# Collaboration between Microsoft and the Danish universities on cybersecurity/Microsoft Defender for X)

# Before we start… Introduction

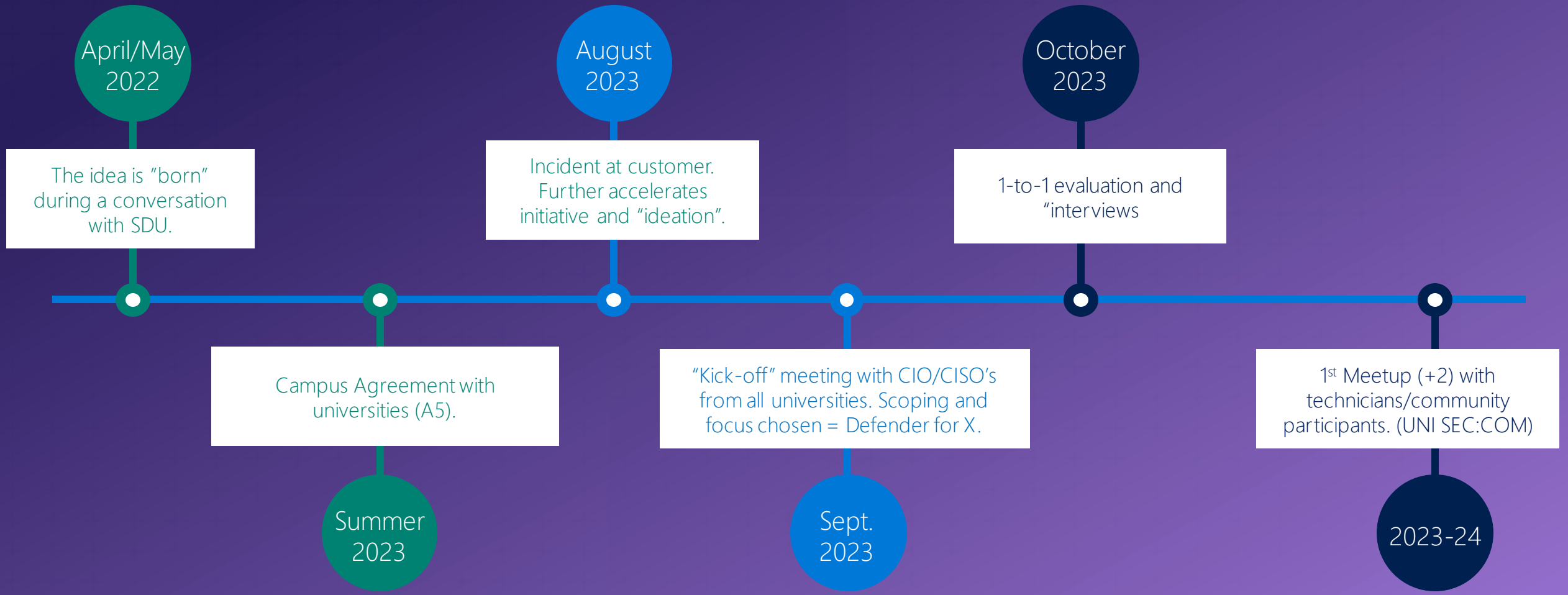
**Bjarke Larsen**
Account Technology Specialist
Higher EDU
Bjlarsen@microsoft.com
Mobile: +45 61780667

- Worked at Microsoft for 6 years.
- My role:“Bridge-builder” & “Translator”
- Focused on enabling you to be successful (on *our* platform)
- *“Don’t re-invent the wheel”*
- *“Steal with pride”?*

# Todays agenda:

| | |
|---|---|
| 16:30 – 16:35 | A timeline on the collaboration. |
| 16:35 – 16:40 | Setting the stage… |
| 16:40 – 16:45 | Looking back: Learnings, reflections and findings |
| 16:45 – 16:50 | How we work together: Status, cadence, activities and format |
| 16:50 – 16:55 | Looking ahead: Focus for 2024. |
| 16:55 – 17:00 | Aligment and “asks” between stakeholders. |

# Timeline: From idea until now



# Disclaimer

**When working with 9 different organization's and with a large variety of people and competences. The following challenges, achievements, insights and recommendations are generalizations based on the shared experiences between Microsoft and the community members.**

**The *generalization* is our perceptions – NOT facts! Talk to your own people to learn more.**

# Setting the stage…

- Microsoft have a shared agreement with all member organizations (A5)
- Focus is on heightening security, activation and hardening.
- Create a safe space to share concerns and learnings
- Members are encouraged to share best-practice and knowledge
- Work towards a “University security base-line”
- Utilize (free) programs, offerings and SME from vendor/Microsoft.

# Looking back: Some numbers…

- The community have **46 members**
- There have been **29 “ask for help”/discussions** resulting in **29 solutions/”case closed”**
- Free offerings (Fasttrack/MCI) have been used **5 times.** To accelerate and upskill members (workshop, training).
- **11 members** joined the free SC-200 SOC training
- **~30 security-related meetings** between Microsoft and members
- **3 successful in-person “Meet-ups”**☺

# Looking back: Some words…

- Community achievements-to-date:
  - Members are activily participating - Sharing more questions, opportunities and challenges.
  - (Mostly) Succeeded in what we set out to do!
  - Showed resilience and commitment to the task(s) and community.
  - Understood our current limitations (time, people, competences)
  - Onboarded more people to the organizations (and community)
  - Started training and planning for the future
  - Involved and utilized each other, programs, offerings and partners
  - Great talks and participation in “Open office”/”Meet-ups”

# Looking back: Findings and challenges

- The starting point was/is not the same.
- Every organization is organized and works differently.
- The number of resources  are different – but the job/goal is the same.
- Daily tasks, RoB, processes and ownership of tasks are not clear and/or documented. The mandate, support and trust in the Security team is “blurry”
- The ownership (responsibility/accountability) of the Cybersecurity agenda is owned by…? (“Who owns the security agenda?”)
- It is easy to start – but hard to finish (the tasks)

# Community cadence, activities and format

- A teams-channel for all members →
- Bi-weekly: Open Office
- Monthly: Status on focus-area
- Quarterly: IRL Community Meet-Up.


Future expansions/ideas:

- Community Github Repo [TBD]
- Documentation library
- “80/20 project” template
- Emergency phone-list

# Status on the “Defender for X” → “Traffic light”

| Danish University Cybersecurity Community // Traffic Lights | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | AAU | AU | CBS | DTU | ITU | KU | RUC | SDU |
| **Defender for Endpoints** | | | | | | | | |
| Linux | Sorry – This is confidential ☺ | | | | | | | |
| Servers | | | | | | | | |
| Mac devices | | | | | | | | |
| Windows devices | | | | | | | | |
| **Defender for Idendity** | | | | | | | | |
| Enabled & configured | | | | | | | | |
| **Defender for Office** | | | | | | | | |
| Enabled & configured | | | | | | | | |
| **Other topics** | | | | | | | | |
| Incident Response Plans | | | | | | | | |
| Intune for Mac | | | | | | | | |
| Intune for BYOD | | | | | | | | |
| Backup & Restore - AD | | | | | | | | |
| Backup & Restore - Office365 | | | | | | | | |
| AD-tiering | | | | | | | | |
| Defender for Cloud | | | | | | | | |
| Defender for IoT | | | | | | | | |

# Looking ahead: Community focus and input

What?:

1. Improving collaboration and build trust across teams and organization.
2. Get (consistent) executive support, understand mandate and responsibility
3. A common “vocabulary” and “baseline” (Enabling “Community SOC”?)
4. Clear overview on SME/Point of Contact
5. Work with new and additional insights (E.g. in relation to SOC/SIEM?)
6. How to leverage AI? (Security Co-pilot?)

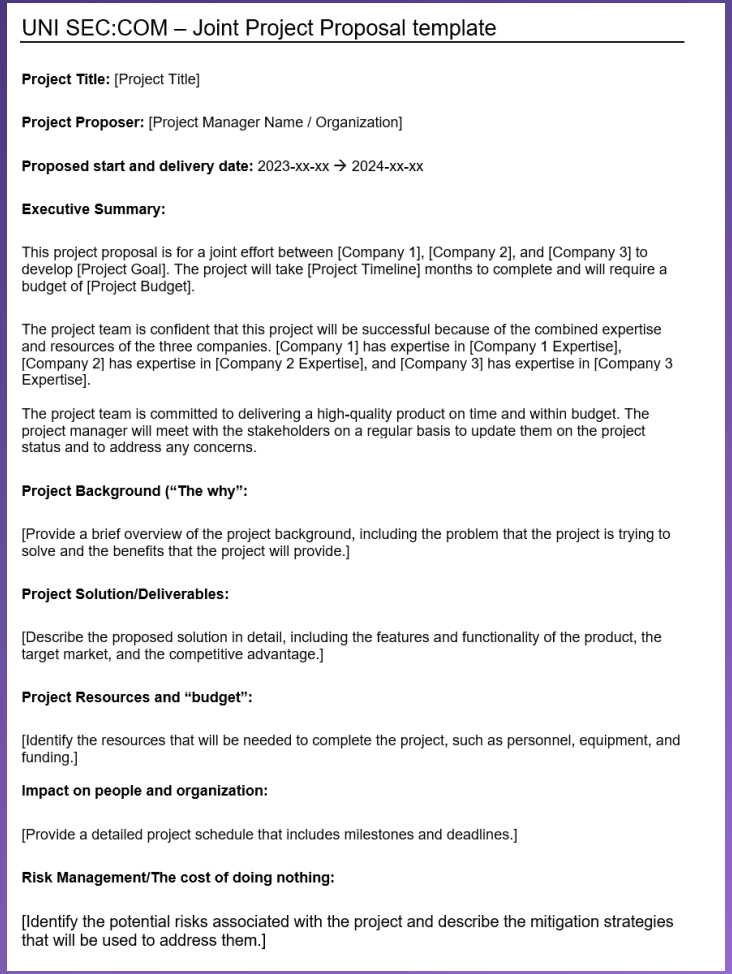
How?:

1. Strengthen collaboration through ***“80/20 projects”*** [WIP]
    1. Standard community template to leadership
    2. Community-driven sprints
2. Looking at options for “how-to-enable” a “Community SOC”
3. Create a Github repository with: Security Best-practice playbooks/automation rules. [TBD]

# Improving collaboration: “80/20 project” template

Template should capture:

- Show that: “20% effort, 80% value across”
- Answer the “why?”
- What it “cost” (time/$?) and when it is done.
- Who and what it impacts?
- Explain/Highlight “risk”/cost of doing nothing.



UNI SEC:COM – Joint Project Proposal template

**Project Title:** [Project Title]

**Project Proposer:** [Project Manager Name / Organization]

**Proposed start and delivery date:** 2023-xx-xx → 2024-xx-xx

**Executive Summary:**

This project proposal is for a joint effort between [Company 1], [Company 2], and [Company 3] to develop [Project Goal]. The project will take [Project Timeline] months to complete and will require a budget of [Project Budget].

The project team is confident that this project will be successful because of the combined expertise and resources of the three companies. [Company 1] has expertise in [Company 1 Expertise], [Company 2] has expertise in [Company 2 Expertise], and [Company 3] has expertise in [Company 3 Expertise].

The project team is committed to delivering a high-quality product on time and within budget. The project manager will meet with the stakeholders on a regular basis to update them on the project status and to address any concerns.

**Project Background (“The why”:**

[Provide a brief overview of the project background, including the problem that the project is trying to solve and the benefits that the project will provide.]

**Project Solution/Deliverables:**

[Describe the proposed solution in detail, including the features and functionality of the product, the target market, and the competitive advantage.]

**Project Resources and “budget”:**

[Identify the resources that will be needed to complete the project, such as personnel, equipment, and funding.]

**Impact on people and organization:**

[Provide a detailed project schedule that includes milestones and deadlines.]

**Risk Management/The cost of doing nothing:**

[Identify the potential risks associated with the project and describe the mitigation strategies that will be used to address them.]

# Asking each other for help (Community ←→ Leadership)

Some examples on what is being asked about from the “Technicians” to “Leadership”

- It’s a evolving marathon – not a sprint. Be consistent!
- Help us with understanding **our** mandate on where and what we (community members) can/can not “dictate” when it comes to IT security.
- Help make sure senior-leadership (continually) have our back. Especially when it hurts. We will make mistakes!
- Give feedback on ideas and projects on cybersecurity.

# Alignment: Making sure we are heading in the right direction (provides value!)

- What is top-of mind for the **CIO/CISO's?**
  - Focus-area?
  - Strategy?
  - "Must-win battles"?

- Be aware of external "influencers"
  - NIS2?
  - ISO 27XXX?
  - Other regulatory of external demands?
    (E.g. DKCERT/Datatilsynet/Rigsrevisionen/Digitaliserings-styrelsen mfl.)

# Thank you – Open floor/QnA

# Q&A