

*Unlocking Business  
Opportunities with NIS2  
Compliance*

A Readiness Playbook for  
Microsoft Channel Partners

May 2024

# Your NIS2 Readiness Playbook





*NIS2.0 is a pivotal step in enhancing cybersecurity for customers, significantly improving their capabilities to handle the ever-evolving cyber threats. For Microsoft Security partners, NIS2.0 represents a significant opportunity to lead the way in cybersecurity, offering comprehensive solutions that align with the directive's standards. This is not just about compliance; it's about setting a new benchmark for cybersecurity excellence and becoming a trusted advisor to customers navigating this new landscape.*

Mikko Viitaila

National Technology Officer, Microsoft Western Europe

# Welcome to Unlocking Business Opportunities with NIS2 Compliance:

## A Readiness Playbook for Microsoft Channel Partners

The Network and Information Systems Directive 2 (NIS2), a significant milestone in European Union cybersecurity legislation, is set to take effect in October 2024. It establishes a baseline of cybersecurity measures for organizations providing essential services across sectors such as municipalities, healthcare systems, financial services, and manufacturing firms (15 sectors in total). Compliance with NIS2 isn't merely a box-ticking exercise; in many cases, it is a customer necessity and, in all cases, a strategic business opportunity.

### Capturing Your NIS2 Opportunity:

- **Train Your Sales & Technical Team:** Make sure you have identified the right training paths for your sales team. If you want to identify additional opportunities for growth, you can assess your current offerings and competencies.
- **Choose the Right Customers/Prospects:** Identify organizations within the 15 sectors covered by NIS2 that can benefit from your expertise. These are the entities seeking to enhance their cybersecurity resilience and achieve optimal health in their digital defences.
- **Create a Complete, Profitable, Recurring NIS2 Offer:** Craft a comprehensive NIS2 solution that goes beyond compliance. By offering a holistic package, you position yourself as a trusted partner in safeguarding your customers' cyber health.
- **Develop Your Sales/Marketing Business Outcome Narrative:** Articulate the value proposition of your NIS2 services. Highlight how compliance not only protects critical infrastructure but also contributes to long-term cyber wellness. Your narrative should resonate with organizations aiming for robust security position.
- **Train Your Sales & Technical Team on your NIS2 Offer:** Equip your sales force with the knowledge to engage effectively with customers about NIS2 requirements. Understand their pain points, address concerns, and emphasize the positive impact on their overall cyber health.
- **Partner Up!:** If your customers have needs you do not offer, collaboration is key. Consider a partner-to-partner (P2P) approach, leveraging complementary skills and resources.

### Getting Started:

Begin by reviewing our NIS2 readiness guide.

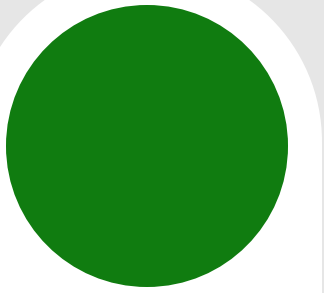
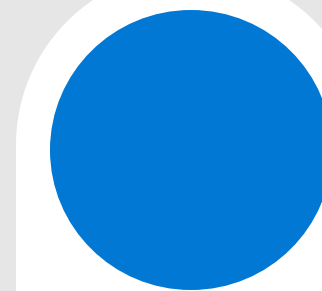
Transform regulative compliance into a strategic advantage, ensuring your organization thrives in the ever-evolving cybersecurity ecosystem while helping your customers achieve cyber security health.

# Unlocking Business Opportunities with NIS2 Compliance:

## A Readiness Playbook for Microsoft Channel Partners

### Agenda

- The NIS2 Opportunity
- How to Capture Your NIS2 Opportunity:
  - Choose the right customers/prospects
  - Create your complete, profitable, recurring NIS2 Offer
  - Partner up! Use a P2P approach if needed
  - Create your sales and marketing business outcome narrative
  - Train your Sales & Technical teams
- How to get Started
- Additional Resources



# The NIS2 Opportunity



# 168

**days until NIS2 compliance needs to be in place.** Captured 2 May 2024

# 61%

**of partners surveyed estimate their security business will grow >10% in 2024. With this approach, we see that as being >20%.**

# 12

**weeks on average it will take a customer to manually be NIS2 compliant. 2-3 if automated.**

# NIS2 Objectives and Accountability

## NIS2 Objectives

### Manage Security Risk

Ensure cyber security risk assessments are carried out

### Protecting Against Cyber Attack

Implement technical and organisational measures

### Detecting Cyber Security Incidents

Stay on top of cyber security threats through training and risk management programs

### Minimizing The Impacts of Cyber Security Incidents

Manage risks appropriately

## NIS2 Principles

- A1: Governance
- A2: Risk Management
- A3: Asset Management
- A4: Supply Chain

- B1: Service Protection Policies and Processes
- B2: Identity & Access Control
- B3: Data Security
- B4: System Security
- B5: Resilient Networks and Systems
- B6: Staff Awareness and Training

- C1: Security Monitoring
- C2: Proactive Security Event Discovery

- D1: Response and Recovery Planning
- D2: Lessons Learned



**Trusted Advisor Tip**  
Management will be held personally accountable for non-compliance



# NIS affects various sectors, including...

## Essential Entity

Large companies are part of the sectors of high criticality listed in Annex I of the Directive.

**A large entity is defined as a company with at least 250 employees**

Or

with an annual turnover of at least 50 million euros or an annual balance sheet total of at least 43 million euros.

Failure to do so can result in:

Fine of >10 million Euro or 2% of global annual turnover for **essential entities** and >1.7 million Euro or 1.4% of global annual turnover for **important entities**

## Important Entity

Medium-sized enterprises operating in the sectors of high criticality of Annex I of the Directive, Large or medium-sized enterprises in the sectors of Annex II of the Directive that do not fall into the essential entity category (due to their size or the type of entity involved).

**A medium-sized enterprise is defined as one with at least 50 employees**

Or with an annual turnover (or balance sheet total) of at least 10 million euros, but with fewer than 250 employees

And no more than 50 million euros annual turnover or 43 million euros balance sheet total.

# NIS2 Target Sectors

## Essential sectors:

-  Energy
-  Transport
-  Banking
-  Financial market infrastructure
-  Health sector
-  Drinking water
-  Wastewater
-  Digital Infrastructure
-  IT service management
-  Public administration
-  Space

## Important sectors:

-  Postal and courier services
-  Waste management
-  Chemicals
-  Food
-  Manufacturing of medical devices
-  Digital providers
-  Research organizations



### Trusted Advisor Tip

Regardless of where a company is located, if selling into the EU and appropriately sized, companies must be compliant.

# What do customers need for NIS2 Compliance?

a mandatory legal foundation

a strong technical cyber protection foundation

internal processes and cyber security governance

cyber security awareness trainings for everyone

proof of NIS2 compliance - at any given time

identify cyber breaches and report to authorities

fix cyber breaches and report completion

continuously operate, monitor and improve

**Forever.**



*Make no mistake: the European legislation has been formally adopted in 2022. The requirements are clear and will not change. The EU member states are legally required to write national legislation based on the current text of the NIS2. They can expand the requirements a little, but the crux of the matter is solidly clear.*

Benedikt Marijnen

Lawyer, Founder of Waveland European Lawyers

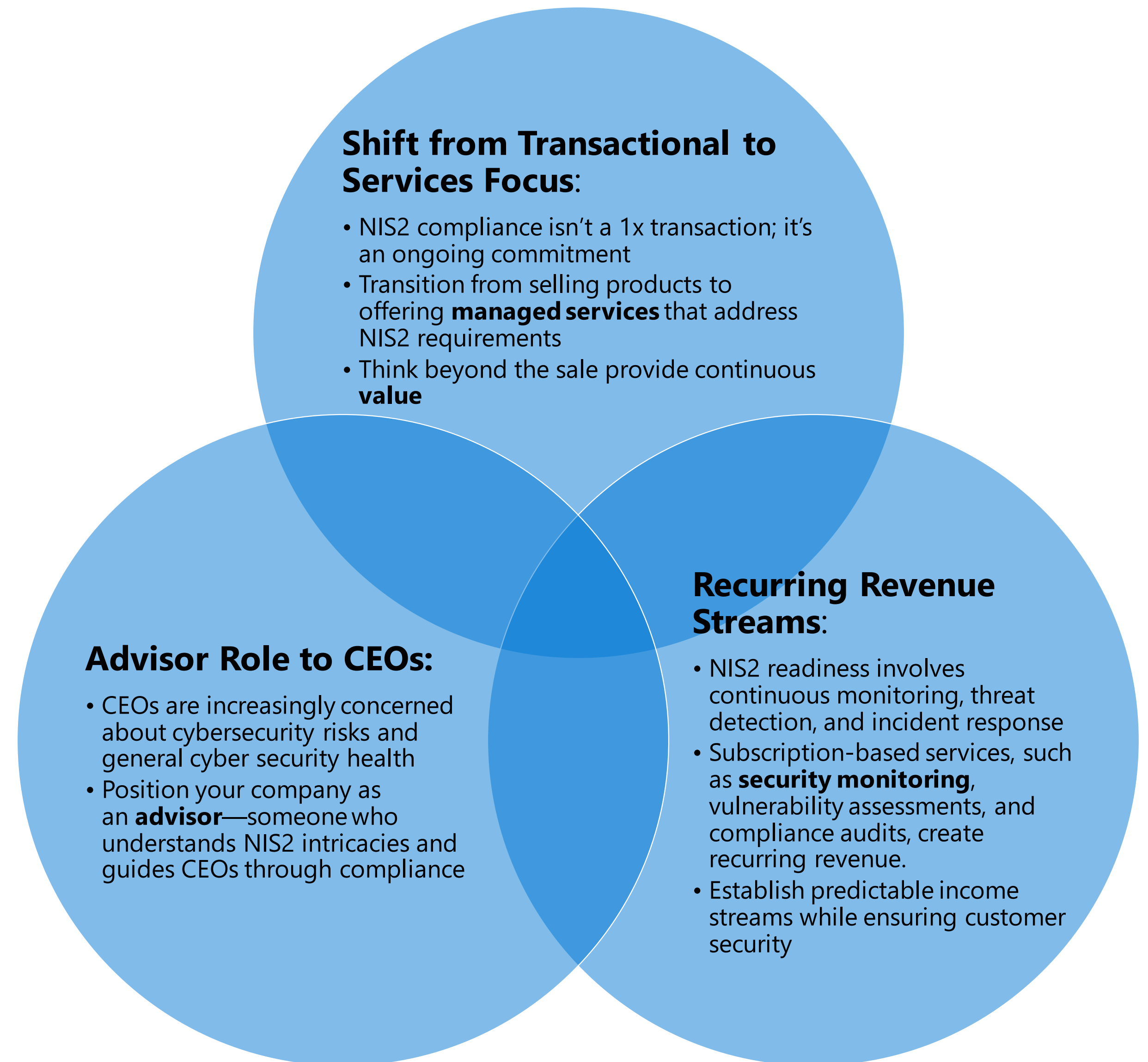
# NIS2 makes doing business safer in the EU

It will prepare us for future cyber threats and make sure everyone plays their part in making sure we are secure.

**This is your opportunity to build your**

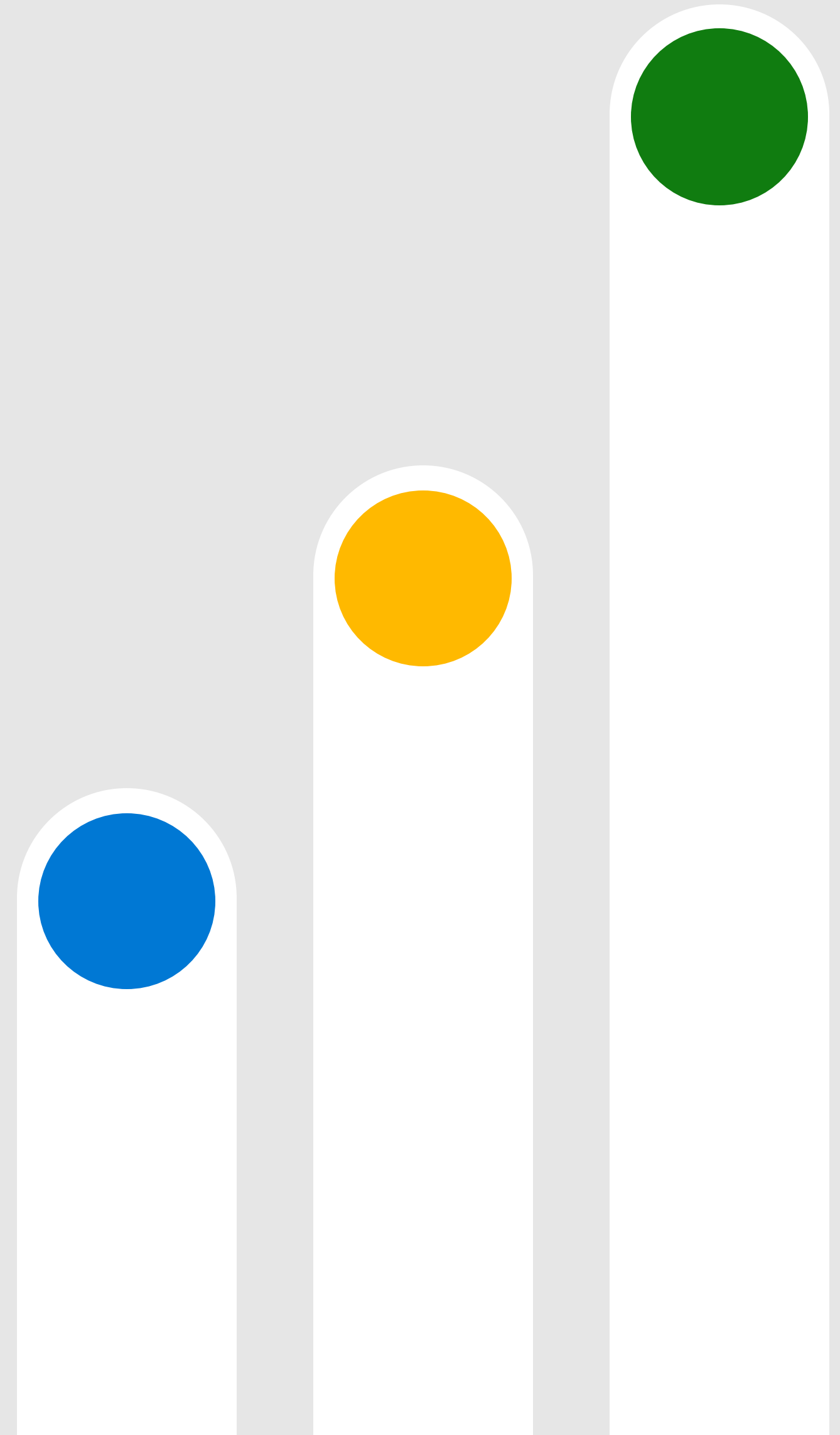
**Practice**

**focused on Cyber Security Health and Business Resilience**



Deadline for compliance with NIS2  
Directive is approaching fast.

**Do you already  
have an agreed  
plan with your  
customers for  
NIS2?**



# How to Capture Your NIS2 Opportunity



# 4 steps to target the full NIS2 business opportunity

In this section, we take you through how to ...

- ① Choose the right customers/prospects
- ② Create your complete, profitable, recurring NIS2 Offer
- ③ Develop your NIS2 sales/marketing business outcome narrative
- ④ Train Sales team to engage with customers on business outcomes and technical team



# Step 1:

## Choose the right customers/prospects

In this section, we will take you through how to choose which of your current customers are targets for NIS2. If you want to, you can also apply the same approach for a competitive play.

# Step 1: Know your customers/prospects

## 3 Starter Questions:








1. Who are your targets?
2. Which departments do you work with at these targets?
3. How much do you know about them?

# Who? →

## Essential sectors:

-  Energy
-  Transport
-  Banking
-  Financial market infrastructure
-  Health sector
-  Drinking water
-  Wastewater
-  Digital Infrastructure
-  IT service management
-  Public administration
-  Space

## Important sectors:

-  Postal and courier services
-  Waste management
-  Chemicals
-  Food
-  Manufacturing of medical devices
-  Digital providers
-  Research organizations



### Best Practice Tip:

Use Microsoft Cloud Ascent to filter your customer base for target customers.

# Who do you work with at these targets?

Identify all of your current contacts, rate the quality of that contact  
Connect in LinkedIn with anyone you do not have as a contact



Chief Security Officer



CEO



DPO



Compliance Team



CFO/Legal



CIO & IT Dept



CMO/COO/CCO

# How much do you know about them?

Now that your core targets are identified, how much do you know about them?

Knowing more about your customers is important for identifying the right narrative for a NIS2 discussion

## Do you know...?

### 01 CEO

- Have they committed a high degree of Cyber Security Health to Shareholders?
- What would the impact of a production stop be?
- Have any of their industry peers in country or region been attacked?
- Do they have high employee turnover?

### 04 Compliance Lead/Manager

- Do they have a compliance lead?
- Are they in a highly regulated industry?
- Do they have ISO and other certifications?

### 02 CFO/Legal

- Are they selling in high-risk verticals?
- Are they selling in multiple EU countries with different legislation?
- Have they calculated their potential 'cost of breach' against costs to be NIS2 compliant?

### 05 Data Protection Officer

- Have they had a data breach?

### 03 CISO, CIO, CTO, Director IT

- What is their IT Maturity?
- Resources overloaded?
- Still running old legacy staff and End-of-Life/Support systems?
- What is their Microsoft IT Footprint?
- What is their Microsoft Security Score?
- Are they in a high-risk vertical?

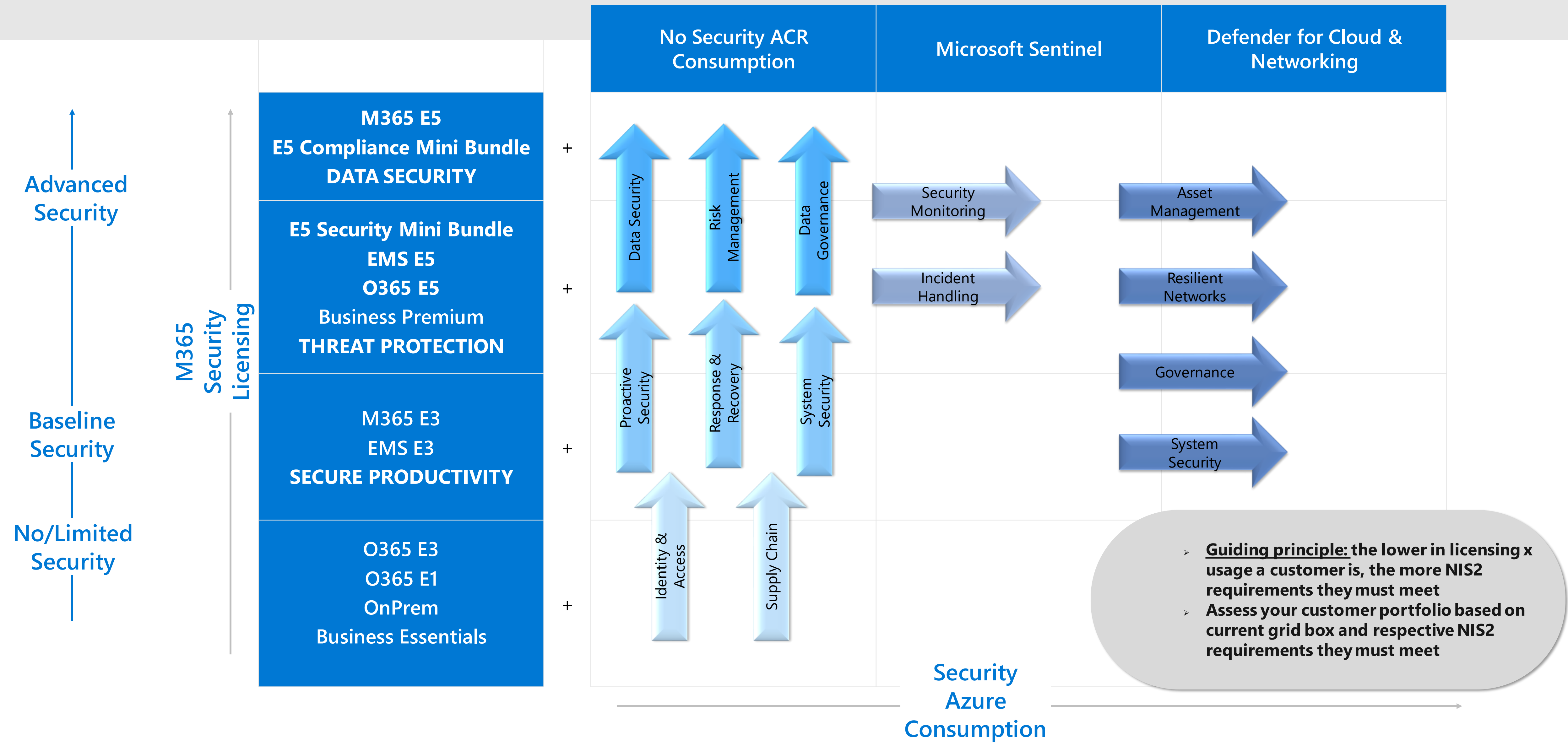


#### Best Practice Tip:

**Check downstream targets:** customers who work with NIS2 target accounts and want/need to be compliant



# Customer Profiles Subject to NIS2



# Checklist

Personas are important, but best practice is moving toward highly **effective customer intelligence** gathering and analysing.

- If unconnected, combine databases
- Identify NIS2 Targets based on guidelines
- Do a data quality check (e.g. replace office@)
- Where you do not have contacts, identify and connect in LinkedIn Sales Navigator
- If you have/can get information from [page 22](#), add to data quality
- Identify starter revenue opportunities based on analysis. You may want to revise this up, if you choose to repackage your Offer in the next section
- If you would like to make a competitive play, identify prospects using the same segmentation
- Don't forget to leverage [Microsoft Cloud Ascent](#) data (updated monthly)
- Use [Microsoft Lighthouse for Microsoft 365](#) to see security foundation and needed actions for customers
- Use [Microsoft Sales Advisor](#) to identify customer target list for targeting

## Ongoing

- Establish process to collect, cleanse, analyse, act, reflect regularly

## Step 2:

## Create your NIS2 Offer

In this section, we will take you through how to create your NIS2 Offer; including relevant partner-to-partner (P2P) opportunities.





*Packaging isn't merely functional - it's a powerful tool for conveying value, captivating customers, and outshining competition.*

Per Wergren

former Worldwide President of IACMP

# It's all about packaging

Many IT companies just sell hamburgers and fries ... separately

Experts sell a Happy Meal

Many good products pulled together to offer an Experience

... providing a better experience at a higher profit margin





*Microsoft is a Security platform provider that can be the baseline of all solutions you offer to your customers depending upon where they are on their NIS2 journey.*

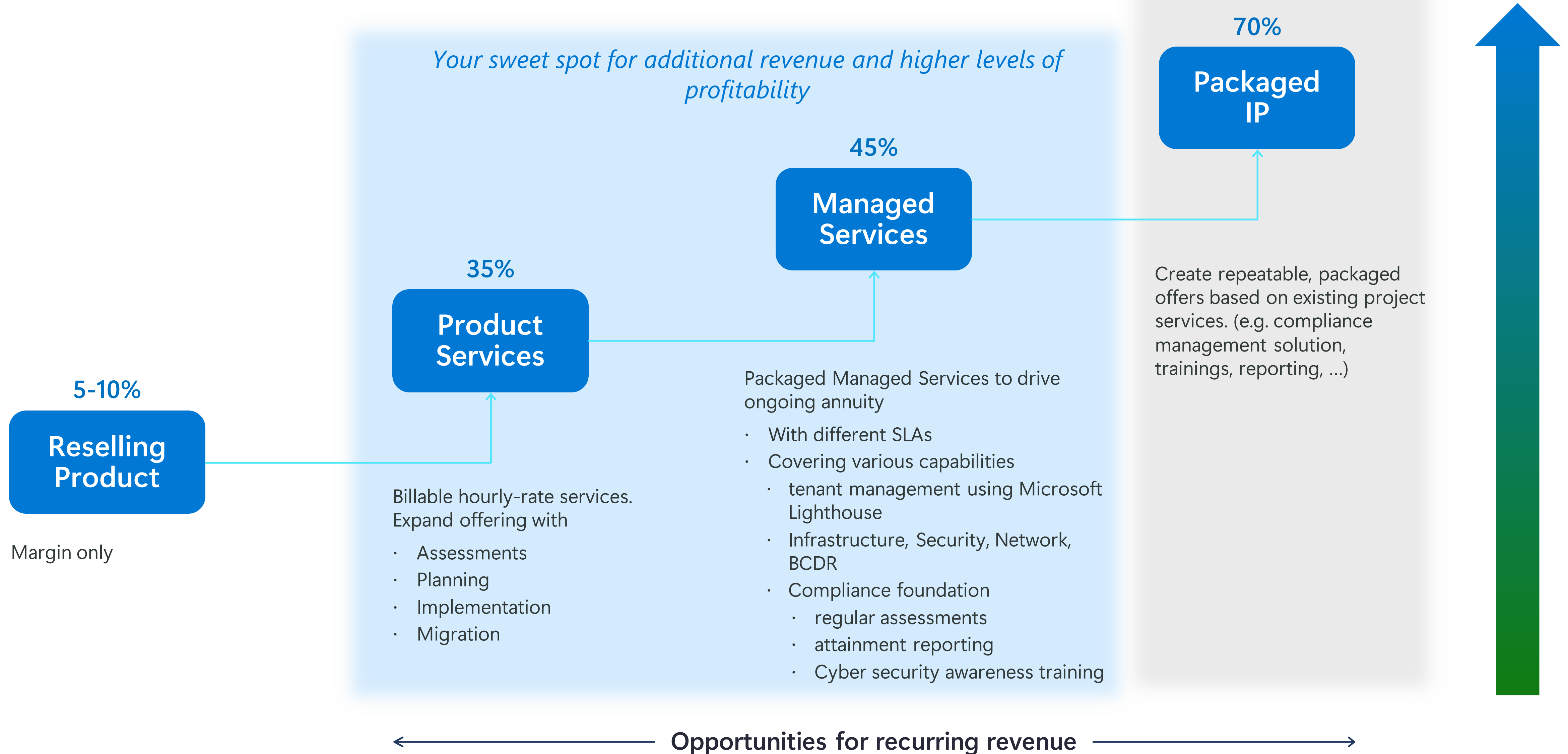
*The Directive, also introduces many more concepts such as regular employee training, monitoring of cybersecurity infrastructure health, etc. that can be additional revenue streams for you to offer to complement the technology part of your offer.*

Leahanne Hobson

Founder/CEO Alinea Partners

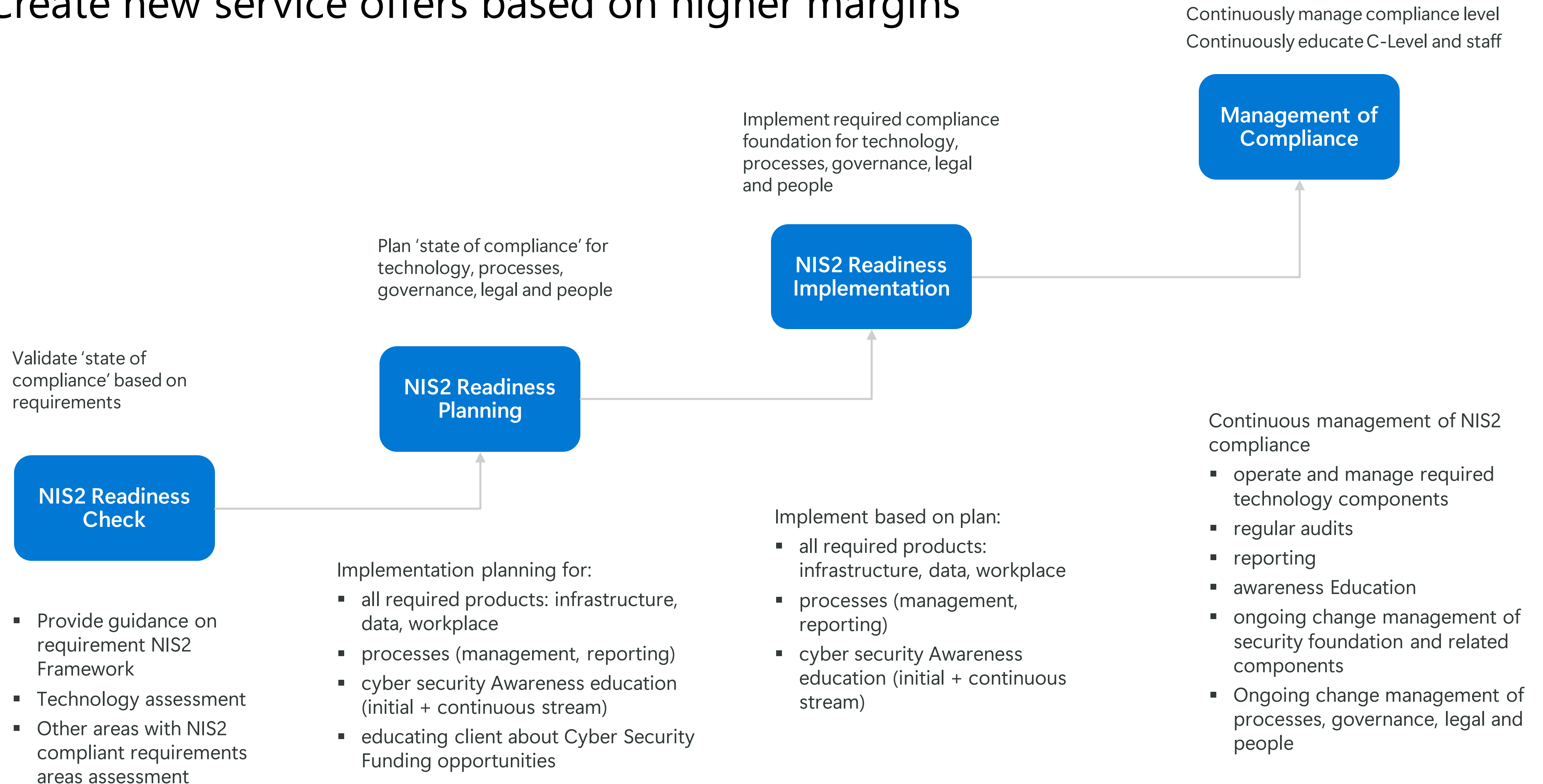
# Journey to higher profitability

Create new service offers based on higher margins



# NIS2 Compliance Journey – Your Opportunities

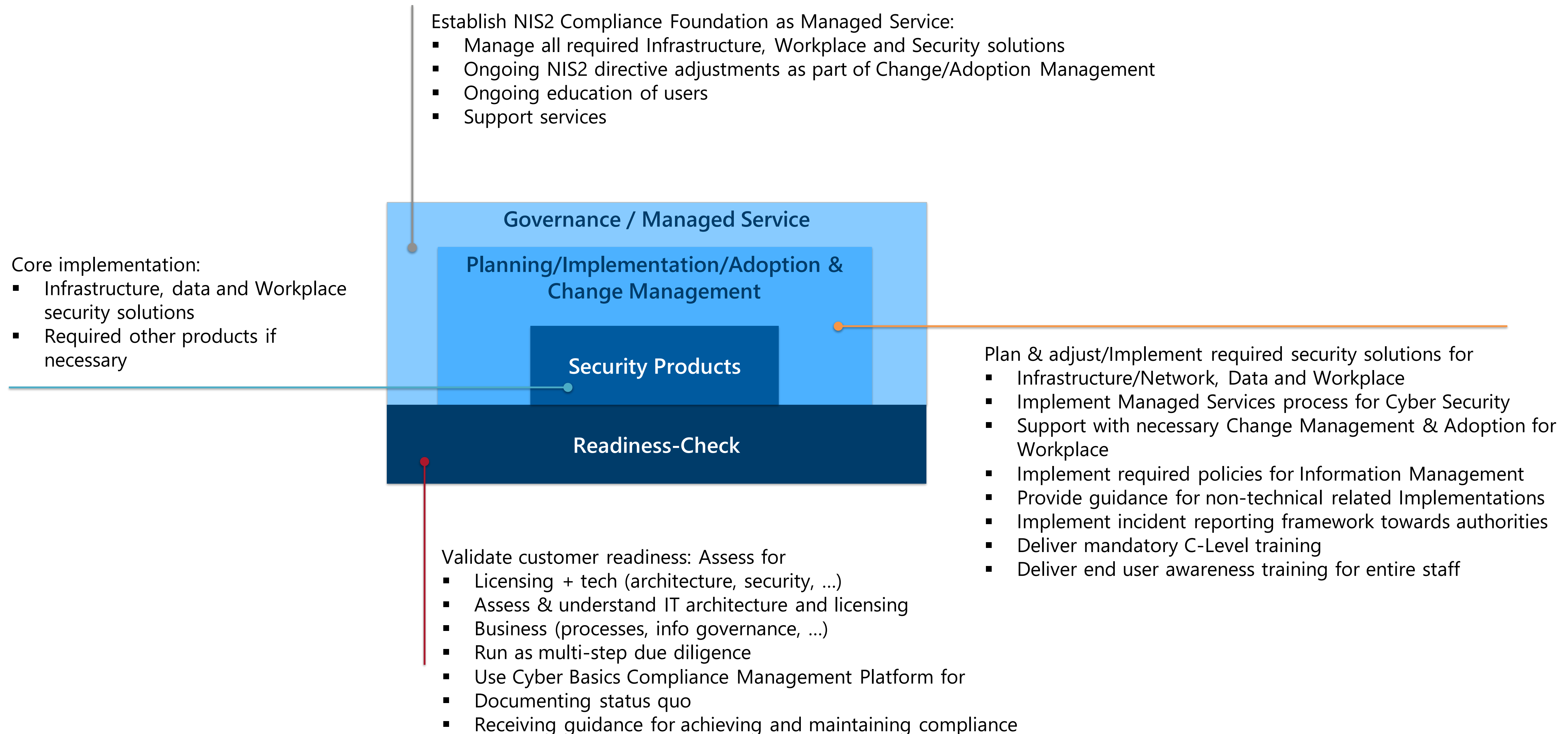
Create new service offers based on higher margins



# Your Offer Framework Elements

Build your offer based on layers around a core Security implementation to increase coverage of value chain and control.

OPTION: Add [Secret Ingredient #1](#)



# NIS Objectives mapped to Microsoft Solutions

## High Level Summary

NIS Principles	Microsoft Solution
Governance	<a href="#">Defender Cloud Security Posture Management (CSPM)</a> , <a href="#">Entra</a> , <a href="#">Purview Compliance Manager</a> with NIS2 assessment template (search for "ENISA") + ISO templates
Risk Management	<a href="#">Defender XDR</a> and <a href="#">Purview Insider Risk Management</a>
Asset Management	<a href="#">Defender CSPM</a> , <a href="#">Defender for Endpoint</a>
Supply Chain	<a href="#">Defender XDR</a> , <a href="#">Entra</a> and <a href="#">DevOps</a> , <a href="#">Dynamics Supply Chain Management</a>
Service Protection	<a href="#">Defender for API</a>
Identity & Access	<a href="#">Entra</a> , <a href="#">Defender for Office 365</a>
Data Security	<a href="#">Purview</a> ( <a href="#">Information Protection</a> , <a href="#">Data Loss Prevention</a> , <a href="#">Insider Risk Management</a> , <a href="#">Unified Data Governance</a> , <a href="#">Data Lifecycle Management</a> , <a href="#">Records Management</a> ), <a href="#">Microsoft 365 backup</a> , <a href="#">Azure Backup</a> , <a href="#">Defender for Office 365</a> , <a href="#">Defender for Cloud Apps</a>
System Security	<a href="#">Defender for Endpoint</a> , <a href="#">Defender for IoT</a> and <a href="#">Intune</a>
Resilient Networks	<a href="#">Azure Network Security</a> including 3rd party integration with the major NDR vendors
Staff Awareness	<a href="#">Purview Policy Tips</a> , <a href="#">O365 Phishing Simulation</a> and <a href="#">Learning Paths</a> , <a href="#">Security Copilot</a>
Security Monitoring, Incident Management	<a href="#">Microsoft Sentinel</a> , <a href="#">Security Copilot</a>
Proactive Security	<a href="#">Defender XDR</a>
Response and Recovery	<a href="#">Defender XDR</a> , <a href="#">Azure Backup and Recovery</a> , Purview <a href="#">Data Lifecycle Management</a> and <a href="#">Records Management</a>
Lessons Learned	N/A (Open AI)

# NIS Objectives mapped to Microsoft Solutions

## Deep Dive per Workload, Functionality and Licensing Program

We heard your feedback that you need a robust overview of the full Microsoft Security stack, its functionalities and available licensing programs mapped to NIS.

Utilise our NIS x Microsoft Security Product Map build your customer services or advisory offer and answer questions like:

- *What products do I need from Microsoft to meet NIS requirements (vs. what I have already?)*
- *Is a small customer under 300 seats covered with M365 Business Premium?*
- *What add-ons are needed to meet NIS2?*
- *Can I buy E5 add-ons to existing M365 Business Premium or M365 E3?*
- *Does M365 Business Premium support Data Security requirements for Copilot and NIS2?*

### Mapping NIS 2.0 Duties to the Microsoft Zero Trust

Verify explicitly | Use least-privileged access | Assume breach

**Governance A & G**

**Identities I & J**

**Devices H & I**

**Zero Trust policy**

**E** NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

**Security in network and information systems acquisition, development and maintenance**

From acquisition to maintenance, ensuring network and information systems security is paramount. Ongoing maintenance demands constant monitoring, timely patches, and regular security assessments to safeguard data integrity and operational stability.

**Sentir B, E, F**

**Defender Vulnerability Management**

Defender Vulnerability Management (DVM) delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices. Leveraging Microsoft threat intelligence, breach likelihood predictions, business contexts, and... Defender Vulnerability Management rapidly and... biggest vulnerabilities on your most critical assets... recommendations to mitigate risk.

**Cloud Security Posture Management**

Cloud Security Posture Management (CSPM) provides... that helps you efficiently and effectively improve yo... visibility into your current security situation.

**F** NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

**Policies and procedures to assess the effectiveness of cybersecurity risk-management measures (1)**

Although there are many methods and frameworks for policies, procedures and assessing the effectiveness of cybersecurity risk-management measures, common steps are:

- Understand the security landscape of your organization, including its assets, systems, vendors, and regulations
- Identify gaps in your current cybersecurity controls, such as outdated software, weak passwords, or phishing vulnerabilities
- Create a team of qualified and experienced cybersecurity professionals who can monitor, respond, and improve your security posture
- Determine the informational value of your assets and prioritize them based on their importance and sensitivity
- Analyze and address the risks that pose the most threat to your assets, using tools such as penetration testing, risk scoring, and mitigation strategies

Get started with **DVM** and **CSPM**

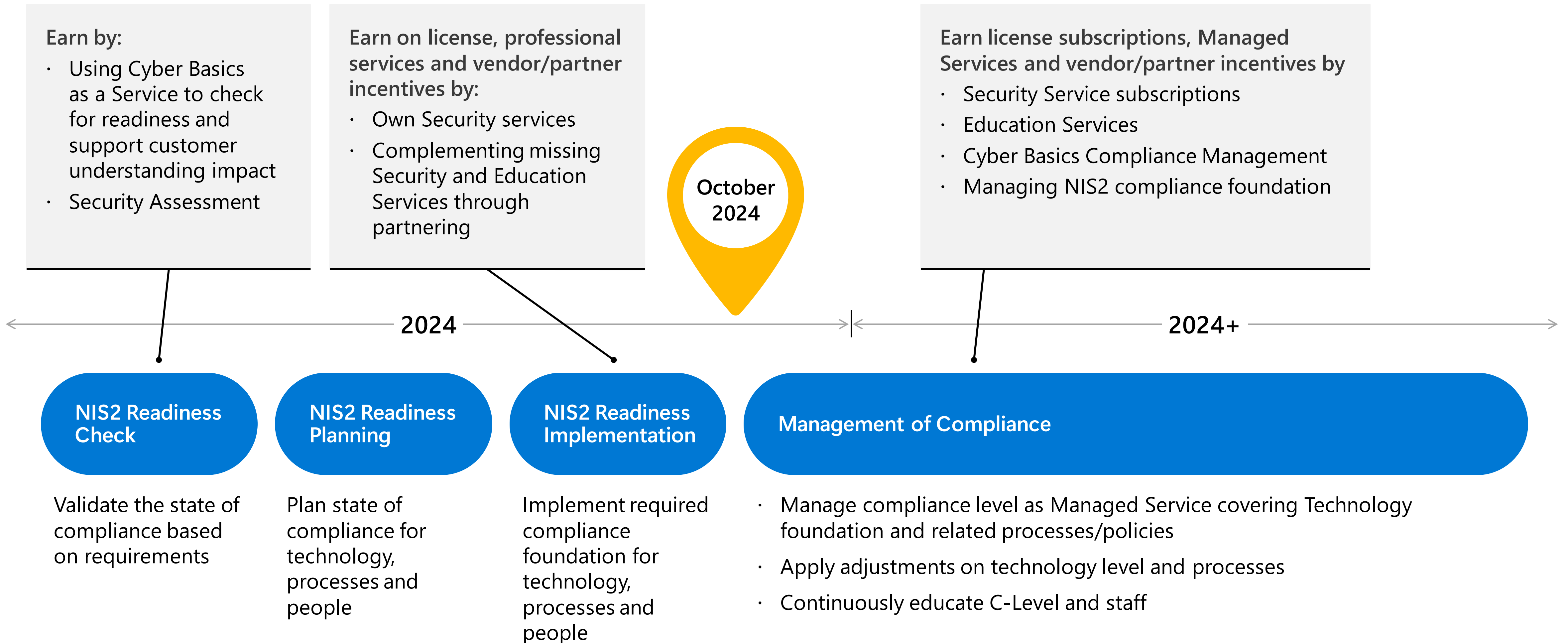
More information on [Zero Trust](#)

Download our NIS x Microsoft Security Product Map [here](#)




# Your business opportunity

There are various business opportunities for you to support your customers in achieving NIS2 compliance, and even more in helping them maintain it through clever Managed Services added to the core technology stack.



**Partner up! Use  
a P2P approach  
if needed**





*We put a NIS2 Compliance Management platform in the centre of gravity and wrapped Security Services, a Management layer around it. We also added "hands-on" support to continue to be part of the customer's journey.*

SoftwareOne

# Secret Ingredient #1

## Automate NIS2 Compliance Management with CyberBasics

If you are not a Compliance or NIS2 expert, but want to provide your customers with the service, CyberBasics can be a solid addition to your Offer Package

It is a Management System to **implement and manage NIS2**

- including **all legal requirements**
- including **base technical assistance**
- including **base legal assistance**
- designed for **Enterprise / SME / Supply Chain Partners**
- as an **annual** license
- providing **Proof of compliance** with the NIS2 legislation at any time.



**CyberBasics lets you walk your customers through NIS2 step-by-step.**  
**Contact for a CyberBasics Demo: Erik-Jan Frieser [ejfrieser@frsch.nl](mailto:ejfrieser@frsch.nl)**

# Cyber Basics NIS2 Compliance Management Process

## Assessment

NIS2 readiness: Organization status?

Direct insight into the status in relation to the requirements of NIS2, showing what security services, processes, legal foundation are missing.

## Knowledge

Obtain & Share

All knowledge about the relevant requirements of NIS2. Sharing knowledge across the organization

## Implementation

always insight into status

Policies and procedures readily available. Already written for the organization. Supplementing with your own business operations

## NIS2 organizational management

Structured entry requirements. Always insight into progress and status

## Communication throughout the organization

Tasks and assignments to all employees of the organization. Overview status handling, archive all actions.

## Demonstrable NIS2 Compliant

Continuous, internal management, manageable, improvement organization

All compliance management + status in 1 online system. Essential laws and standards available on 1 platform for your organization.

# P2P Framework for NIS2

To achieve and maintain compliance with the NIS2 Directive, a comprehensive approach is essential. While you may not possess all the skills and capacity to address every aspect, it's advisable to take initiative and coordinate efforts beyond your organization's direct capabilities.

Collaborating peer-to-peer with partners who can fill in the gaps not only maintains your leadership role with your customer, but also enhances your potential for revenue and profit growth.

## Cyber Security / NIS2

### Project Management/Change Management

### Compliance Management/Legal

### Change & Adoption Management

#### Security Services

- Infrastructure
- Workplace/Applications
- Data
- Managed Services

#### Education/Awareness

- Initial C-Level training
- Initial staff training
- Continuous Security Awareness Education

Cyber Security / Liability Insurance

# Checklist

- Assess your NIS2 Offer status quo
- Evaluate the Offer Framework outlined in this chapter
- Identify the elements you want to offer your NIS2 customer targets
- Consider partnering if other gaps identified
- Ensure you can deliver the offer
- Evaluate value guidance for your profitability on [page 28](#) and adjust your offer pricing accordingly

For additional help and relevant contacts, refer to the end of the Playbook

## Step 3:

### **Develop your NIS2 sales/marketing business outcome narrative**

In this section, we will take you through how to create your NIS2 business outcome messaging and recommend some marketing and sales tactics



# Where customers struggle

NIS2 pain points where end users are challenged already

40%

Limited visibility into IT environment<sup>1</sup>

39%

Lack of knowledge for incident response<sup>1</sup>

35-44%

Unskilled personnel<sup>1,2</sup>

48%

Struggle to adapt employee training programs<sup>2</sup>

32%

Legacy apps creating cybersecurity exposure<sup>2</sup>

## Source:

- 1) The State of Threat Detection, Investigation and Response Report 2023, IDC
- 2) 2023 Cybersecurity Research Report, Rackspace and Microsoft



## Trusted Advisor Tip

Strengthen your trusted advisor positioning. Ask leading questions around these struggles

# Conversation Starters

Now that your core targets are identified, and you know a bit more about them, try to identify the right conversation starters

## 01 CEO

- How is the company adapting its strategies to comply with the new NIS2 directive?
- What impact do you foresee NIS2 having on our overall business operations and risk management?

## 04 Compliance Lead/Manager

- What processes are in place to monitor and report on your adherence to NIS2 regulations?
- How can we proactively address any compliance gaps identified during NIS2 assessments?

## 05 Data Protection Officer

- How is data protection being enhanced to meet the privacy and security standards of NIS2?
- What communication channels exist for reporting data breaches in accordance with NIS2?

## 02 CFO/Legal

- How is the financial planning being adjusted to ensure resources are allocated for NIS2 compliance?
- What budget considerations are in place to address cybersecurity investments required by NIS2?

## 03 CISO, CIO, CTO, Director IT

- What steps are being taken to enhance cybersecurity measures in light of the NIS2 requirements?
- What processes are in place to monitor and report on our adherence to NIS2 regulations?
- How can we proactively address any compliance gaps identified during NIS2 assessments?

### Trusted Advisor Tip

CISO or Compliance Managers do not always talk to their CEOs. You can help them address the NIS2 Compliance urgency and help them secure sufficient budget to get it done.

You can also raise the business outcome issue of risk management with the CEO – supporting the CISO in getting budget for risk management.

# Building your NIS2 business outcome narrative

Your NIS2 sales briefing and customer facing deck should cover the following

- Why You? Explain your competency for supporting NIS2 compliance attainment
- Why them? Why do they need to be NIS2 compliant? Explain the relevance of NIS2 for their specific industry and business context
- Outline your customized approach to achieving compliance. The steps you will take them through and why
- Next steps

## Trusted Advisor Tip

Education and asking disruptive questions will position you as a trusted advisor

Are you familiar with the legal requirements for NIS2?

Does your insurance cover your NIS2 exposures and potential penalties?

Do your employees have a plan for connection usage and data sharing from remote locations (home, internet café, airport, hotel...)?

# Building your NIS2 business outcome narrative

Some of your answers may be a version of .....

"NIS2 isn't just about technology; it's about safeguarding an entire organization.

CEOs and top-level leadership must engage in this critical dialogue to protect their business, ensure resilience, demonstrate leadership and navigate the evolving cybersecurity landscape.

As your trusted IT partner, we bring a unique blend of expertise and commitment to ensuring NIS2 compliance. Here's why you should choose us:

- 01** Deep Understanding of NIS2: We've immersed ourselves in the intricacies of NIS2. Our team stays up-to-date with the latest requirements, ensuring that your organization not only meets the baseline but also goes beyond compliance.
- 02** Tailored Solutions: Compliance isn't a one-size-fits-all approach. We'll assess your specific needs, industry context, and existing infrastructure to create a customized roadmap. Our solutions align with your business goals while enhancing security.
- 03** Holistic Approach: NIS2 isn't just about checkboxes; it's about cyber health. We focus on end-to-end security, from risk assessment to incident response. Our comprehensive approach covers technical, organizational, and procedural aspects.
- 04** Proven Track Record: Our success stories speak for themselves. We've helped organizations across sectors achieve compliance. From critical infrastructure providers to digital services firms, we've navigated the complexities effectively.
- 05** Collaboration and Training: We'll train your team, ensuring they understand NIS2 requirements and can proactively manage risks.
- 06** Responsive Support: Compliance isn't a one-time event. We're here for ongoing support, monitoring, and adjustments. Our commitment extends beyond implementation.

# Identify NIS2 sales and marketing triggers

Your customer triggers will be based on your specific customer knowledge, but some to consider

## End-of-Life Systems and Software

Organizations using outdated systems or software face higher risks

Identify clients still relying on legacy technology that may not meet NIS2 requirements

Position your services as a solution for upgrading and ensuring compliance

## Incident History and Vulnerabilities

Analyze past security incidents and vulnerabilities

Organizations with a history of breaches or vulnerabilities are more likely to prioritize compliance

Highlight how NIS2 can enhance their security health

## Budget Allocations and Priorities

Organizations allocating budget for cybersecurity enhancements are likely to invest in NIS2 compliance.

Understand their spending priorities and align your proposal accordingly.

## Management Awareness and Accountability

Gauge management awareness of NIS2 and its implications.

Organizations with proactive leadership are more likely to prioritize compliance.

Engage decision-makers directly to discuss compliance strategies.

# Identify your NIS2 Sales and Marketing approach

Your approach will be based on your previous best practices, but some to consider

- Digital campaigns
- Social advertising
- Educational workshops or webinars
- 1:1 account reach-outs
- Tailored assessments and gap analysis
- Thought leadership educational content
- Podcasts

Check Campaign in a Box content for NIS2  
<https://aka.ms//NIS2-Security>

# NIS2 Partner Resources

## Partner Enablement Gallery: <https://aka.ms//NIS2-readiness>


- All enablement assets stored in one place as they become available
- Detailed Microsoft Solutions x NIS Product Map
- Hyperlinks to previous and upcoming webinars on NIS2
- Other useful assets

## NIS2 Campaign-in-a-box: <https://aka.ms//NIS2-Security>

- Customizable marketing assets to combine with your GTM efforts
- Very useful to share with your own sellers esp. the nurture email templates!

### Network and Information Systems 2 (NIS2) Directive series

LEARNING PATH  
Last Modified 2024-01-24



The Network and Information Systems 2 (NIS2) Directive is set to be the most comprehensive European cybersecurity directive yet. It covers 15 different sectors and comes into effect in Oct 2024.


The directive aims to harmonize cybersecurity requirements and their enforcement across member states by setting a benchmark of "minimum measures," which include risk assessments, policies and procedures for cryptography, security procedures for employees who have access to sensitive data, multifactor authentication, and cybersecurity training.

It also directs companies to create a plan for handling and reporting security incidents, as well as managing business operations during and after a security incident.


The following resources have been designed to help you to understand the scope of NIS2 and how you can use the Microsoft Security solutions to support your customers on getting compliant with NIS2.

#### This campaign's content


Showing 1-4 of 4 assets




Level 100 NIS2 webinar  
What NIS2 is and how to prepare your organization and your customers.  
2024-01-24



Level 100 NIS2 webinar PDF  
What NIS2 is and how to prepare your organization and your customers.  
2024-01-24








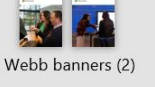
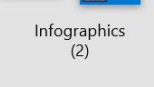


Level 200 NIS2 webinar  
Technical guide on how Microsoft Security solutions map to NIS2.  
2024-01-24



NIS2 campaign in a box  
GTM resources to engage with customers on compliance with NIS2.  
2024-01-24

### NIS2 Campaign Asset Library

PROMOTION	ACQUISITION	CONSIDERATION	DECISION AND ENABLEMENT
 Promo email	 Guide	 Nurture emails (3)	 Pitch deck
 Social ads (#)	 Gated landing page	 Forrester TEI report	
 Webb banners (2)		 Infographics (2)	

To co-sell enabled partners: tag inbound referrals in Partner Center with '#NIS2' @ Marketing Campaign ID &/or Referral Name

# Checklist

- Use guidance in this Playbook for outlining and answering questions on [page 42](#)
  - ✓ Why You? See some examples on [page 43](#)
  - ✓ Why them? See Playbook [Step 1](#) on Choose the right customers/prospects
  - ✓ Outline your customized approach to achieving compliance. See Playbook [Step 2](#) on Create your complete, profitable, recurring NIS2 Offer
- Create a sales briefing document
- Create a customer facing deck



## Step 4:

# Train Sales and Technical Teams

In this section, we cover the points you should cover in sales training to support your sales team in knowing how to engage with customers about NIS2 requirements and objection handling.

# Train your Sales and Technical Teams

Technical Training will be important for delivery of your NIS2 Offer.

- ❑ Check the Resources slides at the end of the Playbook for sales and tech enablement options per readiness level and how to get started

Train your dedicated sales team on:

- ❑ Why this is a C-Level conversation and sale
- ❑ Business outcome narrative (perhaps per customer set)
- ❑ Details around your NIS2 Package
- ❑ Your chosen Sales Motion (event, 1:1 calling ....)
- ❑ Your Offer for supporting NIS2 Compliance
- ❑ A well thought through Q&A for any questions/objection handling
- ❑ Specific Calls to Action (CTAs)



## Trusted Advisor Tip

- NIS2 brings compliance discussions squarely into the boardroom.
- CEOs need to be aware of their direct accountability and potential suspension of duties.
- Highlight how NIS2 compliance aligns with their role in ensuring organizational security

# Objection handling (1/2)

## 01 Objection: "Why should we invest in NIS2 compliance?"

**Responses:** "NIS2 compliance isn't just about ticking boxes; it's about safeguarding your business, reputation, and customer trust. Non-compliance could lead to hefty fines and operational disruptions. Investing in NIS2 compliance ensures your organization's resilience against cyber threats. It's a proactive step to protect critical assets and maintain business continuity."

## 02 Objection: "Our IT department can handle security."

**Responses:** "While IT plays a crucial role, NIS2 compliance is a strategic business issue. It involves leadership accountability, risk management, and legal implications. Absolutely, but NIS2 compliance requires cross-functional collaboration. We'll also work closely with your IT team to implement effective security measures."

## 03 Objection: "It's too complex and costly."

**Responses:** "Complexity is a reality, but the cost of non-compliance can be far higher. Let's focus on risk mitigation and long-term benefits. We'll tailor a cost-effective solution that aligns with your business needs. Compliance pays off in terms of security and reputation."

## 04 Objection: "Our competitors aren't prioritizing NIS2."

**Responses:** "Being proactive sets you apart. NIS2 compliance demonstrates your commitment to security and resilience. True, but forward-thinking organizations gain a competitive edge by staying ahead in cybersecurity. Let's lead the way."

# Objection handling (2/2)

**05** **Objection: "Our existing security measures are sufficient."**

**Responses:** "NIS2 raises the bar. Let's assess your current measures and enhance them to meet evolving threats. Agreed. NIS2 builds upon existing practices. We'll fine-tune your security posture to align with the directive."

**06** **Objection: "Our industry isn't a prime target."**

**Responses:** "Cyber threats spare no sector. NIS2 covers critical infrastructure, and we're part of it. Even seemingly low-risk sectors face cyber risks. Let's proactively protect your operations."

**07** **Objection: "Our leadership doesn't need to be involved."**

**Response:** "Leadership accountability is key. We'll help you champion NIS2 compliance and ensure alignment."

**08** **Objection: "We'll handle it internally."**

**Response:** "Absolutely. Our expertise complements your internal efforts for a robust NIS2 strategy."

**09** **Objection: "We'll wait until the deadline."**

**Response:** "Proactivity pays off. Let's start now to avoid last-minute rush and ensure compliance. Starting early ensures a smooth transition. Let's stay ahead of the curve."



# Frequently asked questions (1/2)

## Q: Can Microsoft solutions ensure full compliance with NIS2 across all sectors?

A: Microsoft solutions provide a robust foundation for NIS2 compliance across various sectors by offering extensive security, compliance, and privacy management features. However, full compliance also depends on how these solutions are implemented and integrated into an organization's specific operations and compliance strategies.

## Q: Are there any specific industries that benefit more from Microsoft's security & compliance solutions?

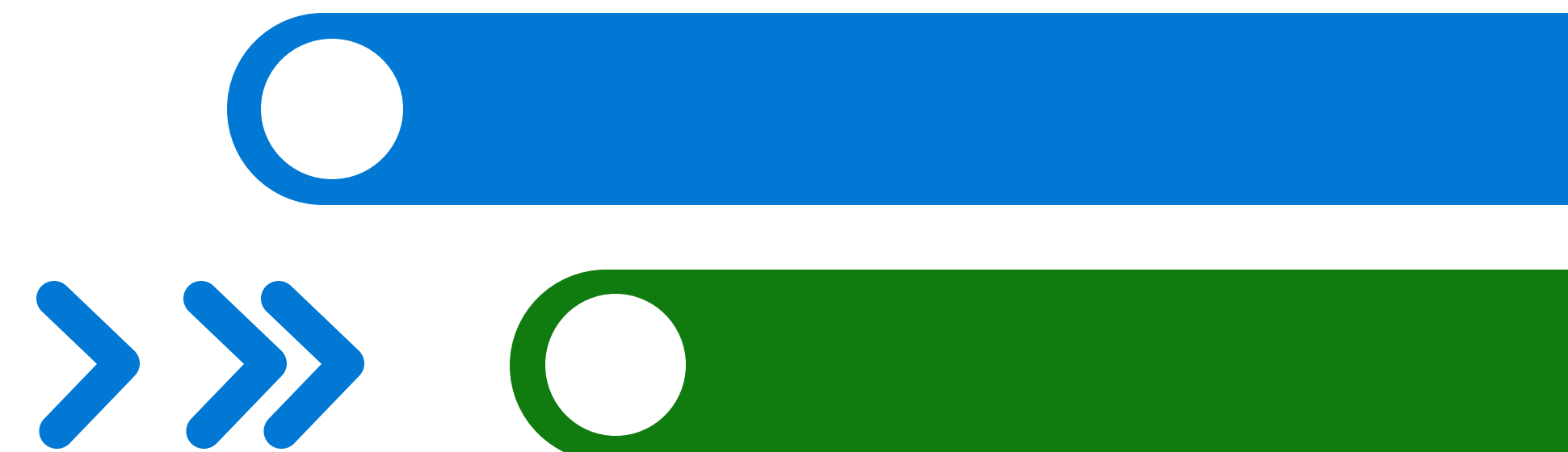
A: While Microsoft's security and compliance solutions are versatile and scalable across a range of industries. Focusing on compliance solutions specifically, sectors with heightened sensitivity to data protection and security regulations, such as healthcare, finance, and public services, may find particular value in the comprehensive features offered by M365 Security, Purview, and Priva. These sectors are also subject to NIS2.

## Q: How does Microsoft keep its compliance solutions updated with evolving NIS2 requirements?

A: Microsoft continuously monitors regulatory developments and updates its compliance solutions to reflect new requirements and best practices. This includes regular software updates, enhancements to security and compliance features, and the provision of up-to-date guidance and resources through the Microsoft Trust Center and other channels.

## Q: Does Microsoft have to comply with NIS2?

- We fall within the scope of the NIS 2 Directive.
- We are committed to complying with NIS 2. We are closely monitoring the legislative developments and partnering with policymakers on the elaboration of the implementing acts.
- We have been dedicated to having strong security practices for over 20 years, many of which are now reflected in international standards and best practices. As such, Microsoft has already taken many of the Cybersecurity Risk-Management Measures identified in Article 21 of the NIS2 Directive. Security and trust are corporate values and central to our mission.
- We are dedicated to aiding customers in the adoption of resilient solutions while adhering to the principles of shared responsibility. Microsoft offers an all-in-one suite of security, compliance, and privacy solutions that streamline the journey to achieve NIS2 compliance



# Frequently asked questions (2/2)

## Q: How to respond to customer questions related to the Directive/law itself if I am not a cybersecurity legal expert?

A: Unless you employ an in-house DPO to consult your customers, we'd always recommend customers reach out to preferred cybersecurity legal experts to ensure they receive independent advice based on their organization and sector classification. Microsoft is a technology provider dedicated to aiding customers in the adoption of resilient solutions while adhering to the principles of shared responsibility. Microsoft offers an all-in-one suite of security, compliance, and privacy solutions that streamline the journey to prepare for NIS2.

## Q: What would be the first step to offer to a customer once NIS2 is brought into conversation?

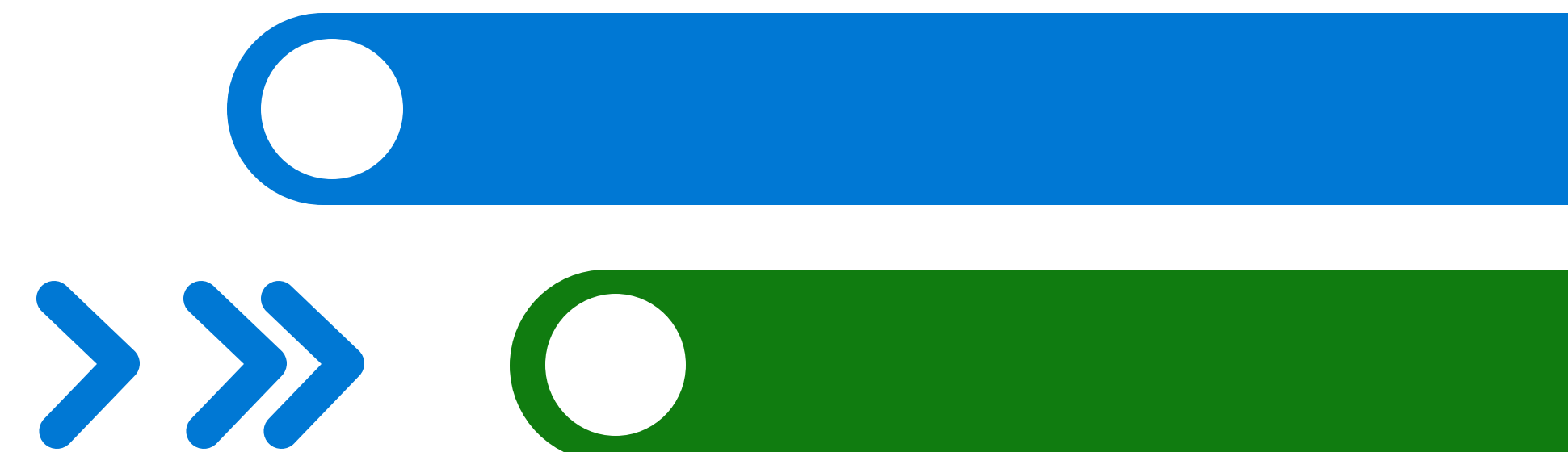
A: The recommended and most common next step is conducting a cloud solution assessment of the customer infrastructure to understand its preparedness for NIS2 in depth, potential gaps and build a tailored to the results plan. In many cases, customers already have technology that can help them meet some NIS2 requirements, though often that has to be deployed, and have to acquire new solutions for what they are missing, i.e. data security, supply chain security. Microsoft funds free assessments for customers delivered by partners if they don't have the IP or don't want to invest in building your own cloud solution assessment. Reach out to your designated Microsoft contact to find out more.

## Q: What is the ideal Microsoft solution for SMB customers subject to NIS2?

A: We recommend Microsoft Business Premium and, depending on their business, Azure Security elements. However, every customer is different and would have different gaps they need to address relevant to NIS2. Always make sure to check the latest Customer Maturity x NIS2 Matric on Microsoft's [NIS2 Partner Training Gallery](#).

## Q: What is the ideal Microsoft solution for Mid size to Enterprise customers subject to NIS2?

A: We recommend Microsoft M365 E5 in combination with Azure Security (Defender for Cloud and Microsoft Sentinel. However, every customer is different and would have different gaps they need to address relevant to NIS2. Always make sure to check the latest Customer Maturity x NIS2 Matric on Microsoft's [NIS2 Partner Training Gallery](#).



# Checklist

- Train your sales & technical team
- Follow-up with a sales briefing document
- Provide them with a list of their target customers and appropriate Calls to Action (CTAs)

# Additional Resources





# FY24 Partner Sales Enablement Options

## Sales

### Sales Bootcamps

This multi-day sales training led by Microsoft sales specialists focuses on providing advanced knowledge for selling the four Microsoft Cloud solution areas. Become proficient at starting sales conversations, solving customer challenges, pitching Microsoft cloud value, and overcoming objections by showcasing real-time customer benefits.

**Capabilities Achieved:** Build Solution Area pipeline and sell the Microsoft Cloud

**Duration:** Multi-(part)day live deliveries

**Roles:** Sellers, BDM's, Solution Sellers

### Microsoft Cloud Executive Enablement Series (Podcast and Vodcast)

This series provide partners with a front row seat to discussions hosted by Microsoft senior leaders and experts on the latest cloud trends and technologies. Gain a unique perspective on the business value of the Microsoft Cloud and ways to engage with customers.

**Capabilities Achieved:** Executive strategy for achieving business outcomes with the Microsoft Cloud

**Duration:** 15-30 minute on-demand videos

**Roles:** Executives, Sales Leaders, Sellers

### Partner Sales Acceleration Program (PSAP)

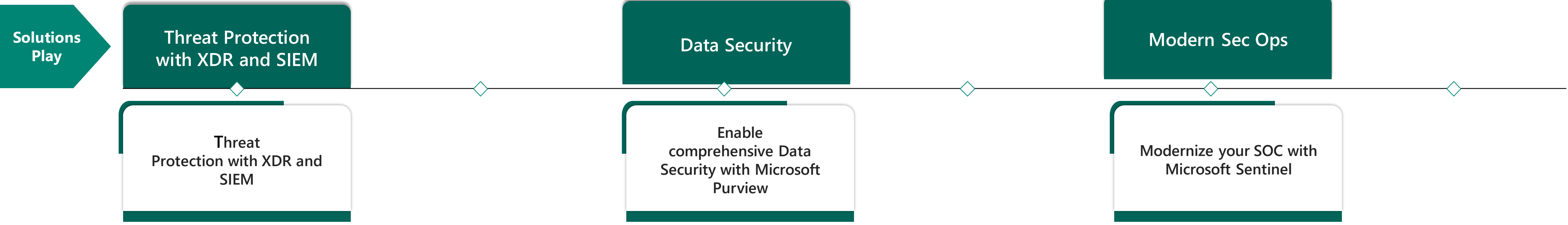
This program offers best practices and presentation resources that will guide you in shaping a business-first sales model. It will help you navigate the six "moments that matter" conversations with various decision makers who will ultimately select the company to implement their solution.

**Capabilities Achieved:** Increase knowledge across the Microsoft Cloud & build solid sales strategies

**Duration:** 2-3 hours per Solution Area, on-demand

**Roles:** Sellers, BDM's, Sales Leaders

# Security Sales Enablement



## Threat Protection with XDR and SIEM

- The state of cybersecurity and defense systems
  - Supercharging threat detection and defense
- A look into attacks
  - Microsoft SIEM & XDR solutions
- Microsoft Security Copilot
  - Identity Threat Detection and response
- Defending endpoints and cloud apps
  - Managing vulnerability and external attack surface
- Why Microsoft?

## Enable comprehensive Data Security with Microsoft Purview

- Data Security challenges
  - Microsoft's solution – Microsoft Purview
- Information Protection
  - Insider Risk Management
- Data Loss Prevention
  - Adaptive Protection
- End to end demo scenario
  - Why Microsoft Purview?
- Customer evidence
  - Licensing
- Getting started with Data Security

## Modernize your SOC with Microsoft Sentinel

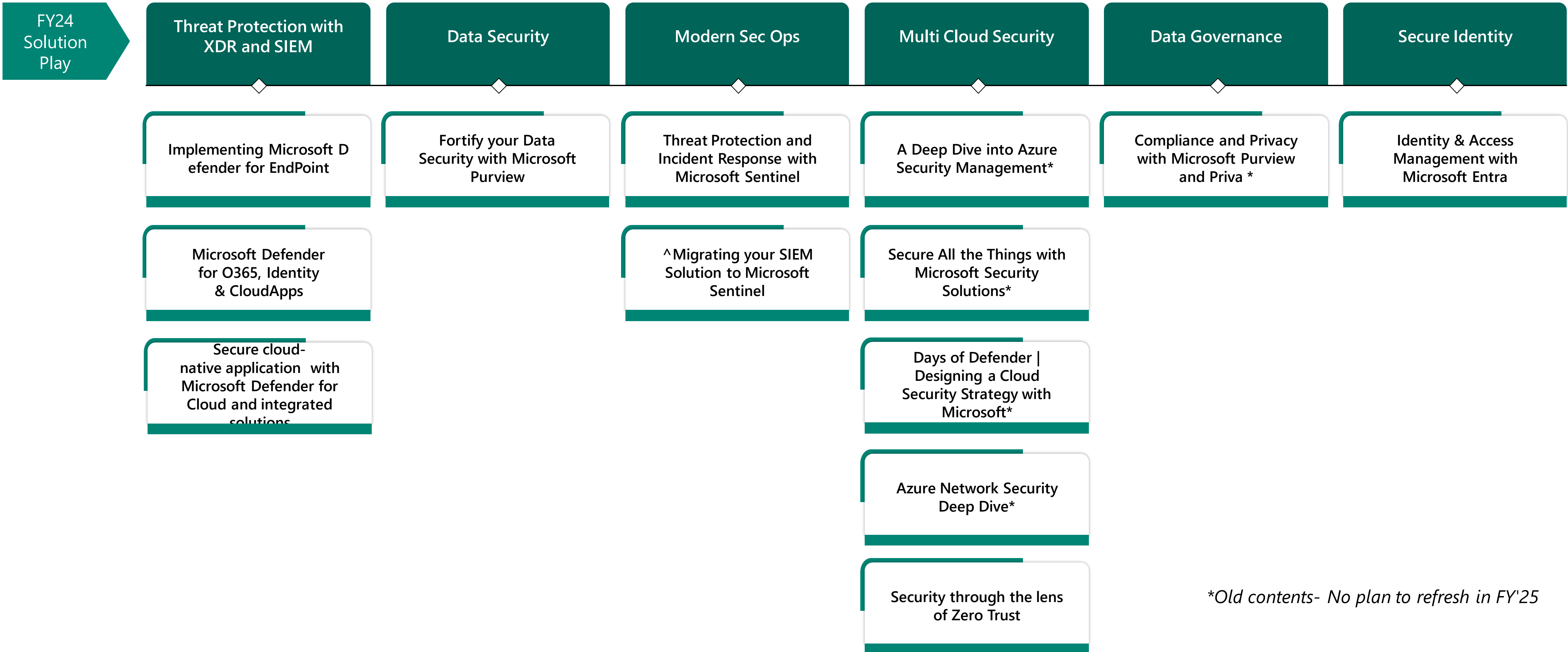
- Security challenges and Microsoft Sentinel
  - Simplified threat protection and response strategy
- Business and Technical capabilities
  - Data collection and archiving
- Better SIEM and XDR protection
  - Microsoft Sentinel and AI with Security Copilot
- Why Microsoft?
  - Saving costs with Microsoft Sentinel
- Customer momentum
  - Get Started
- Partner Guidance

# Security Depth Technical Enablement



Below sessions are available either as On-Demand or as an upcoming live sessions here : [Technical Depth Bootcamps](#)

*\*Please note that not all sessions are available as of today and we keep adding more contents as we build.*



*\*Old contents- No plan to refresh in FY'25*

# Learning plan: Threat Protection and Incident Response

## AUDIENCE

Targeted for security operational professionals that design and manage their threat protection and response systems.

- User who collaborates with organizational stakeholders to secure information technology systems.
- Goal is to reduce organizational risk by rapidly remediating active attacks in the environment.
- Advises on improvements to threat protection practices.
- Refers violations of organizational policies to appropriate stakeholders.

Relevant partner roles:

- Security consultant/architect
- Endpoint Security consultant
- SOC analyst

### Legend

- Workshop
- Bootcamp
- Microsoft Learn

## Beginner

### Security, Compliance, Identity Fundamentals (SC-900)

#### Learning path

##### [MS Learn](#)

- Describe the concepts of security, compliance, and identity
- Describe the capabilities of Microsoft security solutions

## Intermediate

### Microsoft Security Operations Analyst (SC-200)

#### Learning path

##### [Available now](#)

- Microsoft Defender for Endpoint Microsoft 365 Defender
- Mitigate threats using Microsoft Defender for Cloud
- Configure your Microsoft Sentinel environment
- Perform threat hunting in Microsoft Sentinel

## Advanced

### Implementing Microsoft Defender for EndPoint

#### [Check Upcoming/Ondemand events](#)

- Zero Trust & Deploying MDE
- Onboarding and configuring Devices

### Secure cloud-native application with Microsoft Defender for Cloud and integrated solutions

#### [Check Upcoming/Ondemand events](#)

- Microsoft Defender for Cloud, Defender for DevOps and Defender Integration with Microsoft Sentinel

### Microsoft Defender for O365, Identity & Cloud Apps

#### [Check Upcoming/Ondemand events](#)

- M365 Defender and MDO
- Securing SaaS apps with Defender for Cloud Apps
- Protecting cloud environment with MDI

### Threat Protection and Incident Response with Microsoft Sentinel

#### [Check Upcoming/Ondemand events](#)

- Deploying Microsoft Sentinel
- Threat Intelligence and Investigation
- UEBA analytics architecture

### Other training resources

Microsoft Defender for Endpoint Ninja Course, [Self-guided blog](#)

Microsoft 365 Defender Ninja Course, [Self-guided blog](#)

Microsoft Defender for Cloud Apps Ninja Course, [Self-guided blog](#)

Microsoft Defender for IoT Ninja Training, [Self-guided blog](#)

Microsoft Defender for Identity Ninja Course, [Self-guided blog](#)

Security Community Technical Webinars, [Stay updated](#)

# Learning plan: Microsoft Sentinel

## AUDIENCE

Targeted for security operational professionals that design and manage their threat protection and response systems.

- User who collaborates with organizational stakeholders to secure information technology systems.
- Goal is to reduce organizational risk by rapidly remediating active attacks in the environment.
- Advises on improvements to threat protection practices.
- Refers violations of organizational policies to appropriate stakeholders.

Relevant partner roles:

- SOC analyst
- Security operations team
- SIEM/XDR team

### Legend

- Workshop
- Bootcamp
- Microsoft Learn

## Beginner

### Security, Compliance, Identity Fundamentals (SC-900)

#### Learning path

##### [MS Learn](#)

- Describe the concepts of security, compliance, and identity
- Describe the capabilities of Microsoft security solutions

## Intermediate

### Microsoft Security Operations Analyst (SC-200)

#### Learning path

##### [Available now](#)

- Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
- Configure your Microsoft Sentinel environment
- Connect logs to Microsoft Sentinel
- Create detections and perform investigations using Microsoft Sentinel
- Perform threat hunting in Microsoft Sentinel

## Advanced

### Migrating your SIEM Solution to Microsoft Sentinel

#### [Check Upcoming/Ondemand events](#)

- Microsoft Sentinel basic concepts
- Planning the migration
- Migrating to Microsoft Sentinel from the Legacy SIEM
- Post-migration optimization

### Threat Protection and Incident Response with Microsoft Sentinel

#### [Check Upcoming/Ondemand events](#)

- Deploying and configuring Microsoft Sentinel
- Threat Intelligence and Investigation
- UEBA analytics architecture

## Other training resources

Microsoft Sentinel Ninja Course, [Self-guided blogz](#)

Security Community Technical Webinars, [Stay updated](#)

# Data Security Learning Journey

## AUDIENCE

Targeted for those who plan and implement controls that meet organizational compliance needs.

- User who plans and implements controls that meet organizational compliance needs.
- Responsible for translating requirements and compliance controls into technical implementation.
- Assists organizational control owners to become and stay compliant.
- Creates policies and rules for content classification, data loss prevention, governance, and protection.

Relevant partner roles:

- Compliance teams
- Data security teams
- Cloud architects
- Implementation consultants

### Legend

- Workshop
- Bootcamp
- Microsoft Learn

## Beginner

### Security, Compliance, Identity Fundamentals (SC-900)

#### Learning path

##### [MS Learn](#)

- Describe the concepts of security, compliance, and identity
- Describe the capabilities of Microsoft compliance solutions

## Intermediate

### Microsoft Purview Information Protection Administrator (SC-400)

#### Learning path

##### [Available now](#)

- Implement Information Protection in Microsoft 365
- Implement Data Loss Prevention
- Implement Data Lifecycle and Records Management

## Advanced

### Fortify your Data Security with Microsoft Purview

#### [Check Upcoming/Ondemand events](#)

- Identify and protect sensitive data across your hybrid environment using Purview Information protection
- Prevent accidental leakage of sensitive information using Purview Data Loss Prevention (DLP)
- Intelligently detect and mitigate critical risks with Microsoft Purview Insider Risk Management

## Other training resources

Become a Microsoft Purview eDiscovery Ninja: [Self-guided blog](#)

Microsoft Purview Information Protection Ninja Course: [Self-guided blog](#)

Microsoft Purview Data Loss Prevention Ninja Training : [Self-guided blog](#)

The Microsoft Cloud App Security (MCAS) Ninja Training: [Self-guided blog](#)

Microsoft Compliance Manager (MSCM) Ninja Training: [Self-Guided blog](#)

Microsoft Purview One-Stop-Shop (OSS) [Self-guided site](#)

# Cloud Security Learning Journey

## AUDIENCE

Targeted for individuals who manage the security of their Azure and third-party software as a service (SaaS) cloud environments.

- Users who plan and implement controls to meet organizational security and compliance needs.
- Those responsible for translating requirements, and security and compliance controls into technical implementation.
- Those who help organizational control owners manage cloud security for Microsoft and third-party platforms according to organizational requirements.
- Those who create policies and rules for data loss prevention, IaaS/PaaS security, virtual networking security and governance, and protection of cloud assets.

Relevant partner roles:

- Azure administrators
- Security teams
- Data security owners
- Cloud Architects
- Implementation consultants

### Legend

- Workshop
- Bootcamp
- Microsoft Learn

## Beginner

### Security, Compliance, Identity Fundamentals (SC-900)

#### Learning path

##### [MS Learn](#)

- Microsoft 365 Defender
- Secure your cloud applications in Azure
- Implement resource management security in Azure
- Implement network security in Azure

## Intermediate

### Azure Security Engineer (AZ-500)

#### Learning path

##### [Available now](#)

- Safeguard multi-cloud apps and resources with cloud security solutions from Microsoft
- Implement virtual machine host security in Azure
- Manage identity and access in Azure Active Directory
- Manage security operations in Azure

## Advanced

### Azure Security Management Deep Dive

##### [Check Ondemand events](#)

### Secure All Things with Microsoft Security solutions

##### [Check Ondemand events](#)

### Designing a Cloud Security Strategy with Microsoft

##### [Check Ondemand events](#)

## Other training resources

Microsoft Defender for Cloud Ninja Training [Self-guided blog](#)

Microsoft Cloud App Security (MCAS) Ninja Training, [Self-guided blog](#)

Azure Network Security Ninja Training [Self-guided blog](#)

Security Community Technical Webinars [Stay updated](#)

# Fortify your Data Security with Microsoft Purview

In this workshop you will understand how Microsoft Purview delivers comprehensive data security by integrating information protection, data loss prevention and insider risk management. You will learn how Microsoft Purview Information Protection helps you discover, identify, classify, and protect sensitive data that is business critical, then manage and protect it across your environment. With Data Loss Prevention, you can automatically protect sensitive information from risky and unauthorized access across apps, services, endpoints, and on-premises files. Insider Risk management features in Microsoft Purview can help you detect, investigate, and take action on critical risks in your organization, including data theft, data leaks, and security policy violations. As a Microsoft partner, you can use this knowledge to help your customers understand and mitigate their data risks.

## Duration

3 days (4 hrs/day)

## Level

Intermediate

## Hands on Labs

Yes

## Course Prerequisites

None

## Target Audience

Technical

## Suggested Supplementary Certification

SC-400



Security



Data Security

## Day 01

### Identify and protect sensitive data across your hybrid environment using Purview Information protection

- Why Data security?
- Microsoft's approach to Data Security
- Microsoft Purview Information protection
- Sensitive Information types
- Trainable Classifiers
- Content and Activity Explorer
- Sensitivity Labels and Policy
- Encryption
- Double Key Encryption
- Ecosystem and Extensibility

### Hands on Labs

- Assigning Compliance Roles and exploring Microsoft Purview portal
- Managing Sensitive Information Types
- Managing Trainable Classifiers
- Working with Sensitivity Labels

## Day 02

### Prevent accidental leakage of sensitive information using Purview Data Loss Prevention (DLP)

- Challenges with preventing data leakage
- Microsoft Purview Data Loss Prevention overview
- Prepare for DLP
- DLP Policy
- DLP endpoint policy
- On-premises DLP
- Working with Alerts
- Adaptive Protection

### Hands on Labs

- Deploy Double Key Encryption
- Creating and Managing DLP Policies

**Available as On-demand on LevelUp or Join the upcoming Live session [Security Depth \(on24.com\)](#)**

## Day 03

### Intelligently detect and mitigate critical risks with Microsoft Purview Insider Risk Management

- Insider Risk challenges
- Microsoft Purview Insider Risk Management Solutions Overview
- DLP vs Insider Risk Management
- Communication Compliance
- Insider Risk Management
- Analytics Setup
- Information Barriers
- Privileged Access Management
- Protect User and device access
- Customer Lockbox

### Hands on Labs

- Configuring Insider Risk Management
- Exploring the capabilities of Adaptive Protection
- Configuring Communication Compliance
- Configuring Information Barriers

**Recommended for all MW/Security Partners**



# Security Ninja Trainings – Step up you game

Security Ninja Course	Link	Alignment to Solution Play/Workloads
Microsoft Defender for Cloud Apps:	<a href="#">Microsoft Defender for Cloud Apps Ninja Training: June 2022 Update - Microsoft Community Hub</a>	Threat Protection ,Cloud Security , Information Protection & Governance
Defender for Endpoint:	<a href="#">Become a Microsoft Defender for Endpoint Ninja - Microsoft Community Hub</a>	Threat Protection
Defender for Identity	<a href="#">Microsoft Defender for Identity Ninja Training - Microsoft Community Hub</a>	Threat Protection ,Identity and Access Management
Microsoft 365 Defender	<a href="#">Become a Microsoft 365 Defender Ninja</a>	Threat Protection
Defender for Office 365	<a href="#">Defender for Office 365 Ninja Training (microsoft.com)</a>	Threat Protection
Microsoft Sentinel:	<a href="#">Become a Microsoft Sentinel Ninja: The complete level 400 training - Microsoft Community Hub</a>	Microsoft Sentinel
Microsoft Sentinel Notebooks	<a href="#">Azure Sentinel notebook ninja - the series! (microsoft.com)</a>	Microsoft Sentinel
Microsoft Sentinel Automation Ninja:	<a href="#">Become a Microsoft Sentinel Automation Ninja! - Microsoft Community Hub</a>	Microsoft Sentinel
Microsoft Defender for Cloud:	<a href="#">Become an Azure Security Center Ninja (microsoft.com)</a>	Cloud Security
Microsoft Defender Threat Intelligence:	<a href="#">Become a Microsoft Defender Threat Intelligence Ninja: The complete level 400 training</a>	Threat Protection
Azure Network Security:	<a href="#">Azure Network Security Ninja Training - Microsoft Community Hub</a>	Cloud Security
Microsoft Defender for IoT:	<a href="#">Microsoft Defender for IoT Ninja Training - Microsoft Community Hub</a>	Threat Protection
Microsoft Purview Information Protection:	<a href="#">The Microsoft Purview Information Protection Ninja Training is here! - Microsoft Community Hub</a>	Information Protection & Governance
Microsoft Purview eDiscovery:	<a href="#">Become a Microsoft Purview eDiscovery Ninja - Microsoft Community Hub</a>	Information Protection & Governance
Microsoft Purview Data Loss Prevention:	<a href="#">The Microsoft Purview Data Loss Prevention Ninja Training is here! - Microsoft Community Hub</a>	Information Protection & Governance
Microsoft Compliance Manager (MSCM):	<a href="#">Microsoft Compliance Manager Ninja Training</a>	Information Protection & Governance
Communication Compliance:	<a href="#">Become a Communication Compliance Ninja - Microsoft Community Hub</a>	Information Protection & Governance
Insider Risk Management:	<a href="#">Become an Insider Risk Management Ninja - Microsoft Community Hub</a>	Threat Protection
Must Learn KQL:	<a href="#">GitHub - rod-trent/MustLearnKQL: Code included as part of the MustLearnKQL blog series</a>	Microsoft Sentinel
Attack Simulation Training:	<a href="#">Attack Simulation Training   Virtual Ninja Training with Heike Ritter - YouTube</a>	Threat Protection



# Best way to get started

For more information and to Get Started!

[Leahanne.Hobson@Alinea-Partners.com](mailto:Leahanne.Hobson@Alinea-Partners.com)

1

## **Do your Capability Assessment for NIS2**

Know your Portfolio and Capability Status Quo to understand what you are missing and get recommendations to get started. This will support your NIS2 Offer Development and Training requirements.

2

## **Offer Development**

Create your NIS2 Offer/Service Package.  
→ consider P2P: Option Cyber Basics demo

3

## **Train your Technical Team on Microsoft Security Portfolio**

Get ready on the technology side.

4

## **Train your Sales Team on your NIS2 Offer and Sales Motions**

Get ready to sell to business leadership.

5

## **Go Sell!**