

Weakest link in Cybersecurity

2023

Petteri Hallikainen, Nordics Cybersecurity Lead





Become cyber-resilient in the
Microsoft Cloud

Learn how Avanade helps you speed innovation, securely, at every step.

Petteri Hallikainen
Nordics Cybersecurity Lead

Talks about #cloudfirst, #cybersecurity, #transformation, #businessstrategy, and #digitalbusinesstransformation

Espoo, Uusimaa, Finland · [Contact info](#)

Avanade
Lappeenrannan teknillinen yliopisto

Responsible for growing the Nordics cybersecurity business with the power of Avanade and the Microsoft and Accenture ecosystem. Doing this by working with a team tasked to provide a holistic approach through advisory, implementation and managed services, to help secure enterprises faster and with less risk – In short Protecting trust - the foundation of every business and organization.



To deliver securely to our customers, we must secure very complex working environment first

We define what matters

Avanade Advisory helps leaders make the most of their investments by identifying and prioritizing practical actions to embrace continual change and drive more business value from Microsoft ecosystem technologies. Our practitioners can help you ready your organization for AI responsibly, make your technology investments work harder, monetize data, break down internal silos, manage change and meet your ESG goals.

We make what matters

Through Avanade X, we use data, creativity and engineering at scale to help businesses imagine beyond their convention, give technology purpose and make what matters. Our Avanade X experts can help you shape powerful customer experiences, create workplace experiences that value and empower your employees, and develop compelling new products and services that build competitive advantage.

We power what matters

With the most certifications and Gold-level competencies of any Microsoft partner, we're uniquely positioned to help businesses grow and seize their greatest opportunities from the Microsoft ecosystem. Whether it's preparing your data for an AI-first world, redefining the future of work or taking full advantage of the cloud, we help you maximize your investment and transform your business.

60,000

**Professionals
working in 28
countries around
the globe**

5,000+

**Clients served
worldwide since
2000**

46%

**Of Fortune 500
companies are
Avanade clients**

18x

**Winner of
Microsoft Global
Alliance SI
Partner of the
Year**



Still, humankind hasn't learned anything



Your personal and company data are protected in this chat

Hello, this is Bing! I'm the new AI-powered chat mode of Microsoft Bing that can help you quickly get **summarized answers** and **creative inspiration** 🧠.

are cybersecurity breaches caused by human error?

✓ Searching for: **cybersecurity breaches human error**

✓ Generating answers for you...



Your personal and company data are protected in this chat

According to the web search results, the answer is yes. Most of the cybersecurity breaches are caused by human error, either intentional or unintentional. The World Economic Forum reported that 95% of all cybersecurity incidents can be traced to human error ¹ ². Some of the common human errors that lead to cybersecurity breaches are downloading infected software, using weak passwords, compromising IP addresses, and not updating the software ³. Therefore, it is important to raise awareness and adopt good practices among users to prevent cyberattacks ⁴.



In most cases it's about human mistakes

Microsoft leaks 38TB, Xbox secrets

Two separate data exposure incidents in one week.

Whoops, Samsung workers accidentally leaked trade secrets via ChatGPT

Toyota Suffers Data Breach from "Mistakenly" Exposed Access Key on GitHub



#1 Priority is therefor People which no tech can replace



Marc Randolph ✓
@mrandolph

I never believed that Netflix would crack down on Password sharing.

I reminded everyone that one of our earliest principles was to “make it easier for people to do what’s right, rather than make it harder to do what’s wrong.”

Implement a formal security framework like zero trust with enforced automation to enable people access and share they work

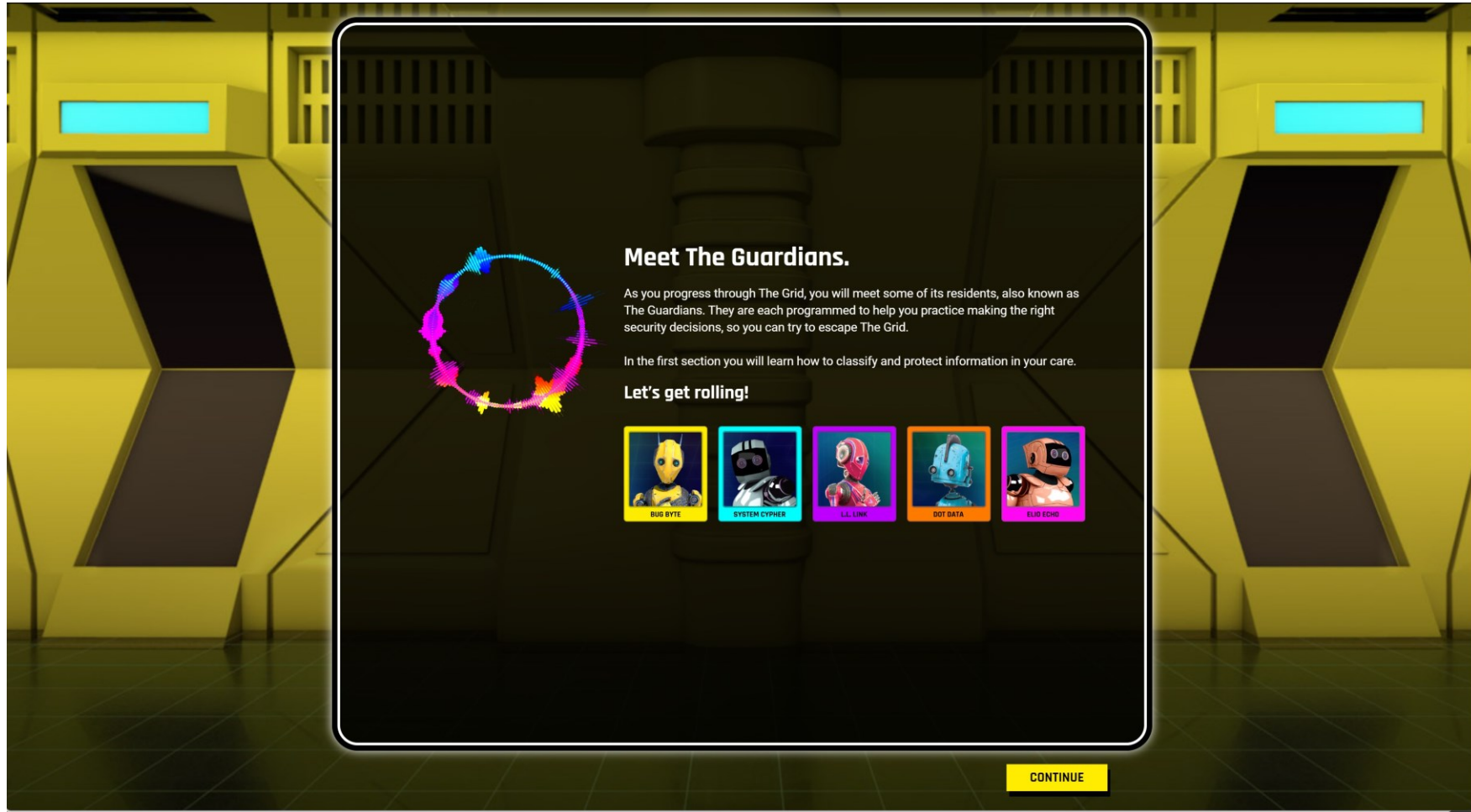
Build employees with strong knowledge about cybersecurity

Create a strong cybersecurity culture and make it every one priority, integral habit on everyday life



Think differently about training and educating

We have taken an approach to build education inside a video games which are employee mandatory trainings



Example how to Prioritize how you develop

Assume

[GitHub - github/safe-settings](https://github.com/github/safe-settings)

Enable

Zero Trust framework

Nobody will read recommendations

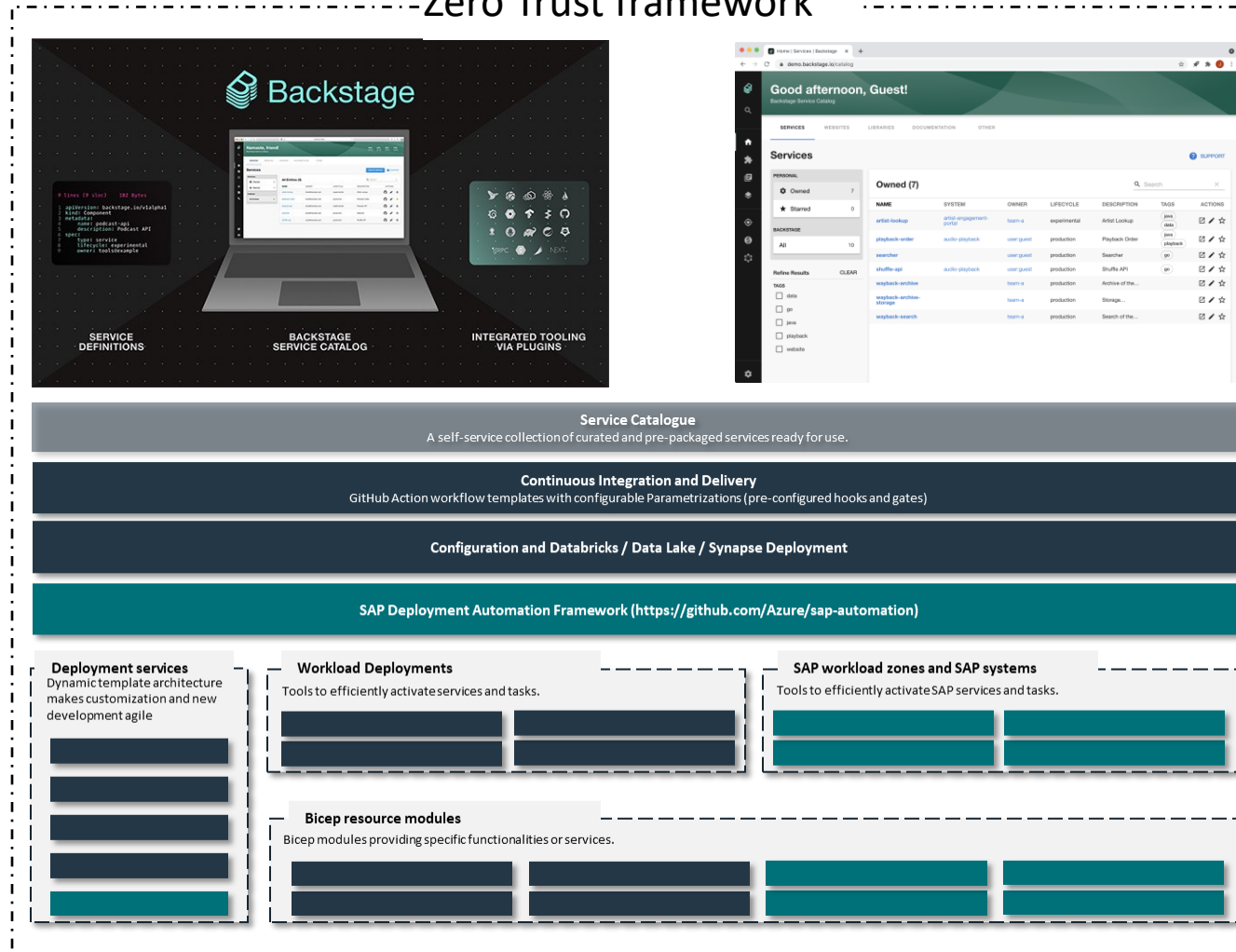
Everyone is under time pressure and hurry

Individuals has their own habits and beliefs

Automate

Enforce

Least-Privilege



Success formula is simple still today

Educate users

Follow a robust security framework

Enforce via Automation

Signaling and Security Graph

Single pane view



Your organization is only ever as secure as its weakest link

Thank you