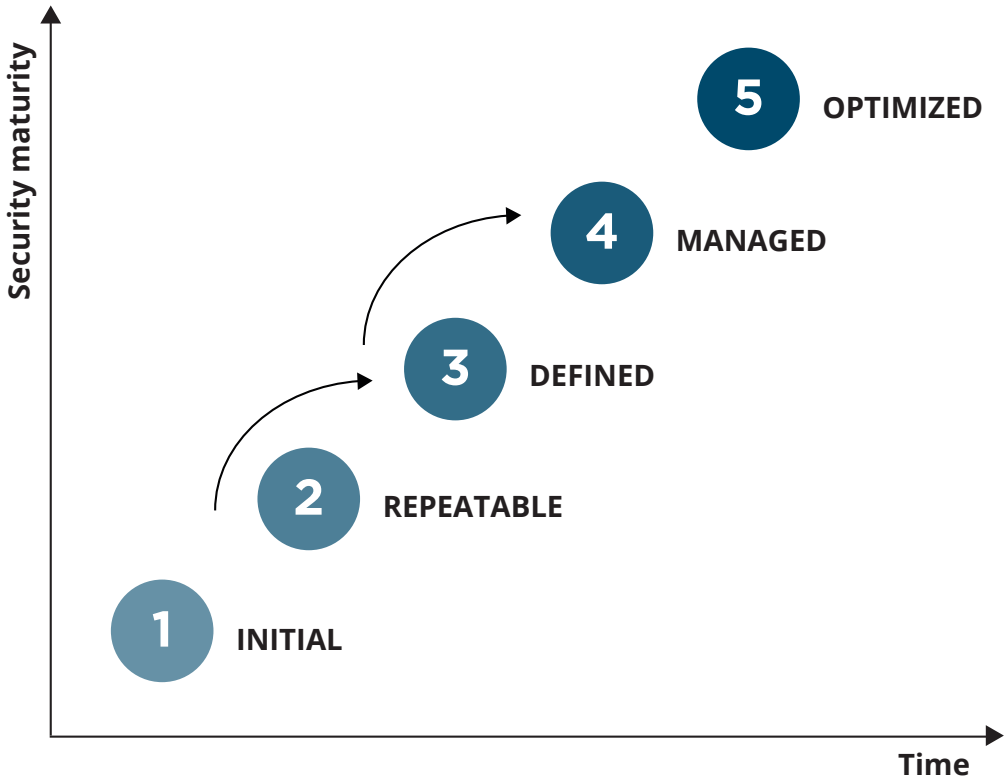
# Security Consulting

## Mapping out your route to effective security protection

Although you may be aware of the need to increase your cybersecurity, it may not be clear where to start, what activities to launch, or how to prioritize them. Without a clear direction, initiatives can become misplaced, unstructured, and ultimately fail to achieve the desired reduction in your organization's risk profile.

Leveraging our extensive knowledge and expertise from consulting and security activities, we offer a unique range of security advisory services. We begin with an initial security assessment to help you gain an understanding of your current threat landscape, pain points, and desired risk profile. We then work with you to develop a roadmap for implementation of identified security initiatives – taking into account all aspects of the security landscape; including people, processes and technology areas.

You will benefit from full access to our team of both consultants and technical subject matter experts throughout your journey to achieving optimized cybersecurity operations.



# Regulatory Compliance

## Staying on top of regulations and industry requirements

At NNIT we have vast experience of working with compliance consultancy across heavily regulated industries that handle highly sensitive data – from GxP quality guidelines and regulations to sector-specific regulatory standards such as the Sarbanes-Oxley Act.

We use this experience to work with new regulations such as the EU General Data Protection Regulation (GDPR), which requires all private businesses and public authorities to implement a sufficient level of IT security and security awareness to protect personal data processed in the organization.

NNIT also help clients adhere to the equally important Network and Information Security (NIS) Directive, which demands providers of critical infrastructure services to take appropriate technical and organizational measures to manage threats to networks and information systems.

Furthermore, we advise clients on various regulatory compliance projects e.g. e-Invoicing, Internal Rating Based (IRB) models, and optimization of AML/KYC processes by utilizing both existing and new technologies in the area of RegTech.

# Quality is the core of our business

Being a company born within the pharmaceutical industry ensures that the elements of quality, compliance and security are a natural part of our DNA.

We understand the importance of delivering the right level of security protection to provide our customers with peace of mind, so they can focus their efforts on core business activities.

# Application Security

## Is your business-critical data secure?

Cybersecurity threats have never been as diverse as they are today, and almost every day new threats emerge. Hackers target the weakest points of organizations in increasingly sophisticated ways, and very often they look to exploit vulnerabilities in applications to gain access to business data.

In the era of digital transformation, the need to secure applications that access business-critical data is higher than ever. It is no longer enough for organizations to only rely on infrastructure security controls to protect their assets. Applications must include built-in security controls to withstand current cybersecurity threats, and organizations should continuously improve the security posture of their applications by adopting secure software development life cycle activities such as security training, threat modeling, and security testing.

Considering security throughout the entire software development life cycle will minimize the risk of security incidents and significantly improve the protection of your business-critical data while maintaining the agility and productivity of your development teams. Security must be taken seriously, even for non-business critical applications in order to prevent attackers from gaining backdoor-access to other critical assets within your organization. In the digital ecosystem, hackers will attack the weakest link.

NNIT's team of application security experts are ready to assist your development teams on their journey to adopt the secure software development life cycle. Our services include:

- Secure software development life cycle advisory
- Application security health check
- Application penetration testing
- Developer training course in application security principles
- Provide general application security design and implementation advisory in areas such as privacy by design, threat modeling, design review, and secure coding.

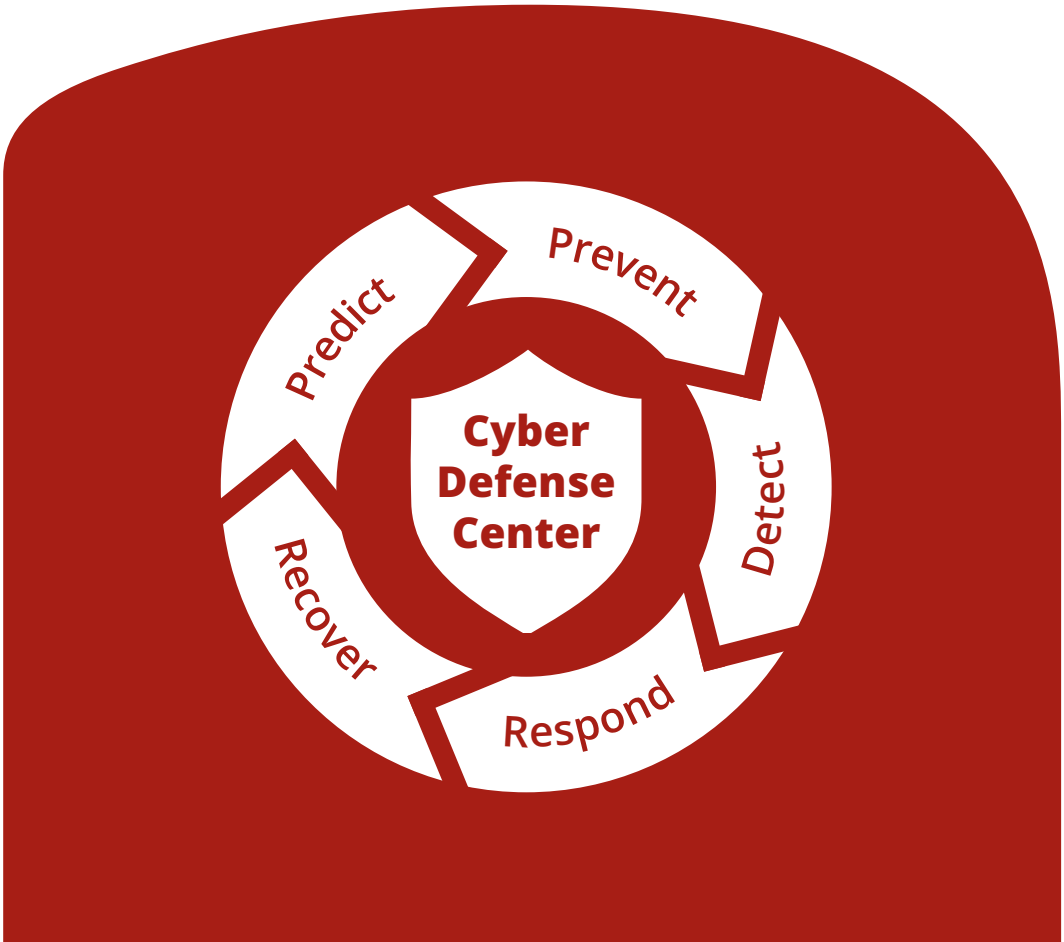
# Cyber Defense Center

## Let NNIT be your first call

Advanced cybersecurity threats and attacks have fundamentally changed the way organizations prioritize and invest in IT security. While preventing attacks is still the primary strategy for securing an organization, breaches will inevitably occur. This makes the need for fast and effective breach detection and response more important than ever.

With the increasing attack sophistication comes increasing detection complexity. Breach detection and response are high-complexity tasks, requiring skilled and experienced security professionals who are both hard to come by and expensive to keep on 24/7 rotation.

Expand your existing protection with true enterprise-class detection and response capabilities with NNIT Cyber Defense Center – one of only a few non-state owned certified CERT teams in Denmark. This will provide you with world-class experts on call to assist you with security needs 24/7.



# Cloud Security

## Securing your data in the cloud

One of the biggest deterrents for companies looking to migrate to the cloud is a concern over cloud security. While no IT investment or transformation is without risk, cloud computing can be an attractive, agile, and cost-effective alternative to traditional IT solutions – provided that you take appropriate steps to ensure cybersecurity.

To help ensure a smooth transition to the cloud, NNIT offers a range of cloud security advisory services to help you identify and mitigate any security risks.

Our Cloud Security Decision Model helps you assess any security aspects of solutions or services considered for cloud migration. The model investigates the security aspects of both the cloud service provider and their associated solution, and allows you to migrate securely to the cloud.

# Identity & Access Management

## Who has access to your confidential data?

The increasing adoption of technology in both business and personal spheres is leading to vastly complex security reservations. Consequently, it is becoming increasingly difficult to maintain control of data and access. As a result, organizations become more vulnerable to security threats, and generally less efficient.

The advancement of cloud-based services presents new challenges and opportunities for managing user identities and access. For this reason, it is vital that processes and policies exist to provide the right people with the right access at the right time – in a secure, compliant, and auditable manner.

Identity and Access Management processes grant users controlled access to applications, systems, and files. Unstructured data, however, falls outside this category and must be addressed specifically. The amount of unstructured data is growing exponentially and is found in all documents, pictures, emails, and a number of other data repositories. With legislation such as the EU General Data Protection Regulation (GDPR), unstructured data represents a huge risk to organizations.

NNIT can support you on your journey to establishing the policies, processes and the right IAM systems to help you safely administrate and protect your IT infrastructure and sensitive information assets in the future.

# Managed Security

## Cost-effective management and monitoring of security solutions

Managing security systems is a complex and time consuming task, as it requires the right workforce with the appropriate in-depth technology insight to operate them. This is why organizations are increasingly turning to Managed Security Services as a way to ensure that the organization's fundamental IT infrastructure security is in place, while allowing them to focus on their core business instead.

NNIT offers both traditional operation manning as well as Detection and Response on security systems with the NNIT Cyber Defense Center. NNIT also offers a systematic approach to managing an organization's security needs. The services cover different functions that includes 24/7 monitoring and management of intrusion detection systems, firewalls, log management, patch, upgrades, security audits, security assessments and emergency response.

Managed Security Services also allows flexibility, as it is gives you the possibility to scale up and down on your security setup as your need for protection evolves.


SAMSUNG

## About NNIT

NNIT A/S is one of Denmark's leading IT service providers and consultancies. NNIT A/S offers a wide range of IT services and solutions to its customers, primarily in the life sciences sector in Denmark and internationally and to customers in the public, healthcare, enterprise and finance sectors in Denmark.

**www.nnit.com**


NNIT A/S Østmarken 3A DK-2860 Søborg Tel: +45 7024 4242
NNIT Switzerland Bändliweg 20 CH-8048 Zurich Tel: +41 44 405 9090
NNIT Germany c/o Regus Herriotstrasse 1 DE-60528 Frankfurt am Main Tel: +49 69 66 36 98 73
NNIT Czech Republic Explora Jupiter Bucharova 2641/14 2.NP CZ-158 00 Prague 5 Tel: +420277020401
NNIT USA 4 Research Way Third Floor Princeton New Jersey 08540 Tel: +1 (609) 945 5650
NNIT China 20th floor, Building A, Jin Wan Mansion, 358 Nanjing Rd. CN-Tianjin 300100 Tel: +86 (22) 5885 6666
NNIT Philippines Inc. 10/F, 2251 IT Hub 2251 Chino Roces Avenue Makati City 1233 Tel: +63 2 889 0999
NNIT United Kingdom c/o MoFo Notices Limited CityPoint One Ropemaker Street London